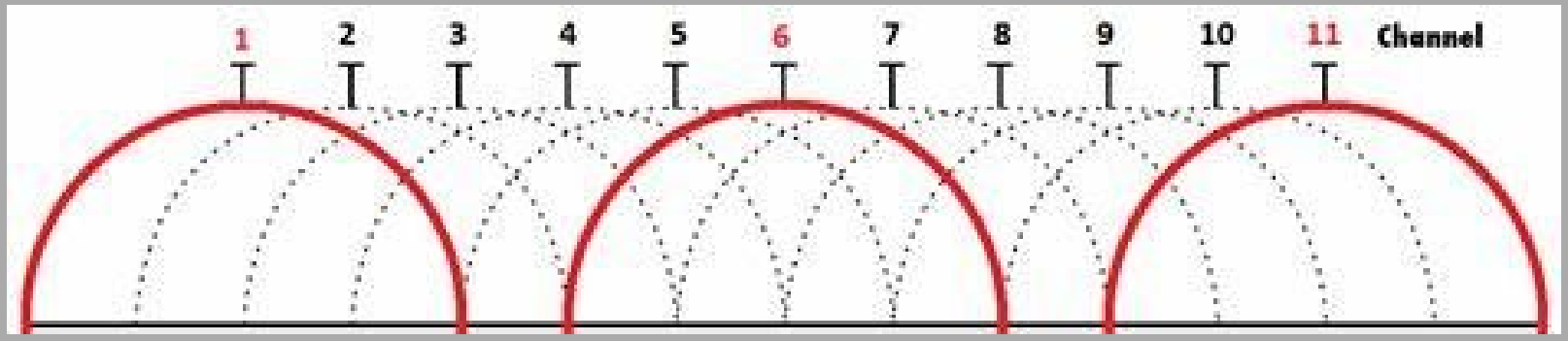
Wi-Fi

(Wireless Fidelity)

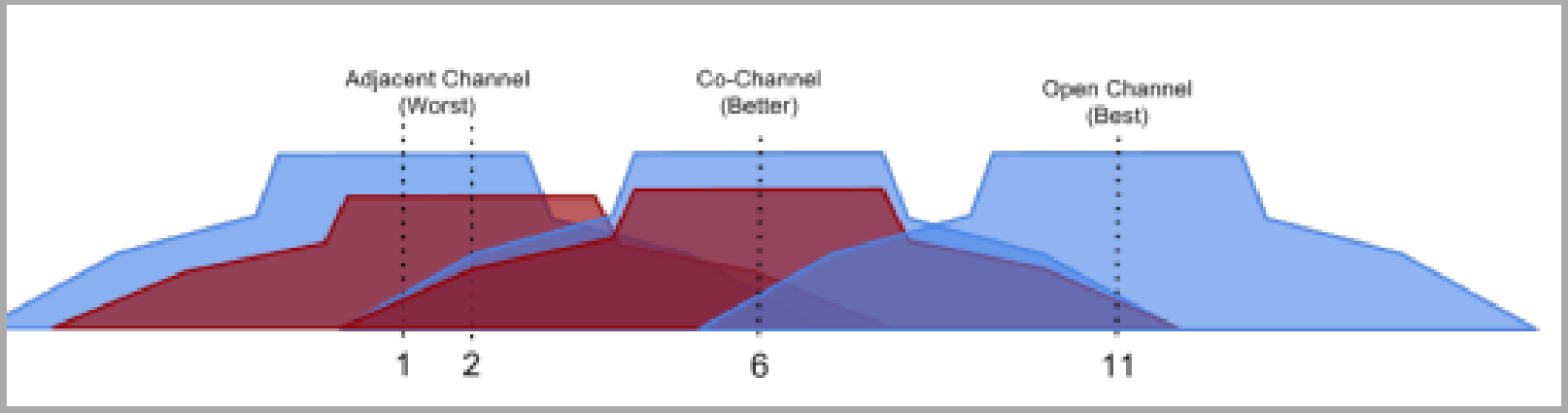
IEEE 802 is a family of IEEE standards dealing with local area networks and metropolitan area networks.

IEEE 802.11 is part of the IEEE 802 set of LAN protocols, and specifies the set of media access control (MAC) and physical layer (PHY) protocols for implementing wireless local area network (WLAN) Wi-Fi computer communication in various frequencies, including but not limited to 2.4 GHz, 5 GHz, and 60 GHz frequency bands.

