SACM Virtual Interim
October 13, 2016

Note takers: Jessica Fitzgerald-McKay

Summary

We had another fairly productive meeting. Requirements update to DM-001 was made, and that draft and the vulnerability scenario draft are ready to be progressed. We discussed open issues in SW M&A and our Information Model drafts, and received an update on COSWID and our I-D roadmap (informal).

Our Way Forward looks something like the following, so that we are in a good position for work during IETF 97 (the entire WG should participate in one or more of these items):

- Requirements and vulnerability drafts in progress (i.e. being shepherded through IESG) – chairs have the ball on this one.
- SW M&A
    - Consensus call on issue #7 (nature of reported software)
    - Consensus call on issue #2 (include software identifier in all records)
    - Further discussion required on issue #3 (include installation location of software)
        - General agreement that location should be included, but there are caveats to consider – such considerations should happen on the list
    - Further discussion required on issue #6 (MTI data models)
        - General agreement did not feel present
        - There was some support for relying on "what exists in IANA" as a SHOULD
- Information Model
    - A lot more discussion seems to be needed for this draft
        - On circular subjects – would it be possible to use references instead of structure so that we avoid circular situations?
        - Metadata information elements – are these necessary or are they duplicative?
        - Assorted data model questions – all of these need to be discussed on the list, though at least one person felt that it may be too soon (we haven't nailed down enough about the Information Model itself, much less the data models that may support it)
    - Ensure that MILE indicators are covered by the SACM IM
- COSWID
    - Adoption call on the list
- Roadmap
    - Ongoing discussion about what makes sense
    - Generally positive on the visualization
    - Noted that the roadmap put the Architecture as the top priority

Raw Notes

- not much feedback on just about anything on the list
- requirements draft and vulnerability assessment scenario: nothing left to do before progressing the drafts

Software Message and Attributes for PA-TNC

- no feedback on -02 on list
- off-list conversations lead to tracked issues in GitHub repository
- needs a reviewer! Particularly need comments on open issues!

- Biggest Issue is #7 (nature of reported software)
    - Current draft reports only installed software, do we need to report running software and installation packages as well?
    - Dave suggests keep scope on installed software
    - Danny says you can check for running software/installation packages with OVAL
        - reporting installed software with OVAL is a hassle, so focusing this draft on installed software with Software M&A is a benefit
    - many other expressed support for keeping a more narrow scope
    - Adam and Karen to call for consensus on list

- Issue #2 (Include software ID in all messages)
    - in -02 draft, you either report full record or software identifier
    - but, this causes problems if the recipient cannot parse the full record
    - by always reporting Software ID as a separate field, you can do a lot even if you can't parse the full record
    - Jim thinks this is a good idea, as endpoint will be more consistent about generating data than the recipient will be
    - Adam agrees
    - no dissent
    - Adam and Karen to call for consensus on list

- Issue #3 (Installation Location)
    - good idea to include, if you need to know where to patch
    - Dave says its a helpful to include to differentiate instances when trying to perform asset management
    - Henk believes location information is essential, but can be difficult. Some installation locations are in RAM, or in remote file systems, or are constantly changing
        - Charles asks if you would consider the software to be installed in those cases? Software can be run without being installed, and SW M&A was meant to cover only installed software.
        - Dave suggests using a URI to accommodate these "difficult" cases, Henk thinks this is a fine idea
        - Adam says we may have to draw a line on the scope at some point

- Dave says, if we use URI, we can make a scheme later to deal with those edge cases
  - Charles to draft our a solution for others to look at, get comments on
  - Adam would like to see this settled in a few weeks

- Issue #6 (MTI Data Models)
  - -02 draft can accomadate 256 data models
  - names SWID 2015 and 2009 data models
  - what does MTI data model mean, as, technically, the only dependency is that endpoints have to be able to derive a software id from the record?
  - Jim asks if we are talking about the SACM data model, or the data model used to communicate between endpoint and NEA server?
    - Charles says between endpoint at server
    - Jim asks if you can convert between 2015 and 2009 SWID tag? Charles says yes, but Jim doesn't like to require the endpoint to do that.
    - Charles was interpreting MTI to mean that, if an endpoint claims conformance with this standard, they have to be able to derive data in a given format. It doesn't preclude the endpoint from using other data models. (<-- I may be messing this conversation up)
    - Dave says that you can make a meaningful identifier that is not actually tied to the SWID tag, and that will conform to the standard.
    - Dave suggest recommending that the identifier be derived from the data models listed in the IANA registry when possible (i.e., making it a "should"). There may not need to be an MTI.
    - Adam is concerned about not having an MTI. Jess asks if a Posture Collector could be required to handle an MTI data model, while allowing it to send other types of data as available?
    - Charles asks if a MTI data model requirement should belong in another document
    - Dave asks if the requirement would be that the Collector must recognize an instance of an MTI data model on the endpoint and collect it if it does?
    - Adam suggests this is an architectural issue, we need to better understand our architectural requirements
    - Charles would like to see a test implementation, see what we can demand of endpoints and what we cannot
    - Dave says we can propose this as a code stand project
    - Kathleen says we need projects entered into Code Stand by October 19 (codestand.ietf.org)
      - we can make clear that this is a draft, will continue to be revised, in notes section
      - Code Stand designers would love feedback on the submission process
  - [someone] will submit the proposal to Code Stand

