Lecture Notes Prepared By SWARNALATA SAHOO

4th Semester, Computer Science & Engineering

Information Security-(Th-5)-A

UNIT-I

Introduction to Information Security

Information Security : Information Security is the practice of protecting information from unauthorized access, use, disclosure, modification, or destruction to ensure confidentiality, integrity, and availability.

importance of information security : Cyber threats are increasing, and hence it's vital to have the right strategies and tools in place. Any negligence can lead to hefty financial and reputational losses. Information security helps safeguard an organization's data, systems, and operations from ever-evolving cyber threats. It allows businesses to:

- Protect the confidentiality, integrity, and availability of data.
- Prevent operational disruptions and maintain seamless day-to-day business functions.
- Meet compliance, regulatory, and legal obligations for safeguarding sensitive information.
- Maintain customer trust and brand reputation by avoiding exposure of sensitive information.
  Safeguard intellectual property to maintain profitability and competitive advantage.
  Align IT and cyber security strategies with overall business goals.

Key Principles of Information Security :

The CIA Triad is the foundation of Information Security and consists of three principles:

1. **Confidentiality.** Roughly equivalent to privacy, confidentiality measures are designed to prevent sensitive information from unauthorized access attempts. It's common for data to be classified according to the amount and type of damage that could be done if it fell into the wrong hands. More or less stringent data security measures can then be implemented according to those categories.

   Example: Password protection and encryption.

2. **Integrity.** The consistency, accuracy and trustworthiness of data must be maintained over its entire lifecycle. Data must not be changed in transit, and steps must be taken to ensure it can't be altered by unauthorized people. Example: Hashing and checksums.

3. **Availability.** Information should be consistently and readily accessible for authorized parties. This involves properly maintaining hardware and technical infrastructure and systems that hold and display the information.

   Example: Backup systems and protection against DoS attacks.

All three principles work together to protect information systems effectively.

Types of security threats and attacks:

- **Malware:** Malware stands for malicious software. This encompasses a wide range of harmful programs that can infiltrate a network through vulnerabilities. Malware can steal data, corrupt files, disrupt operations, or even take control of systems. Examples include viruses, worms, Trojan horses, ransom ware, and spyware.
- **Phishing:** Phishing attacks attempt to trick users into revealing sensitive information, such as usernames, passwords, or credit card details. Phishes often use emails or fraudulent websites that appear legitimate. Once a user enters their information, the attacker can steal it and misuse it.
- **Hacking:** Hacking is the act of compromising digital devices and networks through unauthorized access to an account or computer system. Hacking is not always a malicious act, but it is most commonly associated with illegal activity and data theft by cyber criminals.

- **DoS Attacks:** Flooding DoS attacks aim to overwhelm a network or system with traffic, making it unavailable to legitimate users. Attackers can flood the target with a massive amount of data requests, causing it to crash or become unresponsive. This can disrupt critical operations and cause significant financial losses.

Risk management and risk mitigation strategies :

Risk management in Information Security is the systematic process of identifying, analyzing, and reducing risks that can affect information assets. The objective is to minimize the impact of threats and vulnerabilities on organizational systems.

Steps in Risk Management

1. **Risk Identification:**
   Identifying critical assets, possible threats (malware, hacking), and vulnerabilities. This involves conducting comprehensive risk assessments across all critical areas –finance, operations, IT, legal, third parties and more
2. **Risk Analysis:**
   Analyzing the likelihood of threats and their potential impact. This allows you to prioritize which risks need immediate attention and which can be monitored over time.
3. **Risk Evaluation:**
   Prioritizing risks based on severity.
4. **Risk Mitigation:**
   Applying controls to reduce risk. A good mitigation plan outlines who is responsible, what actions will be taken, when they will be done, and how success will be measured. It should also include communication plans and contingency measures.
5. **Risk Monitoring:**
   Continuous review and improvement. Continuous monitoring helps you assess whether mitigation efforts are working and adjust your plan if conditions change.

Risk Mitigation Strategies

- **Firewalls and intrusion detection systems:** Firewalls act as barriers, blocking unauthorized access by filtering incoming/outgoing traffic based on security rules. IDS monitors networks for suspicious activities, providing early threat detection and alert generation.
  Data encryption: Converts sensitive data into unreadable formats, ensuring that even if data is breached, it cannot be read by unauthorized parties.
- **Regular backups:** Involves securely storing copies of critical data to allow rapid restoration and minimize downtime in the event of ransomware or other catastrophic data loss.
- **Access control mechanisms:** Restricts system access to authorized personnel using methods like Multi-Factor Authentication (MFA), role- based access control (RBAC), and password management.
- **User awareness training:** Educates employees to recognize phishing, social engineering, and other common threats, mitigating the risk of human error, which is often the weakest link in security.

Effective risk management helps organizations prevent security incidents and ensure business continuity.

Information security standards ISO/IEC 27001 and NIST :

ISO/IEC 27001

ISO/IEC 27001 is an international standard for establishing, implementing, maintaining, and improving an Information Security Management System (ISMS).

Key Features:

- Risk-based approach
- Security controls for data protection

- Continuous improvement

Benefits:

- Improves information security
- Reduces risks and incidents
- Enhances customer trust
- Supports legal compliance

NIST Cyber security Framework

Developed by the National Institute of Standards and Technology, NIST provides guidelines to manage cyber security risks.

