SACM Notes

IETF 100

Summary

The briefest of briefs… SACM met at IETF 100 and discussed the working group's current status, a change in chairs, and a pending re-charter effort, among other topics. The group's immediate concern is ensuring we have sufficient and appropriate milestones supporting possible work items in our proposed re-charter.

Terminology will be updated and kept current; there seemed to be some interest in reviving the architecture effort.

Raw Notes

Jarrett Lu

Unfortunately, Jarrett's notes didn't survive and we no longer have access to them.

Roman Danyliw

SACM @ IETF 100
Wednesday Session I
9:30 - 12:00 - Sophia

Chairs: Adam Montville (outgoing), Christopher Inacio (incoming), Karen O'Donoghue

1. WG Status
==========
presenters: chairs
slides: https://datatracker.ietf.org/meeting/100/materials/slides-100-sacm-chair-slides/

The chairs summarized the status of the working group.
** Adam Montville is stepping down as chair; Chris Inacio is the incoming new chair
** A new charter for the WG is with the IESG

The agenda was bashed as follows:
** (Jarrett Lu) Adding terminology discussion
** (David Waltermire) Adding document status and next steps

2. ROLIE Core and ROLIE Software Descriptor
==========
presenter: Stephen Banghart
slides: https://datatracker.ietf.org/meeting/100/materials/slides-100-sacm-rolie-and-rolie-software-extension/
drafts: draft-ietf-mile-rolie-13 anddraft-ietf-sacm-rolie-softwaredescriptor-00

Banghart summarized the status of the ROILE draft (in MILE and currently being revised for IESG feedback) and the software descriptor extension.

Q: (Chris Inacio): how many have read the October version of the draft?

: (WG count) ~2
Comment: (David Waltermire): the authors can't do more with the draft without WG feedback

3. Data and Control Plane Security Baselines
==========
presenter: Liang Xia
slides: https://datatracker.ietf.org/meeting/100/materials/slides-100-sacm-network-infrastructure-device-management-plane-security-baseline/
drafts: draft-xia-sacm-nid-dp-security-baseline-00
: draft-dong-sacm-nid-cp-security-baseline-00

Liang Xia introduced two drafts related to collection and messaging for security posture.

Q: (Eric Voit) What is the boundary between YANG push and PANIC? How does PANIC relate to attestation?
A: (Liang Xia): YANG push is a good starting point. Ability to conduct attestation is important for operator trust. The issued need to be considered as a whole.

Q: (Chris Inacio): How many have read the draft?
: (WG count) ~6 people

Q: (Stephen Banghart): What is the goal of the draft -- register additional YANG models?
A: (Liang Xia): Collect postures from network devices; and conduct smart filtering
A: (Stephen Banghart) Is it fair to say that the YANG models that align to SACM are being defined
A: (Liang Xia): Yes
A: (Stephen Banghart): To reiterate the AD's feedback, there are a lot of existing models to choose from already
A: (Henk): In the context of security, the use of the term baseline is confusing. There is a deconfliction to be done relative to what is already defined.
A: (Liang Xia): Yes, baseline term might not be correct.

Q: (Chris Inacio, as contributor): A lot of YANG modules were defined. Do you anticipate publishing guidance on what the values should be for these elements?
A: (Liang Xia): No, this work is trying to specify what information is needed. Providing concrete values may be difficult.

4. Management Plane Security Baseline
==========
presenter: Qiushi Lin
slides: https://datatracker.ietf.org/meeting/100/materials/slides-100-sacm-network-infrastructure-device-management-plane-security-baseline/

Qiushi Lin introduced

Q: (Henk Birkholz): Both I2NSF and SACM are developing modules for state of end-points; and it seems redundant. This draft has a lot of overlap with draft in I2NSF. It may be resolved during this afternoon's meeting to resolve YANG modules. Maybe we need only one YANG modules? Some of these models look identical.
A: (Eric Voit): +1. The interest in YANG push in SACM is good. Please also come to the NETCONF meeting tomorrow because this work is almost at WGLC.

