

**Computer Networks Assignment 2**



**Name: Muhammad Shaheer.**

**Roll No: 20p-0480**

NATIONAL UNIVERSTIY OF COMPUTER AND EMERGING SCIENCES, FAST- PESHAWAR CAMPUS Department of Computer Science & Software Engineering

Q1: Explain why security matters for Wi-Fi networks wireless.

**Introduction:**

In the contemporary digital era, Wi-Fi networks play a vital role in providing seamless internet access and facilitating device communication. However, this convenience comes with the inherent risk of unauthorized access and data breaches. Wireless security protocols are essential for safeguarding our data and preventing malicious actors from intercepting sensitive information. Wireless security is paramount in safeguarding data on Wi-Fi networks. As our reliance on Wi-Fi grows, understanding various wireless security protocols becomes crucial. This document delves into the significance of wireless security for Wi-Fi networks, highlighting its pivotal role in protecting sensitive data from potential threats and unauthorized access.

Best Practices for Wi-Fi Security

- Use Strong Passwords

- Enable Encryption (WPA2 or WPA3)

- Regularly Update Firmware

- Hide Your Network

- Implement Network Segmentation

- Monitor Network Activity

Q2: Describe the core ideas of wireless security in an easy-to understand way.

**Basic Concepts:**

Wireless security involves implementing measures to protect Wi-Fi networks from unauthorized access and data interception. Key concepts include encryption, authentication, and secure key management. Encryption ensures that data transmitted over the network is encoded and can only be decoded by authorized parties. Authentication involves validating the identity of devices attempting to connect to the Wi-Fi network. Secure key management ensures that cryptographic keys used for encryption and authentication is handled in a way that prevents unauthorized access. Wireless security is the prevention of unauthorized access or damage to computers or data using wireless networks, which include Wi-Fi networks. The term may also refer to the protection of the wireless network itself from adversaries seeking to damage the confidentiality, integrity, or availability of the network. The most common type is Wi-Fi security, which includes Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA). WEP is an old IEEE 802.11 standard from 1997.

* It is a notoriously weak security standard: the password it uses can often be cracked in a few minutes with a basic laptop computer and widely available software tools.
* WEP was superseded in 2003 by WPA, a quick alternative at the time to improve security over WEP. The current standard is WPA2;
* Some hardware cannot support WPA2 without firmware upgrade or replacement. WPA2 uses an encryption device that encrypts the network with a 256-bit key; the longer key length improves security over WEP. Enterprises often enforce security using a certificate-based system to authenticate the connecting device, following the standard 802.11X.

Q3: Introduce at least three common wireless security protocols like WEP, WPA, WPA2, or WPA3.

**Types of Security:**

Wireless networks implement various security protocols to safeguard data transmission and protect against unauthorized access. Here are three common wireless security protocols:

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

- Introduced in 1997, WEP was an early encryption standard.

- Considered insecure due to vulnerabilities that can be exploited.

The earliest wireless security protocol, WEP, is considered outdated and vulnerable to cracking. Its static encryption keys and weak algorithms make it easy for hackers to gain access to Wi-Fi networks

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

- Addressed WEP's weaknesses, introduced in 2003.

- Enhanced encryption methods, such as TKIP, to improve security.

An improvement over WEP, WPA introduced stronger encryption algorithms and dynamic key renewal to enhance security. However, it still had some limitations, paving the way for its successor, WPA2.

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

- Current widely used protocol.

- Utilizes the more secure AES algorithm for encryption.

Widely adopted in both personal and enterprise settings, WPA2 offers robust encryption and authentication mechanisms, making it the most secure and widely used wireless security protocol to date.

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

- The latest standard, introduced for enhanced security.

- Introduces stronger encryption, individualized data encryption, and protection against brute-force attacks.

The latest addition to the WPA family, WPA3 further enhances security by introducing new features like stronger encryption algorithms, perfect forward secrecy, and enhanced key negotiation.

Q4: Highlight the pros and cons of each security protocol in a straightforward manner.

