Chapter 3
Virtualization

Mastering Cloud Computing

Coleman Kane
(based on material by Paul Talaga)

UNIVERSITY OF Cincinnati

Virtualization

Typically synonymous with *hardware virtualization* and *IaaS.*

Causes for current interest:

- Increased computing power
- Underutilized hardware
- Lack of space
- Greening initiatives
- Rise of administration costs

UNIVERSITY OF Cincinnati

Characteristics of Virtualization

To create a virtual version of something:

- software environment (hardware vm)
- storage
- network (software defined net or VPN)

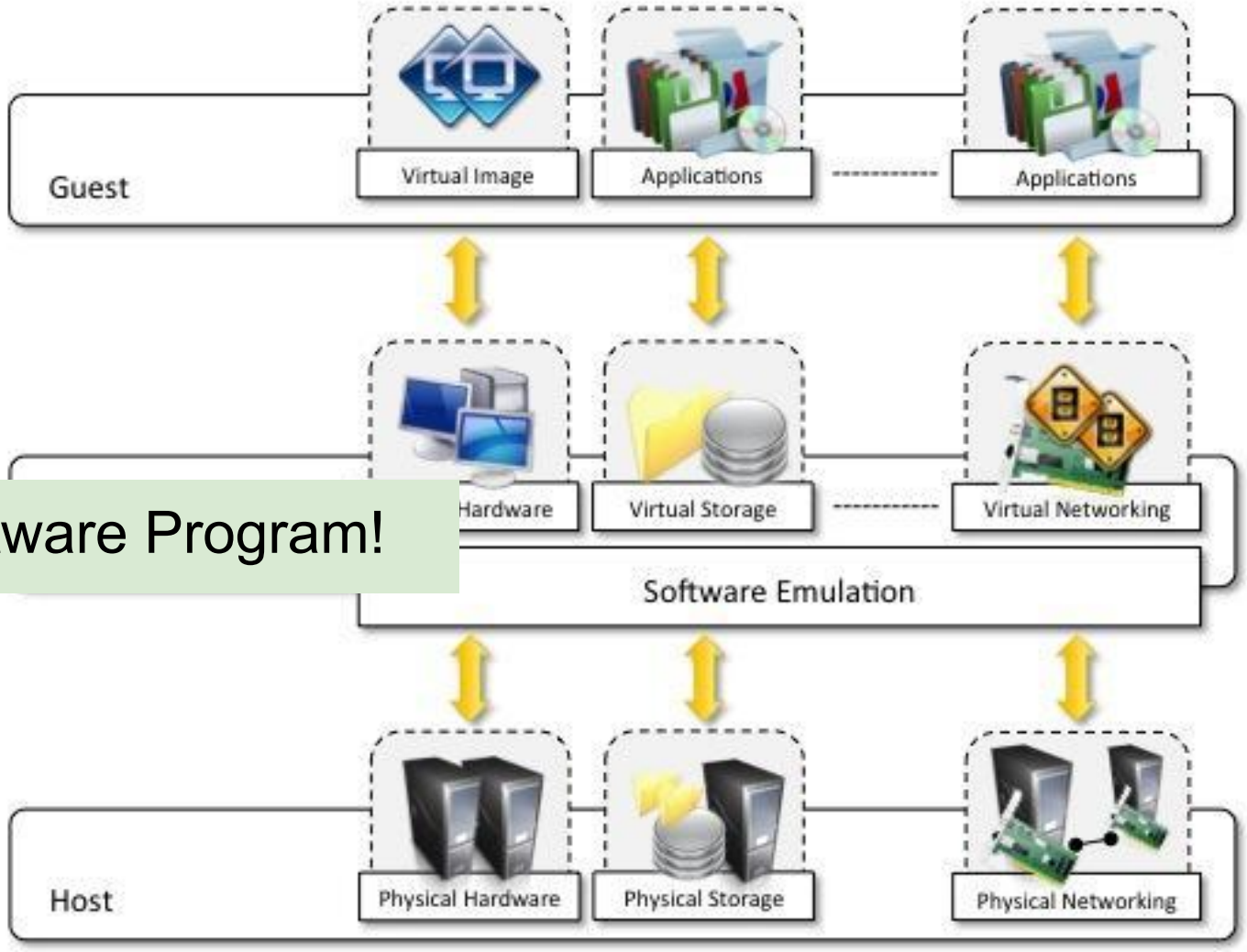
3 Components:

- Guest
- Host
- Virtualization layer

Started with IBM CP/CMS in early 70s

UNIVERSITY OF Cincinnati

A Software Program!



