Wireless Security Protocols

**Assignment 2**

**20P-0005**

**Talha Hassan**

**Computer Network Lab**

**Introduction:**

Wireless security is a critical aspect of safeguarding data on Wi-Fi networks. With the proliferation of wireless connectivity, the need to protect sensitive information from unauthorized access and potential cyber threats has become increasingly vital. Ensuring robust wireless security is essential for maintaining the privacy and integrity of data transmitted over Wi-Fi networks.

**Basic Concepts**

Wireless security revolves around fundamental principles that include:

**Encryption**:The process of encoding data to prevent unauthorized access. In wireless networks, encryption ensures that only authorized parties can decipher the transmitted information.

**Authentication:** The verification of the identity of users or devices trying to connect to a Wi-Fi network. This prevents unauthorized access and ensures that only legitimate users gain entry.

**Access Control:** Managing and restricting access to the Wi-Fi network based on user credentials or other authentication methods, preventing unauthorized users from connecting.

**Types of Security Protocols**

**1: WEP (Wired Equivalent Privacy)**

One of the earliest wireless security protocols.

**Pros:**

Easy to set up.

Compatible with older devices.

**Cons:**

Weak encryption, vulnerable to attacks.

Limited security compared to newer protocols.

**2: WPA (Wi-Fi Protected Access)**

Introduced as a replacement for WEP, providing enhanced security.

**Pros:**

Improved encryption compared to WEP.

Supports various authentication methods.

**Cons:**

Vulnerable to some attacks, especially WPA-PSK.

**3:WPA2 (Wi-Fi Protected Access 2)**

The successor to WPA, addressing its vulnerabilities.

**Pros:**

Stronger encryption.

Robust security features.

**Cons:**

Still susceptible to some attacks (e.g., brute force).

**4: WPA3 (Wi-Fi Protected Access 3)**

The latest standard in wireless security, providing enhanced protection.

**Pros:**

Improved encryption algorithms.

Enhanced protection against offline dictionary attacks.

**Cons:**

Limited adoption as of now.

Compare and Contrast

**Compare and Contrast**

**Encryption Strength:**

WEP: Weak.

WPA: Moderate.

WPA2: Strong.

WPA3: Very strong.

**Vulnerabilities:**

WEP: Highly vulnerable.

WPA: Vulnerable to some attacks.

WPA2: Relatively secure.

WPA3: Enhanced security.

**Real-Life Examples**

**Home Networks:**

WEP: Rarely used due to security concerns.

WPA2: Widely adopted for its balance of security and compatibility.

**Public Wi-Fi (Cafes):**

WPA3: Increasingly being implemented for improved security.

**Future Trends**

As technology advances, future trends in wireless security may include:

**AI-driven Security:** Integration of artificial intelligence for real-time threat detection and response.

**5G Security:** Enhancements in security protocols to align with the rollout of 5G networks.

**IoT Security**: Focus on securing the increasing number of Internet of Things (IoT) devices connected to Wi-Fi networks.