Attestation Results for Secure Interactions

draft-voit-rats-attestation-results-01

IETF 111, July 29th 2021, RATS WG

Eric Voit
Cisco
evoit@cisco.com

Henk Birkholz
Fraunhofer SIT
henk.birkholz@sit.fraunhofer.de

Thomas Hardjono
MIT
hardjono@mit.edu

Thomas Fossati
Arm Limited
Thomas.Fossati@arm.com

Vincent Scarlata
Intel
vincent.r.scarlata@intel.com

Summary

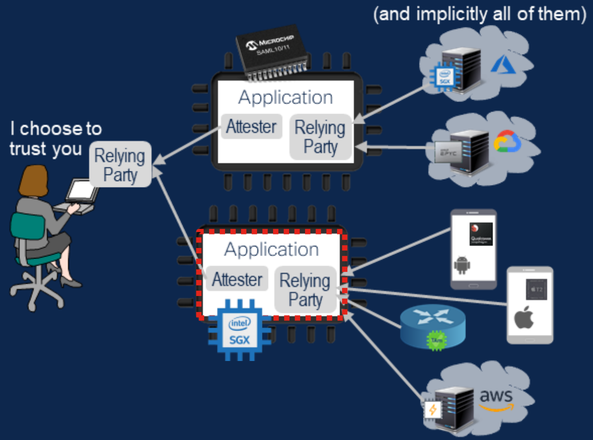
- Contents
  - Object definitions for Attestation Results (AR) to support Secure Interactions between Attester and Relying Party
  - How the Attester can augment AR to improve scale and speed of appraisal
  - State Machine for the Appraisal Policy for Attestation Results
- Two implementations
  - Trusted Path Routing (Proprietary – Cisco)
  - Veraison (Open Source – Confidential Compute Consortium)
- Ask: WG Adoption

Remote Attestation in a Heterogenous World

- Many types of Attesting Environments (AE)
- What may be trusted by Relying Party

Identity	Hardware type, software build, developer ....
Verifier Appraisals	Sw integrity, config ok, attester recognized, ...
Freshness	Nonce, trusted timestamp, ...

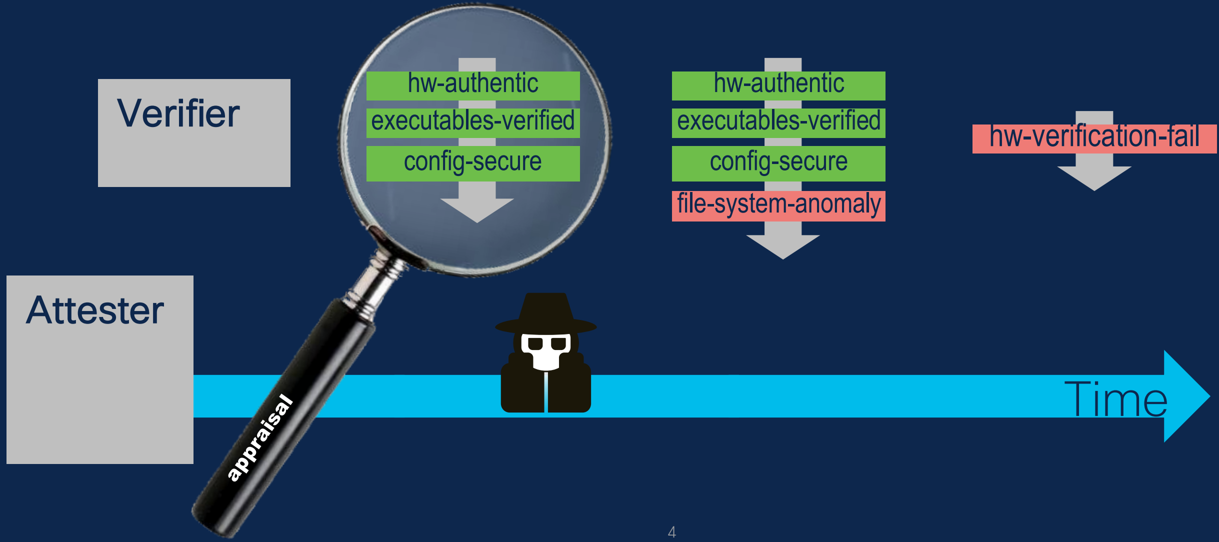
Support varies by AE chip type > Attester > Verifier



- Relying Party cannot support ∞ language permutations
  - And a mix and match across L1 ↔ L7 platforms is coming if IETF RATS succeeds
- Need: Shared definitions/structures for Verifier Appraisals coming to Relying Party
  - Will help scale and Interop
  - Reduce transcoding/mapping between sequentially bound sets of Attesters
  - Could be encoded in EAT, YANG, CDDL, etc...

