Cloud Computing NETW1009

Lecture 10

Course Instructor: Dr. – Ing. Maggie Mashaly

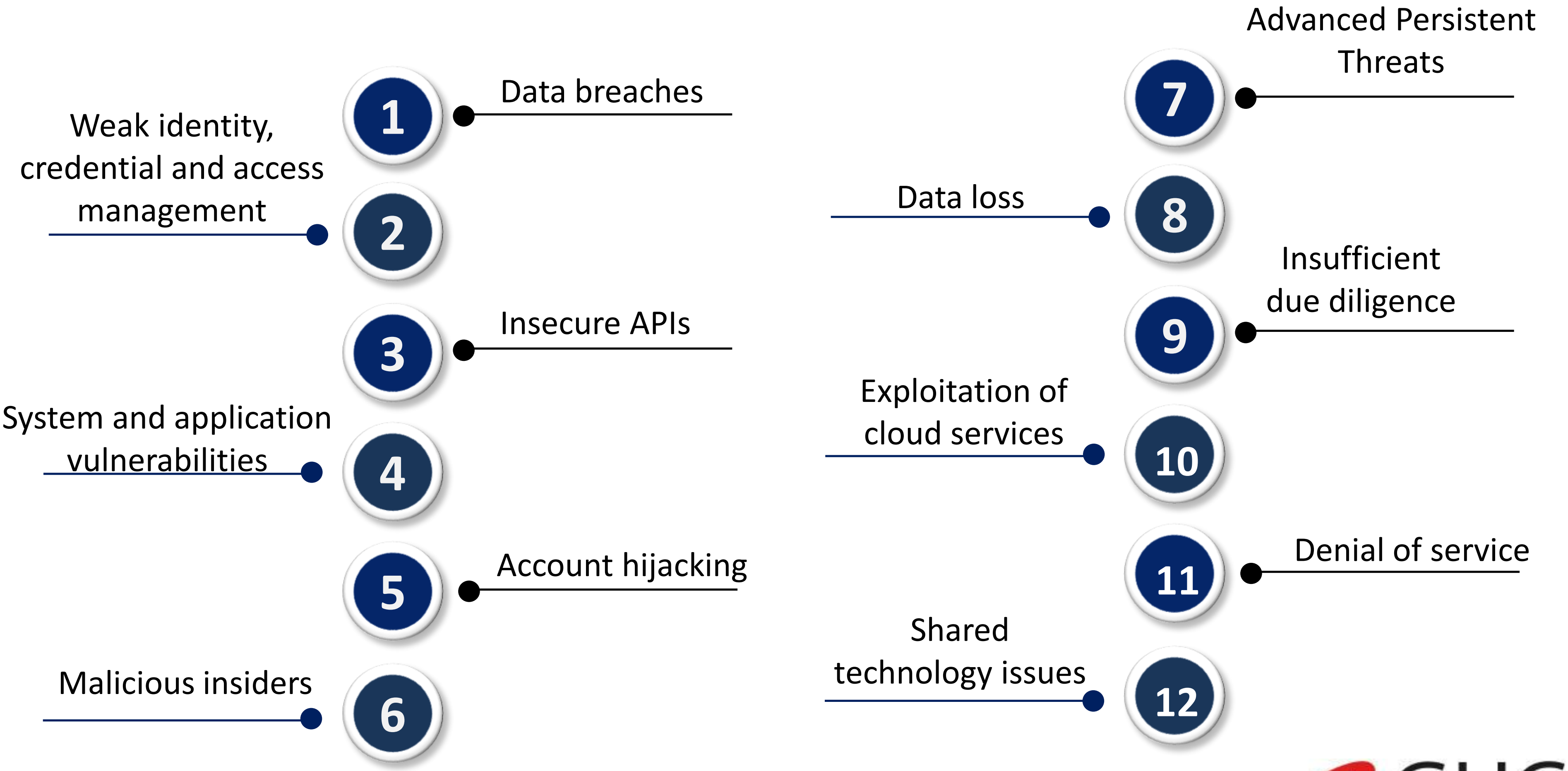
Lecture 10: Cloud Security II

Lecture Outline

- Cloud Security Threats
  1. Data Breaches
  2. Weak Identity, Credentials & Access Management
  3. Insecure APIs
  4. System & Application Vulnerabilities
  5. Account Hijacking
  6. Malicious Insiders
  7. Advanced Persistent Threats
  8. Data Loss
  9. Insufficient Due Diligence
  10. Exploitation of Cloud Services
  11. DoS & DDoS
  12. Shared Technology Issues

Cloud Security : Threats

Cloud Security Threats



1. Data breaches
2. Weak identity, credential and access management
3. Insecure APIs
4. System and application vulnerabilities
5. Account hijacking
6. Malicious insiders
7. Advanced Persistent Threats
8. Data loss
9. Insufficient due diligence
10. Exploitation of cloud services
11. Denial of service
12. Shared technology issues

1. Data Breaches

Data Breach

An incident in which an unauthorized entity gains access to a cloud consumer's confidential data.