Increased Security

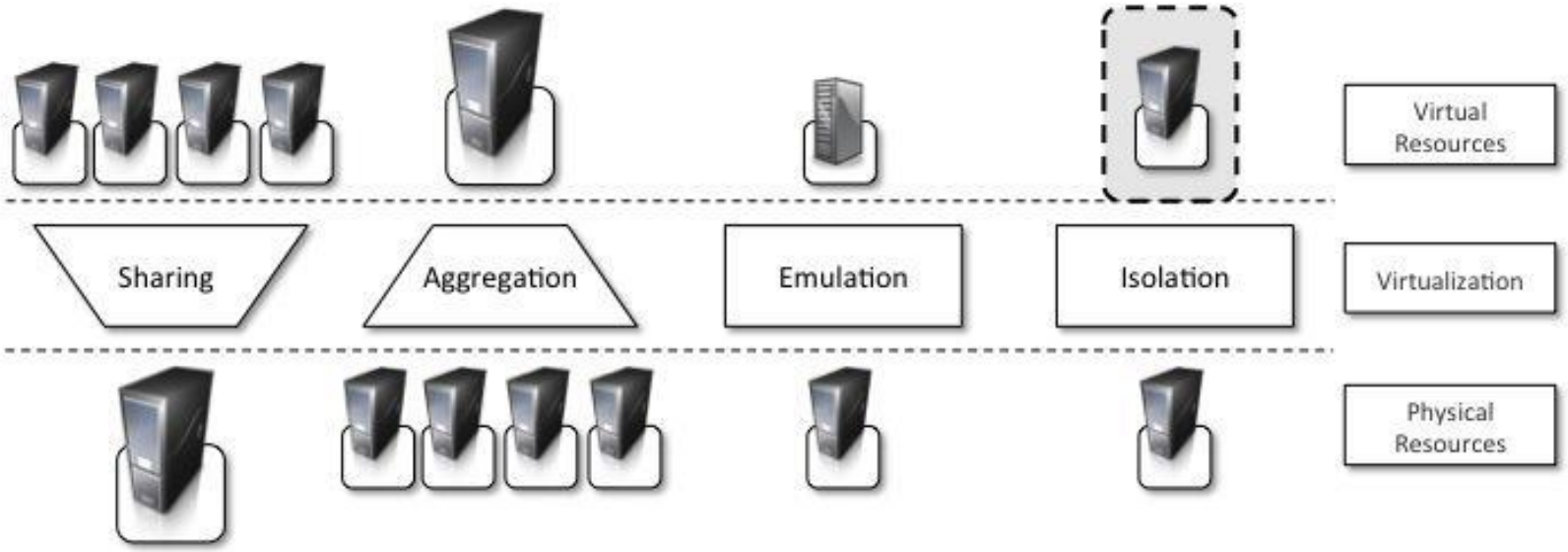
- VM manager can *control* and *filter* activity of the guest.
- Hide information on host
- Sandbox environment (JVM & .Net)
- Adjacent virtualized hosts can't spy on each other (ref, ref)

UNIVERSITY OF Cincinnati

Managed Execution

Additional features:

- Sharing - better utilization
- Aggregation - many looks like 1
- Emulation - provide different hardware to host
- Isolation - security



