Security Configuration Management

Security Automation Conference

September 28, 2010

Kelley Dempsey

Computer Security Division
Information Technology Laboratory

The Threat Situation

Continuing serious cyber attacks on public and private sector information systems, large and small; targeting key operations and assets…

- Attacks are organized, disciplined, aggressive, and well resourced; many are extremely sophisticated.
- Adversaries are nation states, terrorist groups, criminals, hackers, and individuals or groups with intentions of compromising federal information systems.
- Effective deployment of malicious software causing significant exfiltration of sensitive information (including intellectual property) and potential for disruption of critical information systems/services.

The Flash Drive Incident

Targeting U.S. Department of Defense—

- Malware on flash drive infected military laptop computer at base in Middle East.
- Foreign intelligence agency is the suspected source.
- Malware uploaded itself to Central Command network.
- Code spread undetected to classified and unclassified systems establishing digital beachhead.
- Rogue program poised to silently steal military secrets.

McAfee Threats Report (2Q 2010)*

- McAfee saw 550,000 and 280,000 AutoRun attacks (malware that uses USB or portable storage devices to spread) in April and May respectively
- The top detection continues to be the Generic!atr Trojan, which was reported on nearly 9 percent of machines scanned worldwide by McAfee.
- In general, malware being produced is on the increase: 10 million new pieces of malware in the first half of this year! (as opposed to 9 million in the same period last year)
- This makes the first six months of 2010 the most active half-year ever for total malware production.

*http://www.mcafee.com/us/threat_center/default.asp

Potentially Unwanted Programs (PUPS)*

- Created by an entity for a purpose that benefits the entity but usually not the user
- Often alters the security state of the computer on which they are installed or the privacy posture of the computer user
- May intentionally shut down, disable, or weaken security tools such as browser security settings, firewall settings, or AV products.
- Peer-to-Peer file-sharing programs often act as a carrier for PUPs and other malware.
- **A robust and automated security configuration management program would greatly reduce the effectiveness of PUPs and other malware by detecting and preventing installation of unauthorized software** (whitelists, etc.) **and/or notifying administrators of changes to baseline configurations.**

*http://www.mcafee.com/us/threat_center/default.asp – info taken from a McAfee White Paper on PUPs

SCM – What is It?

- Security configuration management is the management and control of configurations for an information system with the goal of enabling security and managing risk.
- SCM does require an ongoing investment in time and resources
- SCM is a continuous, ongoing activity that touches all stages of the system development life cycle
- SCM should be incorporated into any existing organizational configuration management program

Guide for Security Configuration Management of Information Systems

NIST Special Publication (SP) 800-128:

- Provides guidance for implementation of Configuration Management (CM) family controls from 800-53 Rev 3
- Initial Public Draft released 18 March 2010
- Public comments were accepted through 14 June 2010
- Implementation and continued operation of ***many*** **non**-CM controls are dependent on secure configurations and configuration change control

SP 800-128 Phases

- Planning Phase
- Configuring to a Secure State Phase (implementing)
- Maintaining the Secure State Phase
- Monitoring

Planning Phase

- Establish/Develop Organizational and System level policies and procedures (CM-1)
- Develop Configuration Management Plan (CM-1/CM-9)
- Establish Change Control Board (CM-3)
- Develop IS Component Inventory (CM-8)
- Indentify Configuration Items (CM-3)

Configure to Secure State Phase

- Establish Secure Configurations (CM-6/CM-7)
- Implement & test Secure Configurations (CM-6/CM-7) and modify if necessary
- Document the finalized Secure Baseline Configuration (CM-2)

Maintaining Secure State Phase

- Implement Access Restrictions for Change (CM-5)
- Implement Configuration Change Control process to manage changes to the Baseline Configuration (CM-3)
- Conduct Security Impact Analyses for changes (CM-4)
- Document changes (new baseline) and archive previous baseline(s) (CM-2)

Monitor Phase

- Assess configurations on an ongoing basis using automated tools
  - Changes to Baselines (actual configuration settings, unauthorized software, etc.)
  - Changes in IS Component Inventory
- Analyze causes of unauthorized changes
- Report configuration status to senior management [Authorizing Official, RE(F), etc.]
- Monitor Phase activities support the generation of metrics
- Monitor Phase activities support all CM Family controls

