NOTES for SACM Virtual Interim 2016-01-25

AGENDA - SACM WG Virtual Interim - January 25, 2015

1. WG Status – chairs – 5m
2. Open issues on requirements draft – Lisa – 20m
3. Update on information model draft – Danny – 15m
4. Discussion on draft-coffin-vuln-scenario – Danny – 20m
5. TNC specification transitioning – Jess – 20m
6. Update on OVAL – Danny – 35-40m (took far less time)

ADDITION: Terminology Update (added to fill in for OVAL)

7. Way forward – chairs – 5m

Lisa went through outstanding issues in requirements and reminded everyone who submitted issues against the requirements (and all other drafts) to close them when they've been resolved (the submitter is best suited to do so). We also agreed to add an "Addressed" label to issues to signify when an issue is believed to have been addressed by the editors/authors.

Danny presented an update on the information model draft and explained the IPFIX information element notation followed by a couple of examples. The WG should look at the full examples and discuss them on the list.

Danny presented on the vulnerability assessment scenario. It seemed that most on the call agreed that the scenario would be a useful tool to help focus the WG's efforts. Those on the call seemed to agree that we should have another call for adoption after the I-D has been updated.

Jess presented on transitioning TNC specifications into the IETF for SACM work. Taking these specifications under our wing would give us the ability to modify and improve upon them.

Status quo for the OVAL update: Waiting on a signature which would enable IETF to leverage the specification. Once that does happen, there are seven I-D-formatted drafts ready to submit.

Henk presented on the terminology draft, pointing out that we're making progress on firming up definitions applicable across our set of documents. Those on the call agreed with Lisa's suggestion that terms commonly found in the routing domain but used differently here should explicitly say so in their definitions.

Way Forward:

- Wrap up requirements by March 1
- Identify required information models
  - Gaps (potentially use vulnerability scenario)
  - Identify potential data models that may address IM needs
- Focus on vulnerability assessment scenario
- March virtual interim – propose second week in March

RAW NOTES FOLLOW

UPDATED (2016-02) Notes from Danny Haynes

==========
==========
IETF SACM WG Virtual Interim Meeting
12:00 PM EST – 2:00 PM EST
January 25, 2016
WebEx
Minute taker #1: Jessica Fitzgerald-McKay
Minute taker #2: Danny Haynes

==========
Attendees
==========
* Daniel Adinolfi
* Jerome Athias
* Jim Bieda
* Henk Birkholz
* Ron Colvin
* Jessica Fitzgerald-McKay
* Matt Hansbury
* Danny Haynes
* Lisa Lorenzin
* Jarrett Lu
* Robert Lychev
* Adam Montville
* Bill Munyan
* Karen O'Donoghue
* Dan Romascanu
* Jim Shaad
* Josh Stevens
* Dave Waltermire

==========
SACM WG Status (Adam Montville / Karen O'Donoghue)
==========
[Adam Montville]: I would like to introduce Karen O'Donoghue as the new SACM Co-chair as well as thank Dan Romascanu for his service as the SACM Co-chair up to this point.

[Adam Montville]: Reviewed the IETF Note Well (https://www.ietf.org/about/note-well.html) and mentioned that the meeting will be recorded.

[Adam Montville]: Jessica Fitzgerald-McKay and Danny Haynes will take notes.

[Adam Montville]: There has been a bashing request in that the OVAL Update will be shorter and that Henk Birkholz would like to provide a Terminology Update during this time. There was no other agenda bashing.

[Adam Montville]: The Requirements document is moving along although we are five-months late. We are continuing to make progress on the Requirements document and the Vulnerability Assessment Scenario document.

[Karen O'Donoghue]: Who are the two call-in users? Robert Lychev from MIT Lincoln Lab and Dan Adinolfi from MITRE identified themselves.

[Adam Montville]: We are also continuing to make progress on solutions drafts (i.e. TNC and OVAL).

==========
Requirements (Lisa Lorenzin)
==========
[Lisa Lorenzin]: In -001, I don't feel that it reflects WG consensus. On GitHub, I wanted to break it out into two sections. One would be based on future standardization and another would be on proprietary extensions. In the Requirements document, this requirement went from MUST to SHOULD and I would like to propose that we change it back to MUST.

