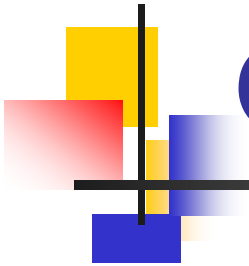


Overview

Domain 1: General Security Concepts

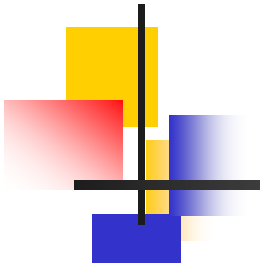
- M1: Introduction to Information Security
  - Key Security Concepts and Models
- M2: Cryptography
  - Encryption, Symmetric/Asymmetric Cryptography, Key Management

Domain 2: Security Threats, Vulnerabilities, and Mitigations

- M3: Threat, Attacks, Vulnerability, and Mitigations
  - Types of Threats, Attacks, and Vulnerabilities, Mitigation Techniques

Domain 3: Security Architecture

- **M4: Cloud Computing**
  - **Could computing, Virtualization, and Cloud Security Controls**
- M5: Network Security
  - Secure Network Design, Network Security Techniques

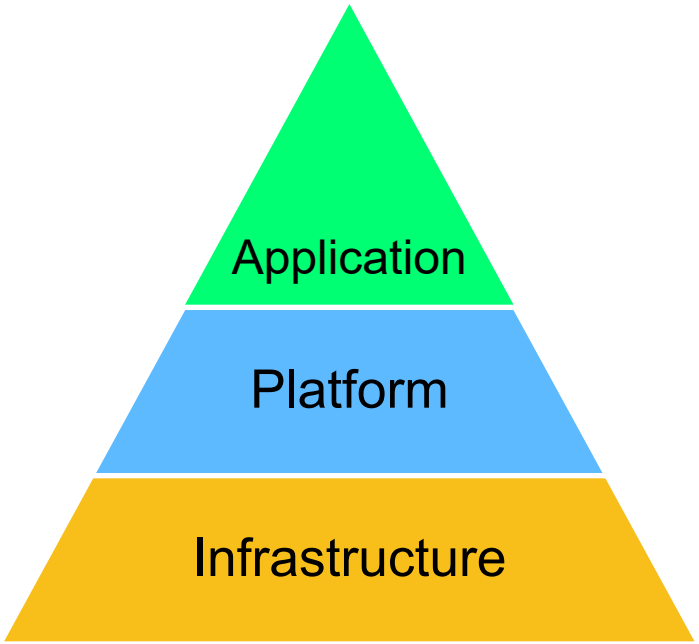


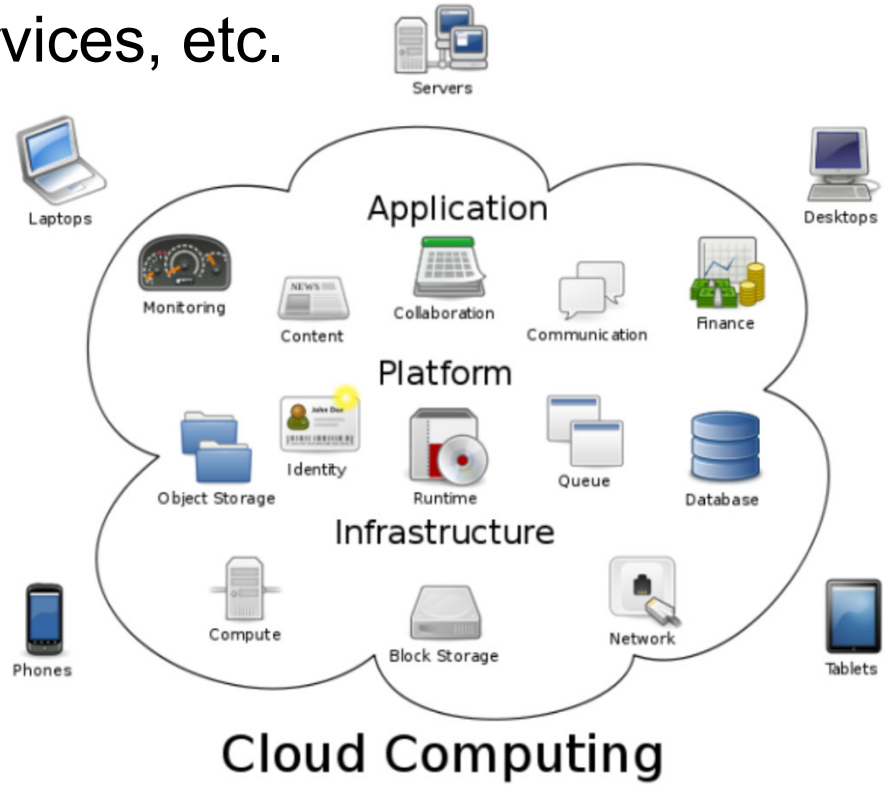
M4. Cloud Security

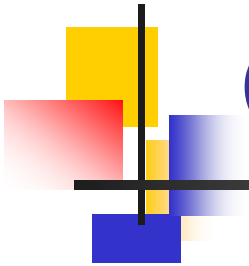
- Cloud Computing
  - Definitions, Roles and Drivers for Cloud Computing
  - Cloud Deployment Models, Categorization of Cloud Service
  - Governance Structure of Cloud Computing
- Virtualization Technology
  - Hypervisor, Types of Hypervisor
- Cloud Security Issues and Controls
  - Virtualization Security Issues: VM Sprawl, VM Escape
  - Complexity, No security Perimeter, Lack of Auditability, Regulatory Compliance
  - Cloud Security Controls: Data Security Control, Cloud Resource Control, Resource Policy, Cloud Network Security Control

