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

```
.------------.
|  Attester  |
|     .-----.|
|     | TPM ||                              .--------------------------.
| Log '-----'|                              | Relying Party | Verifier |
'------------'                              '--------------------------'
    time(VG)                                                       |
valueGeneration(targetEnvironment)                                 |
     | => claims                                                   |
     |                                                             |
     | <--------------requestEvidence(nonce, PcrSelection)-----time(NS)
     |                                                             |
   time(EG)                                                        |
evidenceGeneration(nonce, PcrSelection, collectedClaims)           |
     | => SignedPcrEvidence(nonce, PcrSelection)                   |
     | => LogEvidence(collectedClaims)                             |
     |                                                             |
     | returnSignedPcrEvidence-----------------------------------> |
     | returnLogEvidence-----------------------------------------> |
     |                                                             |
     |                                                        time(RG,RA)
     |         evidenceAppraisal(SignedPcrEvidence, eventLog, refClaims)
     |                                        attestationResult <= |
     ~                                                             ~
     |                                                           time(RX)
```

Log Evidence hashed into TPM PCR

Attestation request received

Nonce generated

TPM Quote Evidence is generated

Log Evidence collected

Evidence Returned

Attestation Results generated

Attestation Results appraised

Attestation Results 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:

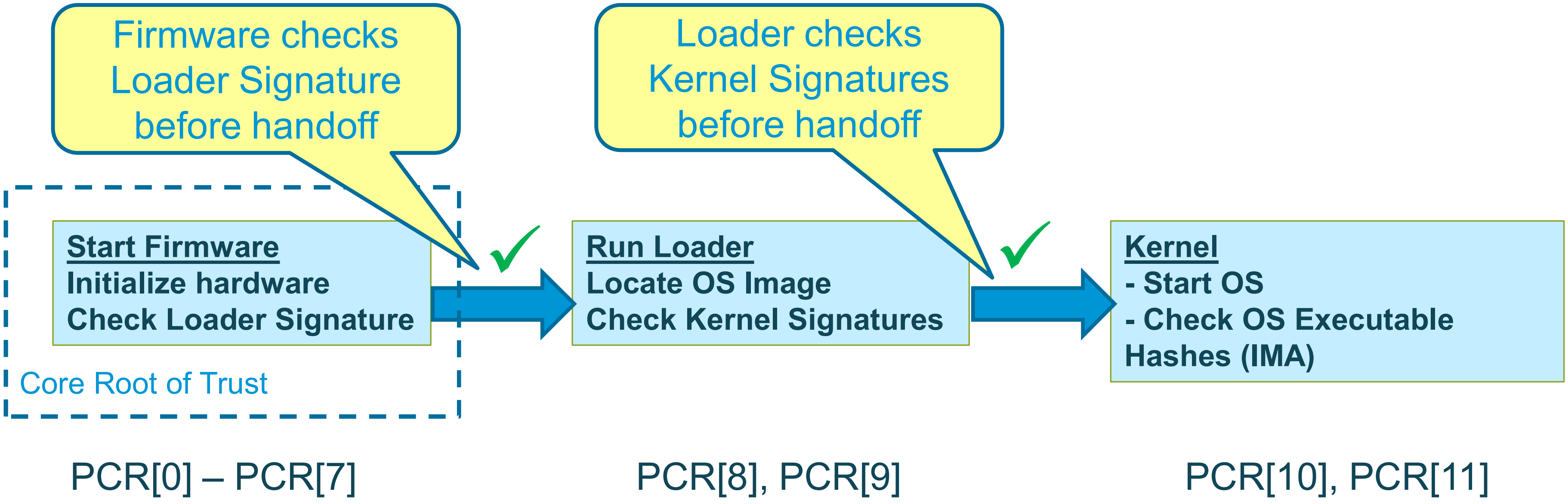
- Code
  - Firmware, OS loader, OS kernel and applications
- Credentials
  - Keys used to authorize operation of routers, e.g. code-signing public keys or network-access private keys (e.g. VPN keys)
- Configuration
  - Security-sensitive configuration files

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



Firmware checks Loader Signature before handoff

Loader checks Kernel Signatures before handoff

Start Firmware
Initialize hardware
Check Loader Signature

Core Root of Trust

✓

Run Loader
Locate OS Image
Check Kernel Signatures

✓

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

PCR[0] – PCR[7]

PCR[8], PCR[9]

