Amirkabir University of Technology
(Tehran Polytechnic)

Cloud Computing

Hardware virtualization-Part2

Seyyed Ahmad Javadi

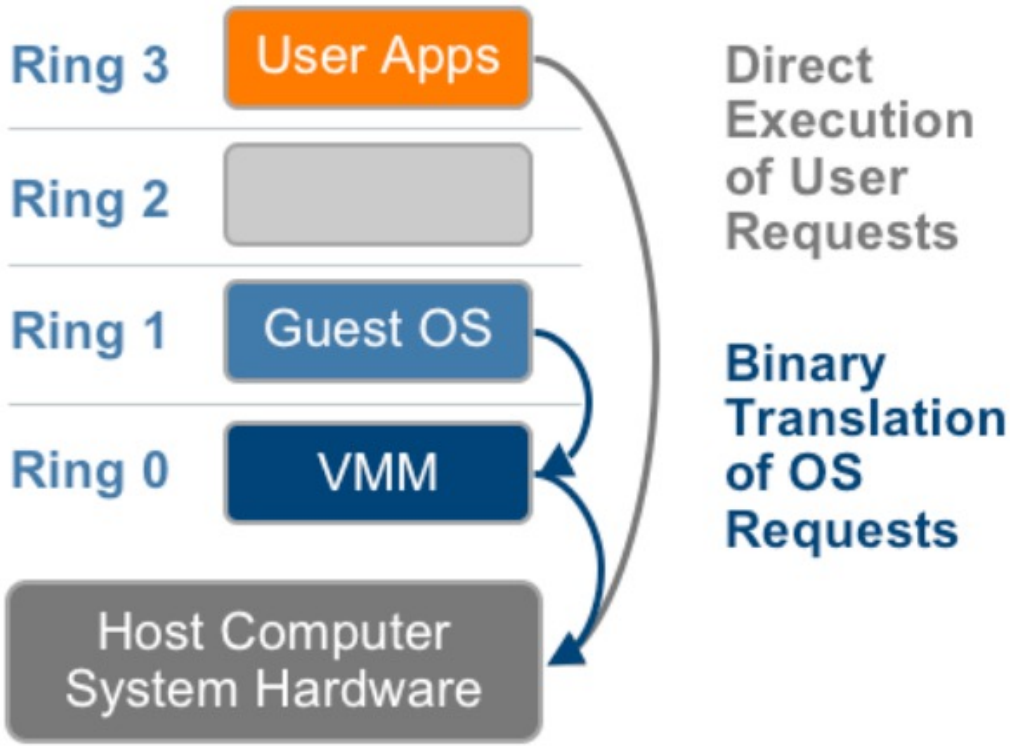
sajavadi@aut.ac.ir

Fall 2022

Virtualization Techniques

- Full Virtualization using Binary Translation
- Hardware Assisted Virtualization
- OS Assisted Virtualization or Paravirtualization

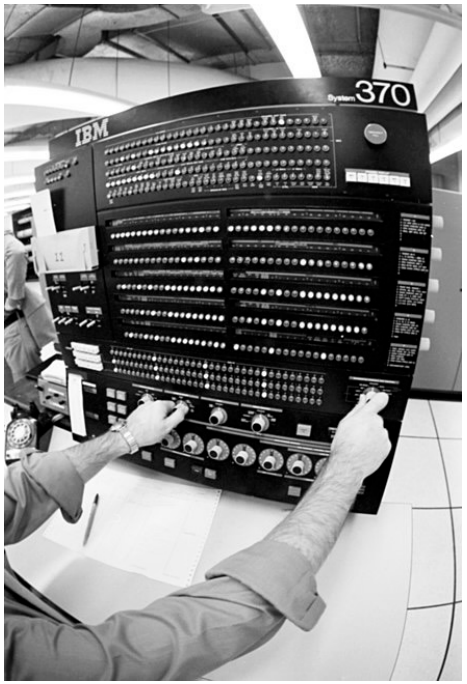
Full Virtualization using Binary Translation