Five Core Functions:

1. Identify: The Identify Function assists in developing an organizational understanding to managing cyber security risk to systems, people, assets, data, and capabilities. Understanding the business context, the resources that support critical functions and the related cyber security risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs.
2. Protect: The Protect Function outlines appropriate safeguards to ensure delivery of critical infrastructure services. The Protect Function supports the ability to limit or contain the impact of a potential cyber security event.
3. Detect: The Detect Function defines the appropriate activities to identify the occurrence of a cyber security event. The Detect Function enables timely discovery of cyber security events.
4. Respond: The Respond Function includes appropriate activities to take action regarding a detected cyber security incident. The Respond Function supports the ability to contain the impact of a potential cyber security incident.
5. Recover: he Recover Function identifies appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cyber security incident. The Recover Function supports timely recovery to normal operations to reduce the impact from a cyber security incident.

Significance

Both ISO/IEC 27001 and NIST help organizations:

- Improve cyber security posture
- Reduce vulnerabilities
- Respond effectively to incidents
- Ensure systematic and standardized security practices

Adopting these standards strengthens organizational security and resilience.

UNIT-II

Cryptography

Cryptography : Cryptography is the science of securing information by converting it into an unreadable form to prevent unauthorized access.

Symmetric Cryptography :

Symmetric cryptography is an encryption technique in which the **same secret key** is used for both **encryption** and **decryption** of data. The sender encrypts the message using the shared key, and the receiver uses the same key to decrypt it.

Working:

- Sender encrypts plaintext using a secret key.
- Encrypted data (cipher text) is sent to the receiver.
- Receiver decrypts cipher text using the same key.

Advantages:

- Fast and efficient for large amounts of data
- Requires less computational power
- Simple to implement

Disadvantages:

- Secure key distribution is difficult
- If the key is compromised, security is lost
- Not suitable for large networks

Examples: DES, AES

Asymmetric Cryptography :

Asymmetric cryptography (also called **public-key cryptography**) is a method of securing data using **two different but related keys** instead of one.

There are **two keys**:

- **Public key** → Shared with everyone
- **Private key** → Kept secret by the owner

Process:

1. Sender encrypts the message using the **receiver's public key**
2. The message travels securely
3. Receiver decrypts it using their **private key**

Example

- You share your **public key** with others
- Someone sends you a message encrypted with that key
- Only **you** can read it using your private key

Common uses :

- Secure websites (HTTPS)
- Email encryption
- Digital signatures
- Online banking

Difference between Symmetric and Asymmetric cryptography:

Symmetric Cryptography	Asymmetric Cryptography
• Uses a single key • Faster in operation • Difficult key • Less secure for large Example: AES	• Uses two keys (public & private) • Slower compared to symmetric • Easy key distribution distribution • More secure networks Example: RSA

DES(Data Encryption Standard):

Data Encryption Standard (DES) is a symmetric block cipher. By 'symmetric', we mean that the size of input text and output text (ciphertext) is same (64-bits). The 'block' here means that it takes group of bits together as input instead of encrypting the text bit by bit. Data encryption standard (DES) has been found vulnerable to very powerful attacks and therefore, it was replaced by Advanced Encryption Standard (AES).

- It is a block cipher that encrypts data in 64 bit blocks.
- It takes a 64-bit plaintext input and generates a corresponding 64-bit ciphertext output.
- The main key length is 64-bit which is transformed into 56-bits by skipping every 8th bit in the key.
- It encrypts the text in 16 rounds where each round uses 48-bit subkey.
- This 48-bit subkey is generated from the 56-bit effective key.
- The same algorithm and key are used for both encryption and decryption with minor changes.

Working of Data Encryption Standard (DES)

DES is based on the two attributes of Feistel cipher i.e. Substitution (also called confusion) and Transposition (also called diffusion). DES consists of 16 steps, each of which is called a round. Each round performs the steps of substitution and transposition along with other operations.

The encryption starts with a 64-bit plaintext that needs to be encrypted using a 64-bit key. Plaintext is passed to Initial Permutation function and key is permuted using Permuted Choice 1 (PC-1).

Initial Permutation

The 64-bit plaintext block is input into an Initial Permutation (IP) function that rearranges the order of bits. The order of bits is changed using predefined table. The IP table is a 8×8 matrix (64 entries) where each entry specifies the new position of a bit from the original plaintext.

Initial Permutation Table							
58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3

Initial Permutation Table							
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

Working of IP Table:

- The first bit of the permuted block is taken from the 58th bit of the original plaintext.
- The second bit comes from the 50th bit and so on.
- The last (64th) bit comes from the 7th bit of the original plaintext.

The initial permutation (IP) happens only once and it happens before the first round. The permutation this function do is fixed and does not depend on the plaintext. This rearranged 64-bit plaintext then go through 16 rounds. Each of this round uses a different 48-bit subkey from the previous round subkey. These subkeys are generated from 64-bit key.

Key Transformation
The 64-bit initial key is converted into 56-bit effective key. This 56-bit key further generates 48-bit subkeys for each of the 16 Feistel rounds.

Conversion of 64-bit Key into 56-bit Key
Initial key first go through Permuted Choice 1 (PC-1) which reduces the key to 56 bits. In PC-1 every eighth bit in key is discarded. That is bit positions 8, 16, 24, 32, 40, 48, 56, and 64 are discarded.

These discarded bits are called parity bits which are used for error checking. Remaining 56 bits are split into two 28-bit halves:

- Left Half (C_i): First 28 bits.
- Right Half (D_i): Last 28 bits

Here i represent the number of the Feistel round.

