SACM Notes from IETF 94

The SACM WG met twice in Yokohama (Tuesday and Thursday). Note takers for both sessions were Danny Haynes and David Waltermire. Jabber scribe for both sessions was Chris Inacio. Many thanks to each of them for their assistance.

The following is taken from a "Way Forward" message sent to SACM's list and combined with a list of other actions captured during the first and/or second session. Then, come complete notes from Danny.

- Progressing Architecture Draft
  - More WG review is required (i.e. object-level security)
    - Leif discussed the need to provide object-level security within SACM. The architecture and requirements might need to be updated to address this. He will post his thoughts to the list. More discussion is needed.
    - Nancy asked for volunteers to help fill in incomplete sections of the document.
    - Dave took an action to post his comments to the list to github and to additionally provide some suggested edits
    - Jess agreed to help provide examples for the architecture draft.
  - Sections need to be filled in
  - It felt like parking the draft is not ideal for the WG (need to confirm on the list)
- Progressing Requirements Draft
  - WG review the draft after next I-D is published, which we will present for WGLC
  - Further privacy comments will be treated as WGLC comments
- Progressing the Information Model
  - Chairs will conduct a poll asking what format for IM expression is acceptable, which will include the four options presented on Tuesday [4] plus "plain English". More than one option can be voted.
  - Endpoint ID Design team should wind down, and move to editorial meetings and be more active with on-list discussions
  - There was discussion for and against use of Yang as an information model. Dan agreed to send thoughts to the list on why Yang should not be used for the SACM information model.
  - Danny will follow up on the list about notion of standardizing reports being out of scope for this phase of work.
  - The information model needs to have a requirement that data models provide timestamps for information described. This is additional to requirements on operations as described in the requirements draft (OP-

001)

- Review SACM Vulnerability draft by 2015-11-20 (two weeks and a day)
  - WG should ask others to review as well
    - OpSec - done
    - SAAG - done
  - WG encouraged to share with their peers
- WG needs to review the Endpoint Compliance Standard by 2015-12-04 (about one month)
  - Jess will update the draft to avoid expiration
  - Feel free to review NEA and/or TNC specifications (if someone can provide a link to an overview of these specifications, please do so)
  - WG should be reminded of the preliminary NEA/TNC review presented at IETF 93 [1] (see also this related thread [2])
  - If a primer is needed, see RFC 5209 [5]
- Chairs to poll for data model priority
- Chairs will poll for specific times for two virtual interims between now and IETF 95
- WG needs to consider reviving expired data model drafts (see [3])
  - If you believe reviving a specific draft should be revived, say so
  - If you also willing to do the work of reviving that draft, say that too

```
================================================
================================================
IETF 94
SACM Session I (5:10 PM JST - 6:40 PM JST)
November 3, 2015
Yokohama, Japan
Minute taker #1: Dave Waltermire
Minute taker #2: Danny Haynes
Jabber scribe: Chris Inacio
================================================
Agenda Bashing (Dan Romascanu / Adam Montville)
================================================
[Nancy Cam-Winget]: I wanted to mention that I will be leading
sessions on both the Requirements and Architecture documents at the
same time.

================================================
Working Group Status (Dan Romascanu / Adam Montville)
================================================
[Dan Romascanu]: The group is still not doing good on milestones.  We
need to decide as a group whether or not we will park core WG
documents in favor of solutions documents.
```

==========
Requirements / Architecture (Nancy Cam-Winget)
==========

[Nancy Cam-Winget]: Thanks for the feedback. One remaining issue added a data model requirement regarding data models or operations. Jim Schaad clarified that maybe it is not a data model requirement rather as an operation of a data model.

[Leif Johansson]: I reviewed the Architecture document. Security requirements talk about authentication, authorization, etc. and doesn't talk about privacy and traceability and need to know when you are hacked. Then we can use *** to know we have been hacked. You might need signals in data models.

[Nancy Cam-Winget]: It might be added at the transport layer.

[Leif Johansson]: I suggest that we don't do that.

[Nancy Cam-Winget]: We talked about this a bunch of times back and forth with the group.

[Leif Johansson]: It is very difficult to determine if the Controller has been hacked.

[Nancy Cam-Winget]: Should I wait for these comments?

[Lucy Lynch]: NSRC made comments about privacy. Asked people to review the document.

[Leif Johansson]: I like revisions as often as possible.

[Nancy Cam-Winget]: I don't mind making as many revisions as possible.

[Chris Inacio]: Kathleen thinks object security is a good thing.

[Dan Romascanu]: Let's put a milestone on the Requirements document. Is there a request to wait?

[Leif Johannson]: Just giving a heads up on the coming changes.

[Chris Inacio]: Can this information be captured in future documents? Could we make it part of the data model?

[Nancy Cam-Winget]: I can make changes, but, it will take a while. I need more comments coming.

[Brian Trammell]: stand-in AD for Kathleen. We can do review and revisions in last call.

[Dan Romascanu]: Can we do it this week and then put it in last call?

[Leif Johannson]: Lots of things seem scary to me.

