Notes for 12/7/09

Use cases for virtual machine:

Want to run Windows inside a window in Linux
Want to develop software for multiple operating systems
Want to run, e.g., FreeBSD for research purposes
Save money by having multiple machines on single hardware
Forensics

Benefits of virtual machines:

1. Timesharing
2. Isolation – like how operating systems protect processes from each other, a virtual machine protects operating systems from each other

Performance vs. isomorphism
Performance—want to run close to hardware
Isomorphic—virtual machine states map to physical machine states

Popek/Goldberg theorem
Privileged instructions – if instruction traps kernel if runs in user mode but not in kernel mode
Sensitive instructions – if instruction runs differently in user space than in kernel space
If SI is a subset of PI, then you are OK

For x86, e.g., popf runs differently in user space than in kernel space, but does not trap the kernel if in user space

Intel/AMD virtualization extensions add extra privilege modes in addition to user_mode and kernel_mode, e.g., kernel_mode_but_unprivileged_vm bit

Shadow page table—optimization so that page tables in virtual machine can point to physical addresses on the physical machine

DMA—for a virtual machine to talk directly to an I/O device, you have to give it kernel privileges
Intell/AMD virtualization extensions have IOMMU's to translate virtual I/O addresses to physical I/O addresses

Paravirtualization—give up on making virtual machine be a transparent physical machine for the sake of performance
Xen uses paravirtualization—if you run Xen guest operating system on a Xen host operating, then the guest OS can make performance optimizations