**CCS354 NETWORK SECURITY**

**PART C**

**UNIT-I INTRODUCTION**

**1. Explain the conventional encryption model with suitable algorithms.**

**Answer:**

Conventional (symmetric) encryption uses a **single key** for both encryption and decryption. It is one of the oldest and fastest cryptographic methods.

**✨ Components of Conventional Encryption Model:**

* **Plaintext** – The original message.
* **Encryption algorithm** – Converts plaintext to ciphertext.
* **Secret key** – Shared between sender and receiver.
* **Ciphertext** – The encrypted message.
* **Decryption algorithm** – Converts ciphertext back to plaintext.

**🔐 Process:**

1. Sender encrypts the plaintext using the encryption algorithm and the shared key.
2. Ciphertext is transmitted over the channel.
3. Receiver decrypts it using the same shared key.

**✨ Examples of Conventional Encryption Algorithms:**

**🔸 Caesar Cipher:**

* Shifts letters by a fixed number.
* Example: HELLO → KHOOR (Shift by 3)

**🔸 DES (Data Encryption Standard):**

* Block cipher using 64-bit block and 56-bit key.
* 16 rounds of Feistel structure.

**AES (Advanced Encryption Standard):**

* Block cipher using 128-bit blocks with 128/192/256-bit keys.
* Consists of 10, 12, or 14 rounds.

**✅ Advantages:**

* High speed.
* Suitable for bulk data encryption.

**❌ Disadvantages:**

* Key distribution problem.
* Lack of scalability for large user networks.

**2. Describe the process and importance of digital signatures. Explain how they ensure message integrity and authenticity.**

**Answer:**

Digital signatures use **asymmetric cryptography** to provide **authentication**, **data integrity**, and **non-repudiation**.

**✨ Process of Digital Signature:**

**📤 Sender:**

1. Compute **hash** of the message using SHA-256.
2. Encrypt the hash with **sender’s private key** – this is the **digital signature**.
3. Attach the signature to the original message and send.

**📥 Receiver:**

1. Decrypt the signature using **sender’s public key**.
2. Compute hash of the received message.
3. Compare both hashes:
   * If they match: Message is authentic and untampered.
   * If not: Message was altered or the sender is not genuine.

**✨ Features:**

* **Authentication:** Only sender’s private key could’ve created the signature.
* **Integrity:** Even a single bit change in the message changes the hash.
* **Non-repudiation:** Sender cannot deny sending the message.

**✨ Applications:**

* Secure software distribution.
* Digital certificates.
* E-governance, legal documents.

**3. Discuss the role of hash functions in network security. Compare different hash algorithms.**

**Answer:**

Hash functions are **mathematical algorithms** that convert input data into a **fixed-length hash value (digest)**.

**✨ Properties of Hash Functions:**

* **Deterministic** – Same input always produces the same output.
* **Irreversible** – Cannot retrieve original input from hash.
* **Collision-resistant** – Difficult to find two inputs with same hash.
* **Fast computation** – Efficiently computed.

**Role in Network Security:**

* **Data integrity check**
* **Digital signatures**
* **Message authentication codes (HMAC)**
* **Password hashing**

**Comparison of Hash Algorithms:**

| **Algorithm** | **Output Size** | **Vulnerabilities** | **Use Case** |
| --- | --- | --- | --- |
| MD5 | 128 bits | Weak (collisions) | Legacy |
| SHA-1 | 160 bits | Broken (collisions) | Legacy |
| SHA-256 | 256 bits | Secure | Modern cryptography |
| SHA-3 | Variable | Secure | Future-ready applications |

**Example:**

If message M1 = "Hello" and M2 = "hello", their hashes are completely different due to the **avalanche effect**.

**UNIT II – KEY MANAGEMENT AND AUTHENTICATION**

**1. Explain the various techniques for the distribution of public keys.**

**Answer:**

The **distribution of public keys** is essential for secure communication in public-key cryptography. If the key is tampered with during distribution, attackers can impersonate users.