Generating 48-bit Round Subkeys
For each of the 16 rounds, right half (C_i) and left half (D_i) undergo circular left shift operation.
For Feistel round 1, 2, 9, and 16 both halves (left and right) undergo 1-bit left shift operation. For others rounds (3, 4, 5, 6, 7, 8, 10, 11, 12, 13, 14, 15) the halves undergo 2-bit left shift operation.

After circular shift operation is performed, C_i and D_i are again combined into 56-bit block. This block then go through Permutation Choice 2 (PC-2). The PC-2 selects and arrange 48 bits out of the 56 to form the round subkey (K_i). These 48 bits are selected on the basis of a predefined table as shown below:

Permutation Choice 2 Table							
14	17	11	24	1	5	3	28
15	6	21	10	23	19	12	4
26	8	16	7	27	20	13	2
41	52	31	37	47	55	30	40

Permutation Choice 2 Table							
51	45	33	48	44	49	39	56
34	53	46	42	50	36	29	32

According to this table 14th bit is placed to first position, 17th bit to second position, 11th bit to 3rd position and so on. The output 48-bit subkey of this table is used to cipher the plaintext in the Feistel round.

For next round we use already left shifted C_i and D_i as left and right half. We again perform the circular left shift operation on both halves. We again combine the result into 56-bit block and use permutation choice 2 to contract this block into 48-bit subkey for next round.

The process of Circular Left Shift and Permutation Choice 2 is followed for 16 rounds and different round subkey (K_i) is generated for each Feistel Round.

Each 48-bit subkey (K_i) is XORed with the expanded right half in the Feistel Round. Below is the explanation of what happens in every single Feistel round.

Feistel Rounds (1 - 16)

Every round receives 64-bits permuted plaintext from the Initial Permutation function and 48-bit transformed subkey (K_i). The permuted 64-bit plaintext is divided into two halves called as Left Plaintext (LPT) and Right Plaintext (RPT). Both of these halves are 32 bit in size. The right half or Right Plaintext (RPT) is processed using Mangler (F) function. Mangler (F) function involves expansion, key mixing, substitution (S-boxes), and permutation (P-box) of RPT.

he RPT first go through Expansion Permutation. In this permutation 32-bit Right Plaintext (RPT) is expanded into 48 bits using expansion box or E-box table.

E-Box Expansion Table					
32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29

E-Box Expansion Table					
28	29	30	31	32	1

The 48-bit expanded block is generated by arranging the bits as in E-Box table.

This expanded block is XORed (⊕) with the 48-bit round subkey that we generated during key transformation process. The XOR or Exclusive OR operation returns '0' as output if both inputs are same, else the out will be '1'. After XOR is performed, the resulting 48-bit block is split into eight chunks of 6-bit size each. Each of the chunk is then fed into a different S-box (S_1 to S_8).
For example, the output of XOR operation is converted into 6 bit chunks as follows:

101010 010001 011110 111010 100001 100110 010100 100111
These 6 bits chunks will be converted into 4 bits using S-Boxes.

S-Boxes are predefined lookup tables which reduces 6 bits chunk into 4 bits. Below is the list of these S-Boxes.
Suppose the first 6-bit chunk is 101010. We divide this chunk into two parts of 2 bit and 4 bit size. First and last bits are combined together for 2-bit part and rest bits make up the 4-bit part.

101010 -> (1)(0101)(0) -> divided into 10 and 0101
We look for these parts in the rows and columns of S_1 table. The number in the cell where row is '10' and column is '0101' is '6' in the S_1 table. The binary value of six is '0110'. This is the 4 bit value that S-Box 1 generated from the 6 bit input '101010'.
6-bit chunk: '101010' converted into 4-bit chunk: '0110'
Similarly we convert every 6-bit chunk into 4-bit value using S-Boxes. This process is called substitution. After that we combine all of these 4-bit chunks to get 32-bit block as output. This 32 bit again get permuted using following table.

P-box Permutation							
16	7	20	21	29	12	28	17
1	15	23	26	5	18	31	10
2	8	24	14	32	27	3	9
19	13	30	6	22	11	4	25

This permutation is called Transposition. The mangler function finishes here. 32-bit block after permutation is the output of mangler function. This block is XORed with 32-bit Left half or Left Plaintext (LPT) that was generated in the beginning of the Feistel round after Initial Permutation (IP). The output of this XOR operation serves as Right Half or Right Plaintext for next round and the initial Right Half (RPT) will serve as Left Half for the next round.

32-bit Swap and Inverse Initial Permutation

After these 16 rounds we get two blocks (Left and Right) of 32-bit each. The two 32-bit halves are again swapped back, resulting in a 64-bit block. This step is called 32-bit Swap in DES encryption algorithm.

Finally, the block undergoes an Inverse Initial Permutation (IP-1). This is essentially the inverse of the initial permutation applied at the beginning.

The result of the inverse initial permutation is the final 64-bit ciphertext which is the encrypted version of the original plaintext.

Decryption in DES (Data Encryption Standard)
Decryption in DES follows the same process as encryption but in reverse order. Since DES is a symmetric-key algorithm, the same key is used for both encryption and decryption, but the subkeys (round keys) are applied in reverse order.

