Meghnad Saha Institute of Technology

Department of Computer Science and Engineering

and

allied (CSBS, CSE-AIML, CSE-DSc, CSE-IoT, CSE-CyS)

Technical Report

Name: SHADMAAN AHMAD

University Roll No : 14200121093

Department: CSE

Year: 4th **Semester:** 7th **Section :** B

Paper Name: CYBER SECURITY

Paper Code: PECCS702E

1. Discuss Security Architecture

Security Architecture refers to the overall structure of an organization's security system that protects its assets from potential threats. It consists of various layers, including hardware, software, policies, procedures, and controls. Security architecture focuses on ensuring the confidentiality, integrity, and availability (CIA) of information and systems.

Key components include:

- **Perimeter Security**: Technologies like firewalls and intrusion detection/prevention systems (IDS/IPS) that guard against external threats.
- **Access Control**: Ensuring only authorized individuals have access to sensitive data, typically managed through passwords, multi-factor authentication, and role-based access.
- **Data Security**: Encryption and other tools that ensure data is stored and transmitted securely.
- **Network Security**: Protects data as it moves across the organization's networks, often using VPNs, network segmentation, and encryption.
- **Incident Response**: Procedures for detecting, responding to, and recovering from security breaches.

A well-designed security architecture enables organizations to identify and mitigate risks effectively, ensuring long-term protection of sensitive information.

2. Difference Between Symmetric and Asymmetric Encryption

Encryption is the process of converting plaintext data into unreadable ciphertext to prevent unauthorized access. The two main types of encryption are **symmetric** and **asymmetric encryption**.

- **Symmetric Encryption**: This uses **one key** to lock (encrypt) and unlock (decrypt) the data. Both the sender and the receiver use the **same key**, so it’s faster but risky because the key has to be shared.
    - Example: It's like having one key for a house that both you and your friend have copies of. If someone else gets the key, they can enter too.
- **Asymmetric Encryption**: This uses **two keys**: a public key to lock (encrypt) and a private key to unlock (decrypt). The public key is shared with everyone, but the private key is kept secret. Only the person with the private key can unlock the data.
    - Example: It's like sending a locked box to someone, but only they have the key to open it, so no one else can read what's inside.

In short, symmetric is fast but less secure because of key sharing, while asymmetric is slower but more secure because no keys are shared.

3. Steps to Analyze Email Application's Security Vulnerabilities

Analyzing the security vulnerabilities of an email application requires a systematic approach to identify potential weaknesses that could be exploited by attackers. Below are the steps to perform a security analysis:

1. **Identify Entry Points**: Determine how data enters the application, such as user login, attachment uploads, or email message transmissions.
2. **Review Authentication Mechanisms**: Check if secure authentication protocols like multi-factor authentication (MFA) are enforced, and ensure passwords are stored securely (e.g., through hashing).

3. **Analyze Encryption**: Ensure that both emails at rest and in transit are encrypted using secure protocols like TLS or SSL.
4. **Test for Common Vulnerabilities**:
    - **Phishing**: Ensure that users are protected from phishing attacks.
    - **Cross-Site Scripting (XSS)**: Test whether email content can inject malicious scripts into the application.
    - **SQL Injection**: Ensure that user inputs are sanitized to prevent injection attacks.
5. **Check Email Attachments**: Analyze the mechanisms in place for scanning attachments for malware or viruses.
6. **Verify Access Controls**: Ensure that users can only access the emails and data they are authorized to, preventing unauthorized data leaks.
7. **Perform Penetration Testing**: Conduct simulated attacks on the email application to identify security flaws.
8. **Review Logging and Monitoring**: Ensure that logs are being kept for security events, and alerts are generated for unusual activity.

By following these steps, organizations can identify vulnerabilities and strengthen the security of their email applications.

4. Explain SSL Protocol

SSL (Secure Sockets Layer) is a cryptographic protocol that provides secure communication over the internet. It ensures that the data transmitted between two systems (typically a client and server) remains private and tamper-proof.

SSL operates by encrypting the data exchanged between the user's browser and the server, protecting sensitive information like passwords,

credit card details, and personal data from being intercepted by attackers. Here's how SSL works:

1. **Handshake**: When a user connects to an SSL-enabled website, the client (user's browser) and server perform a handshake. During this process, the server presents an SSL certificate, which contains the server's public key.
2. **Certificate Verification**: The client verifies the authenticity of the server's certificate. If it's valid, the client proceeds with the secure connection.
3. **Key Exchange**: After verification, the client and server agree on encryption methods and exchange session keys. These keys are used to encrypt and decrypt the data during the session.
4. **Secure Communication**: All data transmitted between the client and server is now encrypted, protecting it from eavesdropping or tampering.

SSL is widely used for securing websites, online transactions, and communications. It has evolved into **TLS (Transport Layer Security)**, the modern version of SSL.

5. Packet Filtering in Firewall (Simple Explanation)

Packet filtering is a basic function of a firewall that controls the flow of data packets between computers on a network. It decides whether to allow or block specific data packets based on predefined rules, such as IP addresses, port numbers, or protocols.

In simple terms:

- A **packet** is like a small package of data sent over the internet.
- **Packet filtering** checks these data packages before they enter or leave a network, allowing only trusted or authorized packets through, while blocking suspicious or unwanted ones.

Think of it like a security guard at a door who only allows people in if they meet certain criteria, such as having the right ID.