Security Content Automation Protocol State of the Union

23 September 2008

presented by:

Tim Grance, Program Manager, Cyber and Network Security Program

The National Institute of Standards and Technology

Agenda

- Information Security Current State
- Security Content Automation Protocol
- SCAP Validation Program Status
- Use Cases
- Possible Future Directions for SCAP
- Next Steps for the Community
- Summary

Thoughts on Current State

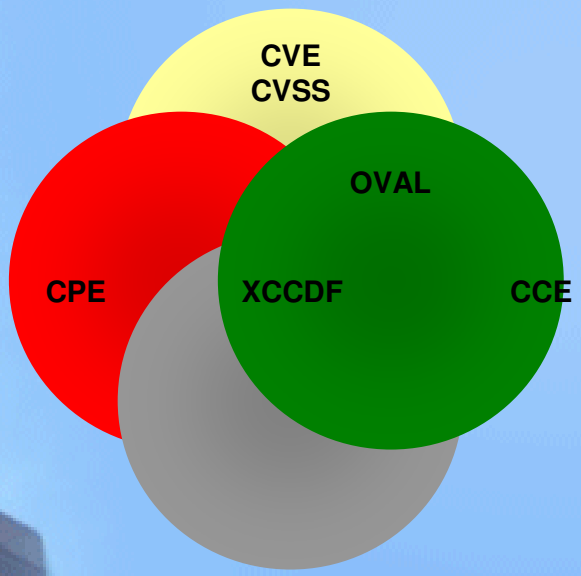
- ***Automation and communication is normally limited to a single discipline*** - vulnerability, compliance, configuration, and asset management remain compartmentalized
- ***Automation and communication usually occurs through proprietary methods*** - therefore data sharing, analysis, aggregation, etc. is typically only possible within a product line
- ***Increasing number of mandates*** - means increasing number of frameworks, standards, regulations, guidelines, sometimes these documents conflict
- ***Relatively static number of security configurations***
- ***Increasing number and complexity of vulnerabilities and threats***

What is SCAP?

How

Standardizing the format by which we communicate

Protocol



What

Standardizing the information we communicate

Content

Sponsored by DHS National Cyber Security Division/US-CERT
National Vulnerability Database
a comprehensive cyber vulnerability resource
NIST National Institute of Standards and Technology

http://nvd.nist.gov

http://checklists.nist.gov

- 70 million hits per year
- 20 new vulnerabilities per day, over 6,000 per year
- Mis-configuration cross references
- Reconciles software flaws from US CERT and MITRE repositories
- Spanish translation
- Produces XML feed for NVD content

SCAP Validation Program Status

As of 19 September 2008, 7 months of operation…

- 9 Accredited labs

Validated Products:

- 11 vendors
- 17 products
- 58 capabilities-based validations
- 12 standards-based validations

…and more to come in 2008.

Use Case: The Office of Management and Budget Federal Desktop Core Configuration

Repeatable Assessments and Uniform Reporting

OMB 31 July 2007 Memo to CIOs: ***Establishment of Windows XP and VISTA Virtual Machine and Procedures for Adopting the Federal Desktop Core Configurations***

July 31, 2007

MEMORANDUM FOR CHIEF INFORMATION OFFICERS

FROM: Karen Evans
Administrator, Office of E-Government and Information Technology

SUBJECT: Establishment of Windows XP and VISTA Virtual Machine and Procedures for Adopting the Federal Desktop Core Configurations

The Office of Management and Budget recently issued policy memorandum M-07-11, "Implementation of Commonly Accepted Security Configurations for Windows Operating Systems," which stated: "agencies with these operating systems [Windows XP and VISTA] and/or plans to upgrade to these operating systems must adopt these standard security configurations by February 1, 2008."

As we noted in the June 1, 2007 follow-up policy memorandum M-07-18, "Ensuring New Acquisitions Include Common Security Configurations," a virtual machine would be established "to provide agencies and information technology providers' access to Windows XP and VISTA images." The National Institute of Standards and Technology (NIST), Microsoft, the Department of Defense, and the Department of Homeland Security have now established a website hosting the virtual machine images, which can be found at: http://csrc.nist.gov/fdcc. The website also includes frequently asked questions and other technical information for adopting the Federal Desktop Core Configurations (FDCC).

Your agency can now acquire information technology products that are self-asserted by information technology providers as compliant with the Windows XP & VISTA FDCC, and use NIST's Security Content Automation Protocol (S-CAP) to help evaluate providers' self-assertions. Information technology providers must use S-CAP validated tools, as they become available, to certify their products do not alter these configurations, and agencies must use these tools when monitoring use of these configurations. Related resources (e.g., group policy objects) are also provided to help facilitate agency adoption of the FDCC.

