Information security

1] Define Authentication. Explain two parts of authentication

→ • Authentication in the Information security is the process of verifying the identity of a user, system or device to ensure that they are who they claim to be.

• Authentication helps protect data and systems by allowing access only to authorized entities.

Types of Authentication

1] Knowledge-Based Authentication (Something You Know):

- Requires information that only the user knowns.
- Examples: Passwords, PINs and security questions.

2] Possession-Based Authentication (Something You have):

- Requires the user to posses a physical or digital object.
- Examples: OTP (one-Time Password), Smart cards and security tokens.

3] Inherence-Based Authentication (Something you are):

- Uses the user's unique biological traits.
- Examples: Fingerprints, facial recognition and voice patterns.

3] Mutual Authentication (optional):

- The server may also present its certificate to the user for mutual trust
- Both parties validate each other's certificate before establishing a connection.

4] Secure connection:

If the certificate is valid, a secure connection (often using SSL/TLS) is established.

Advantages:
- stronger security than passwords
- Eliminates the needs for passwords.
- Supports mutual authentication, enhancing trust.

Use Cases:
- Secure websites using HTTPS (SSL/TLS certificate)
- VPN authentication
- Email encryption and signing
- Code signing for software distribution.

2] Certificate Based Authentication

→ • Certificate Based Authentication is a security mechanism that verifies the identity of users, devices or systems using digital certificates issued by a trusted Certificate Authority (CA).
• Certificate Based Authentication is based on Public Key Infrastructure (PKI), which uses pairs of cryptographic keys (public and private keys) to establish trust and secure communication.

Certificate Based Authentication works:

1] Issuing the certificate:

• A Certificate Authority (CA) issues a digital certificate to the user or device
• The certificate include information like the entity's public key, identity details and the CA's digital signature.

2] Authentication Process:

• When a user or device attempts to access a system, it presents the certificate.
• The server verifies the certificate by checking:
  → if it was issued by a trusted CA.
  → if it has not expired or been revoked.
  → if the certificate matches the entity's private key.

4] Location - Based Authentication:

- Verifies Identity based on the user's geographic location
- Examples: GPS location and IP Address.

5] Behavior - Based Authentication:

- Analyzes patterns of user behavior for verification
- Example: Typing speed and mouse movements

4] Symmetric Key Cryptography

→ • Symmetric Key Cryptography is a type of encryption where the same key is used for both encryption and decryption of data.
• Symmetric Key Cryptography is also known as secret key cryptography because the key must be kept secret between the sender and the receiver to maintain security.

How it works:

1] Key Generation: A single secret key is generated and shared between the sender and receiver.

2] Encryption: The sender uses this key to convert plaintext (original message) into ciphertext (encrypted message).

3] Transmission: The ciphertext is sent over the communication channel.

4] Decryption: The receiver uses the same key to convert the ciphertext back into plaintext.

Types of Symmetric Key Algorithm:

1] Block Ciphers: Encrypt data in fixed-size blocks (e.g., AES, DES).

Example:

- Admin : Can create, modify, delete and view records.
- Manager : Can modify and view records but cannot delete them.
- Employee : Can only view records.

Advantages :

- Simplified Access Management
- Enhanced security
- Scalability
- Reduce Administrative Overhead
- Improved System Performance

Authroization is the process of granting a user's access to specific resources and actions.

2] Role-Based Authorization

→ . Role-Based Authorization (RBN) is a method of controlling access to resources in a system based on the roles assigned to users.
Instead of granting permissions directly to individual users, permissions are assigned to roles, and users gain access based on the roles they hold.

How Role-Based Authorization works:

1] Define Roles: Identify Roles based on organizational structure or job responsibilities/ functions
(e.g., Admin, Manager, Employee).

2] Assign Permissions to Roles:
Specify the actions and resource each role can access.
(e.g., read, write and delete).

3] Assign Roles to users:
Associate users with one or more roles depending on their job requirements.

4] Access Control:
When a user requests access to a resource, the system checks if their assigned role includes the required permissions.

Since only the recipient has the private key, only they can decrypt the message.

