WEP, WPA, WPA2, and WPA3

Wireless Encryption Standards:

- Wireless Equivalent Privacy (**WEP**) - Compromised
- Wi-Fi Protected Access (**WPA**) - Compromised
- Wi-Fi Protected Access 2 (**WPA2**) – Compromised
- Wi-Fi Protected Access 3 (**WPA3**) – Current Standard (with Vulnerabilities)*

Wireless Equivalent Privacy (WEP)

- WEP is the original privacy component of the IEEE 802.11 wireless standard.
  - Was implemented in 1995.
  - Considered compromised and depreciated in 2004, with the earliest reported compromise published in 2001.
  - uses a 24-bit RC4 Initialization Vector (**IV**), which is sent in clear text.
  - It is susceptible to passive network eavesdropping and replay attacks.
  - Can be cracked in minutes and should never be used.

Wi-Fi Protected Access (WPA)

- WPA was designed as a short-term fix for WEP as long-term, more secure solution (WPA2) was being created.
  - Could be implemented as a firmware upgrade to WEP devices (backwards compatible).
  - Still used the RC4 cipher, but **IV** (initialization vector) is now an encrypted hash.
  - Utilizes **TKIP** (Temporal Key Integrity Protocol) to dynamically change the encryption key.
  - Superseded by WPA2 in 2006.

Wi-Fi Protected Access 2 (WPA2)

- IEEE 802.11i Standard long-term replacement for WEP and WPA.
  - **AES** (Advanced Encryption Standard) replaced weaker **RC4** algorithm.
  - **CCMP** (Counter Mode with Cypher Block Chaining Message Authentication Code Protocol) replaced weaker **TKIP**.
  - Key Reinstallation Attack (**KRACK**) vulnerability found in 2017.
    - Vendor patches have been released to address this issue.
    - If you use WPA2, make sure it is patched to resolve the KRACK issue.

WPA3 Has Arrived

- In January, 2018 the Wi-Fi Alliance announced WPA3 as a replacement for WPA2.
  - Some routers already support it as of late 2018, but expect a wider adoption in 2019.
- Utilizes Simultaneous Authentication of Equals (**SAE**) as a means to more securely handle the initial key exchange to address WPA2 KRACK vulnerability.
  - However, was shown to still be vulnerability to KRACK.
  - Vendors have been deploying patches to resolve the vulnerability.
- If your devices support WPA3, consider using it.

WPA Personal versus Enterprise Mode

Personal Mode

- Uses “Pre-Shared Keys” for authentication.
- Pre-Shared Key = Password
- Common for small wireless networks without an authentication serve:
  - home, small office, coffee shop, airport, etc.

Enterprise Mode

- WPA-802.1x Standard
- Used with a central authentication server, such as Windows Active Directory
- Requires the use of a **RADIUS** authentication server
- Uses **EAP** (extensible authentication protocol) for authentication