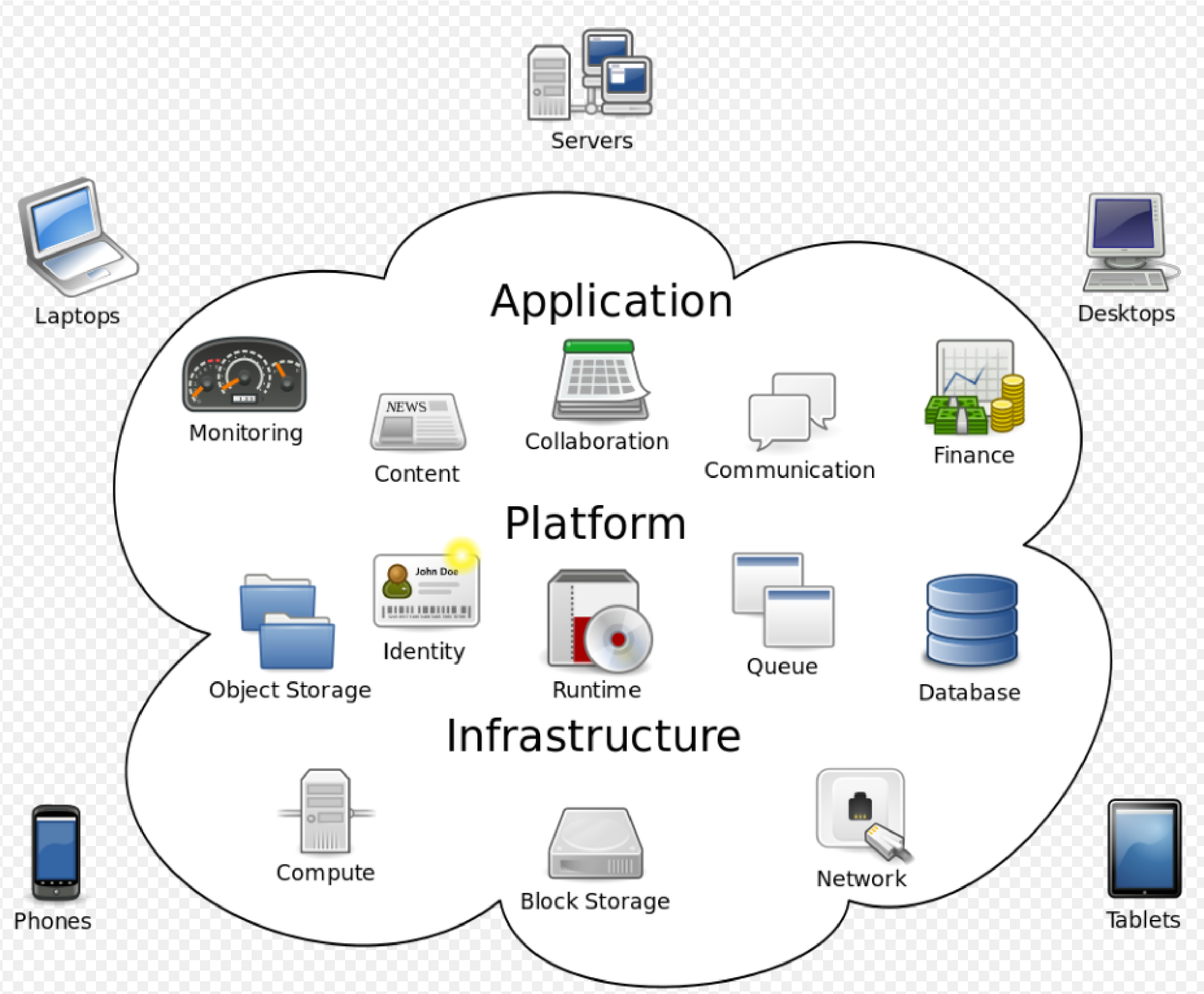
Secure Operating Systems

Nikos Tziritas

Cloud Computing (Part 1)



Cloud computing

What is Cloud Computing? (1/2)

- **Cloud computing** is a type of Internet-based computing that provides shared computer processing resources and data to computers and other devices on demand.
- It is a model for enabling ubiquitous, on-demand access to a shared pool of configurable computing resources (e.g., computer networks, servers, storage, applications and services), which can be rapidly provisioned and released with minimal management effort.
- Cloud computing and storage solutions provide users and enterprises with various capabilities to store and process their data in either privately owned, or third-party data centers[3] that may be located far from the user–ranging in distance from across a city to across the world.

