Virtualization

Traditional OS processes

user

int x80
sys 3 ENTER

int x32 ? windows

kernel

exceptions

I/O completion

PF

guest OS

user

"kernel"

page fault

Exception handling

Virtual CPU:

variables: PC, SP, EIPs,...

insn = *PC + r

switch (insn)

case MOV:

case SMP:

mov CR3

if (s)

else

Bochs emulator

simics
if I/O:
    case device1.type:
        emulate dev1
        ...
        case frame buffer
        coords = F(addr)
        display(data, coords) → X....

        page fault handler:
        if addr ∈ {frame buffer}
        update display

        real
        \underline{fault}
        \underline{- int 80}
        \underline{- page fault}
        \underline{- privileged instr}

        emulated (SW)

        mem[7:0]
virtualizable CPU
IBM mainframe (370?)

68000
8086

VM
hypervisor

user

Popek & Goldberg
FY

all sensitive instructions in user mode must trap
sensitive instruction behaves differently in U, is made innocuous
Virtualizing the unvirtualizable

1) emulate all kernel mode code

HW GOS

u

virtual CPU

BT "binary translation"

2) HW virtualization support

VT & SVM

load k
had cc
trap ?