



Integrating & Automating Security Functions through SCAP

Samara Moore, IT/Cyber Security Policy Advisor
Ari Miller, Sr. Information Security Consultant

U.S. Department of Energy

Agenda

- SCAP De-Mystified
- SCAP Tools
- Benefits of SCAP
- SCAP Use Case: FDCC
- SCM at DOE
- Challenges
- Resources

SCAP De-Mystified

- What is SCAP?
 - Security Content Automation Protocol (SCAP)
 - Set of specifications that provide a standard format and nomenclature, to be used by security software for communicating information on software flaws and security configurations



Enumeration

Vulnerability
Measurement
& Scoring

Expressions &
Checking

SCAP De-Mystified

- What is SCAP?
 - Supports information sharing and interoperability
 - Standard input and output format for vulnerability and configuration management products
 - Standardized expression of security configurations and software flaws
 - Vulnerability management specifications that enable standardized and automated vulnerability management, measurement, and policy compliance evaluation

SCAP De-Mystified

SCAP Protocol Components ¹		
SCAP Component	Description	Maintaining Organization
Enumerations		
Common Configuration Enumeration (CCE)	Nomenclature and dictionary of system security issues	MITRE Corporation
Common Platform Enumeration (CPE)	Nomenclature and dictionary of product names and versions	MITRE Corporation
Common Vulnerabilities and Exposures (CVE)	Nomenclature and dictionary of security-related software flaws	MITRE Corporation
Expression and Checking Languages		
Extensible Configuration Checklist Description Format (XCCDF)	Language for specifying checklists and reporting checklist results	National Security Agency (NSA) and NIST
Open Vulnerability and Assessment Language (OVAL)	Language for specifying low-level testing procedures used by checklists	MITRE Corporation
Vulnerability Measurement and Scoring		
Common Vulnerability Scoring System (CVSS)	Specification for measuring the relative severity of software flaw vulnerabilities	Forum of Incident Response and Security Teams (FIRST)

¹NIST SP 800-117, "Guide to Adopting and Using the Security Content Automation Protocol (SCAP) (DRAFT)"

SCAP De-Mystified

■ Content / Reference Data

Software flaws

- <http://nvd.nist.gov>
- Sources include:
 - US CERT Technical Alerts
 - US CERT Vulnerability Alerts (CERTCC)
 - MITRE OVAL Software Flaw Checks
 - MITRE CVE Dictionary

Security configurations

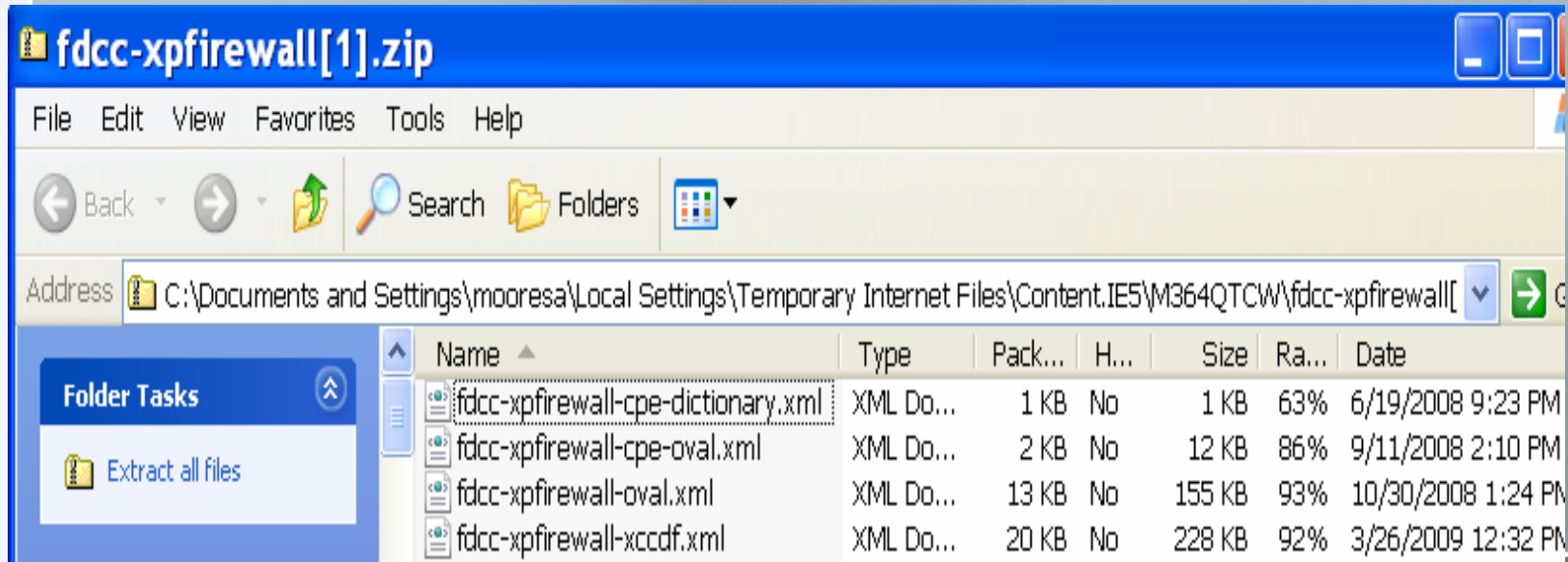
- <http://checklists.nist.gov>
- FDCC currently the only content published by NIST using SCAP protocol
- Other checklists provided
 - Multiple platforms and software
 - Does not use SCAP protocol
 - Content can be used to create custom list using SCAP protocol

