IETF SACM WG Virtual Interim Meeting
February 4, 2014

Attendees:

Jon Baker
Jim Bieda
Henk Birkholz
Nancy Cam-Winget
Mike Cokus
Juan Gonzalez
Steve Hanna
Matt Hansbury
David Harrington
Danny Haynes
Lisa Lorenzin
Dave Misell
Adam Montville
Luis Nunez
Dan Romascanu
Dave Waltermire

Meeting started at 11:00 AM EST (New York time)

Agenda Bashing
Nancy must leave early so requirements will be first on the agenda.

WG status

Nancy has been having trouble submitting her requirements draft. She can't access the submit page. She sent her draft by email so we all have it. She will submit a ticket to get that fixed.

For the use cases, we don't have a new draft. Dave H. and Dave W. will describe where we are.

Requirements

Nancy ran through the new draft that she sent by email - draft-camwinget-sacm-requirements-02 dated Feb 02, 2014

The main changes were a complete rewrite of section 3. Previously, she had security requirements but those were Mom and Apple Pie.

Dan said that we dont need to have a Terminology section since we're just referring to another document. We'll still have that reference but not have a section for it.

Someone said that 'use-cases' doesn't usually have a hyphen in it. Nancy explained that this is part of the way that she's doing references.

Nancy said she didn't change the Reference Architecture Model (section 3.1) much from the last version.

Nancy reviewed Dave Waltermire's comments.

She will change Asset to Endpoint.

Dave W. said that the distinction between collection and evaluation isn't clear here. Nancy said that she mainly wanted to show that attributes can come from a collector or from a repository. Dave W. said that he agrees with this but we also need to show that collection and collection and evaluation are distinct. Nancy said that she will try to prepare a revised architecture. Dave W. said that he's glad to help with that. Nancy accepted his offer. They'll work together offline.

Jon Baker agreed with Dave W. You need to separate the collection method from the evaluation. There are to separate paths for collection. Nancy agreed. She wanted to show this in her diagram but it didn't come out quite right.

Steve Hanna said that there's a missing piece in the architecture: the Collector. At times, the Collector will simply place Attributes into a Repository. At other times, the Attributes may go directly from the Collector to an Evaluator.

Dave W. and Jon Baker said that there are several ways to do collection: periodically, upon request, or triggered by an event (e.g. a change on the endpoint). In all of those cases, there may be instructions that guide the collector on which attributes need to be collected.

Nancy said that the model may be more complex than she thought.

Jim Bieda said that the Evaluator may need to be adjusted to reflect the environment that its running in. He thinks that the model as articulated by Nancy offers plenty of flexibility.

Nancy said that we need to be clear with what the term Evaluator means.

Dave W. agreed and said that we need to use the term consistently throughout all of our documents.

Nancy said that the main piece of work for this WG is having standard protocols for getting attributes to the consumer. Dave W. said that there's more to it. We need to also work on protocols for directing and managing the collection and evaluation of attributes.

Jim Bieda said that the Evaluator and Assessment Consumer could sit on the endpoint so that could solve Dave Ws concern. Nancy said that we need to elaborate on the architectural model. Perhaps a better description will help explain the existing diagram. Jon Baker said that he understood that multiple functions could live on the Endpoint or in an enterprise system.

Steve Hanna suggested that we move this discussion to the email list. Adam and Dan agreed.

Dan asked whether the document can be submitted as a WG draft this time. Dave W. suggested that we get the current version posted as an individual submission and then discuss it on the email list and then move it to WG draft status. Steve Hanna agreed. Dan said we only need three things to make it a WG draft: it's headed in the right direction, it's within the charter, and no other proposals are expected. Still, we agreed that we want this document to come in as draft-camwinget-sacm-requirements-02.txt.

Nancy reiterated her plan to submit the current draft as draft-camwinget-sacm-requirements-02.txt

Dan agreed and asked everyone to provide comments on the email list ASAP so that Nancy can get another draft posted by Friday, February 14. Nancy agreed to post another draft with as many changes as possible, based on the email discussion.

David Misell said that if there's a lot of work required to edit the diagram, others can offer to help her with that. Nancy said that she expects several more iterations on the architecture.

Nancy reviewed the changes to sections 3.2 and 3.3.

Section 3.2 describes the general requirements, mainly taken from her earlier spreadsheet. These were all discussed at the previous virtual interim meeting.

Dave Harrington and others pointed out that OSI layer numbers should not be used in the document. Instead, IETF layers should be used. Nancy agreed and promised to change this in the next version.

Lisa asked whether we would standardize an authorization policy language for controlling access to information. Nancy said we could consider that but at least the need for authorization would be referenced in the security considerations.

