Confidential Computing and Networking

TAC Tech Talk – 7 April 2022

Eric Voit
Principal Engineer
Cisco Systems
evoit@cisco.com

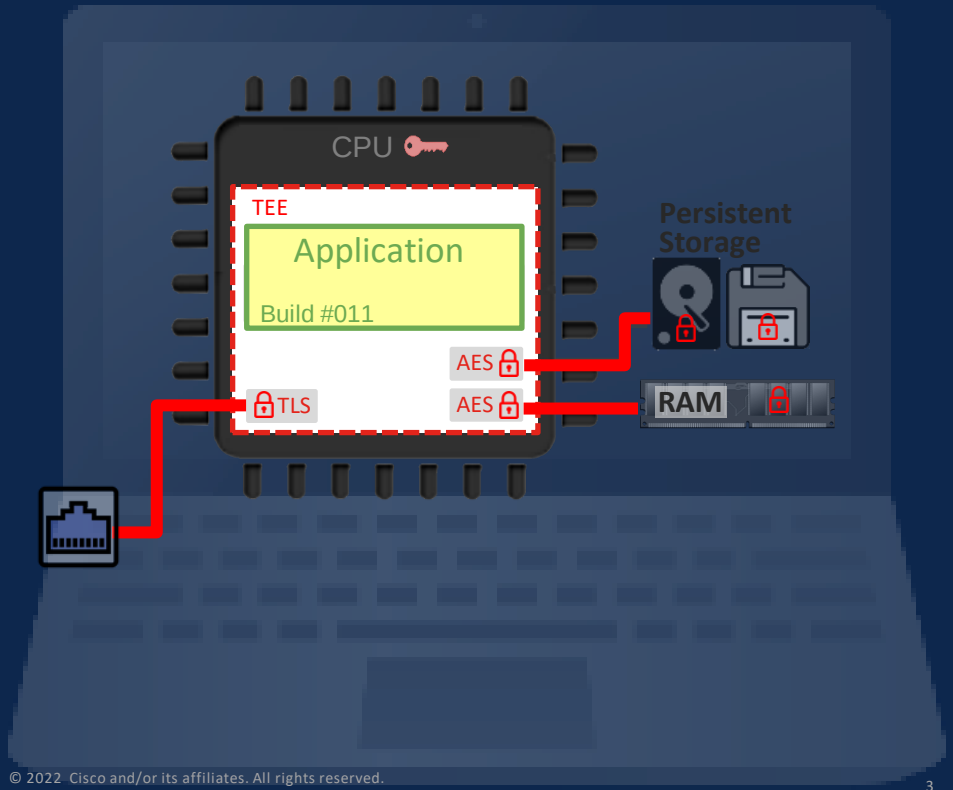
Context

Categorization

Use Cases

Standardization

Confidential Computing

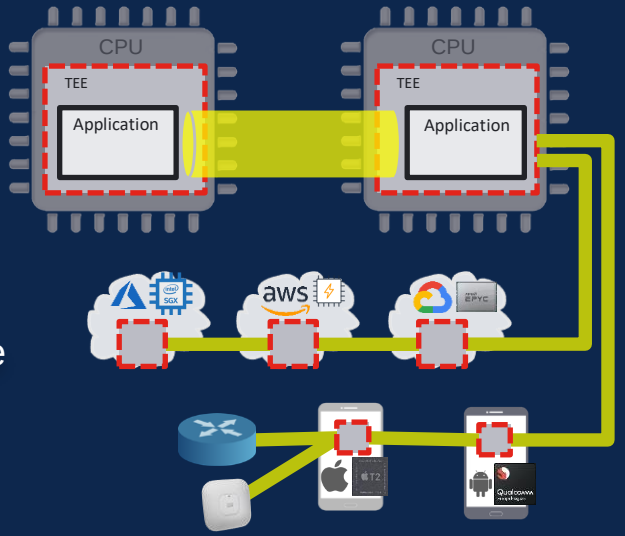


- Competing definitions, can mean:
  - Protection of Data in Use
    - In a hardware based Trusted Execution Environment (TEE)
  - Protection of Data at Rest
  - Application opaque to the Operator
    - Non-repudiable code identity

Confidential Computing, Networked

Opaque clusters of networked compute emerge

- Zero Trust evolves to hardware-signed evidence (non-repudiation+)
- Remote Attestation of security posture and/or peer identity



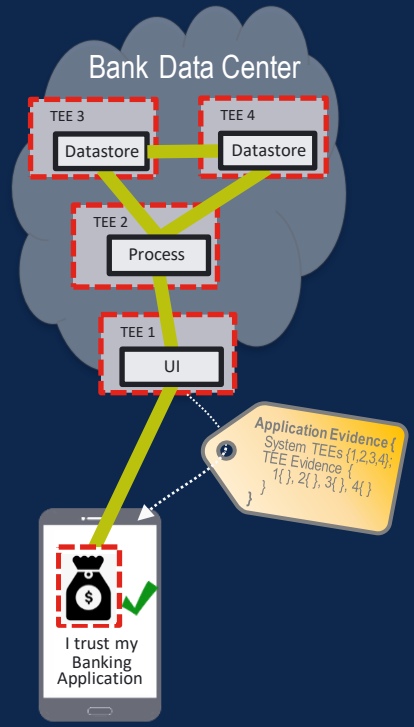
Metcalfe's law: value of network is proportional to the square of the number of connected users of the system (n^2)

