RATS October 23, 2020 Virtual Interim Notes

Chairs: Nancy Cam-Winget, Kathleen Moriarty, Ned Smith
Notetakers: Ned Smith, Jessica Fitzgerald-McKay

Agenda:

1. Agenda Bash (5min)
2. Architecture – Michael (15min)
   • https://tools.ietf.org/html/draft-ietf-rats-architecture-02 (https://tools.ietf.org/html/draft-ietf-rats-architecture-02)
   https://www.ietf.org/proceedings/interim-2020-rats-06/slides/slides-interim-2020-rats-06-sessa-rats-architecture-status-00 (https://www.ietf.org/proceedings/interim-2020-rats-06/slides/slides-interim-2020-rats-06-sessa-rats-architecture-status-00)
3. EAT – Laurence (20min)
   • https://datatracker.ietf.org/doc/draft-ietf-rats-eat/ (https://datatracker.ietf.org/doc/draft-ietf-rats-eat/)
4. Network Device Attestation - Guy (15 min)
   • https://datatracker.ietf.org/doc/draft-fedorkow-rats-network-device-attestation/ (https://datatracker.ietf.org/doc/draft-fedorkow-rats-network-device-attestation/)
5. Interaction Model – Henk (10min)
   • https://datatracker.ietf.org/doc/draft-birkholz-rats-reference-interaction-model/ (https://datatracker.ietf.org/doc/draft-birkholz-rats-reference-interaction-model/)
6. CHARRA Update – Eric (10min)
   • https://datatracker.ietf.org/doc/draft-ietf-rats-yang-tpm-charra/ (https://datatracker.ietf.org/doc/draft-ietf-rats-yang-tpm-charra/)

Attendees:

1. Nancy Cam-Winget, Cisco
2. Ned Smith, Intel
3. Dave Thaler, Microsoft
4. Eric Voit, Cisco
5. Guy Fedorkow, Juniper
6. Ira McDonald, High North Inc
7. Jessica Fitzgerald-McKay, NSA
8. Kathleen Moriarty, Dell

9. Laurence Lundblade, Security Theory LLC
10. Michael Richardson, Sandelman Software Works Inc
11. Peter Yee, AKAYLA
12. Thomas Hardjono, MIT
13. Wei Pan, Huawei
14. Henk Birkholz, Fraunhofer SIT
15. Giri Mandyam, Qualcomm
16. Thomas Fossati, ARM
17. Sarah Helble, The Johns Hopkins University Applied Physics Laboratory
18. Andrew Guinn

Meeting Minutes:
Agenda:

1. Agenda Bash
2. Architecture
   - met 8 or 9 times since last IETF meeting
   - 100 or so pull requests closed
   - think they are done
   - Added section called 'reference values' and two new definitions (reference value provider, reference values)
   - Changed the high level diagram to add RVP entity as a 'stared' box which isn't normative at this time.
   - Lots of new text about the Verifier role that describes the duties a verifier needs to perform.
     - It includes explanations for keys and the expectation they will be provisioned.
   - Freshness and other edits were added
     - The main addition was to add handles in addition to timestamps and nonces.
     - for those who have not read anything since IETF108: https://www.ietf.org/rfcdiff?url1=draft-ietf-rats-architecture-05&url2=draft-ietf-rats-architecture-07 (https://www.ietf.org/rfcdiff?url1=draft-ietf-rats-architecture-05&url2=draft-ietf-rats-architecture-07)
   - The design team believes architecture draft is ready for last call.
   - Nancy: Observed there were others who have read the draft and therefore will issue the last call in 2 or 3 weeks due to holidays etc.
3. EAT
   - Presented slides describing Verifier - trust establishment in the Attester
   - Asks the question "what goes into EAT to identify the key?"

- There should be interoperation between different attesters and verifiers from different vendors (towards a generalized verifier)
- Introduces a verification key ID (VKID)
    - Taxonomy of VKID presented in detail (looking for discussion and feedback)
        1. COSE KeyID as VKID - example: COSE KID header parameter
        2. URI as VKID - could leverage HTTP to identify where to obtain the key (see draft-ietf-cose-x509)
        3. Base the VKID on the Claims - standardize a claim; similar to ARM PSA?
            - Challenges: Need to decode the payload verify things then go back to the rest of the payload
        4. VKID is in Evidence - Attach X.509 cert to EAT - can use COSE X.509 to wrap EAT (I think?) - similar conceptually to other appraches
- Comments
    - Dave Thaler - Q: No strong preference, but should support 2nd and 4th rows. Important to support certificate *chains* not just keys/certificates and those rows do. Nothing in the table is really RATS specific but really applies to any use of COSE, so ideally just reference the cose draft as much as possible.
    - Laurence - The goal isn’t to standardize it but to explain how to do it in the draft.
    - Dave Thaler - #3 requires mixing instance values with class values which means there will be many more EAT tokens generated than would otherwise be required. *[Dave: I don’t recall saying this, have to check the recording as either it wasn’t me or wasn’t my point or I have a bad memory now :]*
    - Henk Birkholz - Is this really only informational - how do we proceed toward consensus? For example what about hash of a public key as a keyid?
        - Dave T. - Row 1 is an example of hash of a key. #2 tells you where to get the key, which #1 doesn’t tell you where to get the key.
        - Henk - How to enable interoperability then?
        - Laurence - No silver bullet - it may take a while
- Endorsement - no formal definition?
    - A set of assumptions were presented
        - For simplicity including ‘reference values’ under Endorsements
    - Do we have an identifier for an endorsement in EAT
        - Add Endorsement ID (EID?) or URI/URL to EAT?
        - EAT origination claim would be replaced by Endorsement URL
        - Dave Thaler in chat pointed out that this definition isn’t consistent with the definition in the architecture draft
        - Endorsements may have information that wouldn’t expect to find in X.509 certificate (such as implicit claims).

