Contribution ID: **388** Type: **not specified**

Going Beyond Confidential Attestation with Trustee

Friday, 20 September 2024 13:10 (20 minutes)

Trustee, formerly referred to as KBS, is a set of attestation and key management services for confidential workloads. In the past year the project has grown considerably, now supporting attestation of 8 different confidential platforms. This talk will briefly introduce the project and these updates but the main focus is ongoing work.

The talk will touch on the community's plan to support device attestation and integrate the CoRIM and EAR standards. We will then dive more deeply into how Trustee can be used to provide secure networking services to confidential guests. We will discuss the limitations of existing networking solutions and the need for specialized approaches to address secure node discovery, attestation, and secret provisioning.

Primary authors: PORTER, Chris (IBM Research); CARVALHO, Claudio; BUONO, Daniele (IBM); DUBEY, Niteesh (IBM); FELDMAN-FITZTHUM, Tobin (IBM)

Presenters: PORTER, Chris (IBM Research); CARVALHO, Claudio; BUONO, Daniele (IBM); DUBEY, Niteesh (IBM); FELDMAN-FITZTHUM, Tobin (IBM)

Session Classification: Confidential Computing MC

Track Classification: Confidential Computing MC