- **Reverse Subkey Application**: The 16 round keys generated during key scheduling are used in reverse order (from K_{16} to K_1) during decryption.
- **Inverse Feistel Function**: The Feistel network structure ensures that decryption mirrors encryption. Each round performs the same operations (expansion, S-box substitution, permutation), but with reversed subkeys.
- **Final Permutation (FP)**: After 16 rounds, the output undergoes the Inverse Initial Permutation (IP), reversing the initial shuffling.

RSA Algorithm :
RSA is an **asymmetric encryption algorithm** based on the mathematical difficulty of factoring large prime numbers.

1. Key Generation

Step 1: Initialize two random large primes as p, q Step 2: Evaluate n as n = p * q
Step 3: Calculate φ(n) = (p – 1) * (q – 1)
Step 4: Select integer value e, gcd (φ(n),e) = 1; 1 < e < φ(n)
Step 5: Calculate d. d = e^{-1} mod φ(n)
Public key PU = {e,n} Private key PR = {d,n}

2. Encryption
   Plain text M < n
   Cipher text C = M^e mod n
3. Decryption
   Cipher text C
   Plain text P = C^d mod n

Let's say we choose p = 61 and q = 53. n = p * q = 61 * 53 = 3233

(n) = (p-1)(q-1) = 60 * 52 = 3120

Let's choose e = 17 (a common choice).

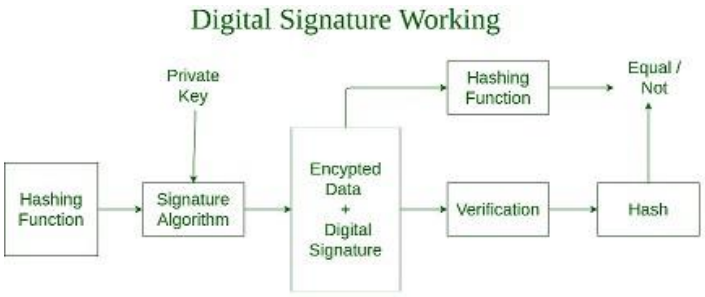
d = 2753 (computed such that (17 * d) mod 3120 = 1)

So, the public key is (3233, 17), and the private key is (3233, 2753). Encryption

To encrypt a message, the sender Uses the public key (n, e) provided by the recipient. Converts the plaintext message (m) into a ciphertext (c) using the formula −
c = m^e mod n.

<u>Digital Signatures with working</u> :
A digital signature is used to verify the **authenticity**, **integrity**, and **non- repudiation** of a message.
Digital signatures leverage cryptographic techniques, including hashing, encryption, and key pairs.
Working:

1. Sender creates a hash of the message
2. Hash is encrypted using sender's private key
3. Receiver decrypts it using sender's public key
4. Hash values are compared



1. Hashing: The first step in creating a digital signature is to generate a unique hash value from the original data. A hash function takes an and produces a fixed-size string of characters.

2. Encryption with private key: Once the hash value is generated, it is encrypted using the sender's private key. This encrypted hash becomes the digital signature. The signer keeps the private key secret. It ensures only they can create a valid signature for their messages. The combination of the original message and its digital signature is then sent to the recipient.

3. Decryption and verification: Upon receiving the signed document, the recipient uses the sender's public key to decrypt the digital signature. This process reveals the hash value that the sender had created originally. The recipient then independently computes the hash of the received document using the same hash function.

Comparison: Finally, the recipient compares the decrypted hash value with their own computed hash value. If both hashes match, it confirms that: The message was indeed sent by the claimed sender (authentication) and The message has not been altered during transmission (integrity)**.**

<u>Public Key Infrastructure (PKI)</u> :

PKI is a framework that manages public key encryption and digital certificates to ensure secure communication.

Main Components:

1. **Certificate Authority (CA):** The CA is a trusted entity that issues, stores, and signs the digital certificate.
2. **Digital Certificate:** This database stores the digital certificate and its metadata, which includes how long the certificate is valid.
3. **Public & Private Keys:** The CA signs the digital certificate with their own private key and then publishes the public key that can be accessed upon request.
4. **Registration Authority (RA):** The RA verifies the identity of the user or device requesting the digital certificate. This can be a third party, or the CA can also act as the RA.

Functions of PKI:

- Secure data exchange
- Authentication
- Trust establishment

Applications:

- SSL/TLS
- Secure email
- E-commerce

UNIT-III

Network Security

Network Security : Network security refers to the practices, policies, and technologies used to protect data during transmission and prevent unauthorized access, misuse, or attacks on a network.

protect data during transmission :

Network security refers to the policies, practices, and technologies used to protect network infrastructure and data from unauthorized access, misuse, modification, or attacks. It ensures confidentiality, integrity, and availability of data.

Methods to protect data during transmission:

1. **Encryption:** Converts data into unreadable form to prevent unauthorized access. Protocols like SSL and TLS are used to secure data transmitted over the internet.
2. **Secure Protocols:** Use of SSL/TLS, IPSec, and HTTPS, FTP ensures that that data is encrypted during transmission.
3. **Firewalls:** Monitoring and Control incoming and outgoing traffic based on security rules.
4. **Authentication:** Ensures only authorized users access the network.
5. **VPNs:** Create secure tunnels over public networks, such as the internet, ensuring that remote users can access company networks safely.
6. **Intrusion Prevention System**: These systems actively scan network traffic to detect and block malicious threats or unauthorized access attempts in real-time.