- Mesh a mix and match of chip types across L1↔L7 platforms
- Ubiquitous Trustworthy Peers

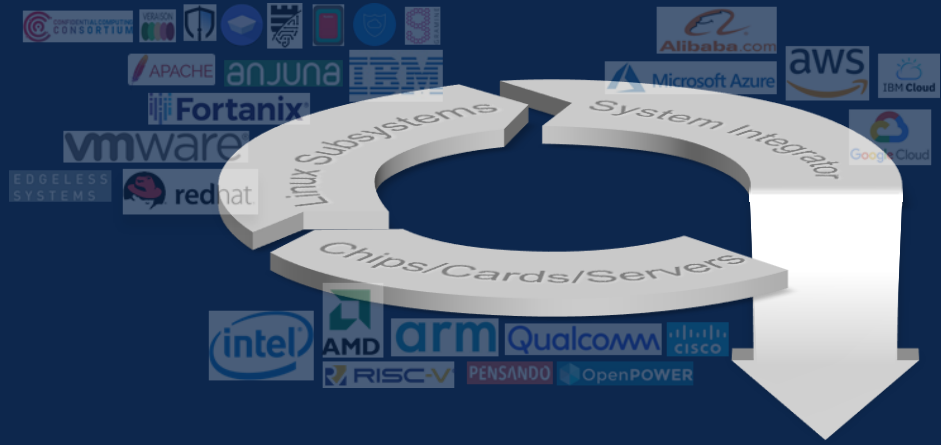
Confidential Application

⚠ We haven't explored terminology in the CCC for this yet

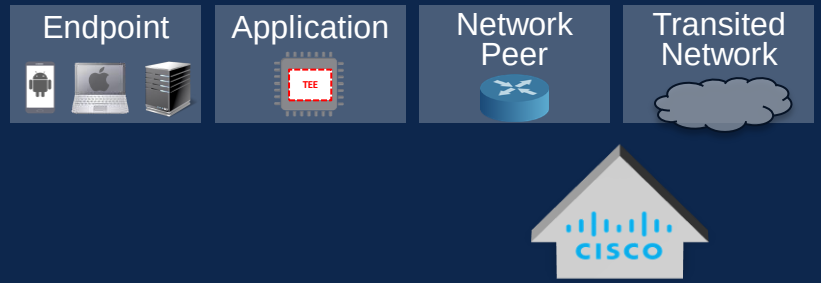
- An application asserting a unified set of Data-in-Use, Data-at-Rest, and Data-in-Transit guarantees throughout all digital systems where sensitive data is visible.
- Dynamic maintenance of the Attestation state of mesh of TEEs which comprise the application.
  - Routing Protocol parallels
- Relevant data to protect will vary based on interested party
- What Evidence (if any) provided to application user?