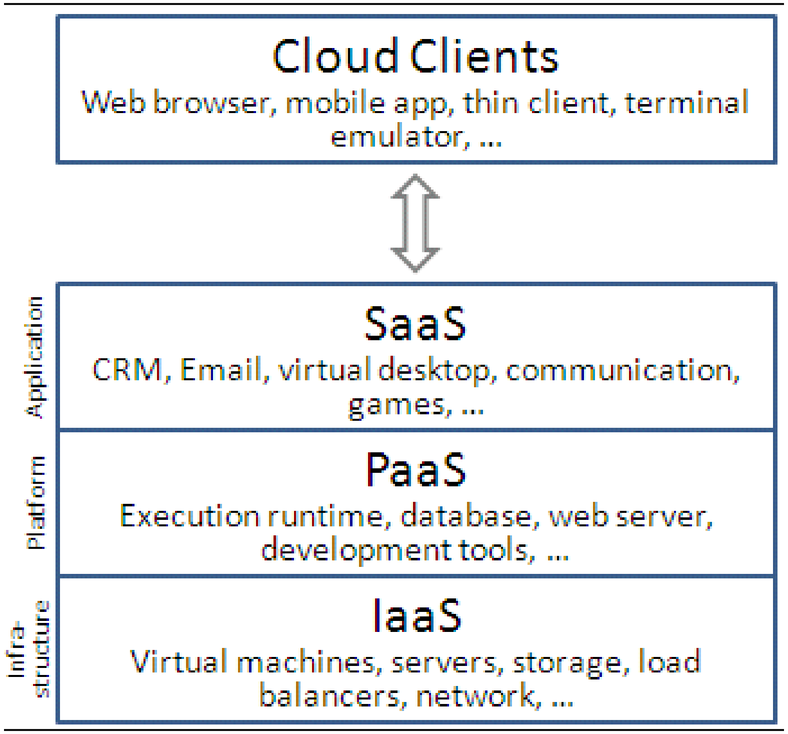
What is Cloud Computing ? (2/2)

- Advocates claim that cloud computing allows companies to avoid up-front infrastructure costs (e.g., purchasing servers).
- As well, it enables organizations to focus on their core businesses instead of spending time and money on computer infrastructure.
- Proponents also claim that cloud computing allows enterprises to get their applications up and running faster, with improved manageability and less maintenance, and enables information technology (IT) teams to more rapidly adjust resources to meet fluctuating and unpredictable business demand.
- Cloud providers typically use a "pay as you go" model.

Service Models (1/2)

- *Software as a Service (SaaS).* The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure.
- *Platform as a Service (PaaS).* The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider.
- *Infrastructure as a Service (IaaS).* The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).

Service Models (2/2)



Cloud Clients

Web browser, mobile app, thin client, terminal emulator, ...

SaaS

CRM, Email, virtual desktop, communication, games, ...

PaaS

Execution runtime, database, web server, development tools, ...

IaaS

Virtual machines, servers, storage, load balancers, network, ...

Security Concerns for Cloud-based Services

- According to Cloud Security Alliance (CSA), over 70 percent of the world’s businesses now operate – at least in part – on the cloud.
- With benefits like lower fixed costs, higher flexibility, automatic software updates, increased collaboration, and the freedom to work from anywhere, 70 percent isn’t a big surprise.
- Although cloud services have ushered in a new age of transmitting and storing data, many companies are still hesitant or make the move without a clear plan for security in place.

Data Breaches

- Cloud computing and services are relatively new, yet data breaches in all forms have existed for years.
- The question remains: “With sensitive data being stored online rather than on premise, is the cloud inherently less safe?”
- A study conducted by the Ponemon Institute entitled “Man In Cloud Attack” reports that over 50 percent of the IT and security professionals surveyed believed their organization’s security measures to protect data on cloud services are low.
- Overall data breaching is three times more likely to occur for businesses that utilize the cloud than those that don’t.

Hijacking of Accounts

- The growth and implementation of the cloud in many organizations has opened a whole new set of issues in account hijacking.
- Attackers now have the ability to use your (or your employees') login information to remotely access sensitive data stored on the cloud; additionally, attackers can falsify and manipulate information through hijacked credentials.
- Other methods of hijacking include scripting bugs and reused passwords, which allow attackers to easily and often without detection steal credentials.

