LINUXCON containercon CLOUDOPEN

CHINA 中国

THINK OPEN

开放性思维

ACRN

ACRN™ : A Big Little Hypervisor for IoT Development

Yu Wang, Intel Open Source Technology Center

Key contributors: Anthony Xu; Jason Chen; Eddie Dong; Bing Zhu; Jack Ren; Hao Li; Kevin Tian

LF ASIA, LLC

Table of Contents

What is ACRN?

ACRN™ is a Big Little Hypervisor for IoT Development

ACRN™ is a flexible, lightweight reference hypervisor, built with real-time and safety-criticality in mind, optimized to streamline embedded development through an open source platform

ACRN Features

Small Footprint

- Optimized for resource constrained devices

Real Time

- Low latency
- Enables faster boot time

Built for Embedded IoT

- Rich set of I/O mediators to share devices across multiple VMs

Adaptability

- Multi-OS support for guest systems like Linux and Android

Open Source

- Permissive BSD licensing

Safety Criticality

- Project is built with safety critical workload considerations in mind

Virtualization User Cases for IOT

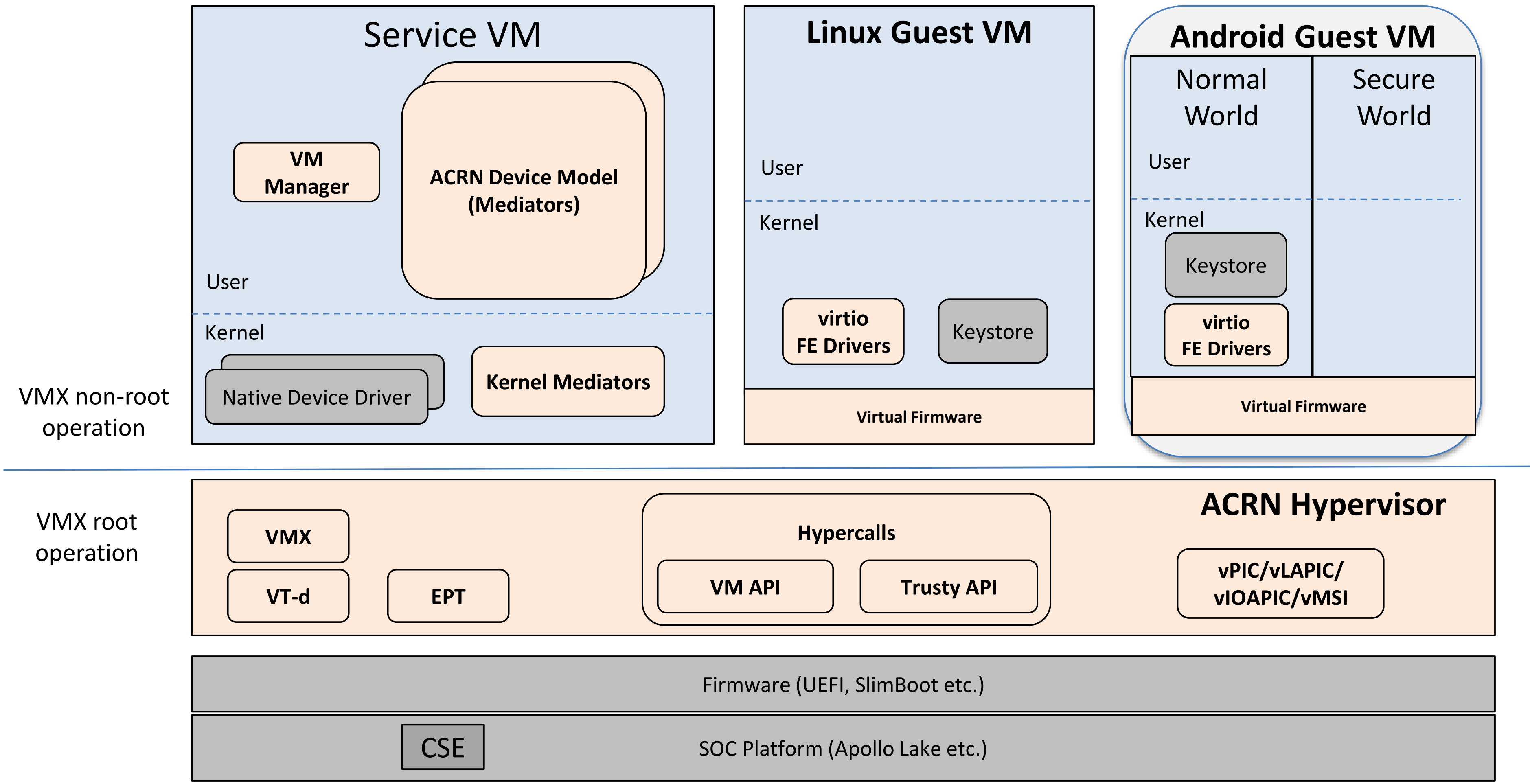
In-Vehicle-Infotainment

Robotics

Precision instrument

Industrial

Architecture Overview



ACRN as a Device Hypervisor

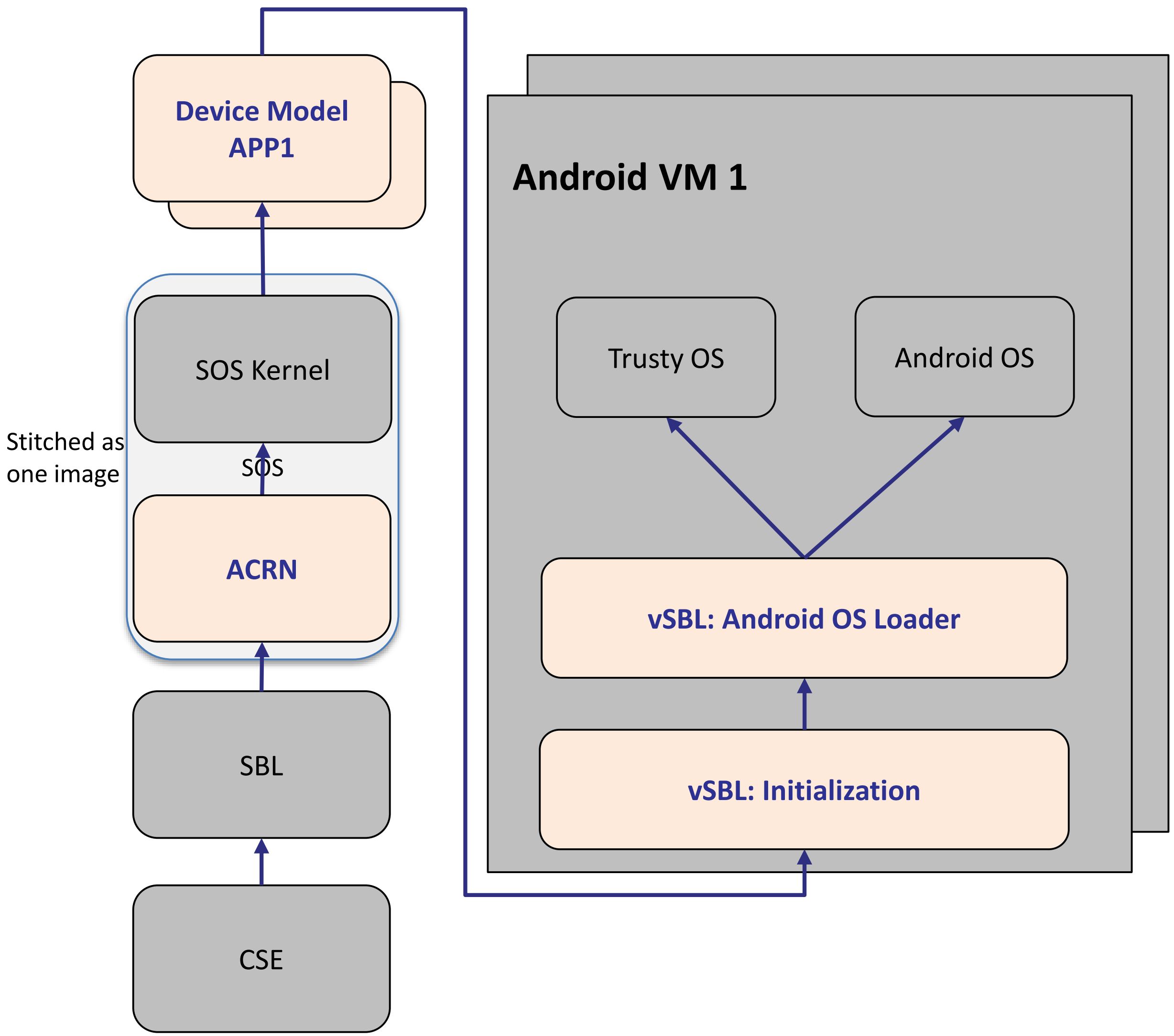
- Small footprint

	KVM	Xen	ACRN
LOC	17M	290K	25K

- BSD licensee
- Be able to cherry pick piece of codes into OSV/OEM’ s own hypervisor
- Verified boot
- Rich I/O mediators

GPU	IPU	CSE	USB	Audio	Ethernet	Block	IOC	Touch
Mediated Passthru	Virtio	Virito	Emu.	Virtio	Virtio	Virtio	Emu.	Virtio

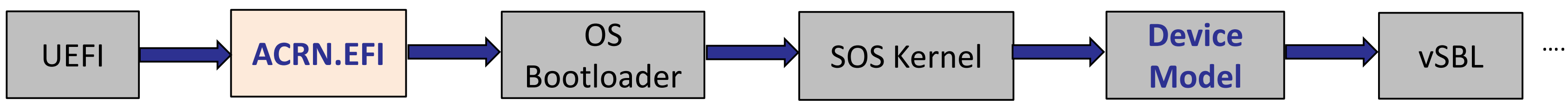
Verified Boot Sequence with SBL



- CSE verifies SBL
- SBL verifies ACRN & SOS Kernel
- SOS kernel verifies DM & vSBL thru dm-verity
- vSBL starts the guest side verification process (reusing the Android verified boot mechanism)

