Cloud Computing

Introduction to virtualization

Seyyed Ahmad Javadi

sajavadi@aut.ac.ir

Fall 2023

Introduction (cont.)

➢ ***Virtualization*** is often ***synonymous*** with ***hardware virtualization***.

➢ Plays a fundamental role in efficiently delivering ***Infrastructure-as-a-Service (IaaS)*** solutions for cloud computing.

https://www.javatpoint.com/infrastructure-as-a-service

Introduction (cont.)

➢ Virtualization techs have a long trail in the history of computer science.

➢ In many flavors by providing Virtual Environments (VE) at the:

- Operating system level

- Programming language level

- Application level

➢ Virtualization technologies provide a VE for not only **executing applications** but also for **storage**, **memory**, and **networking**.

Amirkabir University of Technology
(Tehran Polytechnic)

Major components of a virtualized environment

➢**Guest**

▪ The system component that interacts with the virtualization layer rather than with the host, as would normally happen.
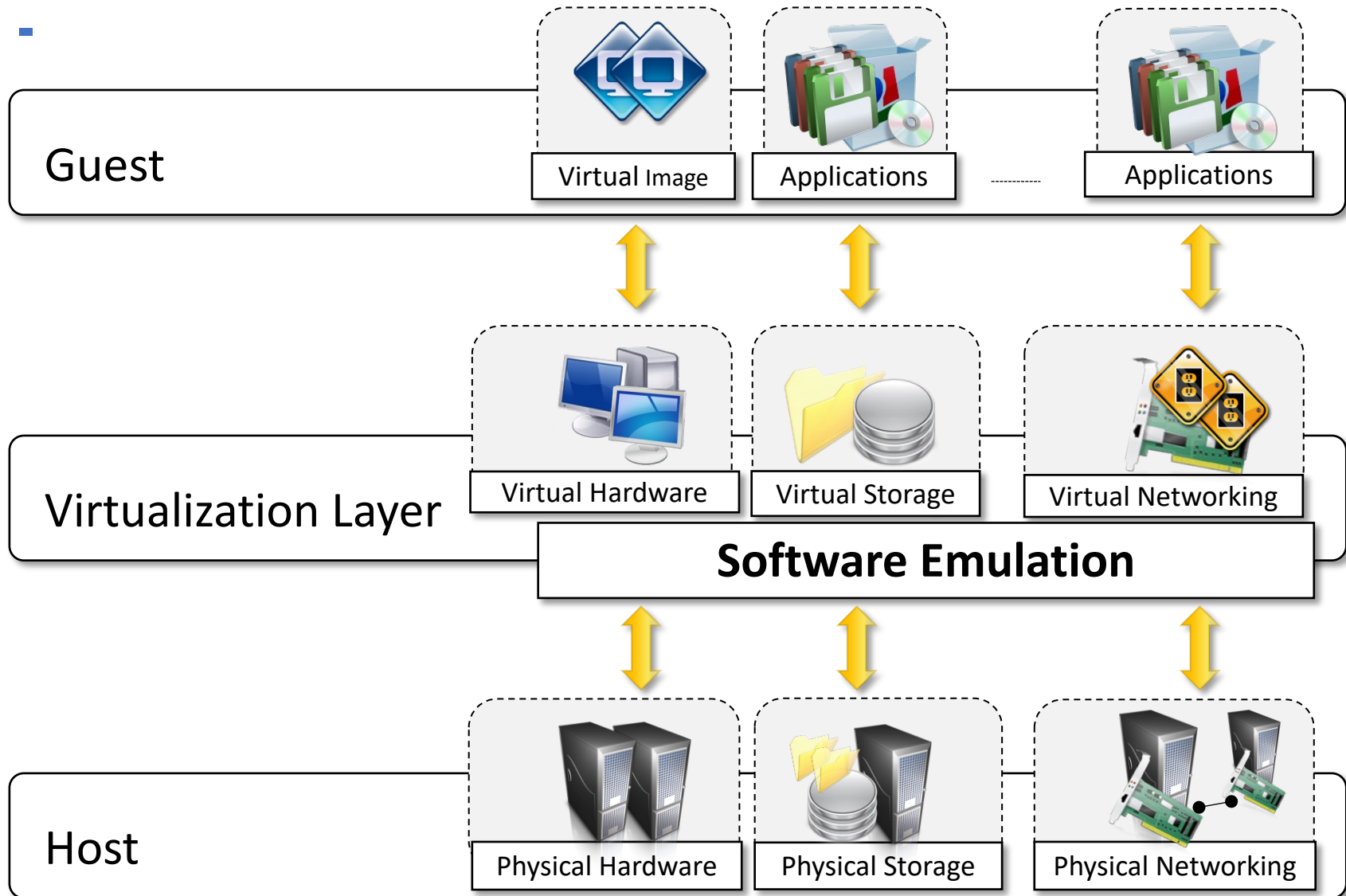
➢**Host**

