Virtualization

Dr. Prasenjit Chanak
Assistant Professor

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

Operating System-Level Virtualization

- Operating system-level virtualization offers the opportunity to create different and separated execution environments for applications that are managed concurrently
- Differently from hardware virtualization, there is no virtual machine manager or hypervisor, and the virtualization is done within a single operating system, where the OS kernel allows for multiple isolated user space instances
- The kernel is also responsible for sharing the system resources among instances and for limiting the impact of instances on each other

Programming Language-Level Virtualization

- Programming virtualization is mostly used to achieve ease of deployment of applications, managed execution, and portability across different platforms and operating systems
- It consists of a virtual machine executing the byte code of a program, which is the result of the compilation process
- Compilers implemented and used this technology to produce a binary format representing the machine code for an abstract architecture
- The characteristics of this architecture vary from implementation to implementation

Application-Level Virtualization

- Application-level virtualization is a technique allowing applications to be run in runtime environments that do not natively support all the features required by such applications
- In this scenario, applications are not installed in the expected runtime environment but are run as though they were
- In general, these techniques are mostly concerned with partial file systems, libraries, and operating system component emulation
- Such emulation is performed by a thin layer—a program or an operating system component—that is in charge of executing the application
- Emulation can also be used to execute program binaries compiled for different hardware architectures. In this case, one of the following strategies can be implemented:
  - Interpretation
  - Binary translation

Application-Level Virtualization

- Application virtualization is a good solution in the case of missing libraries in the host operating system; in this case a replacement library can be linked with the application, or library calls can be remapped to existing functions available in the host system
- Another advantage is that in this case the virtual machine manager is much lighter since it provides a partial emulation of the runtime environment compared to hardware virtualization
- Moreover, this technique allows incompatible applications to run together. Compared to programming-level virtualization, which works across all the applications developed for that virtual machine, application-level virtualization works for a specific environment: It supports all the applications that run on top of a specific environment

Application-Level Virtualization

- One of the most popular solutions implementing application virtualization is Wine, which is a software application allowing Unix-like operating systems to execute programs written for the Microsoft Windows platform
- Windows Application Binary Interface(WABI), which implements the Win16 API specifications on Solaris
- A similar solution for the Mac OS X environment is CrossOver, which allows running Windows applications directly on the Mac OS X operating system

Other Types of Virtualization

- **Storage virtualization:**
- Storage virtualization is a system administration practice that allows decoupling the physical organization of the hardware from its logical representation
- Using this technique, users do not have to be worried about the specific location of their data, which can be identified using a logical path
- There are different techniques for storage virtualization, one of the most popular being network-based virtualization by means of storage area networks (SANs)

Network virtualization

- Network virtualization combines hardware appliances and specific software for the creation and management of a virtual network
- Network virtualization can aggregate different physical networks into a single logical network(external network virtualization) or provide network-like functionality to an operating system partition (internal network virtualization)
- The result of external network virtualization is generally a virtual LAN(VLAN)
- The guest can share the same network interface of the host and use Network Address Translation (NAT) to access the network; the virtual machine manager can emulate, and install on the host, an additional network device, together with the driver; or the guest can have a private network only with the guest

Desktop virtualization

- Desktop virtualization abstracts the desktop environment available on a personal computer in order to provide access to it using a client/server approach
- Desktop virtualization provides the same out- come of hardware virtualization but serves a different purpose
- Similarly to hardware virtualization, desktop virtualization makes accessible a different system as though it were natively installed on the host, but this system is remotely stored on a different host and accessed through a network connection
- Infrastructures for desktop virtualization based on cloud computing solutions include Sun Virtual Desktop Infrastructure (VDI), Parallels Virtual Desktop Infrastructure (VDI), Citrix XenDesktop, and others

Application Server Virtualization

- Application server virtualization abstracts a collection of application servers that provide the same services as a single virtual application server by using load-balancing strategies and providing a high availability infrastructure for the services hosted in the application server
- This is a particular form of virtualization and serves the same purpose of storage virtualization: providing a better quality of service rather than emulating a different environment

Virtualization and cloud computing

- Virtualization plays an important role in cloud computing since it allows for the appropriate degree of customization, security, isolation, and manageability that are fundamental for delivering IT services on demand
- Virtualization technologies are primarily used to offer configurable computing environments and storage
- Network virtualization is less popular and, in most cases, is a complementary feature, which is naturally needed in build virtual computing systems
- Particularly important is the role of virtual computing environment and execution virtualization techniques
- Among these, hardware and programming language virtualization are the techniques adopted in cloud computing systems

