Proposed Remediation Specifications

Matthew N. Wojcik

MITRE

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: Eight related proposed remediation specifications**
  - **The names, data exchange formats, and languages we need to share for remediation interoperability**

Definitions

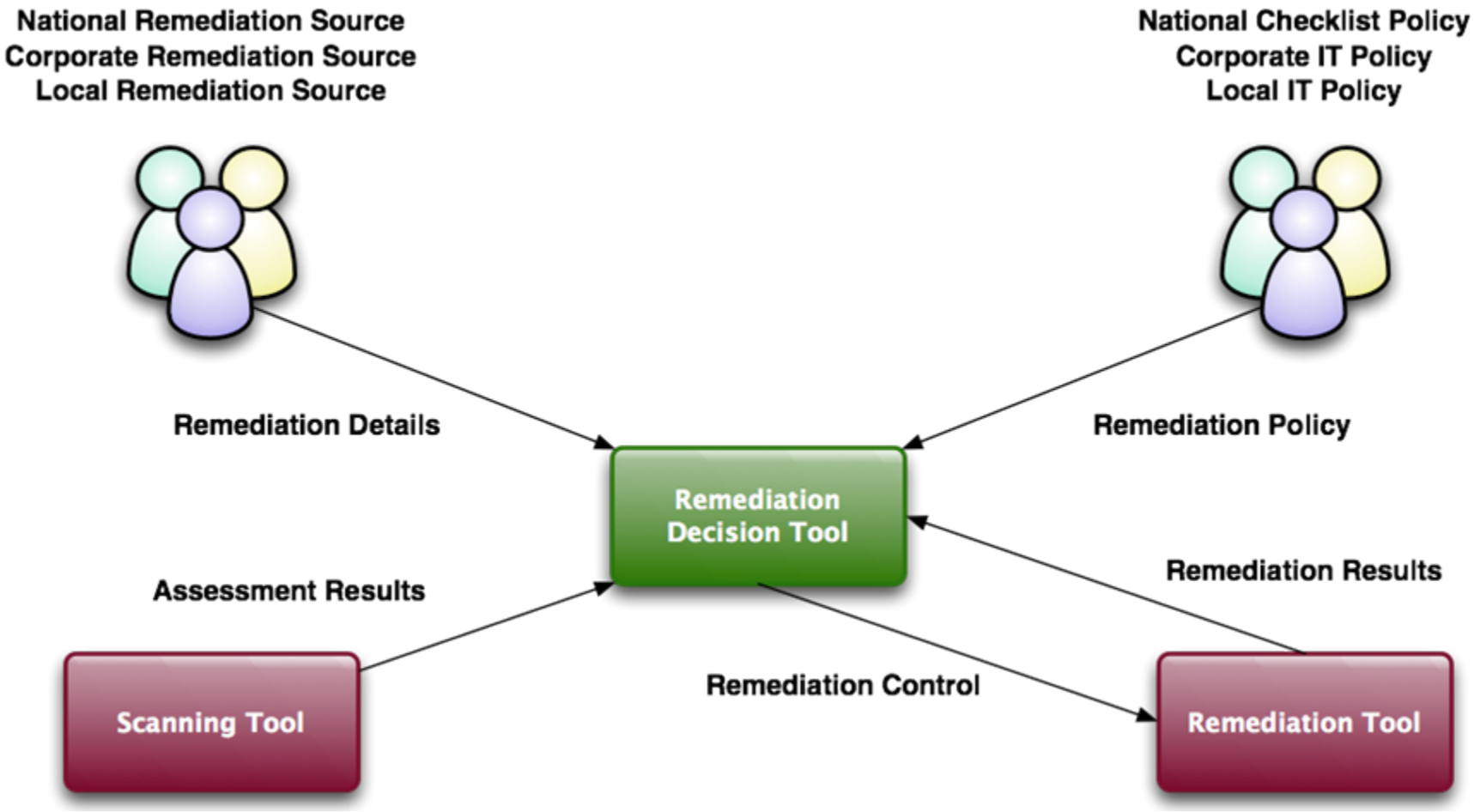
- **Remediation: A security-related set of actions that result in a change to a computer's configuration. May be motivated by discovered vulnerabilities or mis-configurations.**
- **Vulnerability: Something that lets an attacker:**
  - **Execute unauthorized commands**
  - **Bypass restrictions on data 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**

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**

Generic Remediation Workflows



Proposed Specifications

- Common names and basic remediation information
  - Common Remediation Enumeration (CRE)
- Exchange format for these basic details
  - CRE Markup Language (CRE-ML)
- Mappings and other extended remediation information
  - Extended Remediation Data (ERD)
- Exchange format for this additional information
  - ERD Markup Language (ERD-ML)

Proposed Specifications continued

- Method to specify allowed remediations by type of host
  - Remediation Policy Specification
- Specification for directing tools to implement specific remediations on particular hosts
  - Remediation Control Language
- Format for the outcome of remediation attempts
  - Remediation Results
- Language for precise, machine-readable definitions of what steps make up a remediation
  - Open Vulnerability Remediation Language (OVRL)

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

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:4"**
- **Remediation Policy Documents**
  - **"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"**

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.

