SACM
IETF 97
Tuesday, November 14, 0930

SACM met today and we discussed our architectural approach, how to get software identifiers collected from endpoints, and open issues with our information model. We also started considering how we can keep our information model minimized but extendable based on some real-world state collection data.

Next steps include enumerating the functions/interfaces and data that we need flowing through the SACM environment to support our vulnerability assessment scenario. With that said, our way forward looks something like this:

- Get vulnerability scenario and requirements through IESG (it'll be interesting to see what happens given the IESG's official announcement)
- Enumerate the functions/interfaces and data required to support our vulnerability assessment scenario
    - Determine what we do with the "architecture" -- do we put the information into a draft or just a wiki?
- Figure out what we really need in our Information Model
- Consider what a recharter looks like -- get our charter "shaped" to the work (because right now it's not).

We'll plan to hold two virtual interims before IETF 98 if we can -- January + February.

Raw Notes (below) Courtesy of Roman Danyliw

1. Logistics, note takers, status
==========
Presenters: chairs
Slides: https://www.ietf.org/proceedings/97/slides/slides-97-sacm-chair-slides-01.pdf

The chairs presented the status of the working group and the associated drafts.

2. Architecture reboot
==========
Presenter: Jim Schaad
Slides: https://www.ietf.org/proceedings/97/slides/slides-97-sacm-architecture-reboot-00.pdf

Schaad presented an approach to redesign the architecture.

Q: (Dan Romanscanu): Is the scope now the Internet? I thought the charter was for more constrainted enviroments.
A: (Jim Schaad and Dave Waltermire): No, it is still a corporate network with remote locations.

2. Architecture reboot
==========
Presenter: Jim Schaad
Slides: https://www.ietf.org/proceedings/97/slides/slides-97-sacm-architecture-reboot-00.pdf

Q: (Dan Romanscanu): Is the scope now the Internet? I thought the charter was for more constrainted enviroments.
A: (Jim Schaad): No, it is still a corporate network with remote locations.

Comment (Robert Moskowitz): ASN.1 is useful. There is also a trend in IETF to use YANG. It would be valuable to make this mapping so there is consistency across the security area.
A: (Jim Schaad): We won't do it in ASN.1

Comment (Nancy Cam-Winget): In the NEA example, it was listed as a protocol examples. One of many. NEA provides both transport and data model to convey posture attributes
A: (Jim Schaad): Isn't NEA just a binary blob
A (Nancy Cam-Winget): We'd have to clarify in the draft.

Comment (Nancy Cam-Winget): There is little mapping on the slide 4 diagram (SACM cloud) to the existing architecure. The existing architecture was condified abstractly. What you're proposing could be the next iteration with additional detail.
I'd want to seperate the architecture from the data flow. There are also security considerations in this data flow.
(Jim Schaad): There might be disagreement on what is a role (as currently documented in the architecture draft).

Comment: (Kathleen Moriarty, as contributor): In the first revision, this document was parked. "Proxy" and "Cloud" are not good words to use in the architecture (per slide 4) -- be more descriptive. This diagram largely describes the roles rather than the architecture. The previous architecture document was akin to an architecture.
Comment: (Kathleen Moriarty, as AD): These documents were parked. What's the value of un-parking them? IESG will soon be recommending that these types of documents don't get published. The emerging solutions could fit under any architecture.
Comment: (Henk Birkholz): Having a combined, concise view of the architecture will enable the WG the enumerate the and prune the information model. An architecture document might also help drive which protocol is used where.
Comment: (Kathleen Moriarty, as AD): to chairs, how much will working on this architecture delay the working group? This material can be put on the wiki.

Comment: (Adam Montville): Having the reference will help guide discussion in whatever form it takes (e.g., expired draft, wiki).
Comment: (David Waltermire): On the architecture, I would also not like to revisit this document. However, there are a number of protocols under considerations (NEA, XMPP). It's difficult to define the end-state without having a reference for discussion.
Comment: (Kathleen Moriarty, as AD): This would mean there isn't consensus on the architecture. How far apart are we?
Comment: (David Waltermire): ...
Comment: (Kathleen Moriarty, as AD): it looks like what's new here is roles. Does a renamed "cloud" and "proxy" fit into the old architecture.
Comment: (Jim Schaad): The focus on the two documents is different. My proposal doesn't need to be published. I'm having a hard time making my case without producing a document for discussion (e.g., around the 'one-ring data model' or what pieces we need).
Comment: (Kathleen Moriarty, as AD): to chairs, who are we building this document for? I was surprised this topic was un-parked.`
Comment: (Henk Birkholz): There was confusion on the protocols between the left vs. right protocols (per slide 5). The confusion is architectural. That is why we need an update. There is also the work in I2NSF which is beginning to align with SACM.
Comment: (Kathleen Moriarty, as AD): These changes do fit better into a virtualized world which is good.
Comment: (Adam Montville): The solution needs to over both virtualized and not.
Comment: (Jessica Fitzgerald-KcKay): Endorse the inclusion of end-points in the diagram is helpful.

