Lecture Notes

1. Computer Security Concepts

Definition

- Computer security involves protecting **computer systems, networks, and data** from unauthorized access, damage, or disruption.
- Goal: Ensure that resources are **safe, reliable, and accessible to authorized users**.

Key Objectives

1. Protect data and systems from **unauthorized access**.
2. Prevent accidental or intentional **data modification or deletion**.
3. Ensure **system availability** for legitimate users.
4. Maintain **trust and privacy** in digital interactions.

Core Security Principles

- Authentication: Verify user identity.
- Authorization: Control user access to resources.
- Accountability: Track user actions via logs.
- Non-repudiation: Ensure actions cannot be denied later.

---

2. Confidentiality, Integrity, Availability (CIA Triad)

The **CIA triad** is the foundation of computer security:

1. Confidentiality

- Ensures that sensitive information is **only accessible to authorized users**.
- Techniques:
    - Encryption (symmetric/asymmetric)
    - Access control lists (ACLs)
    - Passwords and authentication mechanisms

2. Integrity

- Ensures that data is **accurate, consistent, and not tampered with**.
- Techniques:
    - Hash functions (SHA, MD5)
    - Digital signatures
    - Checksums

3. Availability

- Ensures that systems and data are **accessible when needed by authorized users**.
- Techniques:
    - Redundant systems
    - Regular backups
    - DDoS protection and load balancing

---

3. OSI Security Architecture

Definition

- Security in networked systems can be mapped to the **OSI model layers**, defining where security controls can be applied.

Security Layers & Goals

1. **Physical Layer**: Protect hardware and physical access.
2. **Data Link Layer**: Detect and prevent unauthorized access on the network.
3. **Network Layer**: Secure routing, firewalling, and IP security (IPSec).
4. **Transport Layer**: Protect end-to-end communication (TLS/SSL).
5. **Session Layer**: Secure session management and authentication.
6. **Presentation Layer**: Data encryption and encoding.
7. **Application Layer**: Protect applications, user interfaces, and sensitive data.

ISO/OSI Security Architecture Concepts

- **Security Services:** Confidentiality, integrity, authentication, access control, non-repudiation.
- **Security Mechanisms:** Cryptography, digital signatures, secure protocols, auditing.

---

4. Security Attacks

Definition

- Security attacks are deliberate actions to **compromise the confidentiality, integrity, or availability** of systems.

Types of Attacks

1. **Passive Attacks**
    - Monitoring or eavesdropping on communications without altering data.

    - Examples: Traffic analysis, packet sniffing.

2. **Active Attacks**
    - Modifying or injecting data into the system.
    - Examples: Man-in-the-middle attacks, session hijacking, malware.
3. **Physical Attacks**
    - Direct access to hardware or facilities to steal or damage systems.
4. **Social Engineering**
    - Manipulating people to reveal confidential information.
    - Examples: Phishing, pretexting, baiting.
5. **Network Attacks**
    - Exploit vulnerabilities in protocols or network configurations.
    - Examples: Denial-of-Service (DoS), Distributed DoS (DDoS), IP spoofing.
6. **Software Attacks**
    - Target application or system software.
    - Examples: Viruses, worms, ransomware, buffer overflows.

Defensive Strategies

- Firewalls, intrusion detection systems (IDS), antivirus software.
- Encryption, access controls, secure coding practices.
- Regular software updates and patches.
- User awareness and training.

Key Takeaways

- Computer security protects systems from **unauthorized access and threats**.
- The **CIA triad** ensures data confidentiality, integrity, and availability.
- Security measures can be applied across **OSI layers**.
- Understanding attack types helps design effective **defensive strategies**.