



Improving FISMA Effectiveness and Efficiency Through the Security Content Automation Protocol (SCAP)

**Rob Montgomery, President & Founder
Argosy Omnimedia, Inc.**

September 23, 2008

Today's Presentation

- American Council of Technology / Industry Advisor Council Paper published in January 2008
 - Operational “pain points” of FISMA implementation
 - FISMA compliance management examples of SCAP
- Industry profile: Healthcare
- Compliance process
- Ideas for future automation solutions

FISMA Paper

- [Improving FISMA Effectiveness and Efficiency Through the Security Content Automation Protocol \(SCAP\)](#) – automation for information security assurance and compliance (37pgs)
 - Overview of the NIST SCAP initiative and Mitre
 - Directed to the technology and management staff responsible for FISMA compliance
 - Provides ideas and examples for how automation can improve productivity and quality of cybersecurity management

Cybersecurity Challenges

- Vigilant, proactive security readiness
- IT device complexity
 - Providers – imaging, serology, vitals monitors, EHRs, ePrescribe
- Increasing outsourcing – on and off-shore
- Financial liabilities associated with State breach notification laws
- Expanding regulatory guidelines and standards

Profile: Healthcare

- Begin with a Risk Assessment!
 - [CMS Information Security Risk Assessment Methodology](#)
 - [Risk Management Guide for Information Technology Systems](#)
- Standards and Guidelines
 - [Business Partner System Security Manual \(BPSSM v9\)](#)
- Complexity and resource requirements are device and environment driven

SCAP Standards

 cve.mitre.org	<p>Common Vulnerabilities and Exposures</p>	<p>Standard identifiers and dictionary for security vulnerabilities related to software flaws</p>
 cce.mitre.org	<p>Common Configuration Enumeration</p>	<p>Standard identifiers and dictionary for system configuration issues related to security</p>
 cpe.mitre.org	<p>Common Platform Enumeration</p>	<p>Standard identifiers and dictionary for platform/product naming</p>
 <p>security benchmark automation</p>	<p>eXtensible Configuration Checklist Description Format</p>	<p>Standard XML for specifying checklists and for reporting results of checklist evaluation</p>
 oval.mitre.org	<p>Open Vulnerability and Assessment Language</p>	<p>Standard XML for testing procedures for security related software flaws, configuration issues, and patches as well as for reporting the results of the tests</p>
	<p>Common Vulnerability Scoring System</p>	<p>Standard for conveying and scoring the impact of vulnerabilities</p>

Standards Overlap

- Extensible Configuration Checklist Description Format (XCCDF)
 - originally intended to be used for technical security checklists.
 - expanded to non-technical applications (e.g., owner’s manuals, user guides, non-technical FISMA controls, and items considered “manual procedures

...Overlap (cont)

- DISA STIGs and the NSA Guides are the configuration standards for DoD IA and IA-enabled devices/systems
 - synonyms - lockdown guide, hardening guide, or benchmark configuration
- Security Readiness Review Scripts (SRRs) test products for STIG compliance.

...Overlap (cont)

Information Assurance Support Environment
Your 'One-Stop-Shop' for IA Information

IA News

What's New

Consent Notice

Security Checklists

[Security Checklists](#) | [SRRs](#) | [STIGs](#) | [STIG Home Page](#) | [Whitepapers](#)

- Checklists – prescriptive - [Blackberry](#)
- SRRs – test scripts – [Microsoft Gold Disk](#)
- STIGs – guides – [Database Server](#)
- Both product specific (e.g. MS SQL 2005 CL) and technology generic (e.g. Database STIG)

Automation candidates

- Data repurposing / reuseability
- Constant monitoring
 - network state
 - vendor alerts and patches
 - user and device behavior
- Event or state correlation
- Incident response
- Management status and reporting
- Patch management
- Compliance project management
- Data mining

