OpenHCL: the new, open source paravisor for Confidential VMs

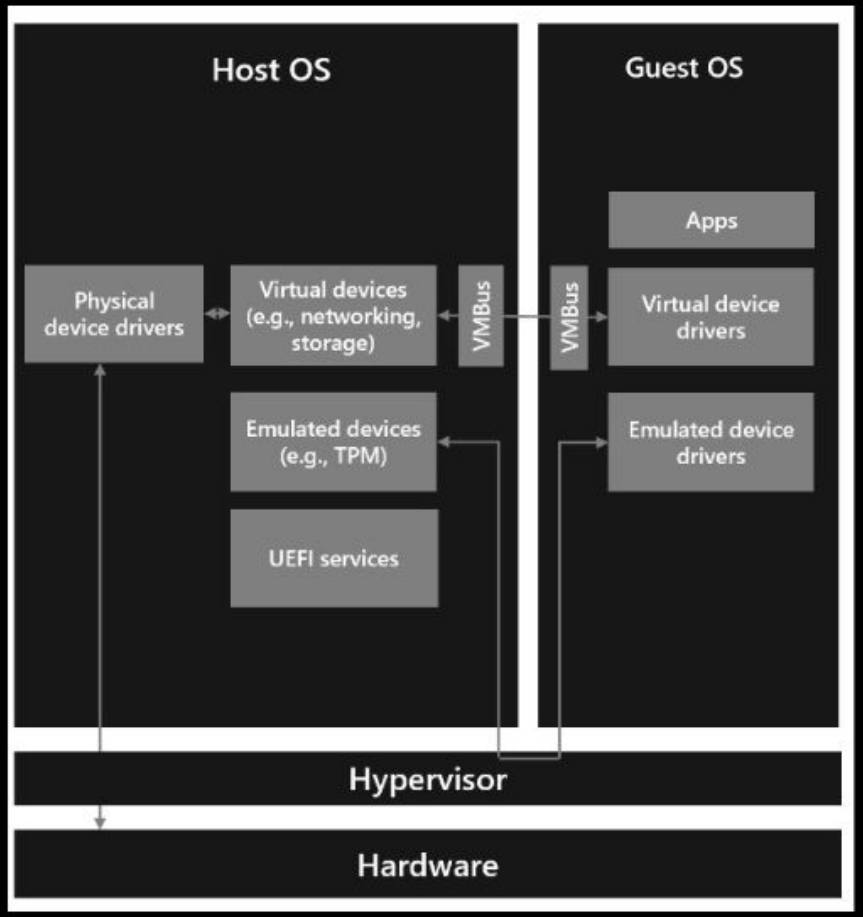
Caroline Perez-Vargas
Confidential computing OS platform PM at Microsoft

What is a paravisor?

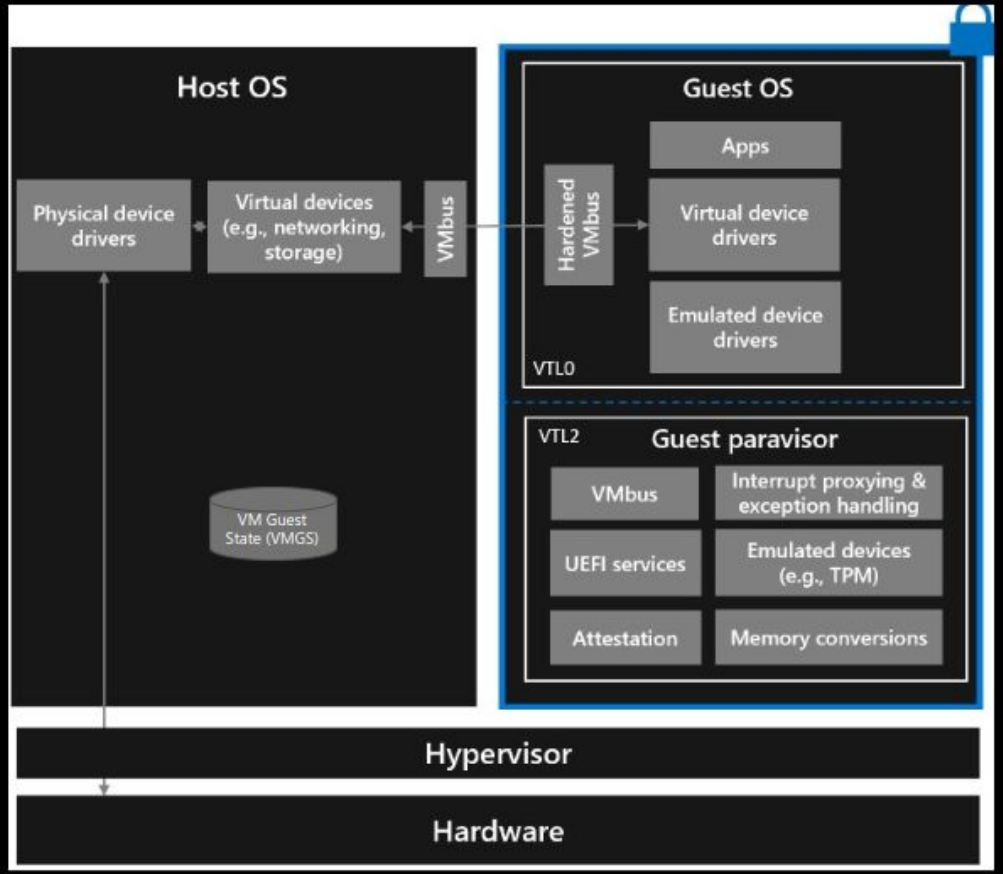
What is a paravisor?