[Dan Romascanu]: If we want flexibility, it is our job to make the standards interoperable and if we want to support proprietary extensions, we need to do that too.

[Lisa Lorenzin]: Agree. We want to have that SACM MUST support standardized extensions and proprietary extensions.

[Ron Colvin]: Is there any requirement on having people report proprietary extensions?

[Lisa Lorenzin]: It doesn't need to be mandated to report the use of proprietary extensions.

[Ron Colvin]: I think it would be good to know about them.

[Lisa Lorenzin]: What would reporting to the WG look like? An email?

[Ron Colvin]: That may be all that is needed.

[Dave Waltermire]: To Ron Colvin's point about extensions, there is no interoperability, but, if there is a need for interoperability then there may be pressure in the market place to support this interoperability.

[Lisa Lorenzin]: Agree, but, we don't want to make this requirement so high-level that it is not useful.

[Ron Colvin]: It would be good to encourage the WG to support this.

[Lisa Lorenzin]: Any objections?

[Jessica Fitzgerald-McKay]: Isn't this requirement implied?

[Dan Romascanu]: We are talking about the ability to create extensions. Somebody can do it. If other things like the Information Model allow people to build in extensions, etc.

[Lisa Lorenzin]: This ensures that all solutions must be extensible and that proprietary extensions are supported.

[Jessica Fitzgerald-McKay]: Yes. Although, this seems like a little overreach, but, I am comfortable with it.

[Lisa Lorenzin]: Any other comments? It seems like we have consensus on the call. Other changes in the document are fairly small. We changed "agility" to "versatility". Nancy Cam-Winget clarified the text for the Push and Pull Access requirement. Cleaned up additional language in the Information Model requirements, clarified identifying the data source, and added cross-referencing where needed. Also, clarified making confidentiality optional. I did not see any other changes that require discussion.

[Adam Montville]: How do changes relate to the 32 open issues on GitHub?

[Lisa Lorenzin]: I am requesting that the WG close out issues based on the changes made in -12.

[Dan Romascanu]: I plan to do that.

[Karen O'Donoghue]: Do people that submit issues close them?

[Lisa Lorenzin]: Yes, we wanted to take this approach in order to ensure that the issues were closed to the satisfaction of the members that opened them.

[Dave Waltermire]: Is there any way to mention that an issue has been addressed?

[Lisa Lorenzin]: We talked about adding a label, but, we haven't done that yet. Are there any volunteers to make labels for this?

[Jim Schaad]: I just added a label for this.

[Lisa Lorenzin]: There are some issues still being discussed.

[Adam Montville]: What are the other issues?

[Lisa Lorenzin]: I will try to mark the issues that have been addressed using the label by tomorrow.

==========
Information Model Update (Danny Haynes)
==========
TODO

[Henk Birkholz]: We still have a factor of influence with respect to information elements and operations that SACM Components should implement and it should impact the Information Model and solutions documents. I am not sure where operations go. I think there is discussion on the list, but, I am not sure where things go. It impacts constraints in the Information Model (i.e. mandatory and optional). If you don’t have this item, you should have this item, or you could have some artificially created label. More information about this can be found on the list and in the notes from the Endpoint ID Design Team.

==========
Vulnerability Assessment Scenario Update (Danny Haynes)
==========
TODO

[Lisa Lorenzin]: I think the Vulnerability Assessment Scenario document is a nice way to focus as a lens to move forward.

[Adam Montville]: As a contributor, I agree with Lisa Lorenzin and think this will help us focus.

[Dave Waltermire]: +1.

[Adam Montville]: It seems like if we don't adopt the Vulnerability Assessment Scenario document, it will be more difficult to keep the WG focused on it.

[Karen O'Donoghue]: If there is consensus, we can adopt and figure out the long-term position after.

[Adam Montville]: We should send out a second call for adoption.

[Jessica Fitzgerald-McKay]: I think it would be good to re-iterate this discussion on the list along with links to previous discussions when we make the second call for adoption.