Other features

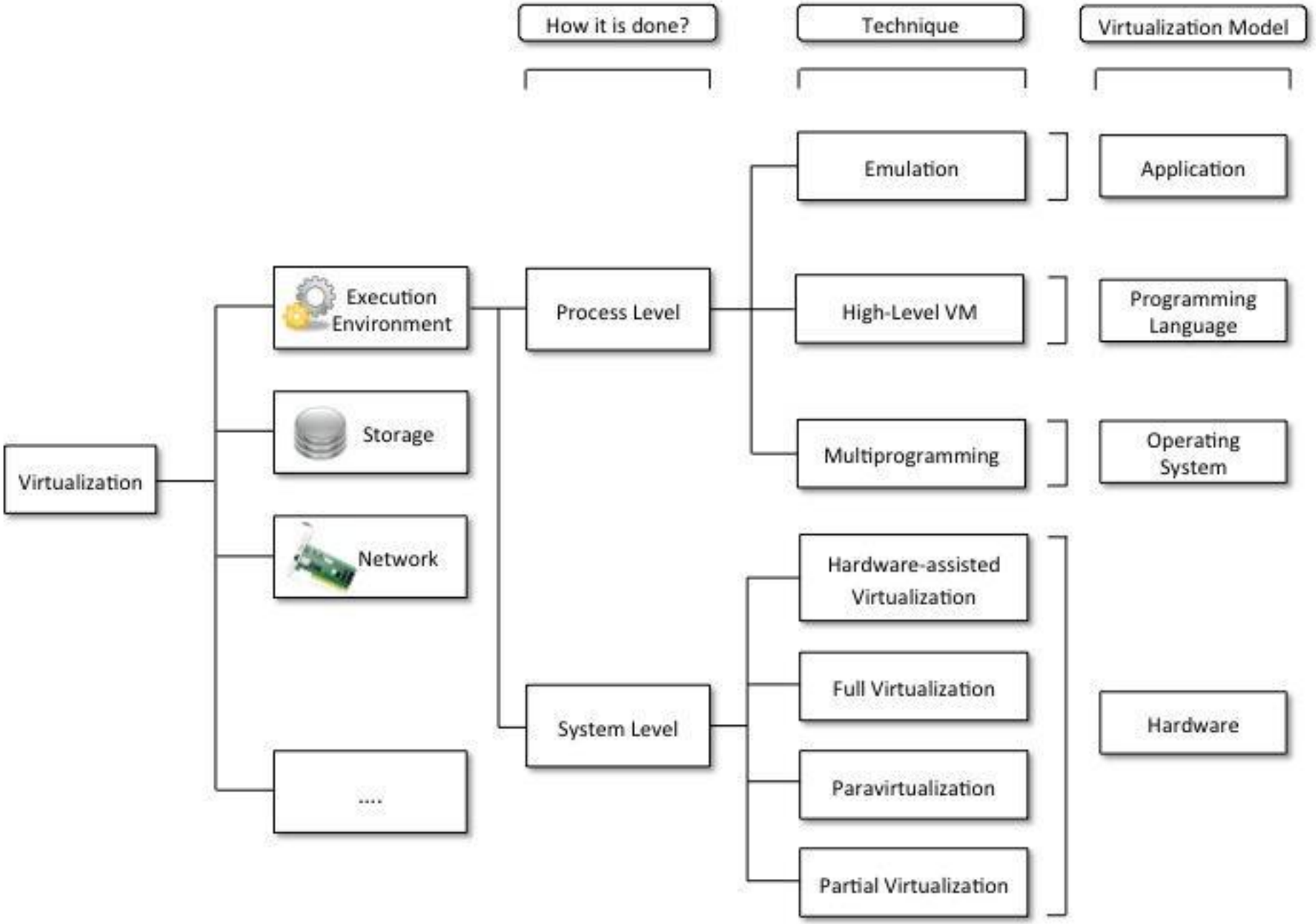
- Performance tuning - tune host for optimal performance - expose custom hardware to guest
- VM snapshots - pausing - saving - resuming
- VM migration - move a vm from one host to another, sometimes *while running*
- Portability - move VM from host to host

UNIVERSITY OF Cincinnati

Virtualization Taxonomy Execution Virtualization

2 Main categories:

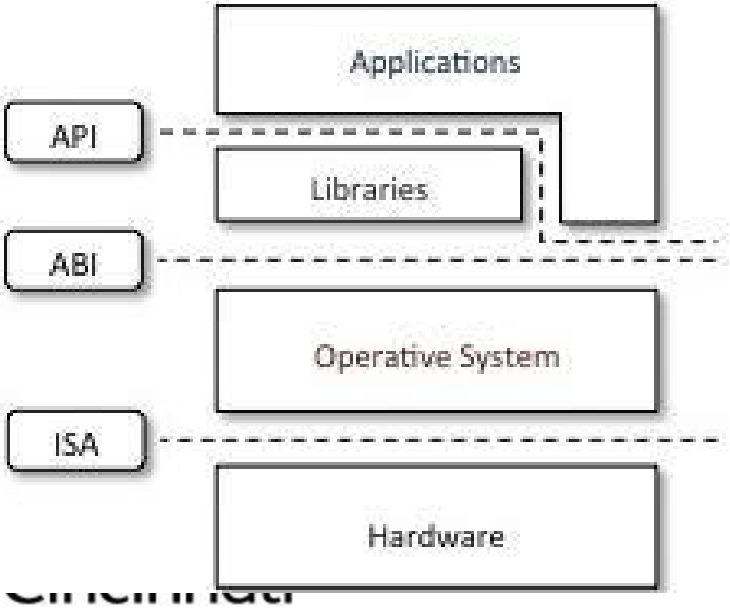
- Process-level - on top of an existing OS
- System-level - Directly on hardware or minimal OS support

