**SHOUZAB KHAN   
SKHAN6**

**CLOUD COMPUTING**

1. In modules 1 and 2, co-tenancy is considered to be a key reason why cloud security is different from traditional computer security. Explain in your own words why it is so.

ANSWER: Co-tenancy means when multiple users share the same cloud infrastructure. It means a malicious user can legally be in the same infrastructure as good users.

In traditional computer security, the organization has full ownership of the servers and machines, while in cloud security, multiple users have access to the server. So, it has more risk of the malicious user entering the server.

In cloud security, if a user finds a way to breach data, he can access and use any other tenant data.

The traditional computer security mainly focuses on the individual system, while as cloud security focuses on the shared servers by many tenants.

**-------------------------------------------------------------------------------------------------------------------------**

2. Consider the following scenario: Your company uses the Nozama cloud service to store sensitive documents. Your task is to analyze the threat model, and as a part of that, you are considering the attacker model. Would you consider the cloud service provider (Nozama) a malicious attacker? Provide at least two arguments each for and against considering Nozama as a potential attacker.

 ANSWER: If a company uses the Nozama Cloud service to store sensitive documents and considers it a malicious attacker or a service provider, we can have arguments for that below.

We can start by giving arguments against Nozama as a potential attacker:

1: Suppose Nozama acts like a malicious attacker and breaches the system data and documents so they can have a lawsuit and legal action against it because they are registered with the government.

2: They can also lose their reputation in the market and, won't get any more clients, and can lose existing customers.

Now Argument for Nozama as a potential attacker:

1: Nozama cloud service can access all your sensitive data and documents stored on the server. Nozama can modify, delete, or temper any data they want. So, if there is any malicious user, they can do anything and can be an attacker.

**-------------------------------------------------------------------------------------------------------------------------**

3. Your company is trying to choose between using a local in-house data server vs. using the Elgoog cloud service to store important data. What are the advantages of using such a cloud-based storage service over the local server? What are the disadvantages?

ANSWER: If a company is trying to choose between an in-house data server and a cloud service to store important data. So,

**the advantage of using cloud-based storage over a local data server** is that it will have an option for scalability, which means you can upsize the data storage and downsize the data storage as per your use at any time.

Cloud servers are also cost-efficient; you don’t have to pay any upfront; you only have to pay for the resources you use.

Cloud-based servers can be accessible anywhere worldwide, just by your mobile or computer. You don’t have to be available in-house to access and use your data.

The cloud-based server has more security and reliability than the in-house data server.

**The Disadvantage of a cloud-based storage server over the local in-house data server** is that a Cloud-based server is shared by many users, which can have issues with security reasons. It means there is a chance of any malicious user on the server.

The other problem with a cloud-based server is that it is always dependent on internet connectivity, which means if your internet connection is lost, your whole server can be down, and nothing can be accessed.

Using the cloud-based server gives you access to everything, but the problem is that you don’t have ownership and control of everything. You must tell the server owner to make changes or customize anything. It means you are dependent on them.

**-------------------------------------------------------------------------------------------------------------------------**

4-MS: Write a threat model for a cloud-based streaming service (here the video files are hosted in the cloud, and the users watch the videos through a web interface). (The threat model should include the following: a) List of Assets b) List of Entry points c) Attacker model, with attacker capabilities and motivation, and d) Vulnerabilities and e) mitigation strategies.

ANSWER:

The thread model for cloud-based video streaming service:

**a: Assets:**

Video Content: video content can be an asset of the cloud-based server, which the attacker can attack.

User Credentials: Users' passwords, email addresses, and names can be stolen.

User Information: The personal details of the user can be breached.

Card Details: Users' card details can be compromised.

**b: List of Entry Points:**

Mobile application: 3rd party applications that have access to the server.

WIFI network: the network connection which has access to the server.

**c: Attacker Model:**

Competitors: The competitors who don’t want the server to grow up

Copywrites: anyone can copywrite the server.

Hackers: the black hat hackers can hack the server, compromise all the data, and sell it.

**d: Vulnerabilities:**

Phishing attack: there can be different tricks to develop user credentials, like sending them SMS and emails.

Denial of services: Denial of service can interrupt the server's service.

Spoofing attack: The attacker may get unauthorized access to the data and services.

**e: Mitigation Strategies:**

Encryption: you can be safe through having strong encryption techniques.

Two-factor authentication: you can turn on 2-factor authentication to be on the safe side.

Education: you can educate the user about fake login pages and emails like phishing attacks.

Security: You can increase the server's security by having 3rd party services.

**-------------------------------------------------------------------------------------------------------------------------**