Lecture 4

Long Question

1.Three Security Dimensions

(1) Confidentiality Information

- **System** may be disclosed or made accessible to people or programs that are not authorized to have access to that information. For example, the theft of credit card data from an e-commerce system is **a confidentiality problem.**

(2) Integrity Information

- **System** may be **damaged or corrupted**, making it unusual or **unreliable**. For example, **a worm** that deletes data in a system is **an integrity problem.**

(3) Availability

- Access to a system or its data that is normally available may not be possible.
- **A denial-of-service attack** that **overloads a server** is an example of a situation where the system availability is compromised.
- **These dimensions are closely related**.
- If an attack makes the system unavailable, then you will not be able to update information that changes with time. This means that the integrity of the system may be exposed.
- If an attack succeeds and the integrity of the system is exposed, then it may have to be taken down to repair the problem. Therefore, the availability of the system is **reduced**.

2.A Specialized Terminology Associated With Security

Term	Definition
Asset	Something of **value that has to be protected.** The asset may be the software system itself or the data used by that system.
Attack	An exploitation of a system's vulnerability where an attacker has

	the goal of **causing some damage to a system asset or assets**. Attacks may be from outside the system (external attacks) or from authorized insiders (insider attacks).
Control	**A protective measure** that reduces a system's vulnerability. Encryption is an example of a control that reduces a vulnerability of a weak access control system.
Exposure	**Possible loss or harm** to a computing system. This can be loss or damage to data or can be a loss of time and effort if recovery is necessary after a security breach.
Threat	**Circumstances** that have potential to **cause loss or harm**. You can think of a threat as a system vulnerability that is subjected to an attack.
Vulnerability	A **weakness in a computer-based system** that may be exploited to **cause loss or harm**.

3. 10 Types of Security Requirements

1.Identification requirements specify whether or not a system should identify its users before interacting with them. (**Log In**)

2.Authentication requirements specify how users are identified.

3.Authorization requirements specify the privileges and access permissions of identified users.

4.Immunity requirements specify how a system should protect itself against viruses, worms, and similar threats.

5.Integrity requirements specify how data corruption can be avoided.

6.Intrusion detection requirements specify what mechanisms should be used to detect attacks on the system.

7.Nonrepudiation requirements specify that a party in a transaction cannot deny its involvement in that transaction.

8.Privacy requirements specify how data privacy is to be maintained.

9.Security auditing requirements specify how system use can be audited and checked.

10.System maintenance security requirements specify how an application can prevent authorized changes from accidentally defeating its security mechanisms.

Short Note

1. Organizational Perspective of Security Levels
   From **an organizational perspective**, **security** has to be **considered at three levels**:
   1. **Infrastructure security**,
      - concerned with **maintaining the security of all systems and networks** that provide an infrastructure and a set of shared services to the organization.
   2. **Application security**,
      - concerned with the **security of individual application systems** or

   related groups of systems.
   3. **Operational security,**
      - concerned with the **secure operation** and **use of the organization's systems**.
      - Figure 1.1 shows an application system stack where security may be compromised
      - The **majority of security attacks are on the software infrastructure of systems**.

- Attackers focus on software infrastructures because infrastructure components, such as **web browsers, are universally available.**

2.Operational Security

.Operational security is primarily **a human and social issue**.

.It focuses on ensuring that the people using the system do not behave in such a way that system security is compromised.

- For example,

Users may leave themselves logged on to a system while it is unattended.

- **A challenge for operational security** is
  - **to raise awareness of security issues** and

to **find the right balance between security and system effectiveness**

3. Infrastructure Security

- Infrastructure security is primarily a **system management problem**, where **system managers** **<u>configure the infrastructure to resist attacks</u>**.
- **System security management** includes **a range of activities:**

1) **User and permission management**
   - adding and removing users from the system,
2) **System software deployment and maintenance**
   - installing system software and middleware and configuring these properly so that security vulnerabilities are avoided.

3)**Attack monitoring, detection, and recovery**

- monitoring the system for unauthorized access, detecting and putting in place strategies for resisting attacks, and organizing backups of programs and data
  .