Federal Desktop Core Configuration and the Security Content Automation Protocol

Ensuring Secure Computer Configurations within the Federal Government

Peter Mell,
National Vulnerability Database
National Institute of Standards and Technology
mell@nist.gov

John Banghart,
Booz Allen Hamilton
banghart_john@bah.com

Sponsored by
DHS National Cyber Security Division/US-CERT
NIST
National Institute of Standards and Technolog
National Vulnerability Database
automating vulnerability management, security measurement, and compliance checking

Federal Desktop Core Configuration (FDCC)

- Standardized security configuration for Windows XP and Windows Vista
- OMB and the CIO council seek to reduce federal systems vulnerability to individual and state sponsored cyber terrorism
  - "OMB Deep Dive" (Office of President initiative)
    - New government wide program (DOD, Intel, Civilian) that leverages existing components
- Deadline for deployment is February, 2008
- Scope of program requires automation

Information Security Automation Program (ISAP)

- Interagency (NIST, NSA, DISA, OSD, DHS) response to the need for consistent standards-based vulnerability management in the federal government and private industry.
- Automate the implementation of information system security controls in the IT systems through security-data sharing in standard formats.
- Security Content Automation Protocol (SCAP) is the technical implementation of ISAP

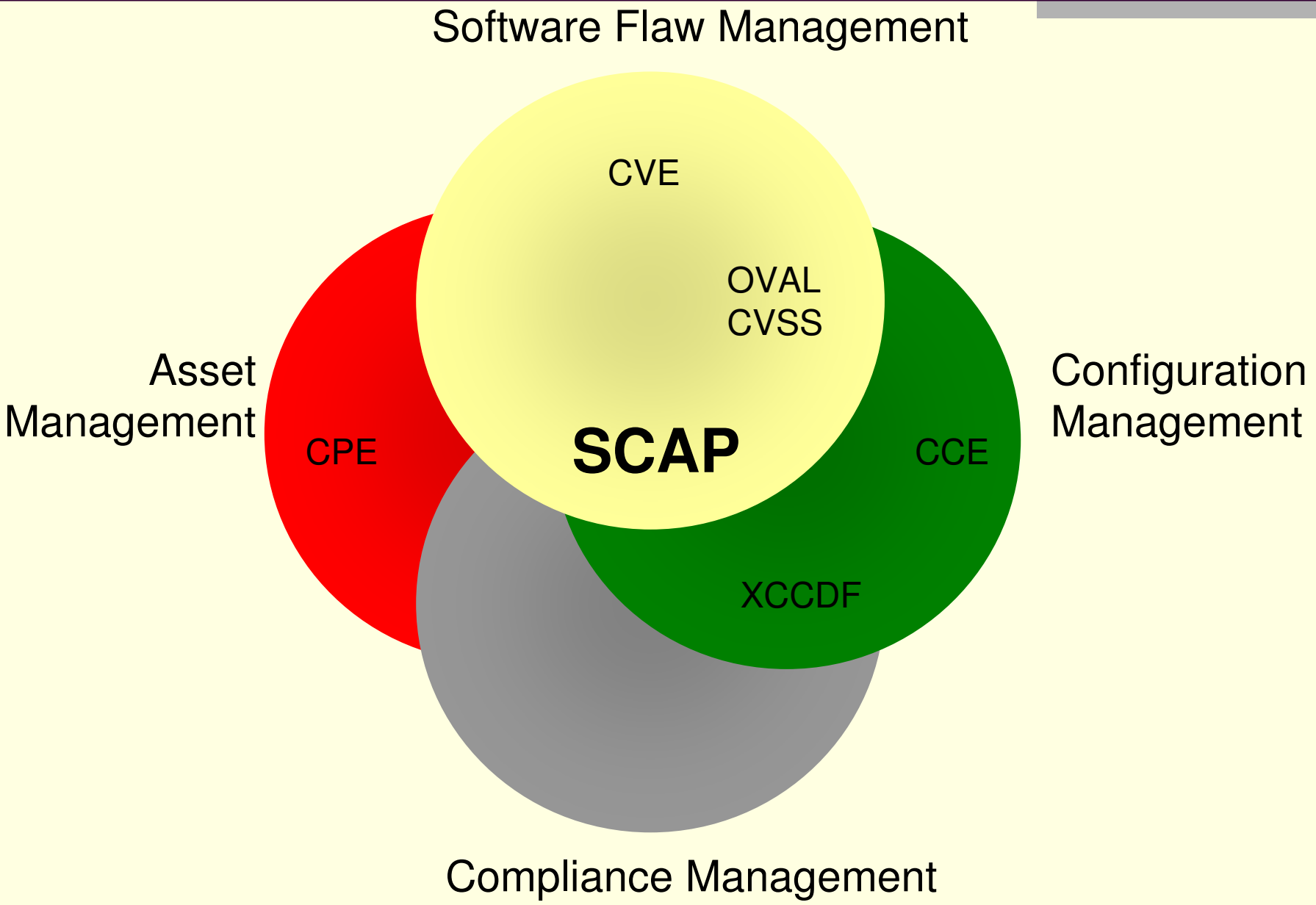
Security Content Automation Protocol (SCAP)