Comment: (Dave Waltermire): This draft seems to be motivate by missing YANG models. I'd like to seem an analysis of what's missing, perhaps with coordination with other YANG exports. Perhaps a draft

identifying the missing YANG element would be as helpful as a solution
A: (Liang Xia): We would like to do this work in SACM, as it is the best place for the end-to-end work. There is a lot of work remaining on managing the network devices. The proposed analysis required, as is the complete solution.

5. Hackathon Report
==========
presenter: Henk Birkholz
(no slides)

Henk Birkholz presented what SACM work occurred during the IETF 100 Hackathon.

Q: (David Waltermire): You noted that there was existing work around declarative and imperative guidance. What drafts should be read?
A: (Henk Birkholz): Let's
A: (David Waltermire): Perhaps we should submit drafts in SACM? Can pointers be posted to the list
A: (David Waltermire): Could the relationship to I2NSF be clarified.
A: (Alexander Clemm): There is also a discussion on MRTG on how policy, intent, service models relate. Perhaps this is a also related
A: (Henk Birkholz): To build a general purpose solution is challenging and they fail; so WG create their own; but then they look related

6. Terminology Discussion
==========

Jarrett Lu noted there has been little discussion on terminology since the Prague meeting. A separate draft of terminology is still needed. How would the WG like to move forward?

Comment: (Henk Birkholz): Both the architecture and information model drafts have expired. The architecture draft is refactoring. Right now the Hackathon was more important and will inform the architecture.

Comment: (Nancy Cam-Widget): The terminology draft is important. For the XMPP-Grid work in MILE, referencing the terminology draft was important.

Q: (Karen O'Donoghue): This draft seems important but is not moving forward.
A: (Nancy Cam-Widget): There should not be many outstanding issues.

A: (Henk Birkholz): to AD, what is the position on supporting drafts?
A: (Kathleen Moriarty): The WG needs to push for publication of such supporting grades. There is also the use of the wiki.
A: (Karen O'Donoghue): Has that worked well? Can this be referenced by a draft?
A: (Kathleen Moriarty): An expired drafts can used instead and then referenced as an informative reference.

(various conversation on advancing the architecture draft)

5. Way Forward
==========
presenter: Chairs

The active drafts in the WG are:

** draft-ietf-sacm-coswid-02 -- (Henk Birkholz) the submission deadline was missed and there are a significant list of changes to add to the draft. This draft also has applicability to SUIT BOF. No additional help is required.

Comment: (Dave Waltermire) WGLC by next meeting would be a good milestone.

Q: (Chris Inacio): Does the update include the use of CoAP?
A: (Henk Birkholz): There should be no reference to CoAP in the document.

Q: (Karen O'Donoghue): When can an updated be submitted?
A: (Henk Birkholz): This could be done by lunch today. This document uses a lot of ISO references and the referenced schema is broken. The draft needs a more concise definition.

** draft-ietf-sacm-ecp-00 -- (Adam Montville) this draft is ready to be updated.

Comment: (Danny): updates will be made per SWIMA.

** draft-ietf-sacm-nea-swima-patnc-01 -- (Karen O'Donoghue) this draft went to WGLC and all comments have been addressed

** draft-ietf-sacm-rolie-softwaredescriptor-00 -- (Stephen Banghart) Nothing more to add beyond earlier request for help.

Comment: (David Waltermire): The authors don't see any outstanding issues. Could there be a WGLC to force WG feedback.
A: (Karen O'Donoghue): We could.
A: (Stephen Banghart): I have no more changes to make.
A: (Karen O'Donoghue): How many people have read any version of the document?
: (WG assessment) ~1
: More feedback please

** draft-ietf-sacm-terminology-13 -- previously discussed

Significant discussion also occurred around the charter and charter milestones that the chairs took as input.