- implements the TEE enlightenments on behalf of the guest OS so the guest OS can run mostly unmodified
- enables guests that are not fully enlightened, which includes legacy and future versions of Windows and legacy versions of Linux, to run inside a CVM
- runs at a higher privilege level: VTL2 on Hyper-V, L1 VM on TDX, VMPL0 on SEV-SNP

Traditional VM



Confidential VM



- Moving emulated devices from the Host OS to the guest paravisor enables Confidential VMs to have a vTPM and Secure Boot.
- Guest firmware can store and access guest state and guest secrets that are inaccessible to the Host OS.
- The paravisor can do interrupt proxying and handle the new special CVM exception type on behalf of the guest OS.
- Remote attestation & Secure Key Management.

OpenHCL overview

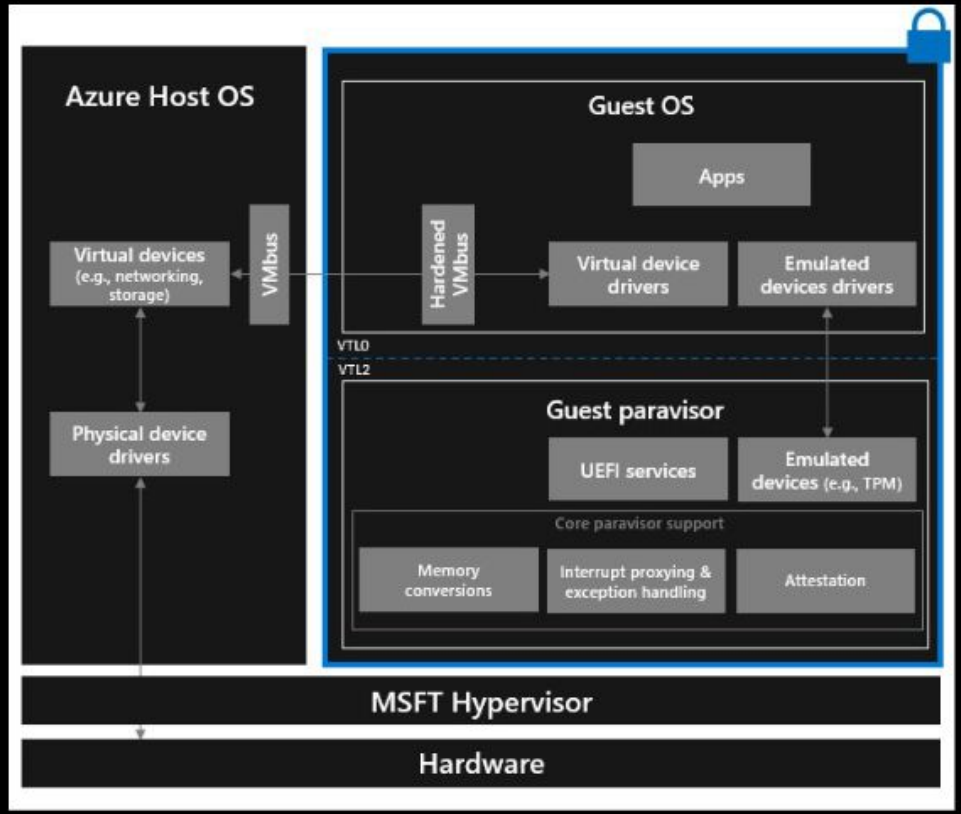
New paravisor (to be open sourced later this year) based on the OpenVMM project which provides other services to the guest:

