RATS Interaction Model for Challenge-Response-based Remote Attestation (CHARRA)

Henk Birkholz {henk.birkholz@sit.fraunhofer.de}
Michael Eckel {michael.eckel@sit.fraunhofer.de}

“IETF 107“, 2nd Virtual Session, April 28th 2020, RATS WG
RATS Interaction Models

• CHARRA (CHAllenge/Response Remote Attestation → this I-D)
  • In general, initiated „by the Verifier“ using a nonce
  • Two implementations:
    YANG Servers running on network equipment &
    BCP 205 implementation https://github.com/Fraunhofer-SIT/charra

• TUDA (Time-based Uni-Directional Attestation)
  • In general, initiated „by the Attester“ using sync-tokens and timestamps
  • BCP 205 implementation upcoming (based on CHARRA implementation)
  • https://datatracker.ietf.org/doc/draft-birkholz-rats-tuda/

• Subscription to Attestation Event Streams
  • In general, initiated „by the Verifier“ using a nonce, then
    maintained „by the Attester“ using sync-tokens and timestamps („hybrid“ CHARRA & TUDA)
  • https://datatracker.ietf.org/doc/draft-xia-rats-pubsub-model/
  • https://datatracker.ietf.org/doc/draft-voit-rats-trusted-path-routing/
Where Do Interaction Models Go?

• As architectural components, they are typically part of the architecture.
• They come with generic information models for internet protocols.
• They are typically used by multiple solutions I-D.

• Option 1: Standalone (for each model)
• Option 2: Standalone (as a bundle)
• Option 3: Merged into the architecture I-D
• Option 4: Merged into (to be) selected solution I-Ds (using that model)

• Other options, different option set?
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.de}

“IETF 107“, 2nd Virtual Session, April 28th 2020, RATS WG
Purpose & Scope

• Background
  • A lot of network equipment devices use YANG-based management interfaces.
  • A lot of corresponding agents already exist.

• Usage
  • **YANG is widely used and deployed, especially** on network equipment and virtual services.
  • Adding Remote Attestation as procedures to **existing and implemented management interfaces** significantly reduces the threshold of adoption.

• Contribution
  • This YANG module defines **RPCs** implementing the CHARRA (CHAllenge/Response Remote Attestation) Interaction Model.
  • This YANG module supports multiple **Roots-of-Trusts** (TPMs) in **composite devices**.
  • This YANG module enables **trustworthy evidence telemetry**.
Content & Application

• Potentially inherit more content about application from the RIV I-D.
• When the architecture semantics are stable, additional English text illustrating the top-level statements will be added – using the terminology specified in the architecture.
Muddy RATS

Henk Birkholz {henk.birkholz@sit.fraunhofer.de}

“IETF 107“, 2nd Virtual Session, April 28th 2020, RATS WG
Discovery of Remote Attestation Services, et al.

- Initial I-D (00) defines a RATS MUD File that can be referenced via IEEE 802.1AR DevIDs.
- The usage of MUD Files & URIs is defined in RFC 8520.
- The MUD File defined points to three sets of things (at least one option has to be included) and is provided by the Endorser that created the DevID (Secure Device Identifier):
  - **Endorsement Documents**: signed Claims Sets that provide assertions about the trustworthy characteristics of roots-of-trusts included in the device that presents the Secure Device Identifier
  - **Reference Integrity Measurements** – RIM: signed Claims Sets that provide reference measurements about Software Components included in the device that presents the Secure Device Identifier
  - **Remote Appraisal Services** – RAS: Verifier services that can appraise the evidence created by the device that presents the Secure Device Identifier
RATS Reference Integrity Measurements
Extension for CoSWID

Henk Birkholz {henk.birkholz@sit.fraunhofer.de}
Patrick Uiterwijk {puiterwijk@redhat.com}
Jessica Fitzgerald-McKay {jmfitz2@nsa.gov}
David Waltermire {david.waltermire@nist.gov}

“IETF 107“, 2nd Virtual Session, April 28th 2020, RATS WG
Concise Software Identity Tags (CoSWID) as RIMs

- CoSWID are a compact, well-defined, and cleaned-up variant of ISO/IEC 19770-2:2015 SWID Tags (Implementation: https://pages.nist.gov/swid-tools/)
  
  - Uses CBOR instead of XML
  - Document structure is defined via CDDL (RFC 8610)

- Currently, two options how to represent RIM via CoSWID are included in the I-D:
  
  - Host Integrity at Runtime and Start-up (HIRS)  
    https://github.com/nsacyber/HIRS/
    
    - Based on the TCG Reference Integrity Manifest Information Model  
  
  - RPM Version Scheme to be used via Linux Distributions

- A third option addressing the Layered Attestation concept recently included in the RATS Architecture I-D will be added in later versions, as well as a „bundle-mechanism“ to group individually signed RIMs.
RATS Endorsement EAT

Henk Birkholz {henk.birkholz@sit.fraunhofer.de}

“IETF 107“, 2nd Virtual Session, April 28th 2020, RATS WG
New Claims: Endorsement Claims

• Initial I-D (-00) kicks off the definition of endorsement Claims to be used in an Endorsement EAT flavor.

• Endorsement EAT are created by Endorsers (as defined in the RATS Architecture I-D).

• Included today are: Component Manufacturer, Component Version, Component Model, Field Upgradable, Shielded Secret Origination, Common Criteria
  - Derived and generalized from the TCG Platform Certificate Profile specification, e.g.:

• The intent of this Claim definitions is to provide assertions about the trustworthiness of various roots-of-trusts and some Attesting Environments, for which Evidence cannot be created by the Attester they are included in.
RATS uccs

Unprotected CWT Claims Sets
(“Unendorsed Tokens“)

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

“IETF 107“, 2nd Virtual Session, April 28th 2020, RATS WG
A Secure Channel „As Good As“ a Signature

- In some usage scenarios (some of which are currently specified by Global Platform) there exists a high level of assurance wrt the trustworthiness of a communication channel (called „Secure Channel“) between two RATS roles.
  - Prominent example: the communication channel that conveys Evidence from an Attester (or its Attesting Environment) to a Verifier
- As a CWT MUST be signed, but not using the CWT Registry would be very inconvenient, this I-D defines a CBOR tag for a CWT Claims Set as defined in RFC 8392.
  - This allows for the use of the CWT Registry and retaining the CWT map structure, while not using a COSE container.
- As a prerequisite, the I-D illustrates the requirements on the Secure Channel and the two peers that are establishing it, as well as derives the conditions, in which it is okay to omit the COSE container and directly use the CBOR tag.