**Public Key Distribution Techniques:**

**🔸 1. Public Announcement:**

* Users publish their public keys.
* Vulnerable to **man-in-the-middle attacks**.

**Example:** Alice publishes her key online, but Eve replaces it with her own.

**🔸 2. Publicly Available Directory:**

* Maintained by a **trusted directory authority**.
* Users can access it anytime.
* Requires **secure communication** with the directory.

**🔸 3. Public Key Authority (PKA):**

* Centralized server responsible for key distribution.
* Follows **authentication protocols**.

**Steps:**

1. Alice requests Bob's public key from PKA.
2. PKA authenticates Alice and provides Bob’s key securely.

**🔸 4. Public Key Certificates (X.509):**

* Public key is bound to user identity and digitally signed by a **Certificate Authority (CA)**.
* Cannot be altered without detection.

**Certificate contains:**

* User ID
* Public key
* CA’s digital signature
* Expiry date

**✅ Advantages of X.509 Certificates:**

* Tamper-proof
* Widely accepted
* Foundation of **Public Key Infrastructure (PKI)**

**2. Explain the working of Kerberos authentication system with a neat diagram.**

**Answer:**

**Kerberos** is a centralized authentication protocol that uses **symmetric key cryptography** and a **trusted third party** (Key Distribution Center).

**✨ Components:**

* **Client (User)**
* **Server (Service provider)**
* **Key Distribution Center (KDC):**
  + **Authentication Server (AS)**
  + **Ticket Granting Server (TGS)**

**🔄 Working Steps:**

1. **Login Request:**
   * Client sends username to AS.
2. **Authentication Reply:**
   * AS verifies and sends:
     + Ticket Granting Ticket (TGT) encrypted with TGS key.
     + Session key encrypted with user’s password.
3. **Service Ticket Request:**
   * Client uses TGT to request access from TGS.
4. **Service Ticket Reply:**
   * TGS sends a service ticket encrypted with server’s key.
5. **Access Service:**
   * Client sends service ticket to server.
   * Server authenticates and grants access.

**✅ Advantages:**

* Prevents password transmission.
* Single sign-on.
* Mutual authentication.

**🔹 3. Explain the principles of remote user authentication using symmetric and asymmetric encryption.**

**Answer:**

Remote user authentication is used when the user and system are connected over an **untrusted network**. Encryption ensures security.

**🔐 Symmetric Encryption-Based Authentication:**

**🔸 1. Challenge-Response Protocol:**

* Server sends random number (nonce).
* Client encrypts it with shared key and sends back.

**🔸 2. Timestamp Method:**

* Client includes timestamp in encrypted message.
* Server verifies timestamp is recent.

**✅ Advantages:**

* Fast
* Less computational load

**❌ Disadvantages:**

* Key distribution is difficult.
* Replay attacks if timestamps are misused.

**🔐 Asymmetric Encryption-Based Authentication:**

**🔸 1. Digital Signature Method:**

* Server sends challenge.
* Client signs with private key.
* Server verifies with public key.

**🔸 2. Certificate-Based:**

* Clients present **X.509 certificates**.
* Server validates certificate with **CA’s public key**.

**✅ Advantages:**

* No shared key needed
* Scalable for large systems

**❌ Disadvantages:**

* Computationally intensive
* Certificate management required

**UNIT III – ACCESS CONTROL AND SECURITY**

**1. Explain the IP Security architecture and the role of IKE in detail.**

**Answer:**

**IPSec** is a protocol suite for securing **IP communications** by authenticating and encrypting each IP packet.

**IPsec Architecture:**

* **Security Association (SA):** One-way relationship between sender and receiver.
* **AH (Authentication Header):** Provides data integrity and authentication.
* **ESP (Encapsulating Security Payload):** Provides confidentiality, integrity, and authentication.

**Modes of Operation:**

* **Transport Mode:** Protects only the payload.
* **Tunnel Mode:** Protects entire IP packet (used in VPNs).