Hardware-assisted Virtualization

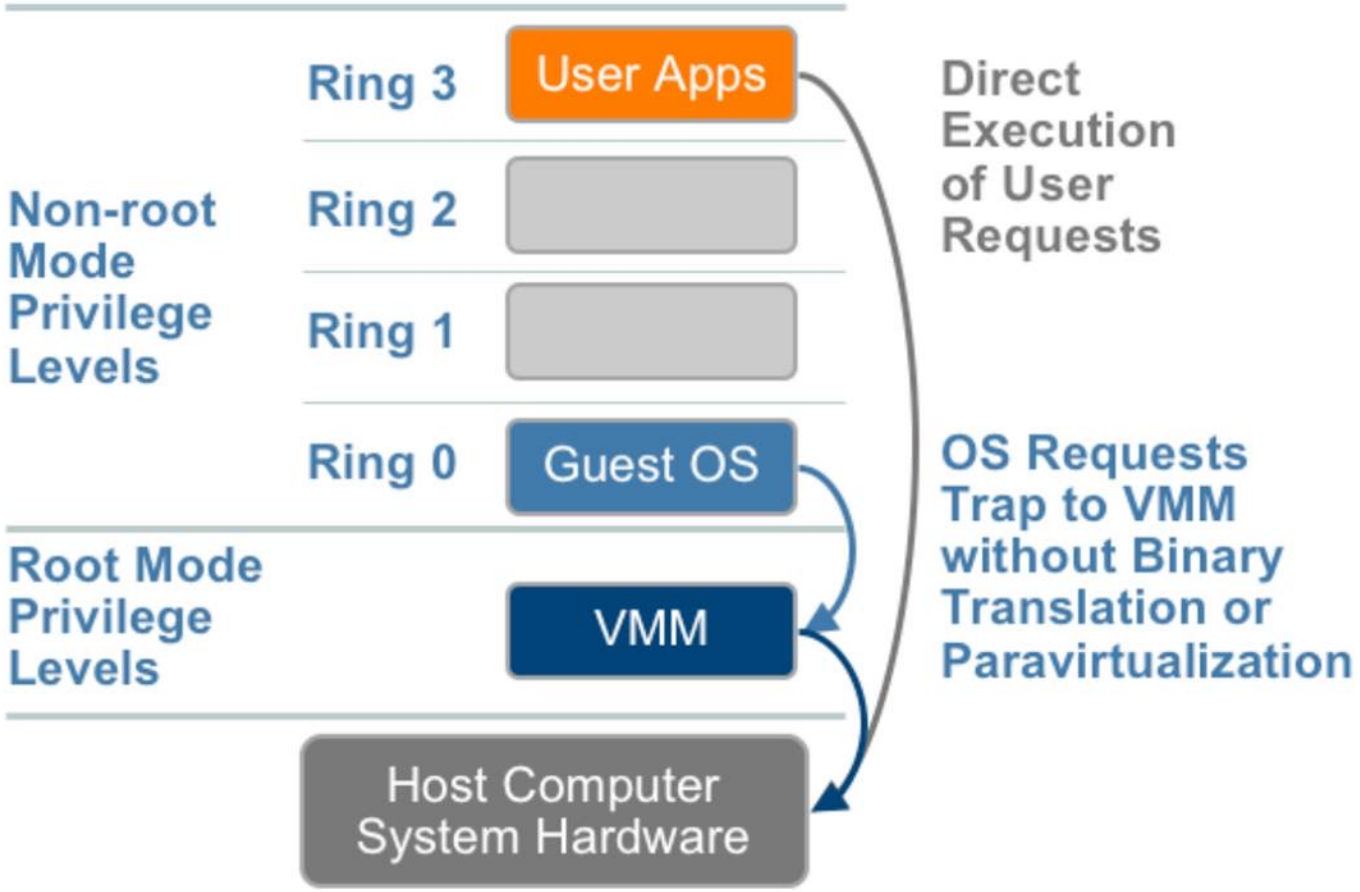
Hardware-assisted Virtualization

- ***Architectural support*** for building a VMM able to run a guest operating system in complete isolation.
- This technique was originally introduced in the IBM System/370.



- Extensions to x86-64b architecture
  - Introduced with Intel-VT and AMD-V.

Hardware-assisted Virtualization (cont.)



https://thecustomizewindows.com/2014/09/hardware-assisted-virtualization/

Intel-VT and AMD-V

- New CPU execution mode feature
- This allows the VMM to run in a new root mode below ring 0
  - **Ring 0P**: privileged root mode (VMM)
  - **Ring 0D** : de-privileged non-root mode (Guest OS)
- Sensitive calls are set ***to automatically trap*** to the hypervisor and handled by hardware
  - Removing the need for either binary translation or para-virtualization.

