SACM Vulnerability Assessment Scenario

SACM Virtual Interim Meeting

05/17/2016

Agenda

- Status
- Open issues
- Next steps

Status

- The I-D was adopted on 4/1[1] and discussed at IETF 95[2,3]

- Added to github.com/sacmwg[4]

- Additional feedback provided on the draft and there is open discussion on the list[5,6]

[1] http://www.ietf.org/mail-archive/web/sacm/current/msg03862.html

[2] https://www.ietf.org/proceedings/95/slides/slides-95-sacm-1.pdf

[3] https://www.ietf.org/proceedings/95/minutes/minutes-95-sacm

[4] https://github.com/sacmwg/vulnerability-scenario

[5] https://github.com/sacmwg/vulnerability-scenario/pull/3

[6] https://www.ietf.org/mail-archive/web/sacm/current/msg03958.html

Managing terminology

- Need to determine which terms in Section 2 should be pulled into the Terminology I-D[1]
  - Vulnerability description information
  - Vulnerability detection data
  - Endpoint management capability
  - Vulnerability management capability
  - Vulnerability assessment
  - Targeted collection

- Which of these terms are expected to be reused in other SACM documents beyond this draft?

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

Clarifying vulnerability detection data

- Defined as "a representation of vulnerability description information describing specific mechanisms of vulnerability detection"
- Is vulnerability detection data the representation of vulnerability description information used by security tools to drive the vulnerability assessment process?
- Furthermore, is vulnerability detection data considered guidance?

Defining targeted collection

- Currently defined as "the task of collecting specific endpoint information from the target endpoint in order to make a determination about that endpoint (vulnerability status, identification, etc.)"
- Does it refer to a server explicitly requesting additional information from the endpoint to supplement automated collection?
- Is this the right term to use in Section 5? Would "supplemental collection" be a better term?

Processing vulnerability description information

- The scenario includes an assumption that an enterprise receives vulnerability description information and processes it into a format usable by security tools

- Is this the same as saying vulnerability description information can be processed into vulnerability detection data?

- Is this related to when we say the enterprise has a means of extracting endpoint information into a form compatible with the vulnerability description information?

Change detection with an endpoint management capability

- The scenario states "the information beyond that which is available in the endpoint management capability can be pushed to the vulnerability assessment capability by the endpoint whenever the information changes"

- Should this be a pull action since the endpoint would know what information is needed until the server requests it? Is there a situation where the endpoint would know this?

Storage of collected data

- The scenario states "incorporates the long-term storage of collected data, vulnerability description information, and assessment results in order to facilitate meaningful and on-going reassessment"

- At the IETF 95 SACM breakout session, the group seemed to be in agreement that SACM is concerned with data-in-motion and not data-at-rest

- Should we update the scenario to align with SACM's emphasis on data-in-motion?

Where do vulnerability assessment attributes belong

- Appendix D.2 provides a list of definitions that describe the various attributes necessary to support the scenario

- Can we move these attributes to the Information Model in the form of Information Elements?

Next steps

- Update the scenario based on feedback from the WG (June 15 VIM)

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