**CCS354 NETWORK SECURITY**

**PART B**

**UNIT-I INTRODUCTION**

**1. Explain the basic principles of cryptography.**

**Answer:**

Cryptography ensures secure communication. Its basic principles include:

* **Confidentiality** – Only authorized users can access information.
* **Integrity** – Ensures information is not altered during transmission.
* **Authentication** – Verifies sender/receiver identity.
* **Non-repudiation** – Sender cannot deny sending a message.

**Key Terminologies:**

* **Plaintext** – Original message.
* **Ciphertext** – Encrypted message.
* **Encryption** – Converting plaintext to ciphertext.
* **Decryption** – Converting ciphertext back to plaintext.
* **Key** – A secret value used in encryption/decryption.

**Types of Cryptography:**

* **Symmetric** – Same key for encryption and decryption.
* **Asymmetric** – Public and private key pair.
* **Hash Functions** – One-way functions for integrity.

**2. Differentiate between symmetric and asymmetric cryptography with examples.**

**Answer:**

| **Feature** | **Symmetric Cryptography** | **Asymmetric Cryptography** |
| --- | --- | --- |
| Keys Used | Single key (same for encryption/decryption) | Public and private key pair |
| Speed | Faster | Slower |
| Example Algorithms | AES, DES | RSA, ECC |
| Key Distribution | Problematic | Easier via public key |
| Use Cases | Bulk data encryption | Digital signatures, key exchange |

**Example:**

* **Symmetric:**  
  Alice and Bob share a secret key. Alice encrypts the message using the key, Bob decrypts using the same key.
* **Asymmetric:**  
  Alice uses Bob's **public key** to encrypt a message. Only Bob can decrypt using his **private key**.

**3. Explain the working and importance of hash functions in network security.**

**Answer:**

Hash functions convert arbitrary input data into a fixed-size hash value (digest).

**Properties:**

* Deterministic
* Irreversible (one-way)
* Collision-resistant
* Fast computation

**Common Algorithms:**  
MD5, SHA-1, SHA-256

**Applications:**

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

**Example:**  
If message M changes, hash H(M) changes drastically, helping detect tampering.

**4. Describe the process of digital signature generation and verification.**

**Answer:**

A **digital signature** ensures authenticity, integrity, and non-repudiation.

**Steps:**

* **Sender Side:**
  1. Compute hash of the message.
  2. Encrypt the hash using sender's **private key**.
  3. Append signature to message and send.
* **Receiver Side:**
  1. Decrypt signature using sender's **public key**.
  2. Compute hash of received message.
  3. Compare both hashes — if same, message is valid.

**Applications:**  
E-Governance, SSL/TLS, Secure Email.

**5. Describe conventional encryption techniques with examples.**

**Answer:**

Conventional encryption (symmetric) includes:

* **Caesar Cipher:**  
  Shifts letters by a fixed value (e.g., A → D)
* **Transposition Cipher:**  
  Rearranges characters (e.g., columnar transposition)
* **DES (Data Encryption Standard):**  
  56-bit key, block cipher, now outdated.
* **AES (Advanced Encryption Standard):**  
  128/192/256-bit key, highly secure, used globally.

**Key Points:**

* Fast and efficient.
* Secure for closed environments.
* Key distribution is the biggest challenge.

**UNIT II – KEY MANAGEMENT AND AUTHENTICATION**

**1. Explain symmetric key distribution techniques.**

**Answer:**

Symmetric key distribution is crucial for secure communication. Key techniques include:

* **Manual Distribution:** Physically sharing keys, suitable for small networks.​
* **Key Distribution Center (KDC):** A trusted third party that distributes session keys.​
* **Diffie-Hellman Key Exchange:** Allows two parties to generate a shared secret over an insecure channel.​
* **Kerberos Protocol:** Uses a KDC to authenticate users and distribute session keys securely.​

Each method has its own advantages and challenges concerning scalability, security, and practicality.

**2. Describe the components and functioning of Public Key Infrastructure (PKI).**

**Answer:**

PKI enables secure electronic transfer of information. Key components:

* **Certificate Authority (CA):** Issues and verifies digital certificates.​
* **Registration Authority (RA):** Verifies user identities before certificates are issued.​
* **Digital Certificates:** Contain public keys and identity information, following X.509 standards.​
* **Certificate Revocation List (CRL):** Lists revoked certificates.​

Functioning:

1. User requests a certificate from RA.​
2. RA verifies identity and informs CA.​
3. CA issues a certificate, binding the user's identity to their public key.​
4. Users can now use these certificates for secure communications.​

**3. Explain the Kerberos authentication protocol.**

**Answer:**

Kerberos is a network authentication protocol using secret-key cryptography.

