A YANG Data Model for Challenge-Response-based Remote Attestation Procedures using TPMs

draft-ietf-rats-yang-tpm-charra-18

IETF 113, March 2022, RATS WG

H. Birkholz
M. Eckel
Fraunhofer SIT

S. Bhandari
ThoughtSpot

E. Voit
B. Sulzen
Cisco

L. Xia
Huawei

T. Laffey
HPE

G. Fedorkow
Juniper
Relationship between drafts

Full WG

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

- **draft-ietf-rats-reference-interaction-models**
  - Terms
  - Types of informational flows

- **draft-ietf-rats-ar4si**
  - Trustworthiness Claims
  - Algorithm which enables Verifier to trust AR delivered via the Attester

Routers / Switches

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

- **draft-ietf-rats-yang-tpm-charra**
  - YANG definitions & RPCs
  - TCG Algorithm registry

- **draft-ietf-rats-network-device-subscription**
  - Provably fresh events
  - RFC-8639 based YANG subscriptions

- **draft-voit-rats-trustworthy-path-routing**
  - Specific objects and encodings for algorithm
  - YANG model for provisioning
Status
One last IESG “Yes” or “No Objection” to pass

- Tweaks made during ongoing IESG review
  - Appendix describing IMA, as Linux Kernel could not be referred to as Normative.
  - YANG model references included
  - XPATH syntax tweaks suggested by requested XPATH experts. Proposal included in new v18.
- No scope / functionality changes
- Nothing seen at this time expected to block Ballot closure and document acceptance
Attestation Event Stream Subscription

draft-ietf-rats-network-device-subscription-01

IETF 113, March 2022, RATS WG
Purpose & Scope

• 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 for the Evidence going into TPM PCRs, and when the PCRs are extended.

• Result
  • Verifier is pushed new verifiably fresh Evidence whenever PCRs change.
Status

- Stable as a direct combination of RFC-8639 & Charra
- Socialize Security Considerations section text (to be written)
- Then request WGLC
Attestation Results for Secure Interactions

draft-ietf-rats-ar4si-02

IETF 113, March 2022, RATS WG

Eric Voit  
Cisco  
evoit@cisco.com

Henk Birkholz  
Fraunhofer SIT  
henk.birkholz@sit.fraunhofer.de

Thomas Hardjono  
MIT  
hardjono@mit.edu

Thomas Fossati  
Arm Limited  
Thomas.Fossati@arm.com

Vincent Scarlata  
Intel  
vincent.r.scarlata@intel.com
Contents

• **Part 1**: Information Element definitions for Attestation Results (AR) generated by Verifier to support Secure Interactions between Attester and Relying Party

• **Part 2**: End-to-end implementation options: (a) Background check, (b) AR Augmented Evidence

• Implementations:
  • [Trusted Path Routing](#) (Proprietary – Cisco)
  • [Veraison](#) (Open Source, aspiration = Confidential Compute Consortium adoption)
Changes since IETF112

- WG Adoption
- Text clarifications on values of specific Trustworthiness Claims
- Mailing list comparison with EAT ‘security-level’
- Mailing list comparison with EAT ‘swresults’
- Continued alignment of instance draft:

Awaiting meaningful market uptake before requesting WG adoption
Trustworthiness Claim Delivery
Based on draft-ietf-rats-architecture: Passport Model

Slide from IETF 111, new Yellow Highlighting
## Section 2.3.1: AR Design Principles for Trustworthiness Claims

<table>
<thead>
<tr>
<th>Design Principle</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>(1) Expose a small number of Trustworthiness Claims</td>
<td>A plethora of similar Trustworthiness Claims will result in divergent choices made on which to support between different Verifiers. This would place a lot of complexity in the Relying Party as it would be up to the Relying Party (and its policy language) to enable normalization across rich but incompatible Verifier object definitions.</td>
</tr>
<tr>
<td>(2) Each Trustworthiness Claim enumerates only the specific states that could viably result in a different outcome after the Policy for Attestation Results has been applied</td>
<td>By explicitly disallowing the standardization of enumerated states which cannot easily be connected to a use case, we avoid forcing implementers from making incompatible guesses on what these states might mean.</td>
</tr>
<tr>
<td>(3) Verifier and RP developers need explicit definitions of each state</td>
<td>Without such guidance, the Verifier will append plenty of raw supporting info. This relieves the Verifier of making the hard decisions. Of course, this raw info will be mostly non-interpretable and therefore non-actionable by the Relying Party.</td>
</tr>
<tr>
<td>(4) Support standards and non-standard extensibility</td>
<td>Standard types of Verifier generated Trustworthiness Claims should be vetted by the full RATS working group, rather than being maintained in a repository which doesn't follow the RFC process. This will keep a tight lid on extensions which must be considered by the Relying Party's policy language. Because this process takes time, non-standard extensions will be needed for implementation speed and flexibility</td>
</tr>
</tbody>
</table>
## Comparing Trustworthiness Claims & swresults (undergoing tweaks in EAT)

<table>
<thead>
<tr>
<th>Attestation target</th>
<th>'executables'</th>
<th>'file-system'</th>
<th>'swresults'</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>All runtime software/object loaded into Attester memory</td>
<td>A Verifier specified set of directories within the Attester file system</td>
<td>A Verifier specified set of software and/or multiple sets of software modules</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Encodable states</th>
<th>Seven</th>
<th>Five</th>
<th>Six. Might need to encode more than one (e.g., Firmware &amp; Kernel)</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Vendor extensible</th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Claim consistency</th>
<th>Common claim generalizations across Verifier generated AR: (Affirming, Warning, Contraindicated, None)</th>
<th>No generalized claim abstractions across generated AR claims</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>RP claim interpretation</th>
<th>Claim always references the full attestation target</th>
<th>Claim references either attestation target or submodule(s). An RP parser must understand context within structured message.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Only encodes information likely to be actioned by RP</th>
<th>Can encode both actionable information as well as supplementary information for debug logs</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Encodings/serialization</th>
<th>Transport independent, example serialization in draft-voit-rats-trustworthy-path-routing</th>
<th>JSON, CBOR, could add more</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Information Model</th>
<th>English prose</th>
<th>English prose &amp; CDDL</th>
</tr>
</thead>
</table>