- NOTE: Each user VM has a DM APP instance in SOS

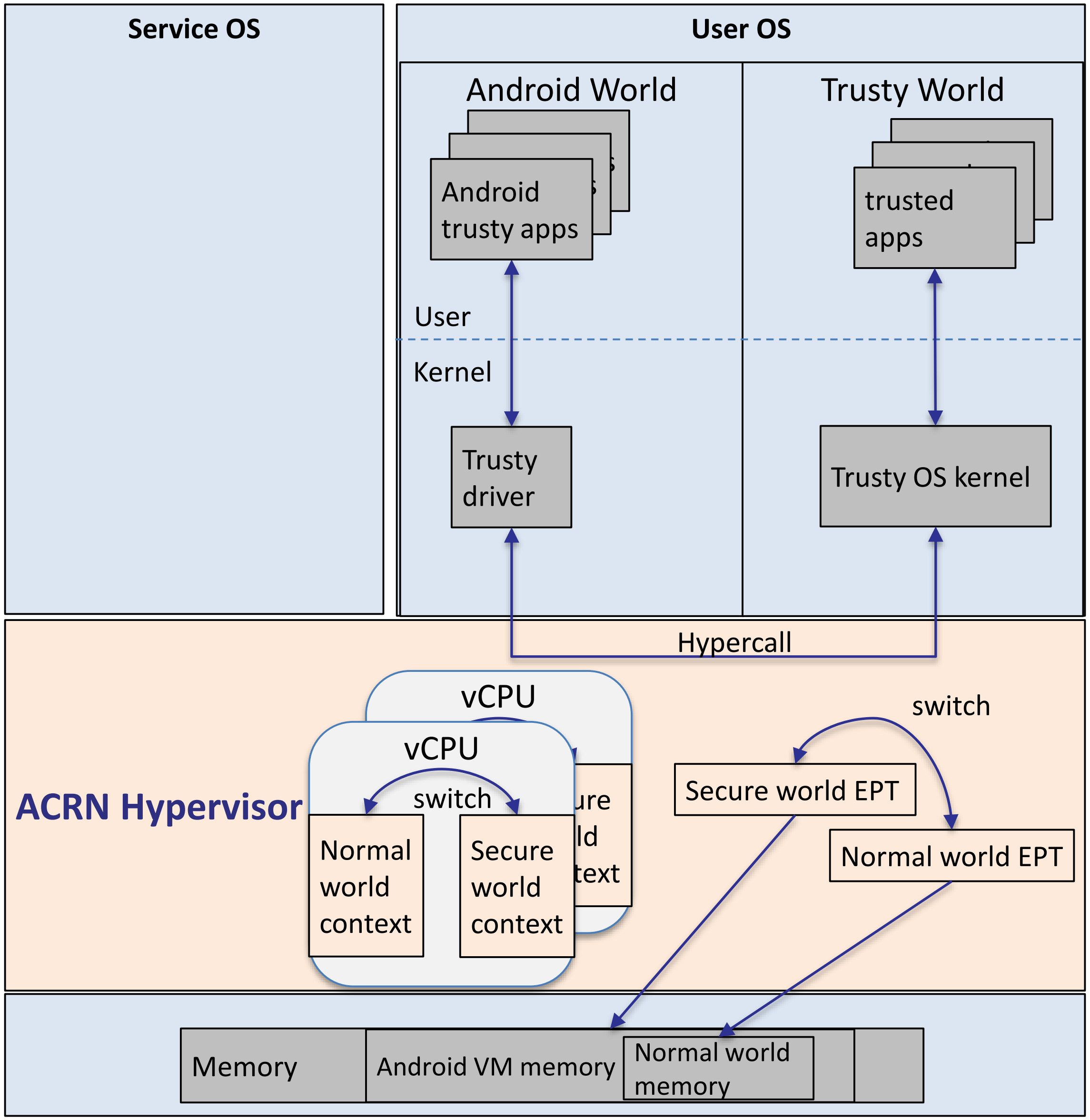
Verified Boot Sequence with UEFI



- UEFI verifies ACRN & OS Bootloader & SOS Kernel
- SOS kernel verifies DM and vSBL thru dm-verity
- vSBL starts the guest side verified boot process

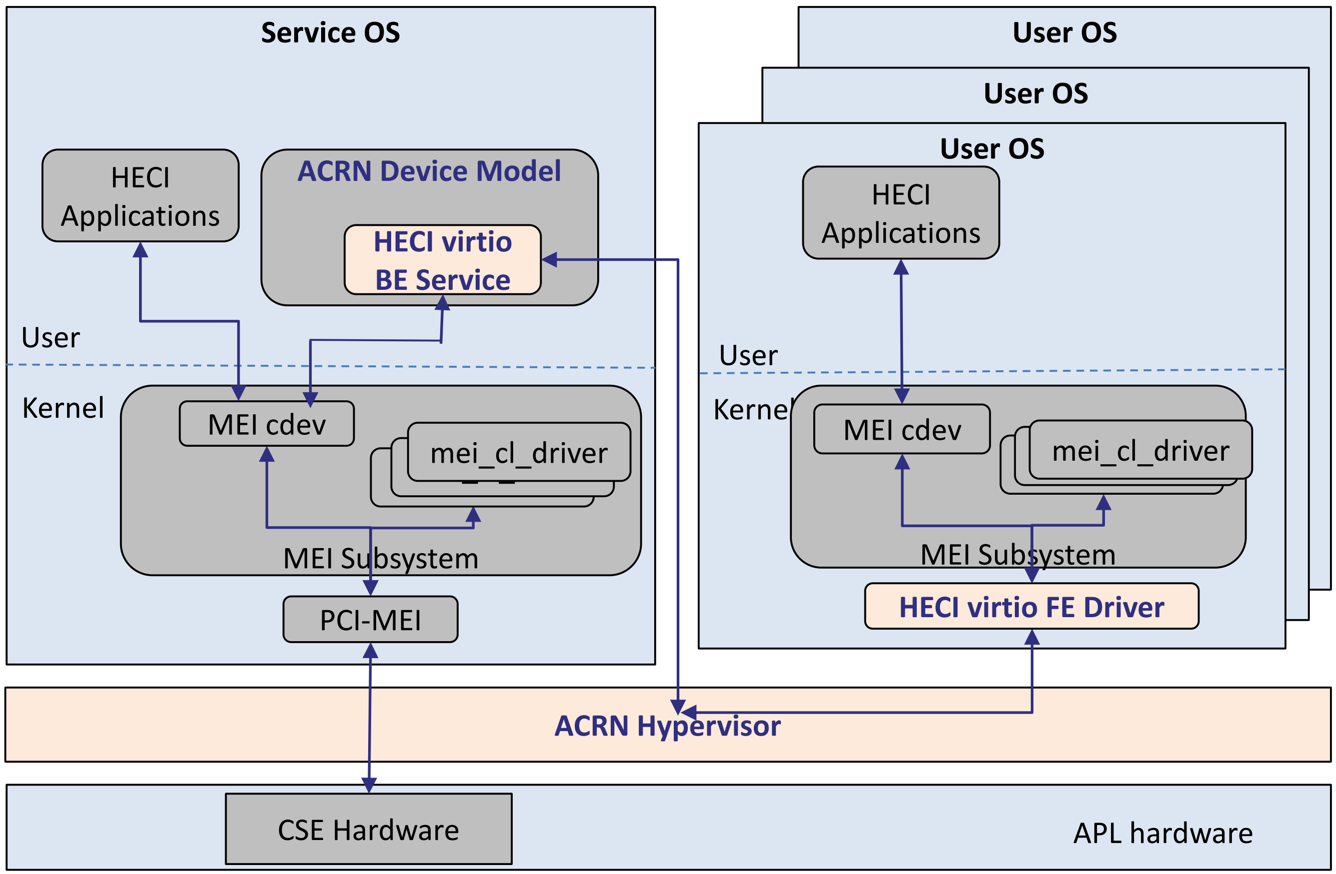
- NOTE: ACRN remains EFI runtime services and boot time services (without interrupt)

Trusty OS virtualization



- Trusty OS is Google released OS for Android secure world which designed to execute in ARM TrustZone mode.
- ACRN hypervisor provide vCPU with different contexts for normal world and secure world. The android OS and Trusty OS can trigger the world switch through hypercall.
- ACRN hypervisor also maintain two EPT tables for different worlds. The secure world memory is invisible for normal world, but not vice versa.

