Draft SACM I-D Roadmap

SACM WG Virtual Interim Meeting

10/13/2016

Agenda

- Status
- Roadmap
- Next steps

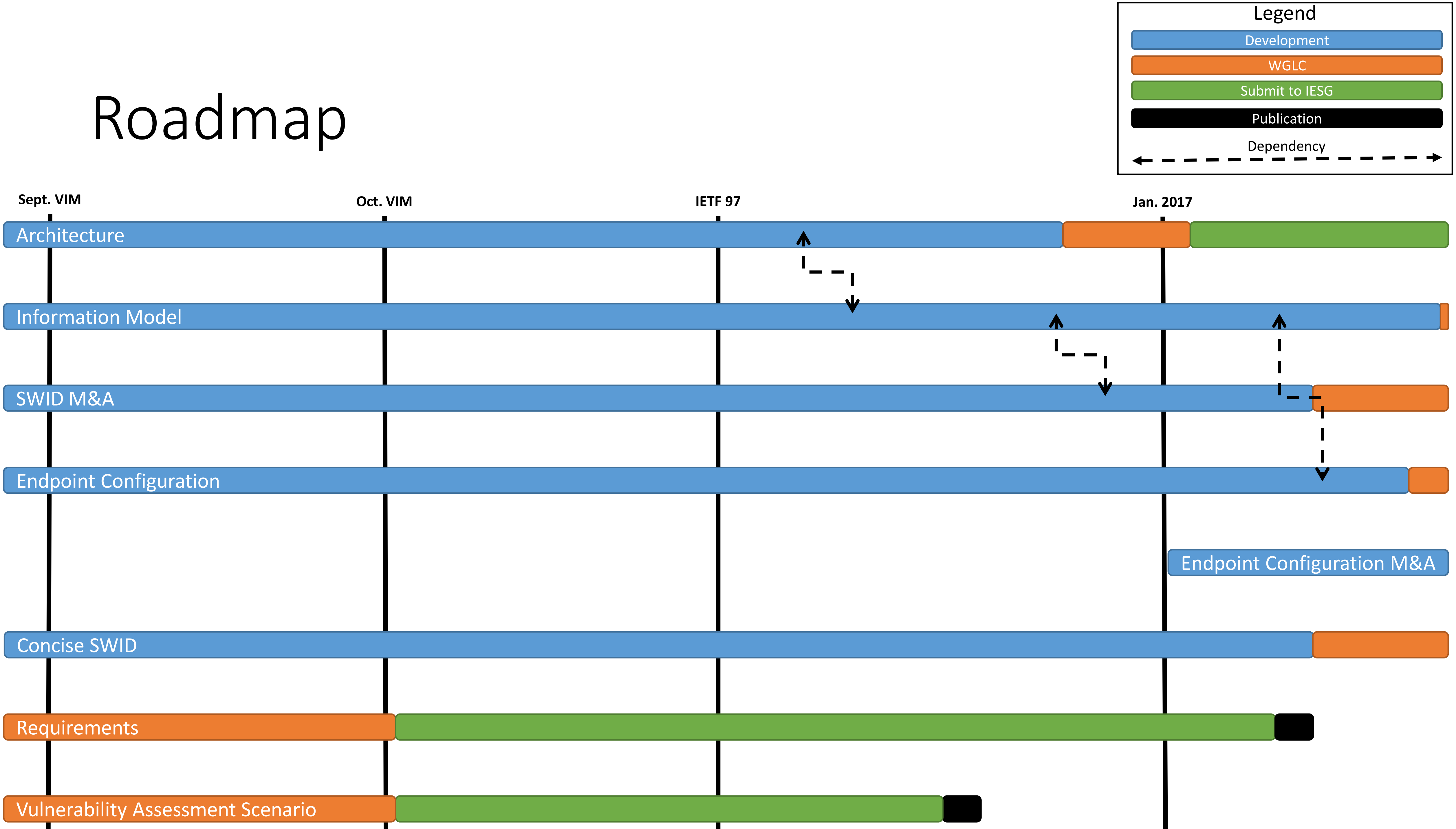
Status

- Developed to help the WG prioritize its current work
- Discussed at the September 13th SACM WG Virtual Interim Meeting[1]
- Put out a request for review and feedback on 09/13[2]

[1] https://www.ietf.org/proceedings/interim-2016-sacm-05/minutes/minutes-interim-2016-sacm-05

[2] https://www.ietf.org/mail-archive/web/sacm/current/msg04414.html

Roadmap


Legend
Development
WGLC
Submit to IESG
Publication
Dependency
Sept. VIM
Oct. VIM
IETF 97
Jan. 2017
Architecture
Information Model
SWID M&A
Endpoint Configuration
Endpoint Configuration M&A
Concise SWID
Requirements
Vulnerability Assessment Scenario

Next steps

- Adjust based on WG review and feedback

- Publish to list and possibly the wiki

Backup Slides

(Slides from 09/13/2016 SACM WG Virtual Interim Meeting)

Legend

- **Importance:** The importance of completing a particular I-D. This is based on the need for consensus around an I-D for the WG to make progress, whether or not other I-Ds are dependent on it, criticality to satisfy the SACM Vulnerability Assessment Scenario [1], etc.

