TPM-based Network Device Remote Integrity Verification

draft-fedorkow-rats-network-device-attestation-05

RATS Virtual
28 April 2020

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

Log Evidence hashed into TPM PCR
Attestation request received
Log Evidence collected
TPM Quote Evidence is generated
Evidence Returned

Log Evidence

Attestation request received
<-- requestAttestation(nonce, PcrSelection) ------- time(ns)
Nonce generated

time(vg)

LogEvidence
SignedPcrEvidence(PCRs, nonce)

logEvidence, SignedPcrEvidence

verifyAttestationEvidence time(rg, ra)

~

time(rx)

Attestation Results generated
Attestation Results appraised

Attestation Results no longer fresh

Attestation Results generated
Attestation Results appraised

Attestation Results no longer fresh
New in Draft -05

• Focus on Operational Prerequisites for the RIV Use Case
• Alignment with RATS-Arch, addition of timing points
• Removal of some TCG-centric material to Appendices
• Addition of “What Evidence does RIV Appraise?”
• Addition of Peer-to-Peer to coordinate with draft-voit-rats-trusted-path-routing
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.
Relationship to other WG drafts

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

Enables WG discussion via shared context

**Profile**
- draft-fedorkow-rats-network-device-attestation
  - 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

Future
- Potential improvements
  - draft-xia-rats-pubsub-model
    - Business context
    - Subscription call flow

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

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

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

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

Definitions operational pre-requisites for

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

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

- draft-ietf-rats-architecture
  - Terminology
  - Topological models
  - Timing definitions
Assuming WG agrees such documentation is needed:

- Where should the WG document current TPM-based router/switch Remote Attestation operational prerequisites?

Option 1
Separate use case context + profile draft

Pro
- Simplifies reading for different types of document users

Con
- Precedent of two WG documents per use case?

Preferred
- If WG agrees, recommend adopting this draft

Option 2
Integrate into draft-ietf-rats-yang-tpm-charra

Pro
- Fewer adopted WG drafts

Con
- Very large merged document
- Elements of the YANG model may be obsoleted based on potential improvements
- Less modularity

Viable
- If WG selects, recommend merging drafts