SACM VIM 20160913

Attendees (throughout the 2-hour meeting):

- Adam Montville
- Karen O'Donoghue
- Kathleen Moriarty
- Charles Schmidt
- Danny Haynes
- Ira McDonald
- Jarrett Lu
- Jim Schaad
- Mike Cokus
- Matt hansbury
- Jessica Fitzgerald-McKay
- Stephen Banghart
- David Waltermire
- Dan Romascanu
- Nancy Cam-Winget
- Henk Birkholz

Note takers: Charles/Danny.

Summary

We had a fairly productive meeting and recognized that some discussions need to happen quickly (i.e. DM-001 in the requirements draft). We discussed open issues on the Software M&A and Infomration Model drafts, were introduced to a proposed I-D roadmap, and heard from Henk on COSWID.

Our Way Forward looks something like this (the entire WG should participate in one or more of these items):

- Requirements draft update and progression (by end of week)
- IM Review with issues raised between now and next interim--open issues discussed at next interim
- Begin, as IM review progresses, focusing upon data model identification/development
- Read and provide feedback on -02 SWID M&A in support of reviewing open issues at next interim
- Review and discuss proposed I-D roadmap on the list, let's settle on something by the next interim
- Hash out the meaning of a data model on the list
- If possible, COSWID review

At the next virtual interim, we'll be discussing open issues on the Software M&A, Information Model, and COSWID drafts. We'll also revisit the I-D roadmap that has been proposed. All of these things require on-list discussion for the next interim to be effective.

Raw Notes

Agenda Bashing

[Danny Haynes] – Suggest putting Roadmap after the IM.

[Jim Schaad] – Would like the IM first.

Status

[Adam Montville] – SWID M&A done. Requirements Draft – hasn't happened.

[Danny Haynes] – I added as part of the IM slides. Can talk about then – hopefully wrap up although Nancy isn't here.

[Adam Montville] – Vuln Scenario – WGLC done. Minor updates. Karen and I should work on shepherding that through.

[Adam Montville] – Charter – added 6 months. Real rewrite probably necessary. Rough roadmap will be discussed. No COSWID discussion on the list (we were going to do that.

Information Model

[Danny Haynes] – The primary open issue is dealing with the first requirement. Some non-critical issues. This won't be long.

[Danny Haynes] – DM-001. This said the DM should have a DM element for each IM element. The way it was interpreted sounded like a 1-1 mapping requirement. That would prevent you from having a specialized DM (just for software). Wanted to revise to say every DM doesn't need to contain the whole IM. Also found some IM/DM requirements issues, but at last meeting the group decided not to go into, but we could revise this requirement based on list discussion. We proposed text; some back and forth. Biggest concern was "artifact" vs. "element". Sounds like preference for "element.

[Danny Haynes] – I took the original text and revised based on feedback. I broke into 2 parts to make easier read. Made two other minor changes. Key thing from the rewrite – we want to include DM elements not mapped to IM. Want to ensure DM developers can create their DM as they wish. Having DM element that may map to more than one IM element. To recap today's discussion – Nancy proposed different text. One was artifacts -> elements. Other minor tweaks. I wasn't sure about the first sentence: each DM element must map to IM element. Seems like this recreates our initial issue. Like to get thoughts of others.

[Ira McDonald] – I like what you have on the screen here rather than Nancy's. Two separate bullets is better. In order to make it clearer, I would say... need to think about. The first sentence needs to be reordered. In the second bullet I would really like to add "or vice versa" to the end of the sentence. Allow one IM to decompose into fragments of meaning – become multiple data elements. Not to 1-1, 1-N, or N-1. It is either. On the first bullet, could we say "If a DM element is derived from the SACM IM, it MUST be associated with at least one SACM IM element (maybe more)." Put the IF at beginning. There is an implicit IF now, but not there.

[Jim Schaad] – I have a problem with the definitive article at the beginning of the sentence. "A" SACM DM or "The" SACM DM.

[Ira McDonald] – I thought we weren't precluding more than one DM.

[Jim Schaad] – But not THE

[Dave Waltermire] – We won't have one SACM DM.

[Adam Montville] – We won't.

[Jim Schaad] – I hope we do.

