CNS-2023-May-PYQ

Q1. [5 Marks]

a. Explain Security Services and mechanisms to implement it.

Q2. [10 Marks]

a. Explain Playfair cipher with example

b. Describe different Block Cipher modes

Q3. [10 Marks]

a. State firewall design principles and its types with advantages.

Q4. [10 Marks]

a. Explain Kerberos Protocol in detail.

Q6. [20 Marks]

a. Define Malware. Explain at least five types with example.

Q1. [5 Marks] - Answers

a. Explain Security Services and mechanisms to implement it.

1. Security Services

Security services are functions provided to ensure **protection of data** and **secure communication** between entities in a network.

Main Security Services (as per OSI model):

1. **Authentication:**
    - Verifies the identity of users or systems.
    - Ensures communication is with a legitimate entity.
    - *Example:* Login passwords, digital certificates.

2. **Access Control:**
    - Restricts unauthorized users from accessing system resources.
    - *Example:* Role-based access control (RBAC).

3. **Data Confidentiality:**
    - Protects data from unauthorized disclosure.
    - *Example:* Encryption using AES, DES.

4. **Data Integrity:**
    - Ensures data is not altered during transmission.
    - *Example:* Hash functions, digital signatures.

5. **Non-repudiation:**
    - Prevents denial of participation in communication.
    - *Example:* Digital signatures in online transactions.

2. Security Mechanisms

These are the **methods or tools** used to implement the above services.

Common Mechanisms:

- **Encryption:** Protects confidentiality.
- **Digital Signatures:** Provide integrity and non-repudiation.

- **Authentication Protocols:** Ensure user identity (e.g., Kerberos).
- **Access Control Lists (ACLs):** Enforce authorization policies.
- **Firewalls and Intrusion Detection Systems (IDS):** Protect against unauthorized access.

Q2. [10 Marks] - Answers

b. Describe different Block Cipher modes

What Are Block Cipher Modes?

Block ciphers encrypt data in **fixed-size blocks** (e.g., 64 or 128 bits). However, real-world data is often longer or shorter than a single block. **Block cipher modes of operation** define how to securely encrypt multi-block data and handle patterns, errors, and dependencies.

Common Block Cipher Modes

1. **ECB (Electronic Codebook Mode)**

- **Working**: Each block is encrypted **independently** using the same key.
- **Pros**: Simple, supports parallel encryption.
- **Cons**: Identical plaintext blocks → identical ciphertext blocks (pattern leakage).
- **Use Case**: Not recommended for sensitive data.

2. **CBC (Cipher Block Chaining Mode)**

- **Working**: Each plaintext block is XORed with the **previous ciphertext block** before encryption.
- **Requires**: Initialization Vector (IV) for the first block.

- **Pros**: Prevents pattern repetition.
- **Cons**: Sequential; one error affects the next block.
- **Use Case**: File encryption, secure messaging.

3. **CFB (Cipher Feedback Mode)**

- **Working**: Converts block cipher into a **self-synchronizing stream cipher**.
- **Encrypts**: IV or previous ciphertext, then XORs with plaintext.
- **Pros**: Can encrypt smaller units (e.g., bytes).
- **Cons**: Error propagation.
- **Use Case**: Real-time data encryption (e.g., voice, video).

4. **OFB (Output Feedback Mode)**

- **Working**: Similar to CFB, but feedback is taken from the **output of the cipher**, not the ciphertext.
- **Pros**: Errors don't propagate; good for noisy channels.
- **Cons**: Vulnerable if IV is reused.
- **Use Case**: Satellite or wireless communication.

5. **CTR (Counter Mode)**

- **Working**: Encrypts a **counter value** (incremented for each block), then XORs with plaintext.
- **Pros**: Fast, parallelizable, no chaining.
- **Cons**: Counter must never repeat.
- **Use Case**: High-performance encryption (e.g., disk encryption, VPNs).

Q3. [10 Marks] - Answers

a. State firewall design principles and its types with advantages.

Firewall Design Principles

Firewalls are security systems that **control incoming and outgoing network traffic** based on predefined rules. Effective firewall design follows these key principles:

Key Design Principles:

1. **All Traffic Must Pass Through the Firewall**
    - Ensures centralized control and monitoring.
    - Prevents unauthorized direct access to internal systems.

