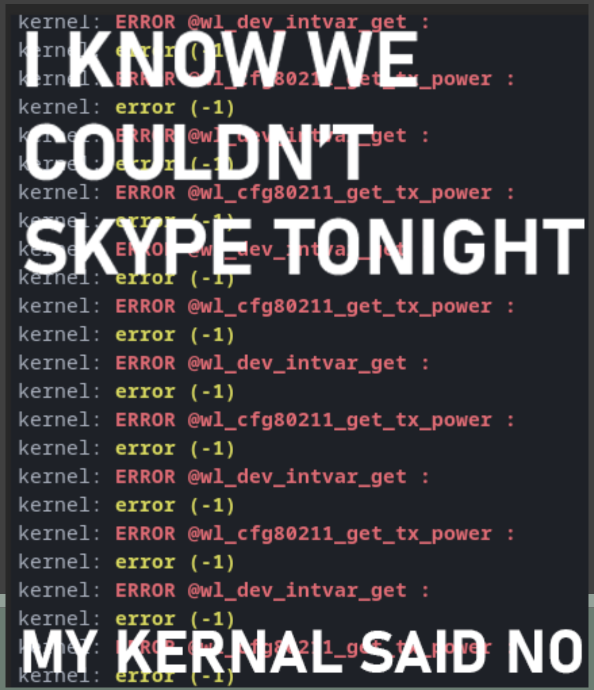
Wireless Networks
&
Malicious Actors



What is WI-FI?

WI-FI was invented when someone lost the ethernet cable
“We going wireless”

THE END

What is WI-FI?

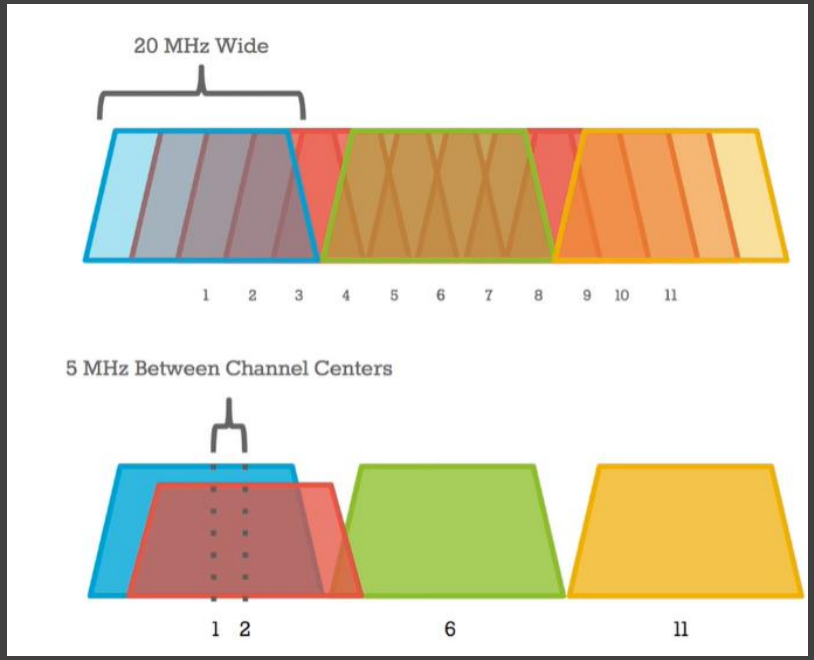
WI-FI is a brand name not an acronym.
WI-FI uses radio waves to transmit information between your device and a WAP / router via **frequencies**:

- 2.4Ghz
- 5Ghz

The IEEE SA (Institute of Electrical and Electronics Engineers Standards Association) decide the standards we see via a process by which proposed standards are voted upon for technical reliability and soundness.
There are currently:
1,200 active standards
650 standards under development

For WI-FI:
802.11 standard defines the protocols that enable communications with current Wi-Fi-enabled wireless devices, including wireless routers and wireless access points.