An attacker may gain unauthorized access to consumers' confidential data in various ways.

To mitigate the risk of data leakage, providers may deploy a multifactor authentication and encryption techniques.

Confidential data may include health data, financial information, trade secrets, PII, and intellectual property.

Example

A leading financial organization had a data breach where the names, social security numbers, birth dates, and addresses of millions of customers was exposed. This attack was due to failure to do a timely patch update to fix a vulnerability in the dependent 3rd party software.

2. Weak Identity, Credentials, & Access Management

Identity management
Establish the attributes of an individual, application, or device

Credential management
Track and update the credentials

Access management
Control and manage access to the authorized users

Recommendation
Strong passwords, and multifactor authentication

Example

A multinational e-commerce organization reported a cyberattack in which the hackers got into the company network using the credentials of few corporate employees.

3. Insecure APIs

- APIs are used in Cloud to perform various activities
- Security of Cloud services depends upon the security of APIs
- The attacker may exploit the vulnerability in an API to carry out an attack
- Mechanism to control insecure API threat:
  - Authentication and authorization, encryption, and avoiding buffer overflows
  - Security review of APIs
  - Restrict access to the API only to authorized users

Example

An online gifts vendor experienced a security breach due to an insecure API. The hackers exploited the vulnerability in the API using the company's mobile application

4. System & Application Vulnerabilities

System and application vulnerabilities are the exploitable bugs in programs

Multitenancy and resource pooling creates an attack surface for the hackers

Vulnerabilities could be because of program errors or intended features

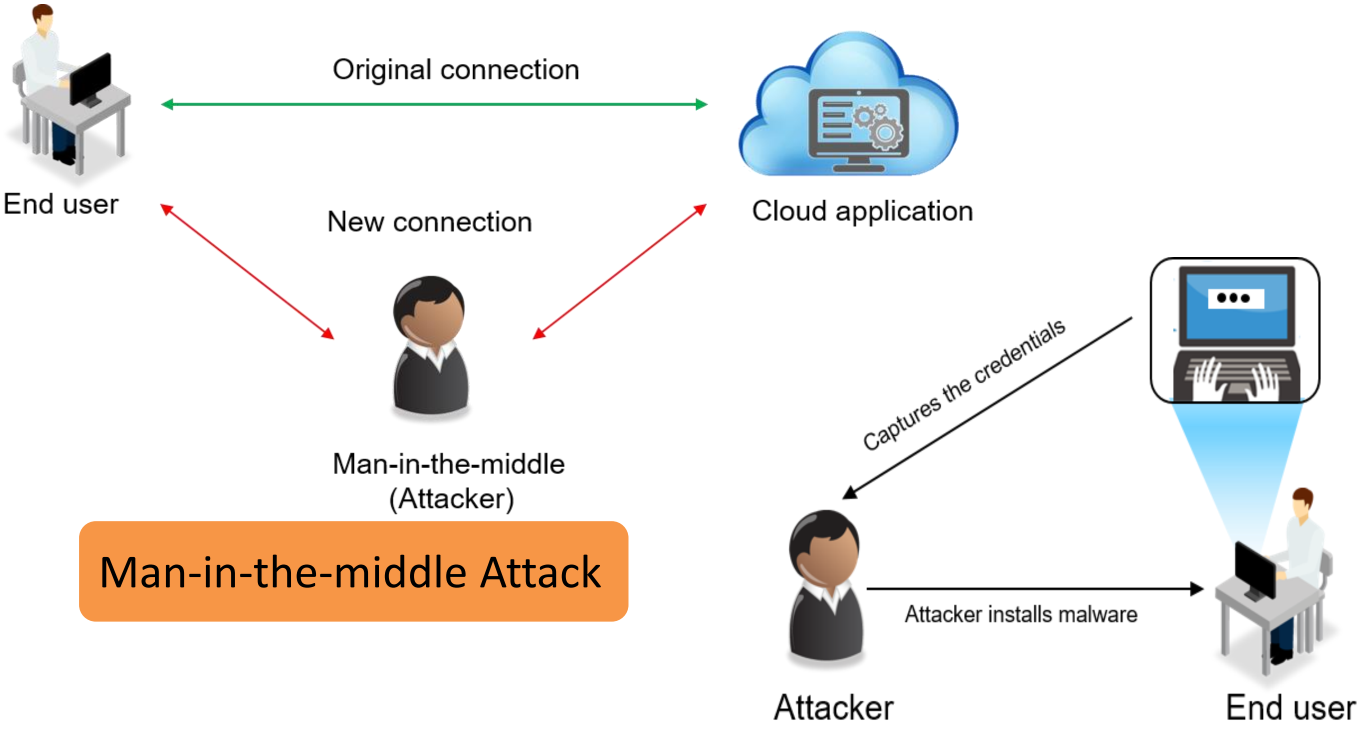
Can be controlled by installing security patches, regular vulnerability scanning, preventing access to complete files

