Virtualization

Dr. Prasenjit Chanak
Assistant Professor

Department of Computer Science and Engineering
Indian Institute of Technology (BHU), Varanasi-221005

Advantages of virtualization

- Managed execution and isolation are perhaps the most important advantages of virtualization
- In the case of techniques supporting the creation of virtualized execution environments, these two characteristics allow building secure and controllable computing environments
- A virtual execution environment can be configured as a sandbox, thus preventing any harmful operation to cross the borders of the virtual host
- Moreover, allocation of resources and their partitioning among different guests is simplified, being the virtual host controlled by a program

Advantages of virtualization

- Portability is another advantage of virtualization, especially for execution virtualization techniques
- Virtual machine instances are normally represented by one or more files that can be easily transported with respect to physical systems
- Java programs are “compiled once and run every- where”; they only require that the Java virtual machine be installed on the host
- The same applies to hardware-level virtualization
- Portability and self-containment also contribute to reducing the costs of maintenance, since the number of hosts is expected to be lower than the number of virtual machine instances
- Finally, by means of virtualization it is possible to achieve a more efficient use of resources

Disadvantages

- Performance degradation
- Performance is definitely one of the major concerns in using virtualization technology
- Since virtualization interposes an abstraction layer between the guest and the host, the guest can experience increased latencies
- For instance, in the case of hardware virtualization, where the intermediate emulates a bare machine on top of which an entire system can be installed, the causes of performance degradation can be traced back to the overhead introduced by the following activities:
  - Maintaining the status of virtual processors
  - Support of privileged instructions (trap and simulate privileged instructions)
  - Support of paging within VM and Console functions

Disadvantages

- When hardware virtualization is realized through a program that is installed or executed on top of the host operating systems, a major source of performance degradation is represented by the fact that the virtual machine manager is executed and scheduled together with other applications, thus sharing with them the resources of the host
- Similar consideration can be made in the case of virtualization technologies at higher levels, such as in the case of programming language virtual machines (Java, .NET, and others). Binary translation and interpretation can slow down the execution of managed applications
- In programming-level virtual machines such as the JVM or .NET, compilation to native code is offered as an option when performance is a serious concern

Inefficiency and Degraded User Experience

- Virtualization can sometime lead to an inefficient use of the host
- In particular, some of the specific features of the host cannot be exposed by the abstraction layer and then become inaccessible
- In the case of hardware virtualization, this could happen for device drivers: The virtual machine can sometime simply provide a default graphic card that maps only a subset of the features available in the host

Inefficiency and Degraded User Experience

- In the case of programming-level virtual machines, some of the features of the underlying operating systems may become inaccessible unless specific libraries are used
- For example, first version of Java the support for graphic programming was very limited and the look and feel of applications was very poor compared to native applications
- These issues have been resolved by providing a new framework called Swing for designing the user interface, nd further improvements have been done by integrating support for the OpenGL libraries in the software development kit

Security Holes and New Threats

- Virtualization opens the door to a new and unexpected form of phishing
- The capability of emulating a host in a completely transparent manner led the way to malicious programs that are designed to extract sensitive information from the guest
- In the case of hardware virtualization, malicious programs can preload themselves before the operating system and act as a thin virtual machine manager toward it
- The operating system is then controlled and can be manipulated to extract sensitive information of interest to third parties

Security Holes and New Threats

- Examples of these kinds of malware are BluePill and SubVirt
- BluePill, malware targeting the AMD processor family, moves the execution of the installed OS within a virtual machine
- SubVirt infects the guest OS, and when the virtual machine is rebooted, it gains control of the host
- Recently, both Intel and AMD have introduced hardware support for virtualization with Intel VT and AMD Pacifica, respectively
- The same considerations can be made for programming level virtual machines: Modified versions of the runtime environment can access sensitive information or monitor the memory locations utilized by guest applications while these are executed
- To make this possible, the original version of the runtime environment needs to be replaced by the modified one, which can generally happen if the malware is run within an administrative context or a security hole of the host operating sys- tem is exploited