[Dave Waltermire] – Better to compose.

[Jim Schaad] – That is fine, but there needs to be one official SACM group DM.

[Ira McDonald] – We don't need to answer here. A DM received from a SACM IM MUST...

[Dave Waltermire] – We are not going to get away with a single DM. There are multiple interfaces with different protocols. A DM per interface is needed.
[Jim Schaad] – In that case, I'm in favor of reopening the requirements draft.
<stunned silence>
[Dave Waltermire] – What else would need to get change.
[Jim Schaad] -Not sure. Will reread.
[Danny Haynes] – If we do that, I have a few other issues with 001, 002, 014. Not sure what the process.
[Adam Montville] – All we wanted to do was edit draft 001. There has been no new information.
[Jim Schaad] – I want to rewrite first sentence in 2.4. Multiple models for different things is a new requirement.
[Ira McDonald] – Agree.
[Adam Montville] – To me we have covered this. If it says THE SACM DM, it depends of your perspective. Could be a decomposed piece.
[Ira McDonald] – I'm not with you. I dislike the definite article unless there will be one normative DM. I don't want that. I want a normative IM.
[Jim Schaad] – I want a normative DM.
[Karen O'Donoghue] – We went down this path already. If we open this up, is it going to be another 6-12 months. Will that help? Better to put out a 90% good version now.
[Dave Waltermire] – Depends on how binding the requirements are going to be.
[Karen O'Donoghue] - <sarcasm>And there is always an in-depth analysis</sarcasm> I see these as guiding development, but if something changes we can change the requirements. But you need to move beyond requirements. Is this good enough?
[Dave Waltermire] – If we had a way to track agreed-upon deltas informally between revisions, we could move forward with this. Would it be possible to establish a wiki?
[Karen O'Donoghue] – We can do that.
[Dave Waltermire] – If we don't do that, we will never be done.
[Karen O'Donoghue] – I can envision Kathleen's face if we ask for 6 more months on requirement. It would be better to move forward now. We agreed at last meeting to make a minor fix to one requirement. It doesn't hurt to revisit.
[Matt Hansbury] – I agree with Karen and Dave – leave well enough alone.
[Ira McDonald] – Jim, relative to that sentence (which bothers me too and there are others and Danny thinks too) WGLC allows us to change bits of sentences. What we send can be changed.
[Jim Schaad] – Usually just small things unless doc goes back to WG.
[Karen O'Donoghue] – The bottom line is, do you want to spend more time talking about requirements, or spend more time maturing the IM and DM?
[Danny Haynes] – If we document everything, I can live with it and we can change it at a later point of time.
[Dave Waltermire] – Agree. This is just a tool to help us develop solutions, which are our real goal.
[Jim Schaad] – I've always been in favor of just publishing the document.
[Karen O'Donoghue] – I think we have rough consensus to publish the document.
[Danny Haynes] – With this one change?
[Karen O'Donoghue] – Can you summarize the difference between your and Nancy's text.
[Danny Haynes] – She doesn't say "derived from the IM". She says each DM element must map to an IM element.
[Ira McDonald] – Which is the main ambiguity with Nancy's text. It conflicts with allowance to have extensions to IM.
[Danny Haynes] – That was the biggest difference. She says each DM element must be associated with an IM element. That was my biggest concern.

[Karen O'Donoghue] – Let's move on and if you and Nancy can agree on a minimum set of changes.
[Danny Haynes] – John Strassner also commented, but is long.
[Ira McDonald] – I agree with Dave's chat note
<Dave Waltermire on chat> One nit... the first example in the second bullet belongs with the first bullet.

