Hardware Assisted Virtualization

In the hardware-assisted virtualization technique we try to execute the instructions of the target machine directly on the host processor, as much as possible.

The Virtual Machine Monitor

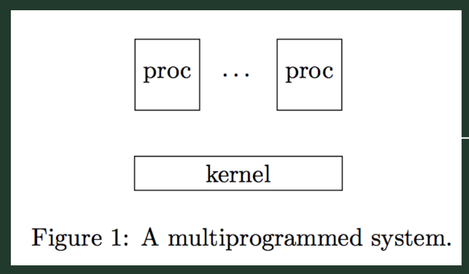

Figure 1: A multiprogrammed system.

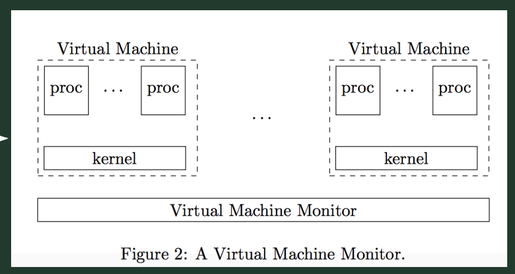

Figure 2: A Virtual Machine Monitor.

Emulating the target CPU ---------- When to trap? any instruction that affects the VMM or the other VMs cannot be directly executed

Emulating the target Physical Memory

Emulating the target I/O devices ---------- Emulating interrupts

The Intel VMX technology

VMX (Virtual Machine eXtensions)

introduces two new operating modes in the Intel CPU

- root mode (根模式适用于在主机上运行的VMM)
  - root/system
  - root/user
- non-root mode (非root模式适用于在虚拟机中运行的guest虚拟机软件)
  - non-root/system
  - non-root/user

The main purpose of these new modes is to put hardware-controlled limitations to the actions performed by the guest system software

Whenever the system code tries to execute an instruction that would either violate the isolation of the VMM, or that must be emulated via software, the hardware can trap it and switch back to the VMM.

enters non-root mode
- **VMLAUNCH** instructions
- **VMRESUME** instructions

returns to root mode ---------- VM exits

Virtual Machine Control Structure (VMCS) ---------- 通常每个虚拟机的每个处理器都有一个

contains all the information needed to manage the new non-root mode

the processor has a register pointing to the current VMCS

VMPTRLD → load the address of a VMCS, making it current

The VMCS data structure has several fields
- Guest state ---------- The state of the processor is loaded from here during a VM enter and stored back here during a VM exit
- Host state ---------- The state of the processor is loaded from here during a VM exit
- VM execution control ---------- specify what is allowed and what is not allowed during non-root mode; unallowed actions will cause a VM exit
- VM enter control ---------- contains several flags and fields that determine some optional behaviors of the root to non-root transition
- VM exit control ---------- contains several flags and fields that determine some optional behaviors of the non-root to root transition
- VM exit reason ---------- contain several informations related to the reason that caused the latest VM exit