Virtuous Cycle Incomplete without Networking



Can I trust my peer



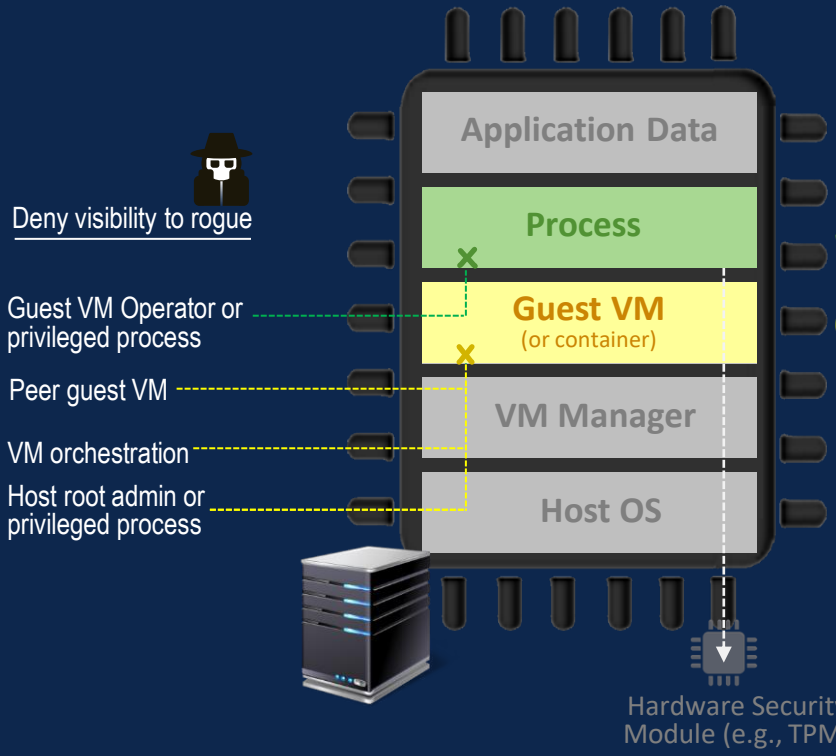
Context

Categorization

Use Cases

Standardization

Categorizing Confidential Compute



Value proposition

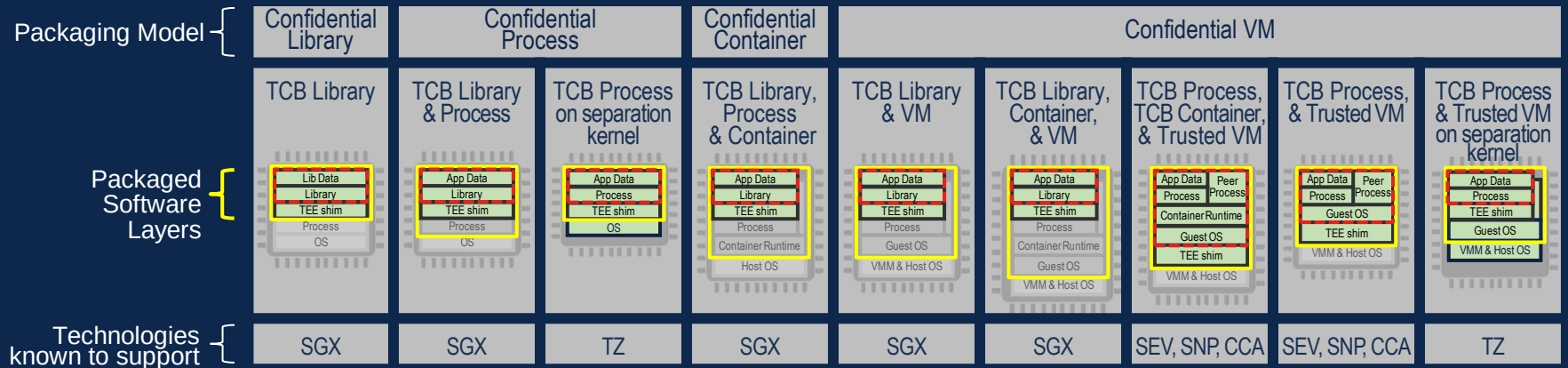
Specific process is opaque

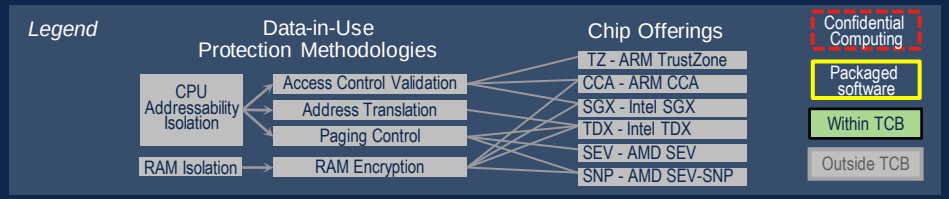
Operates as a walled garden

	CPU Addressability	RAM Encryption
Intel - SGX	✓	✓
ARM - TrustZone	✓	
Intel - TDX	✓	✓
ARM - CCA	✓	✓
AMD - SEV	✓	
AMD - SEV-SNP	✓	✓

