✅ UNIT 1 – INTRODUCTION TO COMPUTER SECURITY

1️⃣ Computer Security Concepts

Introduction

Computer Security refers to the protection of computer systems, networks, and data from unauthorized access, misuse, damage, or disruption. In modern society, where digital systems control banking, healthcare, education, defense, and communication, security has become essential.

Computer security ensures that information remains safe from cyber criminals, hackers, insiders, and accidental threats.

Objectives of Computer Security

The main objectives are based on the **CIA Triad**:

1. Confidentiality

Confidentiality ensures that information is accessible only to authorized users.

If confidentiality is broken, sensitive data may be exposed.

Methods used:

- Encryption
- Passwords
- Access control systems
- Biometric authentication

Example:
Only bank customers should access their account details.

2. Integrity

Integrity ensures that information remains accurate and unaltered.

If integrity is violated, data may be modified illegally.

Methods used:

- Hash functions

- Digital signatures
- Checksums

Example:
Marks in university database must not be modified without permission.

3. Availability

Availability ensures that systems and data are accessible when needed.

If availability is compromised, services may stop functioning.

Methods used:

- Backup systems
- Redundant servers
- Protection against Denial of Service (DoS) attacks

Example:
ATM machines must be available 24/7.

Importance of Computer Security

- Protects personal information
- Prevents financial loss
- Maintains business reputation
- Ensures national security

Conclusion

Computer security is essential for maintaining trust in digital systems. Without proper security measures, systems become vulnerable to attacks and data breaches.

2️⃣ OSI Security Architecture

Introduction

The OSI Security Architecture was developed by ISO to provide a structured framework for security in network systems.

It defines:

- Security Attacks
- Security Services
- Security Mechanisms

This architecture helps in designing secure communication systems.

Components of OSI Security Architecture

1. Security Attacks

A security attack is any action that compromises system security.

There are two types:

(a) Passive Attacks

- Do not modify data.
- Difficult to detect.

Examples:

Eavesdropping

Traffic analysis

Goal: Steal information secretly.

(b) Active Attacks

Modify data or disrupt services.

Easier to detect.

Examples:

- Masquerade attack

- Replay attack
- Message modification
- Denial of Service (DoS)

Goal: Disrupt system operation.

2. Security Services

Security services are designed to counter security attacks.

Major services:

Authentication

Access Control

Data Confidentiality

Data Integrity

Non-repudiation

3. Security Mechanisms

Security mechanisms are techniques used to implement services.

Examples:

Encryption

Digital signatures

Authentication protocols

Firewalls

Access control lists

Conclusion

The OSI Security Architecture provides a systematic way to understand and implement network security by classifying attacks, services, and mechanisms.

3️⃣ Security Attacks

Introduction

A security attack is any attempt to violate system security and compromise data.Attacks aim to break confidentiality, integrity, or availability.

Types of Security Attacks

1. Passive Attacks

Passive attacks monitor communication without altering data.

Characteristics:

- No data modification
- Difficult to detect
- Prevented using encryption

Examples: Release of message contents

- Traffic analysis

2. Active Attacks

Active attacks involve modification or disruption of communication.

Characteristics:

- Data modification occurs
- Can be detected
- Hard to prevent completely

Types:

- Masquerade – Pretending to be authorized user.
- Replay – Re-transmitting captured messages.
- Modification – Changing message content.
- Denial of Service – Blocking system access.

Conclusion

Understanding security attacks is important to design effective defense mechanisms.

4️⃣ Security Services

Introduction

Security services are the functions provided by a system to protect data and communication from security attacks. These services are defined in the OSI Security Architecture and are designed to counter threats such as unauthorized access, modification, and impersonation.

Security services ensure that communication over networks remains safe and trustworthy.

Major Security Services

1. Authentication

Authentication ensures that the identity of a user, device, or system is verified before granting access.

Types:

- Peer Entity Authentication – Verifies identity of communicating parties.
- Data Origin Authentication – Confirms the source of the message.

Example:
Login using username and password.

2. Access Control

Access control prevents unauthorized users from accessing resources.

It defines:

- Who can access
- What they can access
- What actions they can perform

Example:
Only teachers can edit student marks.

3. Data Confidentiality

Ensures that data is protected from unauthorized disclosure.

Implemented using:

Encryption

Secure communication protocols

Example:
HTTPS encryption for websites.

4. Data Integrity

Ensures that data is not modified during transmission.

