The hybrid and the hosted VM models in Figures 5.3(c) and (d), respectively, expose the entire system

to the vulnerability of the host operating system; thus, we will not analyze these models. Our discussion

of virtual machine security is restricted to the traditional system VM model in Figure 5.3(b), where the

VMM controls access to the hardware.

Virtual security services are typically provided by the VMM, as shown in Figure 9.2(a). Another

alternative is to have a dedicated security services VM, as shown in Figure 9.2(b). A secure trusted computing base (TCB) is a necessary condition for security in a virtual machine environment; if the

TCB is compromised, the security of the entire system is affected.

The analysis of Xen and vBlades in Sections 5.8 and 5.10 shows that VM technology provides a

stricter isolation of virtual machines from one another than the isolation of processes in a traditional

operating system. Indeed, a VMM controls the execution of privileged operations and can thus enforce

memory isolation as well as disk and network access. The VMMs are considerably less complex and

better structured than traditional operating systems; thus, they are in a better position to respond to

security attacks. A major challenge is that a VMM sees only raw data regarding the state of a guest

operating system, whereas security services typically operate at a higher logical level, e.g., at the level

of a file rather than a disk block.

A guest OS runs on simulated hardware, and the VMM has access to the state of all virtual machines

operating on the same hardware. The state of a guest virtual machine can be saved, restored, cloned,

and encrypted by the VMM. Not only can replication ensure reliability, it can also support security,

whereas cloning could be used to recognize a malicious application by testing it on a cloned system

and observing whether it behaves normally.We can also clone a running system and examine the effect

of potentially dangerous applications. Another interesting possibility is to have the guest VM’s files

moved to a dedicated VM and thus, protect it from attacks [389]; this is possible because inter-VM

communication is faster than communication between two physical machines.

Sophisticated attackers are able to fingerprint virtual machines and avoid VM honeypots designed to

study the methods of attack. They can also attempt to access VM-logging files and thus recover sensitive

data; such files have to be very carefully protected to prevent unauthorized access to cryptographic keys

and other sensitive data.

There is no free lunch; thus, we expect to pay some price for the better security provided by virtualization.

This price includes: higher hardware costs, because a virtual system requires more resources, such

as CPU cycles, memory, disk, and network bandwidth; the cost of developing VMMs and modifying

the host operating systems in case of paravirtualization; and the overhead of virtualization because the

VMM is involved in privileged operations.

A recent paper [389] surveysVM-based intrusion detection systems such as Livewire and Siren,

which exploit the three capabilities of a virtual machine for intrusion detection: isolation, inspection, and

interposition. We have examined isolation; inspection means that the VMM has the ability to review

the state of the guest VMs, and interposition means that the VMM can trap and emulate the privileged

instruction issued by the guest VMs. The paper also discusses VM-based intrusion prevention

systems such as SVFS, NetTop, and IntroVirt and surveys Terra, a VM-based trust computing

platform. Terra uses a trusted virtual machine monitor to partition resources among virtual

machines.

The security group involved with theNIST project has identified the followingVMM-and VM-based

threats:

• VMM-based threats:

1. Starvation of resources and denial of service for someVMs. Probable causes: (a) badly configured

resource limits for some VMs; (b) a rogue VM with the capability to bypass resource limits set

in the VMM.

2. VM side-channel attacks.Malicious attacks on one or more VMs by a rogue VM under the same

VMM. Probable causes: (a) lack of proper isolation of inter-VM traffic due to misconfiguration

of the virtual network residing in the VMM; (b) limitation of packet inspection devices to

handle high-speed traffic, e.g., video traffic; (c) presence of VM instances built from insecure

VM images, e.g., a VM image having a guest OS without the latest patches.

3. Buffer overflow attacks.

• VM-based threats:

1. Deployment of rogue or insecure VM. Unauthorized users may create insecure instances from

images or may perform unauthorized administrative actions on existing VMs. Probable cause:

improper configuration of access controls on VM administrative tasks such as instance creation,

launching, suspension, reactivation, and so on.

2. Presence of insecure and tampered VM images in the VM image repository. Probable causes:

(a) lack of access control to the VM image repository; (b) lack of mechanisms to verify the

integrity of the images, e.g., digitally signed image.

Sections 9.7, 9.8, 9.9, and 9.10 discuss in depth various aspects related to virtualization and security.