**Internet Key Exchange (IKE):**

IKE establishes **shared keys** and negotiates SA between hosts.

**✨ IKE Phases:**

**Phase 1:**

* Authenticates peers and establishes **ISAKMP SA**.
* Uses main or aggressive mode.

**Phase 2:**

* Negotiates SAs for AH/ESP.
* Creates **IPsec SAs** for data transfer.

**Advantages of IPSec:**

* Works at network layer
* Transparent to applications
* Provides strong security

**2. Explain Secure Socket Layer (SSL) protocol architecture and its working.**

**Answer:**

**SSL** is a cryptographic protocol for **secure communication over the internet**. It has now been succeeded by **TLS**, but many systems still refer to it as SSL.

**SSL Architecture Layers:**

1. **Handshake Protocol**
2. **Change Cipher Spec Protocol**
3. **Alert Protocol**
4. **Record Protocol**

**SSL Handshake Process:**

1. **ClientHello:** Sends protocol version, random number, and cipher suite.
2. **ServerHello:** Server responds with chosen cipher and certificate.
3. **Key Exchange:** Client validates certificate and sends session key encrypted with server’s public key.
4. **Finished:** Both sides exchange “Finished” messages to confirm setup.

**✨ Features:**

* **Authentication:** Using certificates
* **Confidentiality:** Encryption
* **Integrity:** Message Authentication Codes (MAC)

**✅ Applications:**

* E-commerce
* Banking sites (HTTPS)
* Email services

**3. Describe the architecture and functioning of IEEE 802.1X and EAP.**

**Answer:**

**IEEE 802.1X** is a port-based network access control protocol used for **wired and wireless networks**.

**Components:**

* **Supplicant:** End user device
* **Authenticator:** Network switch/AP
* **Authentication Server:** Typically RADIUS

**Working:**

1. Supplicant requests access.
2. Authenticator blocks traffic except 802.1X frames.
3. Supplicant sends **EAPOL** (EAP over LAN) request.
4. Authenticator forwards it to the RADIUS server.
5. Server authenticates and sends response.
6. If successful, the port is **unblocked** and traffic allowed.

**EAP (Extensible Authentication Protocol):**

* Framework that supports multiple authentication mechanisms:
  + EAP-TLS (certificate-based)
  + EAP-MSCHAPv2 (password-based)
  + EAP-TTLS, PEAP

**✅ Benefits:**

* Strong authentication
* Centralized access control
* Compatible with VLANs and wireless

**UNIT IV – APPLICATION LAYER SECURITY**

**1. Explain the architecture and functioning of S/MIME. How does it provide email security?**

**Answer:**

S/MIME (**Secure/Multipurpose Internet Mail Extensions**) is a widely used standard for **secure email communication**.

**✨ Features:**

* **Confidentiality** – Encrypts email content.
* **Authentication** – Verifies sender identity.
* **Integrity** – Ensures message is unaltered.
* **Non-repudiation** – Uses digital signatures.

**✨ Architecture:**

* **Uses X.509 certificates** for public key exchange.
* Built on MIME (Multipurpose Internet Mail Extensions).
* Compatible with email clients like Outlook, Thunderbird.

**Working of S/MIME:**

**Sender:**

1. Hash the message.
2. Sign the hash with sender’s private key (digital signature).
3. Encrypt message using random session key.
4. Encrypt session key with receiver’s public key.
5. Attach both to email and send.

**Receiver:**

1. Decrypt session key using private key.
2. Use session key to decrypt message.
3. Verify signature using sender’s public key.

**✅ Advantages:**

* Seamless integration with existing email systems.
* Based on strong cryptographic standards.
* Ensures secure corporate communication.

**2. Describe the operation of Pretty Good Privacy (PGP). Compare it with S/MIME.**

**Answer:**

PGP provides **privacy and authentication** for email and files. It uses a combination of **symmetric and asymmetric cryptography**.

**✨ Components:**

* **Message encryption** using a symmetric key.
* **Key encryption** using receiver’s public key.
* **Digital signature** using sender’s private key.