802.19 deals with the coexistence of between unlicensed wireless networks



Standard	Released	Speed
Wi-Fi 5/IEEE 802.11ac	2013	450 Mbps/1300 Mbps
IEEE 802.11ad (WiGig)	2012	6.7 Gbps
IEEE 802.11ah (HaLow)	2016	347 Mbps
Wi-Fi 6/IEEE 802.11ax	2019 est.	450 Mbps/10.53 Gbps

WI-FI Basics

What is an WAP? – Wireless Access Point:
This really any device that can function at Layer 2 and can transmit the necessary signals.
It allows any wireless devices to access and interact with existing wired networks. They are also commonly used as mesh extenders for extending signal range
Common types of access point configuration
- Root access point
- Repeater access point
- Bridges
- WAP Gateway
…

What defines a Layer 2 device:
A frame is a protocol data unit, the smallest unit of bits on a Layer 2 network. Not all frames carry user data. The network uses some frames to control the data link itself.

https://youtube.com/shorts/9p0pdiTOlzw?feature=share

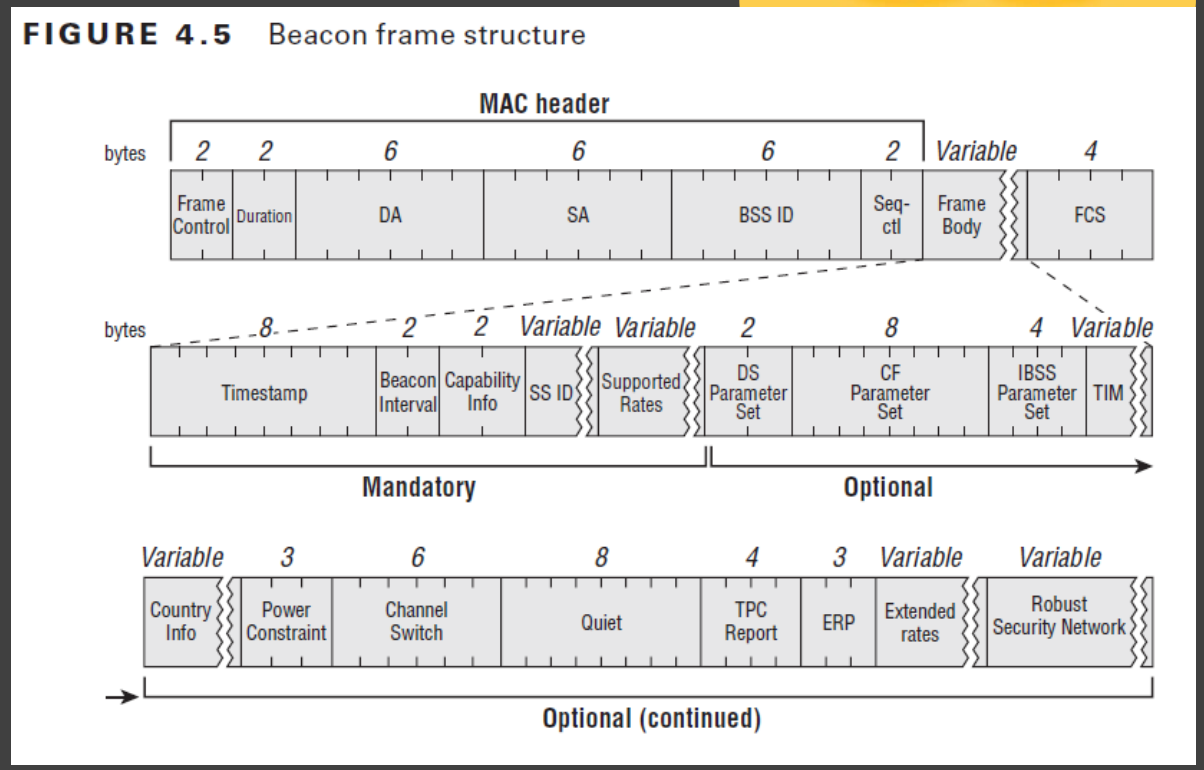
WI-FI Basics

Beacon Frames
Beacon frame is one of the management frames in IEEE 802.11 based WLANs. It contains all the information about the network. A beacon frame allows an access point to advertise its existence, and the frequency channel it is operating on, to devices that want to connect to an access point.