Firewalls :

A **firewall** is a network security system that monitors and controls network traffic based on predefined security rules. It acts as a barrier between trusted internal networks and untrusted external networks.

Types of Firewalls

1. **Packet Filtering Firewall:**
   - Filters packets based on IP address, port number, and protocol.
   - Fast but less secure.
   - Simple and efficient, suitable for basic filtering.
   - Limited in scope, unable to inspect the payload of the packet.
2. **Stateful Inspection Firewall:**
   - Tracks the state of active connections.
   - Allows only legitimate packets.
   - More secure than packet-filtering as they can recognize if packets are part of an established connection.
   - More complex and resource-intensive.
3. **Proxy Firewall:**
   - Acts as an intermediary between user and internet.
   - Hides internal IP addresses.
   - High-level security, can block specific applications.
   - Can introduce latency and require more resources.
4. **Next-Generation Firewalls (NGFW):**
   - Include additional features like deep packet inspection, intrusion prevention systems (IPS), and application awareness.
   - Comprehensive security, capable of handling modern threats.
   - Expensive and complex to manage.
5. **Unified Threat Management (UTM):**

- UTM devices combine several security features, including firewall, antivirus, and content filtering, into one appliance.
- Simplifies security management.
- May not be as powerful or flexible as dedicated solutions.

Firewall Configuration

Firewall configuration involves setting rules such as:

1. Principle of Least Privilege: Only allow traffic that is explicitly required for your network operations. Deny all other traffic by default.
2. Regular Updates: Keep your firewall and its rules updated to protect against the latest threats.
3. Log and Monitor: Enable logging to monitor traffic patterns and detect potential anomalies.
4. Segment Your Network: Use firewalls to segment your network into smaller, manageable zones to limit the spread of an attack.
5. Use Strong Authentication: Ensure that access to your firewall's management interface is protected by strong, multifactor authentication.

IDS & IPS :

Intrusion Detection System (IDS)
IDS is a hardware or software tool that monitors and analyzes network or system activities for signs of unauthorized access or policy violations. It passively scans incoming traffic and compares it to pre-configured signatures or behavioral patterns. IDS alerts the system administrator when potential threats are detected but does not take any active action to block or mitigate them.

Intrusion Prevention System (IPS)
IPS is an advanced security system that not only detects malicious activities but also prevents them from happening in real-time. It intercepts network traffic, compares it to known threat signatures, and immediately blocks or neutralizes suspicious activities before they can cause damage. IPS is proactive, while IDS is primarily reactive.

Comparison

Feature	**IDS (Intrusion Detection System)**	**IPS (Intrusion Prevention System)**
Position	Out-of-band (Passive)	Inline (Active)
Function	Detects & Alerts	Detects & Prevents
Network Impact	Low	High (Potential Latency)
Response	Delayed (Human required)	Real-time (Automated)
Example	Suricata (in IDS mode)	Suricata (in IPS mode)

VPN : A Virtual Private Network (VPN) is a technology that creates a secure and encrypted connection over a public network like the Internet.

Types of VPN:

A) Types based on usage (deployment)

- **Remote Access VPN:** It allows an individual user to securely connect to a private network over the internet, and it is widely used by employees working remotely.
  Site-to-Site VPN: It securely connects two or more separate networks, such as a head office and branch offices, so internal communication remains protected across locations.
- **Mobile VPN:** It is designed for mobile users and keeps the VPN session stable even when the device switches between Wi-Fi and cellular networks.
- **MPLS VPN:** It is a provider-managed enterprise WAN solution that offers scalable connectivity and traffic prioritization, but it typically does not provide end-to-end encryption by default.

B) Types based on Protocols (Tunneling Technology)

- **PPTP:** It is an older protocol that can be fast, but it provides weak security, so it is mainly used only for legacy systems.
- **L2TP/IPSec:** It combines L2TP tunneling with IPSec encryption, which improves security, but it can add performance overhead.
- **Open VPN:** It is an open-source protocol that uses SSL/TLS for encryption, and it is widely adopted because it provides strong security and flexibility.
- **IKEv2/IPsec:** It is a secure and fast protocol that works very well on mobile devices because it reconnects quickly when network conditions change.
  Advantages of VPN:

- Ensures data confidentiality
- Provides secure remote access
- Protects against eavesdropping
- Improves privacy

VPNs are widely used in corporate networks.

HTTPS :

HTTPS (Hypertext Transfer Protocol Secure) is a secure version of HTTP that uses SSL/TLS for encryption.

Advantages of HTTPS:

- Protects sensitive data
- Prevents data tampering
- Increases user trust

HTTPS is essential for secure web communication.

Key Differences Between HTTP and HTTPS

Security & Encryption: HTTP transfers data in plain text, making it vulnerable to interception. HTTPS uses SSL/TLS to encrypt data, ensuring privacy.

Protocol & Port: HTTP operates on port 80. HTTPS operates on port 443.

Trust & Validation:

HTTPS uses digital certificates to verify the website's identity. Browsers often label HTTP sites as "Not Secure".

Performance: While HTTP is theoretically faster, modern enhancements have made the performance difference

negligible compared to the security benefits of HTTPS.

Usage: HTTP is used for basic, non-sensitive browsing. HTTPS is required for websites handling sensitive information (passwords, credit cards) and for improved SEO, as search engines favor secure sites.

