Contribution ID: **252** Type: **not specified**

The elephants in the confidential room: Attestation and verification

Tuesday, 13 September 2022 12:10 (20 minutes)

While a lot of efforts are being put towards platform enabling for confidential computing, there's one fundamental part of the technology that we ignore more often than not: Attestation.

Without having a way to verify that the data we're trying to protect with confidential computing platforms is generated by a TCB that we know and validate, the whole confidential computing trust model falls apart.

As an attestation services client, the confidential containers attestation agent is entirely dependent on the local or remote Key Brokering Services implementation that it talks to. While working on this piece of software we realized how fragmented this part of the confidential computing ecosystem is: From the attestation evidence format to the verification policies or the reference values provisioning, each and every combination of a CSP, a silicon vendor and an OEM creates a new flow to support.

In this talk we will present our current proposals for building generic, vendor agnostic frameworks for attestation, verification and reference values providing services. We'll describe how our modular approach should allow for plugging existing, vendor-specific implementations, formats and flows as services back-ends. But most importantly, we'd like to discuss about a longer term goal: Finding a more uniform, less fragmented path for attestation flows, formats and requirements.

I agree to abide by the anti-harassment policy

Yes

Primary author: Mr ORTIZ, Samuel (Rivos)

Presenter: Mr ORTIZ, Samuel (Rivos)

Session Classification: Confidential Computing MC

Track Classification: LPC Microconference: Confidential Computing MC