800-128 Appendices

- The usual suspects
  - General references
  - Glossary
  - Acronyms
- Sample Templates
  - SCM Plan
  - Change Request
- Best Practices w/references to NIST SPs
- SCM Process Flowcharts

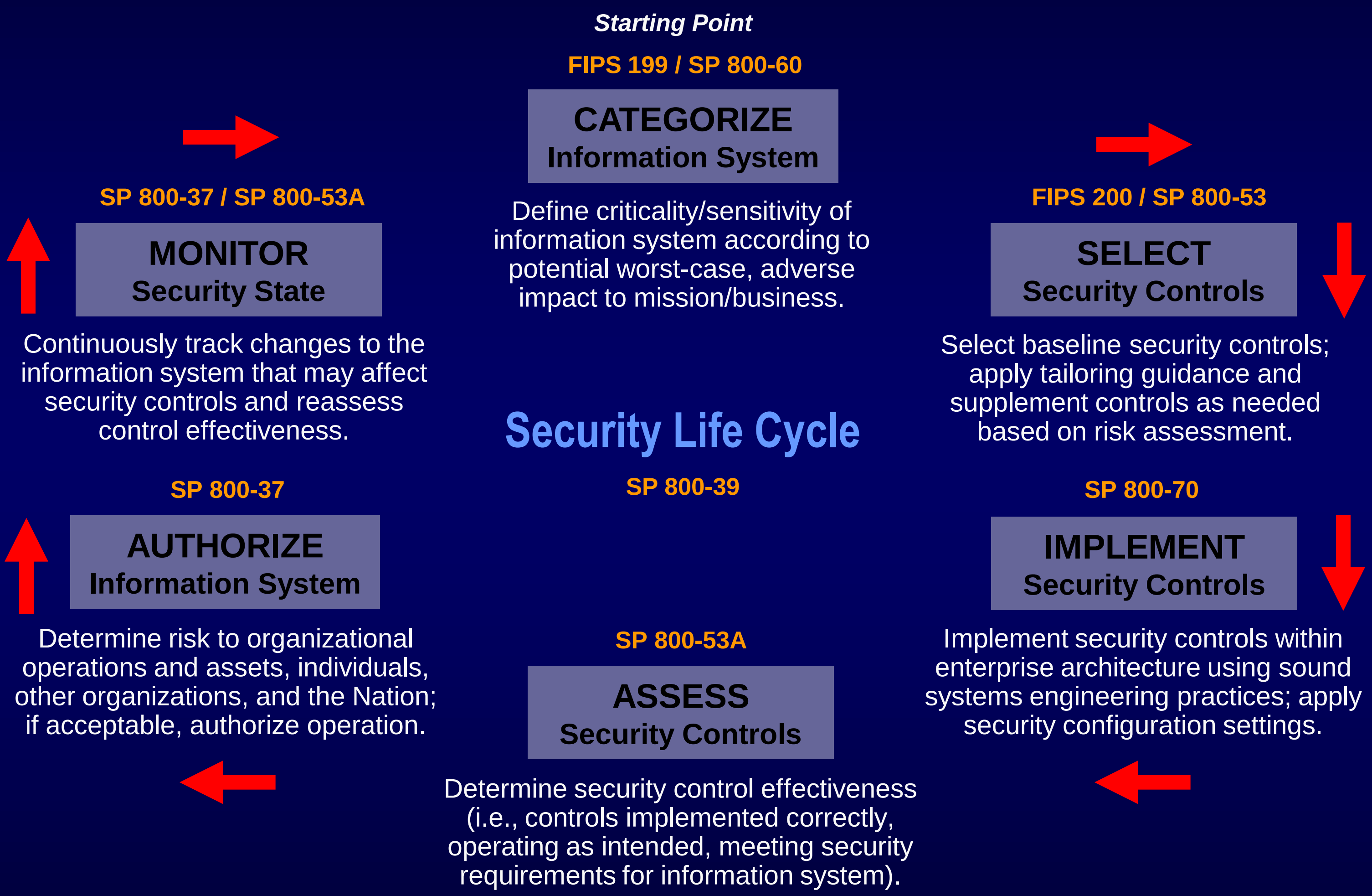
SCM - Why Is It Important?