- out of time, for rest of Charles' slides, we will discuss on list

Information Model

- updated draft is available for comment on list

- Issue #1 (Subjects and Attributes)
  - from terminology document, attributes are atomic, Subjects are composite information element
  - Jim would like to see this represented in the document
    - Danny will add these definitions to the IM
  - Dave asks about composing subjects from other subjects
    - Danny says there are structured data types you can combine

- Issue #2 (Circular Subjects)
  - helpful for network paths and symbolic links, but problematic if the nesting goes to deep
  - what are other use cases for circular subjects, beyond these?
    - Danny will bring this up on list
  - Dave suggests a reference capability, so we don't have to treat everything like a hierarchy
    - Henk and Danny say you can use the label element for this
  - Danny thinks we need to play around with max-depth to see if it can help mitigate the issues surrounding nesting subjects
    - Jim dislikes circular nesting. Nesting itself isn't an issue.
  - Danny doesn't know if IPFIX has this problem or not
    - Jim thinks not

- Issue #3 (attribute and subject names)
  - Should names unique per attribute, or per subject?
    - Danny suggests this is up to the data model implementer, as long as names can be mapped back to the IM.
    - Jim wants this to be clearer in the IM
    - Danny will look at documentation, try to clean it up
  - Adam asks if the issue numbers correspond to GitHub issues, Danny says no. Danny will put these issues in GitHub after the call.

- Issue #4 (metadata elements)
  - some metadata elements are legacy, Danny wants to pull them out
  - some elements are always metadata
  - Jim wants to define sacm/statement and sacm/metadata
    - Danny says that was considered too complex earlier, has that changed?
    - Jim asks if sacm statement contains information that is not in an information element already. Danny says it is just an envelope for other information elements. Jim

says that, if it contains information that is not in another information element, then it is an information element. Danny agrees.

-Issue #5 (Categories)
- do we need them? are they subjects?
- Danny doesn't think there are any information elements that are categories, aside from an example. He would like to introduce a new IM structured datatype
- Danny will post this question on list
- are we expecting categories to be represented in a data model, or will the data model pick one or more choices from the IM?
- Danny and Adam think this should be left to the data model implementer
  - Jim thinks either choice is fine

- Issue #6 (random DM questions)
- do we need new DMs, or should we describe how to leverage existing ones
  - Danny thinks we should fold in existing data models
- do we need a single DM?
  - Danny proposes we provide a framework for communicating information expressed in different data models
    - ex, provide collection, evaluation guidance using various data models
    - Dave and Adam say we should reuse existing data models when possible
    - Henk points out that we should do that for collection, but we might have to do post-processing after collection has occurred, help with communication between components
      - Jim doesn't know/care, wants to focus on IM right now

- Danny will bring rest of questions (minor issues) to the list

Concise SWID

- creating code as Henk updates draft
- working on documentation of attributes (hopes to be done by Seoul)
- still need to translate free text descriptions of "any attribute" into CDDL definitions
  - Dave thinks embedding hashes into CDDL will improve interoperability
- working through the issues Jim raised on list
- Adam wants to hold a call for adoption. No objections.

Roadmap

- need architecture updates, as current solutions rely on NEA
- IM will need updating based on architecture updates
- SWID M&A and Configuration specs are dependent on IM
  - Dave doesn't think SW M&A and IM are dependent on each other. SW M&A is about endpoint data collection, IM is more about providing information to other SACM

components. Either can be done independent of the other.

- Charles agrees, since SW M&A doesn't have a data model.
- Dave points out that netconf and SNMP don't have a dependency on SACM DM either. Kathleen agrees.