UNIT-IV

Security in Operating Systems

Operating System security : Operating system (OS) security encompasses the strategies and techniques employed to protect the OS from threats, vulnerabilities, and unauthorized access. It includes measures like access control, patching, firewalls, intrusion detection/prevention systems, and anti-malware software to ensure the confidentiality, integrity, and availability of the OS and the data it manages.

User authentication : User authentication is the critical checkpoint that verifies users' identities to protect sensitive data from unauthorized access. At its core, it ensures users are who they claim to be via credentials like passwords, tokens, or biometric data.

Biometric authentication : Biometric authentication is a technology that uses biological characteristics to verify a person's identity and grant access to secure systems or locations.

Examples of biometric identifiers include fingerprints, facial recognition, DNA, and retinal scans.

Password-based authentication :

1. The user creates an account by providing a unique identifier such as email, username, or phone number.
2. The user is prompted to create a password, which usually must meet certain complexity requirements.

- The set of credentials is stored in the system's database, usually in an encrypted form to protect against data breaches.
- When a user tries to log in, the authentication system checks their submitted credentials against those stored in its database.
- If they match, the user is granted access.
- If they don't match, the user will be denied entry and may be prompted to reenter their information or reset their password in case they forgot it.

Two-factor authentication (2FA) :

Two-factor authentication (2FA) is a security system that requires two distinct forms of identification in order to access something. Two-factor authentication can be used to strengthen the security of an online account, a smart phone, or even a door. 2FA does this by requiring two types of information from the user a password or personal identification number (PIN), a code sent to the user's smart phone, or a fingerprint before whatever is being secured can be accessed. Authentication ensures that only authorized users can access the OS.

File system encryption and its importance :

File system encryption is a security technique used to protect data stored on a computer or storage device by converting it into an unreadable (cipher) form. Only authorized users with the correct decryption key can access the original data. It ensures that even if someone gains physical or unauthorized access to the storage, the data remains protected.

Types of File System Encryption

1. **Full Disk Encryption (FDE):**
   Encrypts the entire storage device, including the operating system, system files, and user data.
   Example*:* Bit Locker, File Vault.
2. **File-Level or Folder-Level Encryption:**
   Encrypts specific files or directories selected by the user, providing granular control over sensitive data.

How File System Encryption Works

- Data is encrypted using cryptographic algorithms before being written to disk.

- When an authorized user accesses the file, it is automatically decrypted after authentication.
- Unauthorized users see only encrypted, unreadable data.

Importance of File System Encryption

1. **Data Confidentiality:** Protects sensitive information from unauthorized access.
2. **Protection Against Data Theft:** Ensures data remains secure even if a device is lost or stolen.
3. **Prevents Unauthorized Access:** Blocks attackers from reading stored data without keys.
4. **Compliance with Security Policies:** Helps meet legal and organizational data protection requirements.

Safeguards Personal and Organizational Data: Especially important for financial, medical, and confidential records.

<u>OS security hardening techniques and their importance</u> :

OS Security Hardening Techniques

1. **Disabling Unused Services and Ports**
   - Unnecessary services increase security risks.
   - Disabling them reduces entry points for attackers.
2. **Removing Unnecessary Software**
   - Extra applications may contain vulnerabilities.
   - Keeping only required software improves security.
3. **Strong Password Policies**
   - Enforcing complex passwords and regular password changes.
   - Prevents brute-force and guessing attacks.
4. **User Access Control and Least Privilege**
   - Users are given only minimum required permissions.
   - Limits damage from compromised accounts.
5. **Regular Patch Management and Updates**
   - Applying security patches fixes known vulnerabilities.
   - Keeps the OS protected from recent threats.
6. **Enabling Firewalls and Antivirus Software**
   - Firewalls block unauthorized network access.
   - Antivirus software detects and removes malware.
7. **System Logging and Auditing**
   - Logs system activities for monitoring and analysis.
   - Helps in detecting and investigating security incidents.
8. **Secure Configuration Settings**
   - Changing default passwords and settings.
   - Enabling secure boot and encryption features.

Importance of OS Security Hardening

1. **Reduces Attack Surface**
   - Fewer vulnerabilities mean fewer chances for attacks.
2. **Prevents Unauthorized Access**
   - Strong controls protect system resources.
3. **Improves System Stability and Reliability**
   - Secure systems face fewer disruptions.
4. **Protects Sensitive Data**
   - Prevents data breaches and data loss.
5. **Ensures Compliance with Security Standards**
   Helps organizations meet security policies and regulations.

<u>Patch management and update strategies in operating systems.</u>

Patch management is the process of identifying, testing, deploying, and maintaining updates (patches) for an operating system to fix security vulnerabilities, bugs, and performance issues. Effective patch management ensures that the OS remains secure, stable, and up to date.

Patch Management Process

1. **Patch Identification**
    - Security patches and updates are released by OS vendors.
    - Systems are checked to identify missing or required patches.
2. **Patch Assessment and Prioritization**
    - Patches are evaluated based on severity and risk.
    - Critical security patches are prioritized.
3. **Patch Testing**
    - Patches are tested in a controlled environment.
    - Ensures compatibility and avoids system failures.
4. **Patch Deployment**
    - Approved patches are installed on systems.
    - Can be done manually or automatically.
5. **Verification and Monitoring**
    - Confirms that patches are correctly installed.
    - Monitors systems for issues after updates.