Example Assessment

- Combined HIPAA & FISMA
Compliance Information Security Assessment
- Sample applicable NIST specifications – 800- 12, 13, 24, 31, 37, 41, 42, 44, 45, 46, 47, 48, 53, 53a, 58, 61, 64, 91, 92, 94
- Tasks List
 - STIG and Security Checklist Compliance to DISA standards
 - External Penetration Test
 - War Dialing
 - Network Design and DMZ Architecture Review
 - Perimeter Vulnerability Assessment and Penetration Testing
 - Password Cracking Exercise
 - Internal Network Vulnerability and Penetration Testing
 - Wireless Network Review
 - PBX and Voice Systems Review
 - Intrusion Detection and Prevention Systems Review
 - Firewall, Router, Switch and Load Balancer Reviews
 - Audit Logging Review
 - Security Policy and Procedure Review
 - Corporate and IS Incident Response
 - Systems Development Life Cycle (SDLC) Review

Testing Process

- Create/Review Policies, Plans and Procedures
- Establish a baseline by documenting any application specific exceptions
- Test
 - Checklists – inspection, demonstration
 - SRRs – run the scripts against the target systems
- Evaluate results
- Document findings
- Generate corrective actions (e.g. CAP, POA&M)

Testing Scope

- Representative sample – in-depth analysis
- Larger sample or total population – test scripts with structure result data (e.g. SRR result tabulation)
- Tools
- NIST Security Content Automation Protocol (SCAP)