Hardware Virtualization

- Hardware virtualization is an enabling factor for solutions in the **Infrastructure-as-a-Service (IaaS)** market segment, while programming language virtualization is a technology leveraged in **Platform-as-a-Service (PaaS)** offerings
- In both cases, the capability of offering a customizable and sandboxed environment constituted an attractive business opportunity for companies featuring a large computing infrastructure that was able to sustain and process huge workloads
- Moreover, virtualization also allows isolation and a finer control, thus simplifying the leasing of services and their accountability on the vendor side

Hardware Virtualization

- Besides being an enabler for computation on demand, virtualization also gives the opportunity to design more efficient computing systems by means of consolidation, which is performed transparently to cloud computing service users
- Since virtualization allows us to create isolated and controllable environments, it is possible to serve these environments with the same resource without them interfering with each other

Virtual Machine Migration and Server Consolidation

- If the underlying resources are capable enough, there will be no evidence of such sharing
- This opportunity is particularly attractive when resources are underutilized, because it allows reducing the number of active resources by aggregating virtual machines over a smaller number of resources that become fully utilized
- This practice is also known as server consolidation, while the movement of virtual machine instances is called virtual machine migration
- Because virtual machine instances are controllable environments, consolidation can be applied with a minimum impact, either by temporarily stopping its execution and moving its data to the new resources or by performing a finer control and moving the instance while it is running
- This second techniques is known as live migration and in general is more complex to implement but more efficient since there is no disruption of the activity of the virtual machine instance

Virtual Machine Migration and Server Consolidation

- Server consolidation and virtual machine migration are principally used in the case of hardware virtualization, even though they are also technically possible in the case of programming language virtualization

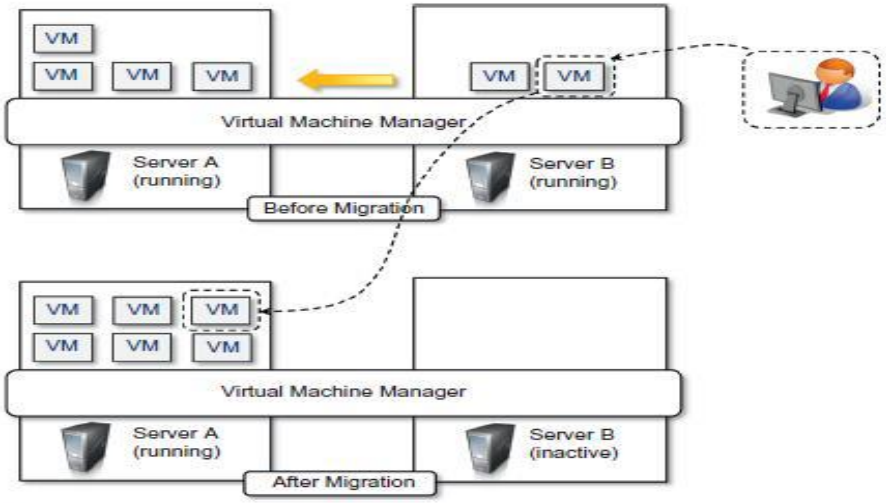

FIGURE 3.10
Live migration and server consolidation.

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, and 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 system is exploited

