SACM Virtual Interim Notes

2015-09-24

The following is an overview of SACM's virtual interim. Thanks to Danny Haynes, Jessica Fitzgerald-McKay and Joshua Lubell for taking notes. Be advised that no recording of this meeting is available.

Meeting Agenda:

1. Notewell/Agenda bashing - 5 min (chairs)
2. Architecture update - 20 min (Nancy/Lisa)
3. Requirements update - 10 min (Nancy/Lisa)
4. Terminology update - 15 min (Henk)
5. Information Model update - 35 min (Danny)
6. OVAL update - 10 min(Danny)
7. Endpoint Compliance - 20 min (Jess)
8. Conclusions - 5 min (chairs)

Important points from this meeting:

- We're going to have a couple of working meetings between now and the submission cutoff for IETF 94 to drive architecture forward
- We determined that another Call for Contributions should be sent out related to the Endpoint Compliance solution draft which would require some TCG-related work to be submitted.
- We should be more proactive with our use of GitHub issues (things that should have been closed, hadn't been; discussions that need to be driven, generally aren't)
- DHS is working with AD and IETF to provide IPR rights for OVAL

Meeting Notes from Jessica

- Lisa gave architecture update
  - editors only using github for open issues, you can see latest xml on SACM doc site
  - latest draft from July F2F, made changes to organization of draft
  - if you have problems with these changes (or have any other comments), post it as an issue
  - Lisa asks what process do we want to use to resolve these open issues
    - Dan says the editor can propose resolutions to these issues, if no one answers, then everyone is okay with the response; or, Lisa can assign these issues to folks, including those who raised the issues
    - Lisa recommends having a couple of calls or web-meetings prior to IETF 94 where interested folks can join and work on the open issues
    - Danny H. wants to give it a try, Adam has no objection, no one else spoke up. So, Lisa is going to pull together a doodle poll to get a good time for anyone interested.
  - Lisa asked Jim if he wants to talk through any of the issues he raised on this call, Jim declined.
  - Lisa asked Henk if he wants to talk thought any of the issues he raised (Henk's

issues were raised prior to IETF 93), Lisa wants to know if she has addressed them with the current revisions

- Henk says Lisa can close his issue (Dan and Adam said Lisa can do that)
- Lisa asked Adam about the issue he raised, Lisa thinks the edit address this. Adam had been acting as a proxy for Henk, Henk said to close the issue.
- this goes on a bit, so I am going to stop capturing the actions taken here. They are all captured in GitHub.
- Anyone who has open issues should check to see if v04 has resolved them or not, and close the resolved issues
- Anyone who makes updates should upload an xml version so that others can always find the current working document
- Deadline for updates for IETF 94 is October 19

-Lisa reviewed Requirements

- Lucy Lynch offered to work on a privacy considerations section in the requirements doc but hasn't been able to yet, Lisa asked that anyone who has thoughts on this draft something up.
- Kathleen said she would review when it comes up for AD review
- Dan reminded Lucy that we would like her thoughts on what this document needs
- Henk thinks some work from the Endpoint ID team could inform this section
- other three open issues are easy to resolve
- current draft (09) reflects changes from f2f in Prague

-Henk provided terminology update

- Henk is going to roll latest version from github on SACM document site (I think?)
- proposed new term "SACM Domain"
- Lisa asked that "Endpoint Role" be added as an open issue on the architecture doc
- Henk has problem with what a data model is. We are focused on an internal data model, rather than a payload data model
- Dan asks if we need different data models.
  - Henk says we may not need different terms, but he is not sure
  - Dan says the data model can be modular. May be a union of different sub-models.
- Henk asks if there are more data plane operations that are needed for interoperability
  - no one has a good answer for this
- Henk asked about how SACM operations will handle content, whether things like policies, guidance, etc., can all be handled the same way

- Danny provided Information Model update

- pushed changes yesterday to restructure info model (framework, assets, elements)
- using triples (subject, predicate, object), will send out proposal soon
- Danny asked if IM is standards track. If so, we need to update the milestone (currently said IM is informational). Dan says chairs can make the change
- sections were lost between v01 and v02. No one has told Danny why. On list

suggestion was to reincorporate text, we can always remove it later. No one on call voiced an opinion

- Danny asks what we call a logical grouping of information (currently called a container)
    - Danny and Ira like "construct"
    - Jim says we do have a hierarchy, Dan agrees
    - Dave says that differentiating between hierarchical or not, it adds complexity to the draft to no purpose
    - Jim says "container" is working so far, don't change it until it breaks
- Josh Lubell suggests. . something I have already forgotten. Folks don't seem to like it, though.
    - Ira suggests "set".
    - Danny will bring this to the list
    - Ira wants Danny to try out different words in different parts of the text, see what works
- Danny asks what to do about reports. Are they out of scope? Do we need standards for reports?
    - maybe we don't define it, but users of SACM can have enough info to generate report
    - Dan R. says "report results" is part of our charter
    - Lisa says that we just need to create a set of standards that enable reporting, we don't beed to specify the content or format of those reports
    - Danny says we will have assessment reports from which a report can be derived
    - Dan wants this to remain an open issue
    - Adam says reports in this context is being considered at a higher level of reporting, we need to figure out where the line is
- Sharif says IM needs to be able to key in on multiple endpoints with a particular attribute (I think?)
    - Danny thinks that should be possible with the current IM
    - Sharif asks if how we extract the information from a repository will be standardized?
        - Danny says the info will be in a known format
- Danny asked about the short-term path forward
    - are we going to focus on solutions drafts now?
    - Dan says we will address this at the end of the call. He wants requirements document to be finalized. Thinks IM can be divided into modules.
- Sharif asks that Danny include in email what sort of skill sets would be required to provide good feedback

-Danny provided update on OVAL

- got positive feedback around OVAL at IETF 93
- in process of converting OVAL into ID format
- working on figuring out how to transfer OVAL IPR to IETF
- will provide technical overview at IETF 94
- Adam asked about the IPR transfer timeline

-Juan says he is working with his lawyers, goal is to get it squared away for October 19 deadline

- in meantime, is prepping info for IETF 94

Meeting Notes from Josh

SACM 9/24/15 Virtual Interim

Lisa Lorenzin - architecture:

Latest XML in IETF repository

Includes changes resulting from IETF meeting conversations

Haven't gotten any feedback yet on these changes.

