# Cloud Security

**Module Number: 01**

## Module Name: Introduction to Virtualization Security

**Version Code: CS1**
**Released Date:12-Dec-2018**

# Introduction to Virtualization Security

## AIM:

To equip students with fundamentals and characteristics of cloud security.

## Objectives of the module:

The Objectives of this module are:

- Explain the key concepts of Cloud Security.
- Explain the evolution of Cloud Security.
- Describe the structure of Cloud Security.
- Explain about Virtualization Security.

## Outcome of the module:

At the end of this module, you are expected to:

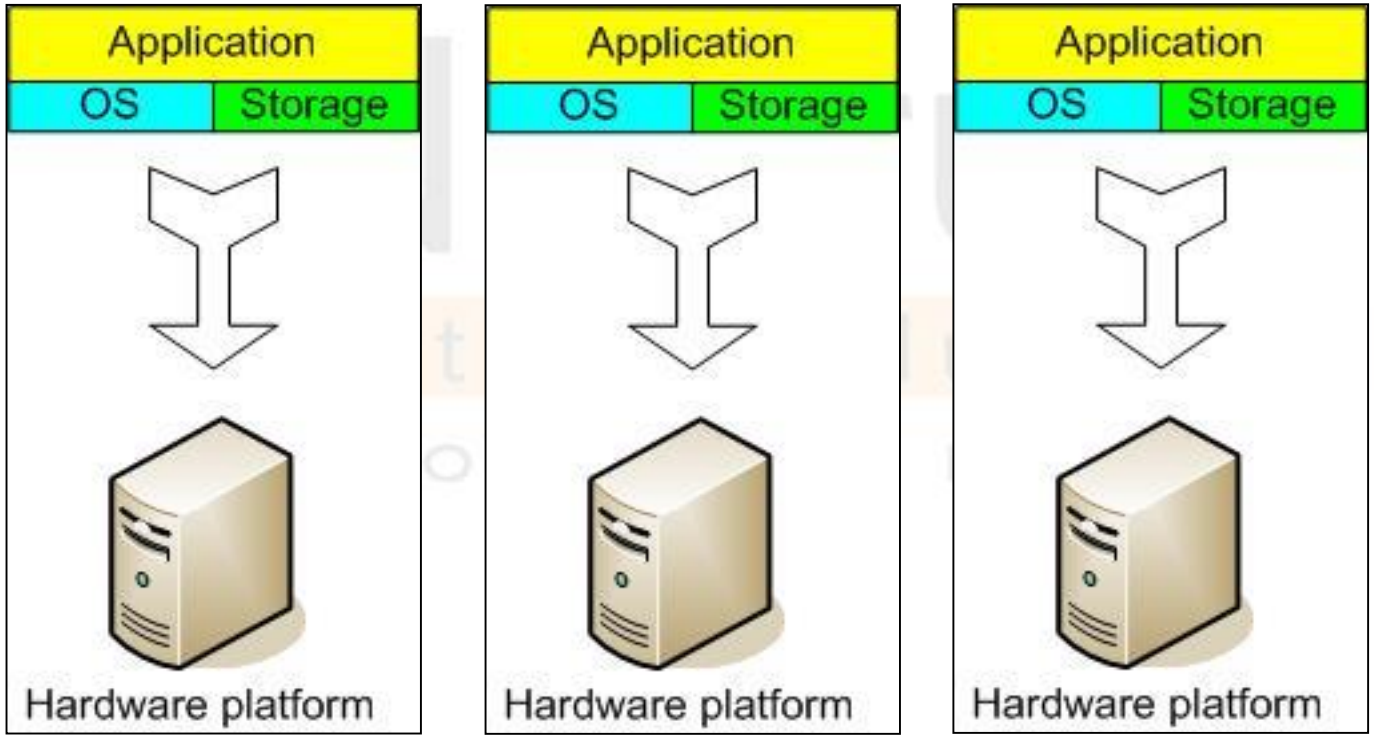
- Define Virtualization Security.
- Explain virtualization features.
- Strategies of Virtualization Security..
- Explain Virtualization risks.

# Introduction to Virtualization Security

## Contents

1. Introduction to Virtualization
2. Risks of Virtualization
3. Hyper jacking and Virtual Machine jumping
4. Strategies and counter measures for addressing Virtualization risks
5. Vulnerabilities and mitigation measures