[Danny Haynes] <slide> - As part of the last update to the IM, in addition to filling out sections we added more IM elements, many based on OVAL. Also pulled in more from Henk and Nancy's individual draft IM. Document is big now. 153 pages and arguably not complete. That said, one thing we may want to do is break up the IM elements, decide which to standardize on, and maybe not include everything in the IM. Maybe pull out some and capture as their own documents. E.g., maybe all Windows based elements go in a separate document. Or maybe based on use case. The IM might just provide guidelines for creating information elements and incorporating into SACM.
[Jim Schaad] – Is it a problem about working on the IM, or finding reviewers.
[Danny Haynes] – More of review. Noncritical – they don't hold up work. May want to think about at some point.
[Dave Waltermire] – Are we going to far by defining all these platform specific items in the core IM. We are never going to enumerate all platforms people care about; we are picking favorites. Sounds like we want an IANA registry to let us grow over time. I'll read and provide feedback.
[Danny Haynes] – Great – I think we agree.
[Jim Schaad] – How much of this information shows up in CSVs in MILE?
[Danny Haynes] – I don't know.
[Jim Schaad] – How much shows up in reports that come in and in MILE work.
[Dave Waltermire] – Indicator information in IODEF reports? I don't know. I'll look.
[Jim Schaad] – Anything that shows up regularly in IODEF should be there.
[Dave Waltermire] – Are we trying to model the entire world of state information. We'll never be done with that. We'll never have DM that cover all that.
[Kathleen Moriarty] – Wouldn't it be better to pull in other DM rather than replicate. Maybe just indicate you will pull in something else that does this.
[Dave Waltermire] – Provide the framing to hook into other stuff.
[Kathleen Moriarty] – Maybe like the SCI RFC to have a framework and have a way to logically put in a DM. Anyone familiar with that? Within the IODEF DM there are hooks for additional data. There is an RFC that extends those hooks so the same data goes in the same places. This way when one party packages and another unpackages you can find. One hook you can put vuln data on; platform data. Placeholders there, rather than building out the whole DM. In the IODEF draft we use existing hash schemas rather than creating. That way the folks that evolve signatures and hashes can do that and we just reference.
[Danny Haynes] – Sounds reasonable. I'll look into.
[Kathleen Moriarty] – I'll put the RFC in chat. <RFC 7203>
[Danny Haynes] – The last other related topic was that when we defined IM elements, we used the same enumeration elements in a few places. If it is just a handful, no big deal, but if it comes up more we may want enumerations as Information Elements. Nothing we need to deal with right now.
[Jim Schaad] – I would be in favor so you don't miss an enumeration when you add an element.

[Danny Haynes] – With this last revision we were able to fill out all the sections that were TBD. They all have text. We defined different types of guidance. Added text for privacy and operational considerations. For now, pending WG feedback, we are looking start working with Information Elements and prototype a DM – get experience using the IM. Might run into issues. Looking to shift to that. Would be happy to get feedback on the [Ira McDonald] – things we are missing, what you

like/don't like, what is confusing. We need feedback. And then close out this requirements issue. Want to bring to WGLC, but want to test first.

[Jim Schaad] – I've been trying to understand. I think we should take this and DM to WGLC at the same time.

[Dan Romascanu] – When you say experience, this means what? Using IM to create at least one DM?

[Danny Haynes] – Yes.

SWID

[Charles Schmidt]: SWID Message and Attributes for PA-TNC. Short agenda. I will spend most of the time going through the latest revision which, unless you are a speed reader, you haven't read because I just sent it out yesterday. So in the latest revision, there are lots of little changes to it. Primarily, what the previous document SWID M&A for PA-TNC talked about: the data element being a SWID message and identifiers being SWID tag identifiers. We have generalized that in the latest draft so the only time it talks about SWID tags is as an example of a data model. We just referred to software records which are something that the endpoint has tracked that are indicative of installed software. This reflects the request that came in at IETF 96. Part of that is that we have added an outline for an IANA table that enumerates the software data models that are used by the document. The idea is that here will be a certain list of data models that an endpoint client (target endpoint) views as supported recalling that the endpoint will not necessarily have a lot of choice in the types of data it is consuming to describe its software. It is going to rely on the sources it has available. What is now software messages and attributes for PA-TNC now says the client (target endpoint) collects that information in one of the standard sets of data models and transmits any combination of those standardized data models across the wire to the server. So, we generalized the data model and we are no longer bound to a specific data model which is what the group agreed on. As part of that, we now are flexible with regard to data models and we can now transmit in a variety of data models at least the messages are capable of doing that. I realize not everyone is going to be thrilled with that (Jim), but, I request that before there are any objections to the multiplicity of data models that we at least get through the examples that I have so we can see what that entails.