Host Embedded Controller Interface(HECI)



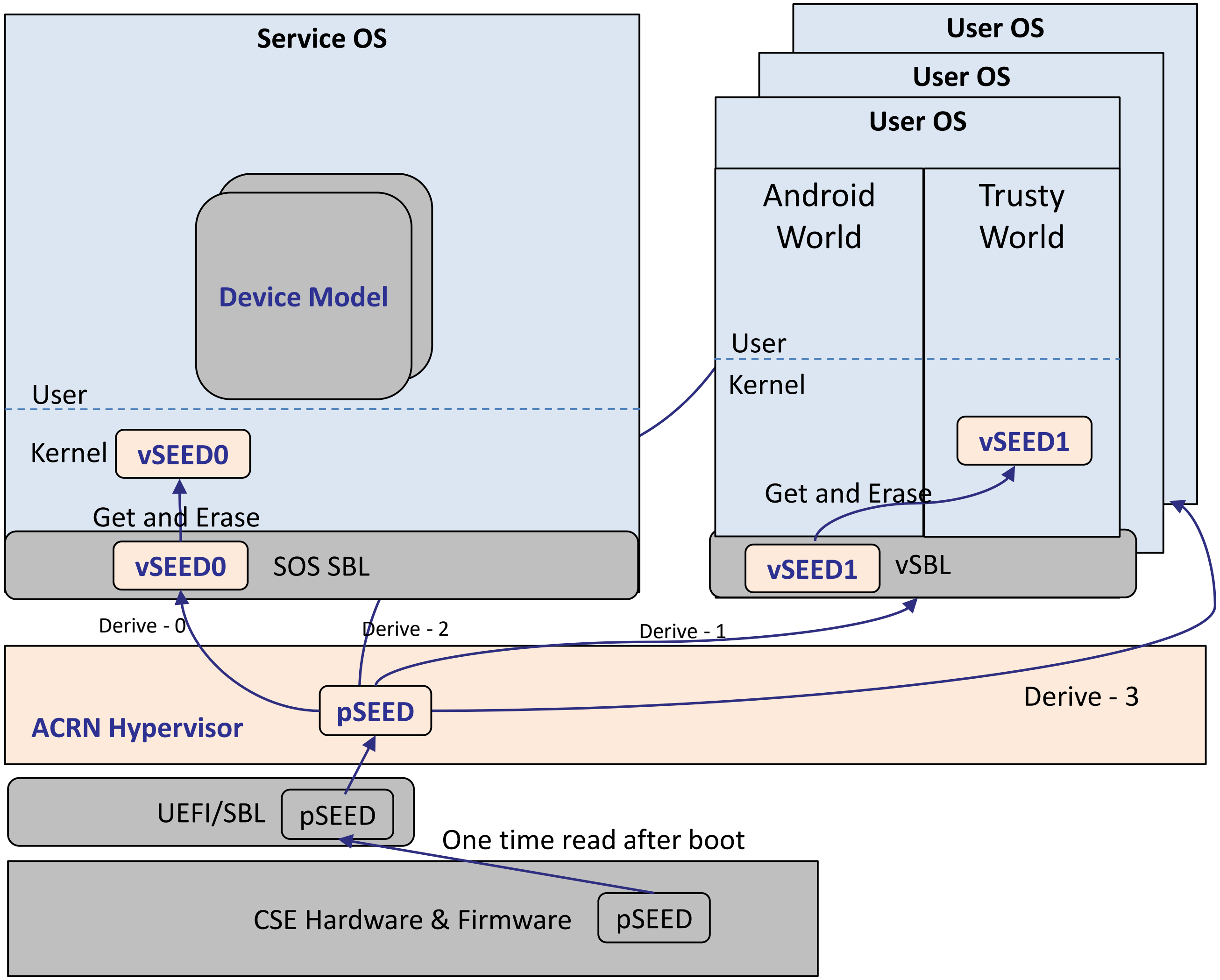
HECI emulator implements a virtio PCIe device to support multiple User OS.

HECI BE will communicate with HECI FE driver to send & receive the HECI messages.

HECI client layer protocol will read/write to SOS MEI cdev directly. And HECI bus messages will emulate in the BE.

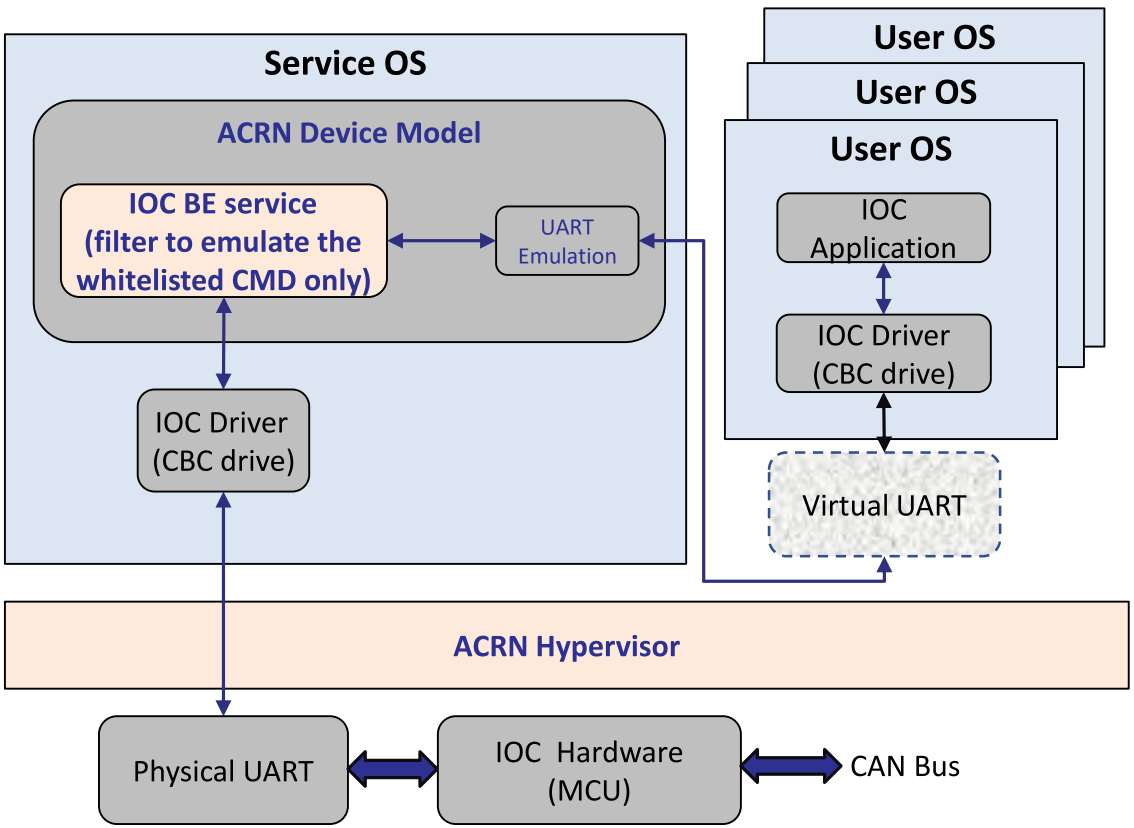
*MEI: Intel Management Engine Interface Linux driver; mei_cl_driver: mei client driver