Implemented using:

Hash functions

Message Authentication Codes (MAC)

Example:
Detecting tampered email messages.

5. Non-Repudiation

Ensures that the sender cannot deny sending a message.

Implemented using:

Digital signatures

Example:
Online transaction receipts.

Conclusion

Security services provide protection against attacks by ensuring confidentiality, integrity, authentication, and access control in communication systems.

5️⃣ Security Mechanisms

Introduction

Security mechanisms are the technical tools and techniques used to implement security services.

While services define *what protection is needed*, mechanisms define *how protection is achieved*.

Types of Security Mechanisms

1. Encipherment (Encryption)

Converts plaintext into ciphertext to ensure confidentiality.

Example:
AES encryption.

2. Digital Signatures

Provide authentication and integrity.

Used in:

- Online banking
- Secure emails

3. Access Control Mechanisms

Control user permissions.

Example:
Role-Based Access Control (RBAC).

4. Authentication Exchange

Protocols that verify identity.

Example:
Two-factor authentication (OTP).

5. Traffic Padding

Adds extra data to prevent traffic analysis.

6. Routing Control

Chooses secure routes for transmitting data.

7. Notarization

Uses trusted third party to verify communication.

Conclusion

Security mechanisms are practical tools that enforce protection and ensure system security.

6️⃣ Models for Network Security

Introduction

Network security models describe how secure communication occurs over insecure networks like the Internet.

The basic idea:
Sender encrypts message → Sends through network → Receiver decrypts message.

Basic Network Security Model

Steps:

1. Sender creates plaintext message.
2. Encryption algorithm converts it into ciphertext using a key.
3. Message travels through insecure network.
4. Receiver uses decryption algorithm and key to retrieve original message.

Diagram (Conceptual):

Sender → Encryption → Network → Decryption → Receiver

Components of Network Security Model

1. Plaintext
2. Encryption algorithm
3. Secret key
4. Ciphertext
5. Decryption algorithm
6. Trusted third party (optional)

Types of Network Security Models

1. Symmetric Key Model

Same key for encryption and decryption.

Problem:
Key distribution is difficult.

2. Public Key Model

Uses two keys:

- Public key
- Private key

Solves key distribution problem.

Conclusion

Network security models provide a structured way to secure communication across insecure networks.

7️⃣ Security Standards

Introduction

Security standards are official guidelines that define best practices for implementing security in organizations and systems.

They ensure uniform and secure implementation of security measures.

Important Security Standards

1. ISO/IEC 27001

International standard for Information Security Management Systems (ISMS).

Focus:

- Risk management
- Policy development
- Security controls

2. SSL/TLS

Used to secure web communication.

Used in:
HTTPS websites.

Provides:

- Encryption
- Authentication

3. IPsec

Provides security at network layer.

Used for:

- VPN connections

4. AES Standard

Advanced Encryption Standard.

Widely used symmetric encryption algorithm.

Importance of Security Standards

- Improve trust
- Ensure compliance
- Reduce risk
- Provide structured security framework

Conclusion

Security standards provide internationally accepted methods to implement and maintain security in organizations.

8 Symmetric Encryption Principles

Introduction

Symmetric encryption is a cryptographic technique in which the **same secret key** is used for both encryption and decryption. It is one of the oldest and most widely used methods of securing data.

It is mainly used to ensure **confidentiality** of information.

Basic Working

Plaintext → Encryption Algorithm + Secret Key → Ciphertext
Ciphertext → Decryption Algorithm + Same Secret Key → Plaintext

Both sender and receiver must share the same key securely.

Principles of Symmetric Encryption

Strong Encryption Algorithm
The algorithm should be secure even if publicly known.

Secret Key
Security depends entirely on keeping the key secret.

Key Distribution
The biggest challenge is securely sharing the key.

Advantages

Fast

Efficient for large data

Less computational power required

Disadvantages

Key distribution problem

Not suitable for large networks

Conclusion

Symmetric encryption is efficient and widely used for securing data, but secure key management is essential.

9️ Symmetric Block Encryption Algorithms

Introduction

Block ciphers encrypt data in **fixed-size blocks** (e.g., 64-bit or 128-bit blocks).

Instead of encrypting one bit at a time, they process blocks of data.

Working of Block Cipher

Divide plaintext into blocks.

Apply multiple rounds of substitution and permutation.

Produce ciphertext block.

