IETF 95 SACM Notes

April 2016

SACM met on Wednesday to discuss it's recently adopted vulnerability assessment draft [1], a couple of individual submissions (software identification [2] and endpoint compliance profile [3]), and the SACM information model [4][5].

Our requirements draft [7] has made it through WGLC and we intend to prepare this for shepherding through the IESG.

During the Wednesday meeting there was consensus, which will be verified on the list, to adopt the software identification I-D [2] as a WG draft.

The endpoint compliance profile draft will be updated at least once more to make some clarifications before the WG is willing to consider adoption.

SACM will met again on Friday to discuss it's terminology draft [6], and the work done this week on solidifying the structure of our information model.

An updated I-D [8] has been submitted, which contains the proposed changes from the WG Information Model draft [4]. Discussions about these updates will be carried forward on the list.

Our "way forward" is relatively straightforward:

- Continue pressing on the Information Model so that it's fully merged by IETF 95
- Get Requirements to the IESG
- Complete call for adoption on SWID M&A
- Work on getting the vulnerability assessment scenario to WGLC relatively quickly
- Decide on how to organize drafts in GitHub

In support of this way forward we will hold two virtual interims, with the first being held sometime the week of May 16, and the second being held sometime the week of June 13. Doodle polls will be sent for each.

[1] https://datatracker.ietf.org/doc/draft-coffin-sacm-vuln-scenario/
[2] https://datatracker.ietf.org/doc/draft-birkholz-sacm-coswid/
[3] https://datatracker.ietf.org/doc/draft-haynes-sacm-ecp/
[4] https://datatracker.ietf.org/doc/draft-ietf-sacm-information-model/
[5] https://tools.ietf.org/html/draft-cam-winget-sacm-information-model-00
[6] https://datatracker.ietf.org/doc/draft-ietf-sacm-terminology/
[7] https://datatracker.ietf.org/doc/draft-ietf-sacm-requirements/

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

Notes As Submitted From Notetakers

SACM WG Meeting Minutes - Session 1
IETF-95

WEDNESDAY, April 6, 2016
1400-1600
Quebracho A

1. Logistics, note takers - chairs - 5 minutes
2. WG status - chairs - 10 minutes
==========
presenters: Adam Montville and Karen O'Donoghue
presentation: https://www.ietf.org/proceedings/95/slides/slides-95-sacm-2.pdf

The chairs, Adam Montville and Karen O'Donoghue, summarized the status of the WG.

The previously published agenda was not modified.

Q (Adam Montville): Any questions on the WG status?
A: none voiced

3. Vulnerability Assessment Scenario - Danny - 15 minutes
==========
presenter: Daniel Haynes
draft: draft-coffin-sacm-vuln-scenario-01
presentation: https://www.ietf.org/proceedings/95/slides/slides-95-sacm-1.pdf

Daniel Haynes presented an overview and current status on the vulnerability assessment scenario draft that was recently adopted as a WG document. Haynes noted that there are currently no solutions drafts covering this use

case. OPSEC has provided good feedback on this draft.

Q: (Nancy Cam-Winget): In considering slide 7, are the dotted data flow boxes to be SACM work in addition to the arrows?
A: (Daniel Haynes): Yes. Also, dotted boxes are optional.
Q: (Nancy Cam-Winget): I'm trying to understand the differences with NEA. Is the contribution of the work additional guidance to the end-point on what will be collected?
A: (Daniel Haynes): Yes. OVAL, et al will provide a richer data model and be extensible.
Q: (Nancy Cam-Winget): NEA already has a communication transport. Will SACM create a new channel for collection and guidance?
A: (David Waltermire): NEA is insufficient to represent all the data that SACM needs. SACM will extend PA-TNC.
A: (Nancy Cam-Winget): Is PB-TNC also being extended?
A: (David Waltermire): No, only PA-TNC.
A: (Nancy Cam-Winget): PA-TNC only provides data types, not message types.
A: (Lisa Lorenzin): PA came from TCG IFM. It is one of several extension mechanisms.
A: (Nancy Cam-Winget): Are we just extended PA or allow multiple different data models to be carried?
A: (Lisa Lorenzin): This is just one instantiation of a data model.

