RATS Agenda - Monday, July 26th – Session II

Room 8, RATS Session 1
Time zone: PDT (UTC-7)

14:30 : 14:35 Agenda Bash & Logistics
(5 min) Nancy Cam-Winget, Kathleen Moriarty, Ned Smith

14:35 : 14:40 RATS Architecture and next steps
(5 min) Michael Richardson
(draft-ietf-rats-architecture-12)

14:40 : 14:50 EAT
(10 min) Laurence Lundblade
(draft-ietf-rats-eat-10)

14:50 : 15:00 CHARRA and RIV
(10 min) Henk Birkholz, Guy Fedorkow
(draft-ietf-rats-yang-tpm-charra-08, draft-ietf-rats-tpm-based-network-device-attest-07)

15:00 : 15:10 Reference Interaction Models and DAA
(10 min) Henk Birkholz
(draft-ietf-rats-reference-interaction-models-03, draft-birkholz-rats-daa-01)

15:10 : 15:25 Concise Reference Integrity Manifest
(15 min) Henk Birkholz
(draft-birkholz-rats-corim-00)

15:25 : 15:30 Attestation Sets
(5 min) Kathleen Moriarty
(draft-moriarty-attestationsets)
RATS Architecture and next steps

- Michael Richardson
EAT Update

- Laurence Lundblade
EAT Update:

• Draft Status
• Semi-permanent UEID and IDevID
• Attestation Results

Laurence Lundblade

IETF 111 July 2021
Planned Contents of an EAT - The Claims

- **HW Identification**
  - OEM, model, version...
  - Unique device identification

- **SW Identification - CoSWID**
  - Author, package, version...
  - Measurement

- **Security Characterization**
  - High-level OS, TEE, secure element, TPM...

- **Running State**
  - Boot and debug state

- **Measurement of Running SW**
  - Runtime integrity check

- **Nonce and Timestamps**
  - Freshness, prevent replay

- **Identify Verifier Input**
  - Endorsements, key ID, reference values...

- **Context, Purpose, Profile**
  - Intended use cases, profile claim

- **GPS Location**

- **Submodules**
  - HW subsystems, TEE, SW process and apps...

- **Nested EATs**
  - One signed EAT inside another

- **Public Keys**
  - Attestation of private keys on the device (e.g., Android key store)

- **Formal Device Certifications**
  - For example, Common Criteria certification; format is GP’s DLOA

- **SW Measurement Results**
  - Results of comparison of SW measurements to reference values
Level of Completion in EAT Draft

- **HW Identification**
  - OEM, model, version...
  - Unique device identification

- **SW Identification - CoSWID**
  - Author, package, version...
  - Measurement

- **Security Characterization**
  - High-level OS, TEE, secure element, TPM...

- **Running State**
  - Boot and debug state

- **Measurement of Running SW**
  - Runtime integrity check

- **Nonce and Timestamps**
  - Freshness, prevent replay

- **Identify Verifier Input**
  - Endorsements, key ID, reference values...

- **Context, Purpose, Profile**
  - Intended use cases, profile claim

- **GPS Location**

- **Submodules**
  - HW subsystems, TEE, SW process and apps...

- **Nested EATs**
  - One signed EAT inside another

- **Formal Device Certifications**
  - For example, Common Criteria certification; format is GP’s DLOA

- **Public Keys**
  - Attestation of private keys on the device (e.g., Android key store)

- **SW Results**
  - Results of comparison of SW measurements to reference values

Progress & change since IETF 110. Draft -10
• Ready for last call, no open issues
• Near completion, reviewed
• Draft text
• Proposed, Interest in

In Github, but not draft
EAT work needed beyond claims

• Rework introduction and related with respect to RATS Architecture
  ◦ Use Architecture terminology: “Attester”, “Verifier”...
  ◦ Remove most of the architecture-related text currently in EAT