Further CRE Examples

CRE will encompass statements such as:

- **“Set minimum password length to 12 characters”**
- **“Uninstall cpe:/a:example:web-browser:3.5”**
- **“Disable FTP 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”**

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

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**

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

ERD Example

ID	erd:/com.example.erd: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

Additional Specifications

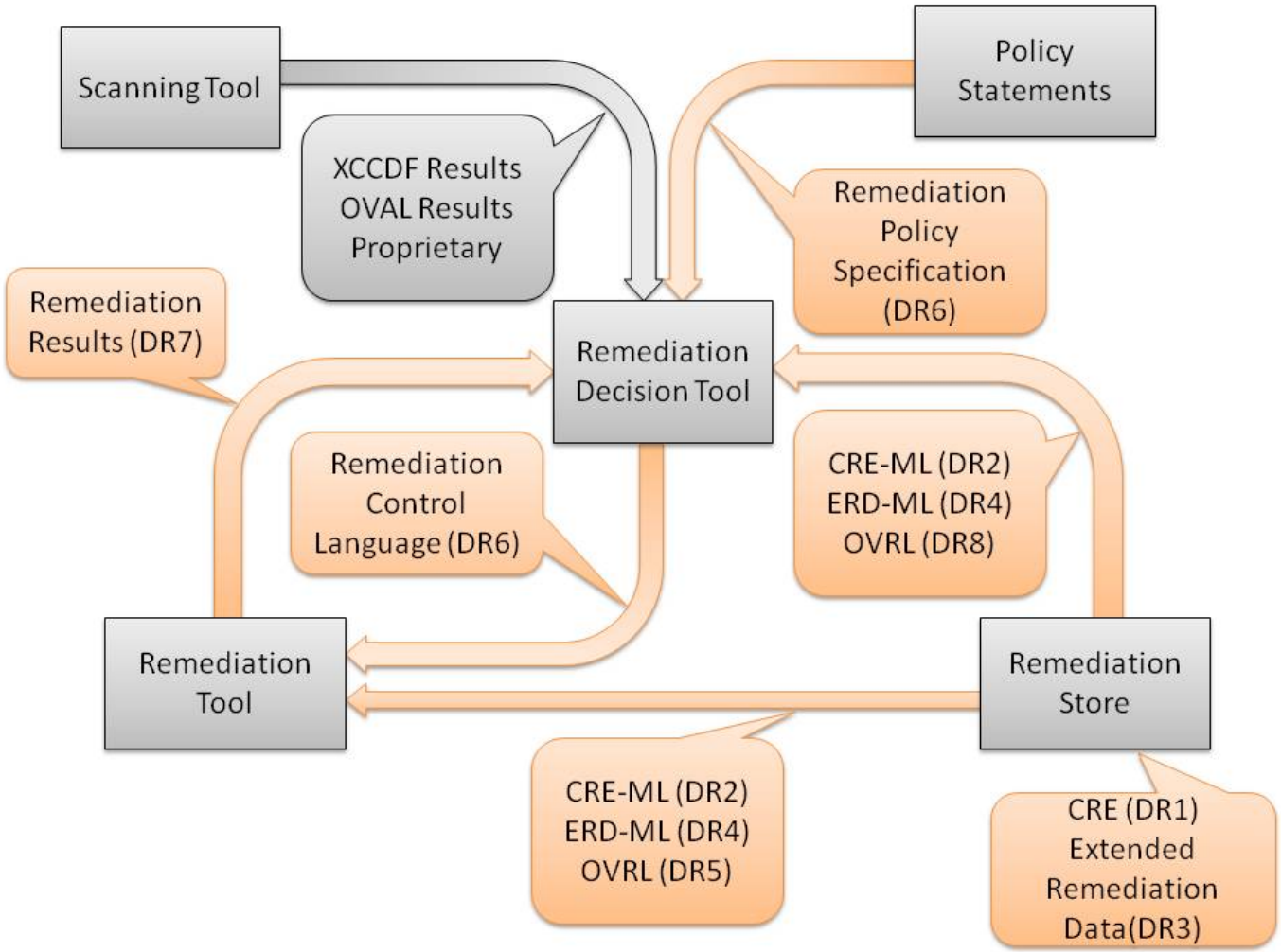
- **CRE-ML and ERD-ML**
  - Simple XML formats to facilitate data exchange
  - CRE samples available for Windows XP SP3 FDCC and patches
  - Initial ERD samples in development

- **Remediation Policy Specification**
  - Format for organizations to document allowed or required remediations by host type
  - Any combination of platform type, vulnerabilities found, configuration status, functional or organizational profile, etc.
  - Analogous to XCCDF assessment documents

Additional Specifications continued

- **Remediation Control Language**
  - Machine-readable input to remediation tool
  - “Perform <CRE list>, with <options>, on <IP list>”
  - No current standardized analog for assessment, but may have similarities to emerging specifications in development
- **Remediation Results**
  - Machine-readable output from remediation tool
  - Success, failure, deferral of remediation attempt
  - Prevent useless continued attempts to perform the same CRE
- **OVRL**
  - Precise machine-readable definition of how to perform a CRE
  - Similar to OVAL

Proposed Remediation Specifications in Context



For More Information

- Come to the "Where We Stand With Remediation" workshop, 3:30 – 4:30 October 29
- 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>