- Comments:
  - Dave Thaler: Proposes a wording modification - All of the above are technically out of scope for the WG. Hence, can’t include normative language in a draft. Propose adding a ref value provider URL.
  - Dave: Implicit claims can be included in a certificate or an endorsement structure.
    - The case the previous table didn’t cover (but was in Michael’s diagram) was the endorser might differ from the reference value provider. If there is a URI available to find the appropriate entity makes sense.
  - Henk: The MUD draft (https://tools.ietf.org/html/draft-birkholz-rats-mud-00 (https://tools.ietf.org/html/draft-birkholz-rats-mud-00)) would be a good way to add pointers to things/entities. Endorsement ID is on the fringe because it mixes evidence with endorsement. Some assumptions don’t apply relative to the content in the architecture draft.
  - Giri: Need to finalize EAT draft to support implementers. See issue 65 https://github.com/ietf-rats-wg/eat/issues/65 (https://github.com/ietf-rats-wg/eat/issues/65)
    - Need approach to unsigned tokens - the UCCS draft didn’t make progress. What is the status for unsigned tokens?
      - Nancy (as individual): There were comments and intention to move it forward.
      - Henk: Need to allocate time to work on it.
  - Nancy (as chair): Restates RATS interest in moving the draft forward.

4. Network Device Attestation
   - Guy Fedorkow update to RIV draft
   - Last call ended Oct 12th (thanks to everyone who commented)
   - 700 lines comment material provided; most had to do with wording
   - One more change required
     - Endorser / Reference Value Provider definitions changed in architecture draft
       - Sections that pertain to reference values will change to RVP where Endorser is currently being used.
       - Many synonyms to ‘reference values’ that need to be updated to use the standardized terminology.
       - Nancy: Reach out to commenters once v05 has been released.
   - Next steps
     - Finish editing tasks
     - Anything else?

- Nancy: Once the updated draft is available then a request for finalization can be made.

5. Interaction Model
    - Henk presenting interaction model draft
    - Three models identified
        1. Challenge-Response:
        2. Time-based:
        3. Streamed:
    - Direct Anonymous Attestation (DAA) is described as a way to address privacy using group signing
    - Current status: Adopted as a WG draft
        - Recently updated
        - Better alignment to terminology in architecture draft
        - Referenced by 4 other drafts
    - Next Steps
        - Section 6. contains normative prerequsites for Attesters.
            - Ask: Is the scope of normative language appropriate?
                - Dave Thaler: Why is there normative language in a document that is informational?
                - Nancy: Asks who has read the document
                - Dave: Not the version that is 3 hrs old
                - Nancy: Looking for the update to go out on the reflector - looking forward to IETF 109
                - Henk: Looking for feedback on the list
        - Section 7. contains generic information elements
6. CHARRA Update
    - Eric Voit presenting
    - Recap
        - Many devices use YANG interfaces
        - This draft defines access to/from TPM 1.2 / 2.0 RPCs
        - IETF “YANG Doctors” review is complete / near complete
        - Reviewed relationship to other RATS drafts
        - Issues addressed
            1. Overall document added text to describe the purpose and context
            2. Added ietf-tcg-algs yang, and created error checks
            3. Added support for netequip_boot logs
            4. Refined models

    5. others…
  - Open Issues
    - Need help with XPATH expressions
    - YANG Doctor comments need to be addressed
    - Maximize commonality between TPM 1.2 and 2.0 RPCs - Can’t track down the original author of the 1.2 RPCs
    - Include tpm-name and node-id in RPCs?
      - Node-id is used to identify a line card when there are multiple line cards
  - More discussion on node-id
    - certificate-name is assumed unique on a multi-linecard attester
      - PRO: multiple line cards are disambiguated
        - Queries won’t change when using node-id
      - CON: redundancy in message contents
        - exposes linecard structures in routers
        - larger code and error conditions to check
      - Eric recommendation is option 1 (use certificate name not node-id)
      - Wei Pan: Node-id is also used in option 1, why is this still needed?
        - Eric: plan on removing node-id in future revisions
      - Wei: Both have pros/cons. Option 1 may be more readable, but option 2 may be better for machines to process - but not passionate one way of the other.
        - Option 1 could have more processing requirements when there is a lead Attester
        - Eric: Even if nod-id wasn’t used, they would still need to be processed and line card mfg’rs would need to assign names.
        - Nancy: Try to resolve the issue on the list.
  - Working last call anticipated after these issues are addressed
  - Henk: Are options mutually exclusive?
    - Eric: The question is how much redundancy needed? Reduancy will result in more errors.
- Next Steps:
  - Nancy: Any more comments?

Meeting adjourned 8:54 PDT