Contribution ID: **280** Type: **not specified**

Secure Interrupt delivery: Lessons Learned from Alternate Injection Enablement

Friday 12 December 2025 13:15 (15 minutes)

To protect SEV-SNP guests against malicious injection attacks, the SEV-SNP Alternate Injection feature facilitates the services of a Secure VM Service Module (SVSM) and its APIC emulation to secure interrupt delivery into an SEV-SNP guest.

This session will explore the lessons learned during enabling Alternate Injection, including KVM, SVSM, OVMF and the guest kernel. It will cover how we bypass the KVM APIC emulation layer with a doorbell page and also do complex VMPL switches when the interrupt for VMPL2 is delivered into the SVSM with Restricted Injection.

Furthermore, the Restricted Injection handler and APIC emulation in the SVSM, and SVSM interaction with KVM, OVMF and the guest kernel, will be quickly illuminated.

Finally, a by-product of the enablement work - one useful trace tool (or a hack, depending on the beholder) for combining KVM and the guest code traces - will be shown.

Primary author: WANG, Melody (AMD)

Presenter: WANG, Melody (AMD)

Session Classification: Confidential Computing MC

Track Classification: Confidential Computing MC