

WEP, WPA and WPA2



Wireless Encryption Standards:

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

** WPA3 is the new standard, but for your exam, WPA2 is the most secure option.*

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 - Superseded by WPA2 in 2006.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**.
 - Considered most secure wireless encryption for this certification exam.

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.
- WPA2 was cracked by researchers in October, 2017.
- If your router supports WPA3, use 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 server:
 - 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