==========
TNC Specifications (Jessica Fitzgerald-McKay)
==========
[Jessica Fitzgerald-McKay]: We are working on solutions documents and have some good news with respect to the TNC specifications. The Trusted Computing Group has a history with the IETF and previously transitioned TNC specifications to the IETF in the NEA WG. Steve Hanna went through each specification and rewrote them, with TCG approval, to satisfy the IPR considerations associated with the specifications. So, we went to the TCG Board and asked if we could transition the documents without having to paraphrase the specifications like what was done for NEA. The TCG Board was supportive of this so we have been working to get the specifications in the IETF Internet-Draft format.

[Jessica Fitzgerald-McKay]: NEA provides a framework the standards-based exchange of posture assessment information with a central server. NEA is primarily focused on transporting health information from endpoints for a comply-to-connect use case. That is, doing a compliance check before an endpoint is granted access to a network. There have been questions about why the specifications haven't been more widely adopted. I think with modifications, we can make these specifications more useful and applicable to SACM. PT-EAP is not that useful for SACM, but, PT-TLS is.

[Jessica Fitzgerald-McKay]: IF-IMC and IF-IMV show how collectors are added, standardized, and used. This will help ensure collectors will communicate with the Posture Broker Client. The same thing goes with IF-IMV for evaluators and the Posture Broker Server on the server side. This should help have collectors and evaluators that can communicate together.

[Jessica Fitzgerald-McKay]: SWID Message and Attributes for IF-M lets us know what software is installed on an endpoint as well as provide notifications for inventory changes that have been made on the endpoint (e.g. software installed, removed, updated, etc.).

[Jessica Fitzgerald-McKay]: Endpoint Compliance Profile talks about how NEA and TNC specifications can be used in SACM. We would also like to submit some of the content from the IF-MAP specification. We are not currently planning to submit the IF-MAP specification because it uses a SOAP binding and we would prefer to have a binding agnostic specification. We also anticipate some of the information in the IF-MAP specification being captured in the SACM Information Model.

[Jessica Fitzgerald-McKay]: Do people have questions on submitting specifications to the SACM WG?

[Henk Birkholz]: The architecture diagram highlights the question about what is a SACM Component. Every function of a collector is a SACM Component, but, it is not clear with this. We need to make it clear what a SACM Component is.

[Jessica Fitzgerald-McKay]: I would like to see this revived on the list as well as the discussion around where a NEA Client fits in.

[Jim Bieda]: Do collectors and validators use the Posture Transport Client and Posture Transport Broker?

[Jessica Fitzgerald-McKay]: It would be clear to put the PT line between the Posture Transport Client and the Posture Transport Server, but, I am struggling to decide if I should go with the TNC or NEA approach.

[Jim Bieda]: It seems to kind of be in conflict with SACM.

[Jessica Fitzgerald-McKay]: Again, we can do a lot to change these specifications.

[Jessica Fitzgerald-McKay]: Next, I wanted to discuss how these specifications apply to the Vulnerability Assessment Scenario at a high level, but, would also be glad to go over it at a lower level. Pre-collection uses PT-TLS, SWID Message and Attributes for IF-M, sends software inventory information to a Repository for assessment. It is important to note that TNC never defined how to store data in the Repository so that is something that we would need to address if we want to. Evaluators can query the data that they need from the Repository. Also, they could use an applicability language to determine if a vulnerability applies. Evaluators may need to request additional information from an endpoint. There is more we can do to improve the specifications as needed.

[Dave Waltermire]: Would OVAL fit in here?

[Jessica Fitzgerald-McKay]: Yes.

[Jessica Fitzgerald-McKay]: We are currently working to convert the specifications into the IETF Internet-Draft format.

==========
OVAL Update (Danny Haynes)
==========
TODO

[Adam Montville]: Is there any timeframe around transitioning OVAL to the IETF.

[Danny Haynes]: It is getting very close. We are waiting on a signature.

[Matt Hansbury]: The snow storm may have impacted this since the U.S. Government was closed.