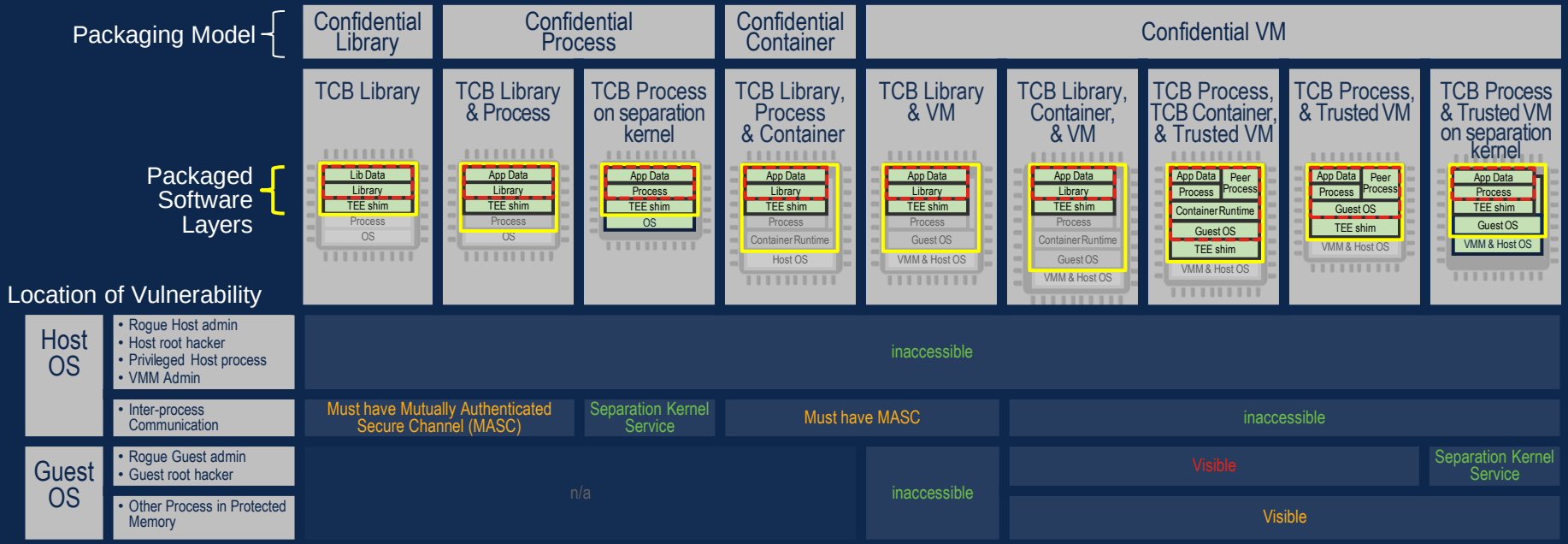
Can't lie about security measurements

Packaging Options using CONFIDENTIAL COMPUTING CONSORTIUM Terminology

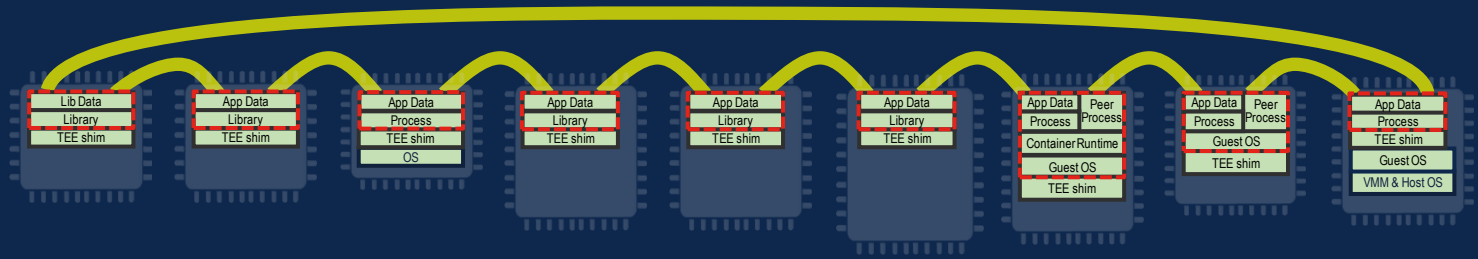




What Actually is Protected

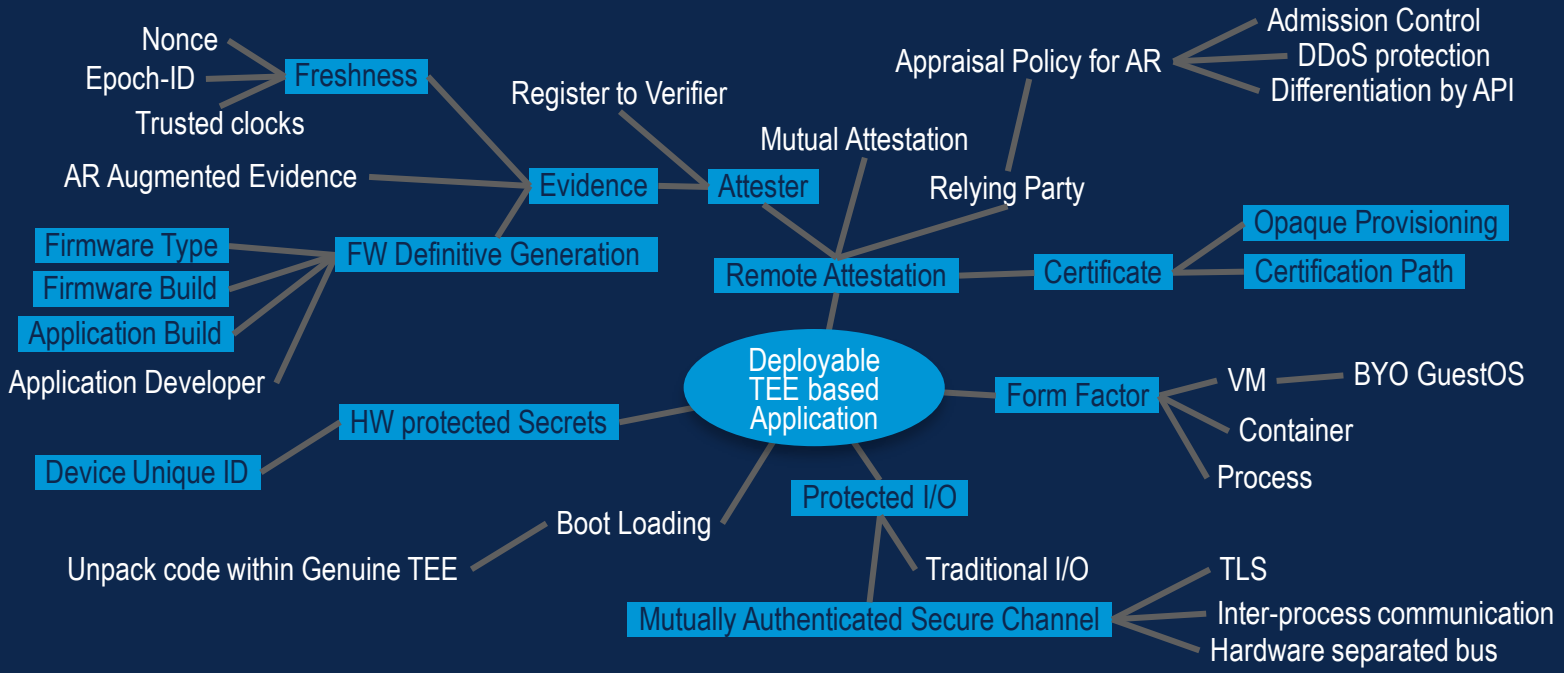


Ubiquitous Trustworthy Peers



- Network a Heterogeneous mix of TEE
- Requires standardization/agreement on Mutually Authenticated Secure Channel (MASC) interaction models and credential formats.

