SPAWAR
Systems Center
ATLANTIC

SCAP Compliance Checker:

Developing a Government-Funded SCAP-Validated Application

Jack Vander Pol
SPAWAR Systems Center Atlantic
September 28, 2010

SPAWAR Systems Center ATLANTIC

Agenda

- About Us
- Why SCAP?
- Benefits of SCAP
- SCAP Challenges
- Moving Forward
- The SCAP Compliance Checker
  - What does it do?
  - Who can use it?
  - Who is using it?
- Demonstration of SCC
- What's Next for SCC?
- Questions

About Us

What is SPAWAR?

- Space and Naval Warfare (SPAWAR) Systems Center Atlantic is a working capital organization
  - Naval engineering facility primarily of civilian engineers and contractors
  - Receives no direct funding from Congress
- www.spawar.navy.mil

About Us (cont)

- Our division specializes in Information Assurance
- We have supported the Internal Revenue Service (IRS) since 2000
  - Performing Certification and Accreditation
  - Developing security policy standards
  - Developing automated compliance verification tools for:
    - Windows NT/2000/XP/2003/2008 R2/7
    - AIX, HP-UX, Linux, Solaris, Mac OS X
    - SQL Server & Oracle
    - Apache, Tomcat, IIS
    - Mainframes
    - Routers & Switches

SPAWAR Systems Center ATLANTIC

Why SCAP?

- Security Content Automation Protocol (SCAP) was the next logical step in the evolution of our compliance automation tools for the IRS
  - Similar to our internally developed methods
  - Allowed results to be easily shared for Federal Information Security Management Act (FISMA), Office of Management and Budget (OMB), etc.
  - Required by OMB

SPAWAR Systems Center ATLANTIC

The Benefits of SCAP

- All validated SCAP applications use the same content
- Easily aggregate standardized data reports from different vendors
- Consistent reporting across organizations
- Large collection of vulnerability content in the OVAL repository

SPAWAR Systems Center ATLANTIC

But…

- While SCAP provides a solid scalable architecture, it is relatively young and has room for growth.

SPAWAR Systems Center ATLANTIC

SCAP Challenges

- Challenges identified in feedback from our end users:
  - Limited SCAP content for many platforms
  - Limited visibility of content in development
  - Content does not always run in validated tools
  - Complexity of writing content

SPAWAR Systems Center ATLANTIC

SCAP Challenges (cont)

- Limited SCAP content for many platforms
  - As of September 2010, production quality content only exists for FDCC:
    - Windows XP (OS and Firewall)
    - Windows Vista (OS and Firewall)
    - Internet Explorer 7
  - The United States Configuration Baseline (USGCB) will soon provide content for:
    - Windows 7
    - Internet Explorer 7
  - No production quality content available for:
    - Any Server OS
    - Any Linux/UNIX OS/Mac OS X

SPAWAR Systems Center ATLANTIC

SCAP Challenges (cont)

- Limited visibility of SCAP content in development
  - A common question: “Is anyone creating content for platform X?”

SCAP Challenges (cont)

- Content does not always run in validated tools
  - The most common question: “Why doesn’t the SCAP content I downloaded from XYZ work in my SCAP validated tool?”
  - No official validation process for SCAP content

SPAWAR Systems Center ATLANTIC

SCAP Challenges (cont)

- Complexity of writing SCAP content
  - No “Easy Button” for SCAP content development exists, yet.
    - Tools under development:
      - G2’s eSCAPe Editor
      - MITRE’s Benchmark Editor
  - XCCDF & OVAL are powerful languages, but with power comes complexity
    - Requires detailed expertise with OS API’s
    - Complex nested logic required to perform many checks
    - Content needs to be thoroughly tested

SPAWAR Systems Center ATLANTIC

The SCAP Community Moving Forward

- As SCAP application developers, we hope to see the community address the following suggestions:

SPAWAR Systems Center ATLANTIC

Moving Forward (cont)

- Improve methods for verifying that SCAP content is “Valid”
  - Essential to the long-term success of SCAP
  - We were excited to see NIST’s presentation “Verification of SCAP Content” on September 27, 2010

Moving Forward (cont)

- Improve ease of reporting and tracking content issues
  - Create a web-based bug tracking facility for major content streams such as FDCC/USGCB
    - Ensure all items are tracked and resolved
    - Provide online and email based notifications of updates
    - Prevent duplication of reported issues
    - Promote more end user testing

SPAWAR Systems Center ATLANTIC

Moving Forward (cont)

- Create a web-based repository for all publicly available compliance checks
  - Centralize content to prevent duplication of effort
  - Allow users to generate custom streams of checks

SPAWAR Systems Center ATLANTIC

Moving Forward (cont)