Insider Threat

- An attack from inside your organization may seem unlikely, but the insider threat does exist.
- Employees can use their *authorized* access to an organization's cloud-based services to misuse or access information such as customer accounts, financial forms, and other sensitive information.
- Additionally, these insiders don't even need to have malicious intentions.

Malware Injection

- Malware injections are scripts or code embedded into cloud services that act as “valid instances” and run as SaaS to cloud servers.
- This means that malicious code can be injected into cloud services and viewed as part of the software or service that is running within the cloud servers themselves.
- Once an injection is executed and the cloud begins operating in tandem with it, attackers can eavesdrop, compromise the integrity of sensitive information, and steal data.

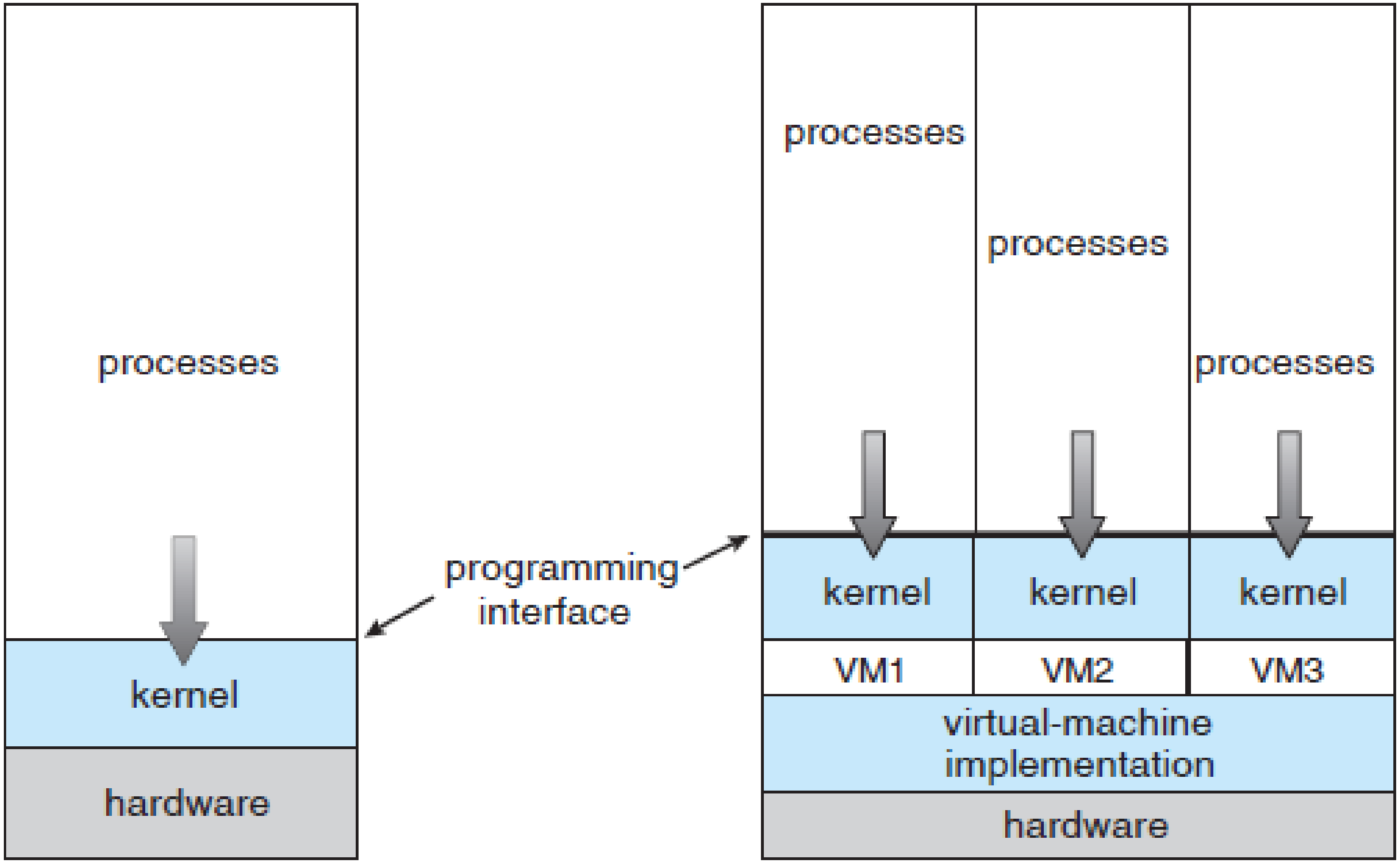
Abuse of Cloud Services

- The expansion of cloud-based services has made it possible for both small and enterprise-level organizations to host vast amounts of data easily.
- However, the cloud’s unprecedented storage capacity has also allowed both hackers and authorized users to easily host and spread malware, illegal software, and other digital properties.
- In some cases this practice affects both the cloud service provider and its client.

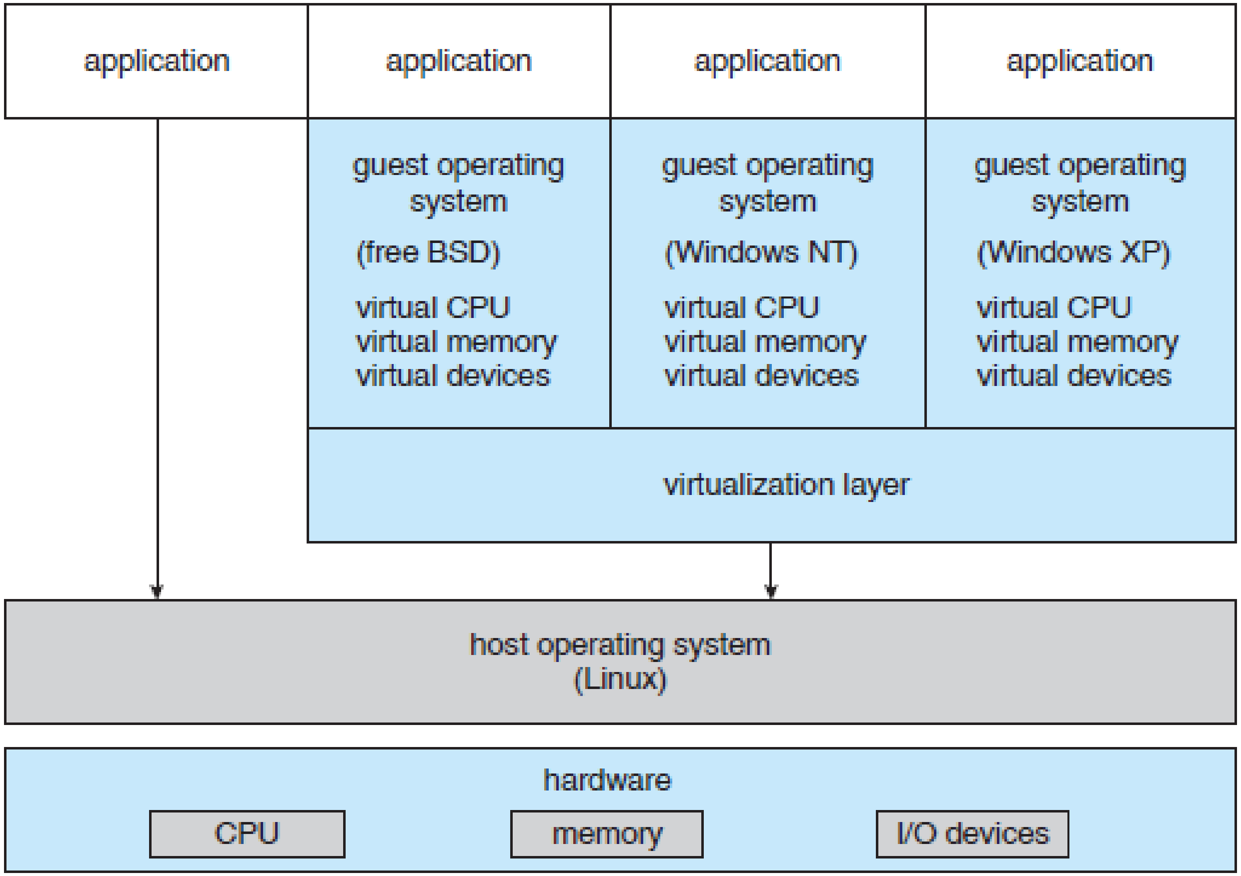
Virtual Machines

- The fundamental idea behind a virtual machine is to abstract the hardware of a single computer into several execution environments.
- The illusion is that each separate execution environment is running its own private computer.