Test/Audit Plan



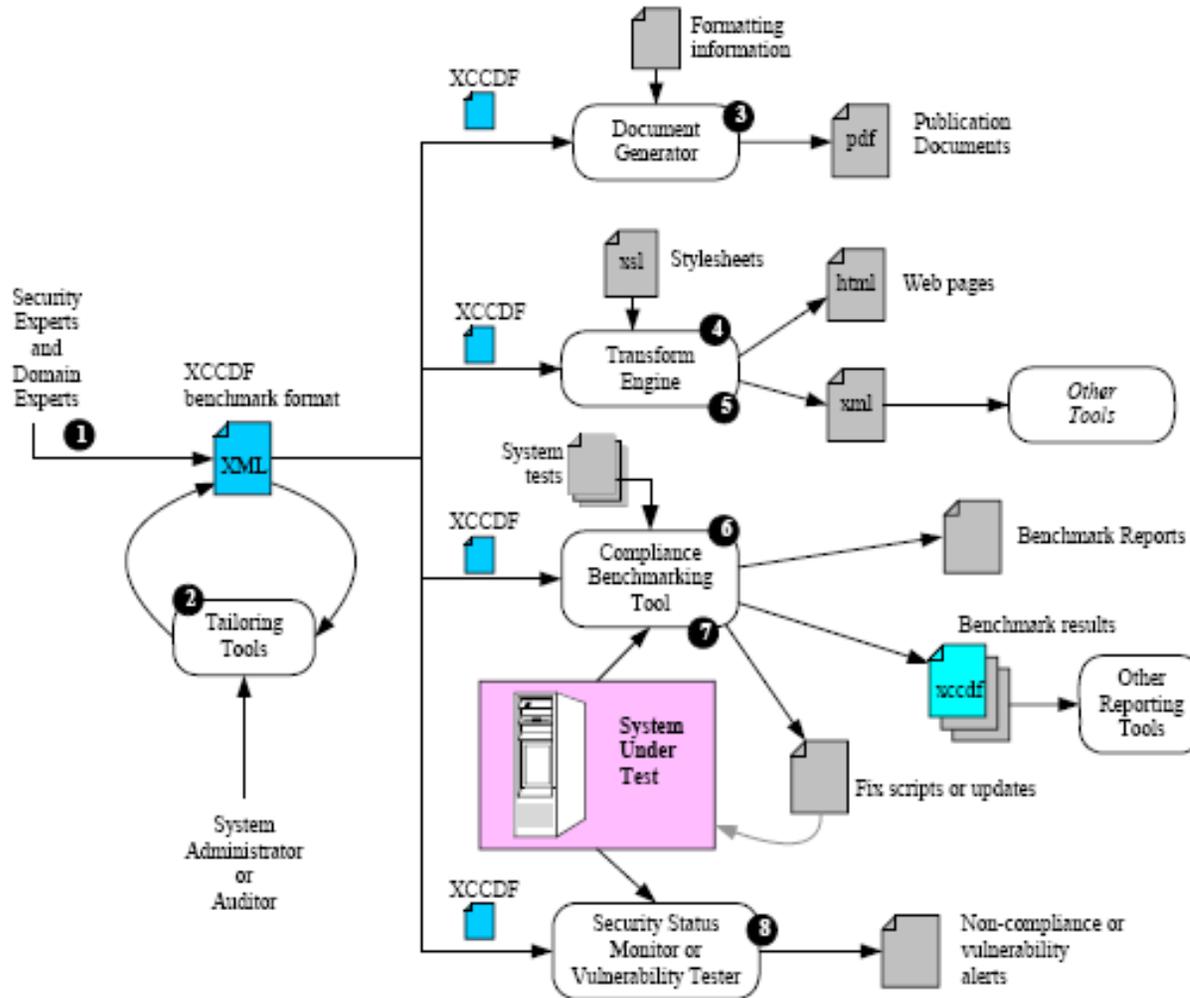
1	STIG ID	VULN ID	Ca	Description	Status	Test Results	Referenc
2	NET0180	V0002990	II	Non-registered or unauthorized IP addresses.	NA	The test requires login into www.nic.mil and checking IP ranges for authorization. This can only be done from .MIL domains.	
3	NET0185	V0003157	II	Unauthorized addresses within Siprnet enclave	NA	While private addresses in the range 192.168 and 172.16 are used in the router configuration, none seem to be used within a SIPRNET enclave.	2.10.8d
4	NET0240	V0003143	I	Devices exist that have standard default passwords	NF	Beginning with version 7.6, the router enforces replacement of the default password.	2.10.8d
5	NET0340	V0003013	II	Warning banner compliance to 8500.2 ECwM-1.	NF		2.10.8d
6	NET0400	V0003034	II	Interior routing protocols are not authenticated	NA	Routing protocols have not been implemented in the configuration.	2.10.8d
7	NET0402	V0014664	II	OSPFv3 routing protocol is not authenticated	NA	OSPFv3 is not defined in the router configuration, as it is used to support IPv6.	2.10.8d
8	NET0408	V0014665	II	Exterior routing protocols must authenticate	NA	Exterior routing protocols such as BGP are not defined in the router configuration.	2.10.8d
9	NET0434	V0015433	II	Group profiles defined in AAA server	NF	No group profiles have been defined.	2.10.8d
10	NET0440	V0003966	II	Emergency accounts limited to one.	NF	The router configuration defines one local emergency account named "admin" and another account, "remote", which is a template user for remote accounts.	2.10.8d
11	NET0460	V0003056	I	Group accounts or user accounts without passwords	NF	The local account "admin" has been configured with a password.	2.10.8d
12	NET0465	V0003057	II	Assign lowest privilege level to user accounts.	NF	Both local user accounts "admin" and "remote" are assigned to the same group "super-user-local" which have full access privileges. Only administrators who require access are provided access to the routers. There is currently not a need to define specific access privileges for the members of the network team.	2.10.8d 2.10.10

- [Juniper Router Checklist](#)

