# Remediation Standardization Status

Matthew N. Wojcik

MITRE

© 2009 The MITRE Corporation. All rights reserved.

# Background

- Goal: Replicate for remediation the success SCAP has had transforming IT security assessment
  - Now that we've found the problems, what do we do about them?
- Approach: Identify technical use cases for remediation and analyze for possible standardization
  - What are common processes for fixing discovered problems, and how could standardization help?
- Result: Proposed remediation specifications
  - The names, data exchange formats, and languages we need to share for remediation interoperability
  - See "Proposed Open Specifications for Enterprise Information Security Remediation" by Wojcik, Wunder, Kerr and Waltermire
- Common Themes: Communication, interoperability and automation

© 2009 The MITRE Corporation. All rights reserved.

# Definitions

- Remediation: A security-related set of actions that result in a change to a computer’s configuration.  May be motivated by discovered vulnerabilities or mis-configurations.

- Vulnerability: Something that lets an attacker:
  - Execute unauthorized commands
  - Bypass restrictions on data access or modification
  - Pose as another entity
  - Affect the availability of a system resource

- Mis-configuration: Any configuration state that does not comply with an organization’s security policy

© 2009 The MITRE Corporation. All rights reserved.

# Basic Identified Use Cases

On one or more computing assets:

- Remediate all problems found by a prior assessment
- Remediate a subset of problems found by a prior assessment
- Apply one or more remediations regardless of current state
  - I.e., initiated by policy rather than an assessment

© 2009 The MITRE Corporation. All rights reserved.

# Common Remediation Enumeration (CRE)

- A method for assigning common identifiers (names) to remediations
  - Similar concept to CVE and CCE

- A CRE entry includes the minimum information necessary to show why the item is in the list, and differentiate it from other entries
  - Increases stability of CRE entries

- CRE data fields:
  - Unique identifier
  - Human-oriented prose description of the remediation
  - Supporting references
  - Metadata about the entry
    - Creation and modification dates, deprecation status, version, provenance

© 2009 The MITRE Corporation. All rights reserved.

# CRE Use Cases

**CRE IDs can be used as unambiguous shared identifiers in:**

- **System Design Requirements**
  - **"Before deployment of systems running cpe:/o:example:foo-os, perform cre:/com.example.cre:4"**
- **Remediation Policy Statements**
  - **"If CVE-2009-XXXX is found on an internet-facing system, acceptable remediation options include cre:/org.example.cre:23 and cre:/com.example.cre:483"**
- **Response to Assessment**
  - **"Perform cre:/org.example.cre:79 on host 10.4.3.204 because it is out of compliance with requirements for CCE-2351-5"**
- **Remediation Results**
  - **"cre:/org.example.cre:4 failed due to lack of disk space"**

© 2009 The MITRE Corporation. All rights reserved.

# CRE Entry Example

| | |
|---|---|
| ID | cre:/org.example.cre:513 |
| DESCRIPTION | Install patch 'WindowsXP-KB971486-x86-ENU.exe'. |
| REFERENCES | (1) http://www.microsoft.com/technet/security/Bulletin/MS09-058.mspx<br>(2) http://support.microsoft.com/kb/971486 |
| Created | 2009-10-15 |
| Modified | 2009-10-15 |
| Deprecated | False |
| Version | 1 |
| Submitted By | ACME Inc. |

© 2009 The MITRE Corporation. All rights reserved.

# Further CRE Examples

Some remediation statements to consider:

- “Set minimum password length to 12 characters”
- “Uninstall cpe:/a:example:web-browser:3.5”
- “Disable telnet server via xinetd”
- “Require CTRL-ALT-DEL for logon, by setting the registry key HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System\DisableCAD to 0”
- “Set file permissions for /etc/shadow to 400”

© 2009 The MITRE Corporation. All rights reserved.

# Comparable Statements

Remediation statements are made at various levels of granularity. What will receive a single CRE vs multiple CREs?