[Charles Schmidt]: There is now a software data model IANA registry and each data model is associated with a 1-byte integer which should be overkill for our needs. There is a multiplicity of data models on the endpoint and the sources could leverage any format, but, the requirement is that it gets converted to one of the supported data model formats when it gets collected by the Posture Collector. The specification currently defines and fleshes out a little bit two data models: ISO 2015 SWID in XML and ISO 2009 SWID tags using XML. This reflects that the group was willing to use SWID tags as one of the base models from which we move forward and in Buenos Aires, everyone thinks the 2015 SWID tag is an overall better data model. The 2009 SWID tag is the data model we are seeing in real world system and people wanted to reflect that. That is what I have written in. There is no reason we can't add additional data models and ensure they are directly supported instead of just through conversion.

[Charles Schmidt]: The other change that predominates throughout the document is previously we had SWID tag identifiers as a concise way to identify software products. This uses 100-bytes as opposed to 10-kilobytes which is the size of a full SWID tag. We retained the concept, but, no longer refer to them as software identifiers. They are still expected to identify software product and version. Every piece of software will have a particular software identifier and each data model defines how you create a software identifier from an instance of that software data model. For example, in the SWID tag cases, you take the two fields in the data model, the reg_id and the unique_id fields, and you turn that into a software identifier. For either types of data

models, you would probably extract different fields and create the identifier. The result is that if a piece of software is reported, using separate data models to the posture collector, those different data models will likely result in different software identifiers even though they represent the same piece of software. This isn't anything that we weren't experience with the previous draft of SWID M&A because at that point we were talking about non-authoritative SWID tags versus authoritative SWID tags. That is, non-authoritative SWID tags would not have the same identifier as authoritative SWID tags. This I not a new issue, but, is an issue that I want to raise. Any questions or concerns about software identifiers?

[Charles Schmidt]: The other change that you will notice is that previously we had an instance identifier because in the old days we had SWID tag identifiers. We had an issue that if a single software product was installed multiple times on an endpoint, the SWID tag identifier for each instance would be the identical and you couldn't tell between the two. We are going to have the same problem here because the identifier is not required to be unique per instance, just unique per product. So, now we are using this thing called a record identifier which is that every time a Posture Collector pulls in a software record, in any data model, it assigns it a unique identifier. This is how we would then distinguish between those two instances because the two instances will be associated with two different records which means two different record identifiers. Then, the server can track instances individually by following the record identifier associated with them. This is actually even easier than what was done in the original document which was a source-specific way of presenting identifiers. This is far simpler. There is a single source; a single party responsible for assigning and managing record identifier sand that is the Posture Collector. That capability is retained. We are just using a different field and a slightly simpler identifier management technique than we had before.

[Charles Schmidt]: The first example is a software identifier inventory message formerly the SWID identifier inventory message. It is largely the same as it was before with one exception. Previously, the software identifier count which was the SWID identifier count is doing the same thing (counting the number of identifiers). What we have added is the Data Model Type field after Last EID. This is the one-byte enumeration by which data models are identified and this says in the following identifier (software identifier), it is derived from a specific data model. That is followed by the Identifier Length and the Software Identifier and the Record ID Length and Record Identifier. The only other difference is previously SWID tag identifiers required two fields: one for the tag creator reg_id and one for the unique_id. Now, those are entirely subsumed by the Software Identifier. This is basically the same message with a few fields reorganized and the addition of a new Data Model Type because we are allowing flexible data models.

[Charles Schmidt]: I have another example here. This is the Software Inventory message. It sends full records. Again, it's basically identical except that we now have the Data Model Type field added and the instance identifier which usually preceded the Record Length and Record fields is now a Record Identifier. So, again, the same format. This would be a great time for comments, questions, screams of horror. Anything?

[Charles Schmidt]: The nominal data flow. If you recall from earlier, this is pretty much the same thing. We have a set of sources and these are just some nominal examples. Nothing is required. The Posture Collector gathers information from each of them. What I have added is this thick arrow which is our translator and each arrow outputs to one of the supported data models by the Posture Collector. The idea is we have multiple sources. They could appear within the Posture Collector's collection of records as different data models. That's fine. As each record comes in, it is assigned a unique record identifier by the Posture Collector and the Posture Collector extracts

a software identifier based on the type of data model used after conversion. Otherwise, it is exactly the same as we saw before. Questions?