- Promote collaboration on content development
  - Create a web-based content development website
    - Advertise ongoing content development efforts and prevents duplication of effort across agencies
    - Facilitate collaboration on large and complicated content streams

Suggestions for contributing to the SCAP effort

- Be proactive:
  - Test the existing SCAP content and report issues to content authors
  - Fund development of publicly available content
  - Fund development of content editing applications
  - Provide feedback to SCAP-Validated application developers
  - Fund development of SCAP Validated applications
    - (such as SCC) ☺

Suggestions for contributing to the SCAP effort (cont)

- Get more knowledgeable in SCAP:
  - Attend SCAP Events:
    - scap.nist.gov/events/
  - Sign up for forums
    - scap.nist.gov/community.html
    - oval.mitre.org/community/registration.html
  - Start using a SCAP validated application!

The SCAP Compliance Checker

- SCC is a SCAP Validated FDCC Scanner
  - SCC Version 1.1 supports

Specification	Version
SCAP	**1.0**
OVAL	**5.4**
XCCDF	**1.1.4**
CPE	**2.2**
CCE	**5.0**

  - Platforms Officially Supported
    - Windows XP (Operating System and Firewall)
    - Windows Vista (Operating System and Firewall)
    - Internet Explorer 7

SPAWAR Systems Center ATLANTIC

SCC - Features

- Runs on Windows 2000/XP/2003/Vista/2008/R2/7
- Local and remote reviews
  - GUI-based
  - CLI-based
- Custom content installation
- Deviation editing
- Custom compliance thresholds
- Creates human readable HTML and text reports
- Aggregates XCCDF results from any SCAP validated application

SPAWAR Systems Center ATLANTIC

SCC - Timeline

Date	Milestone
February 2008	IRS Funded Development Began
February 2009	Officially SCAP Validated
May 2009	Version 1.0 Released
April 2010	Version 1.1 Released
May 2010	NSA Funds New Feature Development
November 2010	Estimated Release Date for Version 2.0

SPAWAR Systems Center ATLANTIC

SCC - Who Can Use It?

- Any Federal Government Employee or Contractor
- No per-seat license costs
- Can be used enterprise wide on any number of computers

SCC - Who's Using It?

As of September 2010

- 159 email requests for software
- 81 unique organizations including:
  - •Internal Revenue Service (IRS)
  - •National Security Agency (NSA)
  - •US Army, Navy, Air Force, & Marines
  - •US Joint Forces Command
  - •Department of Energy (DOE)
  - •Department of Homeland Security (DHS)
  - •Department of Transportation (DOT)
  - •Federal Aviation Administration (FAA)
  - •Federal Bureau of Investigations (FBI)
  - •Department of the Interior (DOI)
  - •National Aeronautics and Space Administration (NASA)
  - •United States Coast Guard (USCG)
  - •United States Geological Survey (USGS)
  - •Department of Defense Intelligence Information System (DODIIS)
  - •National Geospatial-Intelligence Agency (NGA)

SPAWAR Systems Center ATLANTIC

SCC - Software Demonstration

- Basic usage
  - Performing a review
  - Entering deviations
  - Installing new content
  - Generating multi-computer summary reports
  - Viewing reports
- New features for 2.0
  - Updated from OVAL 5.4 to OVAL 5.7
  - Automatically updating patch content
  - Ability to run directly from CD-ROM without installation
  - Performing OVAL vulnerability checks
  - Added support for creating ARF XML results
  - Added support for creating Draft Cyberscope XML results

SPAWAR Systems Center ATLANTIC

What's next for SCC?

- 2010
  - Release of version 2.0 in November 2010
- 2011
  - Validation to SCAP version 1.1
  - Add support for OCIL (Open Checklist Interactive Language)
  - Add support for more platforms
    - Linux?
    - Mac OS X?
    - Solaris?
  - Support for future releases of OVAL (5.8, 6.0 etc..)
  - Other suggestions?

SPAWAR Systems Center ATLANTIC

Special Thanks

- Internal Revenue Service
  - Janice Harrison
  - Denise Crisco
- National Security Agency
  - Lt. Col. Joseph L. Wolfkiel
  - Michael A. Kinney

SPAWAR Contact Information

- SPAWAR Atlantic
  - Jack Vander Pol
  - Kyle Stone
- Email

  scc_lant-scc@navy.mil
- Web

  http://nvd.nist.gov/validation_spawar.cfm

SPAWAR Systems Center ATLANTIC

Closing Thoughts

- SCAP provides the framework for standardized security automation, but it takes a community effort to succeed
- Your involvement matters and helps everyone
  - Push for long term, challenging improvements
  - Fund content development & testing
  - But most importantly, use SCAP