Components:

* **Authentication Server (AS):** Verifies user credentials.​
* **Ticket Granting Server (TGS):** Issues service tickets.​
* **Client and Server:** Entities participating in communication.​

Process:

1. Client requests authentication from AS.
2. AS verifies and provides a Ticket Granting Ticket (TGT).​
3. Client uses TGT to request service ticket from TGS.​
4. TGS issues service ticket.​
5. Client presents service ticket to the server to access services.​

**4. Discuss remote user authentication using asymmetric encryption.**

**Answer:**

Asymmetric encryption uses a pair of keys: public and private.

Process:

1. User sends authentication request.​
2. Server sends a challenge encrypted with user's public key.​
3. User decrypts challenge using private key and responds.​
4. Server verifies response, authenticating the user.​

This method ensures secure authentication over untrusted networks.

**5. What is the role of X.509 certificates in key management?**

**Answer:**

X.509 certificates bind a public key to an entity's identity.

Features:

* **Structure:** Includes subject name, public key, issuer, validity period, and digital signature.​
* **Verification:** Ensures the public key belongs to the entity.​
* **Trust Chain:** Certificates can be chained to a trusted root CA.​

They are essential for establishing trust in PKI systems.

**✅ UNIT III – ACCESS CONTROL AND SECURITY**

**1. Explain the Extensible Authentication Protocol (EAP).**

**Answer:**

EAP is a framework for network access authentication.

* **Flexibility:** Supports multiple authentication methods (e.g., EAP-TLS, EAP-TTLS).​
* **Process:**
  1. Client initiates connection.​
  2. Server requests authentication.​
  3. Client responds with credentials.​
  4. Server verifies and grants access.​

EAP is widely used in wireless networks and PPP connections.

**2. Describe IEEE 802.1X Port-Based Network Access Control.**

**Answer:**

IEEE 802.1X provides an authentication mechanism for devices wishing to connect to a LAN or WLAN.

Components:

* **Supplicant:** Client device requesting access.​[Studocu+1YouTube+1](https://www.studocu.com/in/document/anna-university/network-security/ccs354-ns-viva-qus-please-make-use-of-it/101794736?utm_source=chatgpt.com)
* **Authenticator:** Network device (e.g., switch) controlling access.​
* **Authentication Server:** Validates credentials (e.g., RADIUS server).​

Process:

1. Supplicant requests access.​
2. Authenticator forwards request to Authentication Server.​
3. Authentication Server verifies and informs Authenticator.​
4. Access is granted or denied based on verification.​

**3. Explain the Internet Key Exchange (IKE) protocol.**

**Answer:**

IKE is used to set up a security association (SA) in the IPsec protocol suite.

Phases:

* **Phase 1:** Establishes IKE SA, authenticates peers, and sets up a secure channel.​
* **Phase 2:** Negotiates IPsec SAs for data transfer.​

Features:

* Supports various authentication methods (e.g., pre-shared keys, digital certificates).​
* Ensures confidentiality, integrity, and authentication.​

**4. Discuss the architecture and functioning of SSL/TLS protocols.**

**Answer:**

SSL/TLS protocols secure communications over networks.

* **Handshake Protocol:** Establishes a secure session using asymmetric encryption.​
* **Record Protocol:** Manages data encryption and integrity using symmetric encryption.​

Process:

1. Client and server exchange hello messages.​
2. Server sends certificate.

**5. Explain the characteristics and basing strategies of firewalls.**

**Answer:**

**Characteristics:**

* Packet inspection
* Logging
* Authentication support
* Policy enforcement
* Stateful tracking

**Basing Strategies:**

* **Hardware-based firewall:** Dedicated device.
* **Software firewall:** Installed on general-purpose OS.
* **Cloud-based firewall:** Offered as a service.

**Trade-offs:**

* Hardware: High performance, expensive
* Software: Cost-effective, flexible
* Cloud: Scalable, third-party managed

**UNIT IV – APPLICATION LAYER SECURITY**

**1. Explain the working of Pretty Good Privacy (PGP) in securing emails.**

**Answer:**

PGP secures emails using both **symmetric** and **asymmetric** cryptography.

**Steps:**

* **Encryption:**
  1. Message is encrypted with a random symmetric key.
  2. Symmetric key is encrypted with recipient's public key.
  3. Encrypted message and key are sent.
* **Decryption:**
  1. Receiver uses private key to decrypt symmetric key.
  2. Uses symmetric key to decrypt message.

