NAME:DIVYESH KHUNT SAPID:60009210116 BATCH:D12

Elliptic Curve Cryptography (ECC):

Elliptic Curve Cryptography is a branch of public key cryptography that leverages the mathematical properties of elliptic curves over finite fields. Key components include the elliptic curve equation, a base point on the curve, a public key generation algorithm, and a digital signature algorithm. ECC offers high security with shorter key lengths compared to traditional cryptographic systems, making it computationally efficient. The security advantage lies in the difficulty of the elliptic curve discrete logarithm problem, which forms the basis of its cryptographic strength. ECC finds practical applications in secure communication protocols like TLS and is crucial for securing data in various domains, including IoT devices and mobile communication.

2. **Hash Functions:**

Hash functions are fundamental in cryptography, ensuring data integrity and providing a secure means of storing passwords. Collision resistance ensures that it is computationally infeasible to find two different inputs producing the same hash value. Pre-image resistance guarantees that it is practically impossible to reverse the hash function to retrieve the original input. The avalanche effect dictates that a small change in the input should result in a significantly different output. These properties collectively contribute to the security of cryptographic applications by preventing unauthorized access, maintaining data integrity, and supporting digital signatures. Hash functions are widely used in blockchain, password storage, and message authentication codes.

3. Biometric Authentication System:

Biometric authentication combines unique biological or behavioral characteristics for identity verification. Fingerprint recognition, facial recognition, voice recognition, and iris scanning are common modalities. Fingerprint recognition provides a good balance between security and usability but can be susceptible to spoofing. Facial recognition offers user convenience but raises concerns about privacy and accuracy. Voice recognition is versatile but can be influenced by ambient noise. Iris scanning is highly secure, but the technology can be expensive and intrusive. Combining these modalities can enhance security, creating multi-modal biometric systems. The strength of biometric authentication lies in its ability to provide a unique identifier, but concerns exist regarding privacy, potential data breaches, and the irrevocable nature of biometric information. Evaluating the strengths and weaknesses of each modality is crucial for designing effective and user-friendly authentication systems.

4. X.509 Digital Certificate:

The X.509 digital certificate is a standardized format defining the structure and components of public key certificates. Its components include the version, serial number, signature algorithm, issuer and subject information, validity period, public key, and digital signature. X.509 certificates play a crucial role in establishing trust in online communication by binding a public key to an entity and allowing others to verify its authenticity. In the context of Public Key Infrastructure (PKI), X.509 certificates facilitate secure communication by enabling the distribution and verification of public keys. Certificate Authorities (CAs) issue these certificates, adding a layer of trust to the system. The hierarchical structure of CAs and the use of digital signatures help ensure the integrity and authenticity of the certificates, forming the foundation of secure online transactions.

5. Security Threat Analysis:

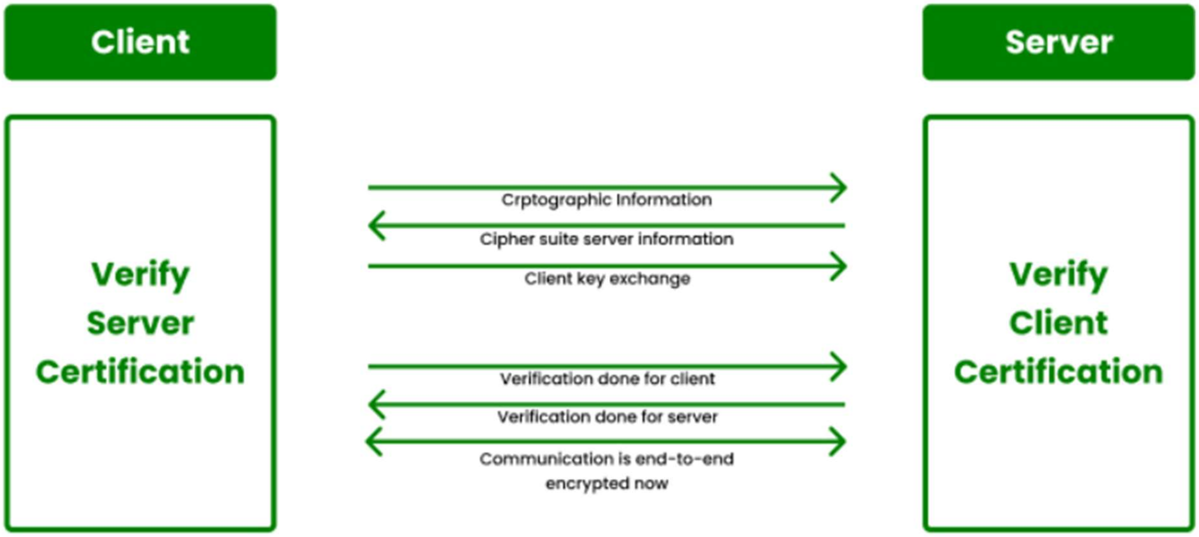
a) Cross-Site Scripting (XSS): XSS involves injecting malicious scripts into web pages viewed by other users. This can lead to the theft of sensitive information, session hijacking, and defacement of websites. Mitigation strategies include input validation, output encoding, and implementing Content Security Policy (CSP).

b) Spoofing Attacks: Spoofing attacks involve presenting false information to gain unauthorized access. IP spoofing masks the source IP address, while email spoofing falsifies the sender's address. Detection techniques include network monitoring, anomaly detection, and email authentication protocols. Real-world examples include the infamous "Man-in-the-Middle" attacks.

c) Phishing Attacks: Phishing relies on social engineering to deceive individuals into revealing sensitive information. Tactics include email and website impersonation. Countermeasures involve user education, email filtering, and multi-factor authentication. Understanding the psychological aspects of victim manipulation is crucial for effective prevention.

6. SSL Handshake Protocol:

The SSL handshake protocol is vital for establishing a secure connection between a client and a server during online communication. Steps include negotiation of cryptographic algorithms, key exchange, and authentication using digital certificates. The handshake employs asymmetric and symmetric encryption to ensure confidentiality, integrity, and authenticity. The use of certificates verifies the identity of the parties involved. SSL/TLS provides a secure foundation for web communication, ensuring that sensitive information remains protected from eavesdropping and tampering during transmission. The SSL handshake is a crucial aspect of this process, laying the groundwork for secure and encrypted data exchange.


Client
Server
Verify
Server
Certification
Crptographic Information
Cipher suite server information
Client key exchange
Verification done for client
Verification done for server
Communication is end-to-end
encrypted now
Verify
Client
Certification