Cloud Computing 1/2

- IT resources provided as a service
  - servers, applications, storages, networks, databases, platforms, security services, etc.







Cloud Computing 2/2

- **Cloud computing** is a model for enabling delivering a shared pool of configurable computing resources to a remote customer over a network (e.g., Gmail, Amazon Web Services, Salesforce.com)

- On-Premises or Off-Premises

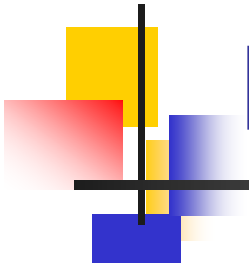
On-Premises vs. Off-Premises

- On-Premises
  - Systems that are on-site
  - The physical system can be accessed

- Off-Premises
  - Systems that are not on-site
  - Cannot be physically accessed

Cloud Computing 2/2

- **Cloud entities**: cloud customer, cloud service provider, cloud service partner, managed service provider (MSP), managed security service provider (MSSP)
  - MSP
    - Manages day to day services to customers
    - Third party - outsourced
    - HR, contract management, vendor management, etc.…
  - MSSP
    - Similar to MSP, but for securing devices
    - Manages firewalls, intrusion detection, VPN management, vulnerability scanning, etc.…

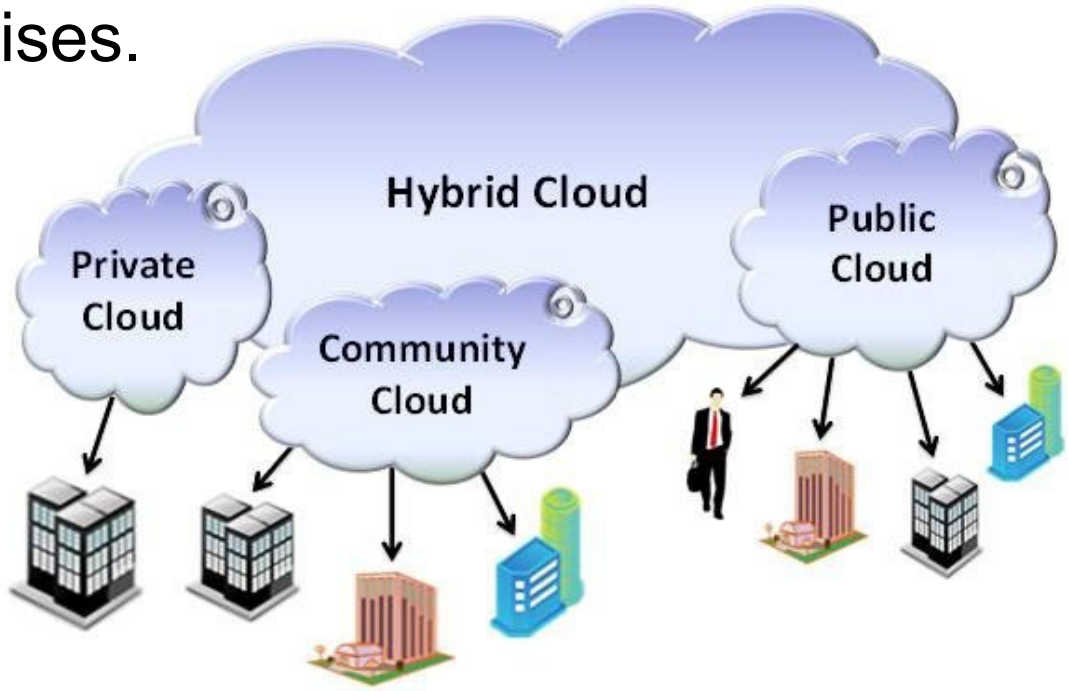


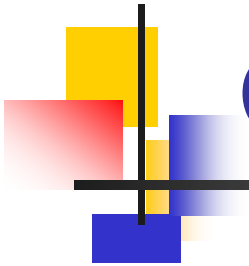
Benefits

- Cost & management
  - On-demand self-service
  - Economies of scale
- Reliability
  - Massive, redundant, shared resources
- Sustainability
  - Hardware not owned
- Elasticity
  - Reduced Time to deployment
  - Expanding and contracting quickly
- Scalability (horizontal and vertical scaling)
  - On demand provisioning, co-locate data and compute

Cloud Deployment Models 1/2

- **Private Cloud**: Computing architecture is dedicated to the customer and is not shared with other organizations.
- **Public Cloud**: Computing infrastructure is hosted at the vendor's premises.