▪ The original env. where the guest is supposed to be managed.
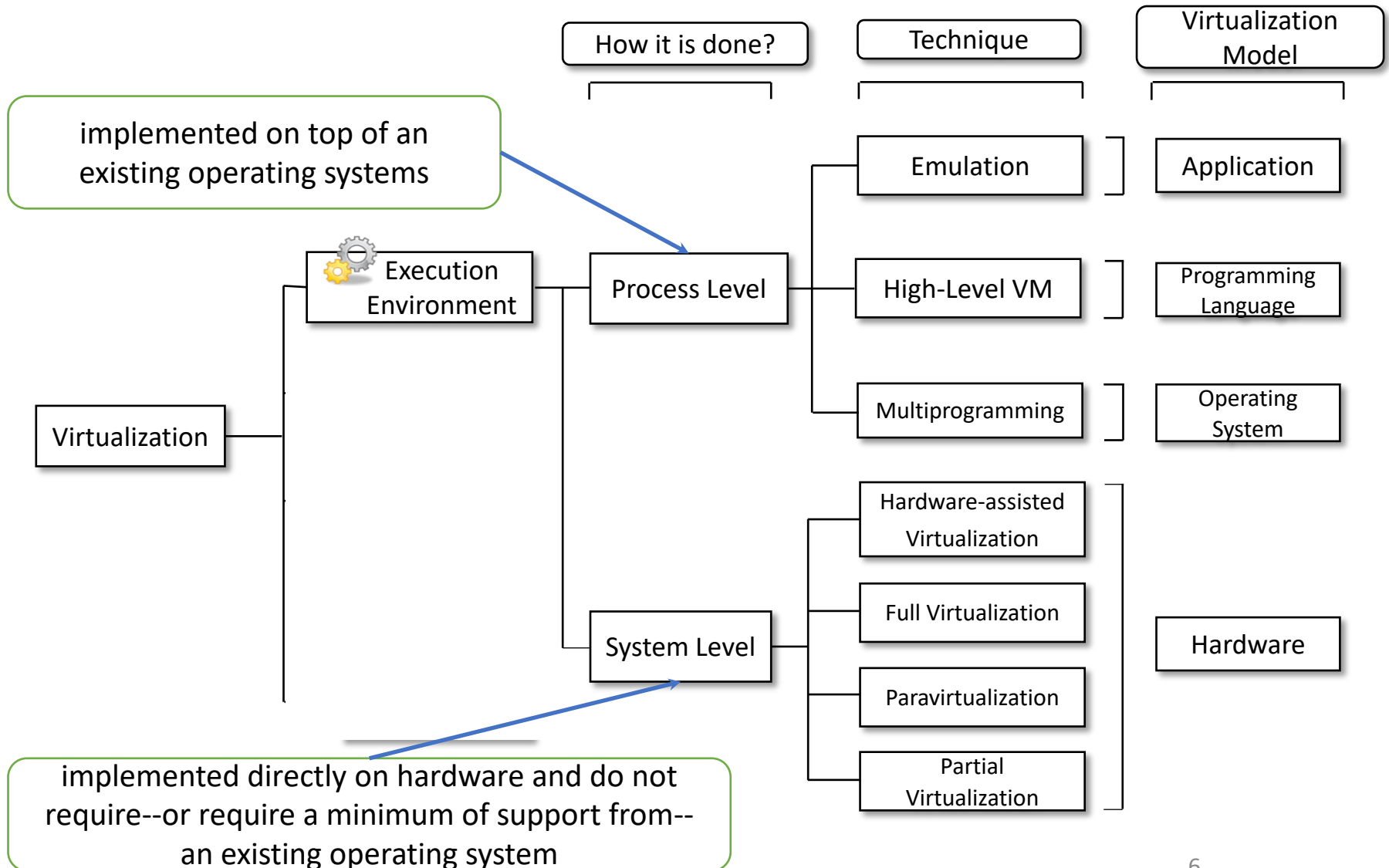
➢**Virtualization layer**

