Contribution ID: **158** Type: **not specified**

Interrupt Security for AMD SEV-SNP

Tuesday, 13 September 2022 13:10 (20 minutes)

Discussion about SEV-SNP support for Restricted Interrupt Injection and Alternate Interrupt Injection. These features enforce additional interrupt and event injection security protections designed to help protect against malicious injection attacks. Safe isolation between an SNP-protected guest and its host environment requires restrictions on the type of exception and interrupt dispatch that can be performed in the guest. Isolated guests are expected to run with the SNP Restricted Injection feature active, limiting the host to ringing a doorbell with a #HV exception. This essentially means when restricted injection is active, only #HV exceptions can be injected into the SEV-SNP guest. The majority of information communicated by the host is specific to the virtualization architecture (e.g. Virtio or VMBus messages) and will be delivered in a manner that is understood by the specific drivers running within the guest.

Description of the GHCB #HV doorbell communication to inject the exception or interrupt and description of the #HV doorbell page and the #HV Doorbell Page NAE event, as documented in the GHCB specification.

Detailed discussions on current implementation of Restricted Interrupt Injection on KVM, specifically about dispatch handling of system vectors and device interrupt vectors optimally from within the #HV exception handler. Also, changes required in the kernel's interrupt exit code path to support #HV exception handler and handling #HV exception with respect to kernel's interrupt enable/disable and idle/wakeup code paths.

I agree to abide by the anti-harassment policy

Yes

Primary author: KALRA, Ashish

Presenter: KALRA, Ashish

Session Classification: Confidential Computing MC

Track Classification: LPC Microconference: Confidential Computing MC