Security Content Automation Protocol

presented by:
Matt Barrett
National Institute of Standards and Technology
Agenda

- Challenges with Current Security Approaches
- Introduction to Security Content Automation Protocol
- How Does SCAP Work
- Linking Configuration to Compliance with SCAP
- SCAP Stakeholders, Contributors, and Early Adopters
- SCAP Validation Program
What is SCAP?

How
Standardizing the format by which we communicate

Protocol

Content

What
Standardizing the information we communicate

http://nvd.nist.gov

• 70 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

CVE
OVAL
CVSS
CPE
SCAP
CCE
XCCDF

National Vulnerability Database
a comprehensive cyber vulnerability resource

Sponsored by DHS National Cyber Security Division/US-CERT
National Institute of Standards and Technology

NIST

NIST

NIST

NIST

NIST

NIST
## Security Content Automation Protocol (SCAP)

**Standardizing How We Communicate**

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CVE</strong></td>
<td><strong>Common Vulnerability Enumeration</strong></td>
<td>Standard nomenclature and dictionary of security related software flaws</td>
</tr>
<tr>
<td><strong>CCE</strong></td>
<td><strong>Common Configuration Enumeration</strong></td>
<td>Standard nomenclature and dictionary of software misconfigurations</td>
</tr>
<tr>
<td><strong>CPE</strong></td>
<td><strong>Common Platform Enumeration</strong></td>
<td>Standard nomenclature and dictionary for product naming</td>
</tr>
<tr>
<td><strong>XCCDF</strong></td>
<td><strong>eXtensible Checklist Configuration Description Format</strong></td>
<td>Standard XML for specifying checklists and for reporting results of checklist evaluation</td>
</tr>
<tr>
<td><strong>OVAL</strong></td>
<td><strong>Open Vulnerability and Assessment Language</strong></td>
<td>Standard XML for test procedures</td>
</tr>
<tr>
<td><strong>CVSS</strong></td>
<td><strong>Common Vulnerability Scoring System</strong></td>
<td>Standard for measuring the impact of vulnerabilities</td>
</tr>
</tbody>
</table>

*Cisco, Qualys, Symantec, Carnegie Mellon University*
Existing Federal Content

Standardizing What We Communicate

- Over 70 million hits per year
- 29,000 vulnerabilities
- About 20 new vulnerabilities per day
- Mis-configuration cross references to:
  - NIST SP 800-53 Security Controls (All 17 Families and 163 controls)
  - DoD IA Controls
  - DISA VMS Vulnerability IDs
  - Gold Disk VIDs
  - DISA VMS PDI IDs
  - NSA References
  - DCID
  - ISO 17799
- Reconciles software flaws from:
  - US CERT Technical Alerts
  - US CERT Vulnerability Alerts (CERTCC)
  - MITRE OVAL Software Flaw Checks
  - MITRE CVE Dictionary
- Produces XML feed for NVD content

In response to NIST being named in the Cyber Security R&D Act of 2002
- Encourages vendor development and maintenance of security guidance
- Currently hosts 114 separate guidance documents for over 141 IT products
- Translating this backlog of checklists into the Security Content Automating Protocol (SCAP)
- Participating organizations: DISA, NSA, NIST, Hewlett-Packard, CIS, ITAA, Oracle, Sun, Apple, Microsoft, Citadel, LJK, Secure Elements, ThreatGuard, MITRE Corporation, G2, Verisign, Verizon Federal, Kyocera, Hewlett-Packard, ConfigureSoft, McAfee, etc.
How SCAP Works

- **Checklist XCCDF**
  - Platform CPE
  - Misconfiguration CCE
  - General Impact CVSS
  - Software Flaw CVE
  - General Impact CVSS

- **Test Procedures OVAL**

- **Patches OVAL**

COTS/GOTS Tools

Specific Impact CVSS Results

Specific Impact CVSS Results
Linking Configuration to Compliance

<Group id="IA-5" hidden="true">
  <title>Authenticator Management</title>
  <reference>ISO/IEC 17799: 11.5.2, 11.5.3</reference>
  <reference>NIST 800-26: 15.1.6, 15.1.7, 15.1.9, 15.1.10, 15.1.11, 15.1.12, 15.1.13, 16.1.3, 16.2.3</reference>
  <reference>GAO FISCAM: AC-3.2</reference>
  <reference>DOD 8500.2: IAKM-1, IATS-1</reference>
  <reference>HIPAA SR 164.308(a)(5)(ii)(D)</reference>
</Group>

<Rule id="minimum-password-length" selected="false" weight="10.0">
  <reference>CCE-100</reference>
  <reference>DISA STIG Section 5.4.1.3</reference>
  <reference>DISA Gold Disk ID 7082</reference>
  <reference>PDI IAIA-12B</reference>
  <reference>800-68 Section 6.1 - Table A-1.4</reference>
  <reference>NSA Chapter 4 - Table 1 Row 4</reference>
  <requires idref="IA-5"/>
  [pointer to OVAL test procedure]
</Rule>

Rationale for security configuration

Keyed on SP800-53 Security Controls

Traceability to Mandates

Traceability to Guidelines
Implement security controls; apply security configuration settings