▪ Recreate the same or a different env. where the guest will operate.

Major components of a virtualized environment (cont.)

Guest

| Virtual Image | Applications | ---------- | Applications |

Virtualization Layer

| Virtual Hardware | Virtual Storage | Virtual Networking |

Software Emulation

Host

| Physical Hardware | Physical Storage | Physical Networking |

Amirkabir University of Technology
(Tehran Polytechnic)

Taxonomy of Virtualization Techniques

implemented on top of an existing operating systems

Virtualization

Execution Environment

How it is done?

Process Level

System Level

Technique

Emulation

High-Level VM

Multiprogramming

Hardware-assisted Virtualization

Full Virtualization

Paravirtualization

Partial Virtualization

Virtualization Model

Application

Programming Language

Operating System

Hardware

implemented directly on hardware and do not require--or require a minimum of support from-- an existing operating system

03/12/2023   Principles of Cloud Computing--S.A.Javadi

Taxonomy of Virtualization Techniques

➢ **Execution Virtualization**

  ▪ **Hardware Level**

  ▪ **Operating System Level**

  ▪ Programming Language Level

➢ Network Virtualization

➢ Storage Virtualization

➢ Desktop Virtualization

➢ …

Execution Virtualization

➢ *Emulation of an execution environment (**env.**)*

➢ ***The env.** is **separate** from the one hosting the virtualization layer*.

➢ Providing support for the execution of programs, such as:

- An operating system

- A binary specification of a program compiled against an abstract machine model

- An application.

Machine Reference Model

➢ Consider **different levels** of the computing stack

➢ We need A reference model that defines **the interfaces between the levels of abstractions, which hide implementation details.**

➢Virtualization techniques **replace** one of the layers **and intercept the calls** that are directed toward it.

