

***Assignment 2***

***Muhammad Rafay***

***20P0018***

***Computer Networks***

***Sec A***

**Wireless Security Protocols: Safeguarding WiFi Networks**

1. **Introduction:**

Wireless security is crucial in today's digital world to protect private information communicated via WiFi networks. As more and more of our devices rely on wireless connectivity, safeguarding these networks is essential to preventing unauthorised access, data leaks, and other online threats.

1. **Basic Concepts:**

The basis of wireless security is the encryption of data delivered and received between devices and the WiFi router. Even if data is intercepted by unauthorized parties, encryption ensures that it cannot be decrypted without the correct key. Authentication methods give an additional layer of protection by verifying the authenticity of devices that are trying to connect to the network.

1. **Types of Security Protocols:**

**WEP (Wired Equivalent Privacy):**

Pros: Simple setup, widely supported.

Cons: Easily cracked, outdated, and lacks robust security features.

**WPA (WiFi Protected Access):**

Pros: Improved security over WEP, uses TKIP encryption.

Cons: Vulnerable to brute force attacks, considered less secure than WPA2.

**WPA2 (WiFi Protected Access 2):**

Pros: Stronger encryption (AES), enhanced security.

Cons: Vulnerable to some attacks, may require hardware updates.

**WPA3 (WiFi Protected Access 3):**

Pros: Enhanced security features, protection against brute force attacks.

Cons: Limited adoption as of now, may require hardware upgrades.

1. **Compare and Contrast:**

**WEP:** Easily compromised, not recommended for secure networks.

**WPA**: Better than WEP but still vulnerable to attacks, suitable for basic security needs.

**WPA2**: Currently a widely used standard with strong security, though not infallible.

**WPA3**: Represents the latest and most secure standard, but adoption may be limited.

1. **RealLife Examples:**

**WEP**: Rarely used due to its vulnerabilities; mostly seen in outdated or legacy systems.

**WPA/WPA2:** Commonly used in homes, cafes, and small businesses to provide a balance between security and compatibility.

**WPA3:** Gradually being implemented in newer routers and devices for heightened security, particularly in enterprise environments.

1. **Future Trends:**

Although WPA3 is the state-of-the-art at the moment, better authentication methods and quantum-resistant encryption are the main topics of ongoing research. With these developments, wireless networks will be even better protected against ever-evolving cyberthreats. However, because industry standards and hardware updates are required, it might take some time before these technologies are widely adopted.