Food for thought:

- "Install patch for MS09-055"
- "Install patch Windows6.0-KB973525-x64.exe"

- "Set permissions on /etc/shadow to 400"

- "Require CTRL-ALT-DEL for logon"
- "Require CTRL-ALT-DEL for logon via local registry edit"
- "Require CTRL-ALT-DEL for logon via Group Policy"

- "Disable telnet server via xinetd"
- "Disable telnet server by changing mode on /usr/sbin/in.telnetd to 0"

© 2009 The MITRE Corporation. All rights reserved.

# Comparable Statements: Method and Effect

**Proposed: Remediation statements that describe the same method and effect receive the same CRE.  Differing method or effect receive different CREs.**

**Rationale:**

- **Allow selection of method appropriate to the environment**
- **Selecting a specific CRE should fully specify the expected system state change**

© 2009 The MITRE Corporation. All rights reserved.

# Comparable Statements Revisited

## Single CRE:

- "Install patch Windows6.0-KB973525-x64.exe" – Applies to multiple versions of Windows (x64 Vista & Server 2008)
- "Set permissions on /etc/shadow to 400" – cross-vendor

## Multiple CREs:

- "Require CTRL-ALT-DEL for logon via local registry edit"
- "Require CTRL-ALT-DEL for logon via Group Policy"

- "Disable telnet server via xinetd"
- "Disable telnet server by changing mode on /usr/sbin/in.telnetd to 0"

## Not CREs:

- "Install patch for MS09-055"
- "Require CTRL-ALT-DEL for logon"

© 2009 The MITRE Corporation. All rights reserved.

# Method & Effect: Some Observations

- Method & Effect must be described in CRE entries
  - Must be clear to the reader how CREs differ

- Different Methods may have the same observable Effects depending on your perspective
  - E.g., GPO and local registry edit may both lead to the same value in the local registry
  - Implication: Careful consideration of M&E is required when creating CREs
  - Implication: It may not be possible for a follow-up assessment of host state to determine which CRE was performed

- Method & Effect content decision allows for cross-platform CREs
  - Question: What are remediation vendors' practices?
  - Question: How will this affect federated CRE creation?

© 2009 The MITRE Corporation. All rights reserved.

# Parameters

Many remediation statements suggest the use of parameters.

Food for thought:

- “Set minimum password length to 8”
- “Set minimum password length to 16”

- “Enable telnet server via inetd”
- “Disable telnet server via inetd”

- “Install cpe:/a:example:web-browser:3.5”
- “Uninstall cpe:/a:example:web-browser:3.5”

- “Install patch foo with the /quiet option”
- “Install patch foo with the /nouninstall option”

© 2009 The MITRE Corporation. All rights reserved.

# Parameters: Some Observations

- Assigning separate CREs for different possible parameter values seems unhelpful in most cases

- Configuration controls with simple literal values lend themselves to parameterization
  - Minimum password length, UNIX file permissions

- Configuration statements with conceptual parameters present more difficulties
  - “Enable/Disable” a service – what are the literal values?

- Selecting a parameter value may lead to other options
  - “Install cpe:/a:example:web-browser:3.5 in D:\Program Files\”

© 2009 The MITRE Corporation. All rights reserved.

# Parameters: Further Observations

- Selecting values for certain "parameters" may require different Methods, which violates the Method & Effect rule
  - "Install/Uninstall" an app

- Relationship to Method & Effect is not consistent with a remediation or parameter type
  - Varies between vendors
  - Varies over time

© 2009 The MITRE Corporation. All rights reserved.

# CRE Entry Scope

Additional guidance is needed to determine allowable scope of a single CRE.

- Remediation statements often imply multiple steps
- "Method & Effect" is a yardstick for comparing remediation statements of similar scope

Food for thought:

- "Install patch foo"
  - Install the patch & reboot
- "Disable telnet server via inetd"
  - Edit inetd.conf & restart inetd
- "Disable specified xinetd brokered services"
  - Edit multiple xinetd configuration files
- "Disable Autorun" [Windows XP]
  - Set NoDriveAutoRun key, NoDriveTypeAutoRun, Non-volume AutoPlay Cancellation

© 2009 The MITRE Corporation. All rights reserved.

