Attestation Event Stream Subscription
draft-birkholz-rats-network-device-subscription-00

Henk Birkholz henk.birkholz@sit.fraunhofer.de
Eric Voit evoit@cisco.com
Wei Pan william.panwei@huawei.com

IETF 108, July 28th & 29th 2020, RATS WG
Purpose & Origin

• Defines how to subscribe to a stream of attestation related Evidence on TPM-based network devices.
  • When subscribed, a Telemetry stream of verifiably fresh YANG notifications are pushed to the subscriber.
  • Notifications are generated when TPM PCRs are extended

• This draft integrates:
  • Section 5 of draft-voit-rats-trusted-path-routing-01
  • draft-xia-rats-pubsub-model
Relationship to other RATS drafts

**RATS Language**
- draft-ietf-rats-architecture
  - Terminology
  - Topological models
  - Timing definitions

**draft-birkholz-rats-reference-interaction-model**
- Interaction models

**Routers / Switches**

**Profile**
- draft-ietf-rats-tpm-based-network-device-attest
  - Use case
  - Operational prerequisites
  - Call flow
  - Evidence evaluation

**Interface Specification**

**Enables WG discussion via shared context**

**draft-ietf-rats-yang-tpm-charra**
- YANG definitions & RPCs for Attester

**Attestation Evidence via Telemetry**
- draft-birkholz-rats-network-device-subscription
  - Provably fresh events
  - RFC-8639 based YANG subscriptions

**Improved reaction speed (Optional)**

**draft-voit-rats-trustworthy-path-routing**
- Trustworthiness Vector
- Stamped Passport definition

**Peer Router Appraisal**

**Enables WG discussion via shared context**
TPM PCR Evidence as Telemetry

draft-ietf-rats-yang-tpm-charra
- Periodic polling
- Reboot loses info/state

draft-birkholz-rats-network-device-subscription
- Events & PCR changes streamed as they happen
- Subscription established right at Boot checks:
  - Hardware integrity
  - Unique identity
  - Boot integrity
  - Filesystem integrity
- Telemetry streaming after Boot checks:
  - New software installed
  - Suspect log message detected
  - Privilege level escalation
  - Etc...
Fresh Security Telemetry

```
<table>
<thead>
<tr>
<th>Attester</th>
<th>TPM</th>
<th>Log '-----'</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Relying Party</td>
</tr>
<tr>
<td>-----------</td>
<td>-----</td>
<td>-------------</td>
</tr>
</tbody>
</table>
```

\[
\begin{align*}
\text{time(VG)} & \quad \langle\text{establish-subscription(<attestation>)}\rangle \quad \text{time(NS)} \\
\text{time(EG)} & \quad \langle\text{filter(<tpm-extend>)\rangle} \quad \langle\text{<tpm12-attestation>} \quad \langle\text{<tpm20-attestation>}\rangle \\
& \quad \text{verify time(EG)} \quad \text{Evidence @ time(RG,RA)} \\
& \quad \sim \\
\text{time(VG',EG')} & \quad \langle\text{filter(<tpm-extend>)\rangle} \quad \langle\text{<tpm12-attestation>} \quad \langle\text{<tpm20-attestation>}\rangle \\
& \quad \text{verify time(EG') \quad Evidence @ time(RG',RA')} \\
\end{align*}
\]
<attestation> Event Stream

- Fresh, streaming Evidence
  - Based on draft-ietf-rats-yang-tpm-charra & YANG subscriptions (RFC-8639)

- YANG Notifications
  - <tpm12-attestation>
  - <tpm20-attestation>
  - <tpm-extend>
    - Objects defined in draft-ietf-rats-yang-tpm-charra
    - Measurements which have extended a PCR

- <replay> of all Notifications since boot

- Verifier can subscribe to PCRs / Notifications of interest via XPATH

- Extensible with other Notifications
### ietf-tpm-remote-attestation-stream.yang

<table>
<thead>
<tr>
<th>Charra</th>
<th>This draft</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>+--rw rats-support-structures</td>
</tr>
<tr>
<td>+--rw rats-support-structures</td>
<td></td>
</tr>
<tr>
<td>+--rw supported-algos*</td>
<td></td>
</tr>
<tr>
<td>+--rw tpms* [tpm-name]</td>
<td></td>
</tr>
<tr>
<td>+--rw tpm-name</td>
<td></td>
</tr>
<tr>
<td></td>
<td>+--rw leafref-to-keystore?</td>
</tr>
<tr>
<td></td>
<td>+--rw (subscribable)?</td>
</tr>
<tr>
<td></td>
<td>+--:(tpm12-stream) {tpm:TPM12}?</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>+--:(tpm20-stream) {tpm:TPM20}?</td>
</tr>
<tr>
<td></td>
<td>+--rw tras:tpm20-pcr-index*</td>
</tr>
<tr>
<td>+--rw marshalling-period?</td>
<td></td>
</tr>
<tr>
<td>+--rw tpm12-subscribed-signature-scheme?</td>
<td></td>
</tr>
<tr>
<td>+--rw tpm20-subscribed-signature-scheme?</td>
<td></td>
</tr>
<tr>
<td>+--rw tpm20-subscription-heartbeat?</td>
<td></td>
</tr>
</tbody>
</table>

- **Attestation Key to be used**
- **PCRs allowed to be subscribed**
- **Maximum delay to bundle evidence**
- **Algorithm for signed results**
- **Keepalive PCR state**
Next

- Interest?
- Your suggestions to the mailing list.
- Potential for adoption call @ IETF 109?