SACM Vulnerability Assessment Scenario

SACM Virtual Interim Meeting

06/15/2016

Agenda

- Status
- Summary of resolved issues
- Open issues
- Next steps

Status

- Discussed various open issues[1] based on mailing list feedback[2][3]
- Continued the discussion on the mailing list
- Posted a new draft on 6/8/16[4]

1. https://www.ietf.org/proceedings/interim/slides/slides-interim-2016-sacm-3-1.pdf
2. https://github.com/sacmwg/vulnerability-scenario/pull/3
3. https://datatracker.ietf.org/doc/draft-ietf-sacm-vuln-scenario/
4. https://www.ietf.org/mail-archive/web/sacm/current/msg03958.html

Summary of resolved issues

- Issue #2 – Clarifying vulnerability detection data[1]
- Issue #3 – Defining targeted collection[2]
- Issue #4 – Processing vulnerability description information[3]
- Issue #6 – Storage of collected data[4]
- Issue #7 – Where do vulnerability assessment attributes belong[5]

1. https://github.com/sacmwg/vulnerability-scenario/issues/13
2. https://github.com/sacmwg/vulnerability-scenario/issues/14
3. https://github.com/sacmwg/vulnerability-scenario/issues/15
4. https://github.com/sacmwg/vulnerability-scenario/issues/16
5. https://github.com/sacmwg/vulnerability-scenario/issues/17

What to do with this I-D?

- What is the end goal for this I-D?
  - Do we want to park it as a WG I-D?
  - Do we want to send it through WGLC and get it published as an RFC?

- Will other WGs benefit from us publishing this I-D as its primary purpose is to focus the work in SACM?

- Are there concerns around publishing the I-D and then having the terms in the Terminology I-D[1] evolve out from under us?

1. https://datatracker.ietf.org/doc/draft-ietf-sacm-terminology/

Issue #1 – Managing terminology[1]

- Consensus at the 5/17 VIM was to leave the terms in the draft and reassess their promotion (move) to the Terminology I-D at a later date

- It was suggested that some terms may be ready for promotion
  - Targeted (now supplemental) collection, endpoint management capability, vulnerability management capability, and vulnerability assessment
  - A proposal for moving these terms was sent to the list and there is ongoing discussion[2]

1. https://github.com/sacmwg/vulnerability-scenario/issues/9
2. https://www.ietf.org/mail-archive/web/sacm/current/msg04117.html

Supplemental collection

- **Definition:** "*The task of collecting specific endpoint information from the target endpoint~~, that is not available from the endpoint management capability, in order to make a determination about that endpoint (vulnerability status, identification, etc.).~~ in response to an observed need during an assessment that cannot be met by existing information from the endpoint management capability.*"*

- **Proposal:** Revise this term and promote it to the Terminology I-D

*This is a slightly different definition than what is in the current Vulnerability Assessment Scenario I-D. Charles proposed this off list and it seems clearer and more concise.

Vulnerability assessment

- **Definition:** *"The process of determining whether a set of endpoints is vulnerable according to the information ~~contained in the vulnerability description information~~ pertaining to the existence of a flaw or flaws in software, hardware, and/or firmware on an endpoint."*

- **Proposal:** Remove reference to "vulnerability description information" and promote this term to the Terminology I-D

Endpoint and vulnerability management capabilities

- **Definition:** *"An enterprise IT capability managing endpoint identity, endpoint information, and associated metadata on an ongoing basis."*

- **Definition:** *"An enterprise IT capability managing endpoint vulnerabilities and associated metadata on an ongoing basis by ingesting ~~vulnerability description information and vulnerability detection data,~~ guidance and endpoint information and performing a vulnerability assessment."*

- **New definition:** *"An enterprise IT capability responsible for managing specific information about an endpoint in support of continuous monitoring processes which may or may not be driven by guidance."*

- **Proposal:** Introduce a definition for "management capability", remove references to "vulnerability description information" and "vulnerability detection data" in "vulnerability management capability", pick a different word other than "capability"*, and promote the terms to the Terminology I-D

*Henk reminded me that "capability" is already used describe what functionality/data a SACM Component can provide. As result, we probably shouldn't overload the term.

Issue #5 – Change detection with an endpoint management capability[1]

- There was a question as to whether supplemental collection information could be pushed by an endpoint management capability to a vulnerability management capability

- Based on discussion, there were cases where an endpoint management capability could learn over time and push additional information to a vulnerability management capability to support future assessments

- **Proposal:** Re-word to state that the endpoint management capability may be re-configured, over time, to push information (previously supplemental information) based on the evolving needs of the enterprise

1. https://github.com/sacmwg/vulnerability-scenario/issues/12

Next steps

- Close out the last two open issues and submit an updated draft

- Continue to develop solution I-Ds that satisfy the steps of the Vulnerability Assessment Scenario