15- Implementing Secure Cloud Solutions

Ahmed Sultan
Senior Technical Instructor
ahmedsultan.me/about

Outlines

15.1- Summarize Secure Cloud and Virtualization Services

15.2- Apply Cloud Security Solutions

15.1- Summarize Secure Cloud and Virtualization Services

15.2- Apply Cloud Security Solutions

CLOUD DEPLOYMENT MODELS

- A cloud deployment model classifies how the service is owned and provisioned.
- It is important to recognize the different impacts deployment models have on threats and vulnerabilities.
- Cloud deployment models can be broadly categorized as follows:
  - ✓ Public (or multi-tenant)—a service offered over the Internet by cloud service providers (CSPs) to cloud consumers, With this model, businesses can offer subscriptions or pay-as-you-go financing, while at the same time providing lower-tier services free of charge, As a shared resource, there are risks regarding performance and security.

CLOUD DEPLOYMENT MODELS (cont.)

- Cloud deployment models can be broadly categorized as follows (cont.)
  - ✓ Private—cloud infrastructure that is completely private to and owned by the organization, In this case, there is likely to be one business unit dedicated to managing the cloud while other business units make use of it, With private cloud computing, organizations can exercise greater control over the privacy and security of their services, This type of delivery method is geared more toward banking and governmental services that require strict access control in their operations.
  - ✓ Community—this is where several organizations share the costs of either a hosted private or fully private cloud, This is usually done in order to pool resources for a common concern, like standardization and security policies.

CLOUD SERVICE MODELS

- cloud services are often differentiated on the level of complexity and pre-configuration provided.
- These models are referred to as something.
- The three most common implementations are infrastructure, software, and platform:
  - ✓ Infrastructure as a service (IaaS): is a means of provisioning IT resources such as servers, load balancers, and storage area network (SAN) components quickly, Rather than purchase these components and the Internet links they require, you rent them on an as-needed basis from the service provider's data center, **Examples** include Amazon Elastic Compute Cloud (aws.amazon.com/ec2), Microsoft Azure Virtual Machines (azure.microsoft.com/services/virtual-machines), Oracle Cloud (oracle.com/cloud), and OpenStack (openstack.org).

CLOUD SERVICE MODELS (cont.)

- ✓ Software as a service (SaaS): is a different model of provisioning software applications, Rather than purchasing software licenses for a given number of seats, a business would access software hosted on a supplier's servers on a pay-as-you-go or lease arrangement (on-demand), Virtual infrastructure allows developers to provision on-demand applications much more quickly than previously, The applications can be developed and tested in the cloud without the need to test and deploy on client computers, **Examples** include Microsoft Office 365 (microsoft.com/en-us/microsoft-365/enterprise), Salesforce (salesforce.com), and Google G Suite (gsuite.google.com).

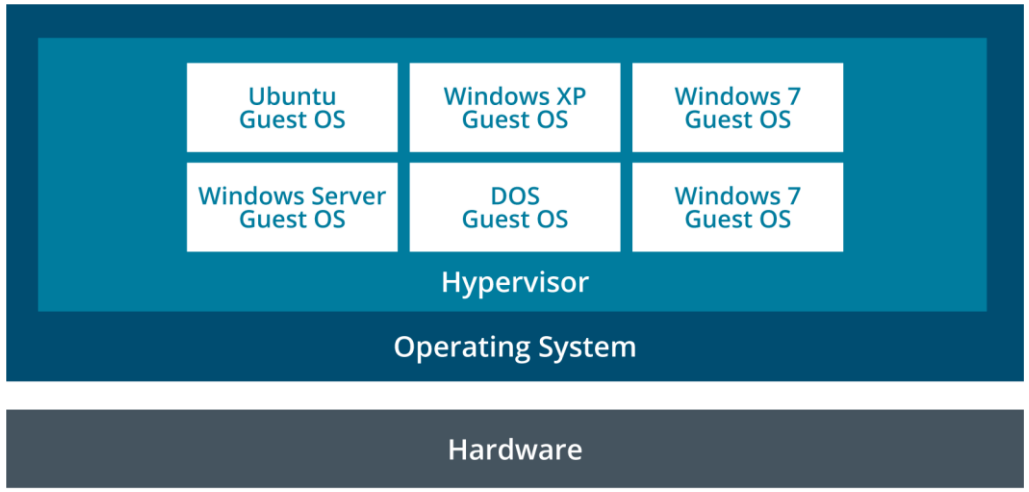
- ✓ Platform as a service (PaaS): provides resources somewhere between SaaS and IaaS, A typical PaaS solution would provide servers and storage network infrastructure (as per IaaS) but also provide a multi-tier web application/database platform on top, This platform could be based on Oracle or MS SQL or PHP and MySQL, **Examples** include Oracle Database (oracle.com/database), Microsoft Azure SQL Database (azure.microsoft.com/services/sql-database), and Google App Engine (cloud.google.com/appengine).

