Contribution ID: **386** Type: **not specified**

SVSM vTPM: From Boot Attestation to Persistent Storage and Beyond

Friday, 20 September 2024 10:00 (20 minutes)

The integration of Secure Virtual Machine Service Module (SVSM) with virtual Trusted Platform Modules (vTPMs) is a critical component in establishing trust and security for confidential virtual machines (CVMs). This session delves into the latest advancements in SVSM vTPM technology, covering a wide range of topics from boot attestation to persistent storage and future development directions.

We will explore how SVSM can be leveraged to perform early boot attestation within firmware, establishing a robust root-of-trust for CVMs. By unlocking persistent SVSM storage, we can provide a stateful vTPM and UEFI variable storage for Secure Boot, enhancing the overall security posture. Additionally, we will discuss extensions made to the keylime attestation framework to accommodate vTPMs and certify CVM attestation integrity through vTPM measurements at boot.

The session will also provide an update on the development status of the SVSM vTPM, highlighting key features and use cases. We will delve into the challenges and potential solutions for achieving persistent vTPM state in the context of confidential VMs, including discussions on guest identity provisioning, early boot attestation, early secret injection, and persistent storage.

Primary authors: CARVALHO, Claudio; GARZARELLA, Stefano (Red Hat); FANELLI, Tyler (Red Hat)

Presenters: CARVALHO, Claudio; GARZARELLA, Stefano (Red Hat); FANELLI, Tyler (Red Hat)

Session Classification: Confidential Computing MC

Track Classification: Confidential Computing MC