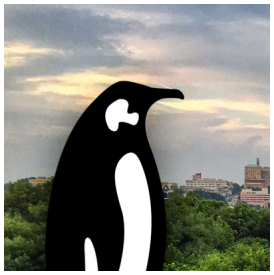

Contribution ID: **201** Type: **not specified**

Secure AVIC: Securing Interrupt Injection from a 'malicious' Hypervisor

Tuesday, 14 November 2023 17:50 (10 minutes)

SEV-SNP is a security feature that protects the confidentiality and integrity of VM memory from 'malicious' hypervisors or other VMs. Secure AVIC is a new HW feature added to SEV-SNP to prevent a 'malicious' hypervisor from generating unexpected interrupts to a vCPU or otherwise violate architectural assumptions around APIC behavior.

One of the significant differences from AVIC or emulated x2APIC, is that Secure AVIC uses a Guest Owned and Managed APIC Backing Page. It also introduces additional fields in both the VMCB and the Secure AVIC Backing Page to aid the guest in preventing (or moderating) interrupts to be injected by a 'malicious' hypervisor.

This proposal provides an overview of the hardware changes introduced by Secure AVIC, as well as the software design changes required on both the hypervisor and guest sides.

Primary author: I, Kishon Vijay Abraham

Presenters: I, Kishon Vijay Abraham; SUTHIKULPANIT, Suravee

Session Classification: Confidential Computing MC

Track Classification: LPC Microconference: Confidential Computing MC