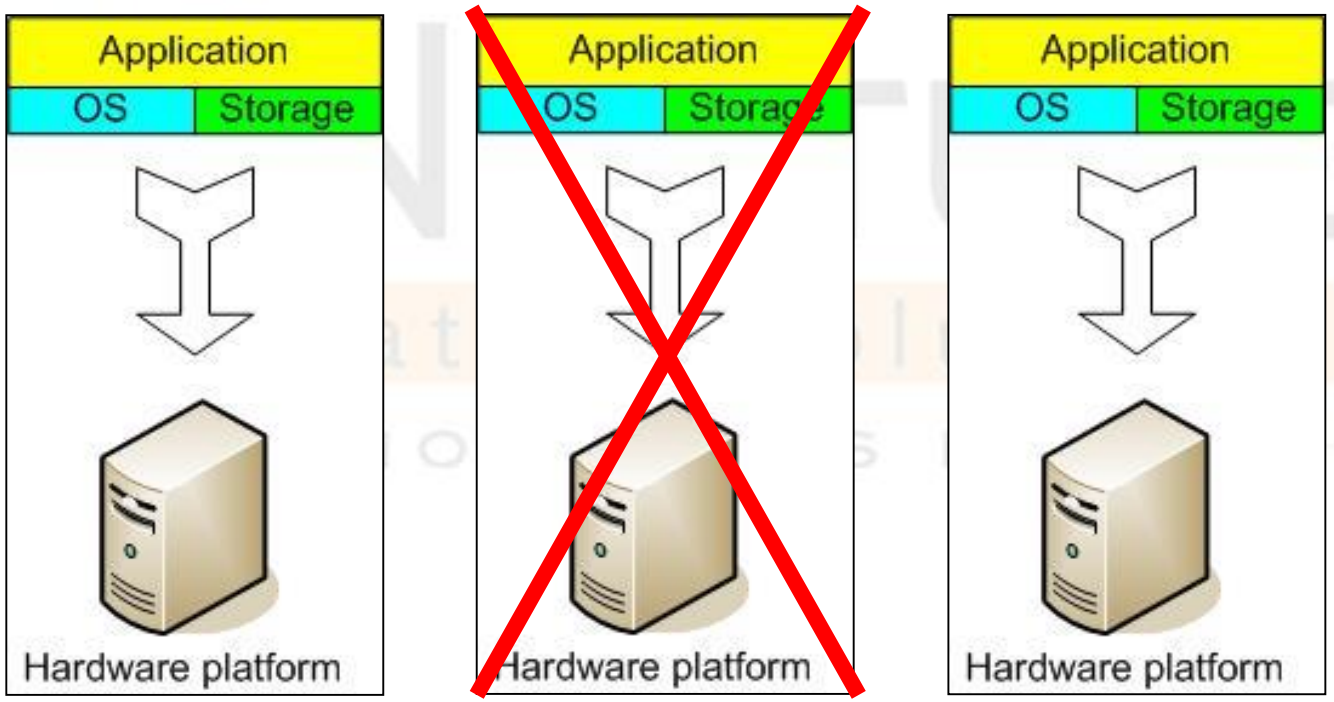
## The Traditional Server Concept



## Bottleneck of Traditional Server Concept

- System Administrators often talk about servers as a whole unit that includes the hardware, the OS, the storage, and the applications.
- Servers are often referred to by their function i.e. the Exchange server, the SQL server, the File server, etc.
- If the File server fills up, or the Exchange server becomes overtaxed, then the System Administrators must add in a new server.
- Unless there are multiple servers, if a service experiences a hardware failure, then the service is down.
- System Admins can implement clusters of servers to make them more fault tolerant. However, even clusters have limits on their scalability, and not all applications work in a clustered environment.

## And if something goes wrong ...



## Need of Virtualization

- Virtual servers seek to encapsulate the server software away from the hardware.
- This includes the OS, the applications, and the storage for that server.
- Servers end up as mere files stored on a physical box, or in enterprise storage.
- One host typically house many virtual servers (**virtual machines or VMs**).
- A virtual server can be serviced by one or more hosts e.g. storage, services, etc.

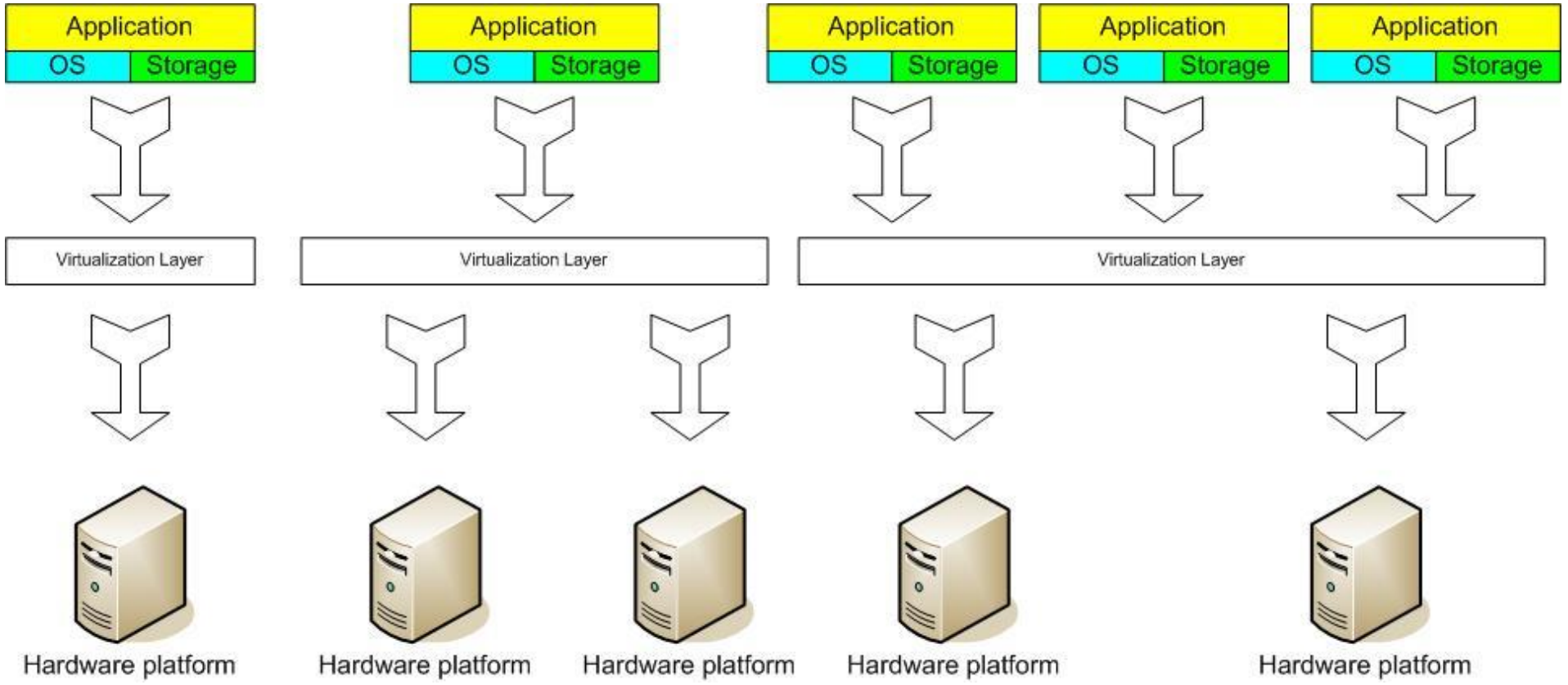
## Virtualization

- In Cloud computing, Virtualization is the basis of providing Infrastructure as a Service (IaaS).
- A single system can concurrently run multiple isolated virtual machines (VMs), operating systems or multiple instances of a single operating system (OS).
- Virtualization maximizes the jobs a single CPU can do.
- Organizations are using virtualization to gain efficiency in platform and application hosting.