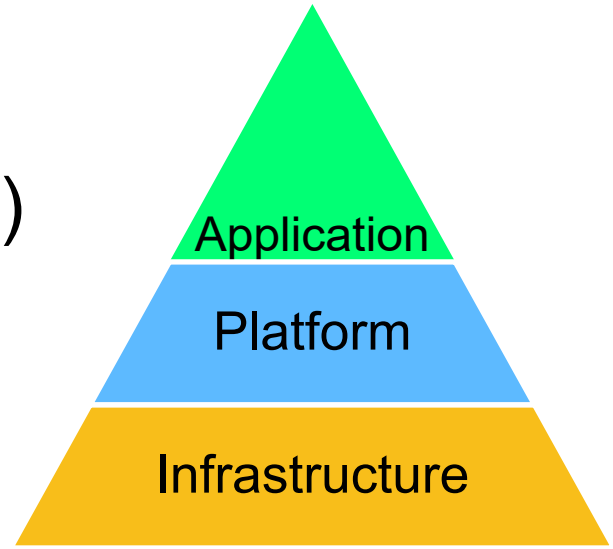
Cloud Deployment Models (2/2)

- **Hybrid Cloud**: Organizations host some critical, secure applications in private clouds. The not so critical applications are hosted in the public cloud
  - **Cloud bursting**: the organization uses its own infrastructure for normal usage, but cloud is used for peak loads.

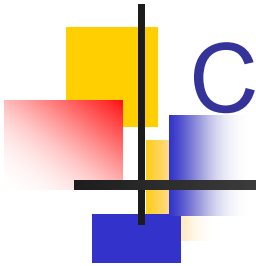
- **Community Cloud:** shared with a consortium

Categorization of Cloud Service

- Everything as a Service (XaaS) notation

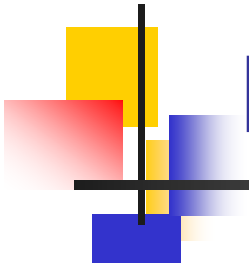


- Software as a service (SaaS)
  - Customer purchases a complete software offering on the cloud.
  - Pay-per-use basis.
  - E.g., Google Gmail, MS Office 365, Dropbox, Salesforce.com's CRM, etc.



Categorization of Cloud Service (Cont.)

- Platform as a Service (PaaS)
  - Purchase app platform to run own application code
  - E.g., AWS Lambda Service, Google Application Engine
- Infrastructure as a service (IaaS)
  - Purchase hardware related services including servers, storage services (database or disk storage) or virtual servers
  - E.g., Amazon Web Services (AWS), MS Azure, Amazon EC2