Functional Requirements – Minimally Deployable Subset



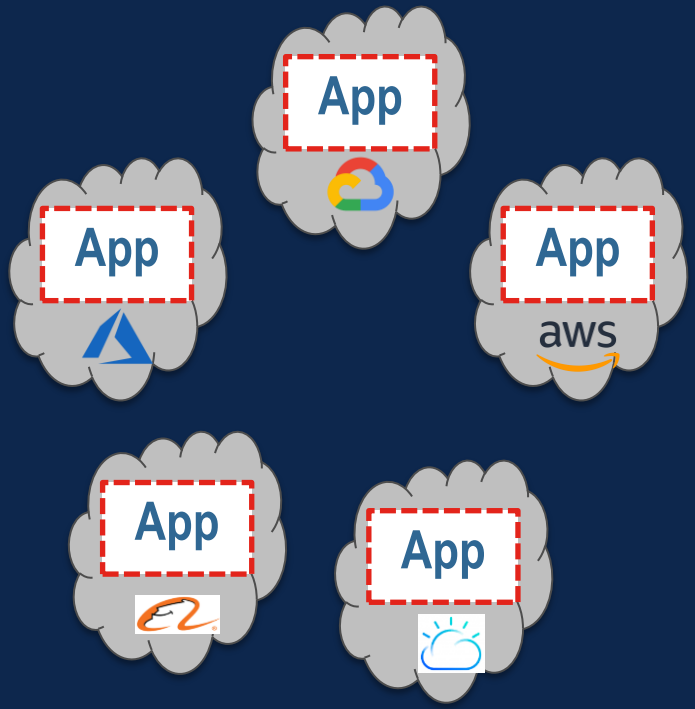
Context

Categorization

Use Cases

Standardization

Networking Applications in Public Cloud



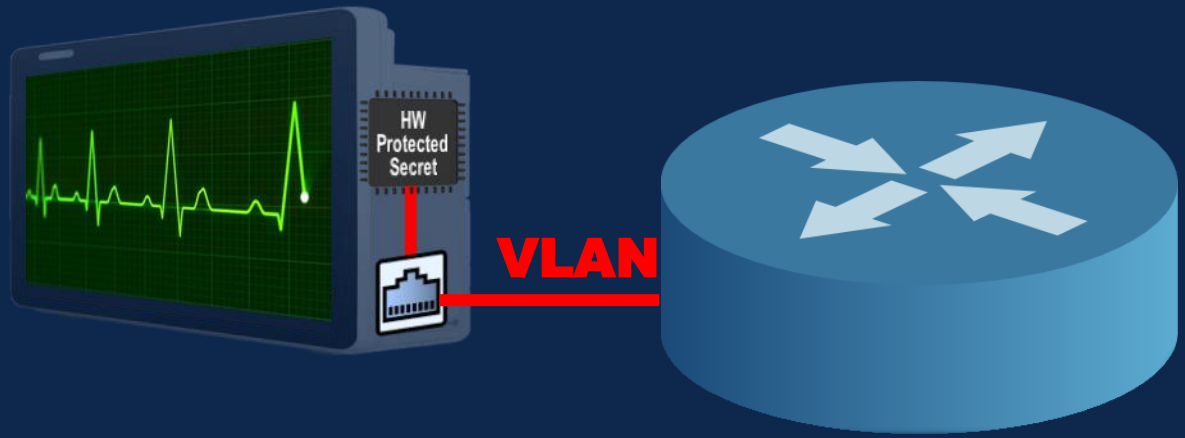
- Opaque Keystore
- Opaque Container Cluster
- Opaque Router
- Opaque Access Credentials
- Opaque Mobility
- Opaque Computing Area Network