Test Results Summary

NETWORK SECURITY CHECKLIST - JUNIPER INFRASTRUCTURE ROUTER													
Checklist Version 7, Release 1.1													
20-Nov-07													
Tabulated Results													
	Device ID	Cat 1				Cat 2				Total			
		Tests	Performed	Failed	Deviation %	Tests	Performed	Failed	Deviation %	Tests	Performed	Failed	Deviation %
Juniper													
	Target#1	5	5	0	0%	37	37	3	8%	42	42	3	7%
	Target#2	5	5	0	0%	37	37	3	8%	42	42	3	7%
	Target#3	5	5	0	0%	37	37	3	8%	42	42	3	7%
	Totals	15	15	0	0%	111	111	9	8%	126	126	9	7%
Scope													
Argosy completed an assessment of every Cat 1 and Cat 2 item within the Juniper Infrastructure Router STIG in order to support task xxxxx. The above table is a tabulation of the results. These results were produced from the use of documentation provided.													
Note 1: The "Tests" columns are based on the most current STIGs as of 3/1/08, and includes all Cat 1 and 2 checks encompassed by the associated STIGs.													
Note 2: The "Performed" columns are a tabulation of the results including all Cat 1 and 2 checks encompassed by the associated STIGs.													
Note 3: The "Failed" column contains the amount of checks that were performed that failed (for example, of the 37 Cat 2 checks that were performed for <client>'s bismark router, 3 of the chee													
Note 4: The "Deviation %" column contains the percentage of checks that were performed that failed (for example, of the 37 Cat 2 checks that were performed for <client>'s bismark router, 3 of the checks failed, equating to a 8% deviation).													
Legend													
NF = Not a Finding													
O = Open (i.e. Finding)													
NA = Not Applicable (i.e. Not a Finding)													
NR = Not Reviewed / Out of Scope (i.e. Gold Disk script does not address)													

XCCDF



Operational Challenge #1

- Risk rating of vulnerability – different tools rate/rank a given vulnerability differently (e.g. high, medium, low, informational)
- Resources – CVE, CCE, & CVSS
- Solution
 - CVSS included within CVE & CCE vulnerability feeds
 - CVSS normalizes the risk scoring for a given vulnerability and configuration

Solution #1

- nvdcve-2008.xml
- SQL injection vulnerability in Cisco Unified CallManager/Communications Manager (CUCM) 5.0/5.1 before 5.1(3a) and 6.0/6.1 before 6.1(1a) allows remote authenticated users to execute arbitrary SQL commands via the key parameter to the (1) admin and (2) user interface pages.

```

</entry>
<entry CVSS_vector="(AV:N/AC:L/Au:S/C:P/I:P/A:P)" CVSS_base_score="6.5" CVSS_exploit_subs
  <desc>
    <descript source="cve">SQL injection vulnerability in Cisco Unified CallManager/C
  </desc>
  <loss_types>
    <avail />
    <conf />
    <int />
    <sec_prot other="1" />
  </loss_types>
  <range>
    <network />
  </range>
  <refs>
    <ref source="BID" url="http://www.securityfocus.com/bid/27775">27775</ref>
    <ref source="FRSIRT" url="http://www.frsirt.com/english/advisories/2008/0542" adv
    <ref source="CISCO" url="http://www.cisco.com/en/US/products/products_security_ad
    <ref source="SECUNIA" url="http://secunia.com/advisories/28932" adv="1">28932</re
    <ref source="XF" url="http://xforce.iss.net/xforce/xfdb/40484">cucm-interface-sql
    <ref source="SECTrack" url="http://www.securitytracker.com/id?1019404">1019404</r
  </refs>
  <vuln_soft>
    <prod vendor="cisco" name="unified_callmanager">
      <vers num="5.0" />
      <vers num="5.0(1)" />
      <vers num="5.0(2)" />
      <vers num="5.0(3)" />
      <vers num="5.0(3a)" />
      <vers num="5.0(4)" />
      <vers num="5.0_4a" />
      <vers num="5.1" />
      <vers num="6.0" />
    </prod>
    <prod vendor="cisco" name="unified_communications_manager">
      <vers num="5.0" />
      <vers num="5.0_1" />
      <vers num="5.0_2" />
      <vers num="5.0_3" />
      <vers num="5.0_3a" />
      <vers num="5.0_4" />
      <vers num="5.0_4a" />
      <vers num="5.0_4a_sul" />
      <vers num="6.0" />
      <vers num="6.0_1" />
    </prod>
  </vuln_soft>

```

Operational Challenge #2

- Various tools identify discrete, isolated patch requirements that are not integrated/aggregated (e.g. O/S, application, I/O card, VM).
- Resources – CPE, CVE
- Solution
 - Network discovery to identify devices
 - Scan device for configuration level
 - Correlate that level with the CPE and CVE data

Solution #2

- CVE file contains links to sites containing patches
- SecurityFocus.com lists patches for download for CVE-2008-0001 “VFS in the Linux kernel before 2.6.22.16,.....”