# Machine Reference Model (cont.)
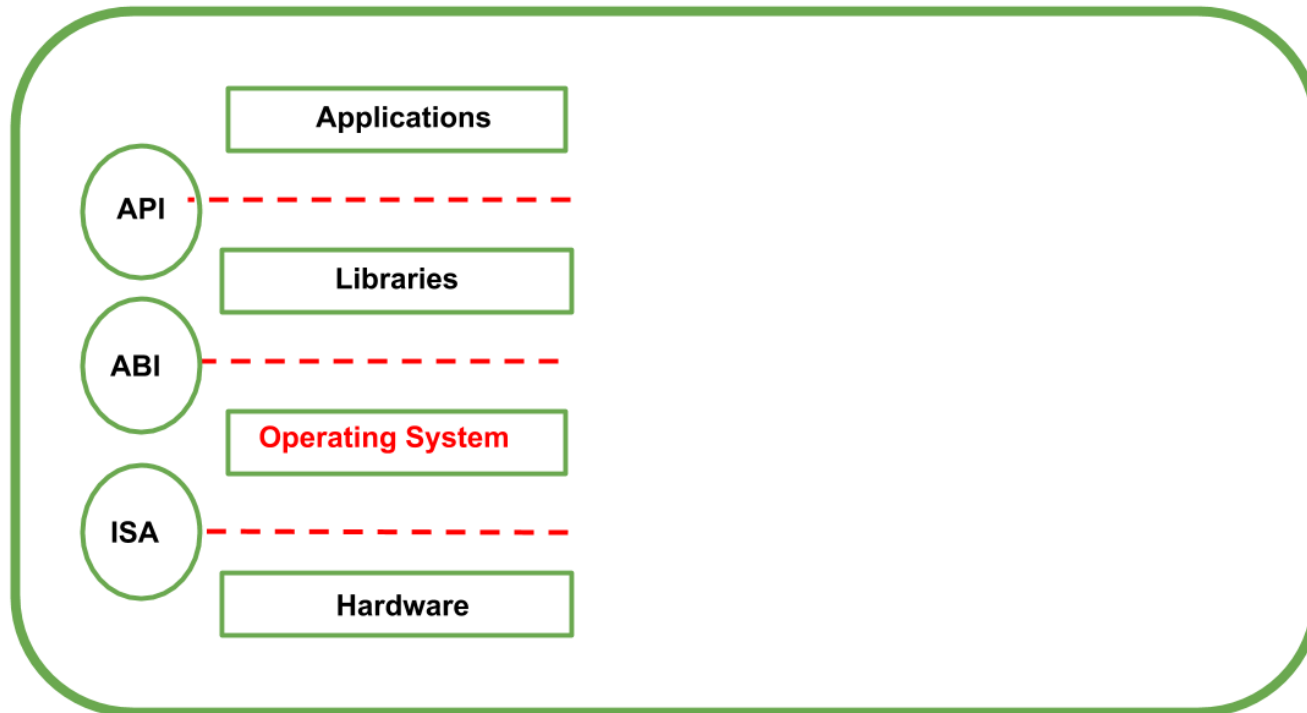
ISA: Instruction Set Architecture

ABI: Application Binary Interface

API: Application Programming Interface

https://www.geeksforgeeks.org/virtualization-a-machine-reference-model/

Machine Reference Model (cont.)

➢ Hardware is expressed in terms of ISA

- ISA for processor, registers, memory and the interrupt management.

➢ ABI separates the OS layer from the application and libraries

- System Calls defined

- Allows portabilities of applications and libraries across OS.

Libraries		Libraries
ABI		ABI
Operating System 1		Operating System 2
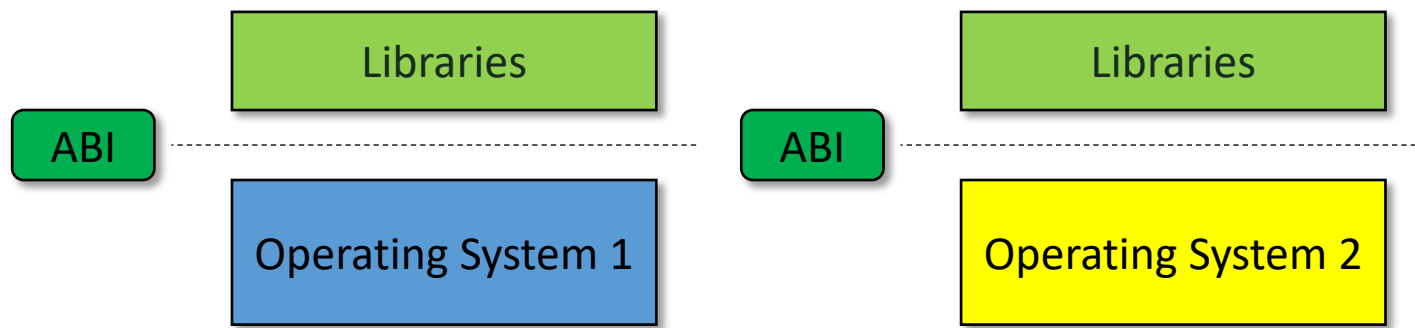
Instruction Set

➢**Non-privileged** instructions

- Can be used without interfering with other tasks.

- They do not access shared resources.

- All the floating, fixed-point, and arithmetic instructions.

➢**Privileged** instructions

- Executed under specific restrictions

- Behavior-sensitive instructions that operate on the I/O.

- Control-sensitive instructions that alter the state of the CPU registers.

Multi-class of privileged instructions

➢ A hierarchy of privileges in the form of ring-based security:

  ▪ Ring 0, Ring 1, Ring 2, and Ring 3.

