Attestation Results for Connectivity

draft-voit-rats-attestation-results-00

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

Remote Attestation in a Heterogenous World

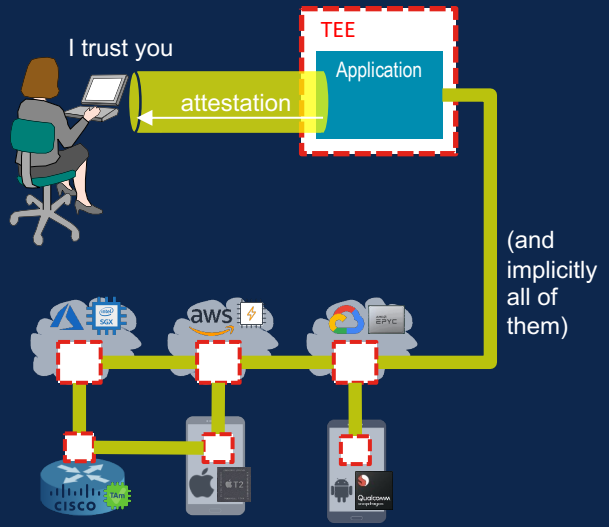
Confidential compute in an umbrella term

- Confidentiality of Code & Data
- Integrity of Code & Data
- Identity of Code
- Confidentiality of Execution