SEED Virtualization



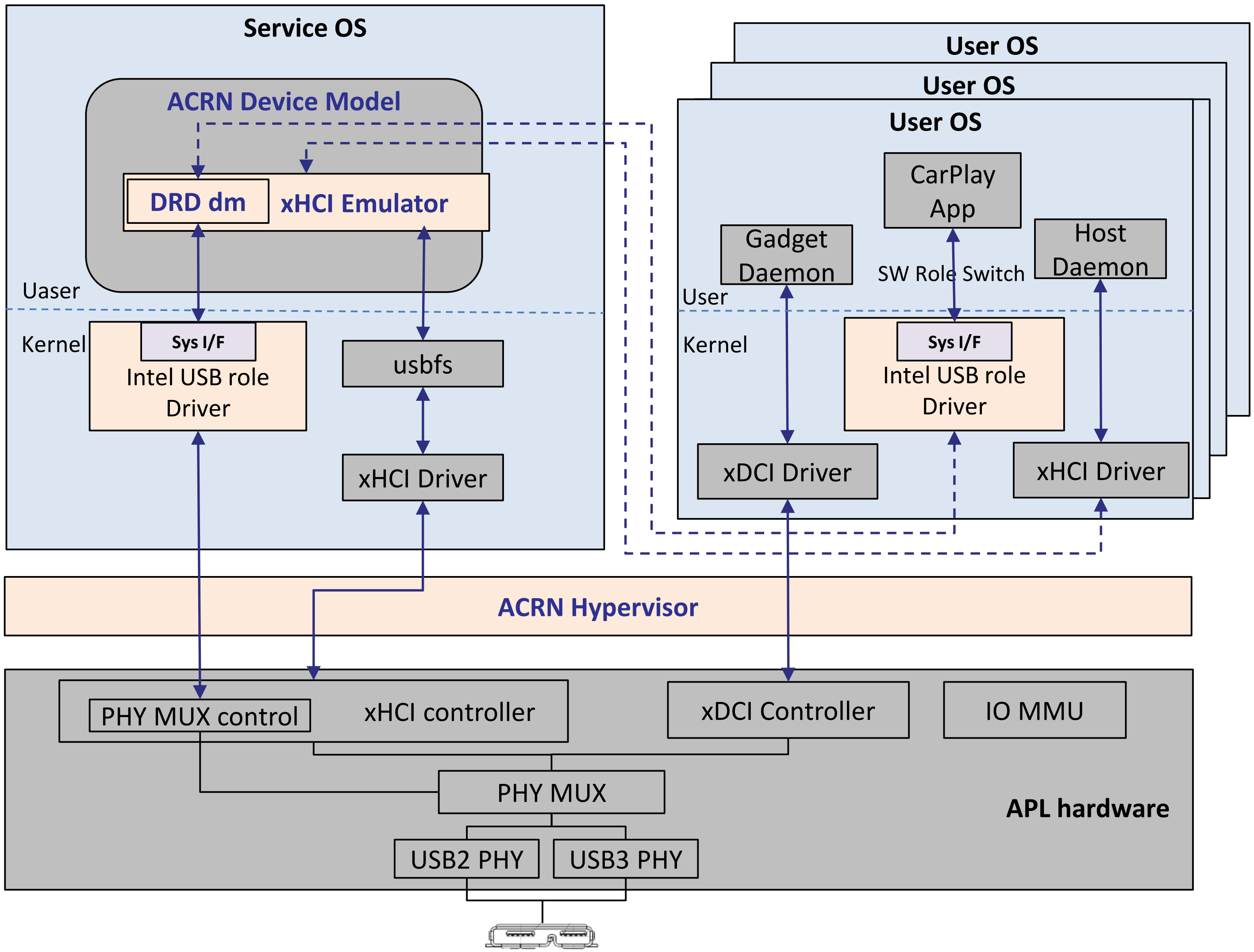
- HV gets pSEED from SBL, which retrieves from CSE through HECI
- Hypervisor implements Key derivation function (HKDF-256) to generate child seeds (vSEED) per request
- Present the derived vSEED to guest VM. Each guest cannot see/derive the other guest’s vSEED

Automotive IO Controller Virtualization



- IOC(IO controller) is a bridge of SoC to communicate with Vehicle Bus. It routing of Vehicle Bus signals(for example, extracted from CAN messages) from IOC to the SoC and back, as well as controlling the onboard peripherals from SoC.
- SOS owns IOC, but UOS may access part features
- Whitelisted CMDs from UOS may be forwarded / emulated
- Support Intel IOC controller only, OEMs may extend

USB Virtualization



xHCI emulator provides multiple instances of virtual xHCI controller to share among multiple User Oss, each USB port can be dedicatedly assigned to a VM.

xDCI controller can be passed through to the specific user OS with I/O MMU assistance.

DRD device model emulate the APL PHY MUX control logic. The frontend re-use the native Intel USB role driver directly which provides sysfs interface to user space of user OS to switch DCI/HCI role in CarPlay SW.

