Automation at Scale
Remote Attestation Sets

Kathleen M Moriarty
Center for Internet Security

March 2021
Scaling Posture Assessment

- Current posture assessment requires add-on tools to assess systems against expected policies and measurements.
- This requires distributed expertise to customize the current standards-based methods (e.g. OVAL/XCCDF, SWIMA/NEA)
- How can we improve posture assessment and make it accessible to businesses of all sizes?
Attestation Local and Remote

- Attestation is essentially signed evidence from a root of trust (RoT)
- Attestations are verified to ensure the signer is trusted
- Evidence in attestations are matched against expected policies or measurements
- If expectations are not met, remediation occurs
- Zero Trust requires verification, identification, encryption, and logs
- Attestation provides verification to the subsequent processes, applications, modules, etc. before execution is permitted
- Attestation aligned to policy sets and are typically performed on system
- Remote attestation is shared through a RESTful interface

Remote Attestation

Local attestation data generated from boot and runtime measurements and configuration for all managed systems, how to scale remote?
Scaling Measured Trust: Attestation Sets

Attestation Sets to specified policy & measurements per component (e.g. NIST, TCG, CIS Benchmarks, etc.), remediated and verified per set on system.

Remote Attestation at Scale:

- Image: NIST SP 800-193
- Controls and Benchmarks verified locally using known frameworks, controls, or benchmarks (e.g. NIST, CIS Benchmarks, TCG, DISA STIGS, etc.)
- App/Container Attested at selected assurance level
- Attested OS to selected assurance level
- TCG’s Reference Integrity Measurement Set
- e.g. Hardware attestation, components are as expected
- Attestation on set of locally verified attestations
- Mapping to Control Frameworks and Risk Alignment

GRC Management to Business Mission

ISO27001
NIST SP800-53
NIST Cyber Security Control Framework
Attestation Set Example

- (Identifier, Attestation Set Name, Integrity Protected Log of attestation evidence verification for set, timestamp, other useful claims) Signed by Trusted Platform Module or software RoT
- Format: Entity Attestation Token (JWT or CWT)
- Protocol: RESTful interface (e.g. RedFish, ROLIE, etc.)
Thank You

Comments welcome and appreciated!

URL: https://www.ietf.org/archive/id/draft-moriarty-attestationsets-00.txt
Status: https://datatracker.ietf.org/doc/draft-moriarty-attestationsets/
RATS Architecture Update

draft-ietf-rats-architecture-10

Henk Birkholz, Dave Thaler, Michael Richardson, Ned Smith, Wei Pan
Status

• Draft -07 had WGLC started after IETF 109, resulted in reviews from:
  • Addressed in -10: Eric Voit, Guy Fedorkow, Thomas Fossati, ...
  • After I-D deadline so not in -10: Kathleen Moriarty as document shepherd
• [https://github.com/ietf-rats-wg/architecture](https://github.com/ietf-rats-wg/architecture) is github repo for design team meetings and issue tracking
• Have had ~weekly design team meetings since IETF 109
• 71 github issues closed since last meeting!
  • (all but Kathleen’s new feedback)
Changes since IETF 109 (draft -07)

• Many editorial improvements
• Moved use cases before terminology section
• More exposition of Reference Values and providers
  • Except missed one spot in -10 (now PR #290)
    • Only hardware needs “Endorser”, but all layers may need Reference Values to appraise
• Expanded freshness section and details of handles approach
  • See next slide
Freshness: 3 styles of approach

• **Synchronized clocks:** typically require...
  • Local clocks (some IoT devices may not have)
  • Secure means of synchronizing them (e.g., ntpsec)
  • Some trusted time source to synchronize to
  • Additional Claims about time sync in Evidence

• **Nonces:** typically require...
  • Extra round trip to acquire the nonce
  • Per-nonce state kept on the nonce generator (Verifier or Relying Party)
  • Some mechanism (e.g., local clock) on nonce generator, to expire nonces
  • Some way to distinguish age of claim value from age of message, if needed

• **Handles:** typically require...
  • Secure means of distributing them (integrity, not spoofed or replayed)
  • Some trusted handle distributor to send them periodically
  • Some mechanism on appraiser to deal with loss of handle distributor availability
    • May still be susceptible to delay attacks
References

• Normative: no changes, all are RFCs
• Informative: added
  • Confidential Computing Consortium “Deep Dive” whitepaper
    • Which also references the RATS architecture doc
  • draft-birkholz-rats-uccs: A CBOR Tag for Unprotected CWT Claims Sets
  • draft-tschofenig-tls-cwt: Using CBOR Web Tokens (CWTs) in Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)
  • NIST “Strength of Function” glossary definition
  • TCG “DICE Certificate Profiles”
Next steps

• Address Kathleen’s comments (all look straightforward)
• Any other comments before submitting -11?
• What would the next step be then?
RATS Reference
Interaction Models for Challenge-Response/Time-Based/Streamed Remote Attestation