4. SWID Message and Attributes for PA-TNC - Dave - 30 minutes
==========
presenter: David Waltermire
draft: draft-coffin-sacm-nea-swid-patnc-00
presentation: https://www.ietf.org/proceedings/95/slides/slides-95-sacm-3.pdf

David Waltermire presented an overview of SWID, its role in the SACM use cases and the data flow of SWID M&A.

Issue #1 (slide 9)

Q: (David Waltermire): Are there any concerns with making the suggested change?
A: none voiced

Issue #2 (slide 10)

Comment: (Chris Inacio): I'd recommend: (a) dropping 2009 tag support; (b) removing the text that describes how to generate and parse the IDs; and (c) using one normative references.

Q: (Jim Schaad) Do you expect that the use 2009 tags will be the minority in the future?
A: (David Waltermire) Yes. More vendors are adopting 2015. There will be a small legacy problem.

A: (Lisa Lorenzin): Let's not penalize early adopters. Those adopters are supporting 2009. Supporting both shouldn't be too hard.
A: (Adam Montville): Legacy support is important.
A: (Lisa Lorenzin): +1

Comment: (Chris Inacio): The current text is imprecise on how epochs are generated.
A: (David Waltermire): Let's discuss to clarify appropriately.

Summary: (David Waltermire): consensus is to keep 2009 support but clarify the language.

Issue #3 (slide 11)

Q: (David Waltermire): Any thoughts on needing to track new version of a tag?
A: (Lisa Lorenzin): It seems valuable to track versioning.
A: (Henk Berkholz): Those SWIDs could be stored in a second repository.
A: (David Waltermire): There are challenges in handling SWID tags not previously seen or the provider changes the tag (and it isn't available in the repository yet)
A: (Henk Berkholz): Keeping version numbers seems like another end-point attribute even if not previously seen.
A: (Lisa Lorenzin): One possible approach would be for SWID to standardize adding a timestamp to an identifier; and these timestamps could be compared when encountered.
A: (David Waltermire): There is some complexity with this given the 2015 specification where the tag ID can't change per install
A: (Lisa Lorenzin): Right, I'm proposing adding new meta-data to indicate freshness.

A: (Jim Schaad): I'm troubled that we wouldn't track the version. Otherwise, how would we know what's there?
A: (David Waltermire): I share this concern.

Summary (David Waltermire): consensus appears to be that we want to track versions but aren't sure how yet.

Issue #4 (slide 12)

Q: (Jim Schaad) Are you expecting installers to support multiple bindings?

Q:(Chris Inacio): The client wouldn't have to support multiple bindings, it would be the server? Couldn't we differentiate with a message field?

Comment: (Lisa Lorenzin): In an ideal world, we'd accommodate the most binding flavors and only restrict further if technically necessary.
Comment: (Jim Schaad): I worry that you could make 2 SWIDs with different

serializations. Then one gets update and the other does not. If we support multiple serializations, clients must support all.
Comment: (David Waltermire): More discussion on the technical details necessary

Comment: (Chris Inacio): The system seems fragile about where to put the SWID
A: (David Waltermire): The SWID spec in 2009 and 2015 is clear on how to handle this behavior.

Issue #5 (slide 13)

Q: (David Waltermire): Should there be an MTI binding for SWID tags (XML? CBOR? JSON?)
A: (Lisa Lorenzin): Is there a binding that is most commonly implemented today?
A: (David Waltermire): There is only one binding today, XML.
A: (Lisa Lorenzin): Then the MTI binding should minimally be XML. It would also seem wise to consider an MTI binding for where we'd like the spec to be.