## Virtualization

- Creating a virtual machine over existing operating system and hardware is referred as Hardware Virtualization.
- Virtual Machines provide an environment that is logically separated from the underlying hardware.
- The machine on which the virtual machine is created is known as **host machine** and **virtual machine** is referred as a **guest machine.**
- This virtual machine is managed by a software or firmware, which is known as **hypervisor.**

## Virtualization



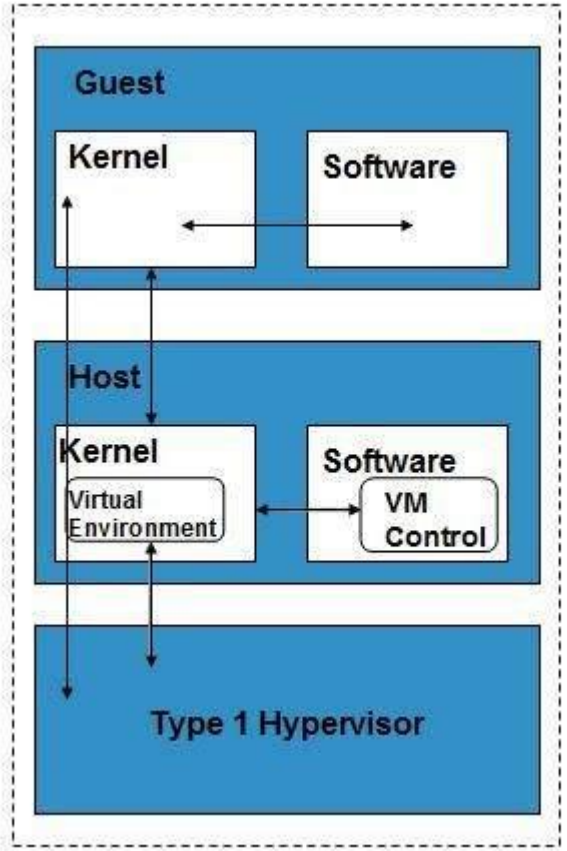
## Types of Hardware Virtualization

Here are the three types of hardware virtualization:

- Full Virtualization
- Emulation Virtualization
- Paravirtualization

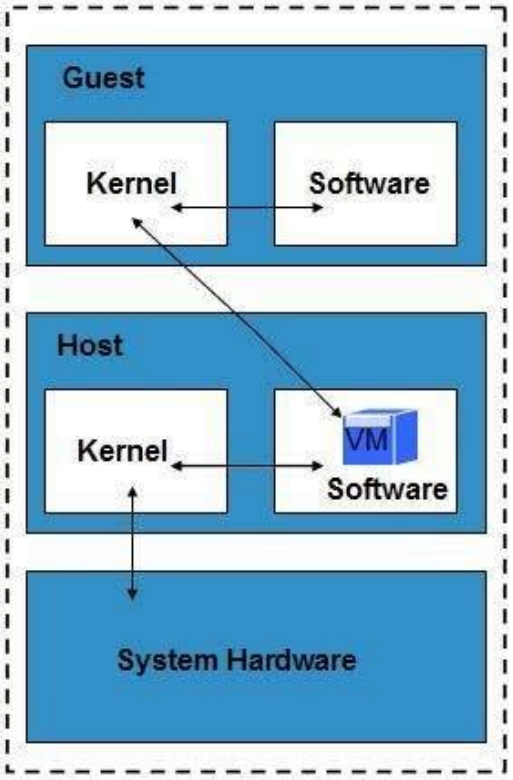
## Full Virtualization

In **full virtualization,** the underlying hardware is completely simulated. Guest software does not require any modification to run.



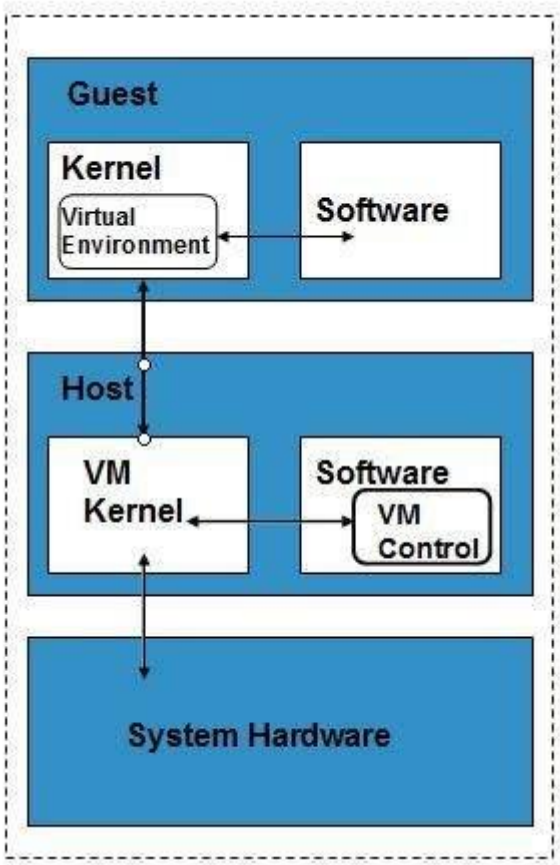
## Emulation Virtualization

In **Emulation,** the virtual machine simulates the hardware and hence becomes independent of it. In this, the guest operating system does not require modification.



## Paravirtualization

In **Paravirtualization,** the hardware is not simulated. The guest software run their own isolated domains.



## Benefits of virtualization

- To determine whether virtualization is the right solution for your organization, you must consider your unique needs and requirements.

- Determine how virtualization would integrate with your existing systems, who will provide support for the virtualized environment, your scalability and security needs, and the overall costs of migrating to a virtual private cloud.