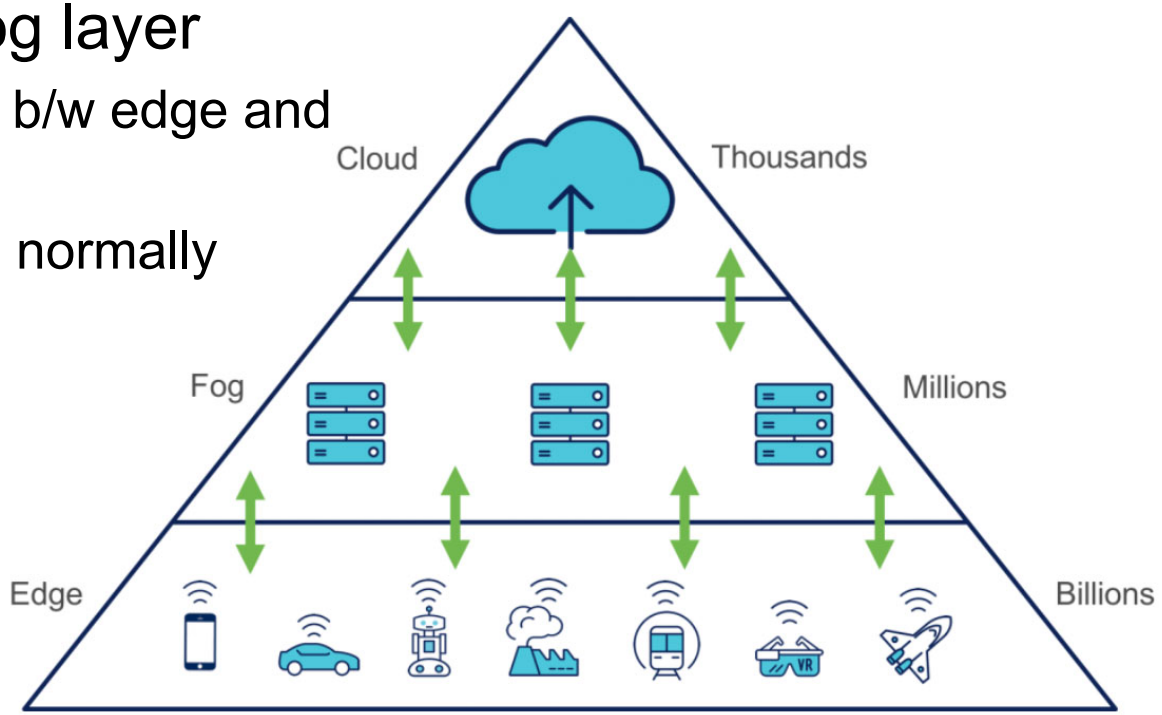


More Refined Categorization

- Application-as-a-service (AaaS)
- Database-as-a-service (DBaS)
- Function-as-a-service (FaaS)
- Information-as-a-service
- Integration-as-a-service
- Management/governance-as-a-service
- Process-as-a-service
- Security-as-a-service (SEaS)
- Storage-as-a-service (STaS)
- Testing-as-a-service

Fog and Edge Computing

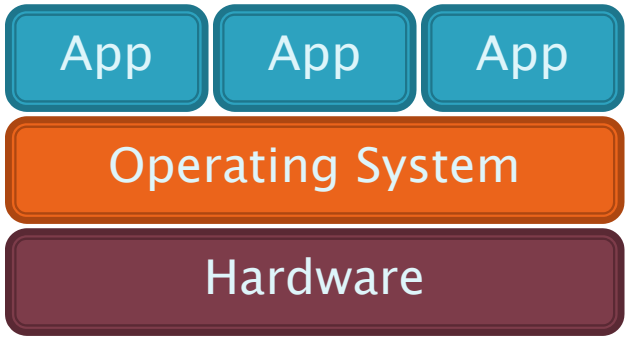
- Edge Computing at edge layer
  - Computing processes closed to the source of data device (IoTs)
  - Smart devices, autonomous vehicles
- Fog Computing at fog layer
  - Ways to handle data b/w edge and cloud computing
  - Computing tasks are normally carried out on a LAN

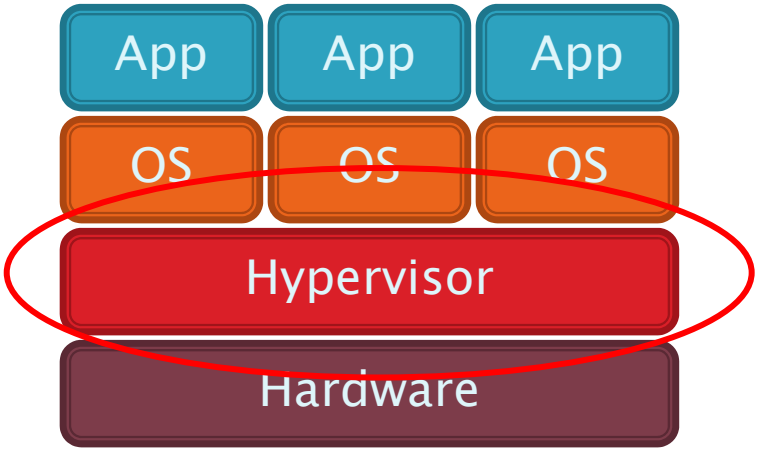


Source: Edge Computing : learn to delegate - OCTO Talks !

Virtualization Technology

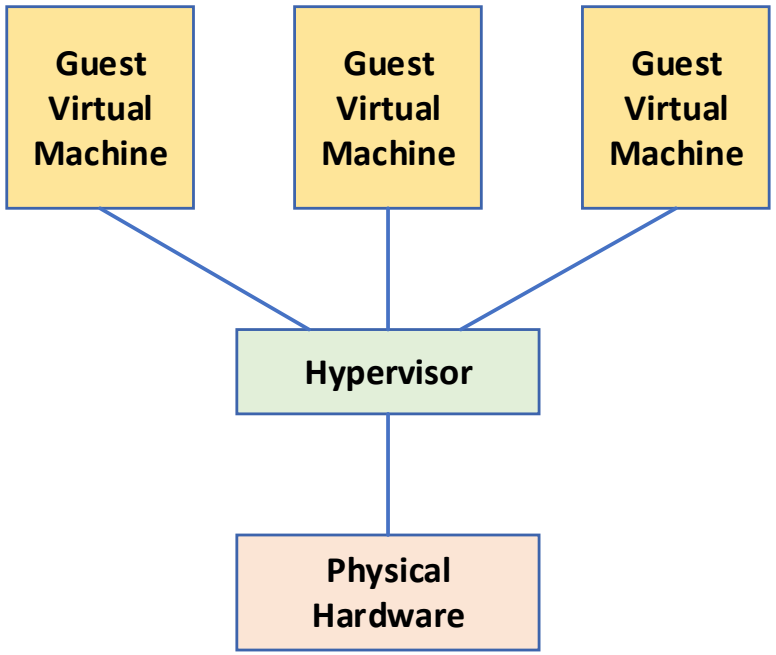
- The driving force behind cloud computing
- A *virtual machine* (*VM*) is a simulated software-based emulation of a computer
- **Hypervisor** (special software for VM monitoring) tricks each guest into thinking it is running on dedicated hardware