# CRE Entry Scope: Lowest Level

**Proposed: CRE entries will be created at the lowest level of abstraction that remediates a CVE, mis-configured CCE, or affects installation status of a CPE**

**Rationale:**

- Avoid CREs with varying levels of abstraction
- Allow granular remediation requirements
- Grouping is easier than decomposition

**Observation:**

- “Atomic” remediation actions may still affect the status of multiple CVEs, CCEs, etc.
- Examples:
  - A patch install may fix multiple CVEs
  - Disabling xinetd (one CCE) will also disable subordinate services (each its own CCE)

© 2009 The MITRE Corporation. All rights reserved.

# CRE Entry Scope Examples Revisited

- ✓ "Install patch foo"
  - Install the patch & reboot
- ✓ "Disable telnet server via inetd"
  - Edit inetd.conf & restart inetd
- ✗ "Disable specified xinetd brokered services"
  - Edit multiple xinetd configuration files
- ✗ "Disable Autorun" [Windows XP]
  - Set NoDriveAutoRun key?  NoDriveTypeAutoRun?  Non-volume AutoPlay Cancellation?

© 2009 The MITRE Corporation. All rights reserved.

# For More Information

- Watch the SCAP Emerging Specifications Page at http://scap.nist.gov/emerging-specs/listing.html
  - Overview whitepaper will be posted shortly, CRE and ERD whitepapers & samples forthcoming
- Monitor the emerging-specs@nist.gov email list
  - Announcements and technical discussions
  - See http://scap.nist.gov/community.html to subscribe
- Email the developers
  - Matthew N. Wojcik <woj@mitre.org>
  - John Wunder <jwunder@mitre.org>
  - Matt Kerr <Matt.Kerr@g2-inc.com>
  - David Waltermire <david.waltermire@nist.gov>

© 2009 The MITRE Corporation. All rights reserved.

# Backup Slides

© 2009 The MITRE Corporation. All rights reserved.

# Extended Remediation Data (ERD)

- ERD defines the additional information about CRE entries needed to fully support the identified remediation use cases
- In most cases, this additional information about remediations is available, but not conveniently collected or presented
- As CRE is analogous to CVE, an ERD record is similar to the NVD entry for a CVE
- Keeping ERD separate from CRE reduces the volatility of CRE entries and allows for localized ERD records
- ERD does not prescribe a schema or presentation format

© 2009 The MITRE Corporation. All rights reserved.

# ERD Use Cases

- Remediation Discovery
  - Which CREs are available on a given platform? For a particular CVE or CCE?
- Remediation Selection
  - Of the possible CREs, which are appropriate for the enterprise or situation? Are there known conflicts with critical applications? Are any superseded?
- Order of Remediation Operations
  - Are there pre- or post-remediation steps that must be taken?
- Localized Remediation Details
  - Specify organization-specific information about CREs

© 2009 The MITRE Corporation. All rights reserved.

# ERD Contents

- Unique ERD record identifier
- CRE reference
- Platform list
  - What can the CRE be run on?
- Indicators
  - Why might the CRE be used? E.g., CVEs, CCEs
- Pre-requisites
- Supersedes
  - Does the CRE render others obsolete?
- Operational impact
- Remediation instructions
  - Human- and/or machine-readable
- Reboot required?
- Metadata about the ERD record

© 2009 The MITRE Corporation. All rights reserved.

# ERD Example

| | |
|---|---|
| ID | erd:/com.example.erd:37 |
| CRE REFERENCE | cre:/org.example.cre:513 |
| PLATFORMS | cpe:/o:microsoft:windows_xp::sp2:home<br>cpe:/o:microsoft:windows_xp::sp2:professional<br>cpe:/o:microsoft:windows_xp::sp3:home<br>cpe:/o:microsoft:windows_xp::sp3:professional |
| INDICATORS | CVE-2009-2515, CVE-2009-2516 |
| PRE-REQUISITES | None |
| SUPERSEDES | cre:/org.example.cre:129 |
| OPERATIONAL IMPACT | None |
| INSTRUCTIONS | Execute WindowsXP-KB971486-x86-ENU.exe |
| REBOOT | True |
| Created | 2009-10-15 |
| Submitted By | ACME Inc. |
| Deprecated | False |

© 2009 The MITRE Corporation. All rights reserved.