Update Strategies in Operating Systems

1. **Manual Updates**
    - Administrator installs updates manually.
    - Suitable for small systems but time-consuming.
2. **Automatic Updates**
    - OS downloads and installs updates automatically.
    - Ensures timely security protection.
3. **Scheduled Updates**
    - Updates are installed at predefined times.
    - Minimizes system downtime.
4. **Centralized Patch Management**
    - Uses management tools to update multiple systems.
    - Common in enterprise environments.
5. **Rollback Strategy**
    - Allows reverting to previous versions if updates fail.
    - Prevents system instability.

Importance of Patch Management

- Protects against known security vulnerabilities
- Prevents malware and cyber attacks
- Maintains system performance and stability
- Ensures compliance with security policies

Security auditing and monitoring:

Security auditing and monitoring are essential OS security practices used to detect, prevent, and respond to unauthorized activities and security threats. They help maintain system integrity, confidentiality, and availability.

1. **Security Auditing**

Security auditing is the process of examining system logs, configurations, and activities to identify security violations or potential threats.

Purpose of Security Auditing:

- Detect policy violations and unauthorized access.
- Investigate past security incidents.
- Ensure compliance with security standards.

2. Security Monitoring

Security monitoring involves continuously observing OS activities in real time to detect suspicious behavior and potential attacks.

Techniques of Security Monitoring:

1. **Real-Time Alerts:** Immediate notification of unusual activity, such as multiple failed logins.
2. **Intrusion Detection:** Monitoring system and network traffic for anomalies.
3. **Performance Monitoring:** Checks for abnormal CPU, memory, or network usage that may indicate an attack.
4. **Log Analysis:** Continuous review of system logs for patterns of malicious activity.

Benefits of Security Monitoring:

- Early detection of attacks or breaches.
- Enables quick response to security incidents.
- Helps maintain system integrity and availability.

UNIT-V

Web Security

Web Security: Web security is the practice of protecting websites, web applications, and web services from cyber threats and attacks.

Cross-Site Scripting (XSS) : XSS is an attack that injects malicious scripts into web pages viewed by other users. Cross-Site Scripting (XSS) is a web security vulnerability that allows an attacker to inject malicious client-side scripts (typically JavaScript) into web pages viewed by other users.

The victim's browser executes the malicious script because it trusts the content is from a legitimate source, enabling the attacker to steal sensitive data, hijack user sessions, or deface websites.

Types of XSS:

1. **Stored XSS:** The malicious script is permanently stored on the target server, such as in a database, a comment field, or a forum post. The script is executed in the browser of every user who views the compromised page. This is considered the most dangerous type because one injection can affect many users automatically.
2. **Reflected XSS:** The malicious script is included in a link sent to a victim, often through social engineering via email or a social media post. The script is "reflected" off a vulnerable web application and executed in the user's browser as part of the immediate HTTP response. This attack is non-persistent and requires the victim to click on the specially crafted link.
3. **DOM-based XSS:** The malicious script is included in a link sent to a victim, often through social engineering via email or a social media post. The script is "reflected" off a vulnerable web application and executed in the user's browser as part of the immediate HTTP response. This attack is non-persistent and requires the victim to click on the specially crafted link.

Prevention Techniques:

- Validate and sanitize user input.
- Encode output in HTML or JavaScript contexts.
- Use Content Security Policy (CSP)

Web Application Development Practices :

Secure web development reduces vulnerabilities during application design and coding.

Key Development Practices

Authentication & Authorization: Implement robust password policies, hashing (e.g., bcrypt), multi-factor authentication (MFA), and role-based access control (RBAC).

Input Validation & Sanitization: Treat all input as untrusted, utilizing server- side validation and prepared statements to prevent injection and XSS attacks.

Data Encryption: Ensure HTTPS for data in transit and encrypt sensitive data at rest, managing keys securely.

Session Management: Generate secure, unique session IDs, enforce timeouts, and use HttpOnly/Secure cookie flags.

Error Handling & Logging: Avoid detailed error messages to users and maintain centralized, active monitoring of security-relevant events.

Dependency & API Security: Scan third-party components for vulnerabilities and apply security best practices to all APIs.

Testing & Maintenance: Integrate SAST/DAST tools into the CI/CD pipeline, conduct penetration testing, and regularly patch software.

Developer Training: Foster a security-first culture through ongoing education on threats and secure coding.

Cookies and secure management of cookies:

Definition:

Cookies store user session data or preferences on the client side.

Secure Management of Cookies

To protect against session hijacking and theft, developers and users should utilize the following security measures:

- **Secure Flag:** Ensures the cookie is only sent over encrypted HTTPS connections, preventing interception.
- **HttpOnly Flag:** Prevents client-side scripts (like JavaScript) from accessing the cookie, reducing risk of Cross-Site Scripting (XSS) attacks.
- **SameSite Attribute:** Restricts the cookie from being sent with cross-site requests, protecting against Cross-Site Request Forgery (CSRF). Options include Strict or Lax.
- **Short Lifetimes:** Set appropriate expiration times (Max-Age) to reduce the window of opportunity for attackers.
- **Encryption:** Sensitive data within cookies should be encrypted.

How to Manage Cookies (User Level)

- **Browser Settings:** Users can view, block, or delete cookies in browser settings (e.g., clearing cache, setting to "Block third-party cookies").

Consent Management: Websites are required to provide options for accepting only necessary cookies.

OWASP and its significance in web security :

Definition:

OWASP (Open Web Application Security Project) is an organization providing guidelines and tools for web security.