==========
Terminology (Henk Birkholz)
==========
[Henk Birkholz]: Sorry for abusing my topic and the general consensus for moving forward. We still don't have a complete Information Model and would like to see a mapping to potential Information Elements for the Information Model. We need to keep in mind that we need to make sure the Information Model supports our needs.

[Danny Haynes]: Agree.

[Henk Birkholz]: Regarding Issue #25, a Data Repository now contains the ability to consume, store, and provide information. Danny, what do you think?

[Danny Haynes]: It looks good to me.

[Lisa Lorenzin]: It seems like Repository uses the operations in a slightly different way.

[Henk Birkholz]: Maybe, maybe not. It leverages operations and is more similar than different. We are aggregating how SACM Consumers and Providers work.

[Dave Waltermire]: Would focus less around the symmetry and asymmetry of Consumers and Providers. Value add is another attribute.

[Lisa Lorenzin]: Would a Repository be a Controller, Provider, and Consumer?

[Henk Birkholz]: Yes.

[Lisa Lorenzin]: A Broker would set up the negotiation. A Proxy would consume and provide information. If you make this change to Repository, we would also need to make the change to Proxy. This is based on a comment made by Jim Schaad a year ago.

[Henk Birkholz]: I added terms for software package, software component, and software instance. It might be a more general component class of software that can be running or not. Similarities may be clearer as drafts progress. Lisa, can you open a draft of the Terminology document in the README and see the editor's version?

[Lisa Lorenzin]: Yes. This is good.

[Henk Birkholz]: Homogenized the definitions of Data Plane and Control Plane. Issues can be raised on the list.

[Henk Birkholz]: We introduced the term SACM Task. Two specific tasks that are already defined are Collection and Evaluation and now we included six additional tasks that are part of the definition of SACM Task itself which originate from the Requirements document. Unfortunately, there is a discrepancy in naming between Collection Task in the Terminology draft and Information Collection in the Requirements draft and what is called Evaluation Task in the Terminology draft and Endpoint Assessment in the Requirements draft. Both definitions somehow conflicted a little bit and this is a to-do for the contributors of both drafts to make it more consistent. It would be great to have this resolved and I raised an issue on GitHub.

[Henk Birkholz]: For the Definition Task, "attribute definition" is not about the definition of an attribute rather what Guidance to use to collect data for an endpoint. Same thing for "policy" definition, it is not conducted by a SACM Component is suspicious as all tasks can be. I am not sure who added these definitions.

[Henk Birkholz]: Are configuration guidance, profiles, and policies all examples of Guidance? It also seems like Guidance is expected to be machine-processable. Is it also allowed to be human-consumable?

[Henk Birkholz]: The term Capabilities, which is defined in the Terminology draft at the moment, only applies to SACM Components and maybe can assess target endpoints. Trying to infer how to get attributes from the target endpoint. This is the information that I wanted to highlight today on GitHub. We may also want to think about how to structure the Terminology document (i.e. SACM specific definitions versus not.). If you have opinions on this, please put them on the list.

[Lisa Lorenzin]: I looked at the diff and noticed that the Control Plane and Data Plane definitions have been expanded with router terms. We are not sending packets. We need to explicitly state when we are using terms differently than industry.

[Jarrett Lu]: There are examples of existing industry definitions and in SACM we use them differently.

[Lisa Lorenzin]: We need to state when we are using them differently rather than implying that we are building on them.

[Jarrett Lu]: Maybe it would be good to reframe existing definitions and say we are doing definition XYZ.

[Lisa Lorenzin]: Maybe, we should say in contrast to definition ABC, we are doing definition XYZ. I will create an issue on GitHub.

[Jarret Lu / Lisa Lorenzin]: Agree.

==========
SACM WG Way Forward (Adam Montville / Karen O'Donoghue)
==========
[Adam Montville]: The Requirements document should be due March 1st and then we can get it to the IESG.

[Karen O'Donoghue]: That makes sense to me.

[Dave Waltermire]: It would be useful to see what work we have left after tagging the issues.