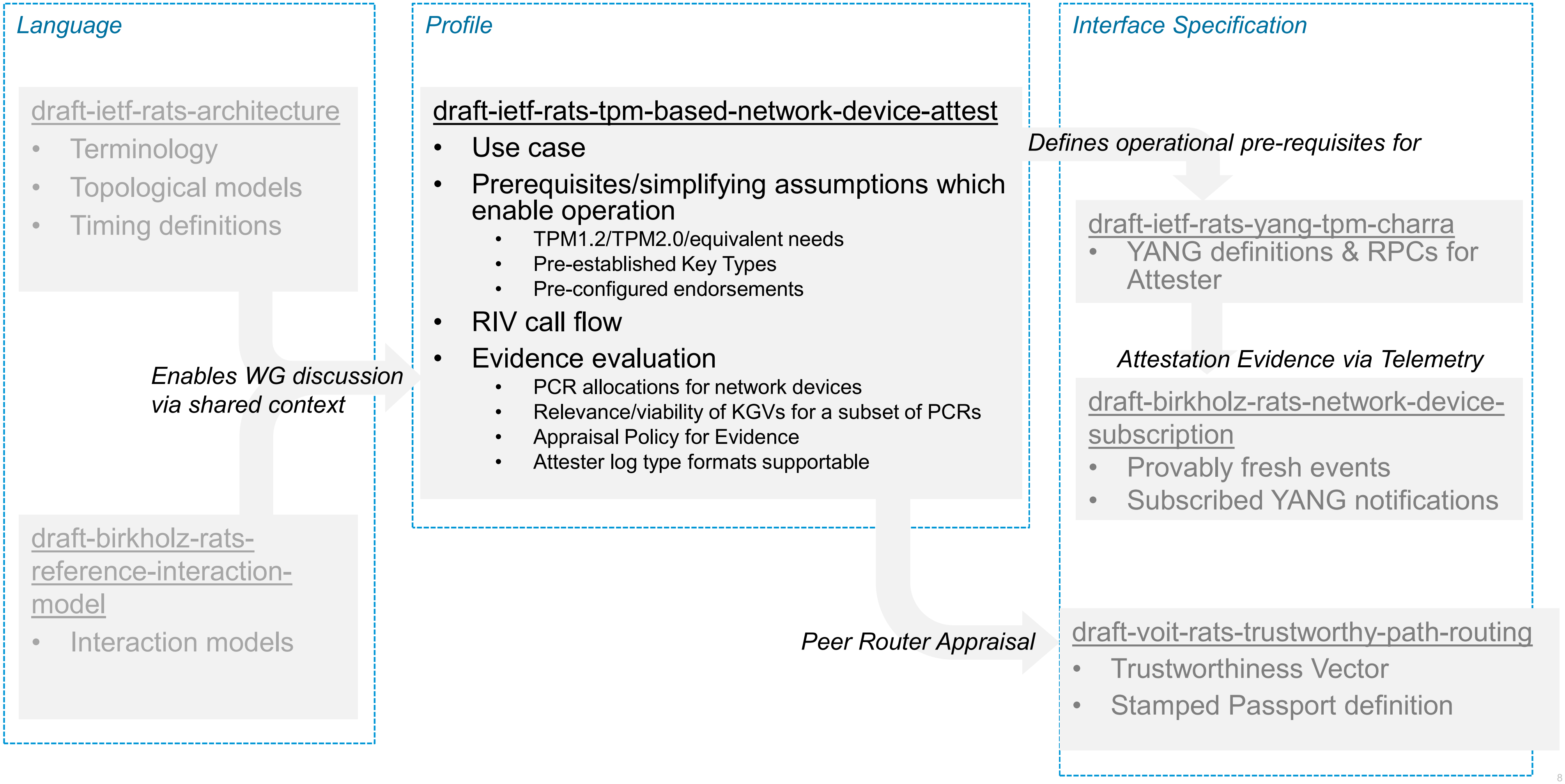
PCR[10], PCR[11]

- See *TCG PC Client Platform Firmware Profile Specification* for details

Section 2.1.1 in Draft -02

	Allocated PCR #	
Function	Code	Configuration
Firmware Static Root of Trust, i.e., initial boot firmware and drivers	0	1
Drivers and initialization for optional or add-in devices	2	3
OS Loader code and configuration, ...	4	5
Vendor Specific Measurements during boot	6	6
Secure Boot Policy. This PCR records keys and configuration used to validate the OS loader		7
Measurements made by the OS Loader (e.g GRUB2 for Linux)	8	9
Measurements made by OS (e.g. Linux IMA)	10	10

Relationship to other WG drafts



Language

draft-ietf-rats-architecture

- Terminology
- Topological models
- Timing definitions

Enables WG discussion via shared context

draft-birkholz-rats-reference-interaction-model

- Interaction models

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

Defines operational pre-requisites for

Peer Router Appraisal

Interface Specification

draft-ietf-rats-yang-tpm-charra

- YANG definitions & RPCs for Attester

Attestation Evidence via Telemetry

draft-birkholz-rats-network-device-subscription

- Provably fresh events
- Subscribed YANG notifications

draft-voit-rats-trustworthy-path-routing

- Trustworthiness Vector
- Stamped Passport definition

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!