• More examples

• Should a verification procedure be included?
Changes since IETF 110

- Added SUEID – Semi-permanent UEID
- Add appendix comparing IDevID to EAT
- Added section on use for Evidence and Attestation Results
- Fill in the key ID and endorsements identification section
- Remove origination claim as it is replaced by key IDs and endorsements
- Added manifests and software evidence claims (CoSWID, SUIT manifests)
- Add string labels and non-claim labels for use with JSON (e.g. label or members of location claim)
- EAN-13 HW versions are no longer a separate claim. Now they are folded in as a CoSWID version scheme.
- Lots of GitHub issues closed
CHARRA and RIV

- Henk Birkholz
- Guy Fedorkow
RATS YANG Module for Challenge-Response-based Remote Attestation Procedures using TPMs

Henk Birkholz <henk.birkholz@sit.fraunhofer.de>,
Michael Eckel <michael.eckel@sit.fraunhofer.de>,
Shwetha Bhandari <shwethab@cisco.com>,
Bill Sulzen <bsulzen@cisco.com>,
Eric Voit <evoit@cisco.com>,
Liang Xia (Frank) <frank.xialiang@huawei.com>,
Tom Laffey <tom.laffey@hpe.com>,
Guy C. Fedorkow <gfedorkow@juniper.com>,

IETF 111, notinsanfrancisco, July 26th 2021, RATS WG
Document Status

• I-D depends on the RATS Architecture and RIV to clear
  • Made the reference to the RATS Interaction Models informative
• xml2rfc outdenting issue
  • Editorial issue that is probably not a blocker, tried working around that via kramdown-rfc2629 hotfixes in v1.5.5 with mixed success
• YANG Doctors comments seem to be all addressed, waiting for further feedback
• Next steps?
TPM-based Network Device Remote Integrity Verification
draft-ietf-rats-tpm-based-network-device-attest-07