Q: (Karen O'Donoghue): How many have read the document? 5
: How many would offer written comments? 2

Q: (Jim Schaad): I find it hard to comment on this draft without getting access to the SWID ISO document?
A: (David Waltermire): NISTIR-800-60 summarizes it
A: (Carsten Borman): I'd recommend making the normative reference to the NIST document, not the ISO document
A: (Karen O'Donoghue): When will the NIST document be published?
A: (David Waltermire): Very soon.

Consensus Call: (Karen O'Donoghue): Should we adopt this document?
Results: Yes. The results will be reconfirmed on the list.

5. ECP - Danny - 15 minutes
==========
presenter: Daniel Haynes
draft: draft-haynes-sacm-ecp-01
presentation: https://www.ietf.org/proceedings/95/slides/slides-95-sacm-0.pdf

Daniel Haynes provided an overview of the ECP draft.

Slide 5 Discussion

Q: (Lisa Lorenzin): Why remove the references to PT-EAP?
A: (Daniel Haynes): We did it to focus the work.

A: (Lisa Lorenzin): However, the WG is not so narrowly focused. I'd like to see the admission control and "already attached to the network" use cases addressed.
A: (David Waltermire): PT-EAP is less compatible for SWID communication
A: (Lisa Lorenzin): Considering bandwidth constraints environment is important.
A: (via Jabber, Jessica Fitzgerald-McKay) Agrees with David Waltermire
A: (David Waltermire): This draft is just a profile.
A: (Lisa Lorenzin): There is a tension between what's desirable and real-world needs. I worry that we are excluding an important set of use cases.
A: (Lisa Lorenzin): There may be better approaches that SWID in bandwidth constrained environments.
A: (Bob Moskowitz): If we open our use cases to cover IoT, we need to really consider the implications. There are a wide variety of options in the IoT landscape. It's too broad to bring to the WG right now.

Comment: (Henk Birkholz) I'd recommend using the term "hardware crypto module" (not "crypto hardware module").

Q: (Karen O'Donoghue): Are we causing a long-term issue for ourselves by pulling PT-EAP out now?
A: (Lisa Lorenzin): Yes, if we only consider connected devices we are handicapping ourselves.
A: (Daniel Haynes): I'd argue for an iterative approach.
A: (David Waltermire): I'm nervous if we ask too much of implementers immediately. This should be part of our consideration.
A: (via Jabber, Jessica Fitzgerald-McKay): We had previously agreed that IoT would be temporarily/deferred as out of scope.
A: (Lisa Lorenzin): I'm not arguing that it should be in scope now, rather let's not try to make a choice that would exlude it long term
A: (Nancy Cam-Winget): IoT is a broad array of technologies.

Q: (Karen O'Donoghue): Who wants to remove PT-EAP now? Think about it more?
A: more participants responded with "think more about it"

Q: (Lisa Lorenzin): How does ECP relate to the vulnerability assessment scenario?
A: (Daniel Haynes): ?
A: (David Waltermire): ECP will evolve through this consideration of this (and other) scenarios.
A: (Lisa Lorenzin): Will ECP support more scenarios beyond vulnerability assessment?
A: (Daniel Haynes): Yes.

Slide 6 Discussion

A: (Nancy Cam-Winget): Why do we need ECP?

A: (David Waltermire): Need a standards track document on how to integrate the SACM components (e.g., where do the MUST and SHOULDS go)

Slide 7 Discussion

Q: (Danny Haynes): Can we remove the references to IF-IMC/IF-IMV?
A: (Lisa Lorenzin): I work for a vendor. We implement the TCG set of protocols. We've also looked at NEA. We found that implementing all of the horizontal interfaces is just a first step. We should standardize something there.
A: (Daniel Haynes): We're just talking about deferring.
A: (Lisa Lorenzin): I like deferring. We just need to eventually have something standardized.

