Wireless Encryption Standards

Wireless Encryption Standards

Standard	Acronym	Status
Wireless Equivalent Privacy	WEP	Compromised
Wi-Fi Protected Access	WPA	Compromised
Wi-Fi Protected Access 2	WPA2	Compromised (with patches)*
Wi-Fi Protected Access 3	WPA3	Current Standard (with vulnerabilities)*

Wireless Equivalent Privacy (WEP)

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 cleartext.
    - 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)

Wi-Fi Protected Access (WPA)

- WPA was designed as a short-term fix for WEP as a 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    - Superseded by WPA2 in 2006.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)

Wi-Fi Protected Access 2 (WPA2)

- IEEE 802.11i Standard long-term replacement for WEP and WPA.
  - **AES** (Advanced Encryption Standard) replaced the 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.

Wi-Fi Protected Access 3 (WPA3)

Wi-Fi Protected Access 3 (WPA3)

- In January 2018, the Wi-Fi Alliance announced WPA3 as a replacement for WPA2.
  - In July 2020, the Wi-Fi Alliance made WPA3 mandatory for device certification.
- Utilizes Simultaneous Authentication of Equals (**SAE**) as a means to more securely handle the initial key exchange to address WPA2 KRACK vulnerability.
  - However, it was shown to still be vulnerable to KRACK.
  - Vendors deployed patches to resolve the vulnerability.
- If your devices support WPA3, consider using it.

WPA Enterprise vs. Personal Mode

INSTRUCTOR
ALTON

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

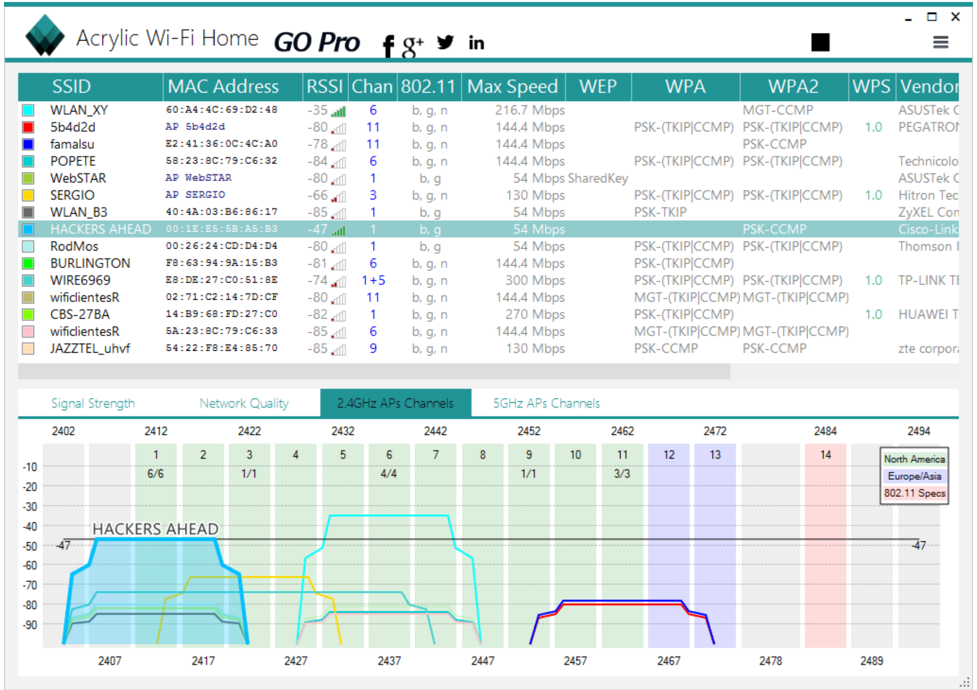
- WPA-802.1x Standard
- Used with a central authentication server, such as Windows Active Directory
- Requires the use of a **RADIUS** authentication server
- Uses **EAP** (extensible authentication protocol) for authentication

Wireless Network Vulnerabilities & Security

INSTRUCTOR
ALTON

Wireless Networking Security Vulnerabilities

- A significant vulnerability of wireless networks is that they broadcast network traffic over the air.
- Since data freely emanate over the air, anyone can intercept it with a transceiver tuned to the correct frequency.
- Since IEEE standardizes the frequencies, they're easy to learn by hackers.