IETF 111 RATS
26 Jul 2021

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

```
Attester
  | TPM |
  | Log '-----'
--------------------------
| Relying Party | Verifier |

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

time(VG) valueGeneration(targetEnvironment) => claims

\[
\text{time(NS)} \quad \text{requestEvidence(nonce, PcrSelection)}
\]

\[
\text{time(EG)} \quad \text{evidenceGeneration(nonce, PcrSelection, collectedClaims)}
\]

\[
\text{returnSignedPcrEvidence}
\]

\[
\text{returnLogEvidence}
\]

\[
\text{time(RG,RA)} \quad \text{evidenceAppraisal(SignedPcrEvidence, eventLog, refClaims)} \quad \text{attributionResult} \quad \text{time(RX)}
\]

Log Evidence hashed into TPM PCR

Attestation request received

TPM Quote Evidence is generated

Log Evidence collected

Evidence Returned

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.
Relationship to other WG drafts

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

**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**
- Defines operational pre-requisites for
  - 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
  - Peer Router Appraisal
    -draft-voit-rats-trustworthy-path-routing
      -Trustworthiness Vector
      -Stamped Passport definition

Enables WG discussion via shared context
Next Steps

- Forward RIV along with CHARRA for IESG review
Reference Interaction Models and DAA

- Henk Birkholz
RATS Reference Interaction Models for Challenge-Response/Time-Based/Streamed Remote Attestation

Henk Birkholz <henk.birkholz@sit.fraunhofer.de>,
Michael Eckel <michael.eckel@sit.fraunhofer.de>,
Wei Pan <william.panwei@huawei.com>,
Eric Voit <evoit@cisco.com>,

IETF 111, notinsanfrancisco, July 26th 2021, RATS WG
Document Status

• Effective final issue was:

• The proposal in the remaining PR #43 was vetted and is now considered to be out-of-scope. Some parts of it might move to a new document and some parts of it could move to existing I-Ds.

• Proposal for next step: request for WGLC
RATS  Direct Anonymous Attestation

Henk Birkholz <henk.birkholz@sit.fraunhofer.de>,
Christopher Newton <cn0016@surrey.ac.uk>,
Liqun Chen <liqun.chen@surrey.ac.uk>,

IETF 111, notinsanfrancisco, July 26th 2021, RATS WG
Document Status

- Around IETF 110, this I-D has been split out of:
- -00 received a good amount of pre-adoption reviews and comments:
  - Thanks to Hannes, Thomas, Wei, Laurence, Ned, and Guy!
- Recent feedback is primarily reflected in new Privacy & Security Considerations content:
- Dave Thaler joins the authors team. Welcome!
- Proposal for next step: Request for WG adoption call (WGAC)
Concise Reference Integrity Manifest

- Henk Birkholz
Describing Attesters to Verifiers: Concise Reference Integrity Manifests

https://datatracker.ietf.org/doc/draft-birkholz-rats-corim/

Ned Smith <ned.smith@intel.com>,
Yogesh Deshpande <yogesh.deshpande@arm.com>,
Henk Birkholz <henk.birkholz@sit.fraunhofer.de>,
Wei Pan <william.panwei@huawei.com>,
Thomas Fossati <thomas.fossati@arm.com>,

IETF 111, notinsanfrancisco, July 26th 2021, RATS WG
RATS Architecture, Conceptual Data Flow in [https://www.ietf.org/archive/id/draft-ietf-rats-architecture-12.html#figure-1](https://www.ietf.org/archive/id/draft-ietf-rats-architecture-12.html#figure-1)
Problem Statement

One or more authorized supply chain actors (OEM, ISVs, SiPs, etc.) need to come together and "describe" an Attester to a Verifier. So, when Evidence from that Attester is passed on to the Verifier, it can use the attributes that apply to the Attester to appraise Evidence against the Appraisal Policy.

Without a standard Information Model / Data Model there is no standard tooling to reduce fragmentation or lower barriers to entry for the supply chain actors.
Problem Context & Scope

The descriptive material that flows from the supply chain to the Verifier can be, for example:

- Measurements, for example, FW – "Reference Values"
- Verification key material, certification status – "Endorsements"

It is also necessary to describe the composition of an Attester from its relevant parts (i.e., its Attesting and Target Environments):

- This is not necessary for very simple attesters (AE:TE=1:1) but can come in handy for more complex topologies where the device structure is reflected in the Evidence structure (e.g., via submodules in EAT).
- Also, it can be useful for factoring out common parts that are reused across different Attesters.

*Out of scope – at least for the moment – is the delivery of Verification Policies to the Verifier by the Verifier Owner.*
RATS Architecture, Conceptual Data Flow in [https://www.ietf.org/archive/id/draft-ietf-rats-architecture-12.html#figure-1](https://www.ietf.org/archive/id/draft-ietf-rats-architecture-12.html#figure-1)
High-Level Design

- Graph Data models (RDF-like) with its own specialized vocabulary and data types

- The "triple" is the core pattern

- Used to define an Attester "ontology" (actually a simple directed property graph)

- Tracking triples provenance via explicit cryptographic methods