**Working of PGP:**

1. Message is compressed.
2. Encrypted with a symmetric session key.
3. Session key is encrypted with recipient’s public key.
4. Message is signed using sender’s private key.
5. Sent to the receiver.

**PGP vs S/MIME:**

| **Feature** | **PGP** | **S/MIME** |
| --- | --- | --- |
| Trust Model | Web of trust | PKI-based (hierarchical) |
| Certificate | User-generated | X.509 certificates |
| Control | User-controlled | Organization-controlled |
| Compatibility | Requires plugins | Built into email clients |

**✅ Conclusion:**

Both provide strong email security. **PGP is user-friendly**, **S/MIME is enterprise-friendly**.

**3. What are the security issues in mobile devices? Explain mobile device security mechanisms.**

**Answer:**

**Security Issues:**

* **Device theft/loss**
* **Malware from untrusted apps**
* **Unsecured Wi-Fi**
* **Data leakage via cloud apps**
* **Jailbreaking/rooting risks**

**Security Mechanisms:**

**Device-Level Security:**

* Screen locks (PIN, biometrics)
* Encryption of internal storage
* Secure boot & Trusted Execution Environment (TEE)

**App-Level Security:**

* App sandboxing
* Permission controls
* App reputation services

**Network-Level Security:**

* VPN for secure communication
* Use of SSL/TLS for data transfer

**Management:**

* Mobile Device Management (MDM)
* Remote wipe and lock
* Enforced security policies

**✅ Best Practices:**

* Avoid jailbreaking
* Install apps only from trusted sources
* Regular software updates

**✅ UNIT V – SECURITY PRACTICES**

**1. Explain the types and characteristics of firewalls.**

**Answer:**

A **firewall** controls incoming/outgoing traffic based on predefined rules to protect networks.

**Types of Firewalls:**

| **Type** | **Description** |
| --- | --- |
| Packet-filtering | Filters packets by IP, port |
| Stateful inspection | Monitors connection state |
| Proxy firewall | Acts as intermediary |
| NGFW | Includes DPI, threat detection |

**✨ Characteristics:**

* Packet inspection
* Access control policies
* NAT and VPN support
* Logging and alerting
* Scalability

**✅ Benefits:**

* Blocks unauthorized access
* Prevents data leakage
* Enforces security policies

**2. Describe the working and types of Intrusion Detection Systems (IDS). How are they useful in network security?**

**Answer:**

IDS monitors network traffic or system activities for suspicious behavior.

**Types of IDS:**

1. **NIDS (Network-based IDS):**
   * Monitors traffic on a network.
   * Placed at network borders.
2. **HIDS (Host-based IDS):**
   * Runs on individual hosts.
   * Monitors logs, file changes.

**✨ Detection Methods:**

* **Signature-based:** Matches known patterns.
* **Anomaly-based:** Detects abnormal behavior using machine learning/statistics.

**⚙️ Components:**

* **Sensors:** Collect data
* **Analyzers:** Analyze data
* **Dashboard/Console:** For alerts

**✅ Importance:**

* Detects intrusions in real-time
* Alerts admins before damage
* Helps in forensic analysis

**3. Explain the design and configuration of firewalls in a network.**

**Answer:**

Firewall design is crucial for **securing network architecture**.

**Firewall Locations:**

* **Perimeter firewall:** Between internet and internal network.
* **DMZ firewall:** Isolates public servers from internal network.
* **Internal firewall:** Controls internal traffic.

**Firewall Configurations:**

* **Default-deny:** All traffic blocked unless explicitly allowed.
* **Default-allow:** All traffic allowed unless blocked.
* **Rules-based:** Allows/denies traffic based on IP, port, protocol.

**✨ Design Considerations:**

* Network size and structure
* Type of data and applications
* Threat landscape

**✅ Best Practices:**

* Use layered firewalls (perimeter + internal)
* Regular rule auditing
* Enable logging and alerting
* Combine with IDS/IPS