SSID (Service Set Identifier)
This is what wireless networks / access points will advertise as the network's name and will broadcats their SSIDs to nearby devices.

BSSID (Basic Service Set Identifier)
This is the AP MAC address of the SSID which is included in all wireless packets. You can be in one SSID but join different BSSID depending on the AP you are connected to

Handshakes with EAPOL – 4 way handshake used for access control in wired / wireless networks (WPA2 uses it for authentication)



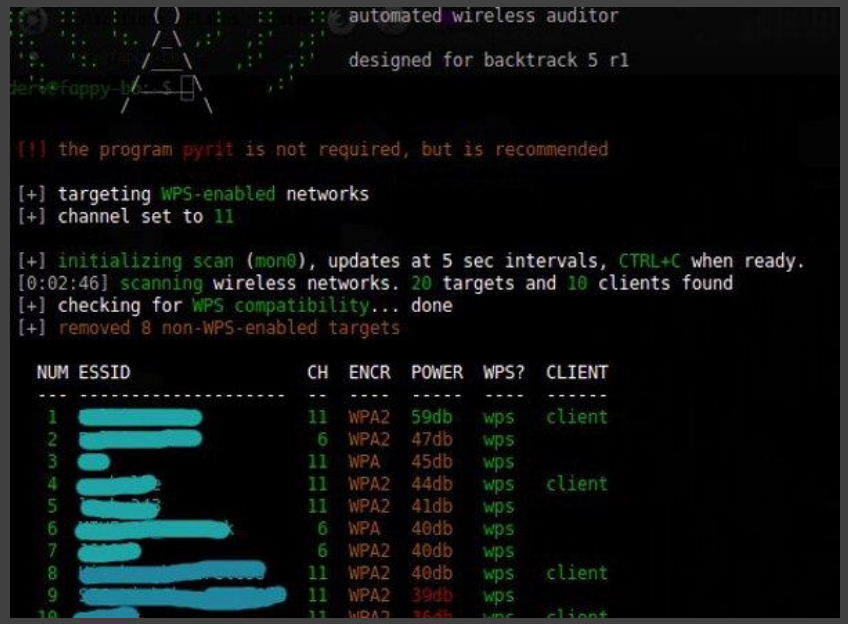
Malicious Actors
&
Attack Vectors

Deauth Attacks

These are the simplest form of attack and are a script kiddies most powerful tool due to its simplicity of use and need for no prior knowledge in networks.

The IEEE 802.11 (Wi-Fi) protocol contains the provision for a deauthentication frame. Under normal usage the AP would send the frame to a client with intentions to completely terminate a connection with the Wi-Fi network.

However, an attacker can send a deauthentication frame at any time to a wireless access point, with a spoofed address for the victim. The protocol does not require any encryption for this frame.



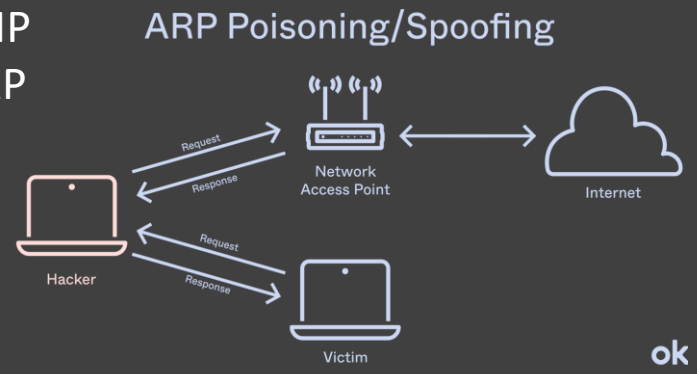
wifite – tool

Mitigation

Unfortunately, there is not practical form of mitigation to stop someone from sending these packets. However, using WPA2 along with long passwords and possibly using things such as “**Management Frame Protection**” you can reduce the capabilities of these attacks effecting you past the inconvenience.