Other mature I/O mediator

- Standard virtio devices
  - virtio storage
  - virtio network
  - virtio console
  - virtio input
- GPU virtualization
  - base on Intel Open Source GVT-g technology

ACRN Roadmap - Proposal

Area	v0.2@Q2'18	v0.5@Q3'18	V0.8@Q4'18	V1.0@Q1'19	V1.x@2019
HW	• APL NUC (UEFI) • KBL NUC (UEFI) • APL UP2 (UEFI)	• APL NUC (UEFI) • KBL NUC (UEFI) • APL UP2 (UEFI)	• APL NUC (UEFI) • KBL NUC (UEFI) • APL UP2 (UEFI)	• APL NUC (UEFI) • KBL NUC (UEFI) • APL UP2 (UEFI)	• APL NUC (UEFI) • KBL NUC (UEFI) • APL UP2 (UEFI) • APL Minnowboard3 (SBL) • ARM
Hypervisor	• VT-x • VT-d • CPU static-partitioning • memory partitioning • Virtio (v0.95) • VHM • EFI boot • ClearLinux as guest	• Virtio (v1.0) • Power Management (Px/Cx) • VM management • ACRN debugging tool • vSBL • AliOS as guest • Zephyr as guest • Logical partitioning without Service OS	• 32bit guest • Guest Real mode • Android as guest • MISRA C compliance • Trusty (Security) • SBL boot *	• vHost • Basic Realtime • Power Management (S3/S5)	• Advanced Realtime • Windows as guest • vxWorks as guest • SGX (Security) • Functional Safety compliance • CPU sharing • ARM
I/O virtualization	• Storage • Ethernet • USB host controller (PT) • USB device controller (PT) • Audio (PT) • WiFi (PT) • Touch (PT) • GPU Sharing	• GPU Sharing • GPU Prioritized Rendering • GPU Surface Sharing • IPU (PT)	• Touch sharing • IOC sharing • Audio sharing • USB host controller Sharing	• IPU Sharing • USB DRD virtualization • CarPlay	• HECI sharing (Security) • CSME/DAL sharing (Security) • TPM Sharing (Security) • eAVB/TSN Sharing • SR-IOV

Call For Action

- Watch, …
  https://github.com/projectacrn/acrn-hypervisor
- … try, …
  https://github.com/projectacrn/acrn-hypervisor/blob/master/doc/getting_started/index.rst
- … and participate!
  https://lists.projectacrn.org/g/acrn-dev/topics

WeChat

WeiBo


LINUXCON
containercon
CLOUDOPEN
CHINA 中国
THINK OPEN
开放性思维
LF ASIA, LLC

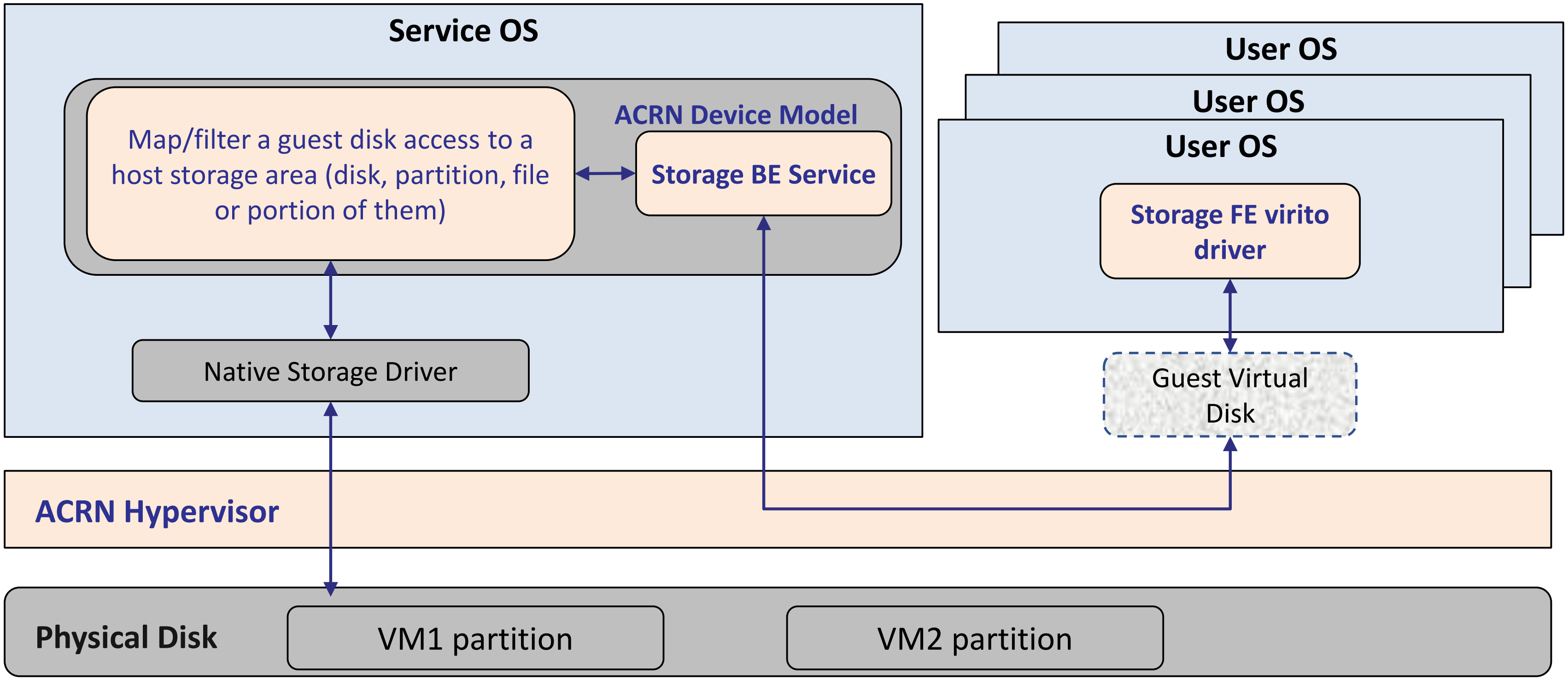
Reference:

- ELC2018 ACRN introduction– Eddie Dong
- Android tamper-resistant anti-replay secure storage solution and its virtualization – Bing Zhu