VMware Workstation Architecture

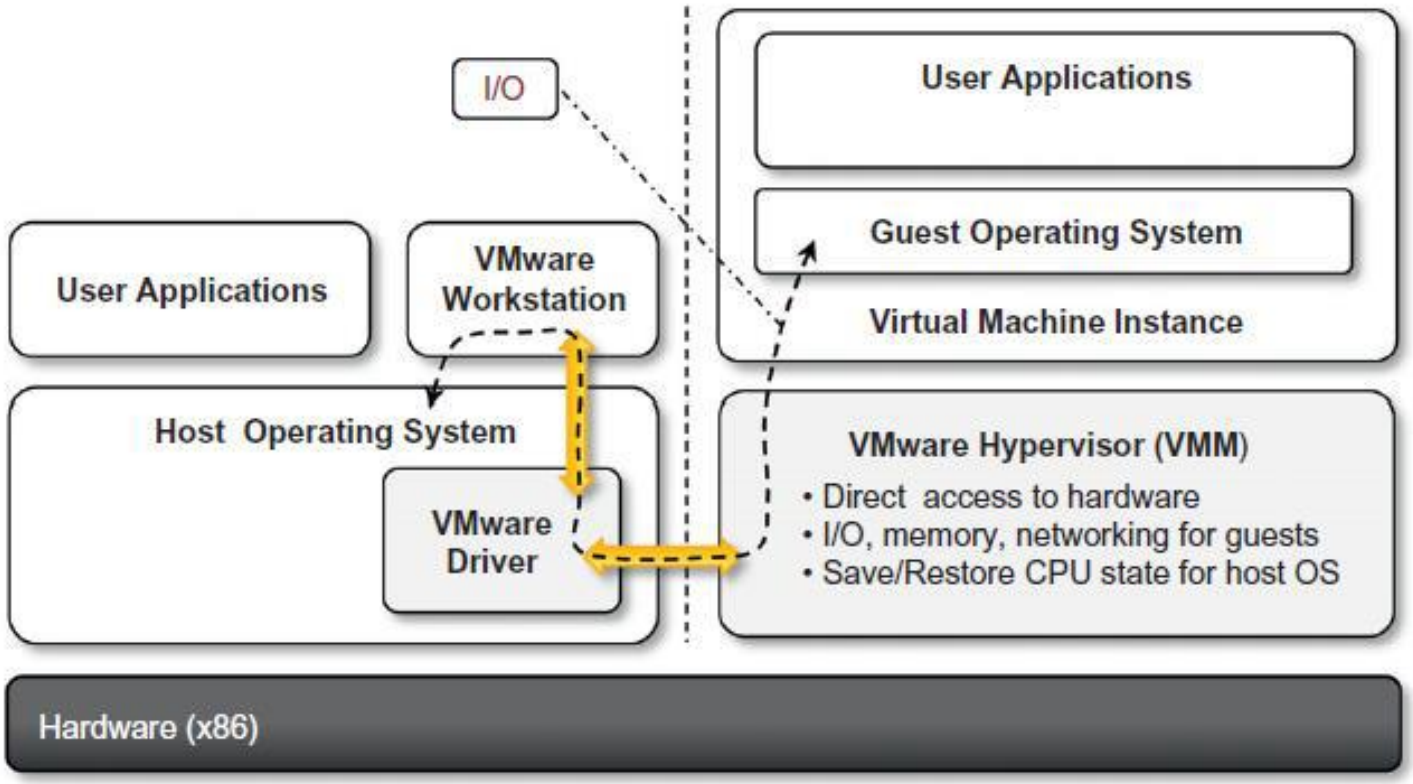

FIGURE 3.13

VMware workstation architecture.