News

Infocus

- ✦ Foundations
- ✦ Microsoft
- ✦ Unix
- ✦ IDS
- ✦ Incidents
- ✦ Virus
- ✦ Pen-Test
- ✦ Firewalls

Columnists

Mailing Lists

- ✦ Newsletters
- ✦ Bugtraq
- ✦ Focus on IDS
- ✦ Focus on Linux
- ✦ Focus on Microsoft
- ✦ Forensics
- ✦ Pen-test
- ✦ Security Basics
- ✦ Vuln Dev

Vulnerabilities

Jobs

- ✦ Job Opportunities
- ✦ Resumes
- ✦ Job Seekers
- ✦ Employers

Tools

RSS

- ✦ News
- ✦ Vulns

Security Research

info
discussion
exploit
solution
references

Linux Kernel VFS Unauthorized File Access Vulnerability

Solution:
The vendor has patched this issue in kernel 2.6.23.14. Please see the references for more information.

Linux kernel 2.6.20.2

- Linux linux-2.6.23.14.tar.gz
<http://www.kernel.org/pub/linux/kernel/v2.6/linux-2.6.23.14.tar.gz>

Linux kernel 2.6.21-RC3

- Linux linux-2.6.23.14.tar.gz
<http://www.kernel.org/pub/linux/kernel/v2.6/linux-2.6.23.14.tar.gz>

Linux kernel 2.6.11.4

- Linux linux-2.6.23.14.tar.gz
<http://www.kernel.org/pub/linux/kernel/v2.6/linux-2.6.23.14.tar.gz>

Operational Challenge #3

- Vulnerability scanners only detect vulnerabilities at the periphery, interfaces or ports. Other vulnerabilities may exist elsewhere or locally.
- Resources – CVE, CCE, XCCDF & OVAL
- Solution – Use the check lists (e.g. XCCDF, STIGs or SRRs) to identify the device, version and list of known vulnerabilities

Solution #3

- OVAL is an open language to express checks for determining whether software vulnerabilities—and configuration issues, programs, and patches—exist on a system.

OVAl

- Represents configuration information of systems for testing;
- Analyzes the system for the presence of the specified machine state (vulnerability, configuration, patch state, etc.);
- Reports the results of this assessment.

CyberSec Resources

- Vulnerabilities & SCAP
 - <http://nvd.nist.gov/home.cfm>
- Security Technical Implementation Guides (STIGS) and Supporting Documents
 - <http://iase.disa.mil/stigs/index.html>
- Commercial checklists, scripts and guides
 - <http://www.cisecurity.org>

For more information.....

Rob Montgomery

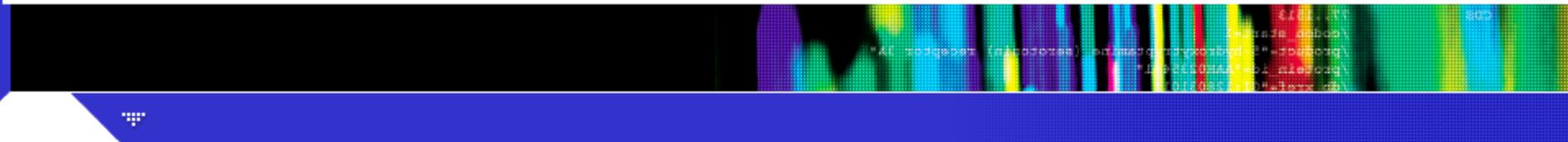
rob.montgomery@argoc.com

301.816.9373 (o)

<http://www.argoc.com>

6701 Democracy Blvd., Ste 300

Bethesda, MD 20817



End