3. Software Identification Draft Open Issues
==========
Presenter: David Waltermire
Slides: https://www.ietf.org/proceedings/97/slides/slides-97-sacm-swima-00.pdf

Q: (David Waltermire): Any feedback on Issue #3? (slide 6)
A: (Henk Birkholz): The URI seems like the top choice. As to "unknown", there might be categories of unknown.
A: (Chris Inacio): Can you check if anyone cares if we use unknown as long as it is specified?
A: (Kathleen Moriarty): +1
A: (David Waltermire): It doesn't look like anyone cares, so something will be picked.

Q: (David Waltermire): Any feedback on Issue #2? (slide 7)
A: (Chris Inacio): Plan for a model where vendor defines a model and then it gets into the registry
A: (David Waltermire): Can't they just registry it?
A: (Chris Inacio): This burns the numbers the vendors have. They won't want that.
A: (David Waltermire): ...

A: (Chris Inacio) How do you know that extension-n belongs to vendor-y. It would be nice to have this
A: (Robert Moskowitz) Many places have adopted the approach to have a IANA enterprise number.
A: (David Waltermire): Is that 32-bit?
A: (Robert Moskowitz): It is less than that.
A: (David Waltermire): We're discussing using an 8-bit number. We'll have to weigh message size format against this flexibility

Q: (David Waltermire): Are there concerns with adding a data source field? (slide 8)
A: no concerns voiced

Q: (David Waltermire): Is there WG consensus to explicit state that the server should parse the message or silently ignore it (slide 9)?
A: no concerns voiced.

Q: (David Waltermire) Is there a problem adding "ISO 2015 CBOR-based SWID Tags" to IANA registry? (slide 10)
A: no concerns

Q: (David Waltermire): Which references/data models should be MTI in this draft (or seperate draft)? (slide 10) Without MTI, there is risk that certain clients wouldn't be able to send certain data models.
A: (Jim Schaad): ...
A: (Roman Danyliw): What's the pentration of 2009 vs. 2015?
A: (David Waltermire): a few vendors are doing one or the other.
A: (Roman Danyliw): With so little adoption, making 2015 MTI seems better.

4. Information Model Open Issues
==========
Presenter: Dan Haynes
Slides:
https://www.ietf.org/proceedings/97/slides/slides-97-sacm-information-model-open-issues-00.pdf

Q: (Dan Romascanu): Can you detail the comment that "one data model is not enough" or did you mean data module? (Slide 3)
A: (Dan Hayes): The SACM data model is likely going to be many data models
A: (Kathleen Moriarty): You are both right. It's an issue of terminology.
A: (David Waltermire): There has been a lot of work on management protocols in IETF and proprietary. We have a few problems with regard to implementations given this diversity.

A: (Kathleen Moriarty): Jim (Schaad) can help with additional data model issues.

Per Issue #68 (slide 4)
Comment (David Waltermire): I'd want to constraint it a bit more to "security posture information".

Per Issue #68 (slide 5)
Q: (Dan Haynes): Given the new language in the draft, have we gotten feedback?
A: (Henk Birkholz) We go private feedback on this matter. We don't a defined interaction model so the input-output are in limbo. This would help people understand and select existing models. With the functions defined, it's easier to define the input-output.

Per Issue #68 (slide 6)

Comment: (Jim Schaad): If we do the first 1, it shouldn't preclude the second approach. The latter is required for proprietary vendor models. There is a lot of benefit to the first.
Comment: (David Waltermire): This sounds good, but unclear in practice. It would be useful to think about the information interactions in a given scenario (e.g., vulnerability assessment) and use that as a back-drop for a specific data model.