VMware Workstation Architecture

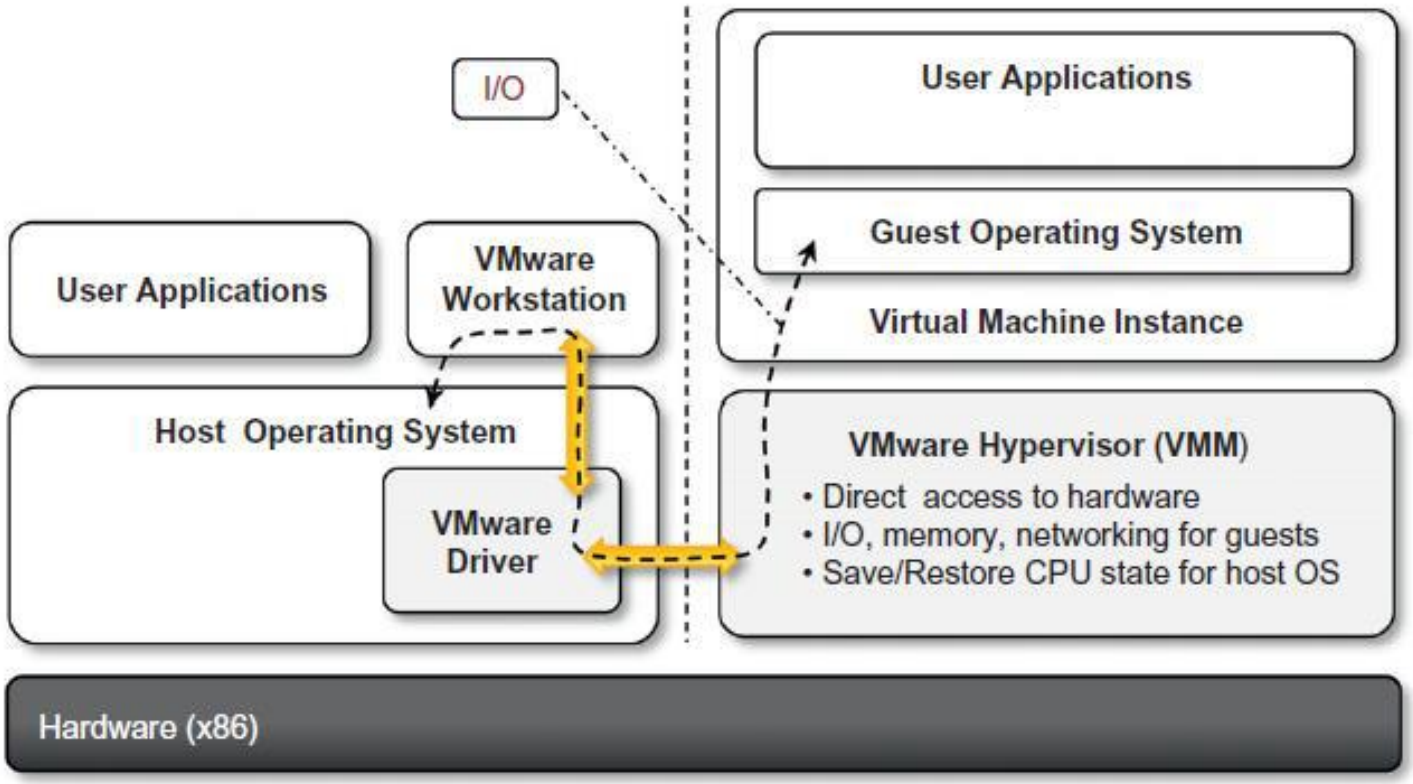

FIGURE 3.13

VMware workstation architecture.