Example

A film entertainment company reported a cyber attack, in which the hackers exploited the bugs in the software program using “Zero-Day” vulnerability.

5. Account Hijacking

Two methods of Account Hijacking are:



Man-in-the-middle Attack

Keystroke-logging malware Attack

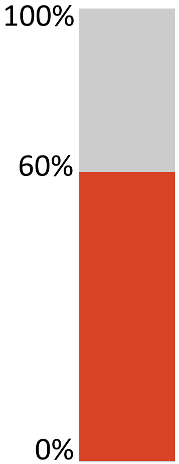
Example

Many social media accounts were hijacked, and hackers posted false messages.

6. Malicious Insiders

A malicious insider could be an organization’s current or former employee, contractor, or other business partner

Can be controlled by having a strict access control policies, disable employee accounts immediately after separation from the company, security audit, encryption, and segregation of duties policies



According to *IBM* report, in 2015, the insiders who had access to organization's systems carried out 60% of the attacks.

Example

A healthcare organization had a data breach where its own employees, medical professionals, inappropriately accessed and printed the patients information.

7. Advanced Persistent Threats

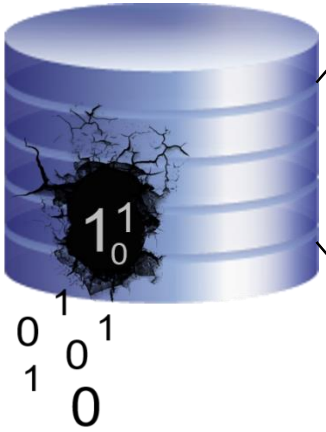
APT typically has 3 phases:

Phase 1	Phase 2	Phase 3
Gain access to the network through legitimate means	They move laterally across the data center network and install malware to achieve their objectives	They adapt to the security measures which were intended to defend against them and harvest valuable information for a long period

Example

An independent civil service agency working for a government discovered a data breach in which the PII including finger prints of millions of government employees was exposed due to an APT

8. Data Loss



Causes

Malicious attacks
Accidental deletion
Natural disasters

Prevention

Data backup
Data protection mechanisms
Service contract

Example

A code hosting and code publishing company was forced to shut down their operations after an attacker deleted their customer data and backup.

9. Insufficient Due Diligence

Cloud Provider

- Should pay due diligence towards who is in charge of what areas, while offering the cloud services.
- Example: A complete understanding of operational responsibilities is required in hybrid cloud.

Cloud Consumer

- Customers must also have a complete understanding of cloud service provider's environment
- Example: Customers must review the provider's data access and retention policies to determine whether they are consistent with the customer organizations policies.

Example

A cloud service provider shuttered its operations and a mail was sent to its customers to move their data in less than two weeks to another service. Customer's due diligence process should be more robust to understand who the provider is; are they funded and secure to sustain in the industry for a longer period, and their SLAs.

10. Exploitation of Cloud Services

Cloud computing services and the resources can be misused to perform unauthorized or malicious activities.

Misuse of cloud services

Cloud computing services and the resources can be misused to perform unauthorized or malicious activities.

Low cost

The cloud services are relatively cheaper, and also few cloud providers offer free trial period.

Mechanism

Service provider should also establish incident response team to address the misuse of resources.