VIRTUALIZATION TECHNOLOGIES AND HYPERVISOR TYPES

- Virtualization means that multiple operating systems can be installed and run simultaneously on a single computer.
- A virtual platform requires at least three components:
  1. Host hardware—the platform that will host the virtual environment, Optionally, there may be multiple hosts networked together.
  2. Hypervisor/Virtual Machine Monitor (VMM)—manages the virtual machine environment and facilitates interaction with the computer hardware and network.
  3. Guest operating systems, Virtual Machines (VM), or instances—operating systems installed under the virtual environment.

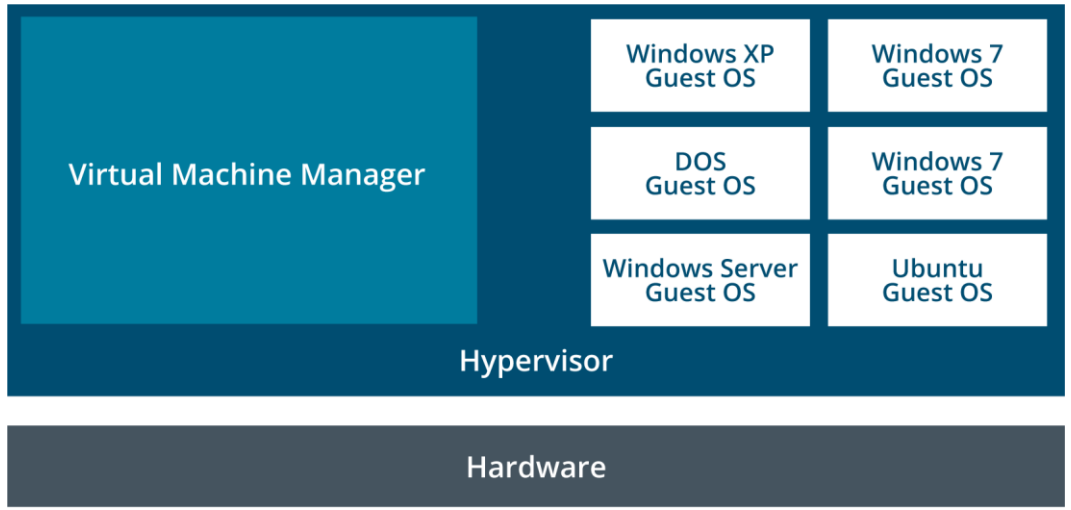
VIRTUALIZATION TECHNOLOGIES AND HYPERVISOR TYPES (cont.)

- In a guest OS (or host-based) system, the hypervisor application (known as a Type II hypervisor) is itself installed onto a host operating system.
- Examples of host-based hypervisors include VMware Workstation, Oracle Virtual Box, and Parallels Workstation.
- The hypervisor software must support the host OS.



VIRTUALIZATION TECHNOLOGIES AND HYPERVISOR TYPES (cont.)

- A bare metal virtual platform means that the hypervisor (Type I hypervisor) is installed directly onto the computer and manages access to the host hardware without going through a host OS.
- Examples include VMware ESXi Server, Microsoft's Hyper-V, and Citrix's XEN Server.



VIRTUAL DESKTOP INFRASTRUCTURE AND THIN CLIENTS

- Virtual desktop infrastructure (VDI) refers to using a VM as a means of provisioning corporate desktops.
- In a typical VDI, desktop computers are replaced by low-spec, low-power thin client computers.
- When the thin client starts, it boots a minimal OS, allowing the user to log on to a VM stored on the company server infrastructure.
- The user makes a connection to the VM using some sort of remote desktop protocol (Microsoft Remote Desktop or Citrix ICA, for instance).
- The thin client has to find the correct image and use an appropriate authentication mechanism.