- **I-D:** Name of the I-D.

- **Description:** Describes what the I-D is and how it relates back to the SACM Vulnerability Assessment Scenario I-D. It also includes bullet points for key milestones that we need to achieve with respect to the particular I-D.

- **Next Delivery:** When we anticipate the next revision (or first in the case of a new I-D) will be published.

- **Projected WGLC:** When we would like to have a WGLC issued for the I-D. This will be highly dependent on WG feedback and discussion.

Roadmap (1)

Importance	**I-D**	**Next Delivery**	**Projected WGLC**
TBD	draft-ietf-sacm-architecture [2]	*TBD*	*TBD*
Description	The current Architecture I-D has been parked in order to gain a better understanding of the solutions being developed by the WG. This revised Architecture I-D will better align the SACM architecture with these solutions. Key Milestones: • Clarify the distinction and interaction between the collection and aggregation of information from endpoints by a central server and the consumption of this endpoint information by distributed SACM consumers. • Capture architectural information needs in the Information Model I-D. • Define specific requirements for capabilities outlined in the SACM Vulnerability Assessment Scenario I-D.		

Roadmap (2)

Importance	**I-D**	**Next Delivery**	**Projected WGLC**
TBD	draft-ietf-sacm-information-model [3]	*TBD*	*TBD*
Description	This I-D will capture the specific information needs for SACM with a current focus on the SACM Vulnerability Assessment Scenario I-D. <u>Key Milestones:</u> • Distinguish between the information needs required to express endpoint information and the information needs required to exchange endpoint information and other data between SACM consumers. • Capture software inventory information, configuration information, and other information required to support the SACM Vulnerability Assessment Scenario I-D. SWID and OVAL should be used as a starting point for identifying these information needs.		

Roadmap (3)

Importance	**I-D**	**Next Delivery**	**Projected WGLC**
TBD	draft-coffin-sacm-nea-swid-patnc [4]	*TBD*	*TBD*
Description	This I-D specifies a protocol for transporting software inventory information from the endpoint to server. It currently supports SWID expressed as XML. Software inventory information is critical to determining whether or not an endpoint is in a vulnerable state. Key Milestones: • Make the I-D more data model independent. • Identify the mandatory-to-implement aspects of the selected data model (if any).		

Roadmap (4)

Importance	**I-D**	**Next Delivery**	**Projected WGLC**
TBD	Data Model for Endpoint Configuration Information*	*TBD*	*TBD*
Description	This I-D specifies a data model for representing endpoint configuration information based on the lessons learned from OVAL. This I-D will support the collection of configuration information from an endpoint which is necessary to support situations in the SACM Vulnerability Assessment Scenario I-D where software inventory information is not enough to determine whether or not an endpoint is in a vulnerable state. Key Milestones: • Experiment with various data formats and select an initial data format for the data model. • Develop a basic data model for expressing the values of configuration information from an endpoint using the selected data format. • Develop a basic data model for expressing which configuration information to collect or monitor from an endpoint. • Get WG review. • Determine if the WG wants to adopt this document.		

Roadmap (5)

Importance	I-D	Next Delivery	Projected WGLC
TBD	PA-TNC Extension for Endpoint Configuration Information*	*TBD*	*TBD*
Description	This I-D extends the PA-TNC protocol to support the collection and transport of endpoint configuration information from the endpoint to the server. <u>Key Milestones:</u> • Using SWID M&A as a template, develop an I-D that supports messages and attributes associated with endpoint configuration information as described above in "Data Model for Endpoint Configuration Information". • Get WG review. • Determine if the WG wants to adopt this document.		

Roadmap (6)

<table>
<tr><th>Importance</th><th>I-D</th><th>Next Delivery</th><th>Projected WGLC</th></tr>
<tr><td><i>TBD</i></td><td>draft-birkholz-sacm-coswid [5]</td><td><i>TBD</i></td><td><i>TBD</i></td></tr>
<tr><td><b>Description</b></td><td colspan="3">This I-D specifies a lightweight data model for representing software inventory information using the CBOR data format. This I-D will provide an additional data format in which to transport software inventory information over SWID M&A. Software inventory is a critical component of the SACM Vulnerability Assessment Scenario.

<u>Key Milestones:</u>
• Get WG review.
• Determine if the WG wants to adopt this document.</td></tr>
</table>

Discussion

- Are there any I-Ds missing from the roadmap?

- Does the following proposal for I-D importance seem reasonable?
  1. draft-ietf-sacm-architecture
  2. draft-ietf-sacm-information-model
  3. draft-coffin-sacm-nea-swid-patnc
  4. Data Model for Endpoint Configuration Information
  5. PA-TNC Extension for Endpoint Configuration Information
  6. draft-birkholz-sacm-coswid

- Are there any thoughts on next delivery and projected WGLC dates for the I-Ds?

References

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

[2] https://datatracker.ietf.org/doc/draft-ietf-sacm-architecture/

[3] https://datatracker.ietf.org/doc/draft-ietf-sacm-information-model/

[4] https://datatracker.ietf.org/doc/draft-coffin-sacm-nea-swid-patnc/

[5] https://datatracker.ietf.org/doc/draft-birkholz-sacm-coswid/

* No I-D is currently available, but, one will be developed.