**SP 800-70**

Implement security controls; apply security configuration settings

**SP 800-37 / SP 800-53A**

Categorize Information System

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

**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 800-37**

Authorize Information System

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

**SP 800-53A**

Assess Security Controls

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

**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

**SP 800-53**

Select Security Controls

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

~ 19% of FISMA Security Controls are fully automated through SCAP

~ 24% of FISMA Security Controls are partially automated through SCAP
Integrating IT and IT Security Through SCAP

- Asset Management
- Vulnerability Management
- Compliance Management
- Configuration Management

- CVE
- OVAL
- CVSS
- CPE
- CCE
- XCCDF
- SCAP

Common Vulnerability Enumeration
Common Platform Enumeration
Common Configuration Enumeration
eXtensible Checklist Configuration Description Format
Open Vulnerability and Assessment Language
Common Vulnerability Scoring System
The objective is to achieve *visibility* into prospective business/mission partners information security programs *BEFORE* critical/sensitive communications begin…establishing levels of security due diligence and trust.
Stakeholder and Contributor Landscape: Industry

Product Teams and Content Contributors

- XACTA
- Belarc
- Shavlik
- MITRE
- eEye Digital Security
- Secure elements
- ThreatGuard
- nCircle
- FuGEN
- McAfee
- Symantec
- Configuresoft
- The Center for Internet Security
- Gideon Technologies
- Tenable
- SecureInfo
- Lumension Security
- NIST
- Premier Data Services
- IBM
- RSA
- Red Hat
Stakeholder and Contributor Landscape: Federal Agencies

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

<table>
<thead>
<tr>
<th>DHS</th>
<th>OMB</th>
</tr>
</thead>
<tbody>
<tr>
<td>NSA</td>
<td>IC</td>
</tr>
<tr>
<td>OSD</td>
<td>DISA</td>
</tr>
<tr>
<td>DOJ</td>
<td>EPA</td>
</tr>
<tr>
<td>Army</td>
<td>NIST</td>
</tr>
<tr>
<td>DOS</td>
<td></td>
</tr>
</tbody>
</table>
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. 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-PRD-INFO. Additional information about the S-CAP can be found at: http://sfpd.nist.gov/scap.cfm.
National Voluntary Laboratory Accreditation Program
More Information

NIST FDCC Questions

fdcc@nist.gov

NIST FDCC Web Site

http://fdcc.nist.gov

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

National Checklist Program

http://checklists.nist.gov

National Vulnerability Database


- SCAP Checklists
- SCAP Capable Products
- SCAP Events

NIST SCAP Mailing Lists

Scap-update@nist.gov
Scap-dev@nist.gov
Scap-content@nist.gov
Contact Information

**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://fdcc.nist.gov](http://fdcc.nist.gov)  
Comments: fdcc@nist.gov
Questions

National Institute of Standards & Technology
Information Technology Laboratory
Computer Security Division
Current State of Information Security
FISMA Compliance Model

30,000 FT

FISMA Legislation
High Level, Generalized, Information Security Requirements

15,000 FT

Federal Information Processing Standards
FIPS 199: Information System Security Categorization
FIPS 200: Minimum Information Security Requirements

5,000 FT

Management-level Security Controls
Technical-level Security Controls
Operational-level Security Controls

Hands On

Information System Security Configuration Settings
NIST, NSA, DISA, Vendors, Third Parties (e.g., CIS) Checklists and Implementation Guidance
Current State Summary - Compliance

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
• Decreased timeline in exploit development coupled with a decreased patch development timeline (highly variable across vendors)
• Increased prevalence of zero day exploits
• Three of the SANS Top 20 Internet Security Attack Targets 2006 were categorized as “configuration weaknesses.” Many of the remaining 17 can be partially mitigated via proper configuration.
Current State: Vulnerability Management Industry

- Product functionality is becoming more hearty as vendors acknowledge connections between security operations and a wide variety of IT systems (e.g., asset management, change/configuration management)
- Some vendors understand the value of bringing together vulnerability management data across multiple vendors
- Vendors driving differentiation through:
  - enumeration,
  - evaluation,
  - content,
  - measurement, and
  - reporting

Hinders information sharing and automation
Reduces reproducibility across vendors
Drives broad differences in prioritization and remediation
Supplemental – SCAP Platform Evaluation Tutorial
Current and Near-Term Use Cases

**Configuration**
- Organization Guidelines (e.g., STIG)
- National Checklist Program
- National Vulnerability Database
- Information Feeds
- Vulnerability Alerts (e.g., IAVA)
- Organization Vulnerability Database

**Misconfiguration Software Flaws**

**Decision and Change Control Process**

- Standardized Checklist
  - XCCDF
- Standardized Test Procedures
  - OVAL
- Risk Decision Report
  - XCCDF
  - CVSS
- Risk Management and Compliance Process

- Risk Management and Compliance Policy
  - XCCDF
  - CVSS
- Compliance Report
  - XCCDF
  - CVSS
- Metrics Report
  - XCCDF
  - CVSS