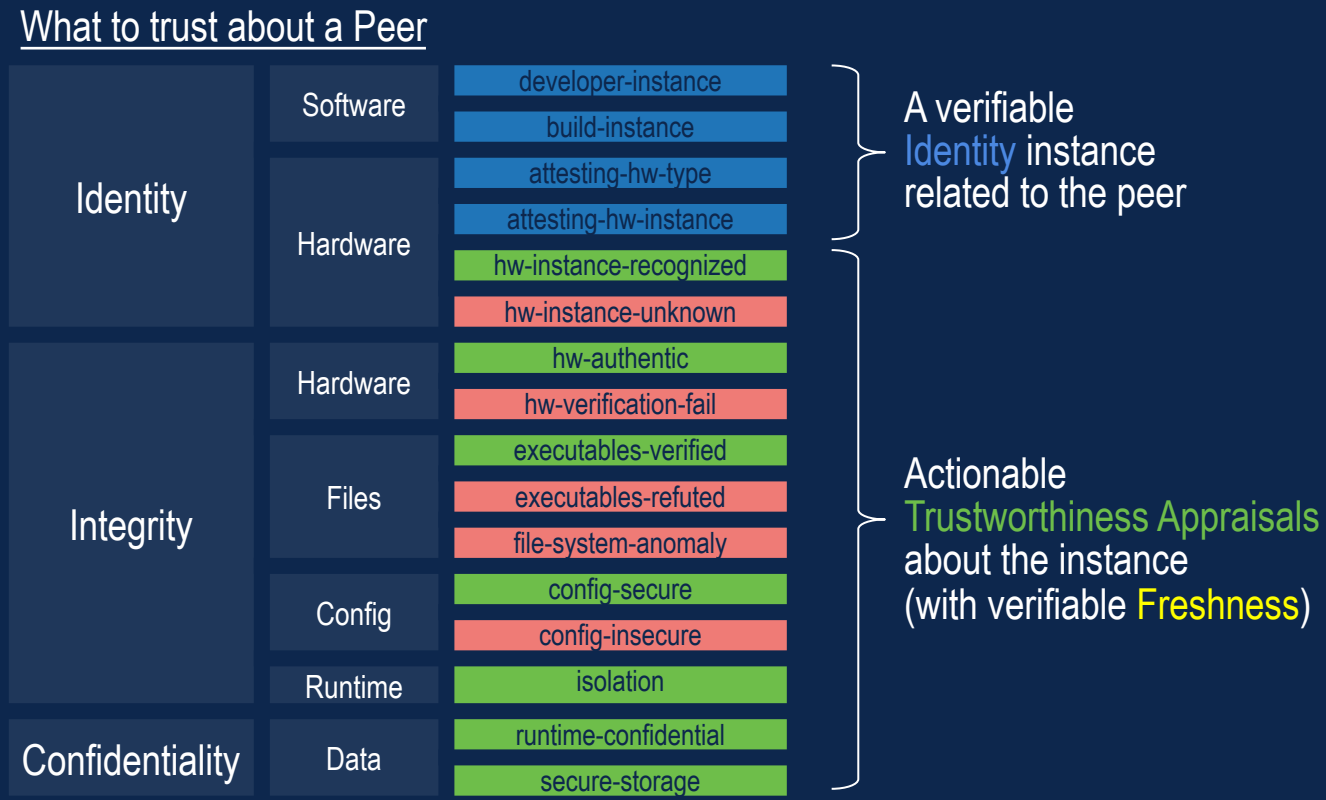
} Support varies by chip type

Opaque clusters of networked TEE

- Secured meshes will span from Local Host through Cloud
- Attest security posture & peer identity
- Mesh a mix and match of TEE types across L1 ↔ L7 platforms



What is Trust for Connectivity?



Build upon IETF’s draft-ietf-rats-architecture

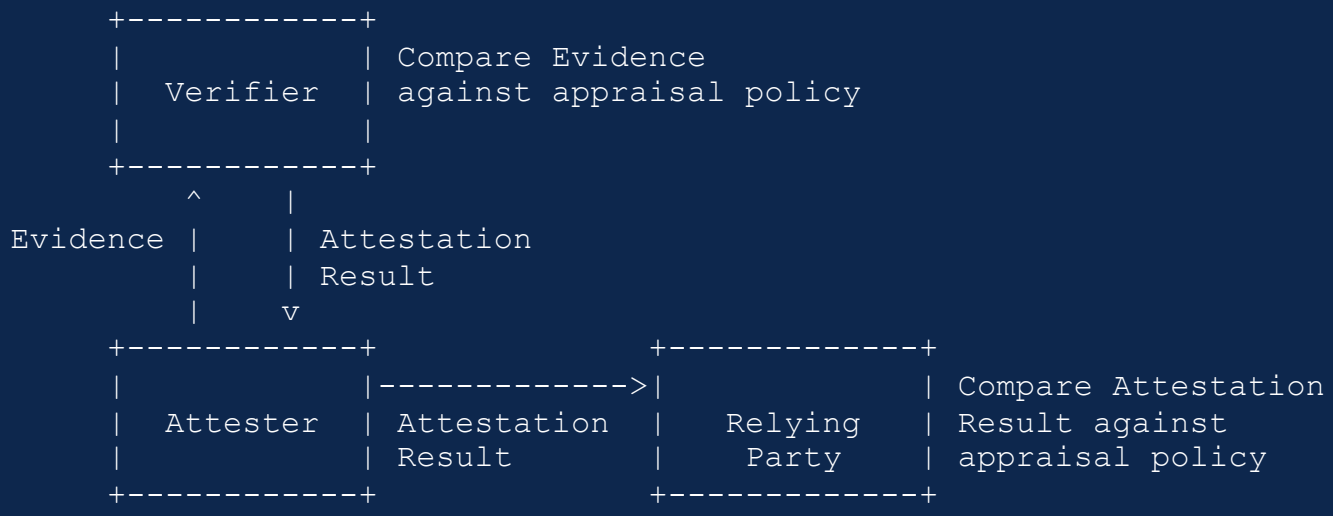
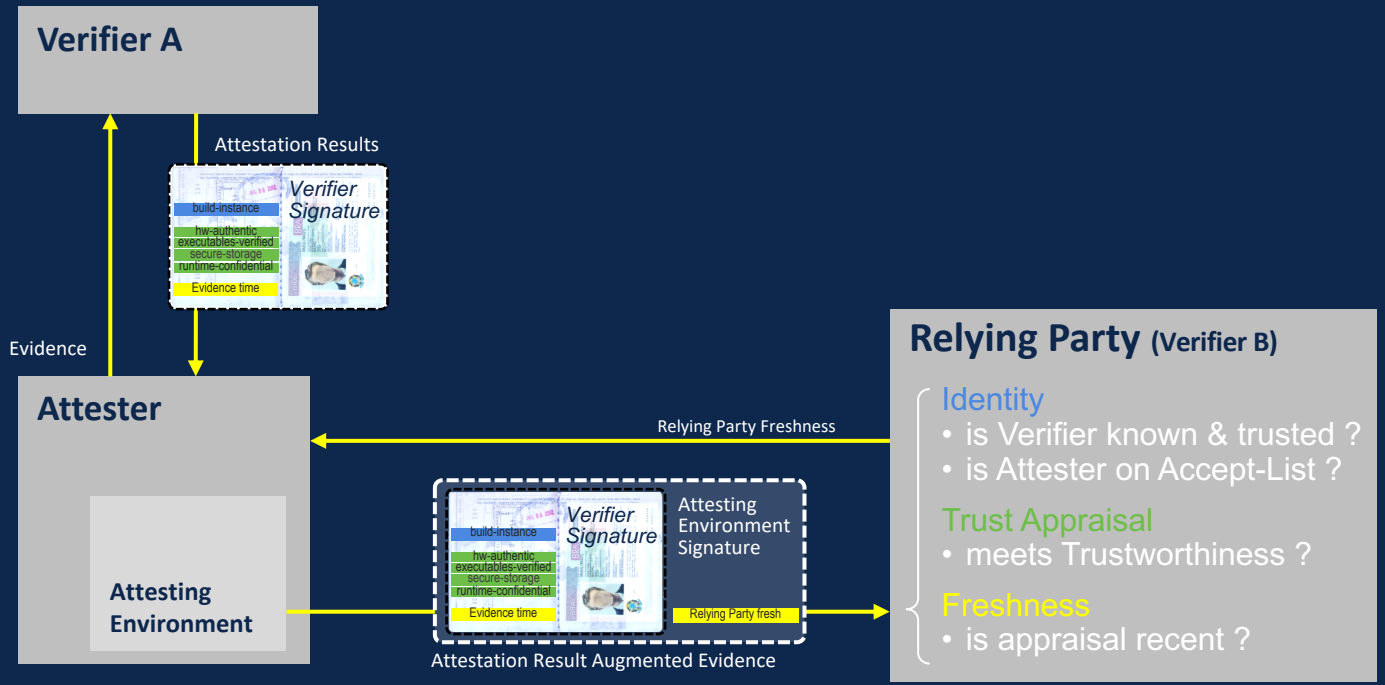