[Adam Montville]: I think most will be satisfied based on comments. We also need to identify endpoints and need the complete the Information Model. Do we need to identify and prioritize data models that we care about?

[Dave Waltermire]: Is this about identifying information needs? The Vulnerability Assessment Scenario will also help us tease out these gaps.

[Adam Montville]: Maybe we want updates to the Information Model from today and additional updates to the Information Model before the next virtual interim meeting in March right before IETF 95. If that sounds reasonable, we can plan for that and work accordingly.

[Dave Waltermire]: We could also identify additional data models that address that as well.

[Adam Montville]: Ok, that sounds reasonable to me.

[Adam Montville]: Another thing that we need to consider is what architecture embodiment that we are going to go with. XMPP-Grid expired and was submitted to MILE. We need to discuss this and choose one to go forward. We could also continue XMPP-Grid in MILE.

[Jessica Fitzgerald-McKay]: Would it be useful to discuss the roles and operations in the Vulnerability Assessment Scenario and our current architecture to show how it fits. Would that help?

[Dave Waltermire]: We have been discussing this and it would be good to define a more concrete architecture that leads towards solutions. We never got to this point although there were plans to do this.

[Lisa Lorenzin]: Agree with parking the Architecture document, but, I don’t agree with moving words around in the Architecture document. I would rather see us focus on how this fits with the Vulnerability Assessment Scenario and then update the Architecture document later.

[Adam Montville]: What do people think about having the next virtual interim meeting during the second week of March?

[Lisa Lorenzin]: I have a conflict early in that week.

[Dan Romascanu]: Just to clarify, you mean the 7th, 8th, 9th, etc.

[Karen O'Donoghue]: Later in the week means closer to the Internet-Draft submission deadline.

[Adam Montville]: Jessica and Danny can you get me the notes for the meeting as soon as possible?

[Adam Montville]: Thank you everyone for attending.

Jess's Crappy Notes

SACM Virtual Interim—January 25, 2016

WG Status (AM)

- Pause arch draft
- Requirements draft moving forward, five months late
- No solutions drafts yet
- Making good progress, turning a corner

Open issues on requirements (LL)

- Diffs between -11 and -12
    - Clarification of existing items, mostly
    - One change that does not reflect consensus is G-001: Broken into 2 sections—future standards and proprietary extensions. Lisa wants SHOULD to be changed to a MUST, for both types of extensions.
        - Ron suggested a requirement that those with proprietary extensions would have to inform SACM. Dave thinks that would be handled by the market. Jess still doesn't understand why we need the proprietary extension clause, but doesn't care enough to argue about it.
        - Consensus on the phone was to change the SHOULD to a MUST, would like group to keep eye out for folks using proprietary extensions for possibility of future standardization.
    - Lots of small changes/conversations from Github, language clean up, cross-references, etc. that did not require discussion

- Adam points out that there are 32 open tickets on Github. Lisa requests that folks with open issues that have been addressed please go close them.
    - Karen asked who closes issues, Lisa explains that the submitter closes the issue when they feel it has been addressed to their satisfaction.
    - Lisa says we had talked about having an "Addressed" label for submitters, says that anyone who knows how to do that should go ahead and get it done. Adam did it on the call.
    - Lisa will tag as "addressed" any issues she is certain are addressed. Folks will check her.

Update on info model (DH)

- -03 changes were formatting, things we had agreed to earlier, some other minor updates
- IPFIX IM syntax was selected out of six choices, lots of good discussion on list about this. Danny provided RFCs that have examples of this IM style. SACM can reuse some IPFIX elements, others we will need to change or create.
- Overview of sytax
    - All elements must have:
        - Name
        - elementId
        - Description
        - dataType
        - status
    - may have
        - dataTypeSemantics
        - units
        - range
        - reference
    - org specific elements must have enterpriseID
    - You can combine information elements using a basic list, subTemplateList, subTemplateMultiList. Lots of words I don't understand.
    - Jess realizes she doesn't need to type all this. Danny's slides exist for us to reference. I will stop now. . . .
    - Danny provided examples of how we might express network interface data
- Next steps: specify existing SACM IEs in IPFIX, think about what is mandatory to implement, look at existing data models
    - We need help on this

