RATS - Virtual Interim

Thursday 20-June-2019,

https://datatracker.ietf.org/meeting/interim-2019-rats-01/materials/agenda-interim-2019-rats-01-rats-01

Participants Present on webex:

1) Michael Richardson (MCR) 2) Nancy Cam-Winget 3) Antti Kolehmainen 4) Carl Wallace 5) Carsten Bormann 6) Cheng-Mean Liu 7) Dave Thaler 8) Eric Voit 9) Giri Mandyam 10) Henk Birkholz 11) Ira McDonald 12) Jessica Fitzgerald-McKay 13) Mike McBride 14) Ned Smith 15) Paul Rowe 16) Simon Frost 17) Wei Pan 18) Call-In User_5 (Simon Frost + others from ARM) 19) Call-in User_6 (Peter @ NSA) 20) Call-in User_7 (never spoke) 21) Call-in User_8 (Paul Rowe) 22) Sergei Trofimov 23) Thomas Fossati 24) Antoine Delignat-Lavaud 25) Russ Housley 26) Sarah H.

Chairs * Kathleen Moriarty (CM) * Nancy Cam-Winget (NC) * Ned Smith (NS) Area Director * Roman Danyliw (RD) – not on the call

Note takers:

mcr cabo

Agenda bashing:

- Agenda bashing, Logistics -- Chairs (<5min)
- Chair's review of document status and logistics - <5min
- Use Cases - <5min
- Document updates:
- Architecture - 5min
- Current data models & serializations (EAT, PSA, TUDA and Reference Interaction model) - 25min
- Information Model start – 10min
- Use Cases – 10-20min
- Next Steps – adoption readiness and AOB (~5-10min)

Chair's Discussion

Dave Thaler: Do we have WG consensus that we want a use case document?
... Nancy: No consensus yet, progress needs to be made first before we decide...
Dave: It is useful to have a place where use cases can be referenced from
Dave: My opinion is that it should be in an RFC, as its own document or as part of, say, an architecture document

Nancy will create an IETF-RATS-WG organization as per the GITHUB ID/RFC.

Michael discusses Use Cases

Michael re use cases: Users are not end systems, they are other attestation systems out there. (I.e., not Sony Pictures, but FIDO)
Dave Thaler: Yes, but keep participants of the "Sony Pictures" kind, "admin use cases"

"Attestation Service"
MCR: TCG scenario, "only machines on network which have attested"... * TE case * network attestation, / Ned: device onboarding

Nancy: in the industry, doing different levels of access control based upon the capabilities of the system.
Eric: Access Control is a specific use case. However, there can be more details such as will access control be done in concert with DHCP, BGP, etc. Protocols specific integration should be addressed within other WGs. This is much like EAP is transported within multiple protocols.

Dave: major architectural impact questions that it needs to answer. needs to answer A or B, or both. The use case document should document the min set of use cases that motivates the major architectural decisions. "whether a relying party trusts the attestion server", the "attestion server" does authorization.
The other case: "claims are put into the token", and the relying party uses those claims to make the authorization decision itself. So, we need a use case for each of these.

MCR gives up the MIC. Henk: trustworthy inventory management, hardware/software compositions. "If one installs a game on the office computer, it can not attest that it is just an office computer"

HENK slides.