ARP Spoofing / Poisoning

ARP (address resolution protocol) – Used to identify which MAC address matches with which IP address, it achieves this by sending a layer2 broadcast message to the entire LAN called an ARP request.
This attack vector is a man in the middle attack consists of abusing the weaknesses in ARP to corrupt the MAC-to-IP mappings of other devices on the network.



Harmful? Yes, since traffic destined for one or more hosts on the local network will instead be steered to a destination of the attacker's choosing. This could lead to leaked information such as credentials.

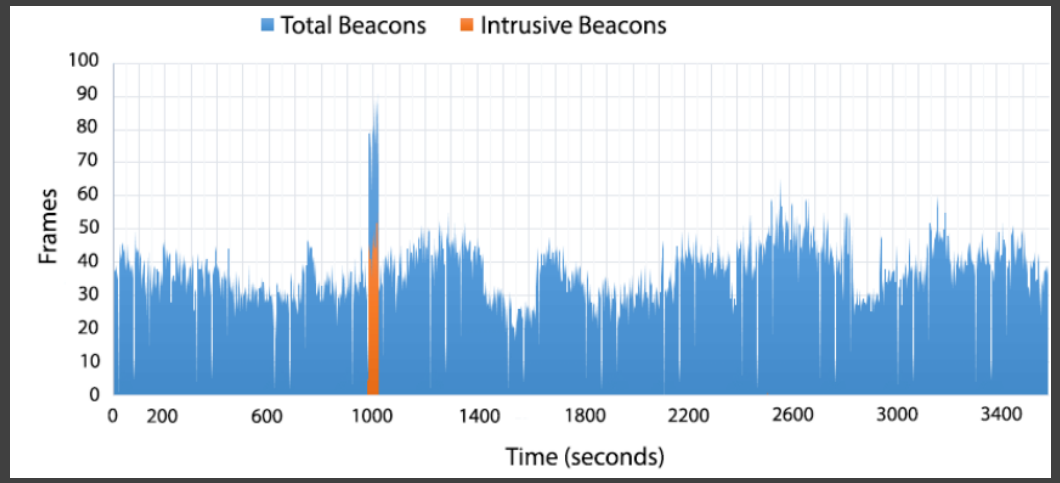
Mitigation:
- Static ARP Tables
- Packet filters
- Dynamic ARP Inspection
- Network Isolation

```
~
❯ sudo bettercap
[sudo] password for tom:
bettercap v2.32.0 (built for linux amd64 with go1.17) [type 'help' for a list of commands]

192.168.0.0/24 > 192.168.0.200 » [01:03:47] [sys.log] [inf] gateway monitor started ...
192.168.0.0/24 > 192.168.0.200 » net.probe on
192.168.0.0/24 > 192.168.0.200 » [01:03:53] [sys.log] [inf] net.probe starting net.recon as a requirement for net.probe
192.168.0.0/24 > 192.168.0.200 » [01:03:53] [sys.log] [inf] net.probe probing 256 addresses on 192.168.0.0/24
192.168.0.0/24 > 192.168.0.200 » [01:03:53] [endpoint.new] endpoint 192.168.0.24 detected as [redacted] (TP-Link Corporation Limited).
192.168.0.0/24 > 192.168.0.200 » [01:03:54] [endpoint.new] endpoint 192.168.0.12 detected as [redacted] (Samsung Electro-Mechanics(Thailand)).
192.168.0.0/24 > 192.168.0.200 » net.[01:04:00] [endpoint.new] endpoint 192.168.0.11 detected as [redacted]
192.168.0.0/24 > 192.168.0.200 » [01:04:10] [endpoint.lost] endpoint 192.168.0.11 [redacted] lost.
192.168.0.0/24 > 192.168.0.200 » [01:04:14] [endpoint.new] endpoint 192.168.0.13 detected as [redacted] (Intel Corporate).
192.168.0.0/24 > 192.168.0.200 » [01:04:24] [endpoint.lost] endpoint 192.168.0.13 [redacted] (Intel Corporate) lost.
192.168.0.0/24 > 192.168.0.200 » [01:04:29] [endpoint.new] endpoint 192.168.0.13 detected as [redacted] (Intel Corporate).
192.168.0.0/24 > 192.168.0.200 » net.show

| IP ▲ | MAC | Name | Vendor | Sent | Recvd | Seen |
|---|---|---|---|---|---|---|
| 192.168.0.200 | [redacted] | enp9s0 | | 0 B | 0 B | 01:03:47 |
| 192.168.0.1 | | gateway | Hitron Technologies. Inc | 11 kB | 0 B | 01:03:47 |
| 192.168.0.12 | | | Samsung Electro-Mechanics(Thailand) | 1.1 kB | 460 B | 01:04:29 |
| 192.168.0.13 | | | Intel Corporate | 173 B | 0 B | 01:04:29 |
| 192.168.0.24 | | | TP-Link Corporation Limited | 3.7 kB | 460 B | 01:04:26 |

↑ 68 kB / ↓ 192 kB / 3890 pkts

192.168.0.0/24 > 192.168.0.200 »
```

