FDCC & SCAP Content Challenges

Kent Landfield
Director, Risk and Compliance Security Research
McAfee Labs

Where we have been

- 1st Security Automation Workshop
  - nearly 20 people in a small room for the day
- 2nd Security Automation Conference and Working Group meetings
  - Nearly 200 attendees
  - Just hoping we were not wasting our time
- 3rd Security Automation Conference
  - 800+ attendees
  - OMB made SCAP mainstream
  - A product demo for the first SCAP tools was given
- 4th Security Automation Conference
  - A real maturing effort
  - Multiple products from multiple vendors demonstrating SCAP
- 5th Security Automation Conference
  - Today, a movement in the industry
  - Talk of integrating SCAP into Cloud Computing, VOIP, Event and Log Monitoring

What a difference a couple years makes!

What is Security Automation?

From this:

…to this

Security Content Automation Protocol (SCAP)

Defined by the NIST SP 800-126: *The Technical Specification for SCAP*

XCCDF	**eXtensible Configuration Checklist Description Format**	XML for specifying checklists and for reporting results of checklist evaluation
OVAL	**Open Vulnerability and Assessment Language**	Standard XML for representing system configuration information, assessing machine state, and reporting assessment results
OCIL*	**Open Checklist Interactive Language**	Standard for expressing and evaluating non-automated (i.e., manual) security checks
CCE	**Common Configuration Enumeration**	Standard identifiers and dictionary for system configuration issues related to security
CPE	**Common Platform Enumeration**	Standard identifiers and dictionary for platform/product naming
CVE	**Common Vulnerabilities and Exposures**	Standard identifiers and dictionary for security vulnerabilities related to software flaws
CVSS	**Common Vulnerability Scoring System**	Standard for measuring and conveying the relative severity of software flaw vulnerabilities

*** Due for release with SCAP version 1.1**

Why Should I Care?

- The power shift created by structured content in other industries
  - ISBN, UPC/Barcodes, etc.
- Interoperability versus lock-in
  - Interoperability good
  - Lock-in bad
- Reduce the cost of managing your networked environments

How SCAP Can Change Auditing

In a future not so far away…

- IT / Operations / Security will not have to stop what they are doing to prepare for an external audit
- Auditors will not need to bring in their own tools to audit the network assets directly
- Signed Benchmarks approved by the Auditor are running on the network
- IT staff hands the auditor the signed benchmark, the signed tailoring settings file and access to the signed results files.
- The auditor can the review the benchmark and the results, verify the signatures and determine if there are areas that the site should be validating / auditing that they currently are not and makes benchmark improvements.
- Their improvements are then put in place and now additional items are validated.
- Operations and management now have a continuous view of the status of there network…

National Checklist Program Website

U.S. Government repository of publically available security checklists

- 128 Checklists currently published on the website
- 17 SCAP-expressed checklists
- 26 additional SCAP-expressed checklists planned for FY2010
- Checklists cover 178 products
- Checklist contributors include
    - Government Organizations (e.g., NIST, NSA, DISA)
    - Vendors (e.g., Microsoft Corporation, Red Hat)
    - Non-profits
    - Federally Funded Research and Development Centers

