Identifying Remediation Options and Tracking Extended Information: Technical Issues

February 24, 2010

Background

- Part of ongoing development effort to bring standardization to the remediation lifecycle
- Shared identifiers for remediation options are seen as key first step
  - Per discussion at Developer Days 2009
  - Tentative name: Common Remediation Enumeration (CRE)
- Certain additional data is seen as important to fully support remediation workflows
  - Tentative name: Extended Remediation Information (ERI)

Background continued

- CRE and ERI fit into a remediation landscape presented at 2009 ITSAC in Baltimore
  - http://scap.nist.gov/events/2009/itsac/presentations/day3/Day3_DoD_Wojcik.pdf
- Revised and expanded version to be available in forthcoming NIST IR
- Today’s discussion will focus on technical questions regarding CRE and ERI
- Goal: Community input on Content Decisions

CRE, ERI, and Remediation Workflows

CRE and ERI are intended to facilitate clear and accurate communication in:

- Disclosure of remediation information, by primary vendor or third-party source
- Remediation policy statements by organizations
- Remediation selection, integrating with assessment results & operational factors
- Documenting policy deviations / registering exceptions
- Specific remediation tasking, manual or automated
- Remediation status reporting

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

Introduction to 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

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 (2) http://support.microsoft.com/kb/971486
Created	2009-10-15
Modified	2009-10-15
Deprecated	False
Version	1
Submitted By	ACME Inc.

Extended Remediation Information (ERI)

- ERI 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 ERI record is similar to the NVD entry for a CVE
- Keeping ERI separate from CRE reduces the volatility of CRE entries and allows for localized ERI records
- ERI does not prescribe a schema or presentation format

ERI 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 may be 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

ERI Record Example

ID	eri:/com.example.eri:37
CRE REFERENCE	cre:/org.example.cre:513
PLATFORMS	cpe:/o:microsoft:windows_xp::sp2:home cpe:/o:microsoft:windows_xp::sp2:professional cpe:/o:microsoft:windows_xp::sp3:home 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

Previous Decision 1

Partial fixes, mitigating actions, workarounds will be assigned CREs as well as “complete fixes”

- Justification: This is a subjective distinction which may vary between organizations for the same remediation action
- Corollary: There must be some mechanism for organizations to indicate whether a CRE is a “complete fix” or something else

Previous Decision 2

CREs will be assigned on a per-platform, rather than cross-platform, basis

- Justification: Strong consensus expressed at ITSAC 2009
- Justification: Significantly increased complexity in expressing ERI for cross-platform CREs
- Consequence: Many more CREs must be issued and maintained
- Feedback from primary-source vendors lacking
- Various details still must be worked out
- General problem: What’s a “platform”?

Basic Content Decision: Method & Effect

When considering remediation statements, details of the Method and Effect of possible approaches will determine how CREs are assigned

Rationale:

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

Method & Effect: Min Password Length

- Example statement: “Set the minimum password length on Windows XP to 18 characters”
- Some possible options:
  - Use local API (NetUserModalsSet)
  - Use a local GPO
  - Use a domain GPO
- How should CREs be assigned for this statement?

Aspects of Method to Consider

- Is the location of the Method important? E.g., change directly on the local system vs. something like domain-level Group Policy

- For local changes, distinguish between a vendor-supplied utility and a third-party application? E.g., GUI to adjust file access control vs. xcacls.exe vs. third-party

Aspects of Effect to Consider

- Immediacy of Effect? Examples:
  - Immediately
  - On service restart
  - On Group Policy refresh
  - On runlevel change
  - On reboot
  - Others?

Aspects of Effect continued

- Permanence of Effect? Examples:
  - Until reboot
  - Until Group Policy refresh
  - Others?

- Scope of Effect?
  - Can it be applied to one machine, or many?
  - E.g., local GPO vs domain GPO

Method & Effect: Min Password Length Revisited

- Identified possible options:
  - Use local API (NetUserModalsSet)
  - Use a local GPO
  - Use a domain GPO
- Observation: These are different Methods with differences in their Effects
- Therefore, they would be assigned separate CREs

Other Comments on Method & Effect

- Should Method and Effect be expressed as separate fields in CRE?
  - Should aspects such as immediacy, permanence?
- Primary or secondary Effects? Examples:
  - “Disable the telnet service by setting permissions on the telnet binary to 0.”
  - “Set the permissions on the telnet binary to 0.”
- It may not be possible for a follow-up assessment to identify which CRE was enacted

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”

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\”

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

For More Information

- Watch the SCAP Emerging Specifications Page at http://scap.nist.gov/emerging-specs/listing.html
  - Overview whitepaper, 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>
  - Chris Johnson <christopher.johnson@nist.gov> (Project Lead)