Attestation and Verification
Season 2: Shrinking The Elephant

sameo@rivosinc.com - LPC 2023
Last Season Recap

Confidential Computing is the protection of data in use by performing computation in a hardware-based Trusted Execution Environment. ([CCC whitepaper](https://example.com))

Protecting data in use is of limited value if you can’t trust who generates and uses it.
Last Season Recap

Confidential Computing is the protection of data in use by performing computation in a hardware-based Trusted Execution Environment. ([CCC whitepaper](https://example.com))

Protecting data in use is of limited value if you can’t trust who generates and uses it.

Confidential Computing without attestation and verification is not confidential.
Last Season Recap

Confidential Computing is the protection of data in use by performing computation in a hardware-based Trusted Execution Environment. ([CCC whitepaper](https://example.com))

Protecting data in use is of limited value if you can’t trust who generates and uses it.

Confidential Computing without attestation and verification is not confidential.

Interfaces, protocols, formats, and manufacturer interactions are very fragmented.

Plumbing an attestation evidence into an attestation service is very challenging.
Attestation Evidence ①

Confidential Guest (TVM)

Trusted Issuer (Relying Party)
Confidential Guest (TVM) -> Attestation Evidence ① -> Trusted Issuer (Relying Party) -> Attestation Evidence ② -> Verifier
Confidential Guest (TVM)

Attestation Evidence ①

Trusted Issuer (Relying Party)

Attestation Evidence ②

Verifier

Attestation Service
Confidential Containers Attestation Service

- Complete open source attestation service
- Architecture agnostic
  - Support for all major attestation evidence formats (TDX, SEV, CCA, SGX, Azure, CSV)
  - Supports external verifiers (Intel Amber)
- Open formats and protocols
- [https://github.com/confidential-containers/kbs](https://github.com/confidential-containers/kbs)
Attestation Evidence Format

- tsm-configfs to converge userspace ABI
- Actual evidence format is still architecture specific
- Entity Attestation Token
  - Content is arch specific, format is standard
  - Please use that!
  - ARM CCA and RISC-V
Reference Values

- IETF CoRIM for the format
- Link between supply chain and reference value provider
Device Attestation

- TVM must attest a device before accepting it
  - Kernel to offload device attestation to the Trusted Device Manager (TDM)
- Once accepted, the device is part of the TCB
  - Combined attestation: TVM attestation must include device attestation results
Device Attestation

TVM
- Trusted Device Manager
- Attestation Agent

Guest Kernel

TSM

SPDM
- TDI (VF)
- TDI (VF)

PCIe Device (PF)

① Detects

Platform Attestation Service

Device Attestation Service
Device Attestation

1. Detects
2. Attestation Request
3. Device Attestation
Device Attestation

TVM

Trusted Device Manager

Attestation Agent

Guest Kernel

TSM

PCle Device (PF)

TDI (VF)

TDI (VF)

① Detects

② Attestation Request

④ Attestation Result

⑤ Accept TDI

SPDM

Device Attestation Service

Platform Attestation Service
Device Attestation

- ① Detects Attestation Request
- ② Attestation Request
- ③ Device Attestation
- ④ Attestation Result
- ⑤ Accept TDI
- ⑥ Probes

TVM

Trusted Device Manager

Attestation Agent

Guest Kernel

TSM

SPDM

PCIe Device (PF)

TDI (VF)

TDI (VF)
Device Attestation

1. Detects
2. Attestation Request
3. Device Attestation
4. Attestation Result
5. Accept TDI
6. Probes
7. TVM Evidence
8. Device Attestation Results

TVM

- Trusted Device Manager
- Attestation Agent

Guest Kernel

- TSM
- SPDM
- PCIe Device (PF)
- TDI (VF)
- TDI (VF)

Platform Attestation Service

Device Attestation Service
Device Attestation

1. Detects
2. Attestation Request
3. Device Attestation
4. Attestation Result
5. Accept TDI
6. Probes
7. TVM Evidence
8. Device Attestation Results
9. TVM Attestation

TVM

Trusted Device Manager

Attestation Agent

Guest Kernel

TSM

SPDM

PCIe Device (PF)

TDI (VF)

TDI (VF)