[Charles Schmidt]: So, this is my summary of changes which is actually not a whole lot. The only real change is that we have unbound this protocol from a single data model which is SWID tags and have now given it the ability to transport a variety of data models that identified using that Data Model Type field. Everything else is pretty much all the same as it was before. We can deliver inventory. We can deliver events. We can do full records which were previously tags. We can do targeted requests. All of the old functionality is still there. We simply have opened up the flexibility in how the protocol can represent the data that it collects. This is a great time for me to stop and wait for someone to say something. Do you like this change? Do you hate this change? What are people's thoughts? <silence>. Do people need to read and review the specification?

[Adam Montville]: I think that is the case.

[Charles Schmidt]: Ok.

[Adam Montville]: I was going to say that I think people might want to digest all the changes.

[Charles Schmidt]: Yeah, it's changes throughout the entire document. I did a diff and it was horrifying, but ultimately, the real question that I've got is people expressed concern about type binding to ISO SWIDs. That's now flexible. We can handle ISO SWIDs as well as other things. We can handle 2020 SWID tags if and when they come out.

[Dave Waltermire]: I like this solution from an agility perspective. If the world rallies around SWID tags and there is a new revision, we can handle that. If the world rallies around a different solution, we can handle that. I think it is a win-win.

[Ira McDonald]: I agree. I like it. Good work.

[Charles Schmidt]: Jim, you were the one who was on the record for wanting one data model.

[Jim Schaad]: That's not what I am on the record for. I want one SACM data model. I am willing to have additional data models.

[Charles Schmidt]: Thanks for the clarification.

[Charles Schmidt]: Alright, I am taking this as you are not hating it. Awesome. I do have some questions. Although, I am not sure we are really in a positon to talk about them, but, I wanted to bring them up to put what I have done in the context of some on-list discussions. One of the discussions, on the list, observed that there were really sort of three classes of software of interest. There is what is installed on an endpoint, there was the presence of packages installed or not installed on an endpoint, and there was a question about running software on an endpoint. Each of those has slightly different parameters surrounding each of those.

[Dave Waltermire]: The issue about packages was an email from Michael Godsey. He was talking about being able to report the presence of installation packages on the device.

[Charles Schmidt]: Yes, you are correct. That is the reference.

[Dave Waltermire]: Right. That is something that SWID tags could effectively support because there would be a corpus tag associated with the installation packages.

[Charles Schmidt]: Yes.

[Dave Waltermire]: If that avenue is pursued, could that just be reported like any other tag would be reported?

[Charles Schmidt]: So, there are some pivot points here. Yes, SWID tags could certainly capture software packages. We have the corpus tags. SWID tags are probably not the right way (without at least some modification) to describe running software because there are probably parameters of running software you want to know. The other pivot point from how you present the data is how the recipient knows what type of information that they have received. So right now, the specification, as written, assumes that it is reporting installed software not corpus tags, not

running software, just installed software. The recipient needs to know if it is getting a record that is describing something that is getting installed.

[Dave Waltermire]: You could make a semantic argument that packages are installed.

[Charles Schmidt]: I think there is a critical difference between having downloaded the RPM and then having installed the RPM.

[Dave Waltermire]: We can slice and dice this argument all day long. A package is an executable piece of code. A package is something that could be made vulnerable (because it executes). I think there are complex issues behind those differences. I think in some cases the difference is a difference without a distinction. In other cases, they are differences with a distinction. It seems like this is something we should try to support.

[Charles Schmidt]: Ok. Alright. Mostly my purpose in raising this is to show where the current specification is with respect to those previous discussions. I think further discussion on-list is a good thing.

[Dave Waltermire]: Can I just clarify one thing about my previous statement. I think running software is a very difficult problem because knowing whether or not it's running, how it's running, when it ran, and all of those questions is a lot of complexity compared to whether or not it is on the device. I think this goes well beyond what we are trying to do with this specification. To me, it feels like that's another layer of the problem that should be addressed with another message specification along the same lines. In some standardization efforts, installation presence and monitoring usage have been separated approaches. I know in ISO the same group that worked on SWID tags developed a companion standard around usage monitoring that there was a separate standard. I would suggest that we steer away from addressing running software problem in this specification.