Amirkabir University of Technology
(Tehran Polytechnic)
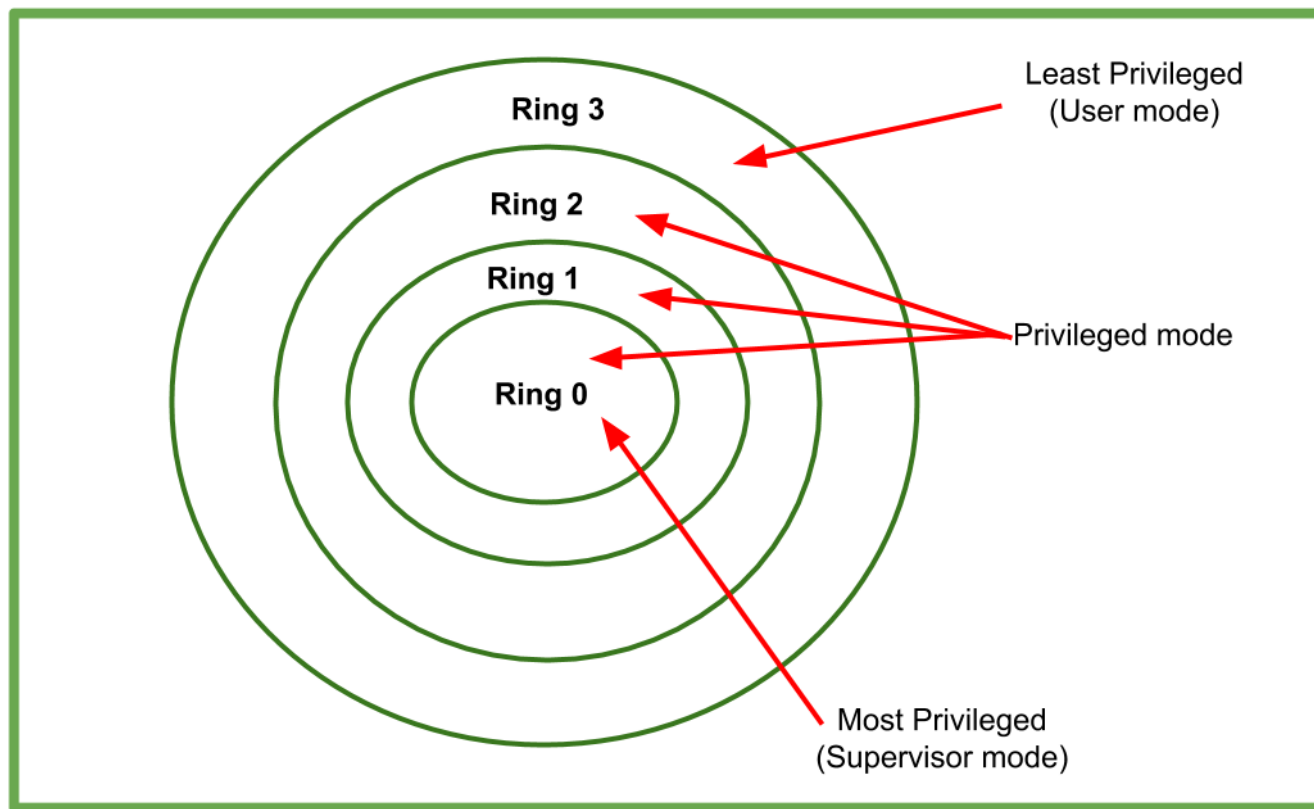
Least execution modes

➢ **Supervisor mode** (master mode or kernel mode)

- ▪ To perform sensitive operations on hardware-level resources.

➢ **User mode**

- ▪ There are *restrictions to control* the machine-level resources.