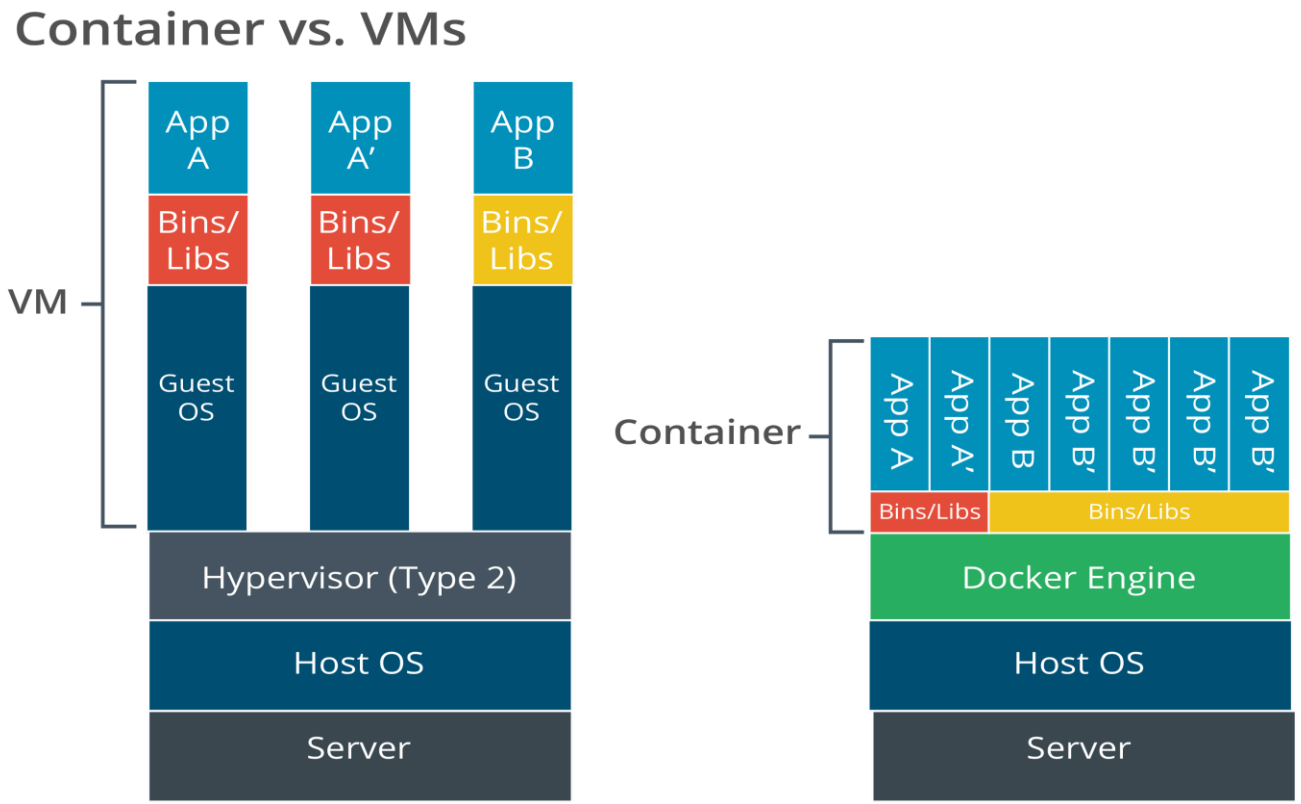
VIRTUAL DESKTOP INFRASTRUCTURE AND THIN CLIENTS (cont.)

- All application processing and data storage in the virtual desktop environment (VDE) is performed by the server.
- The thin client computer must only be powerful enough to display the screen image, play audio, and transfer mouse, key commands and video, and audio information over the network.
- All data is stored on the server, so it is easier to back up and the desktop VMs are easier to support and troubleshoot.
- They are better "locked" against unsecure user practices because any changes to the VM can easily be overwritten from the template image.
- With VDI, it is also easier for a company to completely offload their IT infrastructure to a third-party services company.

CONTAINER

- Container virtualization dispenses with the idea of a hypervisor and instead enforces resource separation at the operating system level.
- The OS defines isolated "cells" for each user instance to run in.
- Each cell or container is allocated CPU and memory resources, but the processes all run through the native OS kernel.
- One of the best-known container virtualization products is Docker (docker.com).

CONTAINER (cont.)



15.1- Summarize Secure Cloud and Virtualization Services

15.2- Apply Cloud Security Solutions

CLOUD SECURITY CONTROLS

- Clouds use the same types of security controls as on-premises networks, including identity and access management (IAM), endpoint protection (for virtual instances), resource policies to govern access to data and services, firewalls to filter traffic between hosts, and logging to provide an audit function.
- Most CSP's will provide these security controls as native functionality of the cloud platform.
- Google's firewall service is an example of this type of cloud native control (cloud.google.com/firewalls).
- The controls can be deployed and configured using either the CSP's web console, or programmatically via a command line interface (CLI) or application programming interface (API).

CLOUD SECURITY CONTROLS (cont.)

- Application Security and IAM
  - ✓ Application security in the cloud refers both to the software development process and to identity and access management (IAM) features designed to ensure authorized use of applications.
  - ✓ Just as with on-premises solutions, cloud-based IAM enables the creation of user and user security groups, plus role-based management of privileges.

CLOUD SECURITY CONTROLS (cont.)

- Secrets Management
  - A cloud service is highly vulnerable to remote access.
  - A failure of credential management is likely to be exploited by malicious actors.
  - You must enforce strong authentication policies to mitigate risks:
    - ✓ Do not use the root user for the CSP account for any day-to-day logon activity.
    - ✓ Require strong multifactor authentication (MFA) for interactive logons. Use conditional authentication to deny or warn of risky account activity.

HIGH AVAILABILITY

- One of the benefits of the cloud is the potential for providing services that are resilient to failures at different levels, such as component, server, local network, site, data center, and wide area network.
- The CSP uses a virtualization layer to ensure that compute, storage, and network provision meet the availability criteria set out in its SLA.
- In terms of storage performance tiers, high availability (HA) refers to storage provisioned with a guarantee of **99.99%** uptime or better.
- As with on-premises architecture, the CSP uses redundancy to make multiple disk controllers and storage devices available to a pool of storage resource.
- Data may be replicated between pools or groups, with each pool supported by separate hardware resources.