Verifier Appraisal

- Periodic appraisal and generation of Attestation Results
- One to Many Trustworthiness Claims assigned during an appraisal cycle
- Attestation Results signed and returned to Attester (for scale/speed)



Normalizing Trustworthiness Claims

Specific claim definitions, extensible

🟩 affirming
🟥 detracting

Trustworthiness Claim	Attesting Environments		
	Confidential Compute		HSM-based (TPM)
	Process-based (SGX, TrustZone)	VM-based (SEV, TDX, ACCA)	
🟩 ae-instance-recognized	Optional	Optional	Optional
🟥 ae-instance-unknown	Optional	Optional	Optional
🟩 hw-authentic	Implicit	Chip dependent	If PCR check ok
🟥 hw-verification-fail	Implicit if not ok	Chip dependent	If PCR don't check ok
🟩 executables-verified	Optional	Optional	If PCR check ok
🟥 executables-refuted	Optional	Optional	If PCR don't check ok
🟥 file-system-anomaly	n/a	Optional	Insufficient
🟩 source-data-integrity	Optional	Optional	Optional
🟩 config-secure	Optional	Optional	Optional
🟥 config-insecure	Optional	Optional	Optional
🟩 target-isolation	Implicit	Implicit	Optional
🟩 runtime-confidential	Implicit	Implicit	Insufficient
🟩 secure-storage	Implicit	Chip dependent	Very minimal space

Normalized Trustworthiness Claims ≠ the same Relying Party policy disposition

- Even with Normalized Trustworthiness Claims, Attesters need not be treated equivalently by the Relying Party
    - Variance in underlying protections of SGX, TrustZone, SEV, TPM, etc. could mean different disposition via the Appraisal Policy for Attestation Results.
    - Each Verifier, or Verifier version, or Verifier appraisal of a specific type of Attester may be trusted differently for different claims