.

# Introduction to Virtualization Security

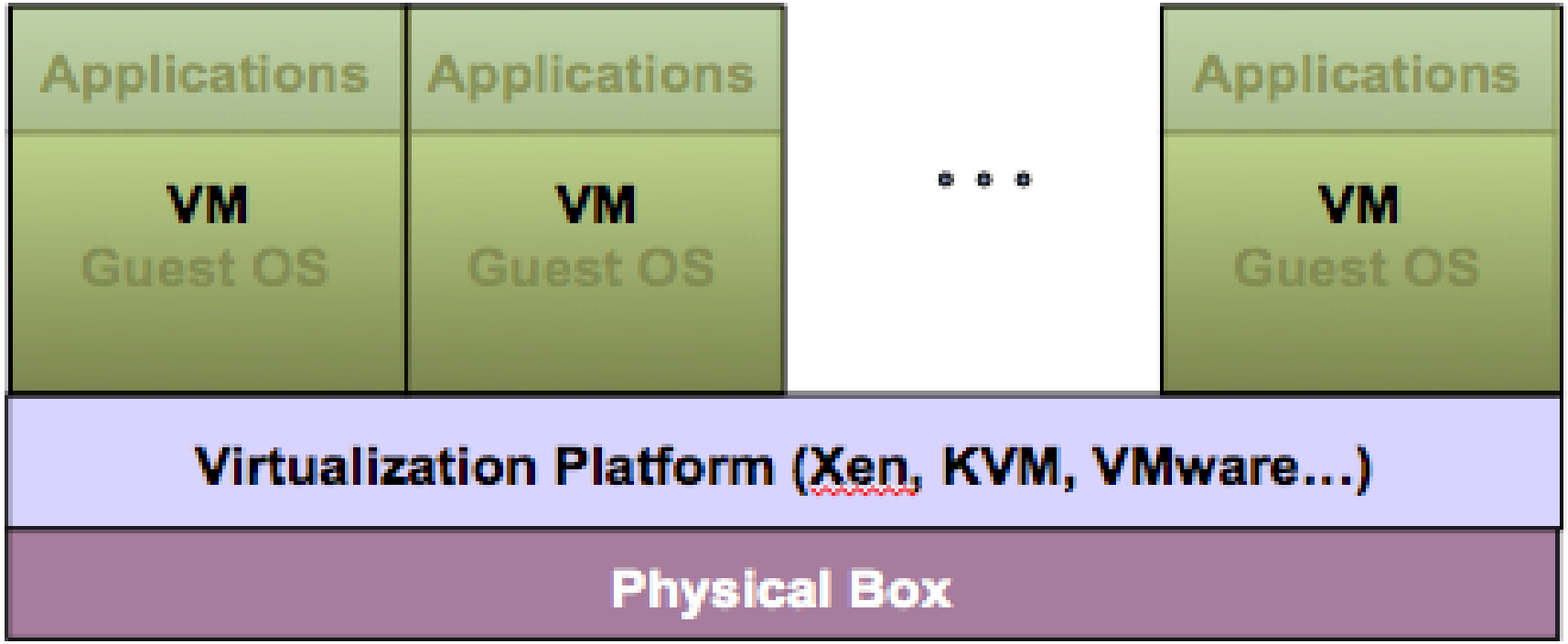
## Definition

- Virtualization is the ability to run multiple operating systems on a single physical system and share the underlying hardware resources*
- It is the process by which one computer hosts the appearance of many computers.
- Virtualization is used to improve IT throughput and costs by using physical resources as a pool from which virtual resources can be allocated.

*VMWare white paper, *Virtualization Overview*

## Virtualization Architecture

- A Virtual machine (VM) is an isolated runtime environment (guest OS and applications)
- Multiple virtual systems (VMs) can run on a single physical system



## Risk of Virtualization

- Sensitive data within a VM
- Security of offline & dormant VMs
- Security of pre-configured (golden image) VM/active VMs
- Lack of visibility and control over virtual networks
- Resource exhaustion
- Hypervisor security
- Unauthorized access to hypervisor
- Account or service hijacking through the self-service portal
- Workloads of different trust levels located on the same server
- Risk due to cloud service provider APIs

## Benefits of Virtualization

- Sharing of resources helps cost reduction
- Isolation: Virtual machines are isolated from each other as if they are physically separated
- Encapsulation: Virtual machines encapsulate a complete computing environment
- Hardware Independence: Virtual machines run independently of underlying hardware
- Portability: Virtual machines can be migrated between different hosts.

## Virtualization in Cloud Computing

Cloud computing takes virtualization one step further:

- You don’t need to own the hardware
- Resources are rented as needed from a cloud
- Various providers allow creating virtual servers:
  - Choose the OS and software each instance will have
  - The chosen OS will run on a large server farm
  - Can instantiate more virtual servers or shut down existing ones within minutes

## Virtualization in Cloud Computing

Cloud computing takes virtualization one step further:

- You don’t need to own the hardware
- Resources are rented as needed from a cloud
- Various providers allow creating virtual servers:
  - Choose the OS and software each instance will have
  - The chosen OS will run on a large server farm
  - Can instantiate more virtual servers or shut down existing ones within minutes
- You get billed only for what you used

## Virtualization Security Challenges

The trusted computing base (TCB) of a virtual machine is too large.

- TCB: A small amount of software and hardware that security depends on and that we distinguish from a much larger amount that can misbehave without affecting security*
- Smaller TCB → more security

*Lampson et al., "Authentication in distributed systems: Theory and practice," ACM TCS 1992

## Virtualization Management Challenges

- **Creating an Excess of Virtual Machines – VM Sprawl**

  On a single host, it is possible to create innumerable virtual machines. Also known as VM Sprawl, this phenomenon is supposed to be common in virtualized worlds. However, without a proper capacity management, this could lead to unnecessary utilization of resources, a shortage of support capacity and an off-balance of workflow.