**Features:**

* Confidentiality
* Digital signatures
* Compression
* Email compatibility

**Advantages:**  
High security, widespread use, user-level control.

**2. Explain S/MIME architecture and its role in secure communication.**

**Answer:**

S/MIME (Secure/Multipurpose Internet Mail Extensions) is used for securing email via:

* **Digital signatures** – for authentication and integrity.
* **Encryption** – for confidentiality.

**Working:**

* Sender signs and encrypts the message.
* Uses X.509 certificates for public key distribution.
* Recipient uses their private key to decrypt and verify.

**Benefits:**

* Standardized
* Works with major email clients
* Secure attachments

**3. What is DomainKeys Identified Mail (DKIM)? How does it work?**

**Answer:**

DKIM prevents **email spoofing** by adding a **digital signature** to outgoing emails.

**Working:**

1. Email server signs header with private key.
2. Publishes public key via DNS record.
3. Recipient server fetches public key and verifies signature.

**Benefits:**

* Authenticates sender domain
* Enhances email security
* Works with DMARC and SPF

**4. Explain mobile device security challenges and protection methods.**

**Answer:**

**Challenges:**

* Device theft
* Insecure apps
* Untrusted Wi-Fi
* Data leakage

**Protection Methods:**

* **Device encryption**
* **Remote wipe**
* **Biometric locks**
* **App sandboxing**
* **VPN usage**
* **Regular updates**

**Best Practices:**  
Use strong passwords, disable unnecessary services, monitor app permissions.

**5. Differentiate PGP and S/MIME.**

| **Feature** | **PGP** | **S/MIME** |
| --- | --- | --- |
| Certificates | Uses web of trust | Uses X.509 CA |
| Encryption | Manual key exchange | PKI-based key exchange |
| Email Client Support | Plug-ins needed | Native support in many clients |
| Flexibility | High user control | Centralized control |

**Conclusion:**  
Both provide robust email security; S/MIME is enterprise-friendly, while PGP is user-driven.

**UNIT V – SECURITY PRACTICES**

**1. Describe the different types of firewalls with examples.**

**Answer:**

**1. Packet-filtering firewall:**  
Filters based on IP, port, protocol.  
Example: Cisco ACL.

**2. Stateful inspection firewall:**  
Monitors connection states.  
Example: Checkpoint.

**3. Proxy firewall:**  
Acts as an intermediary.  
Example: Squid proxy.

**4. Next-generation firewall (NGFW):**  
Includes DPI, malware detection.  
Example: Palo Alto Networks.

**Conclusion:**  
Each firewall offers different levels of protection; combination ensures layered security.

**2. Explain Intrusion Detection Systems (IDS). What are its types?**

**Answer:**

IDS monitors network/system for malicious activity.

**Types:**

* **Network IDS (NIDS):** Monitors network traffic.
* **Host IDS (HIDS):** Monitors individual devices.

**Detection Methods:**

* **Signature-based:** Matches known attack patterns.
* **Anomaly-based:** Detects unusual behavior.

**Components:**

* Sensors
* Analyzers
* Management console

**Example Tools:** Snort, OSSEC

**3. Discuss password management techniques for enhancing security.**

**Answer:**

**Techniques:**

* **Strong password policy:** Minimum length, special characters.
* **Password hashing:** Use bcrypt or PBKDF2.
* **Salting:** Add random data to passwords before hashing.
* **Two-Factor Authentication (2FA):** Adds extra layer of security.
* **Password vaults:** Secure password storage.

**Best Practices:**

* Avoid reuse
* Update regularly
* Monitor login attempts

**4. List and explain firewall configurations and locations in a network.**

**Answer:**

**Firewall Locations:**

* **Perimeter firewall:** Between external and internal network.
* **DMZ firewall:** Between public servers and internal systems.
* **Internal segmentation firewall:** Controls internal traffic.

**Configurations:**

* **Default-deny:** Blocks all unless allowed.
* **Default-allow:** Allows all unless blocked.
* **NAT:** Hides internal IPs.
* **VPN passthrough:** Allows encrypted traffic.

**Conclusion:**  
Proper location and configuration enhance defense.

**5. Explain the characteristics and basing strategies of firewalls.**

**Answer:**

**Characteristics:**

* Packet inspection
* Logging
* Authentication support
* Policy enforcement
* Stateful tracking

**Basing Strategies:**

* **Hardware-based firewall:** Dedicated device.
* **Software firewall:** Installed on general-purpose OS.
* **Cloud-based firewall:** Offered as a service.

**Trade-offs:**

* Hardware: High performance, expensive
* Software: Cost-effective, flexible
* Cloud: Scalable, third-party managed

Let me know if you need **16-mark questions**, **diagrams**, or **PDF versions** of these!

Bottom of Form