- Standardized Change List
  - XCCDF
- Standardized Change Procedures
  - OVAL
- Standardized Measurement and Reporting
  - CVSS
  - XCCDF

**Implement/Remediate**

**Monitor/Assess/Evaluate**

Organization, COTS / GOTS, NIST
Current Problems
Conceptual Analogy (Continued)

Before

After

Error Report

Problem
Air Pressure Loss

Impact
Car Will Not Start (9/10)

Diagnosis Accuracy:
All Sensors Reporting

Diagnosis:
Replace Gas Cap

Expected Cost:
$25.00
XCCDF - eXtensible Car Care Description Format

```
<Car>
  <Description>
    <Year> 1997 </Year>
    <Make> Ford </Make>
    <Model> Contour </Model>
  </Maintenance>
  <Check1> Gas Cap = On </Check1>
  <Check2> Oil Level = Full </Check2>
</Description>
</Car>
```

OVAL – Open Vehicle Assessment Language

```
<Checks>
  <Check1>
    <Location> Side of Car </Location>
    <Procedure> Turn </Procedure>
  </Check1>
  <Check2>
    <Location> Hood </Location>
    <Procedure> … </Procedure>
  </Check2>
</Checks>
```

Error Report

<table>
<thead>
<tr>
<th>Problem</th>
<th>Air Pressure Loss</th>
</tr>
</thead>
<tbody>
<tr>
<td>Diagnosis Accuracy</td>
<td>All Sensors Reporting</td>
</tr>
<tr>
<td>Diagnosis</td>
<td>Replace Gas Cap</td>
</tr>
<tr>
<td>Expected Cost</td>
<td>$25.00</td>
</tr>
</tbody>
</table>
SCAP Content Made Simple

**XCCDF - eXtensible Checklist Configuration Description Format**

```xml
<Document ID> NIST SP 800-68
<Date> 04/22/06 </Date>
-Version> 1 </Version>
<Revision> 2 </Revision>
<Platform> Windows XP </Platform>
<Check1> Password >= 8 </Check1>
<Check2> Win XP Vuln </Check2>
</Maintenance>
</Description>
</Car>
```

**OVAL – Open Vulnerability Assessment Language**

```xml
<Checks>
<Check1>
<Registry Check> … <>
<Value> 8 </Value>
</Check1>
<Check2>
<File Version> … <>
<Value> 1.0.12.4 </Value>
</Check2>
</Checks>
```

**Standardized Checklist**

- CPE
- CCE
- CVE

**Standardized Test Procedures**

**XCCDF**

**CVSS**

**CPE**

**CCE**

**CVE**
Application to Automated Compliance

The Connected Path

800-53 Security Control

Result

800-68 Security Guidance

API Call

ISAP Produced Security Guidance in XML Format

COTS Tool Ingest
Application to Automated Compliance

The Connected Path

800-53 Security Control
DoD IA Control

AC-7 Unsuccessful Login Attempts

800-68 Security Guidance
DISA STIG/Checklist
NSA Guide

AC-7: Account Lockout Duration
AC-7: Account Lockout Threshold

ISAP Produced Security Guidance in XML Format

- <registry_test id="wrt-9999"
  comment="Account Lockout Duration Set to 5" check="at least 5">
  - <object>
    <hive>HKEY_LOCAL_MACHINE</hive>
    <key>Software\Microsoft\Windows\</key>
    <name>AccountLockoutDuration</name>
  </object>
  - <data operation="AND">
    <value operator="greater than">5*</value>
  </data>

800-53 Security Control
DoD IA Control

Result

RegQueryValue (lpHKey, path, value, sKey, Value, Op);
If (Op == ‘>’ )
if ((sKey < Value )
return (1); else
return (0);

800-68 Security Guidance
DISA STIG/Checklist
NSA Guide

AC-7: Account Lockout Duration
AC-7: Account Lockout Threshold

API Call

lpHKey = “HKEY_LOCAL_MACHINE”
Path = “Software\Microsoft\Windows\”
Value = “5”
sKey = “AccountLockoutDuration”
Op = “>“

COTS Tool Ingest
Supplemental – SCAP Value Reference
## SCAP Value

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

What are the NIST Technical Security Controls?

What are the *Specific* NIST recommended settings for individual technical controls?

How do I implement the recommended setting for technical controls? Can I use my COTS Product?

Am I compliant to NIST Recs & Can I use my COTS Product?

Will I be audited against the same criteria I used to secure my systems?
What are the NIST Technical Security Controls?

What are the Specific NIST recommended settings for individual technical controls?

How do I implement the recommended setting for technical controls? Can I use my COTS Product?

Am I compliant to NIST Recs & Can I use my COTS Product?

Will I be audited against the same criteria I used to secure my systems?

Fundamental FISMA Documents

- FIPS 200 / SP 800-53
  - Security Control Selection
- SP 800-53 / FIPS 200 / SP 800-30
  - Security Control Refinement
- SP 800-18
  - Security Control Documentation
- SP 800-70
  - Security Control Implementation
- SP 800-37
  - Security Control Monitoring
  - System Authorization
  - Security Control Assessment
- SP 800-53A / SP 800-26 / SP 800-37