bettercap – tool

Management Frame Attacks

Beacon Flooding Attack: The goal here is to confuse a wireless clients through the spamming of beacons on the network advertising many access points available that don't exist. This is very similar to a DOS attack meaning it won't go undetected on a network.




```
root@kali:~# mdk3 mon0 b -w -g -t -m -c 6

Current MAC: 00:07:50:7C:C2:54 on Channel  6 with SSID: $a7Ii0Rk
Current MAC: 00:04:5A:0E:AA:6A on Channel  6 with SSID: 7#W6g^M3PyZE{K
Current MAC: 00:50:18:6E:BB:0E on Channel  6 with SSID: _QY/{W!g$XF7gSV&w-0JDj;p
:'*
Current MAC: 00:0B:CD:60:C0:53 on Channel  6 with SSID: ?/#BD%9c-o.ox
Current MAC: 00:06:25:25:57:2E on Channel  6 with SSID: VXJ
Current MAC: 00:0D:BD:55:F3:02 on Channel  6 with SSID: W\LUI\lJdMShJB1|dM
Current MAC: 00:03:2F:AA:23:E2 on Channel  6 with SSID: K-Z6?09dsd"4'\;rT}/cA
Current MAC: 00:07:13:56:B2:2B on Channel  6 with SSID: 7CjP8Wr*y`|s<;'QV_*&p;/H
cn=%Y|
Current MAC: 00:20:E0:06:89:F5 on Channel  6 with SSID: ,"TEqHl
Current MAC: 00:0F:66:E7:0F:6A on Channel  6 with SSID: $z
Current MAC: 00:20:E0:6D:8B:24 on Channel  6 with SSID: Lz(tnKf#xDpB_e$
Current MAC: 00:60:1D:1D:27:9F on Channel  6 with SSID: M$pRt0D\66uJy%Hmhl"p*S:L
Current MAC: 00:03:52:4D:59:20 on Channel  6 with SSID: O*6eF.Q4j8sTgG.o-((fT h"
```