Way of exploitation

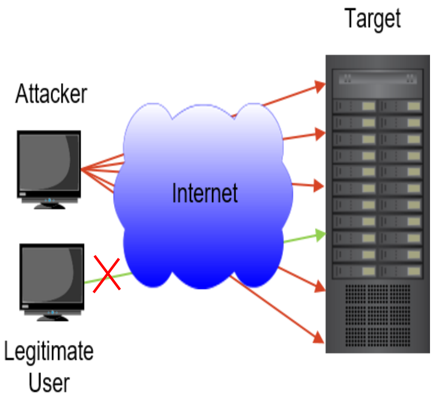
An attacker might use the cloud computing infrastructure to crack an encryption key.

Example

The attackers misused the cloud storage service, to infect the computer systems with a malware using a massive spear phishing campaign.

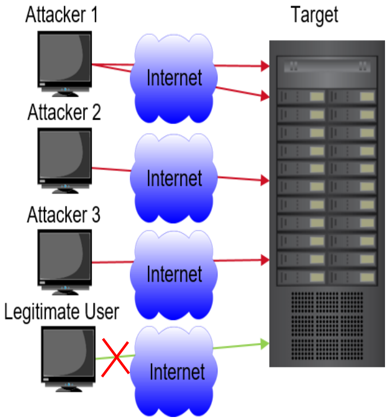
11. Denial of Service & Distributed Denial of Service

Denial of Service



A single attacker carrying out an attack on the target system prevents the legitimate users from accessing the resources. This mechanism causes Denial of Service attack.

Distributed Denial of Service



A Distributed DoS (DDoS) attack is a variant of the DoS attack in which several systems launch a coordinated, simultaneous DoS attack on their targets

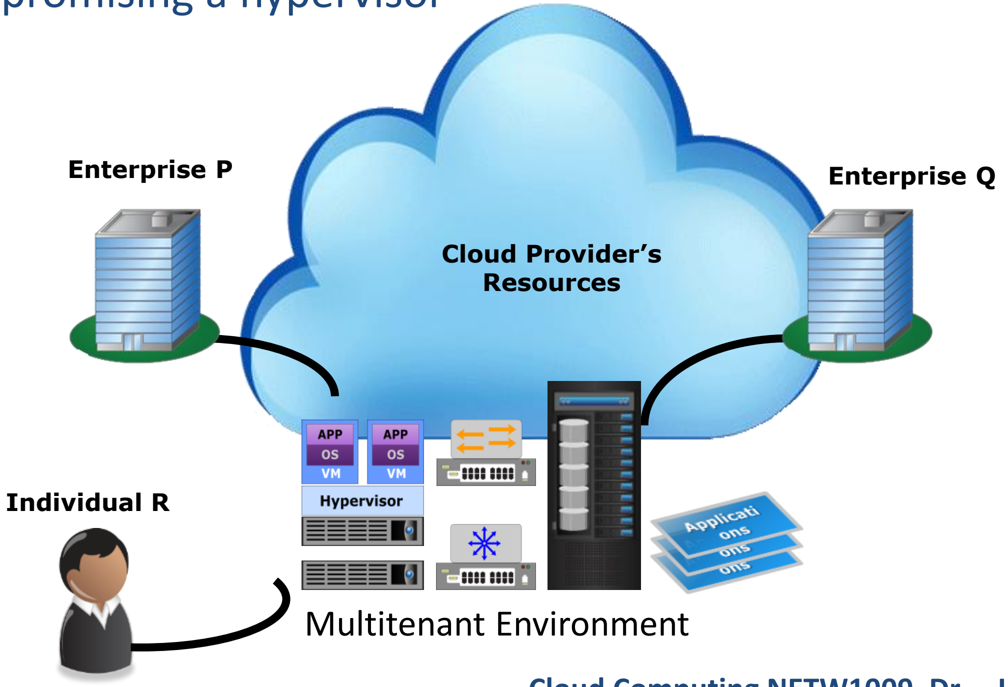
Example

A commercial news and information broadcast company suffered an outage on a New Year's Eve, as a result of the DDoS attack. Their news website and other sites were down for more than three hours.