- Enables standardized and automated vulnerability management, measurement, and policy compliance evaluation (e.g., FISMA and DoD 8500.2/8510 compliance)
- Enumeration of vulnerabilities, misconfigurations, platforms, and impact
- Machine readable security configuration checklists

SCAP Components

- Six open XML standards:
  - Common Vulnerabilities and Exposures (CVE)
    - Dictionary of security related software flaws
  - Common Configuration Enumeration (CCE)
    - Dictionary of software misconfigurations
  - Common Platform Enumeration (CPE)
    - Standard nomenclature and dictionary for product naming
  - eXtensible Checklist Configuration Description Format (XCCDF)
    - Standard XML for specifying checklists
  - Open Vulnerability Assessment Language (OVAL)
    - Standard XML for checking machine state
  - Common Vulnerability Scoring System (CVSS)
    - Standard for scoring the impact of vulnerabilities

SCAP Interoperability



SCAP Vendors

Currently Asserting SCAP Compatibility

McAfee®

secure elements®
audit. evaluate. comply.
- FDCC Scanning Capable

ThreatGuard
- FDCC Scanning Capable

TENABLE
Network Security®

Planned SCAP Compatibility

the CENTER for INTERNET SECURITY

eEye Digital Security®

nCircle
Proactive Network Security

Atlantic Systems Group, Inc.
www.asgcc

SecureInfo
THE INFORMATION ASSURANCE EXPERTS™

SCAP Checklists

- SCAP Checklists:
  - Windows Vista (FDCC Profile)
  - Windows XP (FDCC Profile)
  - Windows Vista Firewall (FDCC Profile)
  - Windows XP Firewall (FDCC Profile)
  - Windows Server 2003
  - Red Hat Linux
  - Internet Explorer 7 (FDCC Profile)
  - Microsoft Office 2007
  - Symantec Antivirus

SCAP Compliance Program

- Ensuring security tools
  - comply to the NIST Security Content Automation Protocol (SCAP)
  - enable agencies to continuously monitor systems against OMB mandated configuration settings (results mapped to FISMA)
- Supports Multiple Initiatives:
  - OMB FDCC Secure Configuration Effort
  - NIST FISMA Implementation Phase II (also applies to NIST HIPAA work)
  - Information Security Automation Program (ISAP): OSD, DISA, NSA, DHS, NIST
  - OSD Computer Network Defense Pilot
  - NIST Checklist Program
  - NIST National Vulnerability Database

SCAP and FISMA

- SCAP checklists have NIST 800-53 mappings for the recommended configuration settings
- SCAP compliant tools report on the compliance of the setting to FDCC and to the corresponding 800-53 technical control(s)
- Report provides evidence chain for due diligence.

Putting It Together

- Procurement
  - Agencies require vendor assertion of FDCC compliance using language from OMB Memo M-07-18
- Agency Software Acceptance Testing
  - Agencies verify accuracy of vendor assertion using SCAP compliant tools
- Routine Monitoring
  - Continuous monitoring of agency computer configurations
    - Ensure that configuration hasn't been altered through patches, software installation, or human interaction
  - NIST FISMA Phase II Certification
- FISMA reporting through 800-53 mappings in SCAP checklists

Moving Forward

Peter Mell,
National Vulnerability Database
National Institute of Standards and Technology
mell@nist.gov

John Banghart,
Booz Allen Hamilton
banghart_john@bah.com