Networking Applications on Premise

- All Applications from public cloud
- Secured Firewall Rules
- Opaque Telemetry

Below Zero Trust

Hardware Secret based Admission Control

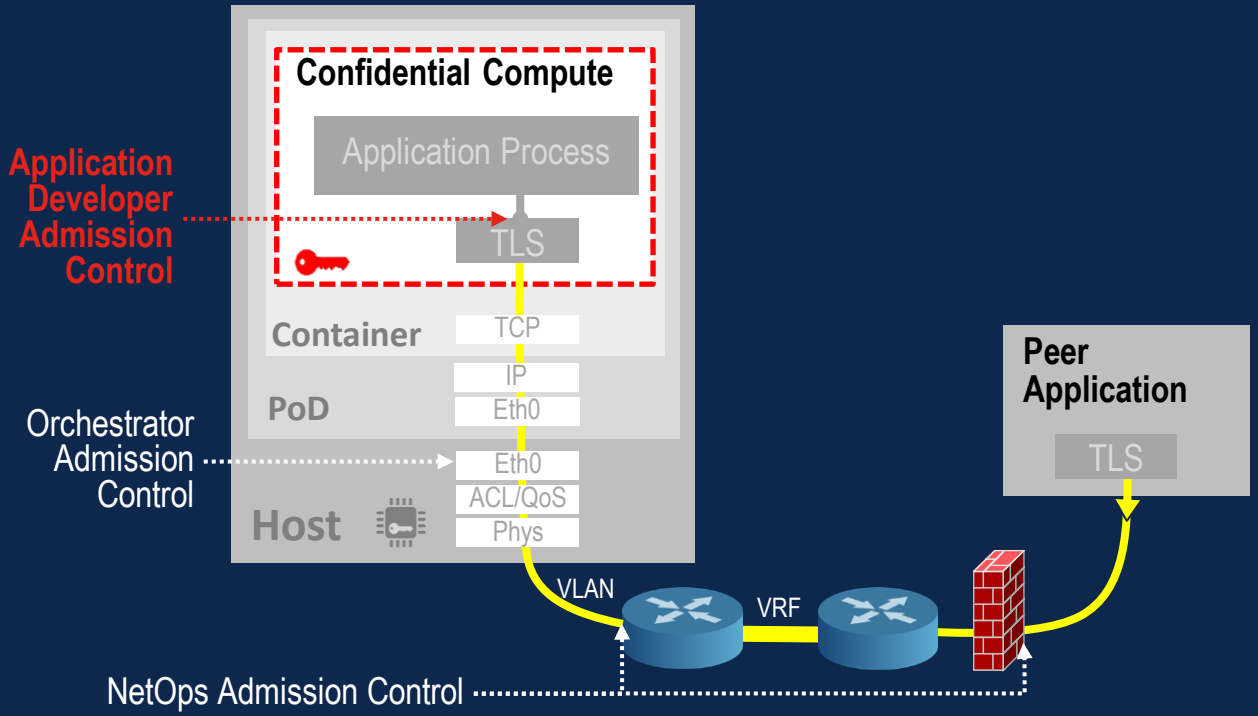


Helps address 60%+ of Malware delivered over encrypted channel

Router Based Applications

- NOS keystore / Datastore
- Containers and Local Apps
- Line Card verified clusters
- Tenant Opaque Telemetry