Discussion on draft-coffin-vuln-scenario (DH)

- Status update
    - Represents way to break large SACM problem space into more manageable pieces
    - Presented in IETF 94, got lots of feedback, integrated that into new version of document
    - Call for adoption on got two responses—folks were confused about the purpose of the I-D
    - -01 available now, add examples of existing protocols and data models, alignment with SACM use cases, feedback from WG
- Discussion
    - "Is this a new use case?"—No, describes subset of SACM problem space, based on existing use cases and building blocks

        - Lisa says this is a nice lens to focus us on a problem space
        - Adam (as contributor, not chair) says this will help us focus, make progress
        - Dave +1s these thoughts
        - Karen also agrees via chat
    - "Will this be merged into solution ID?"—Maybe! It highlights what info a capabilities SACM needs. Solution I-Ds take time, this may help get people interested in SACM work. May make sense to drop some of this text into solutions drafts, editors are welcome to do that.
    - "Do we need to adopt this I-D as a WG I-D?"—preferably, yes. Editors would like to see consensus on this approach. We don't need to progress it beyond WG last call. RFC publication is optional.
        - Adam says that, if we don't adopt it, its hard to use it as a tool to help us focus. Danny agrees.
        - Karen says it will have more standing if adopted, we can decide on its final standing later.
        - Adam says we should issue another consensus call on updated draft. Jess asked that he point to this discussion, and previous discussions, when the call goes out.
- Next steps:
    - Update as open issues and feedback are received
    - Develop roles and operations I-D that describes how this scenario aligns with SACM IM and Architecture
    - Continue to develop solution I-Ds based on TNC and OVAL
    - Henk can finally talk to us! He says that the operations draft may have a strong impact on the solutions drafts. He is not sure where operations fit in-- architecture, IM, terminology, etc. Danny says need to revive this conversation on the list.

TNC spec transitioning (JF-M)

- Hopefully Danny is taking notes. . . .

OVAL update (DH)

- Core data models are in I-D format
- Still working on IPR issues
    - Plan to submit soon
- Next steps
    - Address open issues, determine which data models SACM wants to adopt, updates OVAL Data Models based on lessons learned
    - Once submitted, we are free to make changes to the OVAL specs as we see fit

Terminology

- Henk asks that contributors to solutions/data models make sure they update the IM draft as appropriate
- Review of the purpose of the Terminology I-D
- Updates to most recent version
    - Discussion of definition of repository—Lisa thinks we are overloading terms "consume" and "provide". Henk says it is an aggregate of all three roles: consumer, provider and controller.
    - Modified definitions of software package, software component, software instance

    - Data plane and control plane—included reference in how these terms are typically used
    - New SACM tasks—collection, evaluation, asset classification, attribute definition, policy definition, information collection, endpoint assessment, result reporting
- Open Issues:
    - Attribute definition is not about attribute definition?
    - Policy definition is not conducted by a SACM component?
    - Many open issues about guidance—are configuration, profiles and policies examples of guidance? Is "how to collect" from an endpoint considered guidance?
    - Question about the SACM prefix in terminology, and alphabetical order
    - Jess loves Henk's last slide. "No more content. This is the last slide." ☺

Way forward

- Wrap up requirements by March 1
- Identify required data models??
    - Dave suggests we start with info model gaps using vulnerability assessment scenario
    - Can simultaneously identify data models that address IM needs
- Discuss architecture embodiment on the list—what do we want to do with the xmpp grid architecture v. endpoint compliance architecture
    - Jess suggests describing architecture that meets vulnerability assessment scenario
    - Dave suggests we need a more concrete scenario—there are placeholders to address this at end of architecture draft, what Jess suggests could fit there
    - Lisa thinks moving words in architecture draft is not helpful. We should focus on vulnerability scenario, it will make it more obvious what we need from an architecture
    - Adam says we will focus on vulnerability assessment scenario
- March virtual interim—second week in March
    - Adam will start Doodle poll. Karen notes we will be close to the deadline for Internet Drafts prior to IETF 95.