Q: (Adam Montville): Does that mean we don't know enough to say?
A: (David Waltermire): Getting into the details would help resolve the way ahead.
A: (Dan Haynes) Having looked at the Vulnerability Scenario. Is there a good example of what to flesh out?
A: (Kathleen Moriarty): I'd like to see you inserting yourself into the emerging YANG modules. Some of these modules cover a lot but not all of what SACM needs.
A: (Henk Birkholz): Do you mean the established modules or something emerging.
A: (Kathleen Moriarty): Primarily those that are coming out for publication. There are 100+ modules primarily in routing.
A: (Henk Birkholz): In general this will be possible.
A: (Jim Schaad): There were two YANG projects during the IETF 97 Hackathon -- (a) a catalog of YANG modules; and (b) how the YANG modules fit together into a tree.

Per Issue #10 (slide 8)

Q: (Dan Haynes): Does the WG have feeling on whether we a specific or generic representation?
A: (Jim Schaad): "Choose go"
A: (David Waltermire): Anything that reduces the number of classes is good. +1 for a generic representation.

5. Information Model narrowing IE focus
==========

Presenter: Adam Montville
Slides:
https://www.ietf.org/proceedings/97/slides/slides-97-sacm-narrowing-information-model-01.pdf

Slide #12
Q: (Kathleen Moriarty): Do you need the 6000 recommendations to get to those 5 data types?
A: (Adam Montville): Yes, some of the 6000 recommendations could be reduced.
A: (David Waltermire): The one policy recommendation (e.g., set password length) could apply to different technologies.
A: (Kathleen Moriarty): It depends on what data you use. Consider Mandiant (OpenIOC), of their 500 IOCs only 50 were being used. It's likely different.
A: (Dan Haynes): Mandiant IOC is largely about malware.
A: (Kathleen Moriarty): ...
A: (Chris Inacio): How many man years are invested in developing defining the 5120 benchmarks?
A: (Adam Montville): We don't track that specifically, only the timeline to bring a benchmark to market.

Slide #14
Comment: (David Waltermire): It would be interesting to compare your OVAL test types with the YANG models.
Comment: (Dan Haynes): Are you trying to understand how many OVAL test types are need to confirm CVEs?
Comment: (David Waltermire): Our experience with SCAP was that we didn't need a lot of test types for vulnerability assessment
Comment: (Dan Haynes): I can ask the CVE team on how many test types they need.

Comment (Steve Banghart): We feel that 400 test types is too much.

6. Terminology update
==========
Presenter: Henk Birkholz
Slides: https://www.ietf.org/proceedings/97/slides/slides-97-sacm-terminology-00.pdf

There was no discussion.

7. ROLIE SW Descriptor Extension
==========
Presenter: Stephen Banghart
Slides:
https://www.ietf.org/proceedings/97/slides/slides-97-sacm-rolie-software-descriptor-extension-00.pdf

Banghart presented an introduction to ROILE and it's relevance to SACM.

Slide #8
Comment: (David Waltermire): In additional to request-response, it can also work with existing pub-sub
Comment: (Nancy Cam-Widget): With XMPP there is capability discovery. What you're talking about as 'meta data availible' is an XMPP topic.

Comment: (Nancy Cam-Widget): Would this be an XMPP extension for discovery?
Comment: (David Waltermire): No, ROILE is ATOM-based.
Comment: (David Waltermire): This use case is to enable clients can get notification of new records of interest.

Open Discussion

Comment (David Waltermire): There are multiple extension points -- (a) link (b) information category with IANA registry; and (c) ATOM pub lets you manage arbitrary data elements;
Comment (David Waltermire): Envision using ROILE for the assessment scenarios and vulnerability information

8. Way Forward Discussion
==========
Slides: https://www.ietf.org/proceedings/97/slides/slides-97-sacm-swima-00.pdf

On the topic of whether the WG should use instant messaging:
Q: (Adam Montville): Would there be value in a regular instant messaging capability?
A: (David Waltermire): I use it with Jim Schaad. There are few others.
A: (Kathleen Moriarty): Noticed a preference of using MeetEcho
A: (Stephen Banghart): Jabber is hard to use on Windows. It isn't streamlined.
A: (Adam Montville): We need just need to ensure that decisions are made on the mailing list.

On the topic of the WG charter:
(David Waltermire): The re-charting discussion needs to be revisited in January 2017
(Kathleen Moriarty): The charter is not defined by the work and can be revisited then.