Intel-VT

- Main feature: inclusion of the new VMX mode of operation.

	all four IA-32 privilege levels (rings)	VMX instructions
VMX non-root operation	✓	✗
VMX root operation	✓	✓

VMX Instructions

- "VMX" stands for Virtual Machine Extensions

13 new instructions

VMPTRLD	VMPTRST	VMCLEAR	VMREAD	VMWRITE
VMCALL	VMLAUNCH	VMRESUME	VMXOFF	VMXON
INVEPT	INVVPID	VMFUNC		

- Permit entering and exiting a ***virtual execution mode*** where the ***guest OS perceives*** itself as running with full privilege (ring 0), but the ***host OS remains protected***.

Hardware-assisted Virtualization

- The behavior of the processor in ***non-root operation is limited*** in some respects from its behavior on a normal processor.

- ***Critical shared resources are kept under the control of a monitor running in VMX root operation***.

- VMM is run in VMX root mode
- Virtual machine and the guest OS are run in non-root mode.

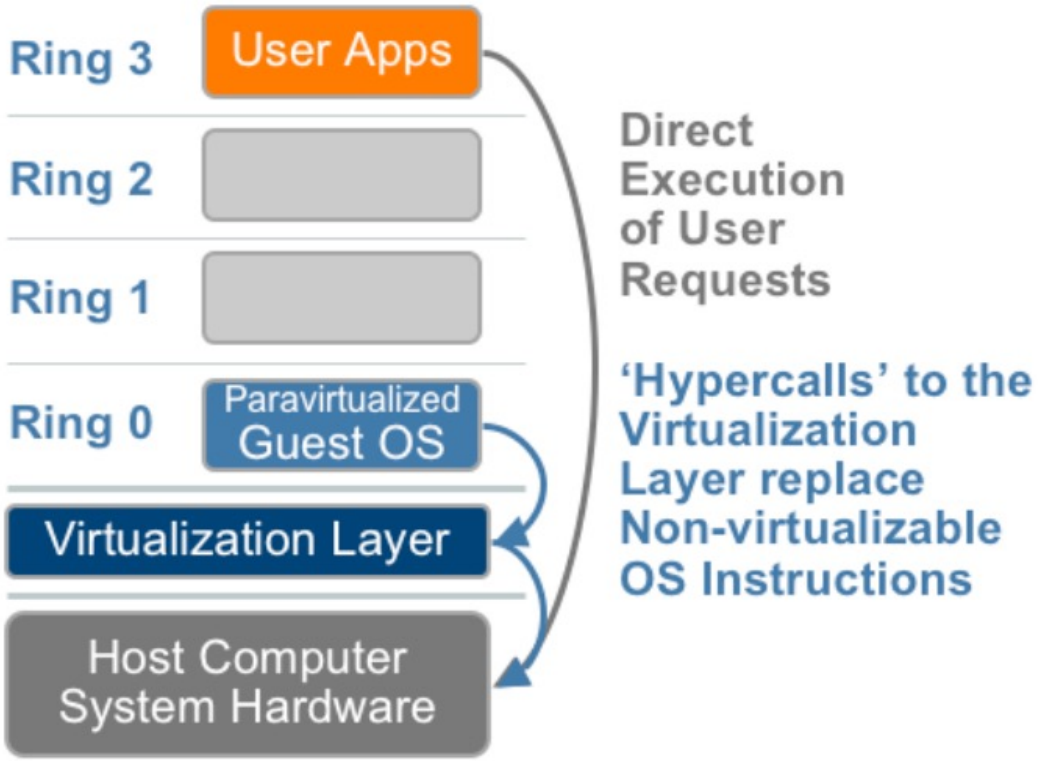
Examples of Hardware-assisted Virtualization

- VirtualBox
- VMware
- Microsoft Hyper-V

Paravirtualization

Paravirtualization

- Paravirtualization refers to communication between the guest OS and the hypervisor to improve performance and efficiency.



Paravirtualization (cont.)

- It is not a transparent virtualization solution
  - Allows implementing ***thin*** virtual machine managers.
  - Remapping the performance-critical operations through the virtual machine software interface.

- Expose a software interface to the virtual machine that is slightly modified from the host
  - As consequence, guests need to be modified.

Paravirtualization (cont.)

- Provide the capability to demand the execution of performance-critical operations ***directly on the host***
  - Preventing performance losses that would otherwise be experienced in managed execution.

- Allows **a simpler implementation of virtual machine managers**
  - VMM have to simply **transfer** the execution of performance-critical operations **directly to the host**.
  - These instructions were ***hard to virtualize***

Paravirtualization (Cont.)