Non-Virtual machine and virtual machine



VMware


application
application
application
application
guest operating system
(free BSD)
virtual CPU
virtual memory
virtual devices
guest operating system
(Windows NT)
virtual CPU
virtual memory
virtual devices
guest operating system
(Windows XP)
virtual CPU
virtual memory
virtual devices
virtualization layer
host operating system
(Linux)
hardware
CPU
memory
I/O devices

VM Escape

- VM Escape happens if the isolation between host and between VMs is compromised
- In VM Escape, the program running in a virtual machine is able to completely bypass the virtual layer (hypervisor layer) and get access to the host machine.
- Since the host machine is the root, the program which gains access to the host machine gains the root privileges and basically escapes from the virtual machine privileges
- This results in a complete break down in the security framework of the environment.

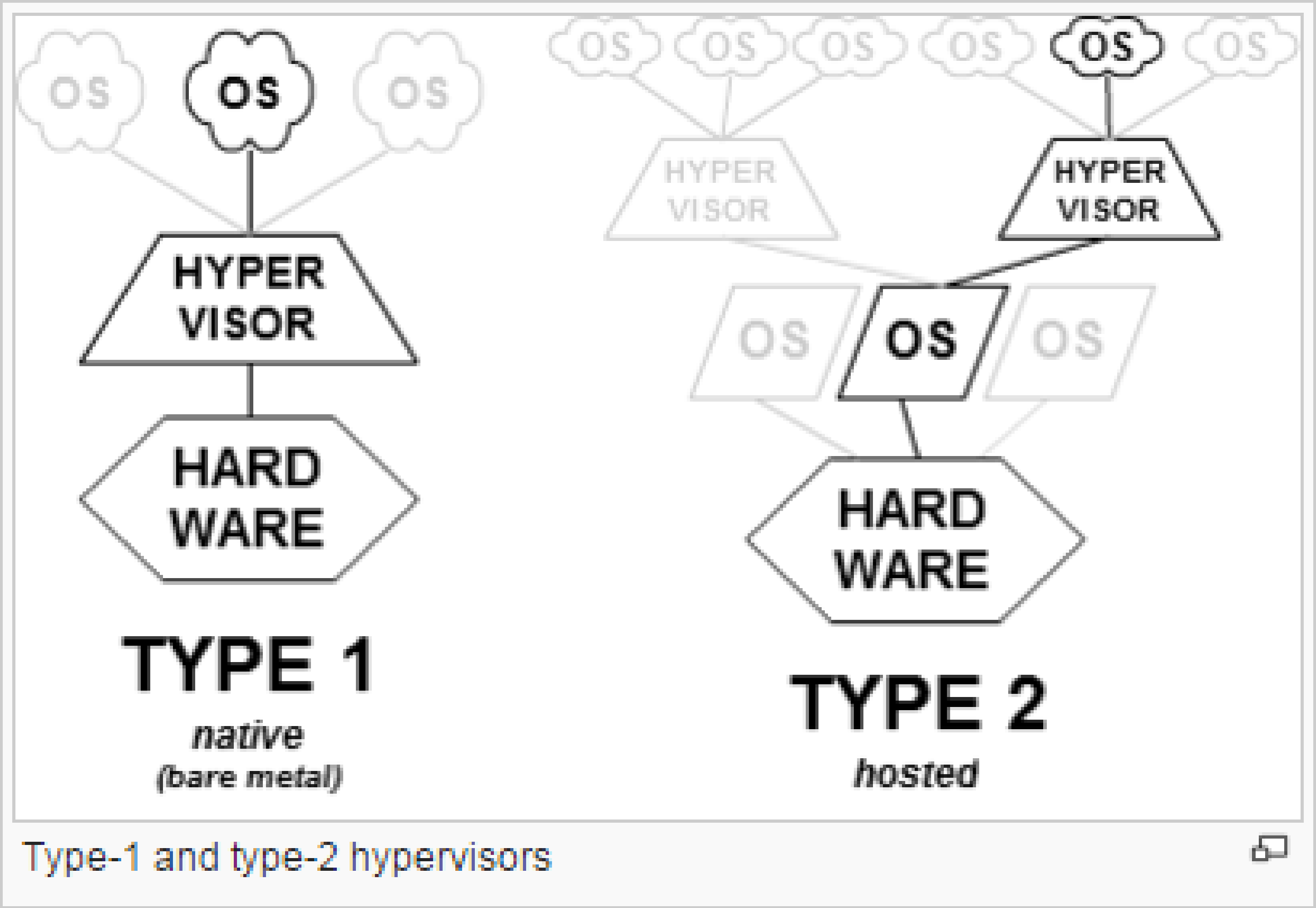
Hypervisor

- The evolution of virtualization greatly revolves around one piece of very important software. This is the *hypervisor*.
- As an integral component, this software piece allows for physical devices to share their resources amongst virtual machines running as guests on to top of that physical hardware.

Hypervisor types

- Type-1, native or bare-metal hypervisors: Run directly on the host’s hardware to control the hardware and manage guest operating systems.
- Type-2 or hosted hypervisors: Run on top of a conventional operating system just as the computer programs do.

Type-1 and Type-2 Hypervisors



Type-1 and type-2 hypervisors

Benefits

- We can run several different execution environments concurrently
- System consolidation
- The host is protected from the virtual machines
- Virtual machines are protected from each other

Protection Issues

- A virus inside a guest operating system might damage that operating system but is unlikely to affect the host or the other guests.
- Because each virtual machine is completely isolated from all other virtual machines, there are no protection problems

Security Issues

- Hypervisors are written to be robust and secure, but, like any other piece of software, they will inevitably contain vulnerabilities, which, if discovered by an attacker, could be exploited.
- Once someone gets to the hypervisor then it's game over, everyone can be compromised.

Keep up to Date with Hypervisor Patches

- Even though hypervisors are essentially a thin software shim between the virtual machines and the hardware, they are still essentially a cut down operating system. This means it still needs patching.