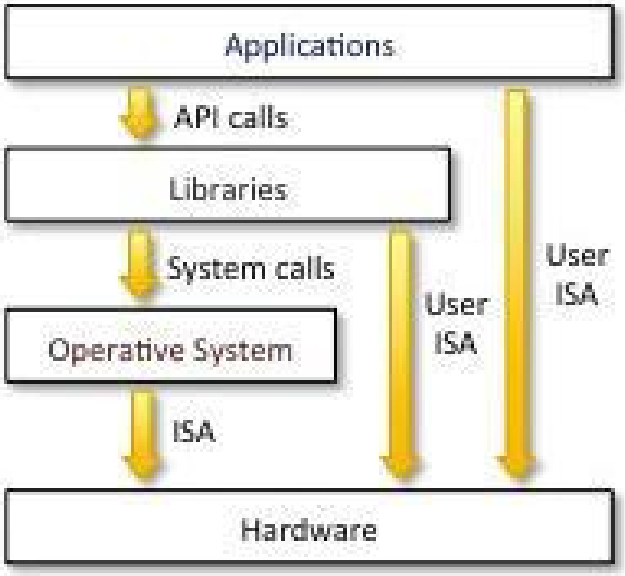

How it is done?
Technique
Virtualization Model
Virtualization
Execution Environment
Storage
Network
....
Process Level
System Level
Emulation
High-Level VM
Multiprogramming
Hardware-assisted Virtualization
Full Virtualization
Paravirtualization
Partial Virtualization
Application
Programming Language
Operating System
Hardware

Machine Reference Model

Defines layer of abstraction

- ISA - instruction set architecture, registers, memory, interrupts
- ABI - application binary interface, data-types, alignment, system-calls
- API - application programming interface, libraries and underlying OS





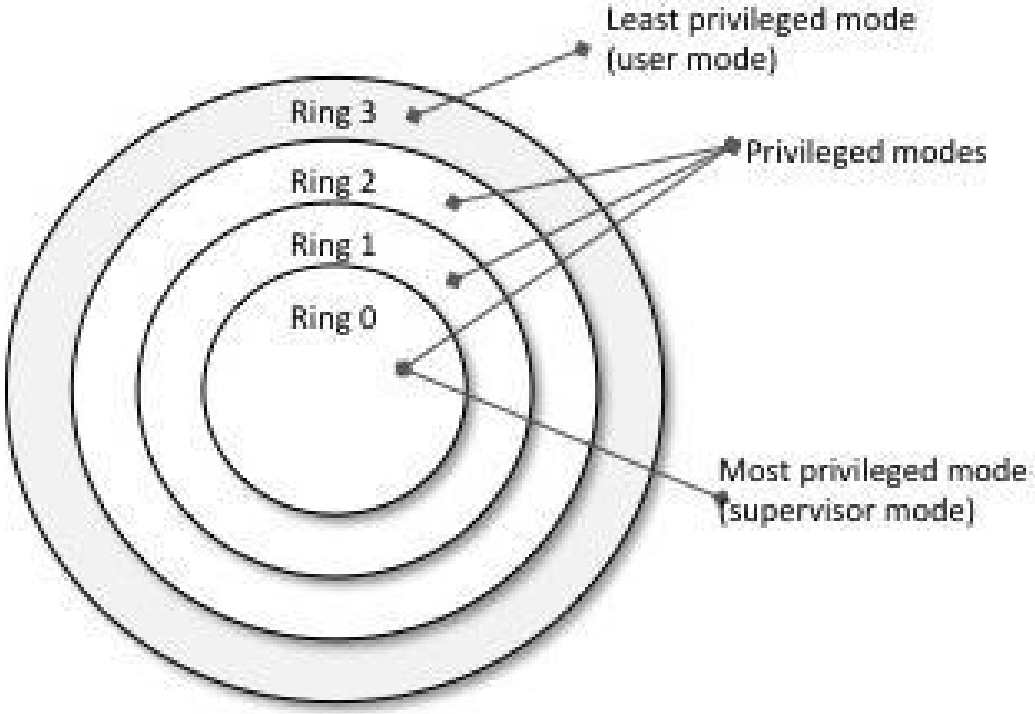
Layered Approach helps with Security

Hardware can allow different layers to execute different instructions.

- Privileged - change shared resources - IO and register changing instructions
- Nonprivileged - safe - don't access shared resources - math instructions

UNIVERSITY OF Cincinnati

Ring for Hierarchy of Privileges



Most recent systems only support 2 levels: Ring 0 for supervisor mode, and Ring 3 for user mode.

UNIVERSITY OF Cincinnati

Current Systems & Hypervisor

Use only 2 levels:

- Ring 0 - supervisor mode (kernel)
- Ring 3 - user mode
  - Sensitive instructions cause trap to kernel

Virtualization adds a *hyper*visor over Ring 0 - in reality they run at same level

BUT - how to isolate different OSs if they all need access to privileged instructions?

