

# Developing a Standardized Remediation Language

September 25, 2008

Chris Johnson  
Computer Security Division  
Information Technology Laboratory



**NIST**  
National Institute of  
Standards and Technology

# Agenda

- Statement of Need
- Goals
- Remediation and the Federal Risk Management Framework
- Terminology
- Data Model Requirements



# Statement of Need

Implement a standard language to express and implement remediation/modification actions for software flaws and system configuration settings



# Goals

- Perform accurate and effective remediation
- Achieve consistent and repeatable results
- Provide interoperability across vendors and tool types
- Maximize reuse of content to reduce time, effort and expense
- Develop an open remediation standard applicable to a wide set of use cases
  - Vulnerability Management
  - Compliance Management
  - Configuration Management
  - Asset Management



# Remediation and the Federal Risk Management Framework

- Federal Risk Management Framework applicability -- *Implement, Assess, Monitor*
- Essential capability for implementing:
  - System configuration changes
  - Vendor software patches
  - Vendor software installation
  - Product updates



# Terminology

- Remediation - effect the changes necessary to remedy a known software flaw or configuration issue
- Modification - action taken to implement a desired change on a system
- Mitigation - action taken to reduce the severity of a security issue



# Data Model Requirements Metadata (1)

- Unique identifier for the modification
- Human-readable description of the modification
- Human-readable description of pre-conditions  
(i.e., state system must be in before modification)
- Reference other related SCAP data  
(e.g., CVE/CCE/OVAL identifiers)
- Express applicability using CPE and CPE metadata



# Data Model Requirements

## Metadata (2)

- Superseded - ability to identify previous remediation content that has been replaced by the current content
- Deprecated - ability to preserve legacy content/capabilities, yet discourage its use (often needed for backwards compatibility)
- Human-readable and machine-readable enumerations of potential side effects



# Data Model Requirements Chaining/Order of Operations

Allow an order of operations to be declared for modifications based on:

- Technical Pre-conditions
- Severity/Operational Urgency
- Other factors (reboot/restart requirements)



# Data Model Requirements Remediation Actions

- Identify modifications that can be performed in parallel
- Choice of multiple acceptable modifications
- Identify modifications that are mutually exclusive
- Return an error/status messages for each modification
- Encapsulate the remediation script or executable
- Allow for enumeration of interactive parameters/metadata



# Data Model Requirements

## Undo/Rollback

- Identify modifications that can be undone or rolled back
- Express temporal constraints on rollback capability
- Encapsulate the undo script or executable
- Return an error/status message for each undo operation



# Data Model Requirements

- Describe reboot requirements
  - Immediate - no user intervention permitted
  - Immediate - upon user acceptance
  - Deferred - user specified
  - Deferred - next reboot
- Describe restart requirements



# General Requirements

- User-directed remediation:
  - Selective remediation - user chooses which modifications to perform
  - Situational tailoring - user-supplied parameters that are used instead of the default settings
- Default remediation
- Policy-based remediation



# General Requirements

- Support source authentication and integrity
  - Provides a basis for establishing trust
  - Means of according a data pedigree
  - Enables attribution and accountability
  - Assists in content stewardship and maintenance



# The Way Ahead

- Submit comments regarding requirements discussed in this presentation
- Describe and submit additional use cases and requirements
- Participate in community discussions



# Remediation Language Information

OVAL Remediation Forum Discussion List

Registration Link:

<http://oval.mitre.org/community/registration.html>

Discussion List Archives Link:

<http://oval.mitre.org/community/archives.html>

Presenter: Chris Johnson

Email: [christopher.johnson@nist.gov](mailto:christopher.johnson@nist.gov)

