Remediation Policy
Workshop Session

Matthew N. Wojcik

September 30, 2010

MITRE

Motivating Scenarios (1 of 3)

A software vendor issues a bulletin:

> “Due to CVE-123 in version 7.1 of our application, we recommend our customers immediately take one of the following actions:
>
> – Upgrade to version 8.0
> – Install patch ABC
> – Disable a component network service
> – Configure the application to use protocol version 3 only.”

Motivating Scenarios (2 of 3)

An enterprise directs all business units:

"By November 1, any computer running application version 7.1 must choose between:

- Uninstalling the application
- Installing patch ABC
- Disabling the component service
- Enabling protocol version 3 only.

Additionally, any internet-facing systems continuing to use the application must enable logging of all remote access.

Upgrading to version 8.0 is not possible due to an ongoing procurement process."

Different instructions are provided for standalone systems and domain members.

Motivating Scenarios (3 of 3)

A group uses the application to provide internal users with network file sharing services. It has multiple data centers across the globe. Its server administrators are notified:

- "Do not uninstall the application or disable the service.
- Do not install patch ABC on servers that also provide database services, as there is a conflict.
- On servers which do not support legacy clients, enable protocol version 3 only.
- On servers which do support legacy clients, enable protocol versions 2 and 3, and file form 1479-22 with John Smith by October 15."

The Way Ahead

- End goal: Create a standard means of expressing such *remediation policy*, to ensure clear communication and enable automation & interoperability.

- Today’s goal: Discuss possible requirements for a Remediation Policy specification
  - Gathering input, not making final decisions
  - Trying to avoid presuming too much about the solution at this point
  - Participation very much needed

Whose Input Are We Getting?

- A quick poll: Who’s in the room?
  - OS and application vendors?
  - Remediation policy makers?
    - At the enterprise level? At a more local level?
  - Network admins or end users that have to respond to policy?
  - Security tool vendors?
  - Familiar with the proposed remediation specifications?
  - Staying with this workshop track?
- Opinions and experience are sought, not official positions!
  - Don’t hold anyone’s organization to a position expressed here today

