Contribution ID: **77** Type: **not specified**

Secure bootloader for Confidential Computing

Monday, 12 September 2022 10:05 (35 minutes)

Confidential computing (CC) provides a solution for data protection with hardware-based Trusted Execution Environment (TEE) such as Intel TDX, AMD SEV, or ARM RME. Today, Open Virtual machine Firmware (OVMF) and shim+grub provided necessary initialization for confidential virtual machine (VM) guest. More important, they acted as the chain of trust for measurement to support TEE attestation. In this talk, we would like to introduce the CC measurement infrastructure in the OVMF together with shim and grub, and how the VM guest uses the measurement information to support TEE runtime attestation. Finally we would like to discuss the attestation-based disk encryption solution in CC and compare the options in pre-boot phase (OVMF), OS loader phase (grub) or kernel early boot phase (initrd) and related cloud use case.

I agree to abide by the anti-harassment policy

Yes

Primary authors: LU, Ken (Intel); YAO, Jiewen; XU, min

Presenters: LU, Ken (Intel); YAO, Jiewen

Session Classification: System Boot and Security MC

Track Classification: LPC Microconference: System Boot and Security MC