- Concise representations (CoMID, CoRIM)
  - Concise Module Identifier are the "hardware component" complement (including firmware) to CoSWID https://datatracker.ietf.org/doc/draft-ietf-sacm-coswid/, which are already used to represent software components.
  - Concise Reference Integrity Manifests are the trustworthy bundles of CoMID and CoSWID
What Kind of Triples Do We Need?

• Reference Values associated with a Target Environment
• Endorsements associated with an Attesting or a Target Environment
• Cryptographic identities associated with Attesting Environments
• Decomposition of a device in its constituent Attesting and Target Environments and their relational features
• Others that we haven’t yet anticipated (built-in extensibility)

• Examples (coming up in the next slides)
Reference Value Statements

Target Environment

“has reference values”

Reference Values

class-id=123abc...

Reference Value Statement

m0=0xfade0000...
m1=0xfade1111...
m2=0xfade2222...
m3=0xfade3333...
m4=0xfade4444...
m5=0xfade5555...
Endorsed Value Statements

Target Environment  "has endorsed values"  Endorsed Values

Endorsed Value Statement

class-id=123abc...
cert-id=0716053550040
Cryptographic Identity Statement

Attesting Environment  "has cryptographic identity"  Key Material

instance-id=xyz789...

key={
  -1:1,
  -2: 'bac5b11cad8f...',
  -3: '20138bf82dc1...',
  1:2,
  2: '11'
}
Next Step: Composition Patterns

• Attester (de)composition
  • i.e., relationships between Attesting and Target Environments within an Attester
Next Step: Composition Patterns (cont.)

• Device layering
  • i.e., how different Attesters come together in a composite device
Next Step: Composition Patterns (cont.)

It turns out that both can be expressed with the same statement:

\[
\text{Attesting Environment } \{\text{class-id}\} \text{ retrieves } \{\text{"claims"|"evidence"}\} \text{ by } \{\text{"active"|"passive"}\} \text{ collection over } \{\text{"trusted"|"untrusted"}\} \text{ path from Environment } \{\text{class-id}\}
\]

where the "object" Environment could be either a Target Environment or another Attesting Environment in a sub-Attester.

Note: There is also a separate statement to describe the environments that compose a certain Attester. (This is effectively just a grouping overlay on top of a device decomposition that can be fully described by the statement above.)
- BIOS retrieves claims by active collection over trusted path from Boot Loader
- Boot Loader retrieves evidence by active collection over trusted path from BIOS
- Boot Loader retrieves claims by active collection over trusted path from Kernel

Based on RATS Architecture, Layered Attester  
https://www.ietf.org/archive/id/draft-ietf-rats-architecture-12.html#figure-3
Next Step Example: Composition Statement

Attesting Environment

“retrieves claims by active collection over trusted path from”

Target Environment

data-type=claims
collection-type=active
path-type=trusted

class-id=123abc...
class-id=456def...

Composition Statement
CoMID & CoSWID Usage: Grouping Statements

• Similar to CoSWID, CoMID tags are the wrapper around a bunch of statements, but pertain to hardware and firmware.

• Like CoSWID tags, CoMID tags allow grouping, identification, typed linking (e.g., *supersedes*, *updates*) with other tags, plus some further encoding optimization in CoMID (e.g., if the statements subject is always the same it can be factored out).

• Grouping criteria are use-case specific. We can *suggest* a few (e.g., for handling FW updates), but we expect best practices to emerge with time and use.
CoRIM Usage:
Grouping Groups of Statements

• CoMIDs and CoSWIDs are grouped into CoRIMs
• CoRIMs are signed by the relevant supply chain actor
• Used as the end-to-end conveyance payload (we don’t define the transport)
• The outer signature augments the triples in the CoMID statements with provenance:
  • “Supply chain actor X says ${CoMID-statement} and/or ${CoSWID-statement}”
Navigating the sea of triples allows a Verifier to construct a comprehensive device/attester description that it can use as the backdrop against which its Appraisal Policy for Evidence is evaluated.
TL;DR

• Information Model Design Authority: TCG DICE WG
• work-in-progress
• Keep an eye on
  • https://github.com/ietf-rats/ietf-corim-cddl
  • https://github.com/ietf-rats/draft-birkholz-rats-corim
  • https://github.com/thomas-fossati/draft-psa-endorsements
This slide is intentionally left...

• ... almost blank
And a few more...

- Attester’s private key has certification path x5chain
- A and B are aliases for Attester
- Attester is a member of Group
- <insert your statement here, the format is extensible>
AE

Key

AE₀

"is instance of" "retrieves claims …"

"has crypto identity"

"has endorsed values"

TE

key=val

key=val

key=val

key=val

"has reference values"
Key

AE

AE₀

AE

TE

"has crypto identity"

"is instance of"

"retrieves claims ..."

"has endorsed values"

"has reference values"

key=val

key=val
Attestation Sets

- Kathleen Moriarty
Thank You!