VMware EXSi Server Architecture

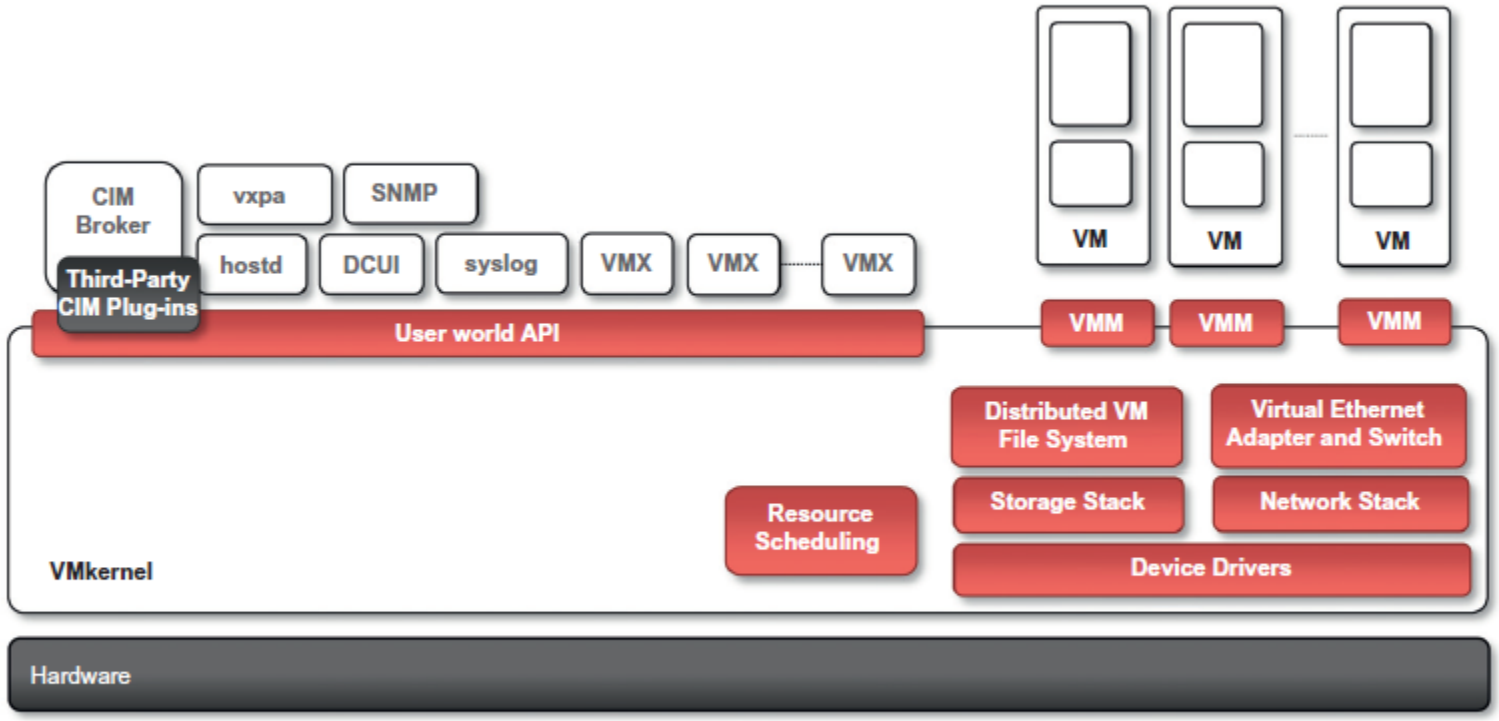

FIGURE 3.15

VMware ESXi server architecture.

