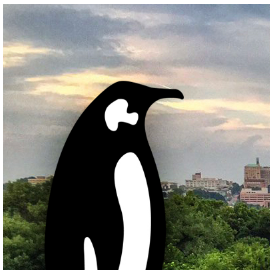

Contribution ID: **213** Type: **not specified**

Remote Attestation in AMD SEV-SNP Confidential VMs

Tuesday, 14 November 2023 14:45 (15 minutes)

The Trusted Platform Module (TPM) is an industry standard that is widely used as hardware root-of-trust for UEFI measured boot, Integrity Measurement Architecture (IMA) and remote attestation. Although virtual TPMs play the same role for VMs, standard vTPMs cannot be safely used for Confidential VMs since their state would be accessible by the hypervisor, which is considered an untrusted entity in the CVM threat model.

The Secure VM Service Module (SVSM) is a firmware component that runs in AMD SEV-SNP Confidential VMs to provide an isolated environment that can be used to run privileged modules, such as a vTPM, without interference from the hypervisor and the guest OS.

In this talk, we will discuss some of the design and implementation challenges we encountered while running a vTPM in the SVSM restricted environment. That includes aspects related to using the vTPM for remote attestation, maintaining and injecting the vTPM state, crypto support, and running the vTPM as a CPL3 module inside the SVSM.

Presenter: CARVALHO, Claudio (IBM)

Session Classification: Confidential Computing MC

Track Classification: LPC Microconference: Confidential Computing MC