[Nancy Cam-Winget]: Dave posted more comments on list. Lots of comments were addressed. Jim Schaad, I don't know where we are at and need more guidance.

[Jim Schaad]: Some issues are still open.

[Dave Waltermire]: I wanted to get comments out before the meeting, put in GitHub, and provide text.

[Dan Romascanu]: Can we do this before Thursday?

[Nancy Cam-Winget]: If others have comments let me know.

[Leif Johansson]: Consumer and Producer trustworthiness is out-of-scope for SACM. This scares me. You are making a command-control network. What happens if you get hacked?

[Nancy Cam-Winget]: There are already authentication schemes.

[Leif Johansson]: That is not good enough for this.

[Nancy Cam-Winget]: Trustworthiness is not in scope for SACM.

[Leif Johansson]: This is a layering issue. ***

[Lisa Lorenzin]: Is a NEA Client a SACM Collector or is it a Provider? This issue is more easily resolved if you up-level this and bring in the Endpoint. I need an explanation of terms for this.

[Henk Birkholz]: The terminology draft now has a collection task (remote, local, etc.). Also, now, it is not a SACM Component.

[Nancy Cam-Winget]: To Lisa's point, it is implementation-specific. Especially now as we define SACM. Now depends on how you implement and you may not have the same components. Do we need to resolve this in the Architecture? I think we can do it in the Terminology document.

[Henk Birkholz]: Send it to the list, but, acknowledge the component. I will raise it for the Terminology document.

[Lisa Lorenzin / Jessica Fitzgerald-McKay]: Strongly disagree.

[Lucy Lynch]: If it can be rolled up to the box how ***.

[Jim Schaad]: The architecture allows components to have multiple roles (i.e. can have collector and not be a SACM Component.

[Lisa Lorenzin]: I want explicit text to say a NEA client could be either.

[Nancy Cam-Winget]: I am thinking about specific functions in a workflow and how we had many examples which were defining what components are and needed terminology for definitions in one place.

[Dave Waltermire]: We need to be clear.

[Nancy Cam-Winget]: It is up to the group.

[Dan Romascanu]: But interfaces operate the architecture.

[Lisa Lorenzin]: Providing an example of a NEA Server is a big one and a NEA Client is a big one.

[Nancy Cam-Winget]: We need to do that in Section 3.1.3.

[Dave Waltermire]: If example no reason to include one.

[Nancy Cam-Winget]: We added sentences for examples, but, they are still TBD. I need help because I don't understand them. I understand, but, we ask for volunteers, but, I don’t know how to make feedback.

[Lisa Lorenzin]: A formal definition needs to work in a standalone document, but, wanted for the document to stabilize.

[Jessica Fitzgerald-McKay]: I can provide examples.

==========
Information Model (Danny Haynes)
==========
I was presenting so I didn't take notes :).

==========
Terminology (Henk Birkholz)
==========
[Henk Birkholz]: We added a few new terms and now need to discuss how Collector and Internal Collector align. Introduced the concept of a SACM Domain which does not (cannot) assess itself. We found IP addresses are difficult to identify without a network interface. Updated the term Attributes to Endpoint Attributes. The Control Plane and Management Plane are now different. Previously they were the same thing. Reading and reviewing the Terminology document is mandatory :).

[Lucy Lynch]: Is there not an attribute exchange on both sides? Risk calculation on both sides?

==========
==========
IETF 94
SACM Session II (9:00 AM JST - 11:30 AM JST)
November 5, 2015
Yokohama, Japan
Minute taker #1: Dave Waltermire
Minute taker #2: Danny Haynes
Jabber scribe: Chris Inacio

==========
Agenda Bashing (Dan Romascanu / Adam Montville)
==========
[Nancy Cam-Winget]: Will we be able to have time on the agenda for the "A Proposed SACM Information Model with Implications to a SACM Data Model" session that we requested?

[Dan Romascanu]: Yes.

==========
ECP Recommendations (Danny Haynes)
==========
I was presenting so I didn't take notes :).

==========
Vulnerability Assessment Scenario (Danny Haynes)
==========
I was presenting so I didn't take notes :).

==========
OVAL Update (Danny Haynes)
==========
I was presenting so I didn't take notes :).

==========
A Proposed SACM Information Model with
Implications to a SACM Data Model
(Nancy Cam-Winget / Henk Birkholz)
==========
[Nancy Cam-Winget]: The Information Model is intended to define structures for data model guidance as well as interface data model guidance. We have defined a statement container structure that consists of SACM metadata information and content. Specifically, the metadata includes GUID, data origin, data source, creation timestamp, publication timestamp, type, etc. The content contains proposed data model content (e.g. OVAL, SCAP, CIM, etc.).

[Dan Romascanu]: IPFIX uses an info element.

[Nancy Cam-Winget]: Henk Birkholz used the term statement because it is not a fact. We need to determine what our SHOULDs and MUSTs are. Regarding the structure the of the data model content, we need MUSTs to define elements for implementers.

[Dan Romascanu]: There is RFC 3444 which describes what an information model is versus what a data model is.