3] Applications:

- Secure communication — HTTPS, email encryption (PGP), VPNs
- Digital signatures - Documents signing, software authenticity
- Authentication - SSL/TLS certificates, SSH Keys
- Key Exchange - Establishing secure symmetric key using Diffie-Hellman

5] Public Key cryptography

→ • Public Key cryptography is a method of encrypting and securing data using two keys: a public key and a private key.
• This system allows secure communication and data exchange over an insecure network without needing to share a secret key in advance.

1] Key components:

a] Public Key: The public key is shared openly and can distributed without compromising security.
• It is used for: Encrypting messages
verifying digital signatures.

b] Private key: The private key is kept secret and known only to the owner.
• It is used for: Decrypting messages
creating digital signatures.

2] How It works:

Encryption and Decryption process

1 The sender retrieves the recipient's public key
• The sender encrypts the message using the public key
• The encrypted message is sent over the network
• The recipient uses their private key to decrypt the message

2] Stream Ciphers: Encrypt data bit-by-bit or byte-by-byte (e.g., RC4).

Advantages:

- Fast and Efficient
- simple to Implement
- Low resource usage
- Good for Bulk Data

Disadvantages:

- Key Distribution Problem
- Scalability Issues.
- Difficult to Rotate Key
- NO Built-In Key Exchange

Best Practice

7] Database Level security

→ • In Information security, Database Level security refers to the protection measures applied directly within the database to safeguard stored data from unauthorized access, breaches and corruption
• (Database Level security ensures the confidentially, integrity and availability of data) stored in the database.

Components of Database Level security:

1] Authentication :
• Ensures that only authorized users can access the database.
• Methods include usernames, passwords, multi-factor authentication (MFA) and biometric authentication.

2] Authorization and Access Control:
• Controls what actions a user can perform once authenticated
• Role-Based Access Control (RBAC) assign permissions based on user roles,
Principle of Least Privilege (POLP) ensures users have only the minimum permissions needed.

3] Encryption:
• Protects data by converting it into a secure format.
• Data at Rest - Encryption of stored data.
• Data in Transit - Encryption of data during transmission using SSL/TLS

5] Certificate Revocation List (CRL):
A list of revoked or expired certificates maintained by the CA.

Uses of Public Key Infrastructure (PKI):

- Secure websites using HTTPS.
- Email encryption.
- Digital signatures for document integrity
- Secure remote access using VPN.

Best Practices:

- ——— " ——— Best Practice are guidelines and strategies designed to protect system, networks and data from ——— " ———
- Best Practice ——— " ——— ——— " ——— of information.

6] Public Key Infrastructure

→ • Public Key Infrastructure (PKI) is a framework of polic roles, hardware, software and procedures needed to create, manage, distribute, use, store and revoke digital certificates and public keys.
• Public Key Infrastructure (PKI) ensures secure electro communication and data exchange by using encryp and authentication.

Key Components of PKI :

1] Certificate Authority (CA) : Issues and verifies digital certificates, ensuring the authenticity of the public key.

2] Registration Authority (RA) : Confirms user identity before the CA issues a certificate.

3] Public and Private Keys :

• Public Key : Shared openly and used to encrypt data.

• Private Key : Kept secret and used to decrypt data.

4] Digital Certificate : A file/document issued by the CA that binds a public key to an entity (user or organization)

6] Hot Backup (Online Backup):

A Hot Backup is taken while the database is online and accessible to users.

7] Logical Backup:

A Logical Backup involves exporting data in the form of SQL statements or other readable formats.

8] Different Type of Database Backups

→ . Database Backups are essential for protecting data and ensuring recovery in case of data loss, corruption or system failure.

. Different Types of Database backups are designed for various recovery needs and storage strategies.

1] Full Backup : A Full Backup creates a complete copy of the entire database, including all data, tables, indexes and transaction logs.

2] Incremental Backup: An Incremental Backup only stores changes made since the last backup (whether it was full or incremental)

3] Differential Backup :
A Differential Backup stores changes made since the last full backup (but not since the last differential backup)

4] Mirror Backup: A mirror Backup create an exact copy of the database in real-time

5] Cold Backup (offline Backup):
A cold backup is taken while the database is offline (not accessible to users)

4] Auditing and Monitoring:

- Tracks user activities and database access.
- Generates logs to identify unauthorized access or suspicious activity.

5] Backup and Recovery:

- Regular backups protect against data loss due to hardware failure, corruption or attacks.
- Ensures quick recovery in case of data corruption or system failure.