- RATS Architecture ROLES
- then goes through the various proposals: EAT, PSA, TUDA, DT: does it have to be a remote source of time? DT points out that if it is trusted, it does not matter if it is remote or not.
- YANG module: datastore and RPC. The attester has to be a "YANG" server. NC: it seems a bit too much TPM oriented.
- Four roots of trust: measurement, reporting, storage, integrity. Looking for development systems that has all four.
- TCG has definition (LINK? one copy is https://www.commoncriteriaportal.org/files/ppfiles/TCG_PP_PC_client_specific_TPM_SecV2_v10.pdf) for these four roots of trust. Also perfectly aligned with NIST document (NIST SP 800)
- Ira also posted the link to GlobalPlatform definitions: http://globalplatform.org/wp-content/uploads/2018/07/GP_RoT_Definitions_and_Requirements_v1.1_PublicRelease-2018-06-28.pdf
- slide about poorly documented challenge/response APIs...
  - created a proof of concept example based upon CoAP/CDDL/CBOR... "running code" (almost)
- "quick ratholing" --- bootstrap of trust from some place (NIST, TCG, GlobalPlatform).
- comparison of NIST and GlobalPlatform links.
- Ned: identified the problem with the term "roots of trust" being inconsistent
  - have to map the terminology out, and distinguish the different semantics.
  - Ira: TCG and GlobalPlatform have been working to harmonizing the terminology (with NIST). There is a formal project to write the mapping white paper. .. guestimate will be done in a year or so. Nancy: Is there a draft? Ira: No, meeting notes and edits.
  - Ira: does FIDO have a glossary. Giri: has a glossary in FIDO, but did not go into the mapping.
  - Giri: Focus on attestions that originate from a RoT. GlobalPlatform and NIST. There are attestions in Adnroid that do not originate in a RoT.
  - Ira: GlobalPlatform ... "extended"^Wsomething-else RoT. Software RoT that can be trusted because it can be attested to.
  - Giri: do not build into the architecture assumptions that are not-secure?
  - DT: do not limit the use cases to those that only have a hardware RoT, rather document what the results will be if the RoT is not anchored in hardware RoT.
  - Ned: definition of RoT is out of scope, but we are going to define ways for interoperability to occur between them.
  - Nancy: define our intent of what the RoT in scope, but not to actually define what it means
  - DT: "if you don't have a hardware RoT, then these are the considerations you have to make"
- DT SUIT WG, uses the term "trust anchor" (not "RoT"),
- NED: the TEEP terminology is at odds with the industry definition?
- DT/Russ: this is not the case, they are identical
- Henk: (did not capture ToR/trust-anchor comment)
- Henk: is JSON an interesting serialization? But if we use CDDL to describe the protocol, then JSON can be described.
- DT: "the thing that comes to the relying party" -- case for it to be JSON, cases for CBOR, and cases for it being X509. Because it has to be carried in different protocols.
  - consider the attester that talks to OPCUA (industrial IoT), and carries X509 certificates to have authorization policy applied by the Relying Party
  - mcr: could you carry CBOR in an X.509 extension?
  - DT: yes, at possible expense of extra CBOR parser that wouldn't otherwise be there, and possible conflict with X.509 claims that might already be standard?

HENK Information Model.

- "consensus on a core vocabulary"
- verifiable (can compare to a reference value) vs non-verifiable (the velocity one is falling) assertions.

Questions:
IRA: did Ned say, to use RoT, but not define it.
NED: Yes. Nancy: we need to clarify the vocabulary.
MCR: I think we are going to use the term, but not try to define them ourselves.
NED: acknowledge that RoT exist, and the industry has many definitions.
Nancy: the mapping is already happening?
IRA: But if the IETF does this mapping, then it will accelerate the mapping by a year.
NED: it is within the scope of the RATS architecture terminology section to identify the terms and explain the mapping.
Simon: it seems to within the ....
Henk: a hardware-agnostic YANG model would need to have an abstraction of the RoT (what functions/primitives they do)

Seal/unseal, rolling hash and ... if one does not define them, then one winds up with the hardware-specific terms.

Henk: Hannes raised the question about claims in CWT vs claims in RATS/EAT.
Giri: tried to answer this question... part of expert review for CWT registry is to make sure the claims do not overlap with other things. The registry is already established, and the experts are already informed.
Ned: what is currently registered might have different semantics, and RATS might need to define a profile for any existing claims, and if they are relevant.
MCR: maybe we need to ask to have IANA add a column about utility for RATS in the CWT claims registry.

Eric: do we want to have a deeper review of what is being attested? Carsten: could add a new column, "recommended for attestion"

Ned: some assertions will be RoT specific, unclear how to handle them yet. there may not be an equivalent way to encode them in CWT, so we would have to have a wrapper. Nancy: continue this discussion on the list: IANA changes, CWT container change...

12:21 Henk is finished.
ACTION: Henk and Dave to help with more specific use cases.

EOB Topics

Discussion about token binding document: table the adoption. MCR re-iterates that the use case document should be adopted (for agenda time-management reasons only), but never published.