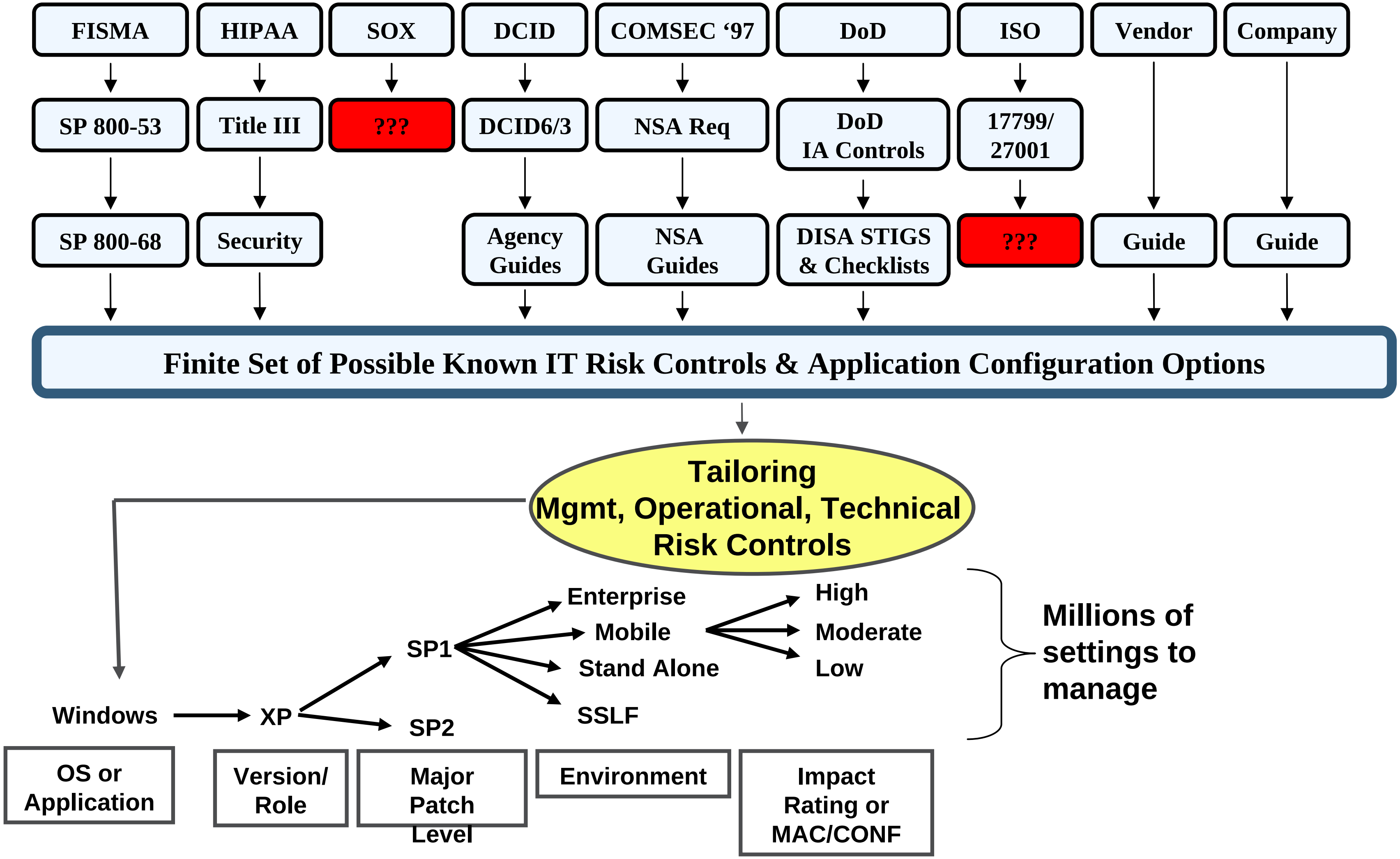
NIST Repository is the1st, but…

- Will not be the only archive of available SCAP content
- Vendors are starting to make SCAP content available on their sites
- Success of the NCP efforts will foster vendors to develop checklists for their products
- Authoritative issue will become a problem – Signing needed now
- Alternative repositories will start to spring up
- Today’s model for public distribution is lacking
- Mixed namespace benchmarks and checks will cause an addressing / access issue impacting evaluation
- Different models for content distribution will emerge

FDCC – Center of the SCAP Universe

- Not…
- A specific use case trying to solve a very important problem for a large organization
- The focus of the SCAP components has been to solve real global problems, not just the Federal Govt's issues
- SCAP is on the verge of transforming auditing as we have come to know it
- Private sector needs SCAP content for more than Windows and more than just FDCC

Compliance and Configuration Management



FISMA → SP 800-53 → SP 800-68

HIPAA → Title III → Security

SOX → ???

DCID → DCID6/3 → Agency Guides

COMSEC '97 → NSA Req → NSA Guides

DoD → DoD IA Controls → DISA STIGS & Checklists

ISO → 17799/ 27001 → ???

Vendor → Guide

Company → Guide

Finite Set of Possible Known IT Risk Controls & Application Configuration Options

Tailoring
Mgmt, Operational, Technical
Risk Controls

Windows → XP → SP1, SP2

SP1 → Enterprise, Mobile, Stand Alone, SSLF

Mobile → High, Moderate, Low

Millions of settings to manage

OS or Application

Version/ Role

Major Patch Level

Environment

Impact Rating or MAC/CONF

Our SCAP Challenge

Produce an entire new set of content from scratch with no development tools, no management, maintenance or publishing infrastructure, assuring each component is completely reusable and all fully tested, being distributed via multiple channels, while using multiple formats for the content whose formats are changing based on the whim of others.