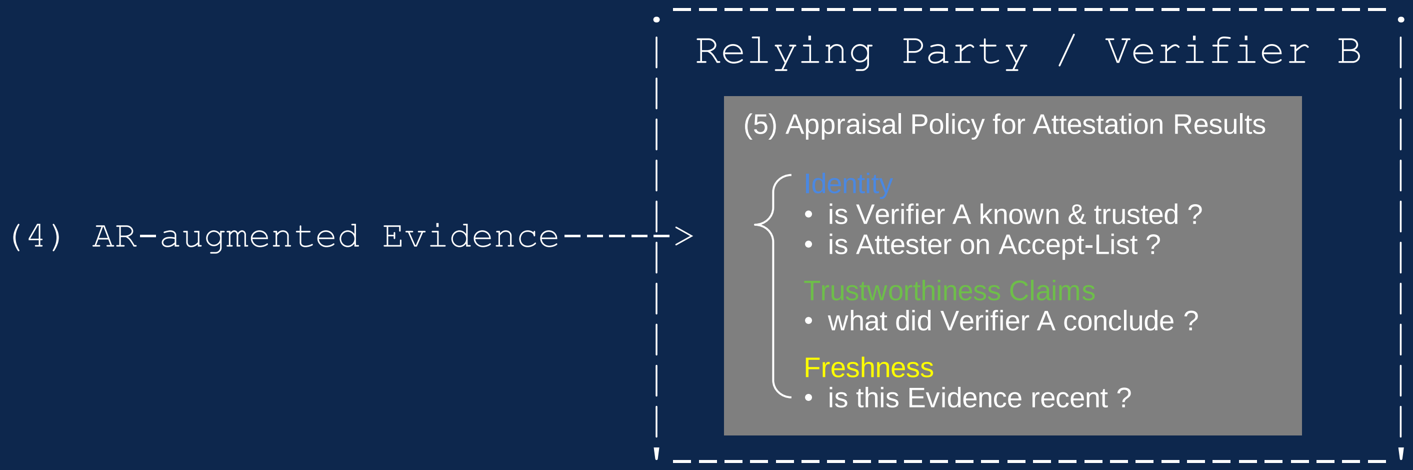
Trustworthiness Claim Delivery

Based on draft-ietf-rats-architecture: Passport Model

```
  .----------------.
  | Attester       |
  | .-------------.|
  | | Attesting   ||             .----------.    .---------------.
  | | Environment ||             | Verifier |    | Relying Party |
  | '-------------'|             |     A    |    |  / Verifier B |
  '----------------'             '----------'    '---------------'
        time(VG)                       |                 |
          |<------Verifier PoF-------time(NS)            |
          |                            |                 |
 time(EG)(1)------Evidence------------>|                 |
          |                          time(RG)            |
          |<------Attestation Results-(2)                |
          ~                            ~                 ~
        time(VG')?                     |                 |
          ~                            ~                 ~
          |<------Relying Party PoF-----------------(3)time(NS')
          |                            |                 |
time(EG')(4)------AR-augmented Evidence----------------->|
          |                            |   time(RG',RA')(5)
                                                        (6)
                                                         ~
                                                      time(RX')
```

Attestation Results Augmented Evidence

- Input to Relying Party’s Appraisal Policy for Attestation Results
- How to review the AR-augmented evidence to ensure no tampering



(4) AR-augmented Evidence----->

Relying Party / Verifier B

(5) Appraisal Policy for Attestation Results

Identity
- is Verifier A known & trusted ?
- is Attester on Accept-List ?

Trustworthiness Claims
- what did Verifier A conclude ?

Freshness
- is this Evidence recent ?

Attestation Results Augmented Evidence

objects needing specification

Trustworthiness Claims of the Verifier +

Identity	Attesting Environment	ae-instance-recognized
		ae-instance-unknown
Integrity	Hardware	hw-authentic
		hw-verification-fail
	Files	executables-verified
		executables-refuted
		file-system-anomaly
		source-data-integrity
	Config	config-secure
		config-insecure
Confidentiality	Target Environment	target-isolation
		runtime-confidential
	Data	secure-storage

Defined in this draft

Verified Identity instance(s) +

Attester	chip vendor
	chip type
	target environment
	target developer
	ae instance
Verifier	verifier developer
	verifier build

- Categories defined in this draft
- Specific objects to be defined in other drafts

Verifiable Freshness

Random Number	nonce
Synchronized Clocks	timestamp
	tuda sync token
Epoch	epoch id

- Categories defined in draft-ietf-rats-architecture Section 10

Current topics being worked by authors

- Categorizing ‘Trustworthiness Claims’ into ‘Endorsements’ and ‘Capabilities’ ?
- Datatype of ‘Trustworthiness Claims’ : move from identities to enumerations ?
- Follow-up drafts. E.g., Encoding in EAP for TLS transport

Summary

- Contents
  - Object definitions for Attestation Results (AR) to support Secure Interactions between Attester and Relying Party
  - How the Attester can augment AR to improve scale and speed of appraisal
  - State Machine for the Appraisal Policy for Attestation Results
- Two implementations
  - Trusted Path Routing (Proprietary – Cisco)
  - Veraison (Open Source – Confidential Compute Consortium)
- Ask: WG Adoption

Trusted Path Routing

draft-voit-rats-trustworthy-path-routing-03

IETF 111, July 29th 2021, RATS WG

Eric Voit
Cisco
evoit@cisco.com

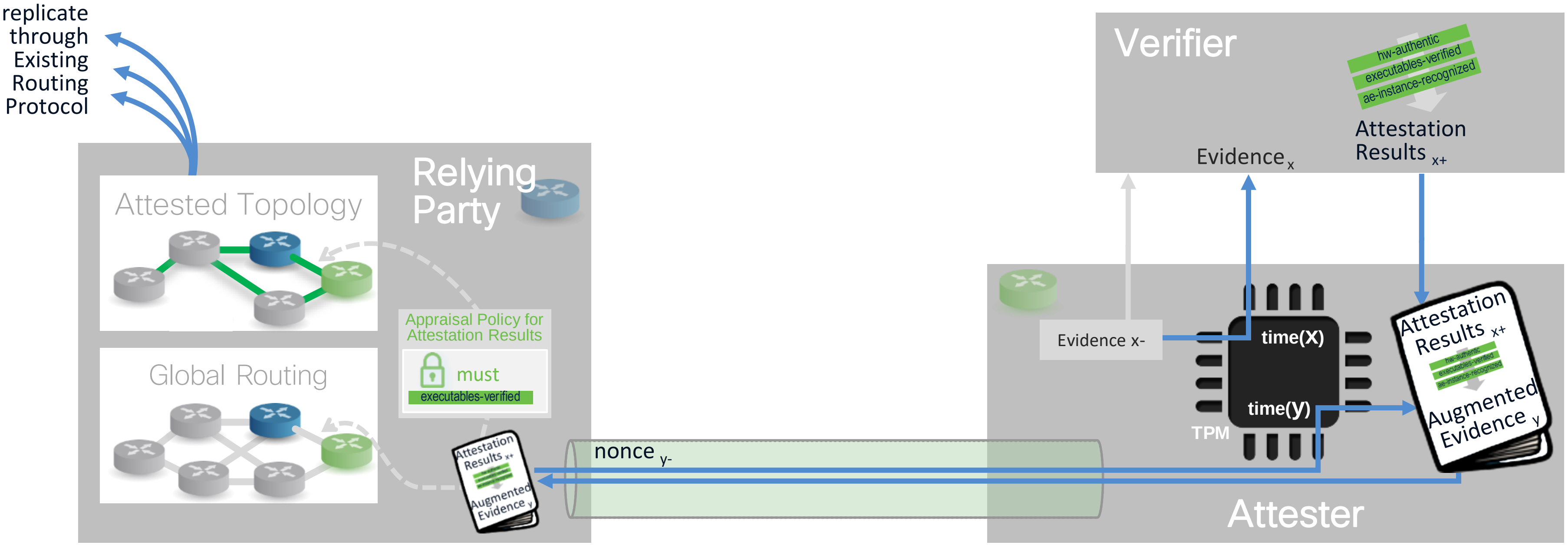
Chennakesava Reddy Gaddam
Cisco
chgaddam@cisco.com

