Information Model Update

SACM Virtual Interim Meeting

01/11/2017
Agenda

• Status

• Open issues

• Next steps
Status

• Submitted -08 on December 5, 2016
  • Various clarifications with respect to subjects and attributes
  • Defined a syntax for category IEs
  • Fixed numerous errors generated by Travis-CI

• Still need to figure out the scope of the IM
Issue #8: Define a provenance/chain-of-custody information module¹

• Captured as a need for provenance and chain-of-custody information in the early meetings of the EID-DT²³

• While the WG wants to support this, there seems to be some consensus around providing extensions points rather than explicit mechanisms

• Is there agreement with this line of thinking? If so, can we close out the issue?

Issue #9: Consider network topology and location information as identifying attributes

- Raised out of the April 17, 2015 EID-DT meeting

- Support location via the locationName IE (Section 7.52)

- Does not currently support network topology information. Some ideas:
  - Network layer
    - L2 (e.g. link-layer-neighborhood, shared-broadcast-domain, broadcast-domain-label)
    - L3 (e.g. next-hop-routing-neighbor)
  - Zones (e.g. internet, enterprise DMZ, enterprise WAN, enclave DMZ, enclave)

Issue #11: Security considerations - IP spoofing

- During an EID-DT Meeting, there was a suggestion that the Security Considerations section should include text about spoofing IP addresses as well as other identifying information.

- Security Considerations section currently operates at a much higher level
  - Authentication, confidentially, integrity, restricted access

- Operational Considerations section focuses on endpoint designation among other things
  - Multiplicity, persistence, immutability, verifiable

- Do we need to capture this in our Security Considerations section? Or, can we close out the issue?

2. [https://www.ietf.org/mail-archive/web/sacm/current/msg02612.html](https://www.ietf.org/mail-archive/web/sacm/current/msg02612.html)
Issue #15: Identification and definition of attributes

• Focuses on naming and defining IEs as well as acceptable datatypes and requirement levels

• The current IM provides naming conventions, a format for defining IEs, and datatypes
  • Still need to figure out which IEs are MTI

• With the exception of selecting MTI IEs, has this issue been addressed and can we close it out?

Issue #17: Identifying attributes

• There was some confusion around the original title of the section concerned with attributes that identify endpoints
  • Suggestion to change the title from "Identifying Attributes" to "Endpoint Identifying Attributes" and to update the first sentence of the section

• The current IM contains a section titled "Endpoint Designation" that addresses identifying attributes as well as includes revised introductory text

• Does the text in the current IM address this issue?

Issue #18: How known⁠¹

• Previously, the IM had a section concerned with how a provider knew about an attribute²

• It was suggested that a "derived" value be added to the collectionTaskType (network-observation, remote-acquisition, self-reported, etc.)³. Also, want to add "authority“ and "verified".

• Does this make sense to the WG? Can we close out the issue after we add "derived"?

---

Issue #25: SACM components (except at endpoints) MUST have time synchronization\(^1\)

- Out of an EID-DT meeting, there was discussion around the need for SACM components to support time synchronization\(^2\)

- From the discussion, two requirements were proposed:
  - SACM components residing on target endpoints SHOULD implement time synchronization and add correct timestamps
  - SACM components that do not reside on target endpoints MUST implement time synchronization and add correct timestamps

- Do these requirements belong in the Architecture draft provided the IM supports the necessary information needs?

---

2. [https://www.ietf.org/mail-archive/web/sacm/current/msg03177.html](https://www.ietf.org/mail-archive/web/sacm/current/msg03177.html)
Issue #26: Terminology change away from the terms "identification", "identity", "identifying"\(^1\)

- At IETF 93, there were concerns raised around identifying endpoints\(^2\)

- Renamed the process of identifying attributes to "endpoint designation", however, the IM still makes reference to "identifying attributes"

- Feedback in the GitHub tracker suggests that, if the terms are accurate, we should use them despite any negative connotations as long as we provide a way to protect privacy in the Privacy Considerations\(^3\) section

- How do we want to proceed on this issue?

2. https://www.ietf.org/proceedings/93/minutes/minutes-93-sacm
Issue #35: Do we care whether an attribute was authenticated or unauthenticated

- As part of the feedback on the Vulnerability Assessment Scenario, it was asked if the WG cared if data was authenticated or unauthenticated

- It was noted that this is closely tied to provenance and we may also want to consider quality of the data

- One suggestion was to add basic enumerations for things like level of authentication, level of assurance, etc.

- How do we want to proceed?
  - Boolean attribute for whether an attribute is authenticated
  - Add enumerations for different levels of authentication, assurance, etc.
  - Something more complex

Next steps

• Continue resolving open issues on the mailing list

• Need to decide on the scope of the IM