TPM-based Network Device Remote Integrity Verification
draft-ietf-rats-tpm-based-network-device-attest-01

IETF 108 RATS
28 Aug 2020

Guy Fedorkow - gfedorkow@juniper.net
Eric Voit - evoit@cisco.com
Jessica Fitzgerald-McKay - jmfitz2@nsa.gov

V1c
Objective

• Standardize operational model for today’s existing but proprietary TPM-based router/switch Remote Attestation solutions.
  • Enables switches/routers to be appraised by non-proprietary controllers/Verifiers.
  • Gives Network Operators needed stability for interfacing operational systems.
Nonce based Background Check Model

1. **Log Evidence hashed into TPM PCR**
   - Time(VG)
   - ValueGeneration(targetEnvironment)
     - => claims

2. **Attestation request received**
   - RequestEvidence(nonce, PcrSelection)
     - Time(NS)
     - Nonce generated

3. **TPM Quote Evidence is generated**
   - EvidenceGeneration(nonce, PcrSelection, collectedClaims)
     - => SignedPcrEvidence(nonce, PcrSelection)
     - => LogEvidence(collectedClaims)

4. **Evidence Returned**
   - ReturnsignedPcrEvidence
   - ReturnLogEvidence

5. **Evidence Appraisal**
   - EvidenceAppraisal(SignedPcrEvidence, eventLog, refClaims)
   - AttestationResult <= |

6. **Attestation Results generated**
   - Time(RG,RA)

7. **Attestation Results appraised**
   - AttestationResults appraised

8. **Attestation Results no longer fresh**
   - Time(RX)
   - AttestationResults no longer fresh

From: draft-birkholz-rats-reference-interaction-model
What Evidence does RIV Appraise?

Section 2.1.1 outlines what we expect to attest with RIV, including:

• Code
  • Firmware, OS loader, OS kernel and applications

• Credentials
  • Keys used to authorize operation of routers, e.g. code-signing public keys or network-access private keys (e.g. VPN keys)

• Configuration
  • Security-sensitive configuration files

RIV is intended to secure the infrastructure, so that subsequent higher-level claims can be trusted.
About TPM PCRs

• TPM Platform Configuration Registers (PCRs) are used to record hashes of attested objects.

• PCR values may be attestable on their own, but often must be used to validate a log of individual objects measured.

• Baseline allocation of events to logs is specified for UEFI BIOS in TCG PC Client Platform Firmware Profile Specification.

• But expect vendor variation, especially non-UEFI platforms.
PCR Allocation for UEFI

- **Start Firmware**
  - Initialize hardware
  - Check Loader Signature

- **Run Loader**
  - Locate OS Image
  - Check Kernel Signatures

- **Kernel**
  - Start OS
  - Check OS Executable Hashes (IMA)

- **Firmware checks**
  - Loader Signature before handoff

- **Loader checks**
  - Kernel Signatures before handoff

Core Root of Trust

- PCR[0] – PCR[7]
- PCR[8], PCR[9]
- PCR[10], PCR[11]

- See *TCG PC Client Platform Firmware Profile Specification* for details
## Section 2.1.1 in Draft -02

<table>
<thead>
<tr>
<th>Function</th>
<th>Allocated PCR #</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firmware Static Root of Trust, i.e., initial boot firmware and drivers</td>
<td>0</td>
</tr>
<tr>
<td>Drivers and initialization for optional or add-in devices</td>
<td>2</td>
</tr>
<tr>
<td>OS Loader code and configuration, ...</td>
<td>4</td>
</tr>
<tr>
<td>Vendor Specific Measurements during boot</td>
<td>6</td>
</tr>
<tr>
<td>Secure Boot Policy. This PCR records keys and configuration used to validate the OS loader</td>
<td>7</td>
</tr>
<tr>
<td>Measurements made by the OS Loader (e.g. GRUB2 for Linux)</td>
<td>8</td>
</tr>
<tr>
<td>Measurements made by OS (e.g. Linux IMA)</td>
<td>10</td>
</tr>
</tbody>
</table>
Relationship to other WG drafts

**Language**

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

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

Enables WG discussion via shared context

**Profile**

- draft-ietf-rats-tpm-based-network-device-attest
  - Use case
  - Prerequisites/simplifying assumptions which enable operation
    - TPM1.2/TPM2.0/equivalent needs
    - Pre-established Key Types
    - Pre-configured endorsements
  - RIV call flow
  - Evidence evaluation
    - PCR allocations for network devices
    - Relevance/viability of KGVs for a subset of PCRs
    - Appraisal Policy for Evidence
    - Attester log type formats supportable

**Interface Specification**

- draft-ietf-rats-tpm-based-network-device-attest
  - Defines operational pre-requisites for
    - draft-ietf-rats-yang-tpm-charra
      - YANG definitions & RPCs for Attester
    - draft-birkholz-rats-network-device-subscription
      - Provably fresh events
      - Subscribed YANG notifications
    - draft-birkholz-rats-trustworthy-path-routing
      - Trustworthiness Vector
      - Stamped Passport definition
  - Peer Router Appraisal

 Juniper Business Use Only
Next Steps

- Another round of Nomenclature Alignment is needed with Arch. doc
  - Some xrefs in RIV need an update.
    - E.g., Specifications for Reference Integrity Measurements have recently been published at https://trustedcomputinggroup.org/wp-content/uploads/TCG_RIM_Model_v1-r13_2feb20.pdf

- But no substantial new content planned

**REVIEW PLEASE!**