mdk3– tool

```
root@kali:~# airodump-ng wlan0


 CH 11 ][ Elapsed: 0 s ][ 2018-11-26 16:29

 BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

 90:CD:B6:83:43:B2  -34        3        0    0   5   65  WPA2 CCMP   PSK  Oppo
 D8:C8:E9:C2:CB:18  -82        2        0    0  10  130  WPA2 CCMP   PSK  perfe
 E4:6F:13:B6:DB:03  -67        3        0    0  10  270  WPA2 CCMP   PSK  Fligh
 F0:D7:AA:E0:4F:E4  -61        6        0    0   3   65  OPN              Ashu
 7A:11:DC:6E:C0:78  -66        7        8    3   3  130  WPA2 CCMP   PSK  LIFCA
 78:11:DC:5E:C0:78  -63        7        0    0   3  130  WPA2 CCMP   PSK  Xiaom
 B8:C1:A2:3B:16:0C  -59        2        4    0  11  130  WPA2 CCMP   PSK  (JTP-
 10:DA:43:72:41:C2  -84        1        1    0  13  54   WPA2 CCMP   PSK  Nextr
 58:D7:59:EC:1F:68  -80        3        0    0   7  130  WPA2 CCMP   PSK  tie d
 0A:28:19:E1:9F:5B  -46        3        0    0   7  130  WPA2 CCMP   PSK  LAPTO
 C0:FF:D4:91:49:DF  -48        1       31   15   7  130  WPA2 CCMP   PSK  NETGE
 0C:D2:B5:49:D5:C4  -66        4        5    2   7   65  WPA  CCMP   PSK  Airte
 50:C8:E5:AF:F6:33  -25        5        0    0   6   65  WPA2 CCMP   PSK  BS1A-
 50:64:2B:CE:B4:F4  -79        0        3    1   1   -1  WPA              <leng
 A8:F5:AC:65:82:7C  -71        1        2    0   1  130  WPA2 CCMP   PSK  Vashi

root@kali:~#
```

airodump-ng– tool

Probe frames: Used probe request frames to scan the area for availability of WLAN network. SSID is included within a probe request (usually in plain text). A WAP will respond with Probe response frames which contains similar information

This way devices can reconnect to WAP that they have connected to before.

Hackers can abuse this via:

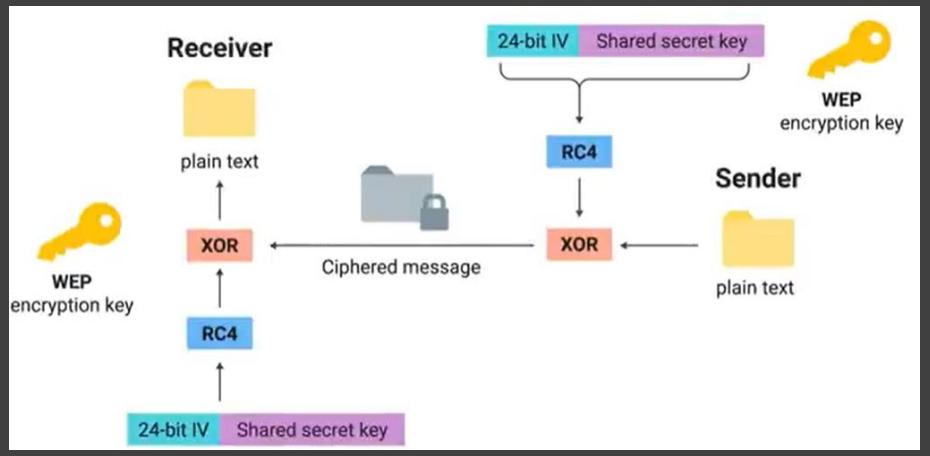
- Active Scanning
- Evil twin (useful for open networks)

WEP

WEP (Wired Equivalent Privacy) – Implements a data encryption scheme which utilizes a combination and mix of user and system-generated key values. 40 bits plus additional bits of system-generated data encryption keys are supported by the original implementations of WEP.
Once WEP has been deployed over a Wi-Fi connection, it will encrypt the data stream using coded keys:
104-bit shared key scheme
40-bit shared key scheme

Why is it bad?
The reason WEP is no longer used to this day is due to hacker's ability to acquire the encryption key. Since the plaintext and cipher text are sent together using easily available tools.

