Vulnerability Assessment Scenario Follow-Up Work

SACM WG Virtual Interim Meeting

01/11/2017

Agenda

- Background
- Objectives
- Approach
- Deliverables
- Next Steps

Background

- Still encountering roadblocks with the Architecture and scope of the IM
- At IETF 97, it was proposed that we simply focus on the interfaces, operations, and data necessary for the scenario[1]
- Sent out an outline for this work on December 19, 2016[2]

1. https://www.ietf.org/proceedings/97/minutes/minutes-97-sacm-00
2. https://www.ietf.org/mail-archive/web/sacm/current/msg04558.html

Objectives

- Identify the tasks that are necessary to execute the scenario and define their inputs and outputs
- Identify the interactions between components in the scenario and define the interfaces and operations required to support them
- Identify the IEs necessary to facilitate the communication of security automation data between components in the scenario
- Validate tasks, interfaces, operations, and IEs by exercising the scenario using multiple CVEs

Approach (1)

- Phase 1
  - Assume components are configured to communicate with each other
  - Create a diagram that shows the components and their interactions with each other (distinguish between required and optional interactions)
  - Identify where different tasks occur in the diagram

- Phase 2
  - For each component, identify the IEs needed to carry out the required interactions and define the necessary interfaces and operations
  - Validate using CVEs

Approach (2)

- Phase 3
  - Identify the IEs needed to carry out the optional interactions and define the necessary interfaces for those interactions
  - Validate using CVEs
- Phase 4
  - Add support for discovery of components and capabilities by other components
  - Validate using CVEs

Deliverables

- Updated Architecture that defines the interfaces and operations required for the scenario
- Updated IM that contains the minimum set of IEs necessary for the scenario
- Multiple examples that use CVEs to validate the scenario

Next steps

- Any questions or comments?
- Is this a work item that the WG wants to pursue?
- Any volunteers to help?