- Xen is ***the most popular implementation*** of paravirtualization.

- The guest operating systems need to be changed

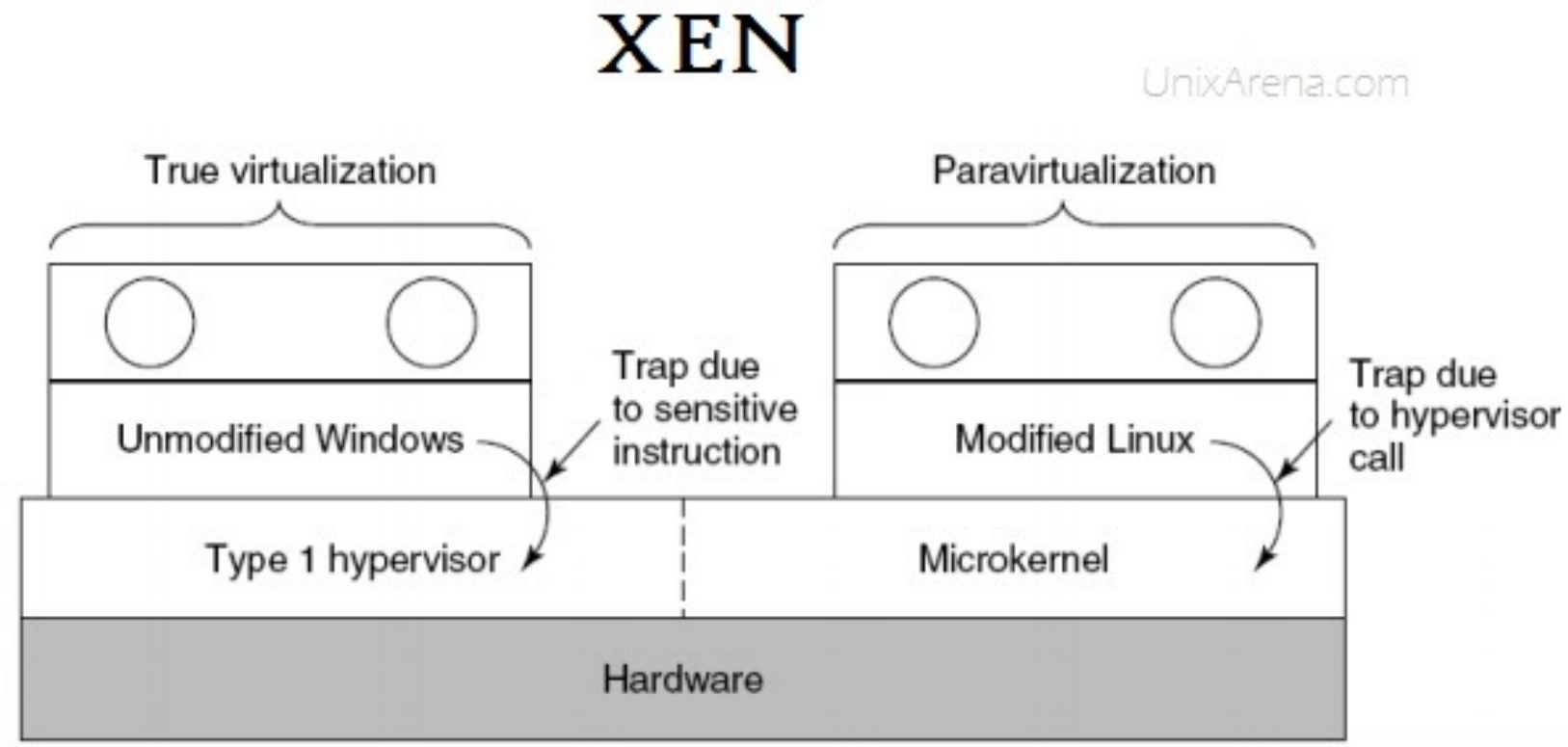
- The sensitive system calls need to be re-implemented with ***hypercalls***
  - Are specific calls exposed by the virtual machine interface of Xen.

Paravirtualization (Cont.)

- With the use of ***hypercalls***, the Xen hypervisor is able to
  - **catch the execution of all the sensitive instructions**
  - **manage them**,
  - and **return the control**

  to the guest operating system by means of a supplied handler.