[Ira McDonald]: Dave, my observation for what it's worth. In terms of correlation of the wide word of security information is TPMs, HSMs, etc. that do remote attestation, attest only exactly the running software and nothing about installed software.

[Dave Waltermire]: Is that because when you are referring to it tends to be firmware and operating system files that are executed at boot time?

[Ira McDonald]: And applications if they have the PC client extensions for a couple more PCRs. They are attesting to a measurement log of a bunch of measured software so all the way up to the running applications, but, after that the file systems.

[Dave Waltermire]: In those cases, are you testing to runnable software or not running software?

[Ira McDonald]: No, running software. It has been loaded and measured. Either by the bootloader for the OS, the drivers, or the OS for the application software and the libraries.

[Jarrett Lu]: Dave, I had agreed that running software can be complicated, but, I think being able to just identifying whether or not software is running or not has value.

[Charles Schmidt]: Just to step in, I don't think anyone is saying we should drop something. The question is does this belong in the specification and if so how. I think the answer is let's deal with the data and the data flows surrounding that. Do the descriptions make sense? Do targeted requests make sense? I fully agree with you that we don't want to ignore running software. People have a policy interest in that and a question of what goes here.

[Dave Waltermire]: Adding reporting of running software would include adding new messages and workflow to drive that collection. We could do that in this spec, but, that would mean another 6 months to a year of work to basically define how you could do running software within the scope of this document. An alternative would be to just develop another document that describes the message and workflow for capturing information about running software that would build on this.

[Charles Schmidt]: I think we want to avoid getting fooled by the similarities because software is involved in the name of all three types. Just because they are all about software, doesn't mean they all require the same set of processes. I think the latter we would want to key off of.

[Ira McDonald]: I agree it is fine to do a separate document Dave, but, I do think the work is of interest to SACM.

[Dave Waltermire]: I would like to understand your use case around TPM a little bit better too.

[Ira McDonald]: Yes, that would be good. Take a look at Andreas Fuchs Internet-Drafts on time-based unidirectional attestation because they take an array in MIBs and one for Yang to SWID tags. It is correlated with a measurement log and ultimately with a bunch of TPM PCRs that go all the way up to PCR 17 that are collective extensions, not separate measurements, extensions of hashes of progressively everything literally from the immutable ground boot loader, the mutable boot loader and on up, but, it is running software.

[Charles Schmidt]: I think this has been productive. I think the consensus (not to use that word) take it to the list. I don't want to eat up more of the time on this.

[Ira McDonald]: I agree.

[Charles Schmidt]: The only other thing that I wanted to mention is that there was another topic that actually dates back to Buenos Aires. Specifically, tracking data sources prior to normalization. This specification doesn't do that, but, the WG did in fact have consensus that it was something of interest so especially since the source can have an impact apart from the choice in data model. Sources may not populate the event in the same data models, for the same products, in exactly the same way. So, that's an open issue. Again, I would like to get feedback maybe on the list. Maybe after people have had time to look at the latest draft and see if the revisions if they still feel that this is something to do. It is something that I acknowledge and there was interest in. I didn't put it into this draft, but, it is something to consider. With that, next steps, keep talking, read the spec. That's really all we have for next steps at this point. I think that we need more discussion on this before we understand exactly if we are happy enough to start WGLC, be enough for the chairs to decide if there is consensus, or if there is more work to do. I suspect there will be at least some suggestions. I hope there will be anyways.

[Adam Montville]: Agree. Thank you. We will continue on the list as part of the way forward.

Roadmap

[Danny Haynes] – This roadmap came out of last IETF meeting. At the end of Friday there were questions about to go next and Karen proposed a Roadmap. This is a first attempt

[Danny Haynes] – The fields in the tables: here is the legend.