Intersecting Organizational Trust Boundaries



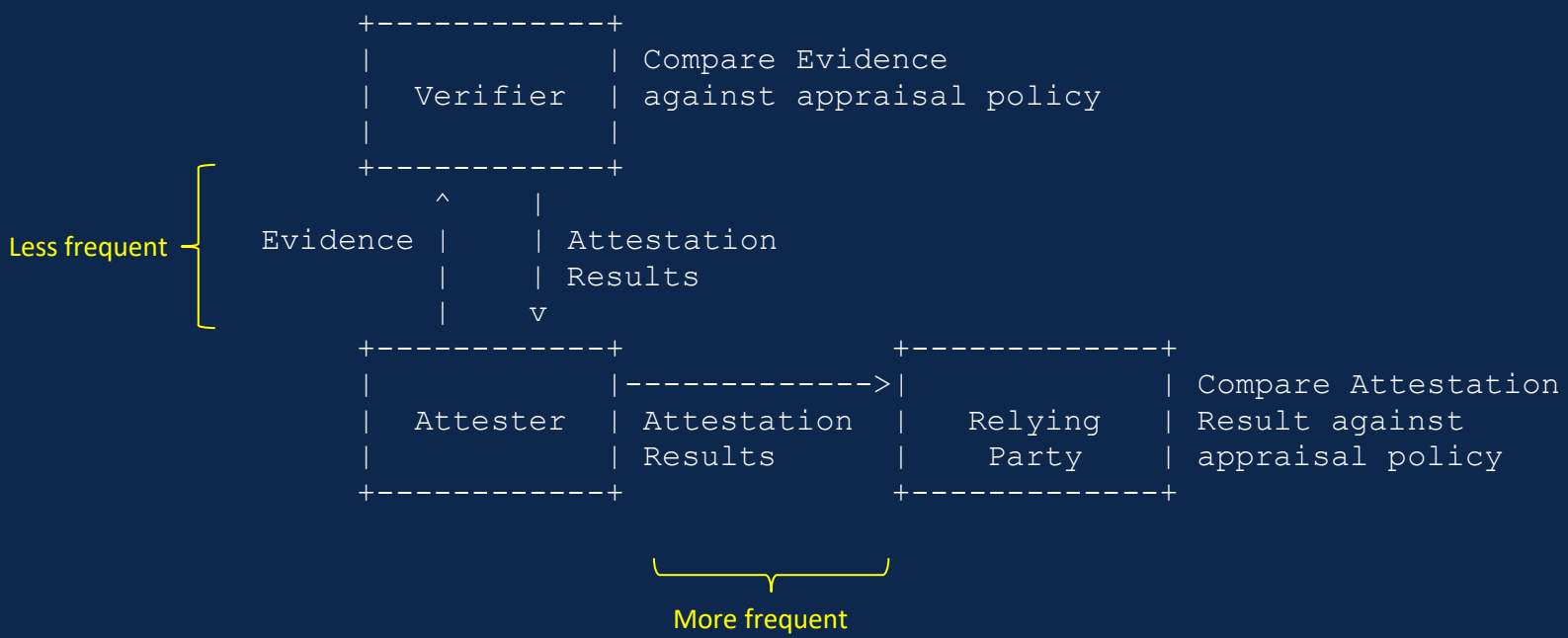
Context

Categorization

Use Cases

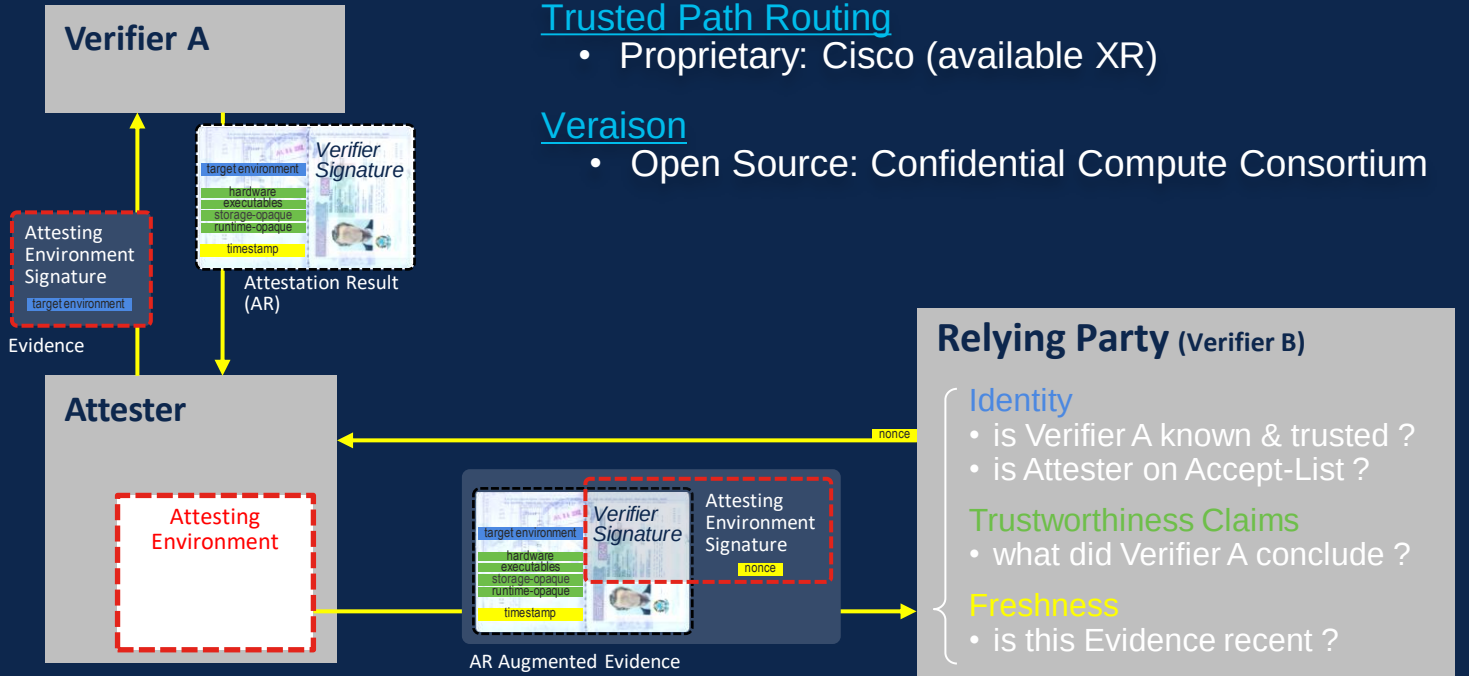
Standardization

Connectivity based on Trustworthiness
Building upon draft-ietf-rats-architecture



draft-ietf-rats-ar4si

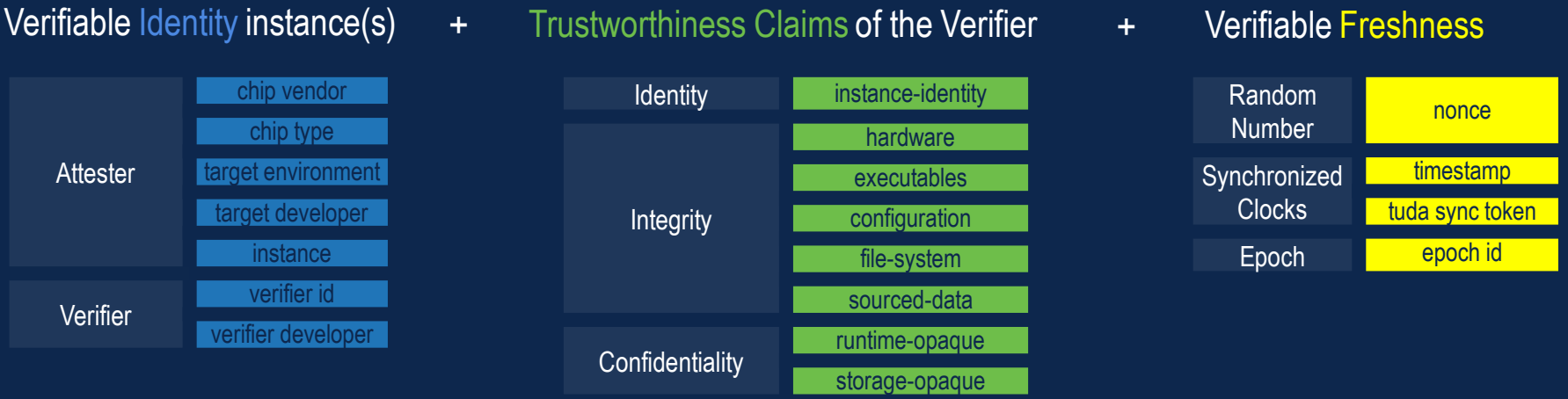
Eric Voit, Cisco, evoit@cisco.com
Henk Birkholz, Fraunhofer SIT, henk.birkholz@sit.fraunhofer.de