Xen Hypervisor



Xen supports both Full virtualization and Para-virtualization

source:https://www.unixarena.com/2017/12/para-virtualization-full-virtualization-hardware-assisted-virtualization.html/

Paravirtualization (cont.)

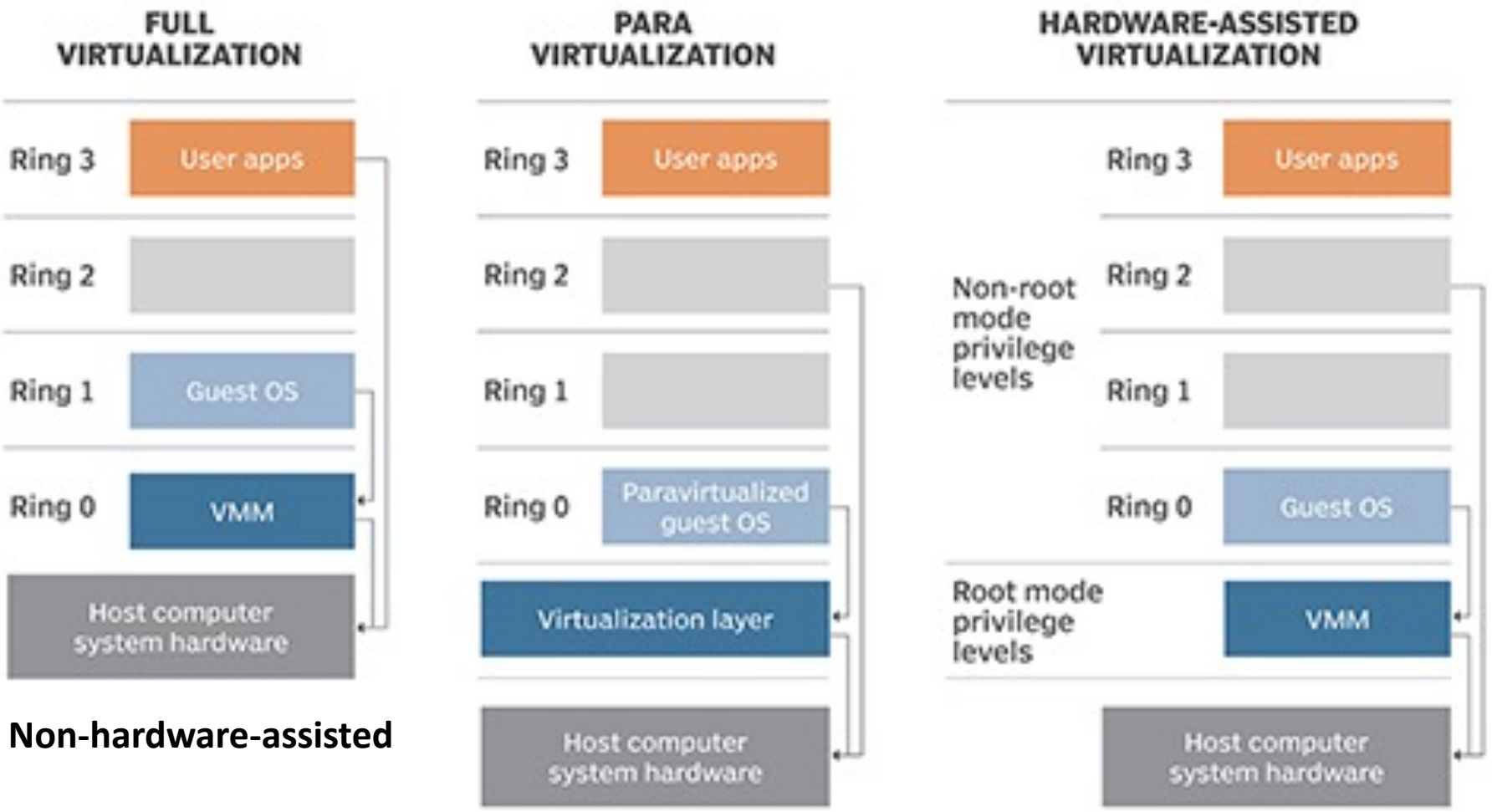
- Open-source operating systems such as Linux can be easily modified
  - Their code is publicly available
  - Xen provides full support for their virtualization

- Components of the Windows family ***are generally not supported*** by Xen unless hardware-assisted virtualization is available.

Overview

Watching a video

System Virtualization Implementation



Non-hardware-assisted

https://searchservervirtualization.techtarget.com/definition/hardware-assisted-virtualization