## Virtualization Management Challenges

- **Misjudgment in Estimating Resource Capacity Required**

  In a virtual server the hardware used is fixed. However resources that needs to be allocated varies and is dynamic in nature. An accurate estimate should be forecasted in order to ensure sufficient resources are assigned to support virtual machines that are run on host hardware.

## Virtualization Management Challenges

- **The Challenge of Backup, Recovery and Continuity**

  In virtualization, traditional back-up and recovery systems so not apply. There is no actual hard drive on which information can be backed up. New backup and recovery software products need to be installed and upgraded regularly, which will include additional costs.

## Virtualization Management Challenges

- **Security and Monitoring**

  As virtualized environments are highly dynamic, with new virtual systems being created indiscriminately, security and monitoring of performance is a major challenge. The hardware resources used in physical environments do apply in securing and monitoring functioning of virtual systems, therefore demanding customized security and monitoring solutions built for virtualized environments

## Virtualization Management Challenges

- **Hesitance in Adopting Virtualization – VM Stall**

  Technology departments are skeptical of migrating core processes and application to virtualized spaces. Companies need specific orientation on the benefits of virtualization such as reduction of costs on hardware and infrastructure maintenance.

## Operational Security Issues

- Most security issues arise not from the virtualization infrastructure itself but from operational issues
- Adapting existing security processes and solutions to work in the virtualized environment
- Most security solutions don’t care whether a machine is physical or virtual
- The datacenter and its workloads just became a much more dynamic and flexible place
- The risk of misconfiguration requires use of best practices specific to virtualization

## Security Advantages of Virtualization

Better Forensics and Faster Recovery After an Attack

- A compromised machine can be cloned in it current compromised state for forensic analysis
- Once cloned the VM can be immediately restored to a known good snapshot which is much faster than a physical server, reducing the impact of a security-related event.

## Security Advantages of Virtualization

Patching is Safer and More Effective

- You can quickly revert to a previous state if a patch is unsuccessful, making you more likely to install security patches sooner
- You can create a clone of a production server easily, making you more likely to test security patches and more likely to install security patches
- VMware Update Manager does patch scanning and compliance reporting, along with patch remediation for both online and offline VMs – again, making it more likely that security patches will be installed

## Security Advantages of Virtualization

More Cost Effective Security Devices

- You can put in place cost effective intrusion detection, vulnerability scanning, and other security related appliances, because you can put them in a VM instead of a physical server

## Security Advantages of Virtualization

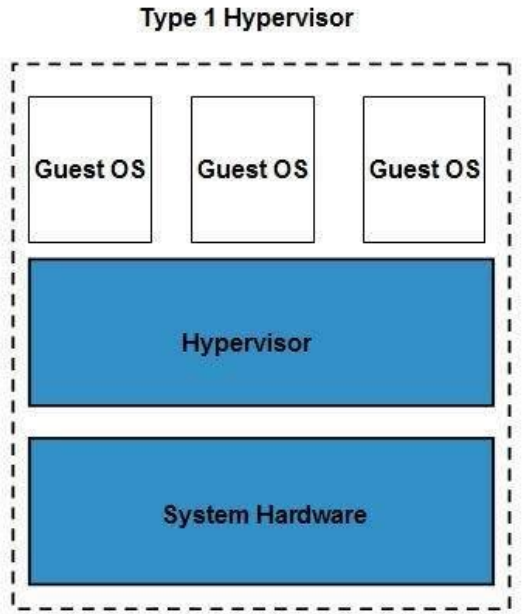
Future: Leveraging Virtualization to Provide Better Security

- Better Context – Provide protection from outside the OS, from a trusted context
- New Capabilities – view all interactions and contexts
  - CPU
  - Memory
  - Network
  - Storage

## Hypervisor

The **hypervisor** is a firmware or low-level program that acts as a Virtual Machine Manager.
There are two types of hypervisor:

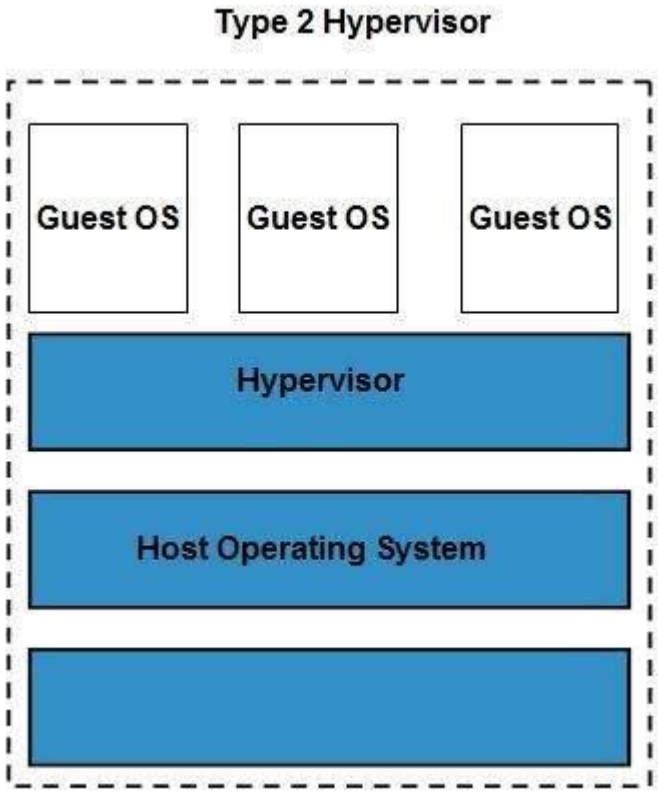
- **Type 1 hypervisor** executes on bare system. LynxSecure, RTS Hypervisor, Oracle VM, Sun xVM Server, VirtualLogic VLX are examples of Type 1 hypervisor.
- The **type1 hypervisor** does not have any host operating system because they are installed on a bare system.



## Hypervisor

- **Type 2 hypervisor** is a software interface that emulates the devices with which a system normally interacts.

