Remediation Tasking
Workshop Session

Matthew N. Wojcik

September 30, 2010

MITRE

Basic Premise

- Remediation Policy specifies what remediations should be applied to what *types* of IT assets
  - Describes potential actions

- When Remediation Policy is applied to a specific network, *remediation tasks* need to be generated and assigned
  - Actual instances of actions to take
  - Outcome of Remediation Manager decision process, expressed to tools or humans that will enact remediations

- The Remediation Tasking Language should allow:
  - Associating particular remediations with specific IT assets
  - “Perform <remediation list>, with <values>, on <asset list>

- No assessment tasking analog really exists in SCAP today

The Way Ahead

- End goal: Create a standard means of expressing such *remediation tasking*, to enable automation & interoperability.

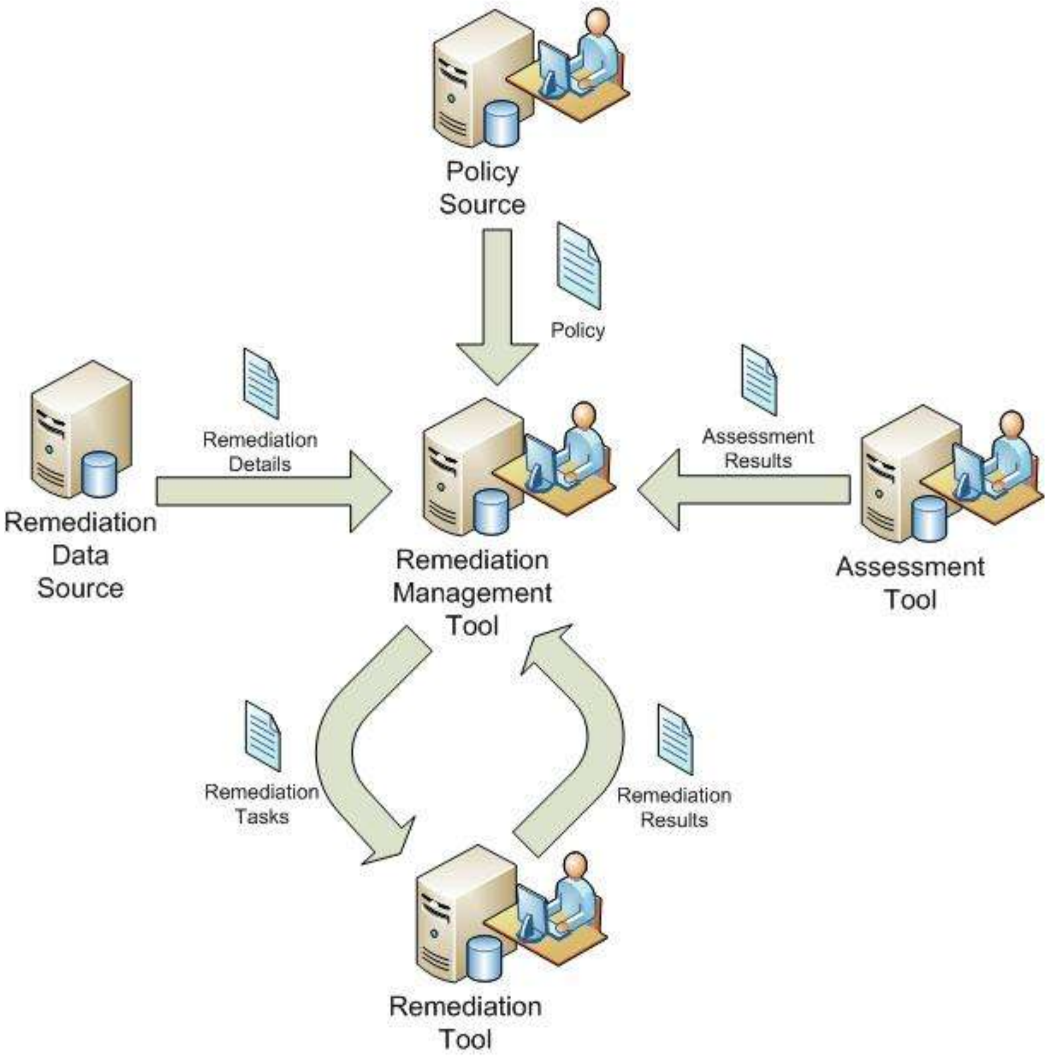
- Today's goal: Discuss possible requirements for a Remediation Tasking specification
  - Gathering input, not making final decisions
  - Trying to avoid presuming too much about the solution at this point
  - Participation very much needed

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

Remediation Tasking 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: Tasking Recipients

- Remediation Tasks are sent to some agency (“Remediation Tool”) that can make changes to the IT infrastructure
  - Software that can directly change effective settings on some set of endpoints
  - Software that can open help desk tickets
  - Software that can send email to end users

- The Remediation Manager must know:
  - Which tasking recipients it is allowed to task
  - What types of tasks they support
  - What endpoints they can affect (directly or indirectly)

- The Manager may have more than one choice of tasking recipient
  - E.g., direct changes vs. opening tickets

Discussion: Should Tasks be Enacted?

- Tasking recipients should not need to decide whether tasks are technically “appropriate” for indicated targets…
  - I.e., “I’m being told to apply CRE-123; do I see something on that system that CRE-123 seems to fix?”
  - That decision process is occurs at the remediation manager, combining remediation policy with the state of the network
  - Remediation tasks are the result of that process

- …but they must know what Remediation Managers are allowed to task them, and for what end systems they can accept tasks
  - Tasking assurance must be very high
  - Tasks from an inappropriate source must be rejected
  - Tasks of an unsupported type result in an error
  - Tasks for systems the remediation tool does not manage are rejected/result in an error

Discussion: Task History

- Need a record of what tasks:
  - Were issued
  - To where
  - For what endpoints
  - Because of which piece of policy
  - Because of what facts about network / endpoint state
  - On whose instigation
  - With what authority

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)