Figure 5: Passport Model

Build upon IETF's draft-ietf-rats-architecture



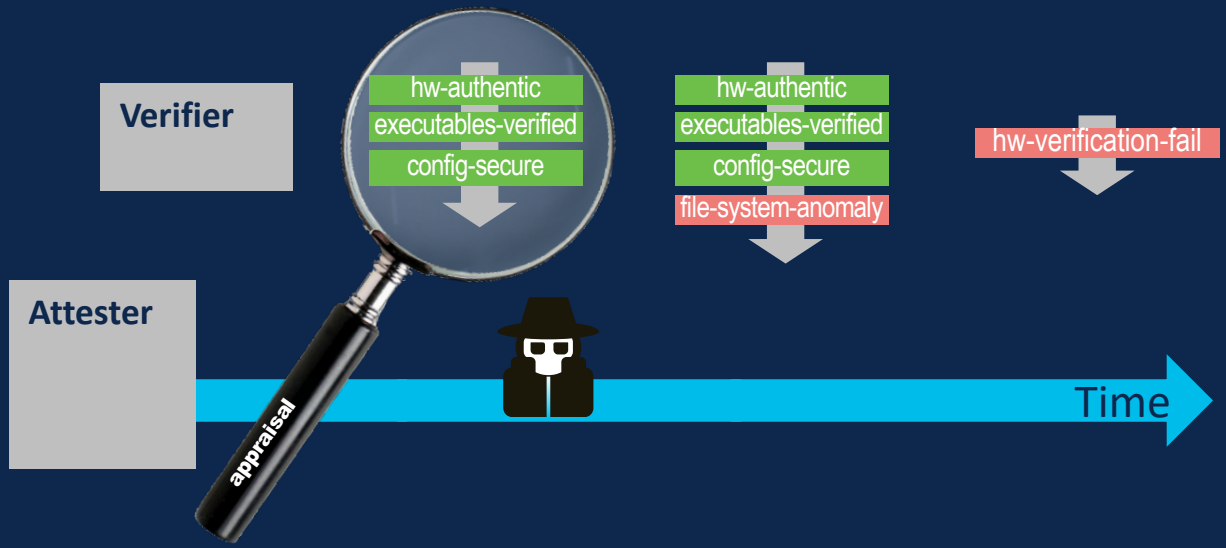
Normalizing Trustworthiness Claims
A starting point for many future discussions