- Therefore, patching your hypervisor becomes just as important. All major vendors provide security updates for their hypervisors.

Be Careful when Allocating Rights and Permissions

- Administrators are the gatekeepers to the hypervisor, and their accounts are the keys.
- Often in less stringent environments an administrator can get into the bad practice of directly assigning rights to users rather than groups, thinking "it's just temporary." This should never happen.
- Using Active Directory groups helps in a number of ways.
  - First, assigning rights to groups ensures that all users in the group that perform the same function have the same rights.
  - Second, it makes life easier when an administrator leaves and someone else has to take over.

Turn Off Unnecessary Services

- Reducing the attack surface of the hypervisor is important.
- Services such as SSH and remote access capable features, not directly needed in every day use, should be turned off.
- VMware vSphere has a very useful feature called Lockdown mode. This prevents any non authorized access directly to the hosts and forces all the management to go through the vCenter management server.
- In a well managed environment there should be no direct host management, but everything should be done through the correct management interface.

Use Service Accounts Wherever Possible

- Any administrator should be using service accounts for their non-human users. Service accounts, as the name implies, should be used for management of services.
- This should be combined with using the principle of least privilege to ensure that the service account has the absolute minimal amount of rights required to perform a service. The really good thing about using this methodology is that it limits what can be done if the account is compromised.

Hyperjacking (1/2)

- The use of hypervisor technology by malware and rootkits installing themselves as a hypervisor below the operating system, known as hyperjacking can make them more difficult to detect
  - because the malware could intercept any operations of the operating system (such as someone entering a password) without the anti-malware software necessarily detecting it (since the malware runs below the entire operating system).

Hyperjacking (2/2)

- For a hyperjacking attack to succeed, an attacker would have to take control of the hypervisor by the following methods:
  - Injecting a rogue hypervisor beneath the original hypervisor
  - Directly obtaining control of the original hypervisor
  - Running a rogue hypervisor on top of an existing hypervisor

