Contribution ID: **197** Type: **not specified**

Attestation and Secret Injection for Confidential VMs & Containers/Pods

Tuesday, 21 September 2021 10:15 (25 minutes)

Attestation is an important step in the setup of a confidential enclave in a public cloud environment. Through this process a guest owner can externally validate the software being run in their enclave before any confidential information is exposed. In this talk, we discuss the design and challenges of measuring and validating a guest enclave, and safely injecting guest owner secrets into the enclave. Our discussion will focus on the AMD SEV architectures (SEV, SEV-ES, and SEV-SNP) and how their hardware-enforced attestation and pre-attestation procedures map onto the deployment of guest VMs and confidential containers (i.e., Kata Containers).

By attending this talk, you will gain an understanding of the attestation and measurement features of the AMD SEV architectures, as well as the challenges of doing attestation for confidential VMs and containers/Pods in a public cloud. In addition, we will overview other attestation approaches such as those of Intel TDx, SecureBoot, and other software-based techniques.

I agree to abide by the anti-harassment policy

I agree

Primary authors: CADDEN, Jim (IBM Research); BOTTOMLEY, James (IBM Research)

Presenters: CADDEN, Jim (IBM Research); BOTTOMLEY, James (IBM Research)

Session Classification: Confidential Computing MC

Track Classification: Confidential Computing MC