- Containers, KVM, Microsoft Hyper V, VMWare Fusion, Virtual Server 2005 R2, Windows Virtual PC and **VMWare workstation 6.0** are examples of Type 2 hypervisor.



# Top hypervisors

## Hypervisor Usage

| Metrics | Primary | Also Use | Plan To Stop | Evaluating |
|---|---|---|---|---|
| VMware | 52% | 21% | 1% | 8% |
| Xen (Citrix & Oracle) | 18% | 32% | 7% | 31% |
| KVM (Fedora, Ubuntu, SUSE) | 9% | 30% | 5% | 19% |
| Microsoft Hyper-V | 9% | 16% | 6% | 18% |
| Red Hat (RHEL, RHEV) | 6% | 29% | 5% | 11% |
| Other | 6% | 14% | 8% | 12% |

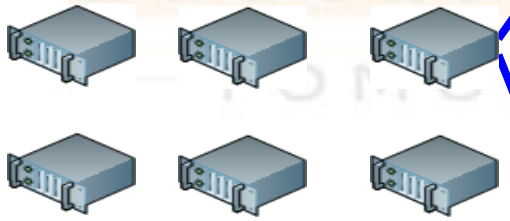
## Need of hypervisor

- Consolidation
- Provisioning
- Security

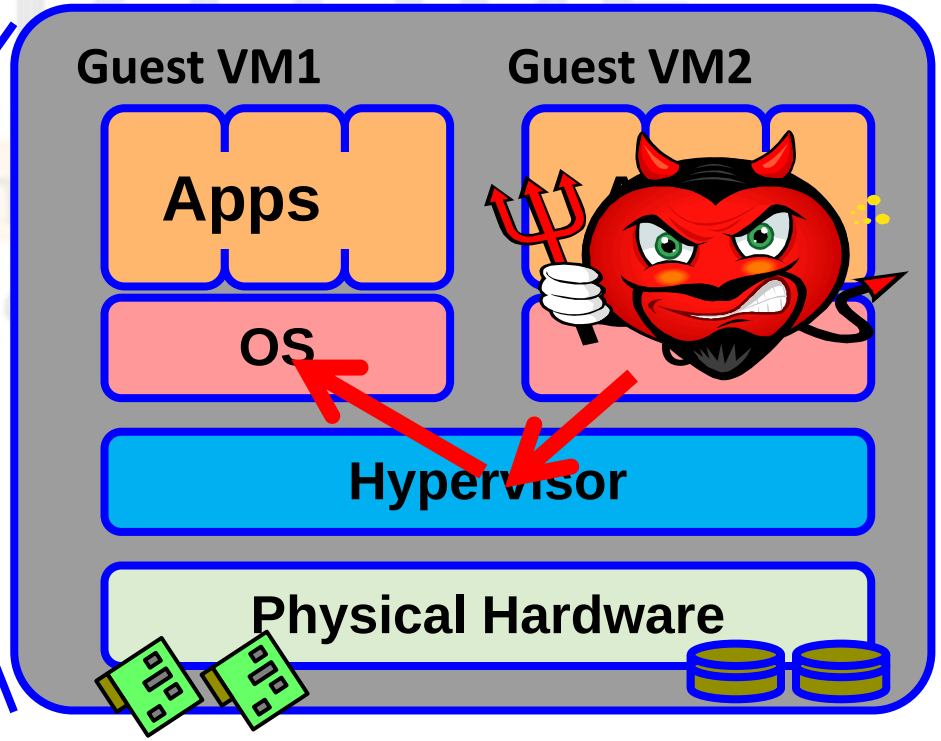
## Hypervisor Vulnerabilities

Malicious software can run on the same server:

- Attack hypervisor
- Access/Obstruct other VMs



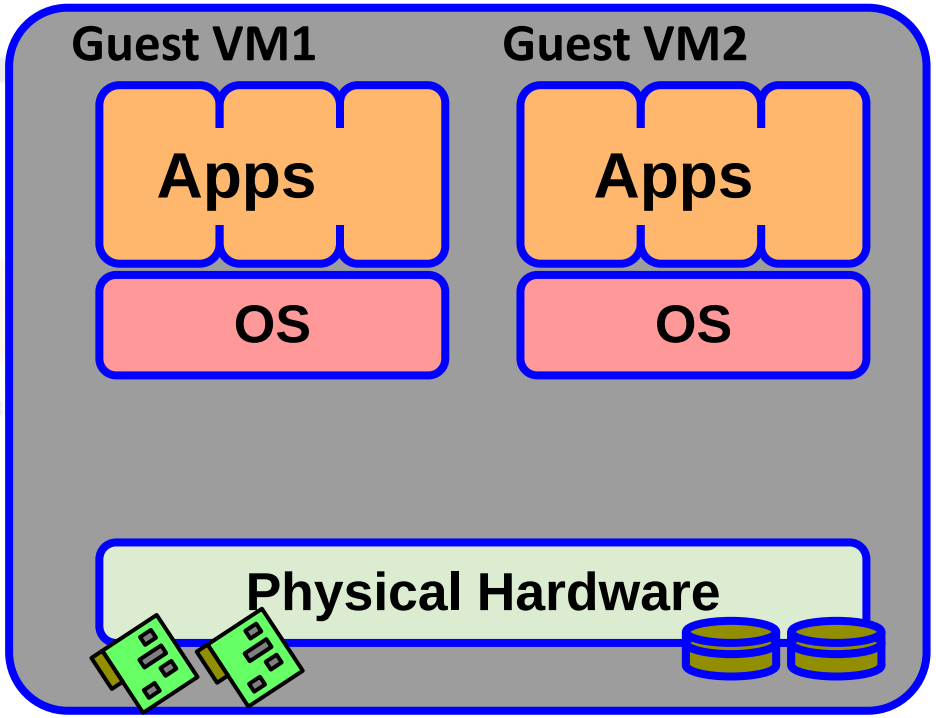
servers



## NoHype*

- NoHype removes the hypervisor
  - There's nothing to attack
  - Complete systems solution
  - Still retains the needs of a virtualized cloud infrastructure