Content Development At A Glance

- XCCDF / OVAL Content – All new

- Policies Developed
  - GLBA
  - HIPAA
  - CobiT
  - SOX
  - ISO27001
  - PCI-DSS
  - CIS Benchmarks
  - ..

- Other Content
  - OVAL Primitives
  - OVAL Compliance Checks
  - Patch Definitions and Benchmarks
  - Application Checks

- Supporting Six OS Families
  - Windows
  - Mac OS X
  - Solaris
  - Red Hat
  - HP-UX
  - AIX

- Supporting Five CPU Architectures
  - X86
  - X64
  - PowerPC
  - RISC
  - SPARC
  - …

- Supporting 40+ separate OS versions

Types of Content

- OVAL Primitives
  - For use in our Benchmark Editor which is a shared component for multiple products
  - Fully schema driven
- OVAL Configuration Checks
- OVAL Patch Definitions and Patch Benchmarks
- Application specific OVAL Checks
- XCCDF Benchmarks (a.k.a. Policies)
- Supporting NAC, Audit and Vulnerability Management

An approach to testing content

- Command line testing using
  - Vendor agent
  - MITRE's Ovaldi

- Development Testing
  - Develop Setup and Definition Test scripts
  - Execute the Definition tests prior to sending to QA
  - Capture System Characteristics during the run

- Initial QA manual testing
  - Assure all part of the submitted testable package are available
  - Run the tests on all applicable / affected systems
  - Integrate the tests into the automation environment

- Automated Testing
  - QA manages and monitors automated testing components
  - Test with multiple OVAL Interpreters to assure content is portable where possible
  - Assure both positive and negative drivers contain all Definition tests

- Managing patch testing via System Characteristics

Content Distribution

- Means to distribute content is not specified
  - Best practices is the only guide we have
- NIST repository forces users to pull content
  - Still working out the content distribution and notification processes
  - Checksums / signing of content needed
- Vendors producing their own content distribute it by their own means
- No way to verify the content is what the guidance authority released
- Other Intellectual Property protection mechanisms needed

SCAP Certification

- Certification is about the product
  - Can it consume a random SCAP compliant document set supplied by NIST to the evaluation lab?
  - Can it evaluate the parameters/values listed in the set?
  - Can it report the proper results in the proper output format?
  - If so, you pass…

- Content certification is not currently an active certification path
  - This is coming… But what does it mean and what are the limits on what can and should be certified?
  - Is certification really going to address interoperability issues between products and tools?

- This whole effort is TBD at present but assuring real interoperability between products is critical to truly realizing the value of security automation.

Localized SCAP Content

McAfee

- Existing McAfee developed SCAP Content
  - Benchmarks, Primitives, Oval Checks
- Created locale specific OVAL compliance checks
- Created locale/OS/version specific patches
- Targeted application checks for desktop security products
- Designed and implemented a process to provide localized content **using the existing SCAP specifications**
  - Creation of content
  - Testing of content
  - Publication of content

Language	Localized
English – US & International (EN)	Y
Chinese – Simplified (ZH-CN)	Y
Chinese - Traditional (ZH-TW)	Y
French (FR)	Y
German (DE)	Y
Italian (IT)	Y
Japanese (JP)	Y
Polish (PL)	Y
Spanish (ES)	Y
Dutch (NL)	Pending
Swedish (SV)	Pending
Portuguese – Brazilian (PT-BR)	Pending
Korean (KO)	Pending

Current SCAP Validated Vendors

Atlantic Systems Group, Inc.
Service-Disabled Veteran-Owned Small Business

BIGFIX

ca Transforming IT Management.

FORTINET

GIDEON TECHNOLOGIES
Know your assets. Know your risk.

hp

iSIGHTPARTNERS
Security beyond the edge

Lumension SECURITY

McAfee

Microsoft System Center Configuration Manager

nCircle

netIQ
An Attachmate Business

QUALYS

RAPID7

Shavlik

SPAWAR
Systems Center ATLANTIC

symantec.

TELOS

TENABLE Network Security

ThreatGuard

Triumfant

Kent Landfield

Kent_landfield@mcafee.com

Office: 972.963.7096

Mobile: 214.385.1138

McAfee