Slide 8 Discussion

Q: (Karen O'Donoghue): How may have read the draft? few
: Plan to read? a few more
: Want to see a revision prior to adoption? 5

Q: (Karen O'Donoghue): How long would it take to do this revision?
A: (Daniel Haynes): It is largely trivial, but the way ahead for PT-EAP needs to be decided. It will be taken to the mailing list.

Q: (Lisa Lorenzin) Are we focused more on SWID and OVAL is largely parked?
A: (Daniel Haynes) Yes.
A: (Karen O'Donoghue) Please summarize this position on the mailing list

Closing

Comment: (Kathleen Moriarty): Thanks to DHS and MITRE for getting these documents submitting to the IETF.

6. Information Model - Danny/Henk - 35 minutes
==========
presenter: Daniel Haynes and Henk Birkholz
draft 1: draft-ietf-sacm-information-model-04
draft 2: draft-cam-winget-sacm-information-model-00
presentation: https://www.ietf.org/proceedings/95/slides/slides-95-sacm-4.pdf

Daniel Haynes and Henk Birholz presented the currents status of the two information model drafts.

Slide 12 Discussion

Comment: (Lisa Lorenzin): The AIE and CIE construct makes the document difficult to read. I recommend using a single word name.
A: (Henk Birkholz): We need some distinction between the types of elements. We can discuss further on the list.

Slide 13 Discussion

Comment: (Chris Inacio): Recommend that you not reuse the IPFIX abstract data structures (e.g., the list structures)

Slide 14 Discussion

Q: (David Waltermire): Is there a way to use the vulnerability assessment scenario to help constrain the IM work in order to make progress?
A: (Nancy Cam-Winget): Don't know how to break the IM into smaller pieces.
A: (Daniel Haynes): Feedback on the IM drafts would be appreciated.
A: (Adam Montville as individual): We need to produce an iteration of the IM that covers just enough for the vulnerability assessment scenario. We don't need to have a fully-defined data model for the first iteration.
A: (Nancy Cam-Winget): We need a container by which to evaluate future info models
A: (Adam Montville as individual): We need make progress on this IM.
A: (Henk Birkholz): The IM could be considered as having more than we need. It is a skeleton that will support inter-op between info models.
A: (Nancy Cam-Winget): The IM may have extraneous things. The IM comes from the documented use cases with an emphasis on not 'hard coding'.
A: (Henk Birkholz): A given element in the IM may serve multiple use cases. We want to re-use then. The IM provides a way to add the data for future messages.

Comment: (Lisa Lorenzin): It would be helpful to see a mapping between the tables of contents of the two IM drafts.
A: (Karen O'Donoghue): Could a tentative mapping be prepped for the Friday meeting? We'll add a agenda slot for Friday's meeting too.
A: (Daniel Haynes): No problem.

Friday 12:20pm - SACM Meeting
Note Taker: David Waltermire

Terminology (https://datatracker.ietf.org/doc/draft-ietf-sacm-terminology/)

- Need feedback wrt data model vs serialization discussion; need to account for different signing requirements for each serialization (http://www.ietf.org/mail-archive/web/sacm/current/msg03859.html)
- Need comments on the definition of "management plane"

- Consider doing a WGLC to finalize this iteration of the terminology. Once consensus is reached, park the draft until new terms need to be added.

Update on Work Since Wednesday Session

- Slide IM merger update: feedback is needed on the mapping and the content to be merged in
- Team will drive discussions on the list based on identified work

Chairs: Way Forward

- Expect two virtual interims in May and June; conflicts June 20th (TCG meeting)
  - June 13th might be good
- Immediately after IETF 95
  - Complete call for adoption on SWID M&A
- By IETF 96 in Berlin
  - Merged information mode
  - Work towards WGLC on vulnerability assessment scenario
    - Need to discuss Adam's pull request on the list
    - Need much more discussion
- Decide on how to organize drafts in github; tentatively use one repo for related collections of drafts