2. **Only Authorized Traffic Is Allowed**
    - Uses rule-based filtering to permit or deny traffic.
    - Based on IP addresses, ports, protocols, and application types.

3. **Firewall Itself Must Be Secure**
    - Hardened against attacks.
    - Runs on a trusted platform with minimal services exposed.

4. **Policy-Based Control**
    - Implements organizational security policies.
    - Supports role-based access and segmentation.

5. **Logging and Auditing**
    - Records traffic events for monitoring and forensic analysis.
    - Helps detect anomalies and policy violations.

Types of Firewalls and Their Advantages

Type	Description	Advantages
Packet-Filtering Firewall	Filters traffic based on IP, port, and protocol. Operates at **network layer**.	Simple, fast, low resource usage
Stateful Inspection Firewall	Tracks active connections and allows packets part of valid sessions.	More secure than packet filtering
Application-Level Firewall (Proxy)	Intercepts and inspects traffic at **application layer** (e.g., HTTP, FTP).	Deep inspection, hides internal network
Next-Generation Firewall (NGFW)	Combines traditional firewall with **IDS/IPS, deep packet inspection**, and app awareness.	Advanced threat protection, granular control
Hardware Firewall	Dedicated physical device placed at network perimeter.	High performance, centralized protection
Software Firewall	Installed on individual systems to protect host-level traffic.	Customizable, good for endpoint security

Q4. [10 Marks] - Answers

a. Explain Kerberos Protocol in detail.

What is Kerberos?

Kerberos is a secure network authentication protocol that uses **secret-key cryptography** and a **trusted third party** to authenticate users and services in a distributed environment. It was developed at MIT and is widely used in enterprise systems (e.g., Windows Active Directory).

Objectives of Kerberos

- **Mutual Authentication**: Both client and server verify each other's identity.

- **Single Sign-On (SSO)**: Users log in once to access multiple services.
- **Confidentiality & Integrity**: Protects data from eavesdropping and tampering.

Key Components

Component	Description
Client	The user or device requesting access.
Authentication Server (AS)	Verifies user credentials and issues a Ticket Granting Ticket (TGT).
Ticket Granting Server (TGS)	Issues service tickets based on the TGT.
Service Server (SS)	Hosts the requested service (e.g., file server, email).
Key Distribution Center (KDC)	Central authority combining AS and TGS.