**Compare and Contrast:**

|  |  |  |
| --- | --- | --- |
| **Protocol** | **Pros** | **Cons** |
| **WEP** | * Simple to set up * Widely supported by devices. * Legacy support for older hardware. | * Outdated and highly vulnerable to security breaches. * Uses a static encryption key, making it easier to crack * Weak encryption algorithms make it susceptible to attacks. |
| **WPA** | * More secure than WEP * Introduces stronger encryption methods like TKIP. * Dynamic key renewal enhances overall security. * Provides better protection against unauthorized access. | * Still has some security flaws * Older than WPA2, making it less secure than the latest standards. |
| **WPA2** | * Widely adopted in both personal and enterprise settings. * Offers robust encryption with the Advanced Encryption Standard (AES). * Provides strong authentication mechanisms. * Reliable and considered highly secure. | * May not be supported by older devices |
| **WPA3** | * Most secure and advanced protocol * The latest and most advanced wireless security protocol. * Introduces stronger encryption algorithms. * Individualized data encryption for improved privacy. * Protection against brute-force attacks is enhanced. | * Not as widely supported as WPA2 due to being a newer standard. * Adoption might require firmware updates for some devices. |

Q5: Share simple instances where these security protocols are used, like in homes or cafes.

**Real-Life Examples:**

**Homes:**

* **Wired Equivalent Privacy (WEP):** WEP might be found in older home routers or devices that lack support for newer protocols. Users with legacy devices may use WEP to secure their home Wi-Fi networks.
* **Wi-Fi Protected Access (WPA) or WPA2:** Most modern homes use WPA or WPA2 for enhanced security. PA or WPA2 is often the default security protocol for contemporary routers, providing better protection against unauthorized access.
* **Wi-Fi Protected Access 3 (WPA3):** Homes with the latest routers and devices may opt for WPA3 to benefit from its improved security features.WPA3 is becoming increasingly popular as more devices support this advanced protocol.

**Cafes:**

* **Wi-Fi Protected Access (WPA) or WPA2:** Many cafes use WPA or WPA2 to secure their public Wi-Fi networks. This ensures that customers can connect securely, protecting their data from potential threats.
* **Wi-Fi Protected Access 3 (WPA3):**Cafes aiming for advanced security might choose WPA3, especially in regions with increased awareness of the latest protocols.WPA3 provides an extra layer of protection for customers using the Wi-Fi network.

Q6: Mention any new developments in wireless security, but keep it simple.

**Future Trends:**

As technology continues to evolve, so will the wireless standards that power our devices. Industry experts predict that 5G will continue to dominate the landscape for the foreseeable future. The rollout of 5G networks worldwide is expected to reach 55% coverage by 2025, providing lightning-fast speeds and unlocking new possibilities for businesses and consumers alike.

Further advancements in wireless standards may also include:

* **Quantum-Resistant Encryption:**
  + Ongoing research aims to develop encryption methods resistant to quantum computing threats.
  + Protects against advanced computational attacks on current encryption standards.
* **Advanced Authentication Methods:**
  + Emerging technologies explore biometrics and multi-factor authentication for enhanced security.
  + Integrating unique identifiers like fingerprints or facial recognition to authenticate devices.
* **AI-Powered Security Solutions:**
  + Implementation of artificial intelligence for real-time threat detection and adaptive security.
  + AI algorithms analyze network behavior to identify and mitigate potential risks.
* **Behavioral Analytics:**
  + Utilizing user behavior analysis to detect anomalies and potential intrusions.
  + Real-time monitoring to identify unusual patterns and protect against evolving threats.
* Enhanced security protocols to protect against cyber threats
* Increased network efficiency to accommodate more connected devices
* Lower power consumption for extended battery life

**References:**

* + https://utilitiesone.com/the-future-of-wireless-standards-predictions-and-speculations
  + https://en.wikipedia.org/wiki/Wireless\_security
  + https://www.techtarget.com/searchnetworking/feature/Wireless-encryption-basics-Understanding-WEP-WPA-and-WPA2
  + https://www.thepowermba.com/en/blog/why-is-security-important-in-your-wifi-network
  + https://www.quora.com/Why-is-it-important-to-use-secure-wireless-networks