VMware EXSi Server Architecture

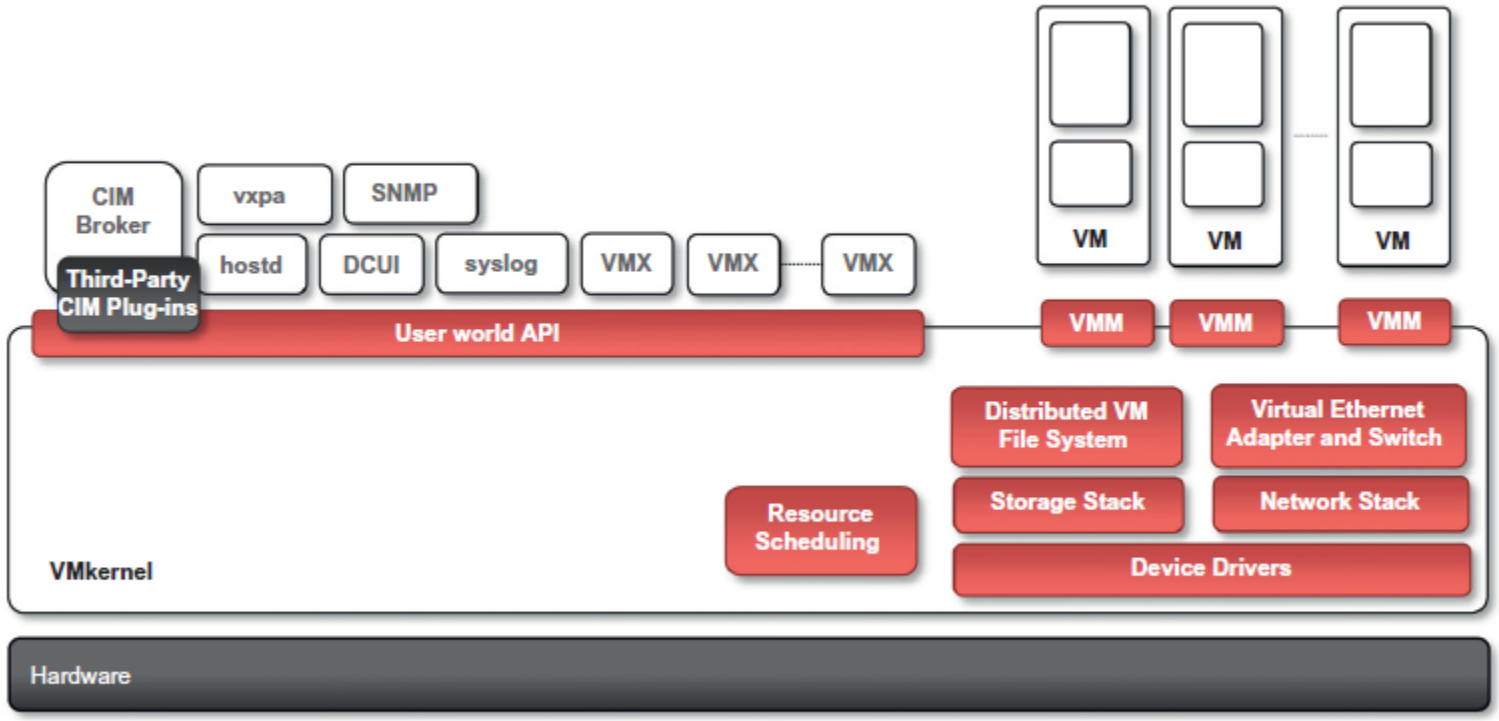

FIGURE 3.15

VMware ESXi server architecture.