Henk Birkholz <henk.birkholz@sit.fraunhofer.de>,
Wei Pan <william.panwei@huawei.com>,
Eric Voit <evoit@cisco.com>,
Christopher Newton <cn0016@surrey.ac.uk>,
Liqun Chen <liqun.chen@surrey.ac.uk>,

IETF 110, notinprague, March 9th 2021, RATS WG
Document Status

• BCP 205 implementations for charra
  • https://github.com/Fraunhofer-SIT/charra
  • https://github.com/veraison/ietf-110-hackathon-demo

• Feedback & Issues
  • Implementation feedback looks good (Thanks, Thomas!)
    • No conceptual issues for a while now
    • Content proved to be useful during implementation
  • 20 issues still open on the github issue tracker

• Towards **WGLC**
  • After all issues are closed, a request for WGLC is planned
  • Reviews are welcome!
RATS Time-based Unidirectional Attestation

Andreas Fuchs <andreas.fuchs@sit.fraunhofer.de>,
Henk Birkholz <henk.birkholz@sit.fraunhofer.de>,
Ira McDonald <blueroofmusic@gmail.com>,
Carsten Bormann <cabo@tzi.org>,

IETF 110, notinprague, March 9th 2021, RATS WG
Document Status

• Content now aligned with maturing documents

• Drop TPM 1.2 or keep it?
  • Slight preference towards keeping it in, as that aligns with

• SNMP and/or YANG?
  • Slight preference towards both
  • Open for comments

• Request for **Working Group adoption**
  • Document is mature enough to move to the WG
  • Open question can be resolved via the WG process
RATS Attestation Result Claims for SUIT
(Software Updates for IoT)

Henk Birkholz <henk.birkholz@sit.fraunhofer.de>,
Brendan Moran <brendan.moran@arm.com>,

IETF 110, notinprague, March 9th 2021, RATS WG
Document Status

- Version -01 now includes
  - polished definitions & naming
  - fixed consistency nits
  - Reference to the SUIT Report concept
  - SUIT Reports become a separate I-D in the SUIT WG
- SUIT Claims have the same scope of semantics as Trustworthiness Vectors
- Upcoming I-D will extend scope to a Trustworthiness Vectors Information Model in RATS
  - And will combine the current Claims content with the Trustworthiness Claims from Trusted Path Routing
  - Information Model I-D in RATS used by
    - Trusted Path Routing in RATS
    - SUIT Report in SUIT
    - Etc.
UCCS

Henk Birkholz <henk.birkholz@sit.fraunhofer.de>,
Jeremy O'Donoghue <jodonogh@qti.qualcomm.com>,
Nancy Cam-Winget <ncamwing@cisco.com>,
Carsten Bormann <cabo@tzi.org>,

IETF 110, notinprague, 9 March 2021, RATS WG

- Use-cases and security limitations
- Review comments to date
- Appropriateness of RATS for this work
- Call for adoption
UCCS: Use-cases and known security limitations

- **Use-case**
  - A Secure Channel which authenticates both endpoints, and provides integrity protection. It may also provide confidentiality.
  - Wish to convey Attestation Evidence from Attester to Verifier over the Secure Channel
  - Attester and Verifier are trusted
  - Examples:
    - TEE using TLS
    - GlobalPlatform Secure Element SCP03 (AES-CBC+CMAC) / SCP11 (ECDSA+PKI)
  - Consider JWT [RFC8725] using algorithm ‘none’

- **Security Limitations**
  - Security properties of Attestation Evidence only guaranteed within the Secure Channel
  - Privacy preserving Secure Channels:
    - Do Claims break the privacy-preserving nature of the secure channel
    - Can Verifier use privacy preserving attestations meaningfully
  - Scope specific security review required per use-case.
Resolution of review comments

- **Russ Housley (RH):**
  - “MUST authenticate Verifier to attester”
  - “MUST protect integrity of communications […].”
    - Text rewritten to clarify the above
  - Integrity protection in both directions needed?
    - Noted only required (“SHOULD”) where confidentiality needed

- **Jessica Fitzgerald-McKay & Mike Jenkins (JF):**
  - “Static symmetric key […] can only authenticate a net, not an entity”
    - Not addressed
  - Suggest claims sets treated as ephemeral by recipient
  - “Transitioning back and forth between self-protected and channel protected CWT […]”
  - “Authentication happens at […] termination, not in the [using] application”.
    - All above addressed
Laurence Lundblade (LL)
  ○ “UCCS should have a very minimal discussion of security [...]”
    ■ Coverage of security is quite extensive

Jim Schaad (JS)
  ○ “Correspondences of secure channel security and equivalent COSE objects”
    ■ Addressed
Appropriate WG for UCCS