- Change happens!
- Once a secure configuration is implemented, subsequent changes must be controlled
- In the absence of SCM, an asset that is securely configured today will most likely not be secure within a short period of time
- SCM ensures configuration changes are controlled (approved, analyzed, tested)

SCM - Why Is It Important? (#2)

- Without SCM, unauthorized, unanalyzed, and untested changes will render systems, networks, and organizations vulnerable to a wide range of threats
- In addition, SCM:
  - Facilitates asset management
  - Improves incident response, help desk, disaster recovery, and problem solving
  - Aids in software development and release management
  - Enables process automation
  - Supports compliance with policies and preparation for audits
- SCM is vital to the establishment and maintenance of security of information and information systems

Risk Management Framework



Starting Point

FIPS 199 / SP 800-60

CATEGORIZE
Information System

Define criticality/sensitivity of information system according to potential worst-case, adverse impact to mission/business.

FIPS 200 / SP 800-53

SELECT
Security Controls

Select baseline security controls; apply tailoring guidance and supplement controls as needed based on risk assessment.

SP 800-70

IMPLEMENT
Security Controls

Implement security controls within enterprise architecture using sound systems engineering practices; apply security configuration settings.

SP 800-53A

ASSESS
Security Controls

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

SP 800-37

AUTHORIZE
Information System

Determine risk to organizational operations and assets, individuals, other organizations, and the Nation; if acceptable, authorize operation.

SP 800-37 / SP 800-53A

MONITOR
Security State

Continuously track changes to the information system that may affect security controls and reassess control effectiveness.

Security Life Cycle

SP 800-39

NIST SP 800-128 and the RMF (#1)

- RMF - Categorize Step
  - Planning Phase of SCM
  - System information types and overall system impact level, along with organization- and system-level assessment of risk, determine the 800-53 baseline to be applied and level of effort for SCM implementation
- RMF - Select Step
  - Planning Phase of SCM
  - Tailor and supplement CM family of controls
- RMF - Implement Step
  - Configure to Secure State Phase of SCM
  - Establish, implement, test for functionality, and document Secure Configurations/Baselines

NIST SP 800-128 and the RMF (#2)

- RMF - Assess Step
  - Configure to Secure State Phase of SCM
  - Test secure configuration implementations for effectiveness (i.e., is the secure configuration operating as intended with respect to protecting the system)
- RMF - Authorize Step
  - Configure to Secure State Phase of SCM
  - Authorizing Official may require changes to the secure configuration and/or implementation of additional controls
- RMF - Monitor Step
  - Maintain the Secure State Phase of SCM
  - Monitor Phase of SCM

NIST SP 800-128 and SCAP

- SCAP = Security Content Automation Protocol
- The primary purpose of SCAP is to improve the automated application, verification, and reporting of commercial information technology product-specific **security configuration settings**.
- SCAP-expressed checklists can **map to secure configuration settings**
- If SCAP-enabled tools are not available, plan ahead by **implementing SCAP-expressed checklists for secure configurations**
- Encourage security software vendors to incorporate support for SCAP specifications (CCE, CPE, CVE, XCCDF)

NIST SP 800-128 and Continuous Monitoring

An effective Continuous Monitoring program includes:

- **Configuration Management and Control Processes**
  - Configuration Management is an important precondition to the success of a Continuous Monitoring program
  - Without configuration control down to the component level, monitoring will result in inaccurate risk data
- **Security impact analyses** on changes to systems and environments of operation
  - SIA determines the extent to which a change may effect implemented security controls
  - SIA is an essential factor for SCM and thus also for Continuous Monitoring

Contact Information

100 Bureau Drive Mailstop 8930
Gaithersburg, MD USA 20899-8930

Project Leader

Dr. Ron Ross
(301) 975-5390
ron.ross@nist.gov

Administrative Support

Peggy Himes
(301) 975-2489
peggy.himes@nist.gov

Senior Information Security Researchers and Technical Support

Marianne Swanson
(301) 975-3293
marianne.swanson@nist.gov

Pat Toth
(301) 975-5140
patricia.toth@nist.gov

Kelley Dempsey
(301) 975-2827
kelley.dempsey@nist.gov

Arnold Johnson
(301) 975-3247
arnold.johnson@nist.gov

Web: csrc.nist.gov/sec-cert

Comments: sec-cert@nist.gov