VMware Cloud Solution Stack

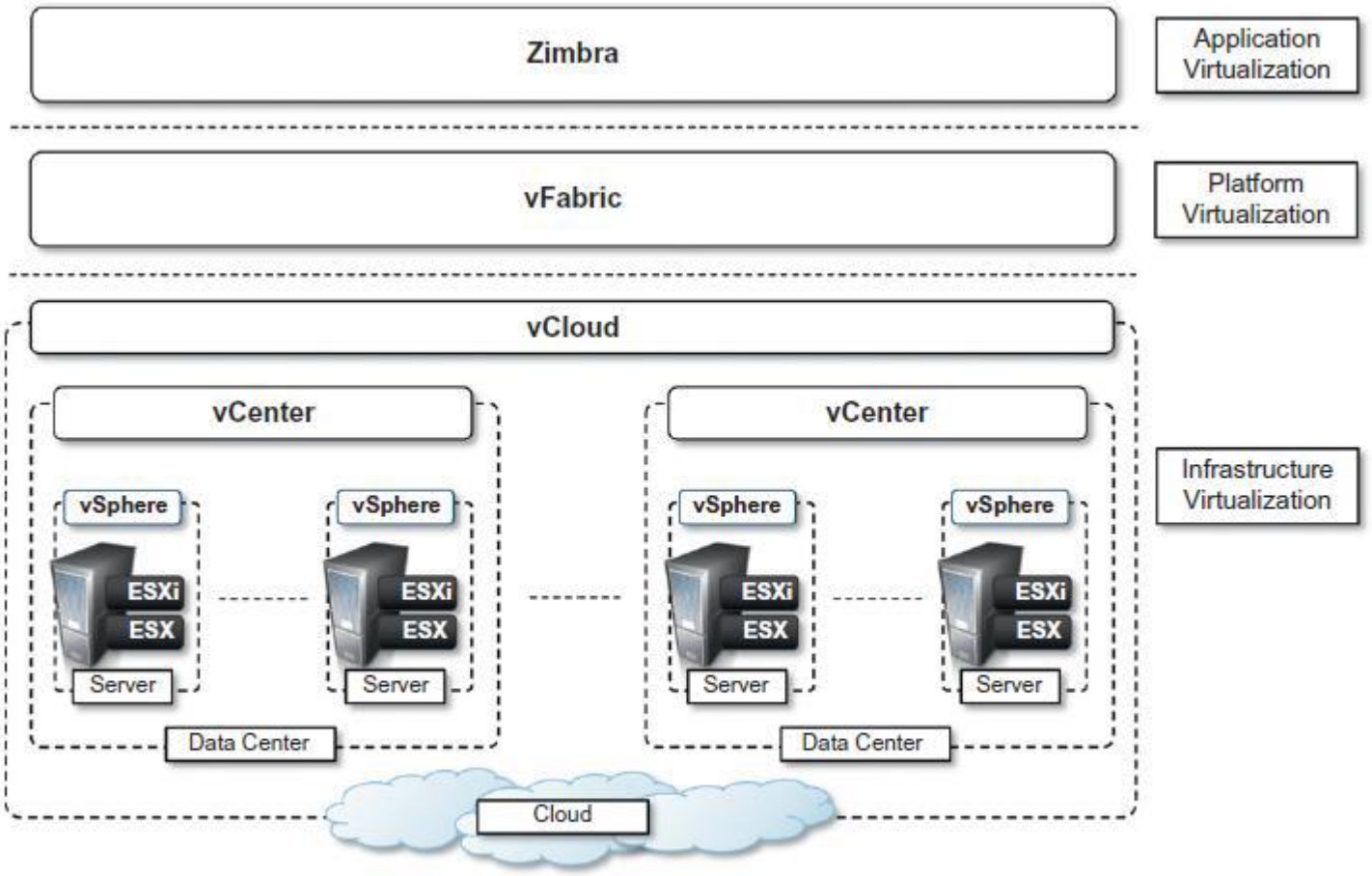

FIGURE 3.16

VMware Cloud Solution stack.

Xen architecture and guest OS management

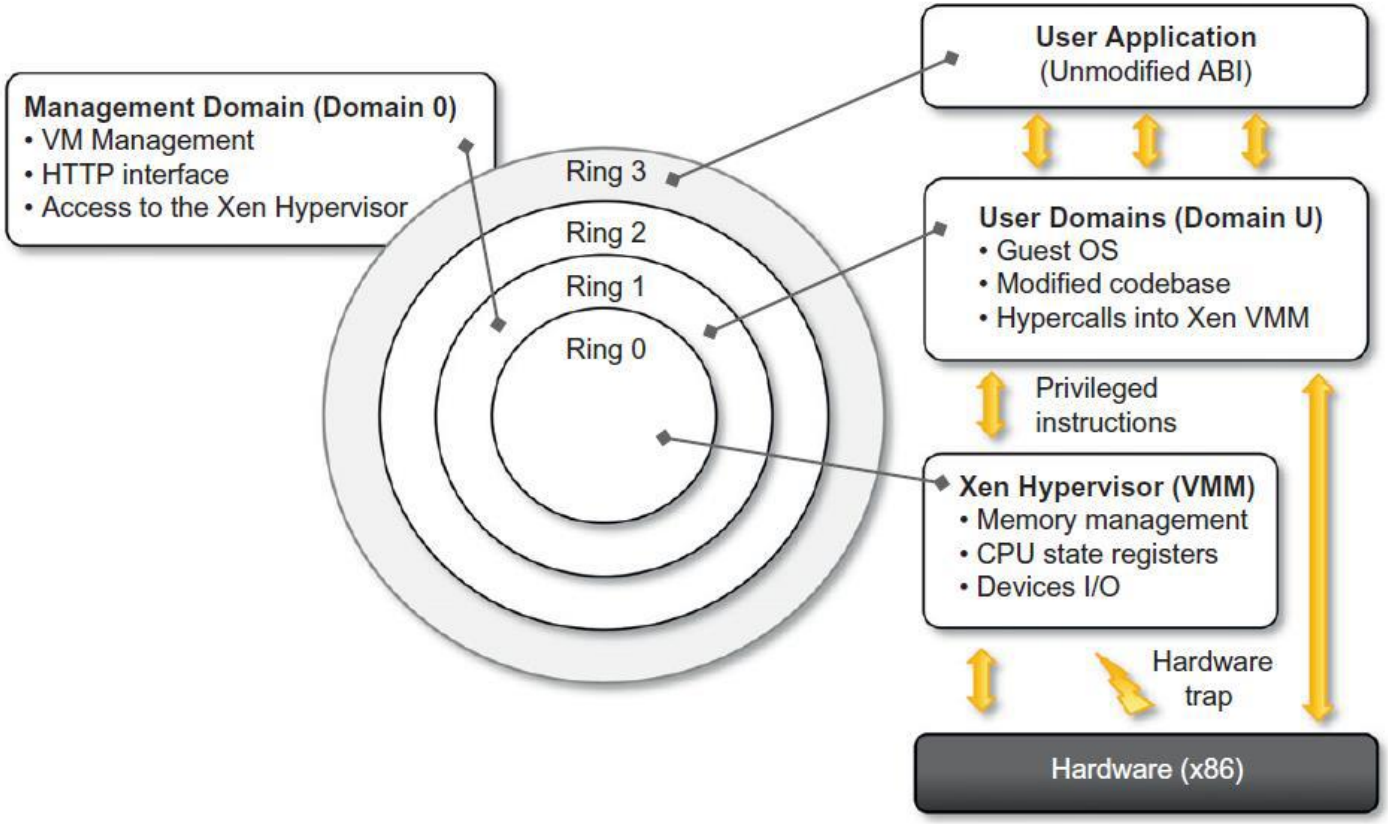

FIGURE 3.11

Xen architecture and guest OS management.