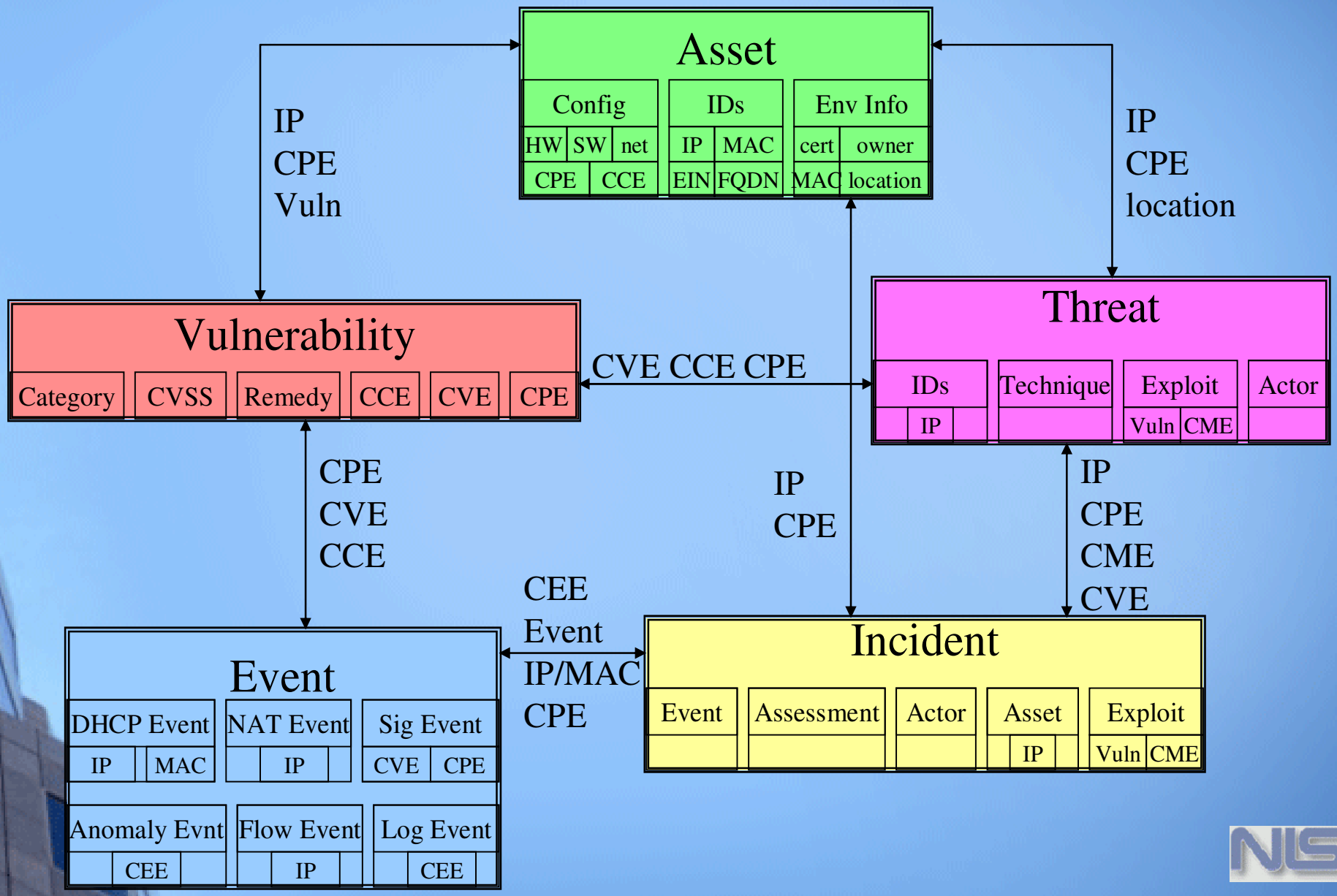
For additional information about this initiative, please call 1-800-FED-INFO. Additional information about the S-CAP can be found at: http://nvd.nist.gov/scap.cfm.

"As we noted in the June 1, 2007 follow-up policy memorandum M-07-18, "Ensuring New Acquisitions Include Common Security Configurations," **a virtual machine would be established "to provide agencies and information technology providers' access to Windows XP and VISTA images."** The National Institute of Standards and Technology (NIST), Microsoft, the Department of Defense, and the Department of Homeland Security have now established a website hosting the virtual machine images, which can be found at: http://csrc.nist.gov/fdcc."

"Your agency can now acquire information technology products that are self-asserted by information technology providers as compliant with the Windows XP & VISTA FDCC, and **use NIST's Security Content Automation Protocol (S-CAP) to help evaluate providers' self-assertions. Information technology providers must use S-CAP validated tools, as they become available, to certify their products do not alter these configurations, and agencies must use these tools when monitoring use of these configurations."**

Use Case: The Office of Secretary of Defense Computer Network Defense Data Pilot

Integrated and Timely Situational Awareness



Use Case: The Payment Card Industry Technical and Operational Reqs for ASVs

Standardized Software Flaw Content and Impact Scores

Version 1.1 of Technical and Operational Requirements for Approved Scanning Vendors (ASVs)

"The **detailed report** must be readable and accurate, and must include the following:

- …
- Detailed statement for each vulnerability found on the customer infrastructure, including:
  - …
  - Industry reference numbers such as CVE, CAN, or Bugtraq ID
  - Severity level - Common Vulnerability Scoring System (CVSS), http://www.first.org/cvss/, base score, as indicated in the National Vulnerability Database (NVD), http://nvd.nist.gov/cvss.cfm (where available)
  - …"

Where Can SCAP Go?

Current SCAP Version

- Continue to reduce the boundary between written specifications and action
- Extend into additional security technologies (e.g., IDS/IPS, firewall)
- Extend into other IT technologies (e.g., asset and configuration management)

Possibilities in the Future

- Expand to implementation and remediation of software flaws and security configurations
- Add impact scoring for security configurations
- Devise methods to group and aggregate software flaws and security configurations
- Feed metrics research into SCAP evolution
- Enhance reporting capabilities

We are open to additional directions, and we want to hear about new use cases

Community Next Steps

- Use SCAP Validated Products
- Publish Checklists in SCAP Format
- Extend SCAP Use Cases
- Take Part in Community Discussions

Summary

- The discipline of Information security is still plagued with inefficiencies
- SCAP seeks to address those inefficiencies through transparency, interoperability, repeatability, uniformity, and ultimately automation
- Proficiency testing through the SCAP Validation Program is well under way - 9 labs, 11 vendors, 17 products, 70 validations
- FDCC, CND Data Pilot, and PCI continue to be viable use cases
- SCAP can be applied to more use cases ‘as is’ and can be evolved for additional functionality
- Everyone has a role to play in making the current state of information security better