Backup

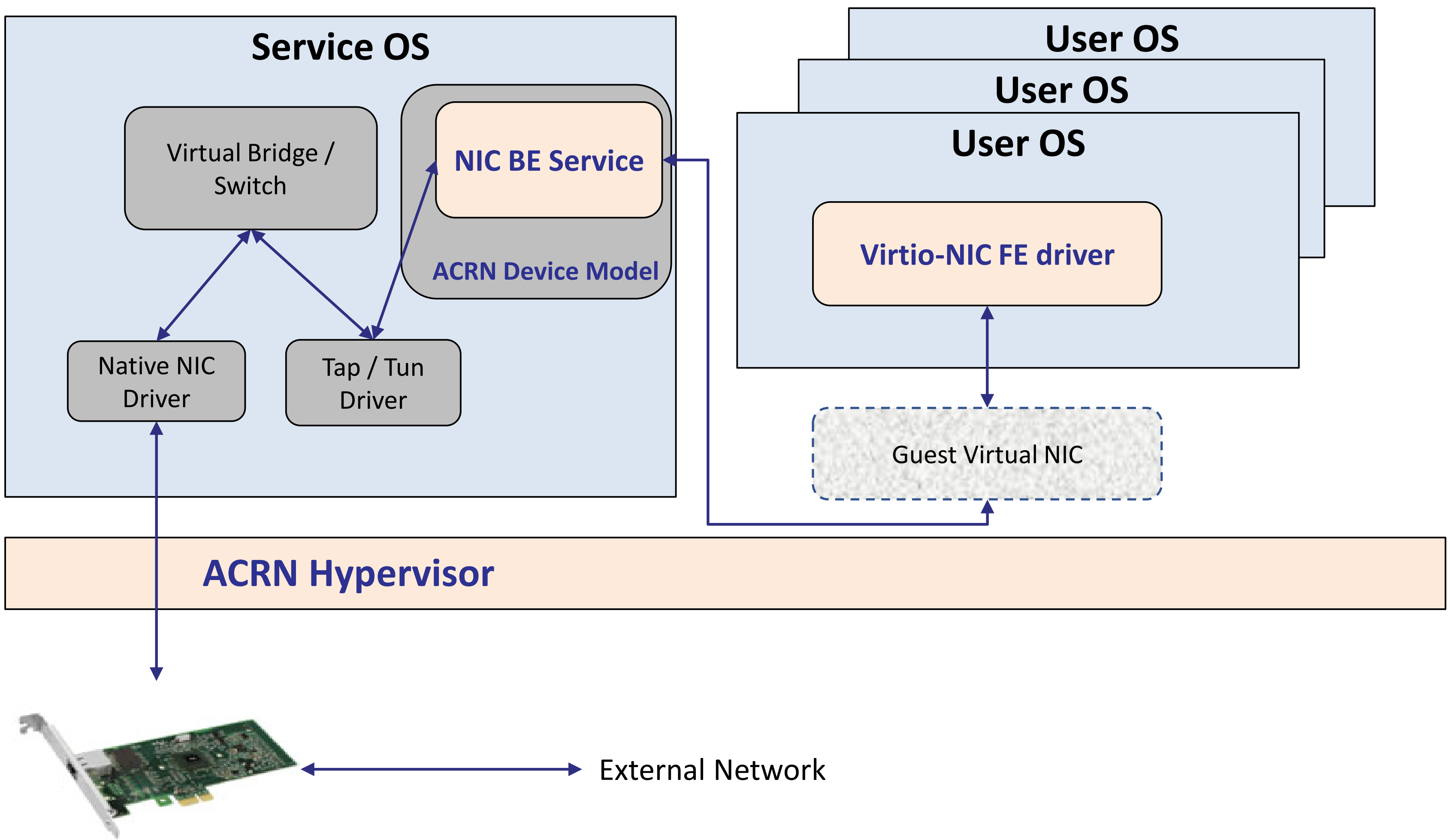
- Storage virtualization
- Network virtualization
- GPU virtualization
- Audio virtualization