Guy Fedorkow
Juniper
gfedorkow@juniper.net

Henk Birkholz
Fraunhofer SIT
henk.birkholz@sit.fraunhofer.de

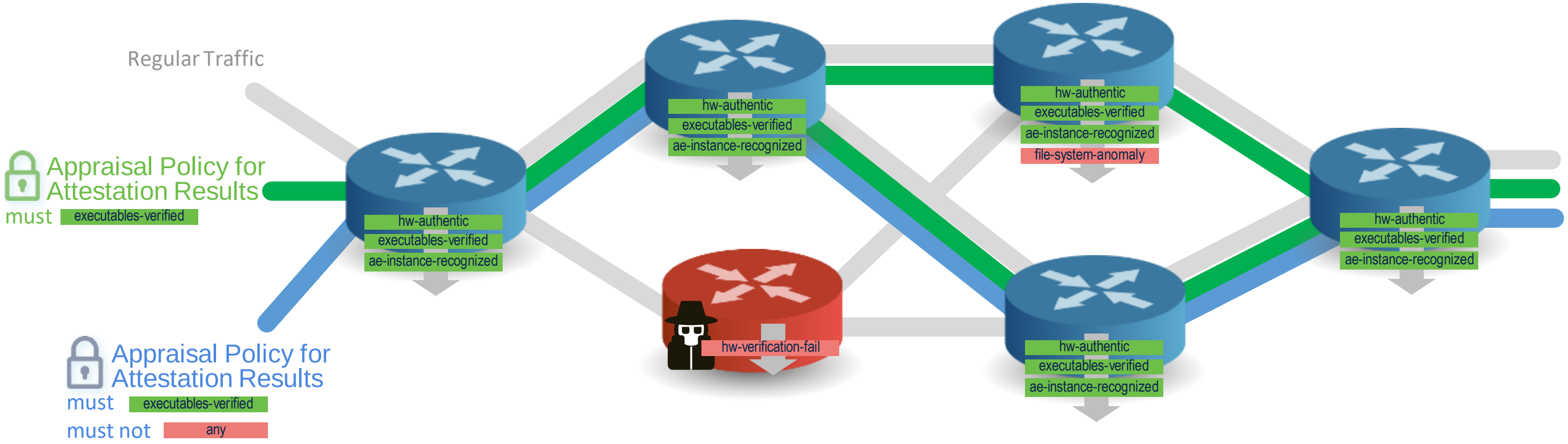
Trusted Path Routing

- Link adjacencies added to Trusted Topology based on latest Relying Party's appraisal of AR Augmented Evidence



Trusted Path Routing - Demo

- Custom topologies dynamically maintained based on Attestation Results



Changed since last draft version

- Extracted the elements to draft-voit-rats-attestation-results:
  - Trustworthiness Claims, Relying Party State Machine, Call Flow.
- Alignment of WGLC comments received on Charra YANG model
- Authorship updated

Next Steps

- Continued alignment with draft-voit-rats-attestation-results (e.g., Trustworthiness Claims structures)

- Definition of EAP payload (separate draft)

- No assertion to adopt until WG makes progress/ adopts draft-voit-rats-attestation-results