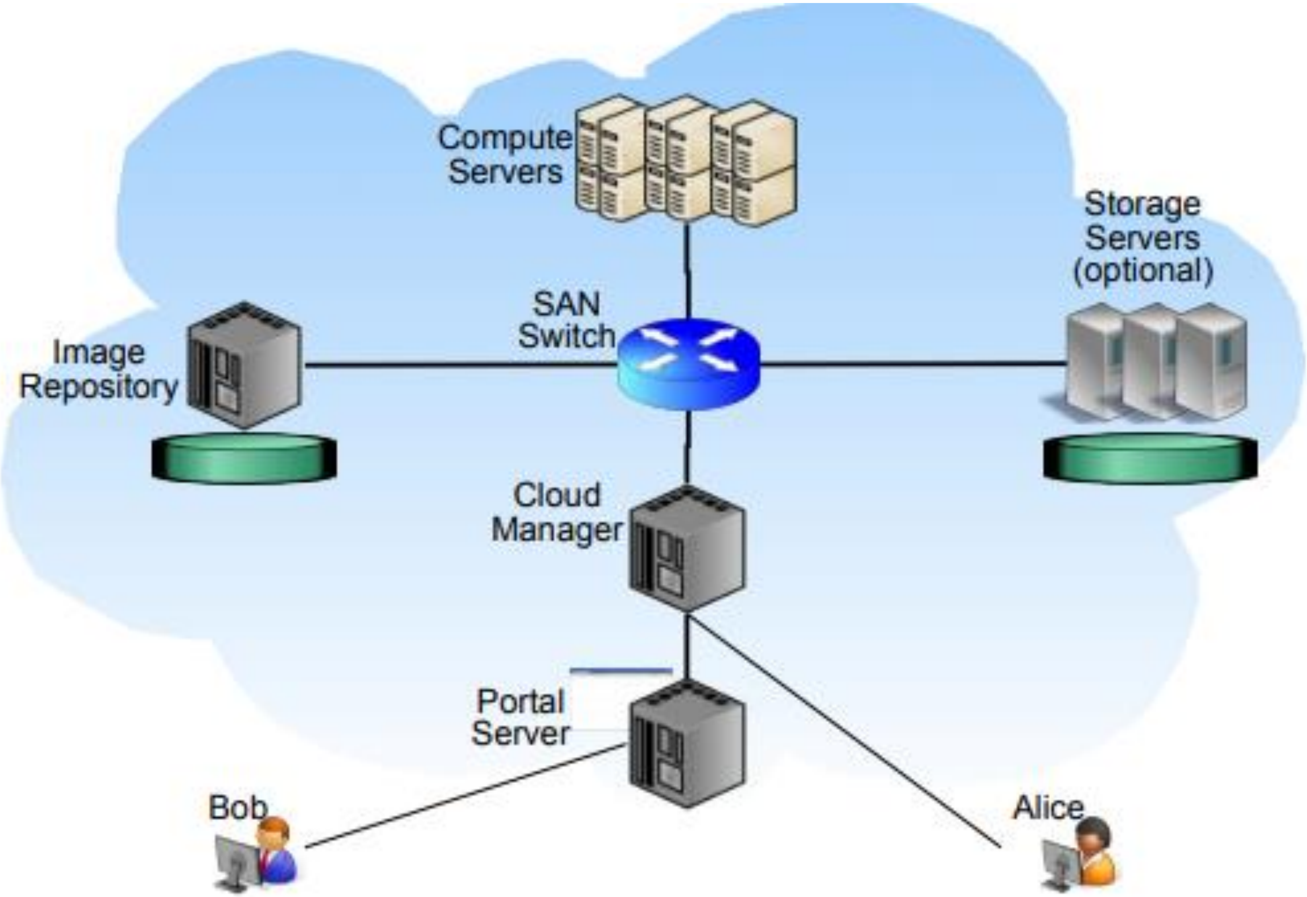
Measure for Hyperjacking

- Additional degree of network isolation
- Enhanced detection by security monitoring

VM Images

- VM images need high integrity, because they determine the initial states of running virtual machines, including their security states
- The security and integrity of such images are the foundation for the overall security of the cloud.
- Many of the VM images are designed to be shared by different and often unrelated users.

High Level Architecture of a Typical Cloud



Cloud Resources

- A cloud provide three types of resources:
  - A collection of virtual machine (VM) images
  - A set of computer servers on which VM images can be run
  - A storage pool to store persistent data

VM Images, Confidentiality, Safety

- The publisher, or owner, of an image is the one who contributes the original image to the repository.
  - He is mostly concerned about confidentiality (i.e., inadvertent leaking of sensitive information and unauthorized access to the image)
- The retriever or consumer of an image is the one who retrieves the image from the repository and runs it on the compute servers
  - He is mostly concerned about safety (e.g., a malicious image that is capable of corrupting or stealing the retriever's own private data.

