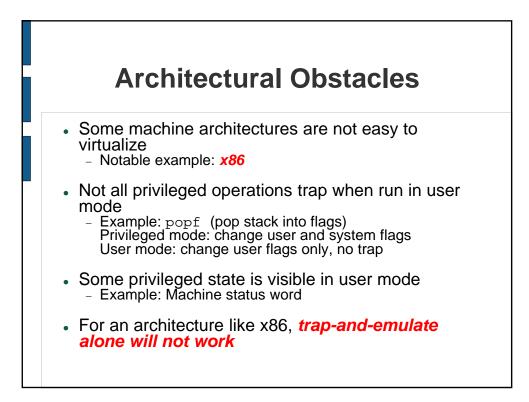


Trap-and-Emulate Virtualization

- Run VMM in privileged mode
- Run OS in user mode
- Privileged operations by the OS will trap
- Trap handler in VMM emulates these operations as if they were run on the virtual machine
- Non-privileged operations can proceed as before with no intervention from the VMM



Virtualization Approaches

Binary rewriting

- Operating system running in VM is *unmodified*
- VMM scans *Guest OS* memory for problematic instructions and rewrites them
- Example: VMware Workstation

Paravirtualization

- Software interface to VMM is not identical to hardware
- Operating systems need to be *ported* to run on VMM
- Simpler VMM and *faster virtual machines* than with trap-and-emulate
- Example: Xen