[Danny Haynes] – Architecture. Left importance, delivery, WGLC blank since we need to discuss. As of right now architecture is parked. Had one solution in mind but parked to understand NEA better. Plans to reflect this? Two types of information – intra SACM communication and endpoint information (SWID, OVAL) which are the payload of SACM components. Need to better distinguish between them. We have had discussions where we talked past each other on that. Maybe go back to architecture once we have talked about this. Also further define the capabilities for the VAS – that is more of an operational use case and with the architecture we can get more specific there. Purpose of these slides is to introduce these and then get more discussion.

[Danny Haynes] – Information Model – Need to split out SACM component needs vs endpoint information. Need to capture different needs with respect to software, configuration needed by VAS. Current IM does this, but there is some more work to do.

[Danny Haynes] – SWID M&A – get software from an endpoint and move to server. In the latest draft it is more DM independent. Also a milestone to understand what is MTI with respect to DM supported by the protocol.

[Danny Haynes] – Endpoint Configuration Information DM – Based on the OVAL work. Needed to supplement the software inventory information provided by SWID M&A to realize the VAS> This is more in early stages. At last meeting we compared different data formats. Now we need to prototype, do a bit more research regarding security mechanisms provided by data formats. Work to develop a chosen DM and work with the group to flesh out.

[Dave Waltermire] – To go back to a previous conversation, do we need a new DM or just describe how to use existing DM? One way to look at: have multiple existing protocols for many purposes. SNMP, Netconf, OVAL – all have DM associated with them related to collecting endpoint state information. Do we need a new DM to unify that, or provide the framing to communicate the information that was collected using the underlying DM.

[Danny Haynes] – We need something for communicating something. I don't think we want to be limited to one DM. Leveraging SNMP and Netconf would be useful. At the same time, OVAL is useful, but there is a lot that can be done to improve it. Probably a combination of all those things.

[Henk Birkholz] – Having a hard time understanding the answer. It is important we have something unified to communicate between SACM components; on the collection side use whatever you can use. Is that what you are saying.

[Dave Waltermire] – That is one way to approach the problem. Have to use whatever exists on the collection side – there are many standards and we don't want to reinvent. ON the broader SACM distribution side, I think we are at a crossroads: do we propagate what we collected, or do we come up with an uber-DM that represents all that data in a new model. That sounds like a large effort and requires reinventing of the wheel.

[Nancy Cam-Winget] – I'm getting confused to. The IM is supposed to be the abstract of the type of information that can be expressed. Do we have one DM that encompasses what SACM is trying to do. From a DM perspective we need to include all the elements, but in the action of collection or configuration, I'm not sure the DM maps one-to-one to the "real-time" dynamic execution of that DM.

[Dave Waltermire] – Not sure what that means.

[Nancy Cam-Winget] – An example could be: we instantiate abstractly in the IM the notion of having an element with a value. In that instantiation, the IM says "one of the elements needs to represent an IP"

[Dan Romascanu] – Good example. We need at least one way to share among the applications that are supposed to be SACM compliant. Otherwise applications are coming from different vendors will not operate.

[Dave Waltermire] – IP is just a data type. What we are actually referring to are configuration – what is assigned to a DNS resolver.

[Dan Romascanu] – Yes, but what we are talking about here are the building blocks.

[Nancy Cam-Winget] – Yes. What I was trying to show, in the IM, we define an "IP address". How it is represented is in the DM. (String, CBOR, etc.) It is an instance that says "I am an IP address". That is what is in the IM. In the requirements, where I thought there was consensus, we were going to have one SACM DM that mapped to the IM. We can define other SACM-compliant DM which could be a subset. Point 2, to your notion of configuration vs. collection, you could have a superset DM. A router wouldn't have a birthday, but can still use the DM without using that element of the DM. That's what I mean by real-time aspect.

[Dave Waltermire] – I understand composing more interesting information from elements. The challenge is – if we hand an implementer 400 elements, that won't happen.

[Nancy Cam-Winget] – Right. I don't know if the IM got discussed, but I think we want the SACM IM at a minimum. We can put extensions to address other things. I am concerned because we have blown up the number of elements. I'm not sure they warrant being in the IM.

[Danny Haynes] – Good observation. We talked about this and raised that concern. Right now we are going to stick in the IM and people can identify which should be extensions.