Key Aspects of OWASP

- **Nonprofit Community:** It operates as an open community, making all its educational materials, tools, and documentation free and accessible.
- **OWASP Top 10:** This widely recognized document ranks the most critical security risks (e.g., Injection, Broken Access Control, Cryptographic Failures) based on frequency and severity.
- **Tools and Resources:** OWASP ZAP (Zed Attack Proxy) is a popular open- source web application scanner. Other resources include the Application Security Verification Standard (ASVS) and the Web Security Testing Guide (WSTG).

Significance in Web Security

- **Standardizing Security:** The Top 10 acts as a, standard awareness document for developers and security professionals, defining best practices to mitigate vulnerabilities.
- **Compliance and Risk Reduction:** Auditors and organizations often use OWASP to guide their security policies and comply with regulatory requirements.
- **Education and Awareness:** It helps developers understand the most common and damaging threats, promoting a proactive "security-by- design" approach.

Continuous Improvement: With global chapters and thousands of volunteers, it provides up-to-date, community-driven insights into evolving cyber threats.

UNIT-VI
Security Policies and Incident Response

Security Policies (access control and data protection policies)

A security policy is a formal document that defines rules, procedures, and guidelines for protecting an organization's information systems and data. It establishes standards for secure operation and helps prevent unauthorized access, misuse, or damage to information assets.

Objectives of Security Policies

- Protect confidentiality, integrity, and availability of information.
- Reduce security risks and cyber threats.
- Ensure compliance with legal and regulatory requirements.
- Define responsibilities of users and administrators.

Access Control Policy

Access control policies determine who can access specific resources and under what conditions.

Types of Access Control

- **Discretionary Access Control (DAC):** Resource owner grants access.
- **Mandatory Access Control (MAC):** Access based on security classification.
- **Role-Based Access Control (RBAC):** Access based on job roles.

Importance

- Prevents unauthorized access.
- Ensures accountability and monitoring.

Data Protection Policy

Data protection policies define how data is stored, processed, and transmitted securely.

Key Measures

- Data encryption.
- Regular backups.
- Access restrictions.
- Data classification and handling procedures.

Benefits of Security Policies

- Improves organizational security posture.
- Reduces risk of data breaches.
- Provides guidance during incidents.

BCP : Access control mechanisms are methods used to ensure that only authorized users can access specific systems, applications, or data. These mechanisms protect sensitive information and prevent unauthorized usage.

Types of Access Control

1. **Discretionary Access Control (DAC):**

In DAC, the owner of the resource decides who can access it. Permissions are assigned based on user identity.

2. **Mandatory Access Control (MAC):**
   Access is controlled by a central authority based on security classifications. Users cannot change permissions.
3. **Role-Based Access Control (RBAC):**
   Access is granted according to job roles. For example, an administrator has more privileges than a normal user.

Importance of Access Control

- Protects confidential data from unauthorized access.
- Reduces insider and outsider threats.
- Maintains data integrity and confidentiality.
- Ensures accountability by tracking user actions.

Access control is a fundamental component of security policies that helps maintain overall system security.

Backup and Recovery Strategies in Disaster Recovery Planning (DRP) :

Backup and recovery strategies are essential components of Disaster Recovery Planning that ensure systems and data can be restored after failures or disasters.

Types of Backup

- **Full Backup:** Creates a complete copy of all data.
- **Incremental Backup:** Saves only the changes made after the last backup.
- **Differential Backup:** Saves changes made since the last full backup.

Recovery Process

- Identifying damaged systems.
- Restoring data from backup.

Testing systems before returning to operation.

Importance

- Prevents permanent data loss.
- Reduces system downtime.
- Maintains business continuity.
- Helps organizations recover quickly after disasters.

Regular backup and testing of recovery procedures are necessary for effective disaster recovery.

Role of Policies and Procedures in Incident Response Management :

Policies and procedures provide structured guidelines for managing security incidents effectively and consistently.

Role of Policies

- Defines responsibilities of incident response team members.
- Establishes reporting and communication methods.
- Ensures compliance with organizational and legal requirements.

Role of Procedures

- Provides step-by-step instructions for handling incidents.
- Helps in proper documentation and evidence collection.
- Reduces confusion during emergencies.

Benefits

- Faster response to incidents.
- Reduced damage and recovery time.
- Improved coordination among teams.
- Helps prevent similar incidents in the future.

Properly defined policies and procedures strengthen an organization's ability to manage and recover from security incidents.

Digital Forensics, Evidence Gathering, and Legal & Ethical Considerations in Information Security :

Digital forensics involves collecting, preserving, analyzing, and presenting digital evidence related to security incidents or cybercrimes. It plays a critical role in investigations and legal proceedings.

Digital Forensics Process

1. **Identification:** Locating potential evidence sources.
2. **Preservation:** Protecting evidence from modification.
3. **Collection:** Acquiring data using forensic tools.
4. **Analysis:** Examining evidence to determine attack details.
5. **Reporting:** Documenting findings for legal or organizational use.

Evidence Gathering

- Maintain chain of custody.
- Use authorized forensic tools.
- Avoid altering original evidence.
- Document every action taken.

Legal Considerations

- Compliance with data protection and privacy laws.
- Authorization before accessing systems.
- Proper handling of sensitive information.

Ethical Considerations

- Respecting privacy and confidentiality.
- Responsible use of security privileges.
- Maintaining honesty and professionalism.

Following forensic procedures and legal guidelines ensures evidence reliability and prevents legal complications.