Security Content Automation Protocol (SCAP) Validation and the Federal Desktop Core Configuration (FDCC)

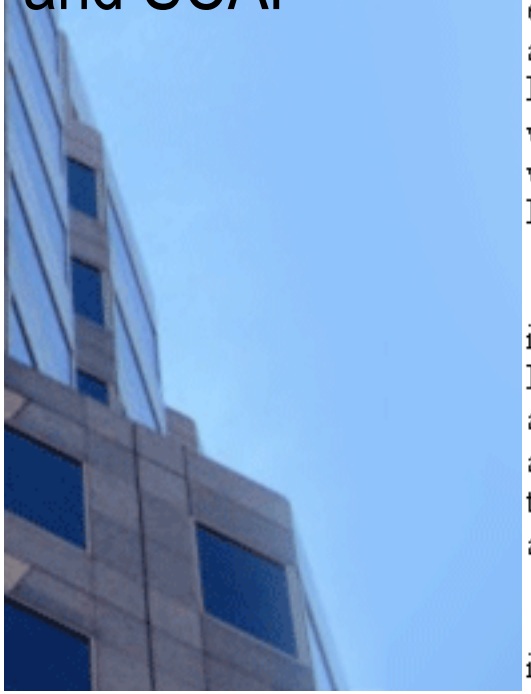
Peter Mell,
SCAP Validation Program Manager
National Institute of Standards and Technology
mell@nist.gov

SCAP Overview

- **Technology for automating and standardizing vulnerability management, measurement, and policy compliance checking**
  - **Automating FISMA technical control compliance checking**
  - **Linking security operations and compliance activities**
  - **Harmonizing auditing and security operations**
- Learn more at http://scap.nist.gov
- Products tested in the SCAP validation program
- FDCC is one of many use cases for SCAP

OMB July 31, 2007 Memo to CIOs

- Discusses policy for FDCC and SCAP



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.

Quote from OMB July 31, 2007 Memo

- "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."

SCAP Validation and Capabilities

- SCAP applies to a wide range of IT security products
  - e.g., Configuration scanner, Vulnerability scanners, Patch checkers, Intrusion detection systems, Malware tools, Asset databases, Vulnerability databases
  - There are 12 capabilities
- ISS LOB SAIR
- For the purposes of FDCC certification and monitoring:

Agencies and IT providers will want to acquire "SCAP Validated FDCC Scanners"

How can information technology providers use SCAP Validated FDCC Scanners?

- OMB Mandated: Certification that software products do not alter FDCC settings

Self Asserts

FDCC Compliance

Product Vendor

Federal Agency

How can Agencies use SCAP Validated FDCC Scanners?

- **OMB Mandated: Monitoring the configuration of XP and Vista installations**
- Acceptance testing of software asserted to be FDCC compliant
- Testing existing software using the FDCC virtual hard disks
- Customize SCAP scans for agency specific configuration policy
- Output can be used as FISMA technical control compliance evidence
  - mapping to 800-53 controls
- Auditing compliance to FDCC
- Scan additional software using SCAP content

Comments on SCAP Product Validation

- NIST IS NOT recommending or mandating products
- NIST IS validating that products conform to the SCAP FDCC test requirements
  - Product correctly implements SCAP
  - Product correctly scans for all applicable FDCC settings
  - Product scans using the Government and Microsoft recommended technical method
- NIST set up the program in only 6 months

Where are the SCAP Validated Products??

NIST will announce the SCAP validated product list by February 1st: http://nvd.nist.gov/scapproducts.cfm

- The initial SCAP validation list may contain
  - Approximately 5 products from 3 vendors
  - Both enterprise capable and single host SCAP products
- The list will be updated daily as new products are validated
- 12 independent laboratories have applied for accreditation to perform SCAP testing

FDCC SCAP Reporting Format

- SCAP Validated FDDC Scanners must output a standard based compliance report
- Agencies can use this to provide NIST “deviation reports”
- NIST WILL NOT judge or evaluate agencies deviations
- NIST WILL provide OMB statistics on which settings are most commonly altered
  - FDCC may be altered by OMB based on results
- March 31 date set for report submission

The method to submit FDCC deviation reports will be posted at http://fdcc.nist.gov

Questions

Peter Mell,
SCAP Validation Program Manager
National Institute of Standards and Technology
mell@nist.gov