[Dave Waltermire] – Haven't done enough to discuss how you would talk about configuration settings that matter to an org. If I am interested in X, I need to compose up IM elements in a larger context. Would be interesting to work through a use case where we had SACM capability that would serve that. Seems like we have part of a solution.

[Nancy Cam-Winget] – Your solution may not look the same as someone else's

[Dave Waltermire] – How do we get interoperability.

[Nancy Cam-Winget] – We cannot be exhaustive.

[Dave Waltermire] – If I start with a Yang representation using Netconf, that gives me some context which I can carry through the system. If starting with 100 different tools are different that doesn't help the org. I would expect some propagation of that info.

[Henk Birkholz] – For this interoperability between SACM components, we need one solution (probably DM).

[Adam Montville] – Need to continue this discussion on list.

[Danny Haynes] – PA-TNC Extension for Endpoint Configuration Information: how do we communicate configuration to server. SWID M&A would serve as a good template. I think being DM agnostic is useful. Write, get WG feedback.

[Danny Haynes] – COSWID – Provides a CBOR representation of SWID tags. Out of the last IETF meeting, the next steps there were to get WG review and determine if WG wants to adopt.

[Danny Haynes] – Main discussion points: is anything missing or anything we want to add new capability? As far as ranking, I have a proposal? I think the architecture is probably top because there have been developments regarding NEA. The information capture there will feed into the [Ira McDonald] – this is a dependency. Also have SWID M&A and Endpoint Configuration – those are dependent on the IM to some degree since the data they represent should be mappable to the IM. Then PA-TNC extension for Endpoint Configuration is after DM. COSWID just because it has not dependencies and also not a blocker on other documents. Any thoughts? Also, if anyone working on these docs has some ideas on next delivery dates and WGLC dates?

[Nancy Cam-Winget] – Goes back to the question: once we have an IM, do we want to define a concise SACM model that maps to the IM. I'm not sure the endpoint configuration information will be sufficient for everything in SACM.

[Danny Haynes] – Agree – other work there.

[Nancy Cam-Winget] – Either we put more DM to address the VAS – doesn't feel like endpoint config is enough. One or more DM that are THE SACM DM or are SACM compliant.

[Danny Haynes] – As new work is being developed we can easily add and readjust.

[Danny Haynes] – For next steps, I'll work with the various draft authors to come up with notional dates. If anyone has feedback on prioritization, let me know.

[Karen O'Donoghue] – I think this will help guide the work and keep it moving. I think this needs some definition but don't over-engineer.

[Danny Haynes] – Would like this done by next week.

COSWID

[Henk Birkholz] – Small status report. Feedback from Jim: we were renaming attributes since some of the types in XML are not necessary. In order to report this there are some changes in the names. The next draft will explain. We plan to incorporate freely available documentation of every attribute

in SWIDs. Also working on compiling all freely available documentation. Will produce exhaustive documentation. Depending on how much work that is, this document is pretty much done. Target mid-early 2017 for final.

DM-001 discussion recap

[Danny Haynes] – From the discussion, we talked about the differences between my proposal and yours. The main concern was the dropping of "Derived from SACM DM element". I interpreted this as meaning "every DM must contain everything in IM".

[Nancy Cam-Winget] – Your update said "at least one SACM IM element", how is that not complete.

[Danny Haynes] – "Derived from". You can also have elements not derived from the SACM IM and that doesn't have that requirement. Allows extensions. If you say each DM element must map....

[Nancy Cam-Winget] – I thought I clarified that it could be derived from. I thought John Strassner said something. I think his may be more complete. I don't mind taking this back to the list if we think we can converge.

[Karen O'Donoghue] – Can we set a hard limit?

[Danny Haynes]/[Nancy Cam-Winget] – I would like to.

[Karen O'Donoghue] – John Strassner, Danny, Nancy, and Henk are the primary participants. Maybe a 48 hour window?

[Nancy Cam-Winget] – Can say that in the response to John.

[Adam Montville] – Between now and October VIM. Requirements update and progression. IM review and raise issue so we are discussion open issues. DM development and identification. Read and provide feedback of SW M&A to discuss at the meeting. Want to discuss and get out Roadmap in a week. There was an important discussion about the meeting od DM – should have that on the list soon. COSWID review.