Storage Virtualization

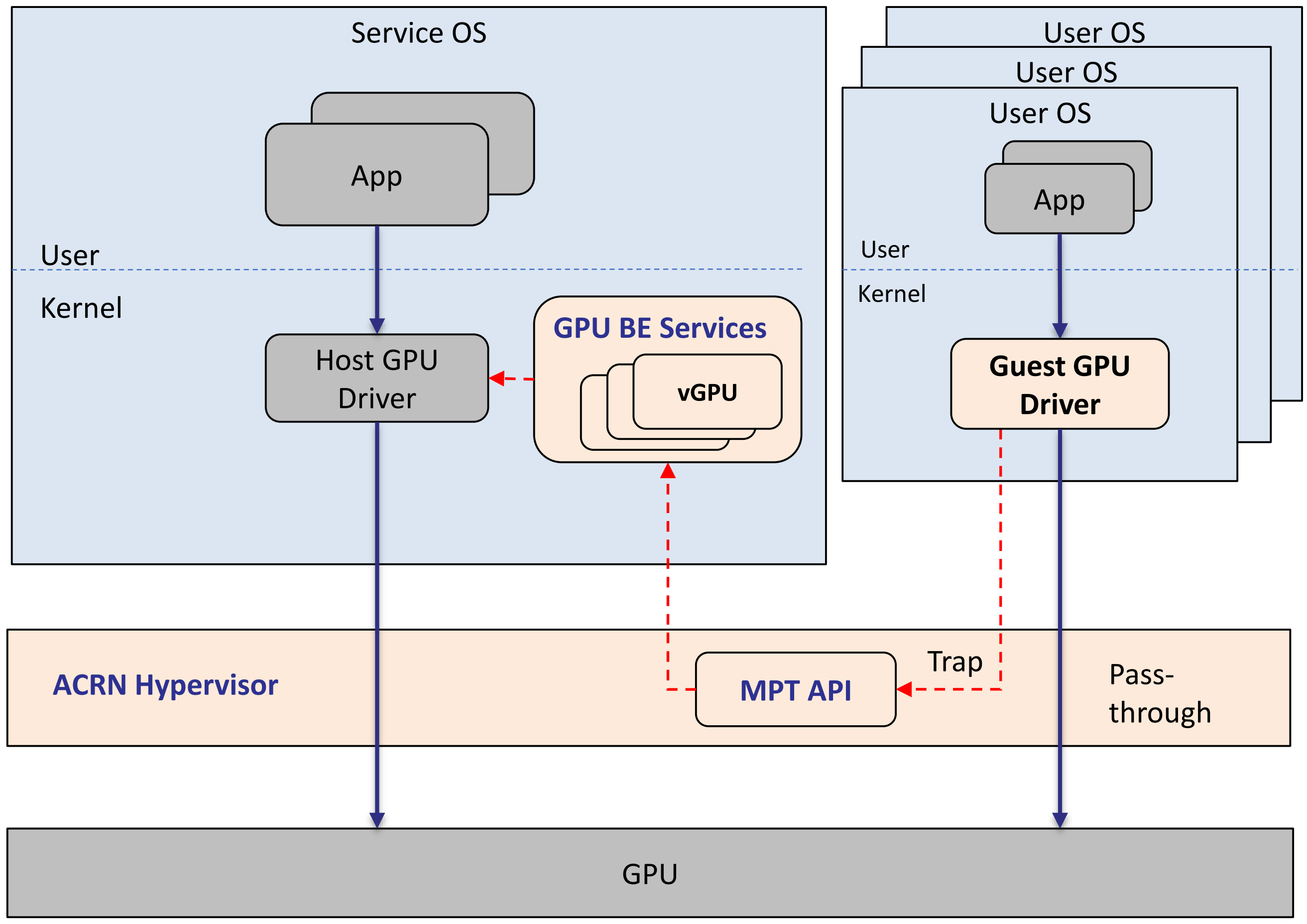


- Map a host storage area (SAR), i.e., disk / partition / file, as a guest disk
- Map a portion of host SAR (start_LBA, size) as a guest disk

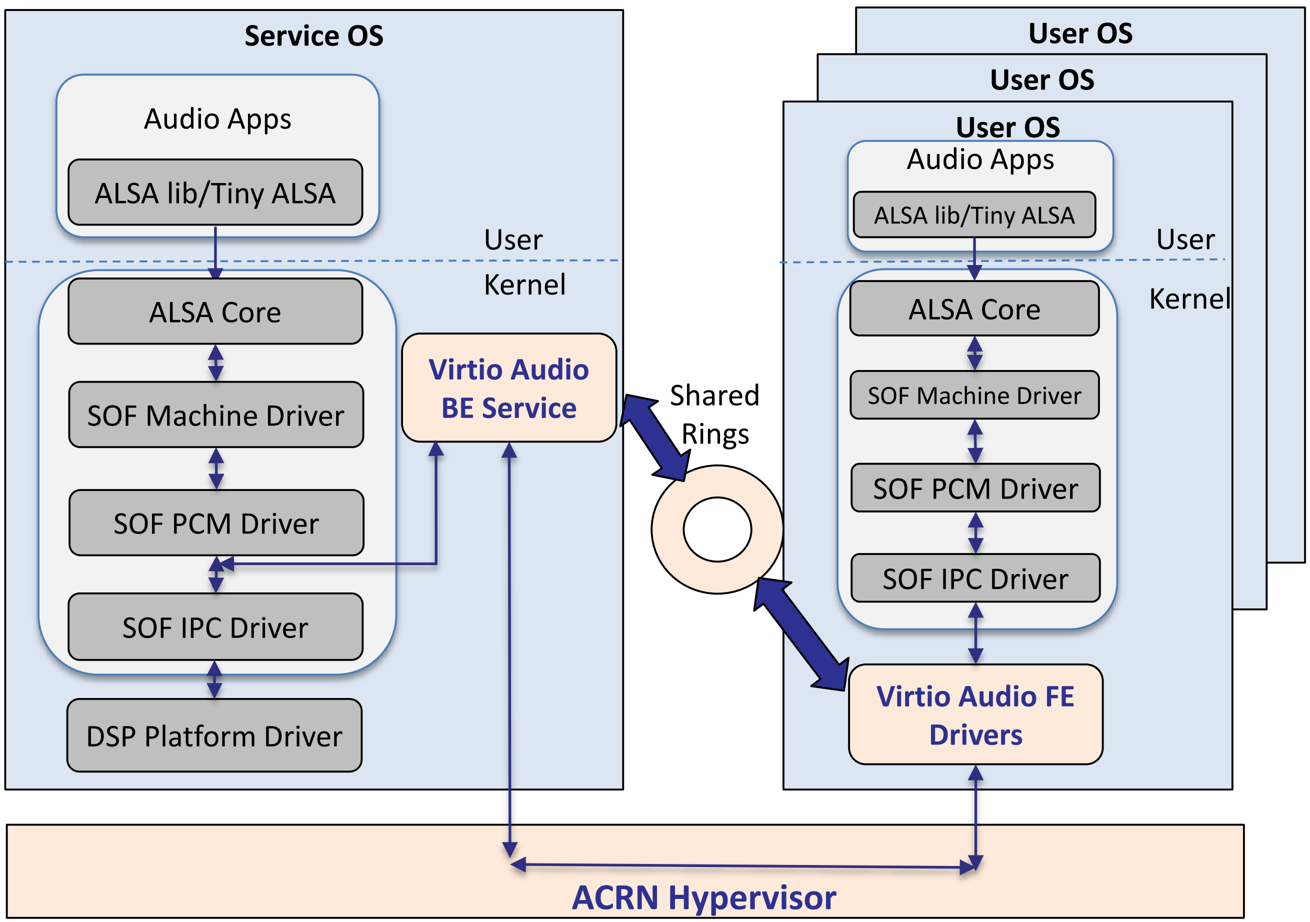
Network Virtualization



GPU Virtualization



Audio Virtualization



ALSA: Advanced Linux Sound Architecture

FE driver communicate with IPC driver thru ops callback of platform driver

FE driver forwards IPC commands to BE service thru virtio shared rings

Service OS can directly access the memory of User OS

BE service communicate with IPC driver thru IPC TX/RX interface of IPC driver

*SOF: Sound Open Firmware; PCM: Pulse-code modulation; IPC: Inter-Processor Communication