- Basic principle: "Where the experts are"
  - In scope for RATS because main use-cases driving the specification arise in RATS (Attestation)

- Other proposals
  - COSE
    - For: Jessica Fitzgerald-McKay
    - Against: Jim Schaad and Ira McDonald
  - ACE
    - As suggested by Jim and Ira
The authors believe that the use-case for UCCS is established
Based on mailing list feedback, RATS is the most appropriate WG
The authors request RATS adoption of the UCCS draft
A YANG Data Model for Challenge-Response-based Remote Attestation Procedures using TPMs
draft-ietf-rats-yang-tpm-charra-05

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

Mar 9th 2021, RATS WG
Purpose & Scope (recap)

• Context
  • A lot of network equipment devices use YANG-based management interfaces.
  • Adding Remote Attestation as procedures to existing and implemented management interfaces significantly reduces the threshold of adoption.

• Contribution
  • This YANG module defines RPCs and a concise datastore implementing the Challenge-Response Remote Attestation Interaction Model.

IETF YANG Doctor review, discussions underway
Relationship to other RATS drafts

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

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

**Profile**
**Defines operational pre-requisites for**
- draft-ietf-rats-yang-tpm-charra
  - YANG definitions & RPCs for Attester

**Interface Specification**
- draft-birkholz-rats-network-device-subscription
  - Provably fresh events
  - RFC-8639 based YANG subscriptions

**Improving reaction speed (Optional)**
- draft-voit-rats-trustworthy-path-routing
  - Trustworthiness Vector
  - Stamped Passport definition

**Enables WG discussion via shared context**
- draft-ietf-rats-reference-interaction-models
  - Interaction models

**Peer Router Appraisal**
- draft-ikef-rats-reference-interaction-models
- draft-ikef-rats-reference-interaction-models

**Attestation Evidence via Telemetry**
- draft-ikef-rats-reference-interaction-models

**Routers / Switches**

**Terminology**
- Topological models
- Timing definitions

**Topological models**
- draft-ikef-rats-reference-interaction-models
- draft-ikef-rats-reference-interaction-models

**Timing definitions**
- draft-ikef-rats-reference-interaction-models
- draft-ikef-rats-reference-interaction-models
Issues Addressed (v03 to v05)

• TPM1.2 Quote1 eliminated (using TPM1.2 Quote2 is sufficient)
• YANG model simplified so that info contained within the signed TPM quote isn't redundantly exposed in the YANG tree
• YANG Doctor comments covered
• Draft repartitioned so that documentation on specific YANG trees is included within their own specific sections
• Example RPCs defined
Open Issues

Within YANG model:

• XPATH expressions to which perform configuration data integrity validation to be closed with YANG Doctors during final review.

• RW on a config node
Next

• WGLC ?
Attestation Event Stream Subscription

draft-birkholz-rats-network-device-subscription

Henk Birkholz, Eric Voit, Wei Pan
Use Cases for RATS

draft-chen-rats-usecase-03

IETF110-2021-RATS

Meiling Chen /China Mobile
Li Su /China Mobile
Objective & Contents

• **Objective**
  - use case considerations from the ISP perspective

• **Contents**
  - Four use case for RATS
  - Two requirements for trusted link
Access authentication based on different method

Requirements:
1. When PSK Auth_Center and IBC Auth_Center cannot communicate directly, use RATS to make the results of one center recognized on another.

Figure 1: different access authentication methods within RATS

Is this scene belongs to RATS?
Application authentication based on different system

![Diagram showing two parties, each with a certificate-based and non-certificate-based authentication platform, exchanging attestation results.]

Requirements: attestation results, appraisal policy, the protocol to transmit the attestation results.

Figure 2: different application authentication methods in RATS architecture
Virtualization-based system

1. Virtualization systems use RATS based on vTPM, but workgroup drafts have no mention to it.

2. So will WG cover the scope of virtualization?
Requirements of trusted routing

Within an ISP

Device Conditions
(evidence) or
(Appraisal results)

Routing Device

Orchestrator

Form a routing path

Figure 3: a trusted link is formed within an ISP in RATS

Between ISPs

Trusted Path

Appraisal results

Trusted Path

<

cross-domain trusted link

Figure 4: a trusted link is formed between ISPs in RATS
New equipment into the network for the innate security of links

1. new router provides evidences to the verifier,
2. the orchestrator feed back the attestation result,
3. trustworthiness assessment, the orchestrator forms routing policies and issues them.
4. the trusted link formed.

Figure 5-2: a new router added to network
Device status updating

1. Collect routing information in real time or periodically:
   - Device information,
   - log information,
   - fault information
   - trusty measure vendors.

2. Forms a path link based on users’ trustworthiness requirements.

Figure 6: a new router added to network
ToDo

• Is there anyone interested in the draft? We can detail it together.
• Suggestions for the next step of my draft

• Comments and co-authors are welcome!