Nancy asked whether we have consensus on including a requirement on filtering. Dave W. asked for more requirements based on Use Case 2.1.3. That goes beyond filtering to event-driven collection vs. query-driven collection. Nancy said that she referenced asynchronicity in REQ-007. Maybe she just needs to reference Use Case 2.1.3 there. Dave said Sure. And we need to talk through how filtering can be done in an event-driven model.

Nancy asked whether the group prefers the term event-driven instead of asynchronous. Lisa and several others said yes. Nancy said that shell make that change.

Dave W. requested specific mention of various kinds of scalability requirements. Nancy pointed out that in section G-003 she talked about datagram size limits. Dave W. said that there are other more specific requirements. He'd like to see those listed in section 3.3.

Dave W. asked if we should reference the SACM WG in the document. We should reference the other documents but not the WG since the WG will go away. Dave H. agreed. Nancy said that shell make that change. Dave W. pointed out that similar changes are needed in the use cases document.

Terminology

Adam added a long list of terms extracted from the use-cases-05 draft. We still have the list of terms from the terminology-01 draft. Next, he intends to get some feedback on which terms we want to define in the terminology draft.

Asynchronous is equivalent to event driven (as per Nancys document, requirement 7)

Lisa pointed out that some of these terms are already defined in the NEA specs. Adam said thats fine but we should note that. Dan asked whether we'd copy the definition in that case or just reference it. Adam said that he's not sure. Maybe it would be easier for readers if we just copied the terms. Dave W. said that in section 2.2 we copied the definition and referenced it. Adam said that seems like a good idea for stable sources.

Dan said that some of these terms are very basic: industry group, for example. Do we really need to define these terms? Dave W. asked people to send an email to the list if they have a definition of these terms from a stable reference.

Dan asked whether we should expect another version of the terminology draft before February 14. Adam said probably not.

Dan said that he'll try to get support for remote participation at the London IETF meeting.

Use Cases

Dave H. reviewed his email where he identified all the QUESTIONS in use-cases-05 and suggested resolutions. He said that most of these have been discussed already. They were reviewed.

For QUESTION 1, Dave H. said that we've discussed this before and agreed that we want to keep the language as it is. Dave M. asked if the user might perform an evaluation directly. Dave H. said that they'd use an application.

For QUESTION 2, Dave H. said that we agreed not to list acquisition methods. There are many and we dont want to try to list all of them. Lisa said she's happy with the proposed text. She asked where we could include a list of protocols. Dave W. said maybe in another document. Dave H. said that the consensus seems to be that we shouldn't mention specific protocols. Steve said maybe in the architecture we could mention some, in conjunction with mentioning which protocols meet which requirements. Lisa

said it could be useful to show what we have in mind but she doesn't feel strongly about it.

For QUESTION 3, Dave H. said that some sort of output from the assessment should be included in the workflow. Dave W. said that we had consensus on this during the last Virtual Interim call. Dave W. read back the proposed text for the draft. Adam suggested that we should use the term result of the evaluation instead of result of the assessment. Steve suggested that we use the term evaluation result. Dave W. read back some proposed text using that term. All agreed.

For QUESTION 4, Dave H. said that Endpoint Discovery probably shouldn't focus on determining the type of endpoint. Instead, it should focus on discovering the set of endpoints. Later, the endpoint type should be determined. That's one of the attributes. Lisa suggested that we say The purpose of discovery is to determine the presence and types of endpoints available for posture assessment.Adam said that determining the existence of endpoints is the first step. Determining the types of endpoints is separate. Dave W. agreed but said that figuring out an endpoints type is also a valuable step to come before the Identify Endpoint Targets step. Dave W. will come up with some draft text for that.

Dan said that Dave H. will continue to review the further questions. We should all respond to his comments to make sure we have WG consensus.

Dave H. said that he's coming back from travel on Monday and will work to get questions resolved in time to provide a revised draft by February 14 with all the questions resolved.

Dave H. asked if people are happy with the direction of the use cases document. Dan, Steve, and Lisa said yes.

Way Forward

Nancy will submit the requirements document as an individual submission. We probably won't see another version of the terminology draft before the February 14 deadline.

Another version of the use cases document will be prepared before the deadline.

Active remote participation is expected at the London IETF. David H. and Adam will be remote. Well try to make best of remote participation tools.

The participants in the virtual interim call were satisfied with the progress in the call (also in the previous virtual interim). We will continue to use this system as needed. However, we won't have another virtual interim until after the London F2F meeting.

Meeting adjourned at 12:50 PM EST (New York time)