SCAP Tools

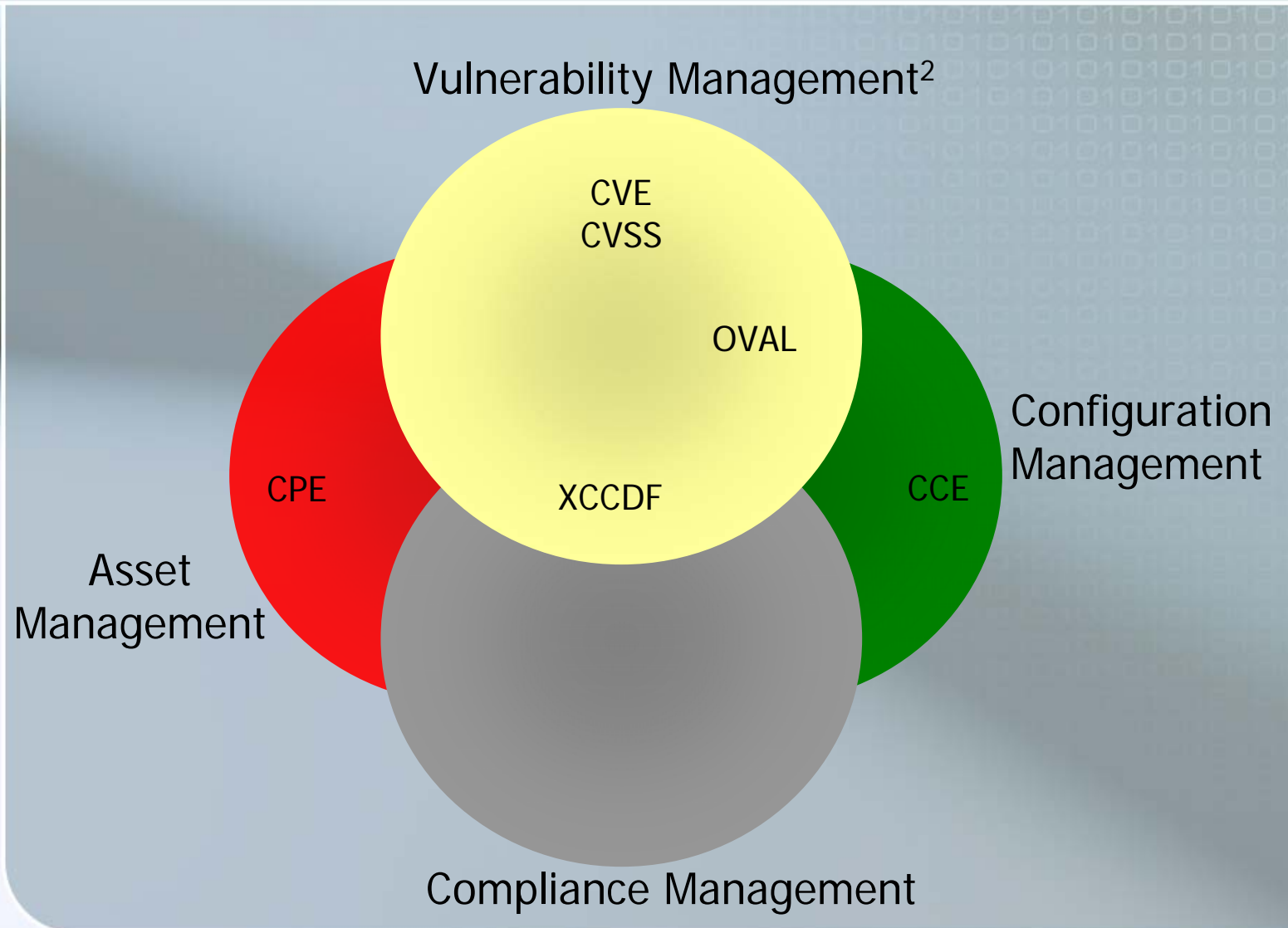
- NIST SCAP Validation Program
 - Independent labs, accredited by the NIST National Voluntary Laboratory Accreditation Program (NVLAP)
 - Conduct the tests contained in the [SCAP Validation Program Derived Test Requirements Document](#), on information technology (IT) security products
 - Based on the test report, the SCAP Validation Program validates the product
 - Validations awarded to vendor products are publicly posted on the NIST SCAP Validated Tools web page at <http://nvd.nist.gov/scaproducts.cfm>
 - 24 validated products
 - 16 vendors