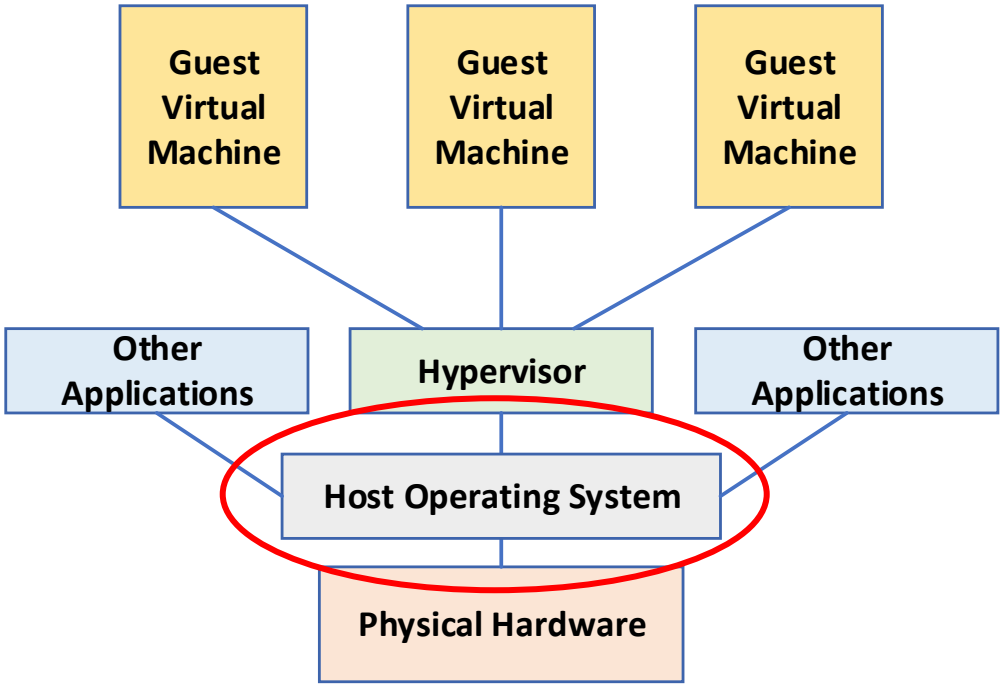


Type 1 vs Type 2 Hypervisor

Type 1 Hypervisor

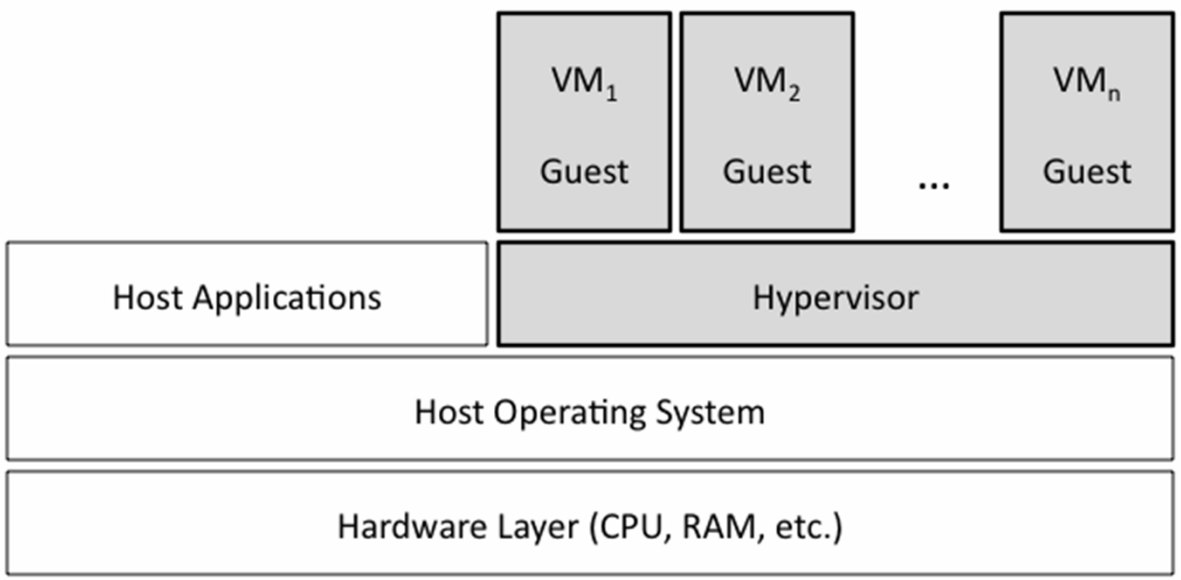


Type 2 Hypervisor



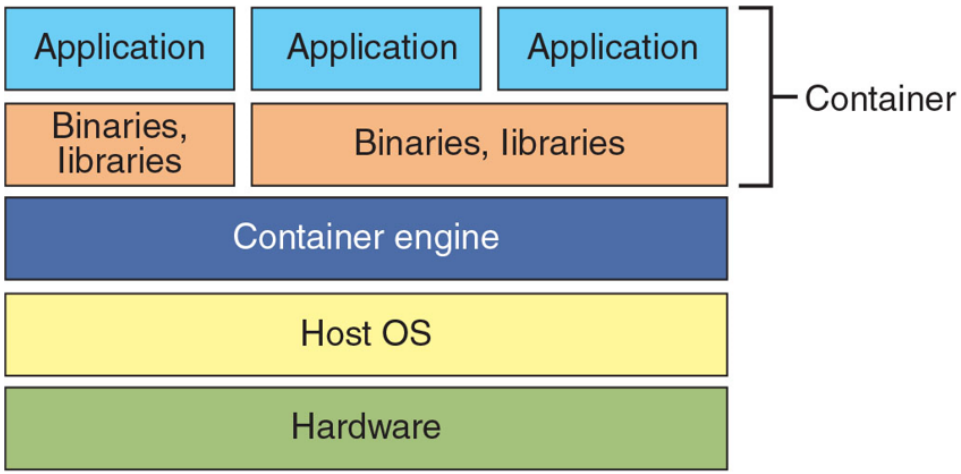
VM Isolation (T2 hypervisor)

- Using a VM for each application provides isolation
  - More than running 2 apps on same server



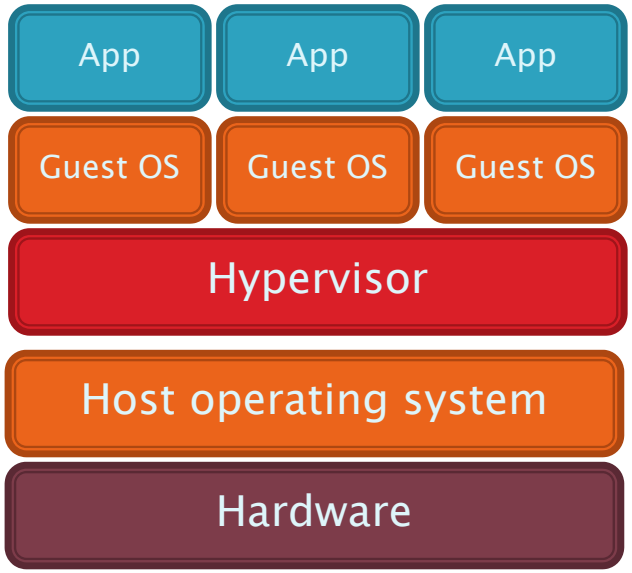
Container

- Lightweight application virtualization software that packages all the code
  - Application is very reliable and runs very quickly
  - Can be used from one environment another