Thomas Hardjono, MIT, hardjono@mit.edu
Thomas Fossati, Arm Limited, Thomas.Fossati@arm.com
Vincent Scarlata, Intel, vincent.r.scarlata@intel.com



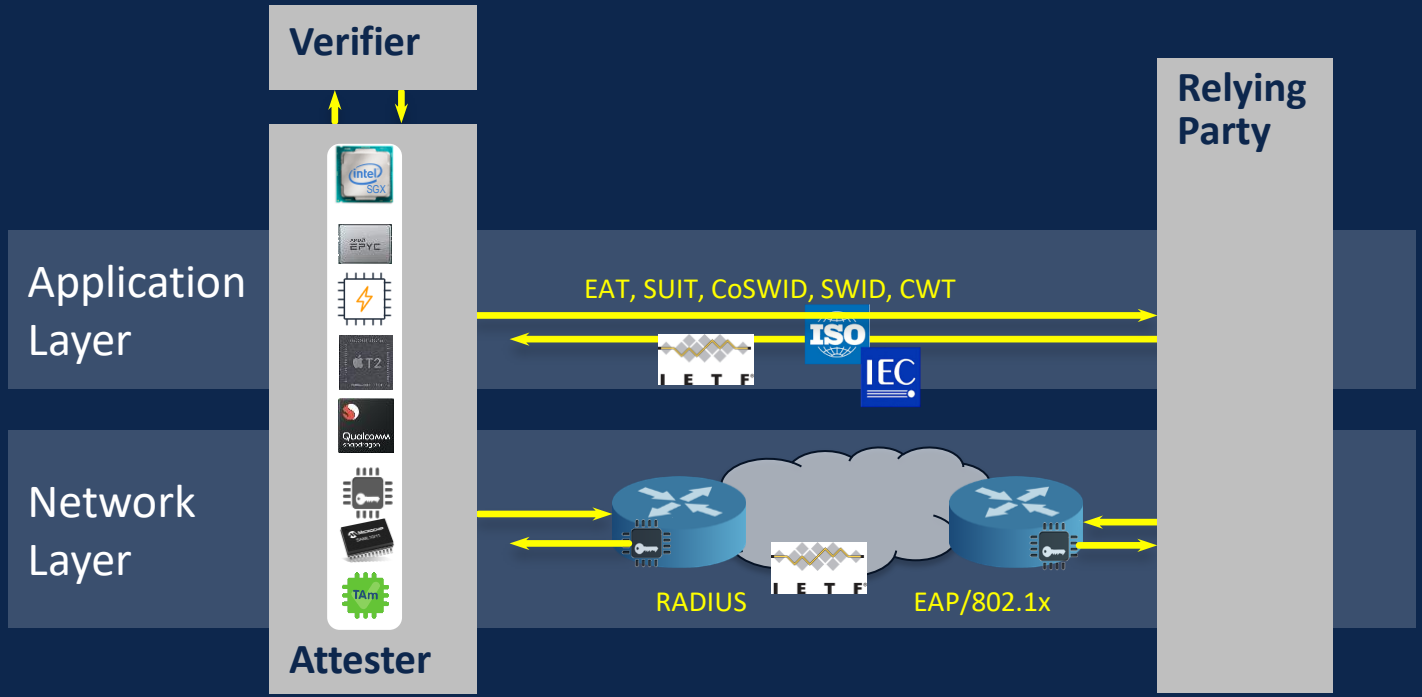
Trusted Path Routing
- Proprietary: Cisco (available XR)

Veraison
- Open Source: Confidential Compute Consortium

draft-ietf-rats-ar4si
Things which the Relying Party might Action



Connectivity based on Trustworthiness




CISCO