How SCAP Works

- Download package with SCAP configuration content and import into any SCAP tool
- Set of XML files provide:
 - List of checks
 - How to do checks, parameters
 - Standard reporting



SCAP – Integrating IT & Security



² Derived from NIST SCAP documentation

Benefits of SCAP

- “More with Less”
 - Security configuration validation
 - Requirements tracing
 - NIST SP 800-53 mapping
 - Standard security enumerations
 - Standard reporting formats
 - Vulnerability measurement

Benefits of SCAP

- Simplifies management of standard security configurations
 - FAR Part 39, section 39.101, paragraph (d) - requires use of common security configurations available from <http://checklist.nist.gov>
 - FDCC
 - Configuration standards
- Streamlines configuration management
- Supports continuous monitoring
 - NIST SP 800-53, CA-7, "Continuous Monitoring"
 - Automated monitoring of selected controls
 - Identification of changes to security configuration
 - Ability to monitor based on risk determination, not limitation of resources

SCAP Use Case: FDCC

■ FDCC Overview

- OMB Mandated Requirement (M-07-11)
Effective February 1, 2008 all federal agencies with Microsoft Vista™ or XP™ operating systems must adhere to these security configuration standards
- Provides a Standard Security Configuration developed through collaborative effort among NIST, DoD, DHS and private sector
 - Supported by SCAP

SCAP Use Case: FDCC

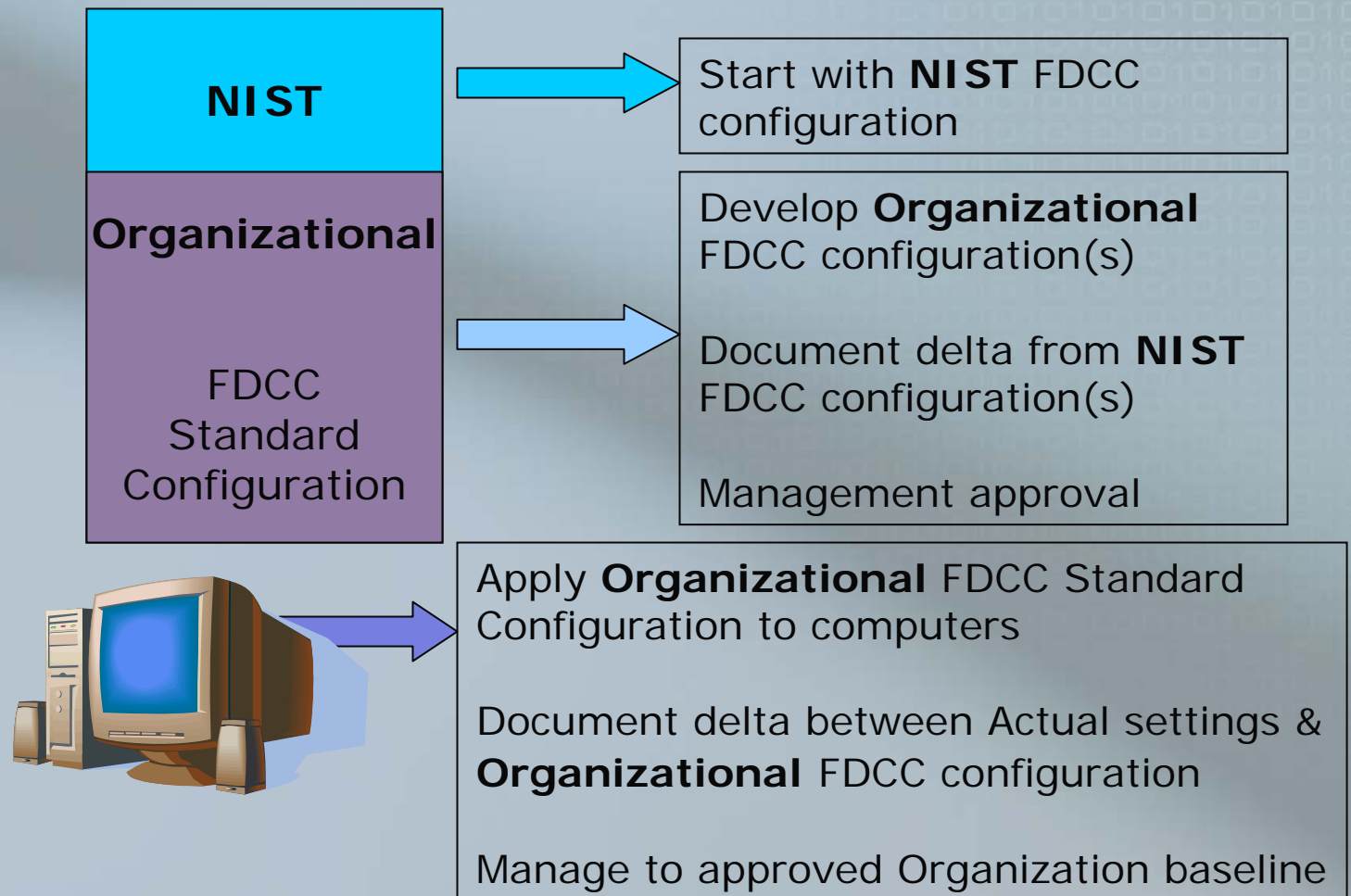
- OMB Requirements for FDCC
 - **Develop** FDCC Standard Configurations to be “adopted and implemented”
 - **Document** differences between Agency FDCC Standard Configurations & NIST FDCC baseline
 - **Implement** FDCC security settings on “all Windows XP and Vista” computers
 - **Include** FAR language in all contracts to support common configuration standards (see OMB M-07-18)
 - *“...new acquisitions include these common security configurations and information technology providers certify their products operate effectively using these configurations. ”*
 - **Use** SCAP tools to automate compliance monitoring