SSID	MAC Address	RSSI	Chan	802.11	Max Speed	WEP	WPA	WPA2	WPS	Vendor
WLAN_XY	60:A4:4C:69:D2:48	-35	6	b, g, n	216.7 Mbps			MGT-CCMP		ASUSTek C
5b4d2d	AP 5b4d2d	-80	11	b, g, n	144.4 Mbps		PSK-(TKIP|CCMP)	PSK-(TKIP|CCMP)	1.0	PEGATRON
famalsu	E2:41:36:0C:4C:A0	-78	11	b, g, n	144.4 Mbps			PSK-CCMP		
POPETE	58:23:8C:79:C6:32	-84	6	b, g, n	144.4 Mbps		PSK-(TKIP|CCMP)	PSK-(TKIP|CCMP)		Technicolo
WebSTAR	AP WebSTAR	-80	1	b, g	54 Mbps	SharedKey				ASUSTek C
SERGIO	AP SERGIO	-66	3	b, g, n	130 Mbps		PSK-(TKIP|CCMP)	PSK-(TKIP|CCMP)	1.0	Hitron Tec
WLAN_B3	40:4A:03:B6:86:17	-85	1	b, g	54 Mbps		PSK-TKIP			ZyXEL Con
HACKERS AHEAD	00:1E:E5:5B:A5:B3	-47	1	b, g	54 Mbps			PSK-CCMP		Cisco-Link
RodMos	00:26:24:CD:D4:D4	-80	1	b, g	54 Mbps		PSK-(TKIP|CCMP)	PSK-(TKIP|CCMP)		Thomson I
BURLINGTON	F8:63:94:9A:15:B3	-81	6	b, g, n	144.4 Mbps		PSK-(TKIP|CCMP)			
WIRE6969	E8:DE:27:C0:51:8E	-74	1+5	b, g, n	300 Mbps		PSK-(TKIP|CCMP)	PSK-(TKIP|CCMP)	1.0	TP-LINK TE
wificlientesR	02:71:C2:14:7D:CF	-80	11	b, g, n	144.4 Mbps		MGT-(TKIP|CCMP)	MGT-(TKIP|CCMP)		
CBS-27BA	14:B9:68:FD:27:C0	-82	1	b, g, n	270 Mbps		PSK-(TKIP|CCMP)		1.0	HUAWEI T
wificlientesR	5A:23:8C:79:C6:33	-85	6	b, g, n	144.4 Mbps		MGT-(TKIP|CCMP)	MGT-(TKIP|CCMP)		
JAZZTEL_uhvf	54:22:F8:E4:85:70	-85	9	b, g, n	130 Mbps		PSK-CCMP	PSK-CCMP		zte corpora

Securing Wireless Network Essentials

- Decrease its Signal Footprint:
  - Lower its Signal Strength and/or Range.
- Implement a Security Protocol
  - WPA2 or WPA3
  - 802.1x (Centralized Authentication)
  - **DO NOT** use WEP or WPA

- Change the Default Administrator Password
- Implement Authentication
- Disable SSID Broadcasting
- Change the Default SSID
- Enable MAC Filtering
- Update Firmware Regularly

Common Wireless Security Threats

Common Wireless Security Threats

- **Rogue Access Point (AP)**: A wireless AP that has been installed on a secured network without any authorization from the network administrator.

- **Evil Twin Access Point**: A malicious wireless AP that advertises the same SSID as a legitimate AP to trick users into connecting to it.

- **War Driving**: Driving around to locate and exploit insecure wireless AP configurations.