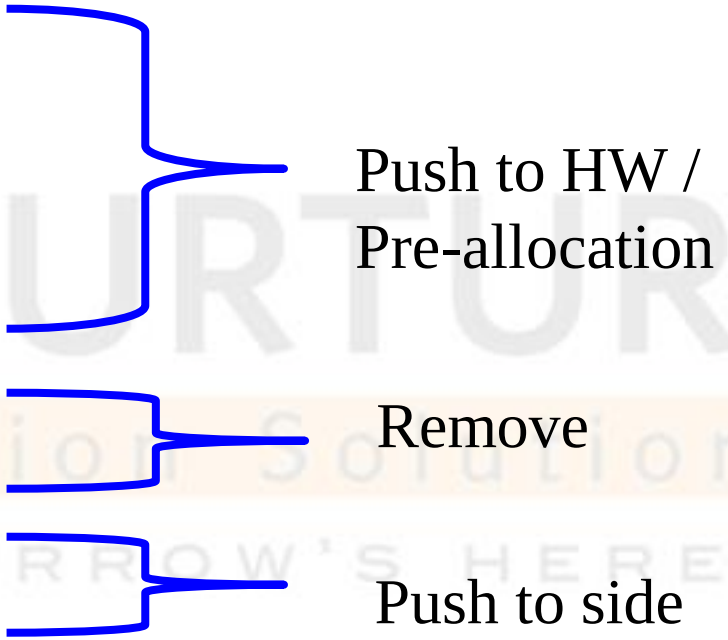
No hypervisor →




*NoHype: Virtualized Cloud Infrastructure without the Virtualization. E. Keller, J. Szefer, J. Rexford, R. Lee. ISCA 2010.

## Roles of the Hypervisor

- Isolating/Emulating resources
  - **CPU**: Scheduling virtual machines
  - **Memory**: Managing memory
  - **I/O**: Emulating I/O devices
- Networking
- Managing virtual machines



## Removing the Hypervisor

- Scheduling virtual machines
  - One VM per core
- Managing memory
  - Pre-allocate memory with processor support
- Emulating I/O devices
  - Direct access to virtualized devices
- Networking
  - Utilize hardware Ethernet switches
- Managing virtual machines
  - Decouple the management from operation

## Blue Pill

The blue pill rootkit is malware that executes as a hypervisor to gain control of computer resources.

The hypervisor installs without requiring a restart and the computer functions normally, without degradation of speed or services, which makes detection difficult.

## Virtual Machine Hyper Jumping

- Virtual machine hyper jumping is the latest type of attack on VM machine that exploits the hypervisor's weakness and allows a virtual machine (VM) to be accessed by malicious user.
- This make possible for malicious user or remote attacker to gain access to the hypervisor, host computer and other VMs in the infrastructure, and similar way being able to jump from one VM and one host to another.
- This is called hyper jumping or virtual machine guest hopping and hence it makes the whole VM infrastructure weak against this type of attack.

## How Can Hyper Jumping Happen?

- There are several reasons that can leave virtual environment to exploit with such type of vulnerability called hyper jumping. One of common issue is less secure Operating system.

- Prevision version of windows particularly the XP operating system that no longer receives the support or security updates from Microsoft, and in windows 7 version that lacks in modern security features and defense against poisoned cookies.

- In virtual environment in case if all traffic passes through the same set of network interface cards (NIC) then an attacker may overload the switch and then switch in order to preserve its performance start pushes all data out on its ports.

## How to Protect Infrastructure from Hyper Jumping?

- Grouping uplinks and separating them is one of the easiest ways to prevent the virtual environment from this vulnerability. Such that separate the database traffic from web facing traffic and prevents the database server to connect directly from internal network.
- You can Use VLANs, which hides the virtual machines from each other and allow the guest to connect only to the gateway.
- Follow basic and common security precautions such as built-in firewall in the virtual environment.
- Running machine with the latest operating system and get critical OS updates and security patches.

## Hypervisor vulnerabilities

- Some threats are focused on the hypervisors themselves
- Many security researchers have discussed flaws with hypervisor code that could allow directory traversal attacks, code execution through buffer overflows
- Other exploits, and even compromise through weak or non-existent credentials and poor management practices.
- The most practical threats to hypervisor platforms include insiders, such as virtualisation and cloud administrators.
- Recent research into side-channel attacks suggests potential compromise of virtual machine data through shared hardware caches and other hypervisor components.

## Hypervisor vulnerabilities

- Most of the announced vulnerabilities affecting ESXi, for example, were announced in 2011 and 2012.
- Numerous critical flaws in memory management and other functions have been found, making application of patches from suppliers a priority for administrators.
- The challenge, of course, is that patching these systems requires moving virtual machines to additional cluster members and coordinating potentially complex change control windows and plans.

## How to lock down hypervisors

- Take extra care in integrating hypervisor into your existing patch management processes. Setting up test systems that mimic production is highly recommended, as this will enable more rapid patching with less potential for negative impact.

- Another key step to take when securing hypervisor platforms is to limit remote and console access to the system. Most hypervisor platforms allow multiple types of access, including SSH, RDP.

- Take a minimalist approach to hypervisor management, allowing only the access explicitly needed to support the business environment.

## Minimizing the threat surface

- Properly configure any available settings and options for the particular hypervisor in use, tuning the system to minimize the threat surface and only allow services needed for successful operation.
- This includes many standard hardening tasks, such as limiting the users and groups on the local system, assessing critical file permissions and integrity, turning off services that are unnecessary, and securing those services that are.
- Every hypervisor platform has a variety of features that need to be evaluated for security, and these will vary from one supplier to the next.
- Securing your hypervisors requires a significant amount of planning and knowledge to manage properly.