12. Shared Technology Issues

Causes for shared technology issues:

- Failure of multitenancy mechanisms
- Exposing one consumer's data to other consumers
- Compromising a hypervisor

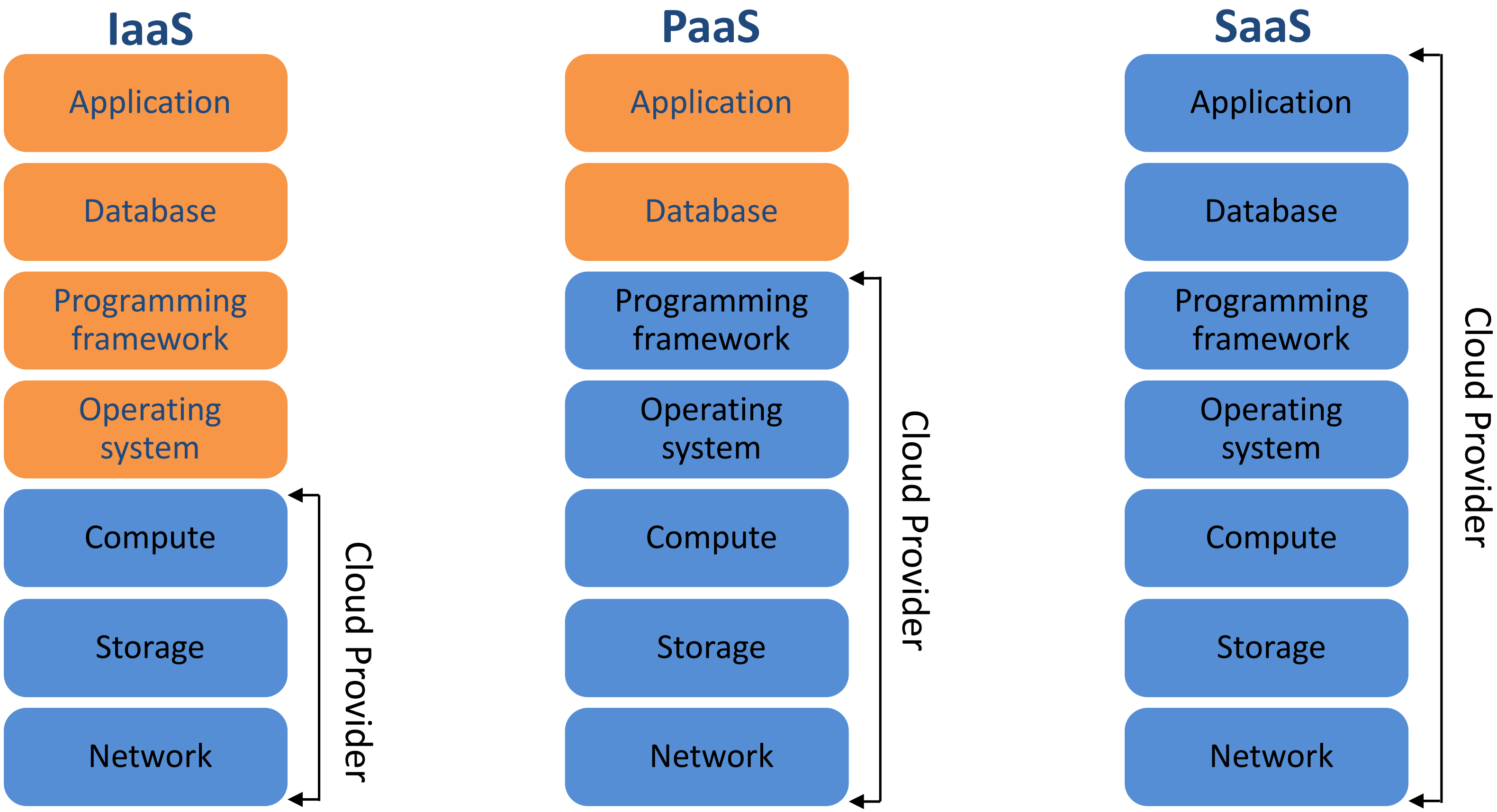


Multitenant Environment

Example

VENOM is a security vulnerability affecting the virtualization platforms. This vulnerability allows an attacker to access the host system along with other VMs running on the system, by escaping a guest virtual machine to steal the sensitive data on VMs.

Security Responsibility in Cloud Service Models



IaaS

Application

Database

Programming framework

Operating system

Compute

Storage

Network

Cloud Provider

PaaS

Application

Database

Programming framework

Operating system

Compute

Storage

Network

Cloud Provider

SaaS

Application

Database

Programming framework

Operating system

Compute

Storage

Network

Cloud Provider

References

- “Cloud Infrastructures and Services - CIS” Course by Dell Technologies
- “Information Storage and Management – ISM” Course by Dell Technologies
- “IT Solutions for Digital Businesses - Virtualization and the Journey to the Modern Digital Workspace” Course by Vmware

For any inquiries e-mail me on:
maggie.ezzat@guc.edu.eg