Contribution ID: **333** Type: **not specified**

OpenHCL: A Linux based paravisor for Confidential VMs

Friday 20 September 2024 11:00 (15 minutes)

Guest operating systems generally require modifications, referred to as enlightenments, to run under different Confidential computing architectures such as AMD SEV-SNP or Intel TDX. To support unenlightened guests, a software component called a paravisor is required. The paravisor runs at a higher privilege level within the guest to provide the appropriate abstractions and security guarantees that the unenlightened guest is unable to implement. The paravisor may additionally offer additional services such as emulated devices like a TPM or device translation between the host and the unenlightened guest.

Here we introduce OpenHCL - a Linux based paravisor with a usermode virtualization stack written in Rust for running unenlightened guests.

Primary author: OO, Chris (Microsoft)

Presenter: OO, Chris (Microsoft)

Session Classification: Confidential Computing MC

Track Classification: Confidential Computing MC