# **57. Wireless Security**

## **Introduction to Wireless Network Security**

* Security is essential in all networks, but it is even more critical in wireless networks.
* Wireless signals are not confined within a wire, meaning any device within range can receive traffic.
* In wired networks, traffic is often only encrypted when sent over an untrusted network such as the internet.
* In wireless networks, encrypting traffic between wireless clients and the access point (AP) is crucial.
* The three main concepts in wireless security:
  + **Authentication**
  + **Encryption**
  + **Integrity**

## **Authentication**

* All clients must be authenticated before associating with an AP.
* In corporate settings, only trusted users/devices should have network access.
  + A separate SSID can be provided for guest users without corporate network access.
* Clients should authenticate the AP to avoid connecting to a malicious AP.
* Authentication methods include:
  + Password
  + Username/Password
  + Certificates

## **Encryption**

* Traffic between clients and APs must be encrypted to prevent unauthorized access.
* All devices on a WLAN use the same encryption protocol, but each client has a unique encryption/decryption key.
* A **Group Key** is used by the AP to encrypt traffic intended for all connected clients.
  + Clients associated with the AP retain this key to decrypt broadcast traffic.

## 

## **Integrity**

* Integrity ensures that messages are not modified by third parties.
* The message sent by the source host should be identical to the message received by the destination host.
* A **Message Integrity Check (MIC)** is added to messages to ensure their integrity.

## **Authentication Methods**

### **1. Open Authentication**

* The client sends an authentication request, and the AP accepts it.
* This method is **not secure**.
* Additional authentication (e.g., captive portals like Starbucks Wi-Fi) may be required before network access is granted.

### **2. WEP (Wired Equivalent Privacy)**

* WEP provides both authentication and encryption.
* Uses **RC4 algorithm** for encryption.
* Requires shared-key authentication where both sender and receiver have the same key.
* WEP key lengths:
  + 40-bit or 104-bit key + 24-bit Initialization Vector (IV) → 64-bit or 128-bit total.
* **WEP is not secure and can be easily cracked.**

## **Extensible Authentication Protocol (EAP)**

* EAP is an authentication framework defining a standard set of authentication functions.
* Integrated with **802.1X**, which provides port-based network access control.
* **802.1X Components:**
  + **Supplicant**: The device requesting network access.
  + **Authenticator**: The device granting access.
  + **Authentication Server (AS)**: Verifies credentials and permits/denies access.

### **EAP Methods:**

#### **1. LEAP (Lightweight EAP)**

* Developed by Cisco as an improvement over WEP.
* Requires a **username and password** for authentication.
* **Mutual authentication** is achieved through challenge phrases between client and server.
* Uses **dynamic WEP keys** (frequently changed for security).
* **Not secure and should no longer be used.**

#### **2. EAP-FAST (EAP Flexible Authentication via Secure Tunneling)**

* Also developed by Cisco.
* Consists of three phases:
  1. **PAC (Protected Access Credential)** generation and transmission to the client.
  2. **Secure TLS tunnel** establishment.
  3. **Client authentication** within the encrypted TLS tunnel.

#### **3. PEAP (Protected EAP)**

* Establishes a **secure TLS tunnel** between the client and server.
* Uses a **server digital certificate** to authenticate the server.
* Additional client authentication occurs within the TLS tunnel.
* Example: MS-CHAP (Microsoft Challenge-Handshake Authentication Protocol).

#### **4. EAP-TLS (EAP Transport Layer Security)**

* Requires **certificates on both the authentication server and all client devices**.
* **Most secure wireless authentication method** but difficult to implement.
* Mutual authentication through digital certificates eliminates the need for additional authentication inside the TLS tunnel.

## **Encryption & Integrity Methods**

### **1. TKIP (Temporal Key Integrity Protocol)**

* Created as an interim security measure before a new standard was developed.
* Security features include:
  + **MIC (Message Integrity Check)** to protect message integrity.
  + **Key Mixing Algorithm** to create a unique WEP key per frame.
  + **Extended IV (48-bit instead of 24-bit)** to mitigate brute-force attacks.
  + **Sender MAC Address in MIC** to track frame sources.
  + **Timestamp in MIC** to prevent replay attacks.
  + **TKIP Sequence Number** to track transmitted frames.
* Used in **WPA version 1**.

### **2. CCMP (Counter/CBC-MAC Protocol)**

* More secure than TKIP.
* Used in **WPA2**.
* Requires hardware support.
* Uses two algorithms:
  + **AES Counter Mode Encryption** (most secure encryption method).
  + **CBC-MAC (Cipher Block Chaining Message Authentication Code)** for integrity.

### **3. GCMP (Galois/Counter Mode Protocol)**

* More secure and efficient than CCMP.
* Supports **higher data throughput**.
* Used in **WPA3**.
* Uses two algorithms:
  + **AES Counter Mode Encryption**.
  + **GMAC (Galois Message Authentication Code)** for integrity.

## **Wi-Fi Protected Access (WPA)**

* The **Wi-Fi Alliance** developed three WPA certifications:
  1. **WPA**
  2. **WPA2**
  3. **WPA3**
* Devices must pass testing in authorized labs to receive WPA certification.
* **Two authentication modes in WPA:**