However, the downfall of WEP came from the small value of IVs removing the randomness from the key generation and within a short period of time all keys are reused making it deterministic.



Possible Mitigation?
DON'T USE WEP

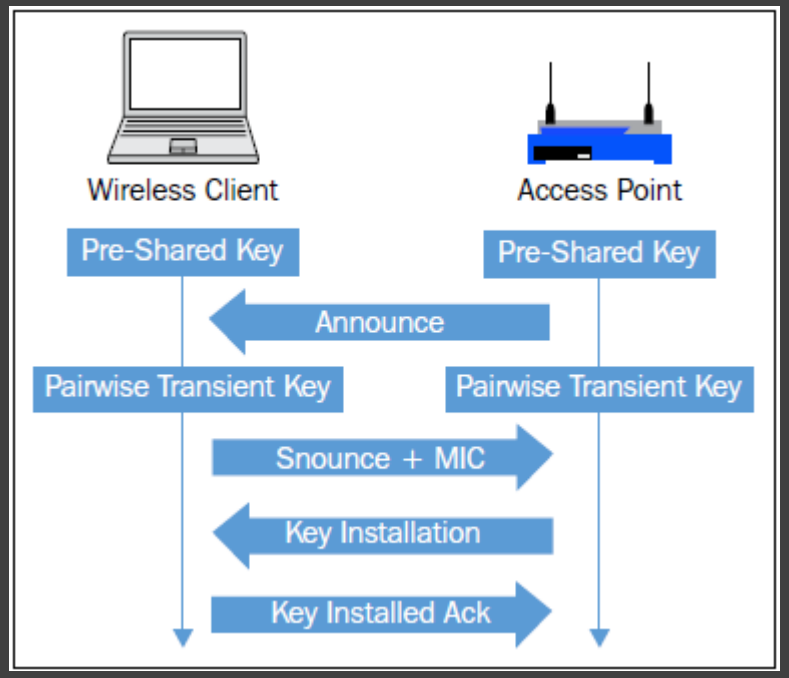
WPA

WPA Wi-Fi Protected Access – WPA uses the temporal key integrity protocol (TKIP), which dynamically changes the key that the systems use. This prevents intruders from creating their own encryption key to match the one used by the secure network.
WPA comes in two flavours

- Personal

  WPA Pre Shared Key (PSK), is the most common authentication method used on wireless networks today

Why is it bad?
PSK has a vulnerability to dictionary attacks. To crack the WPA PSK key, a dictionary, or wordlist, is required and the captured traffic should also contain four-way handshake packets.
Through this a hacker can then use a wordlist to attempt to crack the password similar to how WEP is compromised.



Possible Mitigation?

- VPN to encrypt the handshakes being sent

WPA2 & 3

WPA2:

- Released in 2004
- Uses Advanced Encryption Standard (AES) instead of TKIP
- WPA2 Pre-Shared Key uses keys that are 64 hexadecimal digits long
- Standard encryption used by the US Federal Government

WPA3:

- Released in 2018
- 128-bit encryption in WPA3-Personal Mode
- Offers 192-bit in WPA3-Enterprise mode
- Mandates use of Protected Management Frames
- WPA3 uses Dragonfly Key Exchange system making it resilient to dictionary attacks

Is it perfect?

NO

Big Hak

Tools:

airmon-ng:

- enable monitor mode on wireless interface

airecrack-ng:

- complete suite of tools to assess WiFi network security

airdecap-ng

- decrypt WEP/WPA/WPA2 capture files. Can be used to strip the wireless headers from an unencrypted wireless capture

airodump-ng

- used for packet capture, capturing raw 802.11 frames (particularly suitable for collecting WEP Ivs)

aireplay-ng

- used to inject frames. The primary function is to generate traffic for the later use in aircrack-ng for cracking the WEP

Documentation: https://www.aircrack-ng.org/