Kerberos Authentication Workflow

Step 1: **User Login & TGT Request**

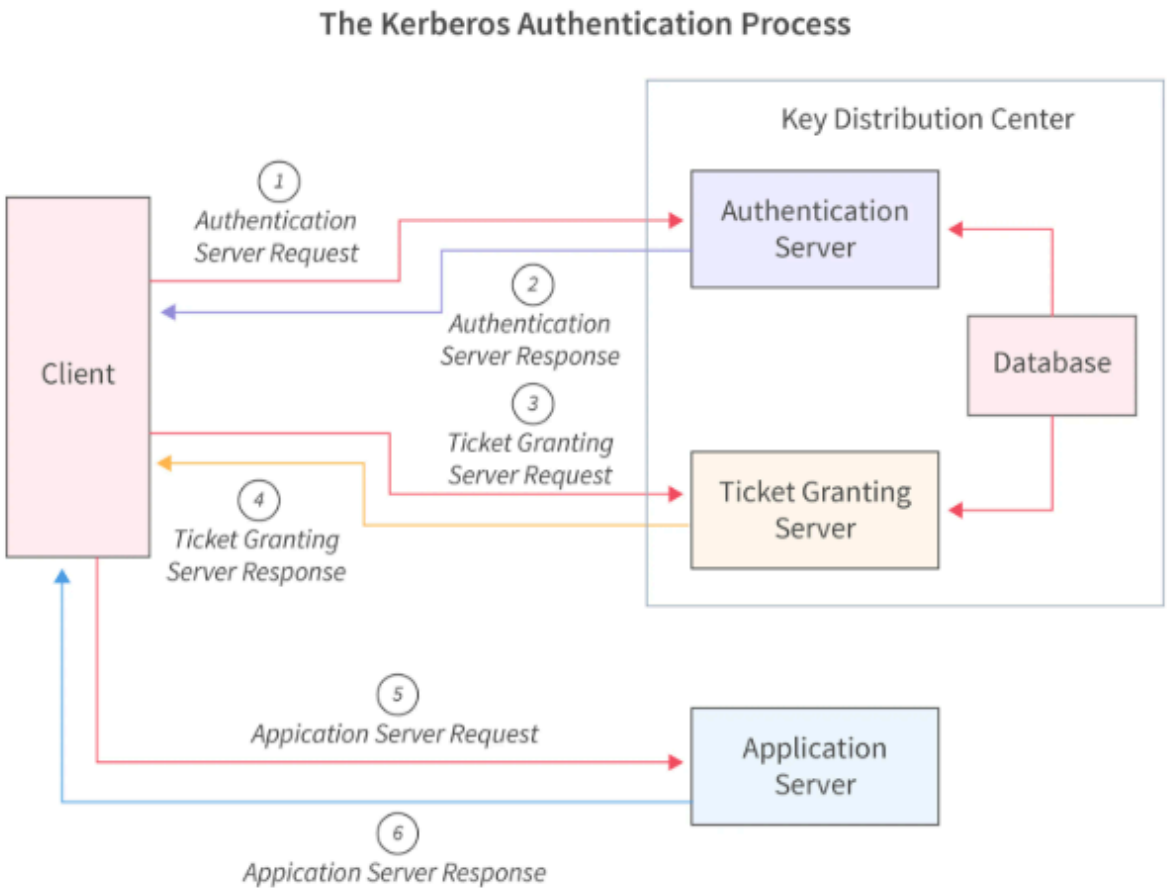
- Client sends a request to the **Authentication Server (AS)** with username.
- AS verifies credentials and sends back a **TGT** encrypted with the client's secret key (derived from password).

Step 2: **Service Ticket Request**

- Client sends the TGT to the **Ticket Granting Server (TGS)** along with the requested service name.
- TGS verifies the TGT and issues a **Service Ticket** encrypted with the service's secret key.

Step 3: **Accessing the Service**

- Client presents the **Service Ticket** to the **Service Server (SS)**.
- SS decrypts the ticket, verifies the client, and grants access.



Security Features

- **Timestamps and Nonces**: Prevent replay attacks.
- **Session Keys**: Temporary keys used for secure communication.
- **No Password Transmission**: Passwords are never sent over the network.

Example Scenario

Sameer logs into his university portal:

1. Kerberos authenticates him and issues a TGT.

2. He accesses the library system, email, and course portal — all using service tickets without re-entering his password.

Q.6 [10 Marks] - Answers

a. Define Malware. Explain at least five types with example.

What is Malware?

Malware (short for *malicious software*) refers to any program or code designed to **disrupt, damage, or gain unauthorized access** to computer systems, networks, or data. It poses serious threats to confidentiality, integrity, and availability of digital assets.

Types of Malware with Examples

1. **Virus**

- Attaches itself to legitimate files or programs and spreads when they are executed.
- Can corrupt files, slow down systems, or delete data.
- **Example**: *ILOVEYOU* virus (2000) spread via email and overwrote files.

2. **Worm**

- Self-replicating malware that spreads across networks without user action.
- Consumes bandwidth and system resources.
- **Example**: *Stuxnet* worm targeted industrial control systems.

3. **Trojan Horse**

- Disguises itself as a legitimate program but performs malicious actions once installed.
- Often used to create backdoors for attackers.
- **Example**: *Zeus Trojan* steals banking credentials.

4. **Ransomware**

- Encrypts user data and demands payment (ransom) for decryption.
- Disrupts business operations and causes financial loss.
- **Example**: *WannaCry* ransomware affected hospitals and companies worldwide.

5. **Spyware**

- Secretly monitors user activity and collects sensitive information.
- Can track keystrokes, browsing habits, and login credentials.
- **Example**: *CoolWebSearch* hijacked browsers and tracked user behavior.