## Self Assessment Question

1. Point out the wrong statement :

   a) Abstraction enables the key benefit of cloud computing: shared, ubiquitous access

   b) Virtualization assigns a logical name for a physical resource and then provides a pointer to that physical resource when a request is made

   c) All cloud computing applications combine their resources into pools that can be assigned on demand to users

   d) All of the mentioned

   **Answer: c**

2. Which of the following type of virtualization is also characteristic of cloud computing ?

a) Storage

b) Application

c) CPU

d) All of the mentioned

**Answer: d**

3. An operating system running on a Type __ VM is a full virtualization.

a) 1

b) 2

c) 3

d) All of the mentioned

**Answer: a**

4. In a _____ scheme, the VM is installed as a Type 1 Hypervisor directly onto the hardware.

a) paravirtualization

b) full virtualization

c) emulation

d) None of the mentioned

**Answer: b**

5. Which virtualization standard does the WebSphere Application Server Hypervisor Edition use?

a) Interoperable Image Format

b) Open Virtualization Format

c) Common Image Format

d) Open Virtual Appliance

**Answer: b**

6. Which capability a virtual network solution must provide?

a) High availability without connectivity redundancy

b) Orchestration of deployment

c) Transfer of vlan configuration keeping the mac and ip address is persistent

d) Automatic expiration of unused elements

**Answer: c**

7. What does the different virtual machines correspond to?

a) Same Server

b) Same Entity

c) Separate entities

d) None of these

**Answer: c**

8. When planning for virtualization technologies in a cloud solution what impacts the evaluation?

a) Management complexity of ethernet patch panels

b) Reduced link utilization

c) Lower operational risk

d) Network performance

**Answer: d**

9. What is not a benefit of Application virtualization?

a) Ability to isolate malicious or damaging applications

b) Ability to separate or group applications into different containers

c) Capability to run application which would otherwise conflict with one another

d) Ability to run non-native operating system applications

**Answer: b**

10. Which of the following is not a virtualization level?

a) Server level

b) Fabric level

c) Storage device level

d) File management level

**Answer: d**

11. Which term is used to describe hypervisor running multiple operating systems simultaneously?

a) Nested virtualization

b) Partial virtualization

c) Para Virtualization

d) Full Virtualization

**Answer: a**

12. What is the function of a hypervisor in a cloud solution?

a) It provides full virtualization

b) It emulates system calls

c) It optimizes CPU and I/O performance

d) It provides the means to share a CPU with multiple operating systems

**Answer: b**

13. Which of the following is not a main objective of virtualization?

a) Lowering IT management costs

b) Improved business flexibility

c) Reduced management and resource costs

d) Increased use of hardware resources

**Answer: a**

14. What is the storage virtualization technique which abstract multiple disk arrays and present them as a single storage resource, called?

a) Disk Virtualization

b) Disk array Virtualization

c) Block Virtualization

d) File System Virtualization

**Answer: c**

15. Which virtualization configuration characteristic is affected by the implementation of cloud infrastructure?

a) Lower server utilization

b) Higher latency

c) Higher transient use

d) Easier dependency/user management

**Answer: c**

## Summary

- System Admins can implement clusters of servers to make them more fault tolerant. However, even clusters have limits on their scalability, and not all applications work in a clustered environment.
- The machine on which the virtual machine is created is known as host machine and virtual machine is referred as a guest machine.
- Most security issues arise not from the virtualization infrastructure itself but from operational issues.
- The blue pill rootkit is malware that executes as a hypervisor to gain control of computer resources
- There are several reasons that can leave virtual environment to exploit with such type of vulnerability called hyper jumping. One of common issue is less secure Operating system.
- Recent research into side-channel attacks suggests potential compromise of virtual machine data through shared hardware caches and other hypervisor components.

## Assignment

1. Write a case study on role of XEN hypervisor in cloud architecture.
2. How does cloud security compare to on-premises security?
3. How does the cloud security sustain disasters affecting data centres or connections, and which data is backed up where?
4. How is security of the cloud service guaranteed when there are legal issues or administrative disputes?
5. Which standards make the cloud service portable and interoperable?

# Document Links

| Topics | URL | Notes |
|---|---|---|
| Virtualization Security | https://www.techopedia.com/definition/30243/virtualization-security/ | This link explains the concept and definition of Virtualization Security. |
| Virtualization Security in Data Centres and Clouds | https://www.cse.wustl.edu/~jain/cse571-11/ftp/virtual/index.html | You will learn Basic virtualization concepts, virtualization vulnerabilities, virtualization in cloud |
| Security Virtualization | https://www.sdxcentral.com/security/definitions/what-is-security-virtualization/ | This link explains about isolation and segmentation of security virtualization |
| Virtualization features and compliance | https://searchservervirtualization.techtarget.com/info/manage/Server-virtualization-compliance-and-governance | This link explains about the features and governance of virtualization |
| Securing the hypervisor | https://www.computerweekly.com/opinion/Securing-the-hypervisor-expert-tips | This link describes the expert view about hypervisor |

# Video Links

| Topics | URL | Notes |
|---|---|---|
| Need of virtualization | https://www.youtube.com/watch?v=WHIrGfNFwVo | This video demonstrates about the basic need of virtualization |
| Hardware enforced Security in hypervisor | https://www.youtube.com/watch?v=s3UfzxY1z40 | This video demonstrates how to implement hardware enforce security in hypervisors |
| Hypervisor | https://www.youtube.com/watch?v=VtXNIy_noWg | This video demonstrates hypervisor |
| Virtualization mechanism | https://www.youtube.com/watch?v=YBcZuIEXbmA | This video explains the mechanism of virtualization |
| Risk with virtualization | https://www.youtube.com/watch?v=Cy5OV_FM3S8 | This video explains the risks of virtualization |

# E-Book Links

| Topics | URL | Page Number |
|---|---|---|
| Overview of Virtualization | https://www.vmware.com/pdf/virtualization.pdf | 4-10 |
| Survey Of Hypervisors | https://pdfs.semanticscholar.org/5b40/872a5a5f4a577db2a00695f7191b2874f98a.pdf | All pages |
| Principles of Virtualization | https://sigops.org/s/conferences/sosp/2015/history/06-herbert.pdf | 1-8 |