  - Similar to virtual machines
    - Contain much less than VM
    - Quicker than VM

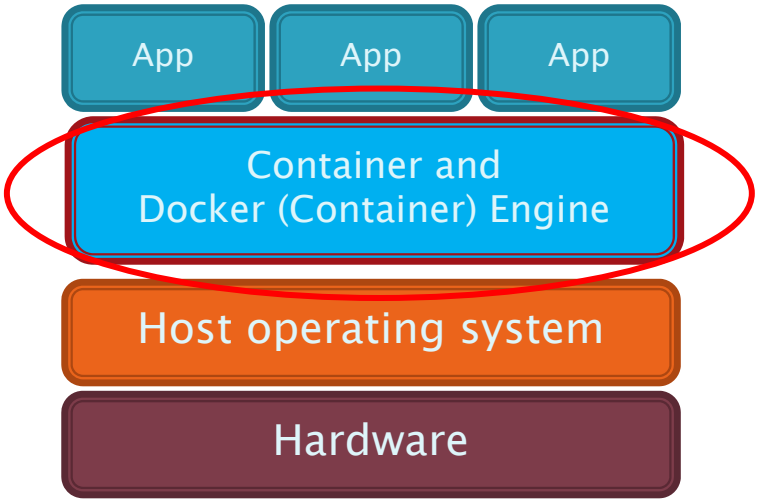


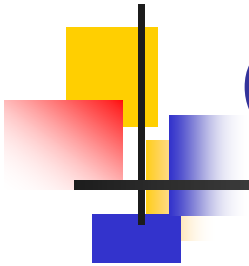
VMs vs. Cloud Containers

Virtual Machines



Containers

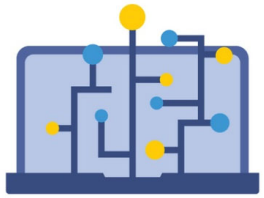




Cloud Security Issues

- Virtualization relevant Issues
  - VM Sprawl, VM Escape
- General Cloud Computing Issues
  - Accountability and Complexity
  - Larger Attack Surface/No Security Perimeter
  - Snapshot Data
  - Lack of Auditability
  - Regulatory Compliance, etc.