Appraisal of:		Trustworthiness Claim	TPM	SGX	TrustZone	Other TEE
Identity	Hardware	hw-instance-recognized	Optional	Optional	tbd	
		hw-instance-unknown	Optional	Optional	tbd	
Integrity	Hardware	hw-authentic	If PCR check ok	Implicit	Implicit	
		hw-verification-fail	If PCR don't check ok	Implicit if not ok	Implicit if not ok	
	Files	executables-verified	If PCR check ok	Optional	Optional	
		executables-refuted	If PCR don't check ok	Optional	Optional	
		file-system-anomaly	Non-PCR check	Optional	Optional	
	Config	config-secure	Optional	Optional	Optional	
		config-insecure	Optional	Optional	Optional	
	Runtime	isolation	If no other apps	Implicit	Implicit	
Confidentiality	Data	runtime-confidential	Insufficient	Implicit	Implicit	
		secure-storage	Very minimal space	Implicit	Implicit	


CISCO

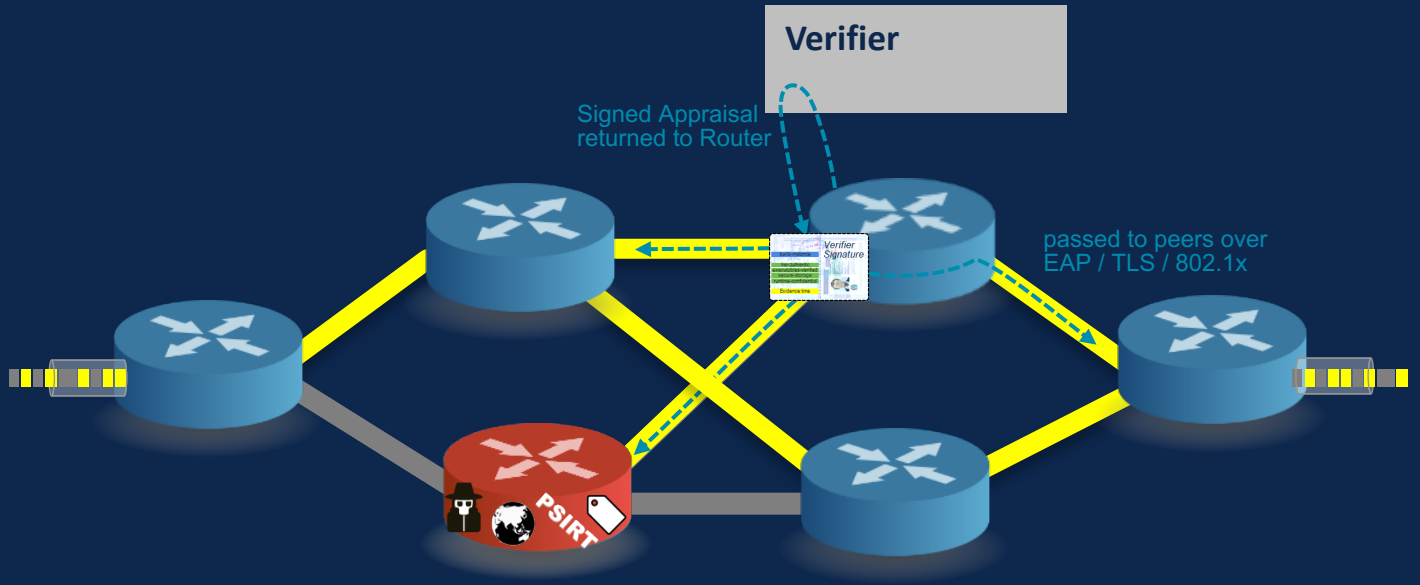
Trustworthiness Appraisal

- One to Many Trustworthiness Claims assigned during an appraisal cycle.



Trusted Path Routing
draft-voit-rats-trustworthy-path-routing

- Operational instance of draft-voit-rats-attestation-results
- Network trust is established via each peer's Link Layer credentials



9

Example Trustworthiness Vector State Machine

- Setting each Trustworthiness Claim is explicit.
- It is possible to not assert **ANY** conclusions after the appraisal.