
Cloud Security
By: Isaac Chang

What is the cloud?

A computer base(aka internet bases) you can connect to via the internet

Why is it important?

Past(Legacy systems)

Pros:

- Allowed companies to store data early on

Cons:

- Old software and hardware that has been outdated
- Legacy systems are usually stored in large data centers that take space and manpower

Future(Cloud):

Pros:

- You don’t need to manage your own physical data center
- Scaling is much easier as a business

Cons:

- For existing companies, it is hard to migrate from legacy systems to the cloud
- Security issues are still at large

How can the cloud be compromised?

Lack of visibility:

- The more services someone has, the harder it is to keep track of everything
- If one service has a vulnerability, it can compromise the whole cloud server

General Overview

Company A figures out their local hardware can't keep up with their business needs

They decide to move their operations to the cloud!

The cloud:
Specialized servers that are accessible through the internet

Offers data storage + computing power

Take advantage of security vulnerabilities and accesses Company A's data and free computing resources

1. Sells company A's data illegally or holds it ransom
2. Uses the computing power to mine cryptocurrency, wasting Company A's money

How do cyber criminals gain access?

1. When clients use their cloud servers, they form a communication thread
2. The client has a type of ID that allows it to connect and run on a cloud server
3. Hackers can intercept that communication thread and get that ID
4. Using that ID, hackers can do whatever the client can do in that cloud server

This is known as session hijacking w/ session sniffing

There are many other ways…

Man In the Browser: Hackers infect victim's computer with malware. When victim visits a website, hackers can send undetected, unwanted orders/commands in the name of the victim. Severe cases include bank transactions

Session Side Jacking: Hackers use packet sniffing to intercept session data. They can use this data to login to the targeted cloud server

Cloud security

Obfuscation: Manipulating data by encryption, deletion, and other techniques. Without knowing the “key”, hackers can’t do much with the encrypted data

Virtual Private Network: Using a VPN, the “communication thread” between client and cloud server is secured. Packet sniffing is basically impossible with VPN

Tokenization: Sensitive data is represented by non sensitive data(tokens). Even if the tokens are stolen by hackers, they can’t be exchanged for the real data without the right tokenization system

Emerging technologies

1. Zero trust model
   - Basically means “zero trust”
   - Each user is isolated to whatever they can do. This prevents lateral movement attacks where hackers use the privileges of one user to access another user’s privileges and so on
2. Extended Detection and Response (XDR):
   - Monitors movement on the cloud, and applies artificial intelligence to find suspicious activities in the cloud

Thanks for listening!

Next lesson: 2/27/2023

Have a great winter break!

Next topic: CTF challenges