VMware Cloud Solution Stack

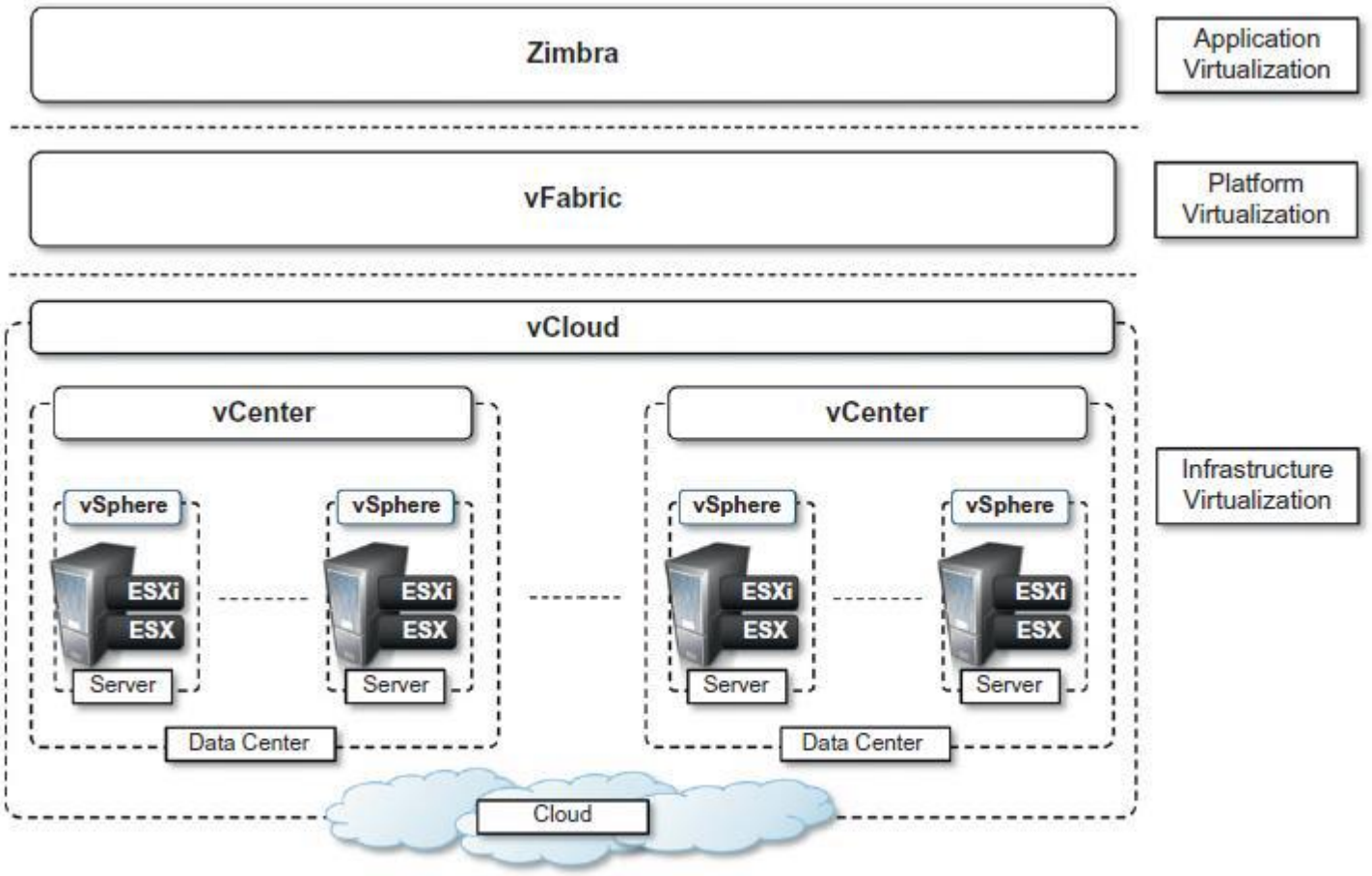

FIGURE 3.16

VMware Cloud Solution stack.

Xen architecture and guest OS management

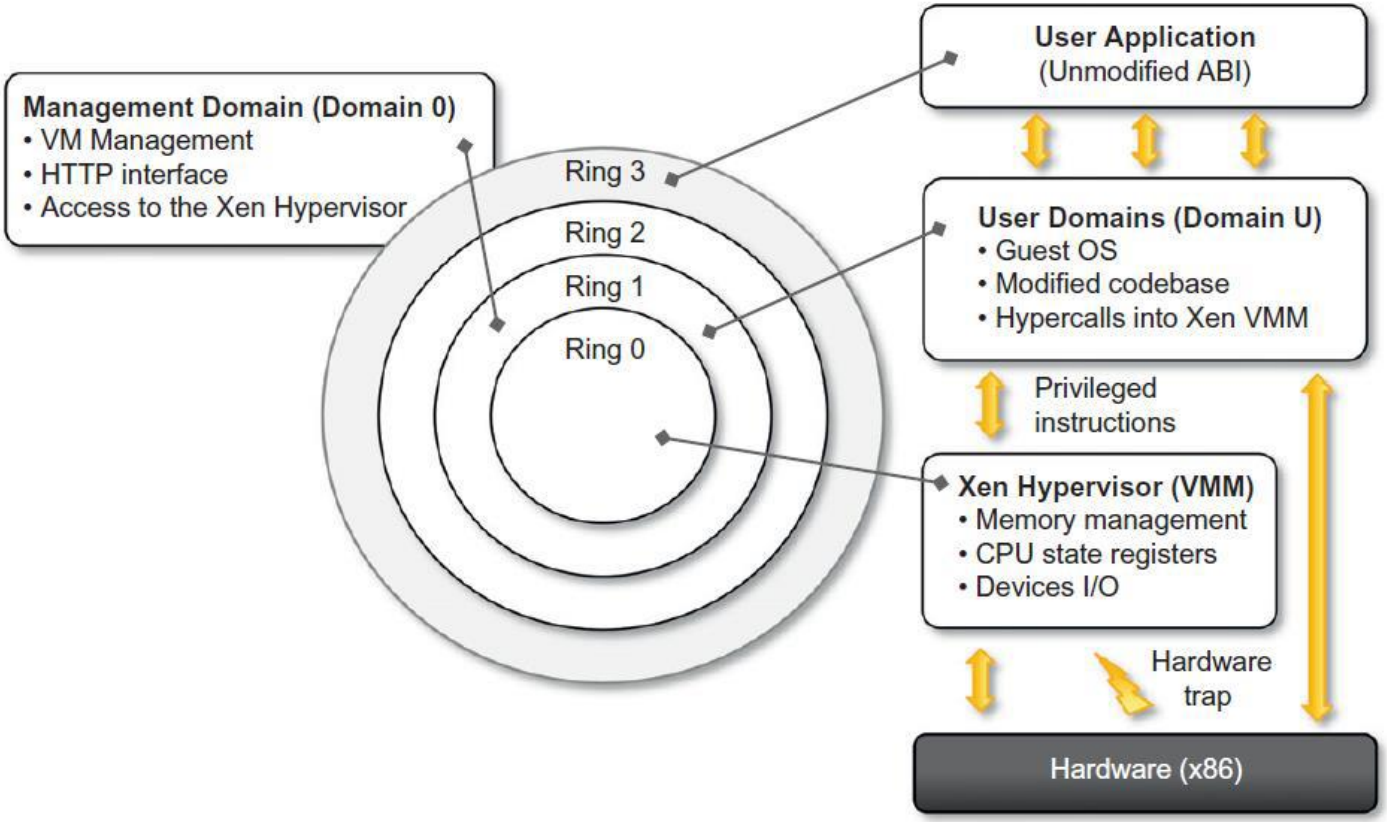

FIGURE 3.11

Xen architecture and guest OS management.