Contribution ID: **385** Type: **not specified**

OpenHCL: A Linux and Rust based paravisor

Friday, 20 September 2024 17:45 (45 minutes)

Virtual Secure Mode (VSM) allows for the ability to run trusted software components within the guest. A paravisor is a trusted software component that runs inside the guest at a higher Virtual Trust Level (VTL), VTL2 that provides services for the guest running in lower VTLs. This can include providing enlightenments for unenlightened guests in a Confidential VM, or providing additional services to the guest in a normal VM, such as vTPM or device translation.

Here we introduce OpenHCL- a Linux based paravisor with a usermode virtualization stack written in Rust. OpenHCL is used in Azure today to provide device translation for legacy guests and vTPM for security. We'll also discuss some thoughts and learnings about writing a usermode VMM in Rust for a paravisor.

A demo will be shown with various different features of OpenHCL. The rest of the time will be dedicated to free form discussion or Q&A.

Primary author: OO, Chris (Microsoft)

Presenter: OO, Chris (Microsoft)

Session Classification: Birds of a Feather (BoF)

Track Classification: Birds of a Feather (BoF)