VM Sprawl



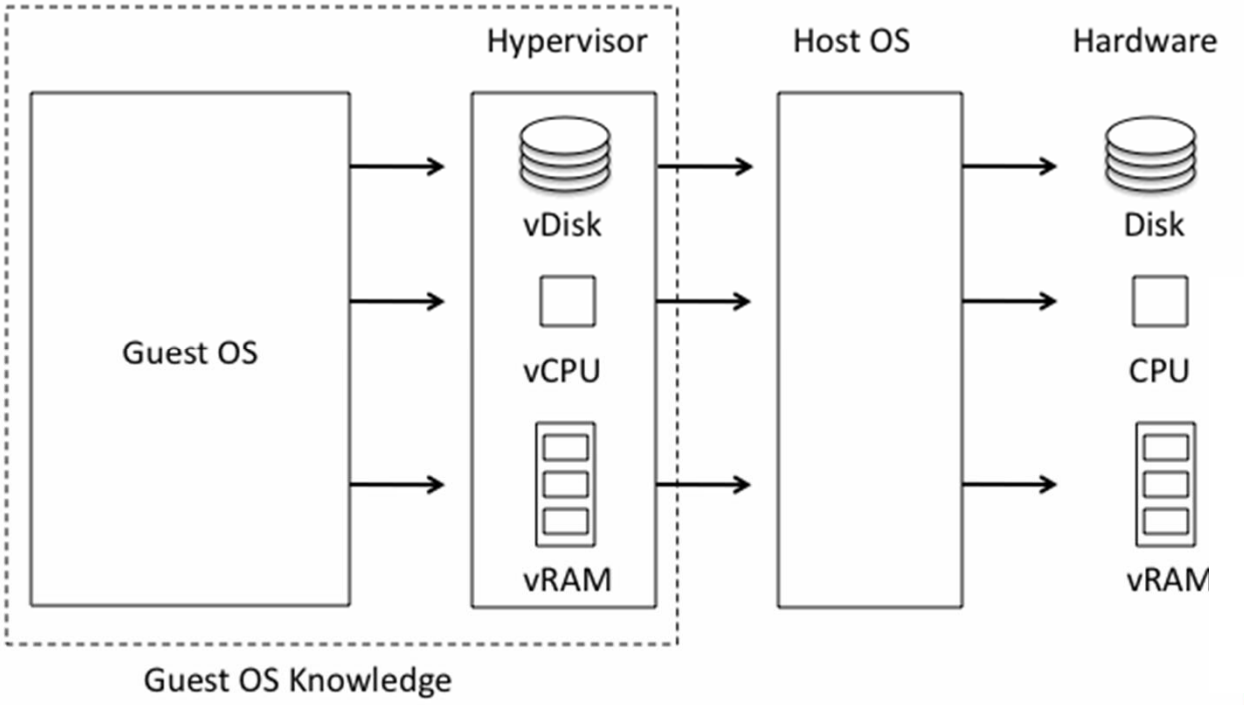
- VM Sprawl – unused and unmaintained servers
  - The disorganization and uncontrolled spreading
  - Caused by lack of management
- VM Sprawl Avoidance
  - Done by an organization (everyone following same policies)
    - Similar storage names and locations
  - Admins can easily locate and use resources on VMs