SCAP Use Case: FDCC

- FDCC Implementation Approach
 - Similar to implementing other checklists
 - Conduct risk assessment
 - Develop POA&M for planned configurations
 - Obtain approved deviation for configurations that cannot be implemented
 - Document in SSP
 - FDCC vs. Other Checklists
 - Supported by SCAP
 - Configurations vetted
 - Standard configuration mandated by OMB

SCAP Use Case: FDCC

■ An FDCC Implementation Approach



SCAP Use Case: FDCC

- DOE FDCC Implementation Approach
 - Mission focused
 - Multiple, diverse missions
 - Federated model
 - Security management programs for each high level mission area
 - Support local risk-based tailoring
 - Each Energy Program Office and/or Sites may have a unique organizational FDCC baseline
 - SCAP allows tailoring
 - Outreach and awareness
 - Began with data calls collecting basic information
 - Conducted multiple conference calls
 - Gradually increased data collected
 - Results show improved understanding and increased implementation

SCM at DOE

- DOE Security Configuration Management (SCM) Program
 - SCM Program Mission
 - Assist in a broad implementation of SCAP configurations to protect DOE information and information systems, commensurate with information value, associated threats, and mission needs
 - SCM Program Vision
 - Departmental adoption of technology standards, automation tools, processes, and configurations that effectively utilize the SCAP to manage security configurations where appropriate

SCM at DOE

- Outreach and awareness activities
 - Promote the understanding and benefits of SCAP
- DOE OCIO provides support for SCAP implementation
- DOE policy requires use of standard configurations, but does not require use of SCAP
 - Except for OMB FDCC SCAP mandate

Challenges

- Good practice, but not required (except for FDCC)
 - Requires initial investment of resources (\$\$, staff, hw, sw)
 - Difficult to add to list without a mandate
- Clear understanding of SCAP
 - Beyond FDCC
 - Realize full potential when used to integrate IT components

Challenges

- Developing a structured enterprise approach
- Resources
 - Tight cyber security budgets with limited funding for non-compliance related requests
- SCAP maturity level
 - Limited content in quantity (other checklists) and quality (false positives)
 - Reporting
 - Validation program

Challenges

- Plans to address challenges
 - Outreach and awareness
 - Presentations and information sessions
 - Flyers and handouts
 - Show the benefits and potential of SCAP, as compared to current operations
 - Enterprise approach
 - Internal workgroup to define scope and implementation plan
 - Utilize enterprise wide agreements
 - Actively participate in SCAP development
 - Share lessons learned and challenges

Resources

- NIST SCAP website - <http://scap.nist.gov>
- National Vulnerability Database - <http://nvd.nist.gov>
- OMB M-07-11, Implementation of Commonly Accepted Security Configurations for Windows O/S
- OMB M-08-22, Guidance on the Federal Desktop Core Configuration (FDCC)

Questions and Discussion

Questions?

Contact Information:

Samara Moore – samara.moore@hq.doe.gov

Ari Miller – ari.miller@hq.doe.gov