- diagnostics (particularly useful to allow debugging CVMs where traditional debuggers are hard)
- device emulation (larger set of emulated devices) via standard devices interfaces
- device translation support via standard devices interfaces - such as NVMe to paravirtualized SCSI

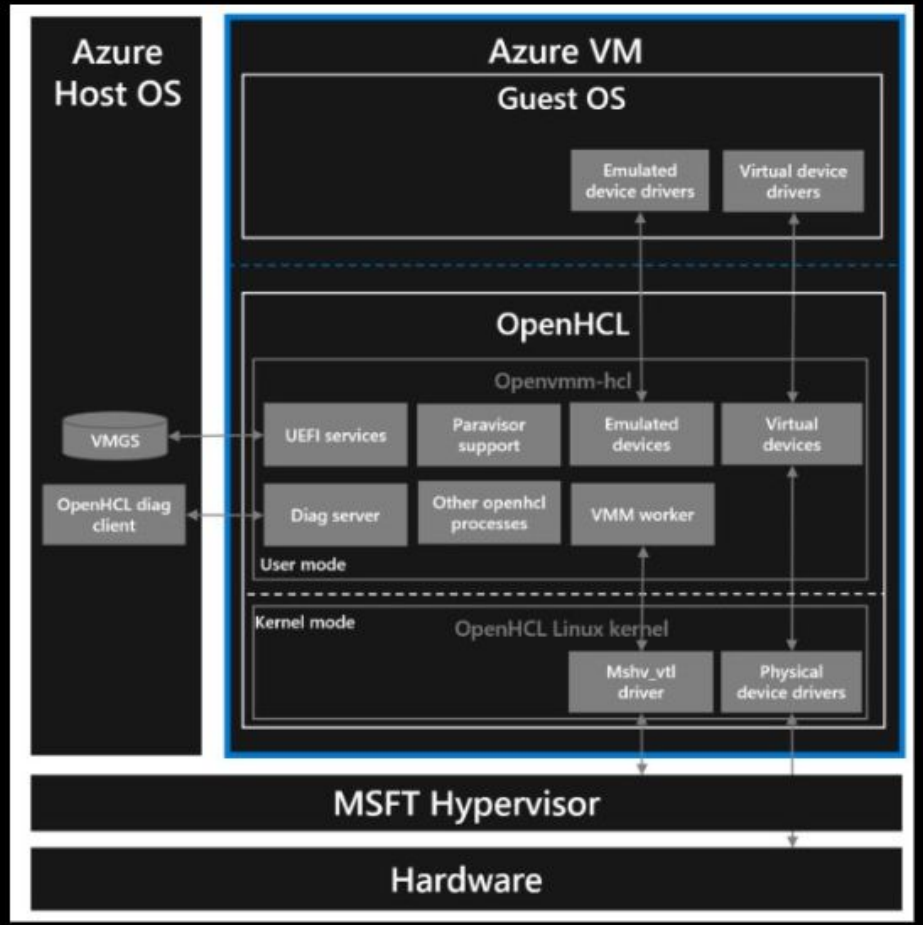
Supports Hyper-V isolation (VTLs) on x86-64 and ARM64, AMD SEV-SNP, Intel TDX

Supports Hyper-V legacy bios, Hyper-V v-firmware and Linux direct boot guests

Old paravisor



OpenHCL paravisor



OpenHCL design philosophy

- Track upstream kernel
  - Aim to upstream all kernel patches or have a path to upstream
- Do as much in usermode as possible
  - Host the VMM itself in usermode
  - Device drivers in usermode
- Do as much in safe idiomatic rust as possible
- Rust async-focused usermode VMM
- Keep VMM code OS agnostic
  - Allows for running outside of OpenHCL

How is OpenHCL different than COCONUT-SVSM?

OpenHCL solves a different problem than COCONUT-SVSM.

COCONUT-SVSM aims to provide services to confidential VMs with fully enlightened guests.

OpenHCL aims to provide services to confidential VMs with guests that are not fully enlightened.