VM Escape

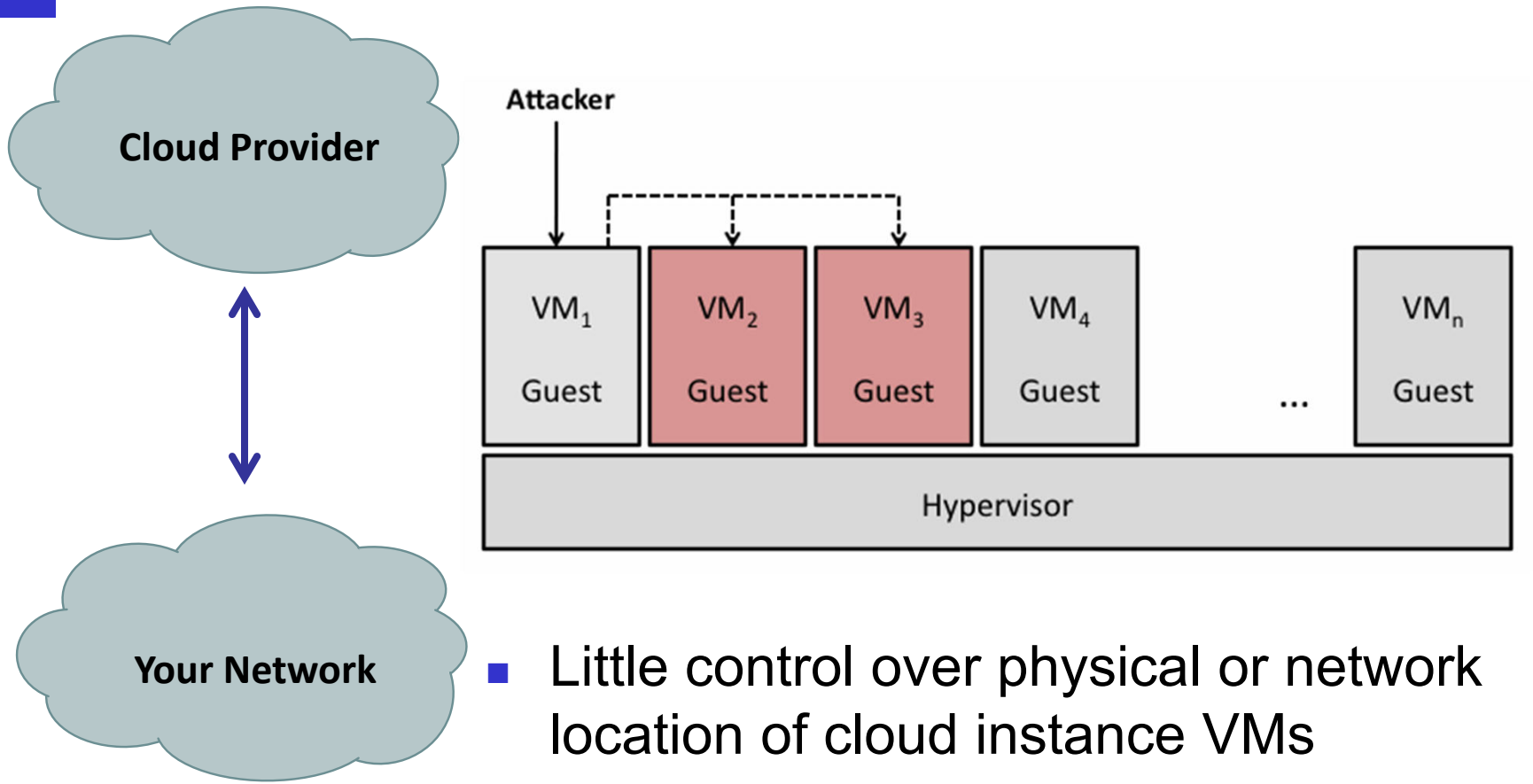
- VM Escape Attacks
  - An attacker gains access to host machine through the VM
- Why is this bad?
  - Attacker can control all the VMs on the system
  - Attacker can have complete control over the host machine

Accountability/Complexity

- Hypervisor is often another layer on top of host OS, adding complexity and vulnerabilities



Larger Attack Surface – No Security Perimeter



- Little control over physical or network location of cloud instance VMs
- Network access must be controlled on a host by host basis.

Lack of Auditability

- Only cloud provider has access to full network traffic, hypervisor logs, physical machine data.
- Need mutual auditability
  - Ability of cloud provider to audit potentially malicious or infected client VMs.
  - Ability of cloud customer to audit cloud provider environment.

Regulatory Compliance

- Cloud service is subject to a wide variety of international, federal, state, and local security regulations (e.g., data sovereignty). A company follows the laws enforced by governing bodies in their geography or rules required.

Cloud Data Security Controls

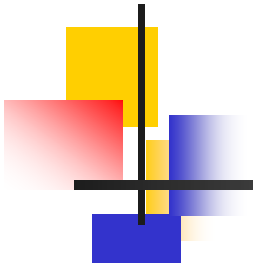
- Data/Storage
  - Storing data on the cloud
  - Important factors:
    - Permissions
      - Who has permission to access the data
      - What data can they access?
    - Encryption
      - Make sure the data is encrypted
      - Protects the data
    - Replication
      - In case some of the data is destroyed
    - High Availability
      - Always accessible

Cloud Resource Controls

- Computing Resource Controls
  - Security Groups
    - Compute security group profile is allocated by using a security group template
      - Includes the cloud account, the location of the resource, and the security rules.
  - Dynamic Resource Allocation
    - Upgrades or downscales cloud resources
      - As demand grows or falls
  - Instance Awareness
    - VM instances must be monitored to avoid an attacker placing an unmanaged VM that could lead to VM sprawl and the VM escape.

Cloud Network Security Controls

- Firewall considerations
  - Cost
    - Can range from free to several hundred dollars per month
  - Segmentation requirements
    - A Zero-Trust model is used in cloud environments
    - In this model, each individual must provide identification to gain access to the cloud environment
  - Cloud Native Controls versus Third-Party Solutions
    - AWS has their own tool, AWS Cloud Formation
    - Third-parties may add tools that provide more flexibility



Summary

- Cloud Computing
  - Definition, Roles and Drivers for Cloud Computing
  - Cloud Deployment Models, Categorization of Cloud Service, Governance Structure of Cloud Computing
- Virtualization Technology
  - Hypervisor, Types of Hypervisor
- Security Issues and Controls
  - Virtualization relevant Issues: VM Sprawl, VM Escape
  - Complexity, No security Perimeter, Lack of Auditability, Regulatory Compliance,
  - Cloud Security Controls: Cloud Data, Cloud Resource, Resource Policy, Cloud Network Security Control