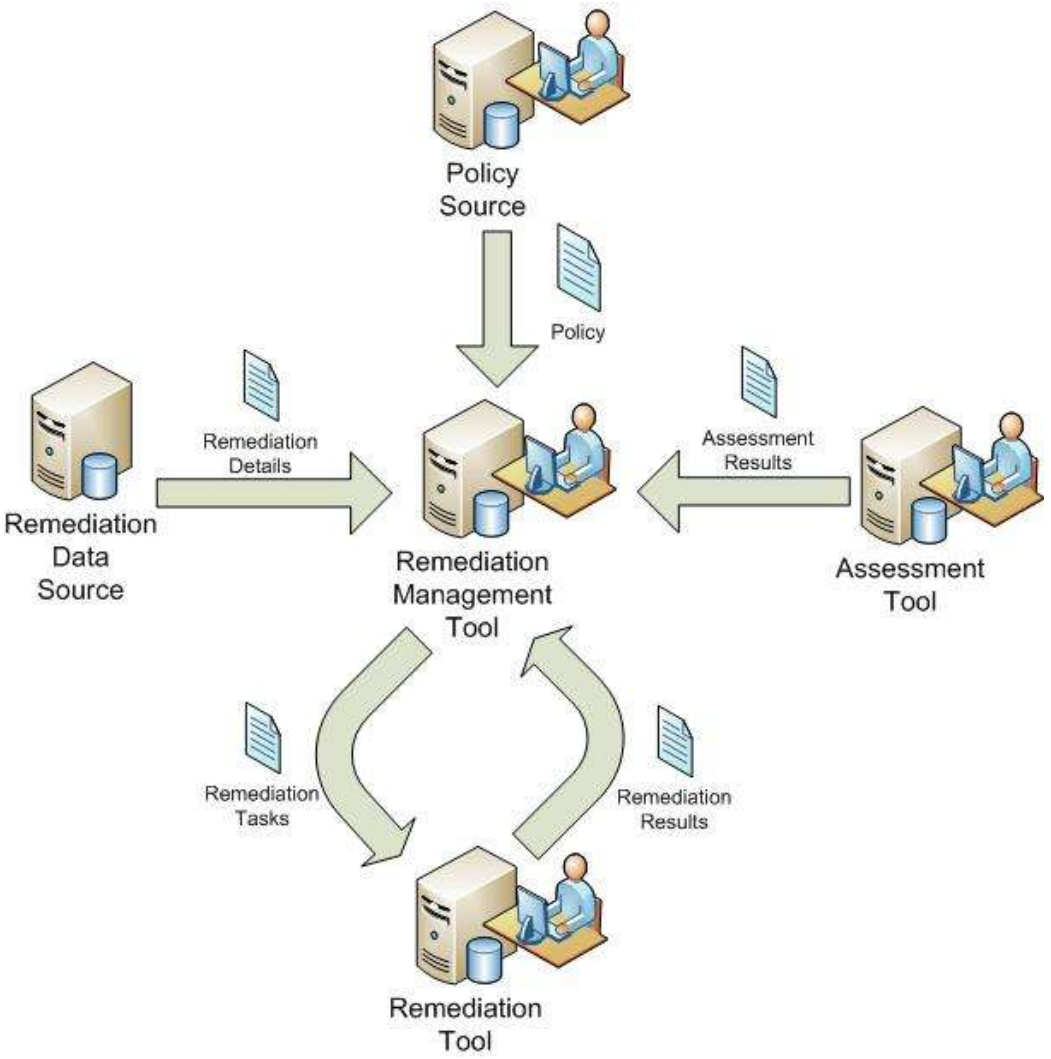
Basic Premise

The Remediation Policy Specification should allow:

- Associating particular remediations with various types of IT assets (not instances)
- Defining asset types by software inventory, vulnerabilities or mis-configurations, organizational unit, etc.
- Stating which remediations are required, allowed, prohibited

Remediation Policy has a rough analog for assessment in XCCDF.

Remediation Policy in the Logical Workflow



Core Assumptions

- Workflow centers on remediation options which are:
  - Identified in advance
  - Well-known
  - Reusable
  - Specific
  - In other words, CREs

- Other use cases may exist
  - Need to be identified and considered
  - For example, “emergent” remediations, crafted based on observed undesired behavior

Discussion: Human Readability

- Generate human-readable policy, or just machine-readable?

- Having one source document avoids maintenance problems

- Certain level of readability required for selecting between remediations allowed by policy, and potentially adjusting values

- Readability will be required if any manual tasks should be supported (e.g., help desk tickets)

- How much is this aspect of XCCDF used today?

Discussion: Remediation Preference

- Should policy support saying that remediations are:
  - Required?
  - Preferred?
  - Allowed?
  - Disallowed?

- Express preference order?

Discussion: Asset Types

- What categories of asset types should be supported?
  - Installed operating system or applications
  - Discovered vulnerabilities
  - Current configuration of software or hardware
  - Organizational unit
  - Network location
  - Geographical location

- How should these be expressible?
  - By SCAP “fact” IDs, such as CPE, CVE, CCE
  - By OVAL definition or ID, for arbitrary machine-measurable statements of applicability
  - By OCIL questionnaire or ID
  - By other conventions for system metadata (IF-MAP or similar?)
  - Free text, for human use?

Discussion: CRE Parameters in Policy

- CREs are parameterized
  - E.g., one CRE for setting the file permissions on a particular file
  - Policy will have to specify parameter values
- Remediation Tasks will have to include parameter values in a predictable, parsable format
- Humans tailoring policy or selecting between CREs during task selection will need “friendly” values
- Implies policy should map between human- and machine-readable parameters

Discussion: Dates, Deadlines, Deferment

- What dates are needed for the policy itself?
  - Creation, modification, effective on, expires on

- Are deadlines needed in remediation policy, or are compliance deadlines sufficient?
  - Possible deadlines:
    - Issue tasks by date
    - Receive task result
    - Receive “success” result

- Remediation tasks are often deferrable by end-users
  - Opportunity to save work
  - Don’t interrupt a presentation or deadline crunch
  - How should policy specify what deferral is allowed?

Discussion: Authority, Scope, Exceptions

- Who issued the policy?
- Who does it apply to?
- Is it mandatory or optional?
  - In whole or in part?
- What is their authority?
- Should the policy indicate when and how an exception must be reported?
  - Or are exceptions handled as part of compliance checking?
  - Decision not to comply may be because the remediation options allowed/required by policy are unworkable in the local environment

Stay Involved!

- 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>
  - Matt Kerr <Matt.Kerr@g2-inc.com>
  - Chris Johnson <christopher.johnson@nist.gov> (Project Lead)