Important Block Ciphers

1. DES (Data Encryption Standard)

64-bit block

56-bit key

16 rounds

Now considered insecure

2. AES (Advanced Encryption Standard)

128-bit block size

Key sizes: 128, 192, 256 bits

Highly secure

Widely used worldwide

Conclusion

Block ciphers like AES are the backbone of modern symmetric encryption systems.

🔟 Random and Pseudorandom Numbers

Introduction

Random numbers are essential in cryptography for generating keys, initialization vectors, and nonces.

True Random Numbers

Generated from physical processes such as:

- Thermal noise
- Atmospheric noise

Completely unpredictable.

Pseudorandom Numbers

Generated using mathematical algorithms.

They appear random but are deterministic.

Used in:

- Key generation
- Encryption algorithms
- Secure protocols

Importance in Cryptography

Weak randomness can break encryption systems.

Conclusion

Secure random number generation is critical for strong cryptographic systems.

1️⃣1️⃣ Stream Ciphers and RC4

Stream Cipher

Stream ciphers encrypt data **one bit or one byte at a time**.

Ciphertext = Plaintext ⊕ Key Stream

They are faster than block ciphers.

RC4

RC4 is a stream cipher developed by Ron Rivest.

Features:

- Variable key length
- Simple design
- Fast performance

Weakness:

- Vulnerable to attacks
- No longer recommended

Conclusion

Stream ciphers are useful for real-time communication but must be carefully implemented.

1️⃣2️⃣ Cipher Block Modes of Operation

Introduction

Block ciphers encrypt fixed-size blocks. To encrypt long messages, we use different modes of operation.

Common Modes

1. ECB (Electronic Codebook)

- Simplest mode
- Same plaintext block → Same ciphertext
- Not secure

2. CBC (Cipher Block Chaining)

- Each block depends on previous block
- More secure than ECB

3. CFB (Cipher Feedback)

Converts block cipher into stream cipher

4. OFB (Output Feedback)

Generates key stream independently

5. CTR (Counter Mode)

Uses counter values

Very fast and parallelizable

Conclusion

Cipher modes improve security and flexibility of block ciphers.

1️⃣3️⃣ Public Key Cryptography Principles

Introduction

Public Key Cryptography uses **two keys**:

Public Key (shared with everyone)

Private Key (kept secret)

It solves the key distribution problem of symmetric encryption.

Working

Encryption:
Public key encrypts message.

Decryption:
Private key decrypts message.

Advantages

No need to share secret key

Secure communication over public networks

Disadvantages

Slower than symmetric encryption

Computationally expensive

Conclusion

Public key cryptography is essential for secure internet communication.

1️⃣4️⃣ RSA Algorithm

Introduction

RSA is a widely used public key cryptographic algorithm.

It is based on the mathematical difficulty of factoring large prime numbers.

Steps in RSA

Choose two large prime numbers.

Compute n = p × q.

Compute Euler's Totient Function.

Choose public key (e).

Compute private key (d).

Encryption: C = M^e mod n.

Decryption: M = C^d mod n.

Security Basis

Security depends on difficulty of factoring large numbers.

Applications

- Secure emails
- Digital signatures
- HTTPS

Conclusion

RSA is one of the most important public key algorithms in modern cryptography.

1️⃣5️⃣ Secure Hash Functions

Introduction

A hash function converts data of any size into fixed-size output.

Example:
Message → SHA-256 → 256-bit hash

Properties

- Deterministic
- One-way function
- Collision resistant
- Fixed output length

Uses

- Password storage
- Digital signatures
- Data integrity verification

Conclusion

Secure hash functions are essential for maintaining integrity and authentication.

1️⃣6️⃣ Message Authentication Codes (MAC)

Introduction

MAC ensures both:

- Integrity
- Authentication

MAC = Hash(Message + Secret Key)

Working

- Sender generates MAC using secret key.
- Receiver verifies MAC using same key.

If MAC matches → Message is authentic.

Applications

- Banking systems
- Secure messaging
- API authentication

Conclusion

MAC provides strong protection against message tampering.

1️⃣7️⃣ Digital Signatures

Introduction

Digital signatures provide:

- Authentication
- Integrity
- Non-repudiation

They use public key cryptography.

Working

Sender hashes message.

Encrypts hash using private key.

Receiver decrypts using public key.

Compares hash values.

If match → Signature valid.

Applications

E-commerce

Online contracts

Government documents

Software distribution

Conclusion

Digital signatures ensure secure and trustworthy digital communication.