[Adam Montville]: I am confused about this because of the representation of an information model discussion from the other day.

[Danny Haynes]: Data origin, data source, etc. from a SACM container are information needs across SACM? The structure content includes atomic elements, group elements, and categorized elements?

[Nancy Cam-Winget]: Yes. We need to decide how deep we categorize. We need to define sets of elements that must be defined for interoperability. Elements must have clear semantic understanding to allow data models to map to SACM elements.

[Dan Romascanu]: What is new here?

[Jim Schaad]: I think we need more than two verbs?

[Henk Birkholz]: These are the highest-level relationships that don't impact data models. Other relationships are allowed.

[Nancy Cam-Winget]: We don't want to prescribe data models.

[Jim Schaad]: Things to name?

[Nancy Cam-Winget]: Maybe it is more complex, but, wanted to start with a base.

[Dave Waltermire]: To Leif's point Tuesday about metadata.

[Nancy Cam-Winget]: This is not exhaustive, but, a start of what we need in SACM.

[Dave Waltermire]: What about some of the content? Some would be repo and origin would be endpoint.

[Nancy Cam-Winget]: Once we have a hardened information model, we can define MUSTs and SHOULDs.

[Dave Waltermire]: See the Vulnerability Assessment Scenario. It identifies attributes. We also need a hardened architecture.

[Dan Romascanu]: We need a representation for the information model too.

[Dave Waltermire]: We need to consider classes of things (e.g. vulnerability assessment, configuration management, etc.).

[Nancy Cam-Winget]: I kind of disagree. We need to reduce scope and I am encouraged by the vulnerability assessment scenario, but, we don't want perfection, but, rather need more guidance for the information model.

[Dave Waltermire]: I think I agree we need a special approach.

[Leif Johansson]: Agree. For Kerberos, they talked to vendors and it was heard. We need to bring vendors into get their thoughts.

[Adam Montville]: Agree.

[Dave Waltermire]: +1.

[Dan Romascanu]: Can we get draft text for the information model?

[Lucy Lynch]: I think this I a good idea about working on this, but, ***.

[Danny Haynes]: I agree.

[Dan Romascanu]: We should discuss representations.

[Leif Johansson]: I like the English version.

[Dan Romascanu]: I believe in previous discussions, can you provide a link for it.

[Leif Johansson]: Kerberos Information Model (https://tools.ietf.org/rfc/rfc6880.txt).

[Nancy Cam-Winget]: I will send information on scope creep regarding the vulnerability assessment scenario to the list or GitHub.

==========
Way Forward (Dan Romascanu / Adam Montville)
==========
[Adam Montville]: We need to reach working group consensus on various items. The first is to park the architecture document, fix issues as available, and then go to last call.

[Nancy Cam-Winget]: Lisa Lorenzin might have some thoughts on this. Specifically around showing how components interact and behave.

[Dan Romascanu]: It doesn't mean park and forget rather it is more of a feedback loop.

[Adam Montville]: We may have more changes. If we get more text, will it be difficult?

[Nancy Cam-Winget]: If I am on GitHub interacting with comments, it should be easier.

[Jim Schaad]: I have never gotten through Section 3 and if we park it in a vacant lot, it will get trashed.

[Adam Montville]: It is more a question of how much work to get it good enough.

[Kathleen Moriarty]: I am fine with both approaches.

[Dan Romascanu]: It seems like there is interest in solutions. (1) More interest in solutions versus these core documents; (2) Do we completely park or not?; Do we work in parallel?

[Nancy Cam-Winget]: I want to hear Jim's comments. With people's comments and examples, we have a bunch of TBDs which break the flow.

[Jim Schaad]: There are two types of feedback. (1) Changes I can toss on GitHub (easy). (2) Questions on how things are supposed to work. If no one replies for six months, I don't know how to get fixed.

[Dave Waltermire]: If we take that approach, we need a more active engagement approach.

[Adam Montville]: I agree.

[Jessica Fitzgerald-McKay]: We should focus on the Architecture and Vulnerability Assessment Scenario documents.

[Adam Montville]: Do we want to adopt ECP? A few hands. Do we want to give more time to review?

[Dan Romascanu]: Let's give more time to review.

[Jim Schaad]: I am confused. Are we talking about protocols?

[Adam Montville]: How much time?

[Dan Romascanu]: A month would be good. We could also have two virtual interim meetings.

[Adam Montville]: Jessica Fitzgerald-McKay needs to resubmit the Endpoint Compliance Standard document.

[Kathleen Moriarty]: Will the Requirements document go to WGLC?

[Adam Montville]: How many people read the Vulnerability Assessment Scenario? About six people.

[Dan Romascanu]: We need to give more time to read and follow up on the OPSEC list as well as mention in the SAAG report.

[Kathleen Moriarty]: Wrap up the Endpoint ID Design Team.

[Adam Montville]: Conclude the Endpoint ID Design Team.

[Dan Romascanu]: Two virtual interim meetings. The first should be the second week of January. Then we will figure out when to have the second virtual interim meeting. We made good progress this week.