**Wireless communication protocols**

Wi-Fi refers to a set of standards that define communication for wireless LANs (Local Area Network).

Wi-Fi standards and protocols are based on the 802.11 family of internet communication standards determined by IEEE (Institute of Electrical and Electronics Engineers). Wi-Fi can also be referred to as IEEE 802.11.

## Wired Equivalent Privacy

**WEP** is a wireless security protocol designed to provide users with the same level of privacy on wireless network connections as they have on wired network connections. Developed in 1999 and is the oldest wireless security standard.

## Wi-Fi Protected Access

**WPA** was created in 2003 to improve upon WEP, although there were flaws within the WEP protocol itself, so they addressed this by introducing Temporal Key integrity Protocol (TKIP). WPA encryption algorithm uses larger secret keys than WEPs making it more difficult to guess the key.

## WPA2 & WPA3

### WPA2

WPA2 was released in 2004 and improves upon WPA by using the Advanced Encryption Standard (AES). Also improves upon the use of Temporal Key Integrity Protocol (TKIP). WPA2 also uses Counter Mode Cipher Block Chain Message Authentication Code Protocol (CCMP) which provides encapsulation and ensures message authentication and integrity. It is very secure and is considered the security standard for all Wi-Fi transmissions today.

#### WPA2 Personal

WPA2 Personal is easy to implement and is best suited for home networks but unmanageable for organizations.

#### WPA2 Enterprise

WPA2 Enterprise works best for businesses applications. It provides the necessary security for wireless networks in business settings. It also provides individualized and centralized control over the Wi-Fi access to a business network. This means that users never have access to encryption keys which prevent potential attackers from recovering network keys on individual computers.

### WPA3

WPA3 was released in 2018 and the key differences between WPA2 and WPA3 are the following:

* WPA3 addresses the authentication handshake vulnerability to “krack” attacks which is present in WPA2
* WPA3 uses Simultaneous Authentication of Equals (SAE) a password authenticated,

cipher-key sharing agreement. This prevents attackers from downloading data from wireless network connections to their systems to attempt to decode it.

* WPA3 has increased encryption to make passwords more secure by using 128-bit encryption, with WPA3-Enterprise mode offering optional 192-bit encryption