Please raise any issues with these changes. Silence will be interpreted as consent!

14 open issues. Question to SACM WG - what process should we use to resolve these issues?

Group consented to scheduling virtual meetings (1 hour each) to resolve open issues with architecture and requirements. Lisa will set up Doodle poll.

[a couple of open issues were closed during this interim]

Deadline for documents is October 19 - will schedule virtual meetings to resolve issues prior to this deadline.

Privacy considerations section needed for requirements doc. Kathleen can suggest text if none provided prior to AD review.

Henk Birkholz - terminology:

Looking for feedback on terms/definitions for SACM roles, data models, operations.

Danny Haynes - Info model update:

IM restructured - changes pushed to GitHub.

Working on proposals to use triples to define IM elements, options for representing elements.

Should IM be on standards track, or should it be informational only? Suggest that it be a standards document. If no objections over next few days, chairs will update milestones to make IM standards track item.

Discrepancies between versions 01 and 02. Any feedback from group on how to re-integrate?

What to call logical grouping of information? "Container" perhaps implies a hierarchy. Group didn't resolve.

Should reports be out of scope? Charter says reports are part of endpoint posture assessment. Is it OK to not proscribe the content of a report, as long as IM includes enough information to enable production of a report.

Strategy for moving forward: current focus is on core WG documents - progress has been slow. Should we change short-term focus from core docs to solutions drafts to attract new contributors?

Next steps: send proposed open issue resolutions to list for last call. Finish triples proposal.

Danny Haynes - OVAL update:

Converting OVAL language spec into Internet Draft format.

Transferring IPR to IETF. DHS legal reviewing.

Hope to have OVAL overview session at IETF 94.

Jessica Fitzgerald-McKay - Endpoint Compliance:

[Jessica gave overview of implementation approach making use of SWID]

Proposal: focus on endpoint self-reporting, in support of use cases including vulnerability, h/w, and s/w asset management. Suggest using NEA protocols.

[Group discussion on how this maps to SACM and how these specs could be modified to support SACM use cases]

Lisa - have started discussions in TCG re. transferring ownership of these docs to IETF. No resistance so far. Would SACM WG be willing to adopt these specs and modify as needed to make them into IETF docs? [needs further discussion]

ECP Notes (Danny Haynes)

[Dan]: How does this work fit into the Information Model work?

[Jess]: ECP provides protocols for transporting posture assessment information.

[Danny]: I would add that the Information Model doesn't define what an attribute is so at the moment there would not be any changes.

[Josh]: Are we looking to have two repositories? One for guidance and one for data?

[Jess]: Conceptually, we will have two repositories, but, it doesn't necessarily have to be implemented that way.

[Josh]: Is this to set up for data warehouses?

[Jess]: Yes, most of this would be virtualized.

[Dave]: We are defining interfaces. If they do that they should be able to communicate.

[Jess]: This is very extensible. I just used SWID as an example, but, it can transfer other types of information.

[Dave]: What protocols can we adopt?

[Jess]: We can adopt the communication protocols (PA-TNC, PB-TNC, PT-TLS/EAP) outright.

[Lisa]: How does this fit in the SACM architecture?

[Jess]: The endpoint would be the producer, the server would be the controller, and the evaluator and would be the consumer.

[Lisa]: PT-TLS would be data transfer, but, would we be missing publish/subscribe capabilities?

[Jess]: Yes, if we do agree at a high-level to use this, we would need to do some things. (1) standardize the interface between repository and evaluators; (2) separate collection and evaluation; (3) develop an applicability language for querying a data store.

[Lisa]: The last two things require new specifications correct?

[Jess]: Yes.

[Dave]: IF-IMC and IF-IMV would be good. SWID Message and Attributes for IF-M is just a detail of PA-TNC.

[Jess]: Server Discovery and Validation and IF-M Segmentation are applicable to SACM. While they are new to NEA, they are not new to TNC.

[Dan]: TCG would be familiar with the process of contributing specifications?

[Lisa]: NEA was not a direct submission of the TNC specifications, but rather, re-written as an open standard for the IETF. Jess is proposing that we take a direct IPR transfer, copy-and-paste approach.

[Dan]: This just needs to be clear.

[Lisa]: The TCG agreed the IETF would take precedence and update the TNC specification as needed or simply point to the IETF specification.

[Dan]: ???

[Lisa]: The approach this time is really just an internal TCG process requesting the TCG Board to waive the IPR rights.

[Dan]: Where are we at with this process?

[Lisa]: We have discussed it with the TCG Board, but, the next step is a formal request. However, before we do that, we need to know if SACM wants to adopt it. I propose a call for consensus so that we can discuss it at the next TCG meeting.

[Kathleen]: So, we need a call for interest and a call for those who are willing to use the specifications.

[Dan]: Are there other proposals?

[Jess]: No.

[Kathleen]: Ok, we will need to check for this. The WG chairs and myself will figure out how to go about this and send a message to the list.