Cloud Computing

Chapter 9

Securing the Cloud
Learning Objectives

- List the security advantages of using a cloud-based provider.
- List the security disadvantages of using a cloud-based provider.
- Describe common security threats to cloud-based environments.
Physical Security

• IT data centers have been secured physically to prevent users who do not have a need to physically touch computers, servers, and storage devices from doing so.

• A general security rule is that if an individual can physically touch a device, the individual can more easily break into the device.
Advantages of Cloud Providers with Respect to Security

- Immediate deployment of software patches
- Hardware and software redundancy
- Timeliness of incident response
- Specialists instead of personnel
Disadvantages of Cloud-Based Security

- Country or jurisdiction issues
- Multitenant risks
- Malicious insiders
- Vendor lock in
- Risk of the cloud-based provider failing
Real World: McAfee Security as a Service

• McAfee now offers a range of security solutions that deploy from the cloud.
• The solutions protect e-mail (spam, phishing, redirection, and virus elimination), websites, desktop computers, mobile devices, and more.
Data Storage Wiping

- Within a cloud-based disk storage facility, file **wiping** overwrites a file’s previous contents when the file is deleted.
Wiping

- The proven solution to securely obliterate partition data.
- Getting rid of an old PC, upgrading to a new hard drive, returning a leased computer, or redeploying a PC within your company?
- It is truly imperative to completely destroy all data from the old partitions.
• A denial-of-service attack is a hacker attack on a site, the goal of which is to consume system resources
  – the resources cannot be used by the site’s users.
Simple Denial of Service

:Loop
ping SomeSite.com
GOTO Loop

• While responding to the ping message, the server can handle fewer other requests
Distributed Denial of Service (DDOS) Attack

- A distributed denial-of-service (DDoS) attack uses multiple computers distributed across the Internet to attack a target site.
Packet Sniffing Attacks

- Network applications communicate by exchanging network packets.
- Each computer within a wired network examines the message address to determine if the message is for an application it is running.
A hacker can write code that lets his system examine the content of each packet that travels past it.

In a wireless network, hackers can simply monitor the airways to intercept packets.
Packet Sniffing in Cloud

- It allows users to connect to applications from anywhere, increases potential risks.

- Users may connect from an insecure network or a network in which the wireless traffic is being monitored.

- The best defense against a packet sniffing attack is to use secure (encrypted) connections.
Man-in-the Middle Attack

• A **man-in-the-middle attack**, a hacker intercepts the messages a user and system are exchanging.
• The hacker can view and/or change the message contents.
Monitoring Device Screens

- Some employees accessed sensitive or confidential data only from within their office, and the data was better physically protected from prying eyes.
- Such data to users who are any place, at any time, and often to any device in cloud case.
- The net result is that within a busy coffee shop or an airport, strangers can see data ranging from human-relations information or customer sales data to student grades, and more.
Malicious Employees

• Companies spend considerable amounts of money trying to protect their data and communications from hackers.
  – IT staffs deploy firewalls, use encryption, monitor network traffic for intrusion, and much more.

• The most difficult challenge for a company to defend itself against is a malicious employee.
Malicious Employees Continued

- IT staff members have access to various system passwords, which means that each may have access to human-relations data, payroll data, e-mail content, and so on.

- By shifting data to the cloud, you move sensitive data away from your own employees.
Hypervisor Attack

- Hypervisor developers such as VMware and Microsoft constantly focus on ways to lock down and secure the hypervisor to reduce risks.

- The hypervisor will remain an attractive hacker target as companies continue to virtualize solutions.
Hackers refer to the process of taking over the hypervisor as a **hyperjacking attack**.

To reduce the chance of a hypervisor being taken over by malicious code the underlying hardware
- To assign a state value, like a cyclic redundancy check (CRC), to the hypervisor.
- If this value changes, the hardware can detect that the hypervisor has been attacked or replaced.
Guest hopping attack: hackers refer to an attack from one guest operating system to another.
The Cloud Security Alliance consists of a large coalition of cloud practitioners, companies, associations, and other cloud stakeholders.

The Cloud Security Alliance is a not-for-profit organization, the goal of which is to promote education of cloud security issues.
Many web applications present forms that users must complete by filling in fields and then submitting the form contents for processing.

The application that receives the form data often stores the data within an SQL database.
SQL Injection Attack Continued

- An **SQL-injection attack** occurs when a malicious user inserts one or more SQL queries within one or more of the fields.
  - For example, the hacker might type the following:
    
    **Smith; DROP DATABASE EMPLOYEES;**

- The command would delete the database of the company’s employees.
• Many cloud-based software as a service (SaaS) solutions are multitenant applications, which means different customers may share underlying resources such as a database.

• If the SaaS application falls victim to SQL injection, it might be possible for a user in one company to view, change, or destroy the data of another company.
The European Network and Information Security Agency (ENISA), based in Greece, promotes cyber security best practices.

Within the ENISA website, you will find a broad range of papers and reports on a variety of security topics.
Improving Physical Security through Colocation

• By using colocated, replicated hardware and software, cloud solution providers reduce many threats to IT resources.
Key Terms

Data wiping
Denial-of-service attack
Guest-hopping attack
Hyperjacking attack

Man-in-the-middle attack
Packet sniffing
SQL-injection attack
Chapter Review

1. List the security advantages of cloud-based solutions.
2. List the security disadvantages of cloud-based solutions.
3. Define and discuss the data wiping process.
4. Discuss how a cloud-based solution provider may reduce the risk of a DDoS attack.
5. Define and discuss hyperjacking attacks.
6. Define and discuss guest-hopping attacks.