VM Images & non-Compliance

- The administrator is concerned with the security and compliance of the cloud system as a whole and the integrity of individual images
- The administrator and consumer are concerned with potential damages caused by malware contained in any image stored in the repository

Publisher’s Risk

- The publisher risks releasing sensitive information inadvertently
- If the publisher sets up the application by running an instance of the image, he may unwittingly create files that should not be made public.
- Suppose that Alice, while configuring an application in a running instance, starts a web browser
  - Alice may publish the history of her browsing session along with her image
- The publisher may want to share the image with only a limited set of users. Therefore, the store should support some form of access control for images.

Retriever’s Risk

- While running a vulnerable virtual machine lowers the overall security level of a virtual network of machines in the cloud.
- Running a malicious virtual machine is similar to moving the attacker’s machine directly into the network, bypassing any firewall or intrusion detection system around the network.
- Using a virtual machine image as the carrier for the Trojan horse makes the hacker’s job easier.

Repository Administrator’s Risk

- Evidence shows that if dormant VM images are not managed (i.e., scanned for worms), a virtual environment may never converge to a steady state.
  - VM images can sporadically run, infect other machines, and disappear before they can be detected.
- Administrators carry a latent security risk that stems from long-lived but inactive images. This risk is often overlooked by administrators due to high maintenance costs.

Solutions to VM Images Security Risks

- An access control framework
- Image filters
- A provenance tracking mechanism
- A set of repository maintenance services

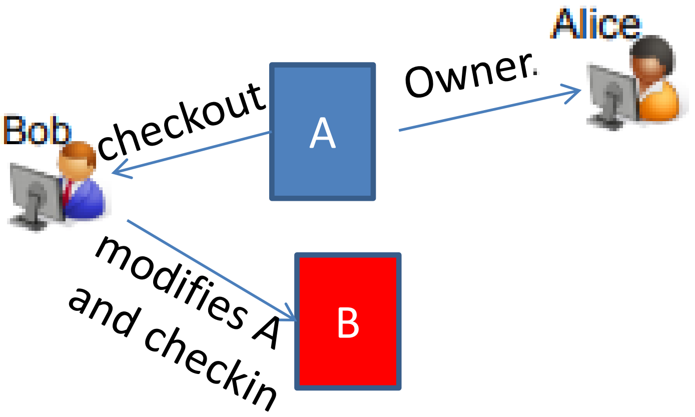
Access Control Framework

- Owner can share images with trusted parties by granting access permissions:
  - Checkin: revising an image and storing the revised image in the repository requires checkin permission
  - Retrieving and running an image requires checkout permission
- Even without checkin permission for an image, a user can retrieve the image, modify it and publish it as a new image.
  - However the provenance-tracking system would not consider the new image to be a revision of the original
- By default an image is private, meaning that no one but the owner and the administrator can access the image

Provenance Tracking

- The system tracks the derivation history of an image by recording the parent image information when a new image is deposited into the repository, along with the information about the operation that resulted in the creation of the new image.

Provenance Tracking Example



The system will record that image B derives from image A through method checkin

Provenance Tracking Discovers Vulnerability

- Considers that the system discovers a vulnerability in image C and applies the latest security patch for it that results in a new image D.
- The provenance information is used in two ways:
  - It can be consumed by an audit system to trace the introduction of illegal or malicious context
  - It can also be used to alert the owners of derived images when the parent image is patched so that the derived images can be patched as well.

Image Transformation by Running Filters

- Filters at publish time can remove or hide sensitive information from the publisher’s original image.
- For example a “remove” filter excludes a file from the original image, and a “hide” filter keeps the file but replaces its content with some safer version (e.g., replacing credit card numbers with invalid numbers)

Filters

- Two types of filters can be applied at publish time:
  - Repository-specific filters and user-specific filters
- Repository-specific filters are system-wide filters that reflect security best practices
- User-specific filters are intended to remove or hide user-specific sensitive content from the images.
  - Since different users may have different notions about what content is sensitive, these filters can only be supplied by the user

Image Maintenance

- Images should be regularly checked for compliance, scanned for malware, and patched with the latest security fixes.
- Maintenance operations are time consuming. The time it takes to start a running instance of an image, scan and patch the instance, and then capture it back to a new image, is on the orders of hours.
- Imagine a repository with thousands or millions of images. It could easily take months to perform just one round of maintenance.