Vulnerability Assessment Scenario Update

SACM WG Virtual Interim Meeting

01/25/16

Agenda

- Status update

- Clarification discussion

- Next steps

Status update (1)

- Developed as the first step in breaking the SACM problem space into smaller, more manageable pieces

- Presented at IETF 94[1] and a review period was initiated[2]

- Received lots of positive and substantive feedback on the list[34567]
  - Editorial changes
  - Areas that require clarification
  - New information needs and capabilities
  - Still some open issues and questions that we need to work through

1. https://www.ietf.org/proceedings/94/slides/slides-94-sacm-4.pdf
2. http://www.ietf.org/mail-archive/web/sacm/current/msg03486.html
3. http://www.ietf.org/mail-archive/web/sacm/current/msg03511.html
4. http://www.ietf.org/mail-archive/web/sacm/current/msg03512.html
5. http://www.ietf.org/mail-archive/web/sacm/current/msg03513.html
6. http://www.ietf.org/mail-archive/web/sacm/current/msg03529.html
7. http://www.ietf.org/mail-archive/web/sacm/current/msg03530.html

Status update (2)

- A call for adoption was initiated[1]
  - Only received two responses – we need more input[2,3]
  - Confusion around the purpose of the I-D and what we planned to do with it[4]

- Changes for -01 include:[5]
  - Feedback from the WG
  - Alignment with the SACM Use Cases
  - Examples of existing protocols and data models that could be leveraged

1. http://www.ietf.org/mail-archive/web/sacm/current/msg03584.html
2. http://www.ietf.org/mail-archive/web/sacm/current/msg03618.html
3. http://www.ietf.org/mail-archive/web/sacm/current/msg03628.html
4. http://www.ietf.org/mail-archive/web/sacm/current/msg03593.html
5. https://datatracker.ietf.org/doc/draft-coffin-sacm-vuln-scenario/

Clarification discussion (1)

Does this I-D represent a new use case? If so, should the charter include additional milestones for this?[1]

- No. Intended to describe a subset of the SACM problem space to guide short-term progress on solutions

- Based on the existing use cases and building blocks defined in *RFC7632*[2]

- Relationships to the use cases in *RFC7632* have been documented in the -01 I-D to make this more clear

1. http://www.ietf.org/mail-archive/web/sacm/current/msg03628.html
2. https://datatracker.ietf.org/doc/rfc7632/

Clarification discussion (2)

Is the I-D intended to be merged into a solution I-D?[1]

- Maybe. Intended to highlight key information needs and capabilities for a specific aspect of the SACM problem space to inform the development of solution I-Ds

- Allows us to demonstrate progress and communicate the intended path for solution I-Ds development
  - Solution I-Ds take time
  - Hope to get more people interested in working on and reviewing solutions

- Some text may make sense to "cut-and-paste" into solution drafts. Solution draft editors are welcome to do this.

1. http://www.ietf.org/mail-archive/web/sacm/current/msg03593.html

Clarification discussion (3)

Do we need to adopt this I-D as a WG I-D?

- Ideally, yes. The editors would like to see this I-D adopted as a WG I-D to show consensus on the described approach

- If it is adopted, we are not asking to progress this draft beyond WG last call
  - RFC publication is optional, I-D intended only to guide an iteration of solutions work

Next steps

- Update this I-D as open issues and questions are resolved or as new feedback is received

- Develop a roles and operations I-D that describes how this scenario aligns with the SACM IM and Architecture

- Continue to develop solution I-Ds that address this scenario based on TNC[1] and OVAL[2] specifications which are being transitioned into the WG

1. https://www.ietf.org/proceedings/94/slides/slides-94-sacm-5.pdf
2. http://www.ietf.org/proceedings/94/slides/slides-94-sacm-6.pdf