UNIVERSITY OF Cincinnati

Another VM Issue

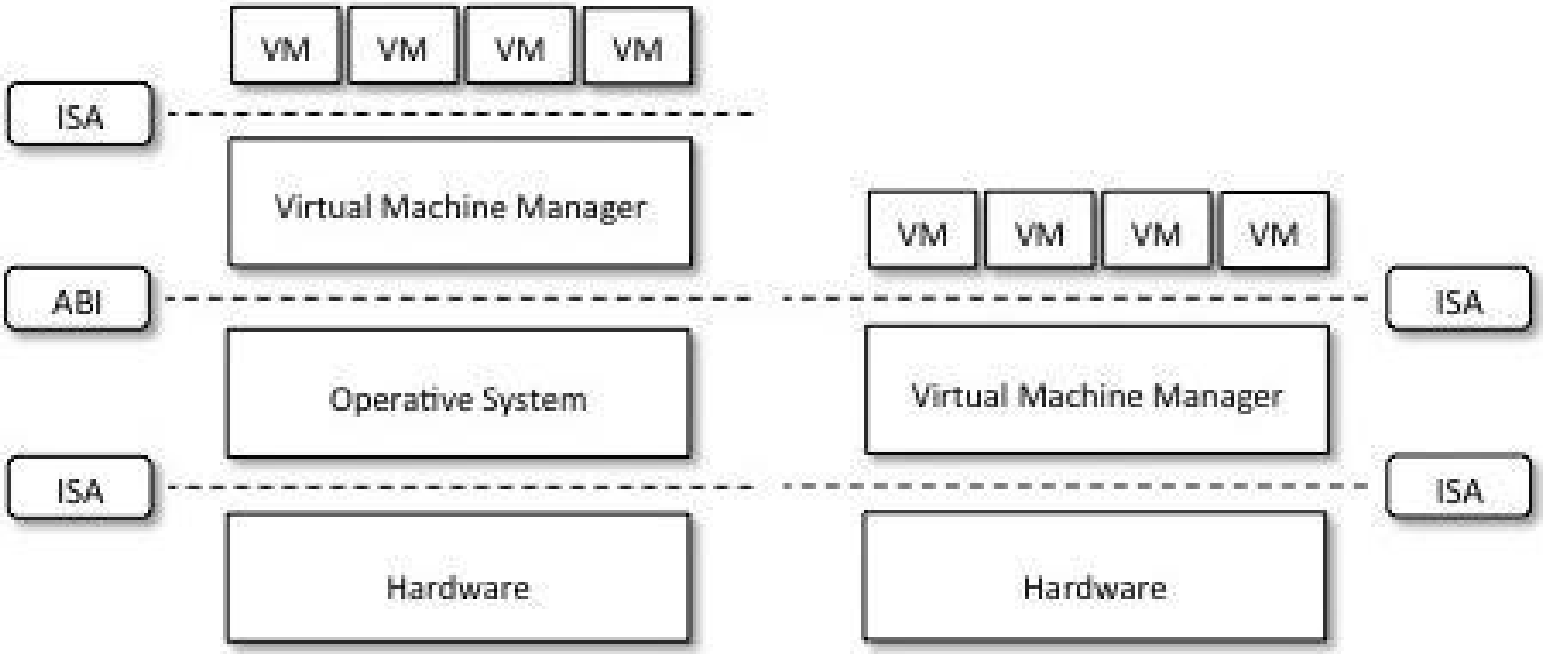
Original ISA had 17 sensitive instructions in user mode - can't cause a trap!

Intel VT & AMD Pacifica moved these to privileged mode.

UNIVERSITY OF Cincinnati

Hardware-level Virtualization

- Virtualizes ISA - *system virtualization*
- Hypervisors manage system - virtual machine manager (VMM)
  - Type I - Runs directly on hardware - *native virtual machine*
  - Type II - Runs in an OS - *hosted virtual machine*



Type Details

- Type I - Runs directly on hardware - *native virtual machine*
  - More resource efficient (no OS in the way)
  - Must reinstall ‘OS’
  - ESX/ESXi just mini version of Linux
  - Ex: VMWare ESX/ESXi, MS HyperV
- Type II - Runs in an OS - *hosted virtual machine*
  - Easier to use, just install the program
  - Ex: VMWare Workstation/Fusion, VirtualBox, Kernel-based Virtual Machine (KVM)

Types are not definitive! KVM uses virtualization features in the kernel, but can do general purpose work. ESX(i?) is linux as well and you can run normal programs.

UNIVERSITY OF Cincinnati

Type II

Type I