October 15 - Lecture #6

How do you make a virtual machine on top of a machine?

Process as abstract virtual machine
Software VM e.g. Java
Hardware VM

- Direct execution of all non-sensitive instructions

Virtual machine

Guest OS

VMM

HW

Emulated execution of sensitive instructions

SW emulator

MT xax (system call)

VMM

Set s bit in proc

PC = MT vector

Direct

Fault -> SW emulator

Fault handling
No I/O with this model.

Certain instructions hard for VMX to emulate. Such instructions are semi-supervisor and semi-user mode.

Handling non-virtualizable instructions:
1. Full emulation of kernel code
2. Binary translation + JIT Compiler
guest

load R1 addr
Store R2 addr

guest asks emulated OS

3 - para-virtualization

- efficient guest modification

hypervisor = virtual machine monitor
OS:

\[ \text{K: } \text{read, write} \]

\[ \text{guest OS: } \text{register sys call handler, page fault handler, update VM registers} \]

4 - hardware virtualization
V

k

bit map

VMM: 01141111

Don't do anything, or have VMM handle.