Least execution modes (cont.)
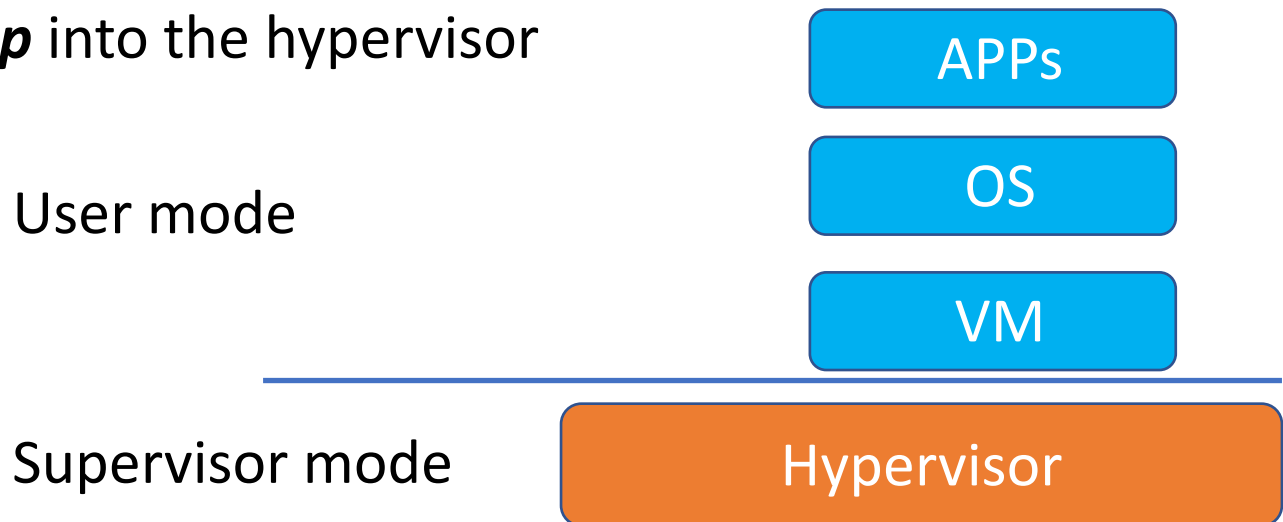
Invoking the privileged instructions is user mode

hardware interrupts occur and trap the potentially

harmful execution of the instruction

Execution Virtualization
What is hypervisor?

➢ **Conceptually**, the **hypervisor runs above the supervisor mode.**

- ▪ From here the prefix **hyper**- is used.

➢ **In reality, hypervisors are run in supervisor mode.**

➢ The division between privileged and non-privileged instructions has posed *challenges* in designing virtual machine managers.

Execution Virtualization
Historical approach for **efficient** virtualization

➤ ***Virtual machine & guest Operating System*** are run in ***user mode***

  - ***Direct execution of non-privileged instructions on the hardware***

➤ ***Hypervisor*** is run in ***supervisor mode***.

➤ Running sensitive instructions in user mode →

  automatically trap into the hypervisor

| APPs |
| OS |
| VM |

User mode

Supervisor mode

| Hypervisor |

Amirkabir University of Technology
(Tehran Polytechnic)

Execution Virtualization
A big challenge

➤ Sensitive instructions *should only be* executed in **privileged mode**.

➤ **Original ISA** lets *17 sensitive instructions* to be called in *user mode*.

➤ *Not able to isolate* multiple operating systems from each other

   ▪ They **can** *access the privileged state of the processor and change it.*

➤ Recent ISA **redesign such instructions as privileged ones**.

   ▪ Intel VT and AMD Pacifica

What is Intel Virtualization Technology (VT)?

➢ Intel VT is the company's hardware assistance for processors running virtualization platforms.

➢ On November 13, 2005, Intel released two models of Pentium 4 as the first Intel processors to support VT-x.

https://searchservervirtualization.techtarget.com/definition/Intel-VT

https://en.wikipedia.org/wiki/Hardware-assisted_virtualization

Int VT extensions

➢ Intel VT-x adds migration, priority and memory handling capabilities.

➢ Intel VT-d adds virtualization support to Intel chipsets that can assign specific I/O devices to specific virtual machines.

➢ Intel VT-c brings better virtualization support to I/O devices such as network switches

https://searchservervirtualization.techtarget.com/definition/Intel-VT