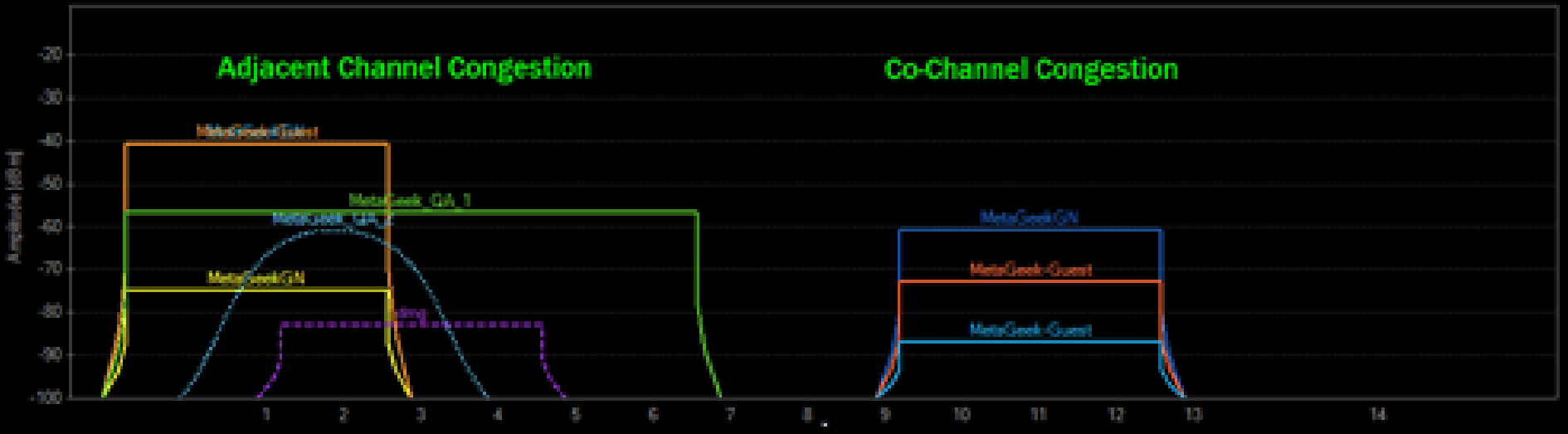
- 802.11-1997 2.4 GHz 1 Mbit/s or 2 Mbit/s (LEGACY)
- 802.11**b** 2.4 GHz 11 Mbit/s (WiFi 1)
- 802.11**a** 5GHz 54 Mbit/s (WiFi 2)
- 802.11**g** 2.4 Ghz 54 Mbit/s (WiFi 3)
- 802.11**n** 2.4 and 5 GHz, up to 600 Mbit/s (WiFi 4)
- 802.11**ac** 5GHz up to 1300 Mbit/s, Wave 2 up to 3,5 Gbit/s (WiFi 5)
- 802.11**ad** (WiGig) 60 GHz, 8 Gbit/s
- 802.11**ax** 2.4+5 GHz (1-6 GHz) up to 14 Gbit/s (WiFi 6)



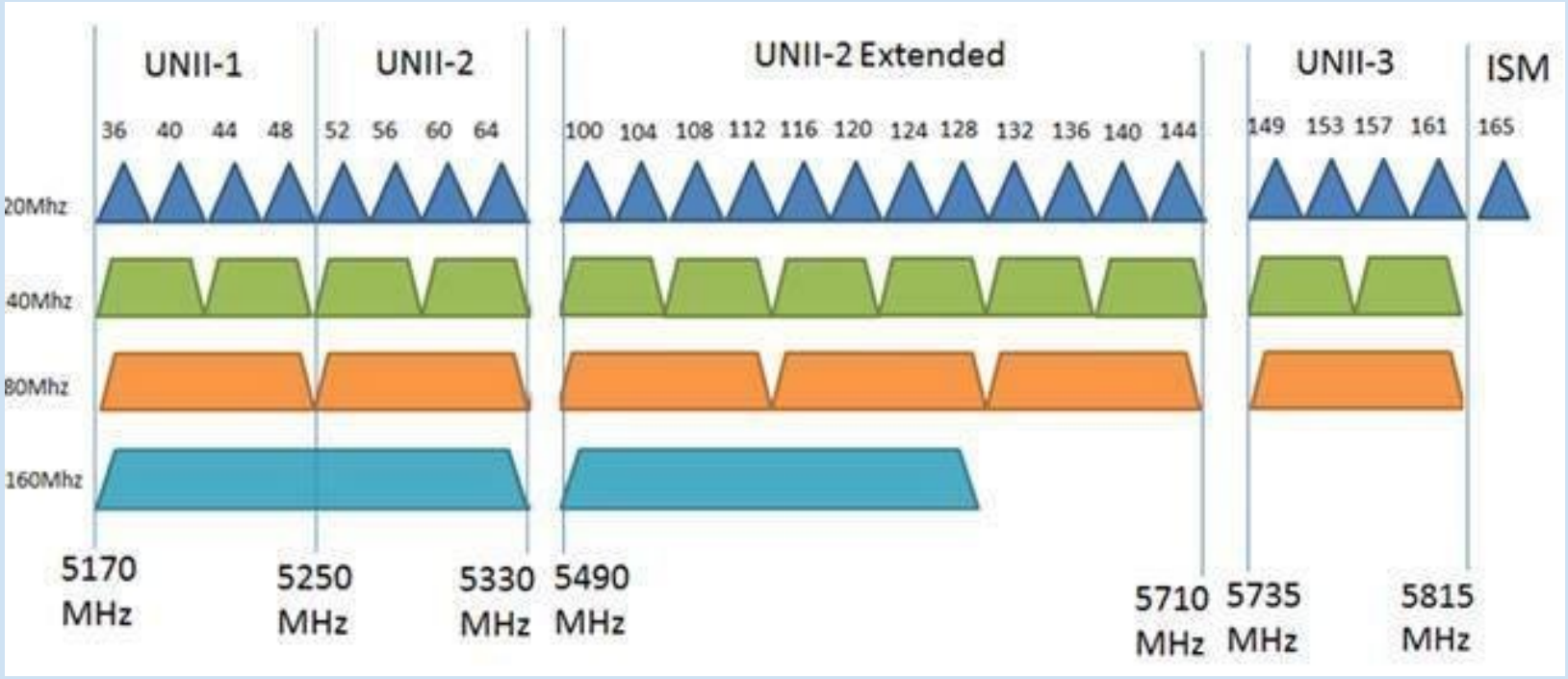
channels on 2.4 GHz band



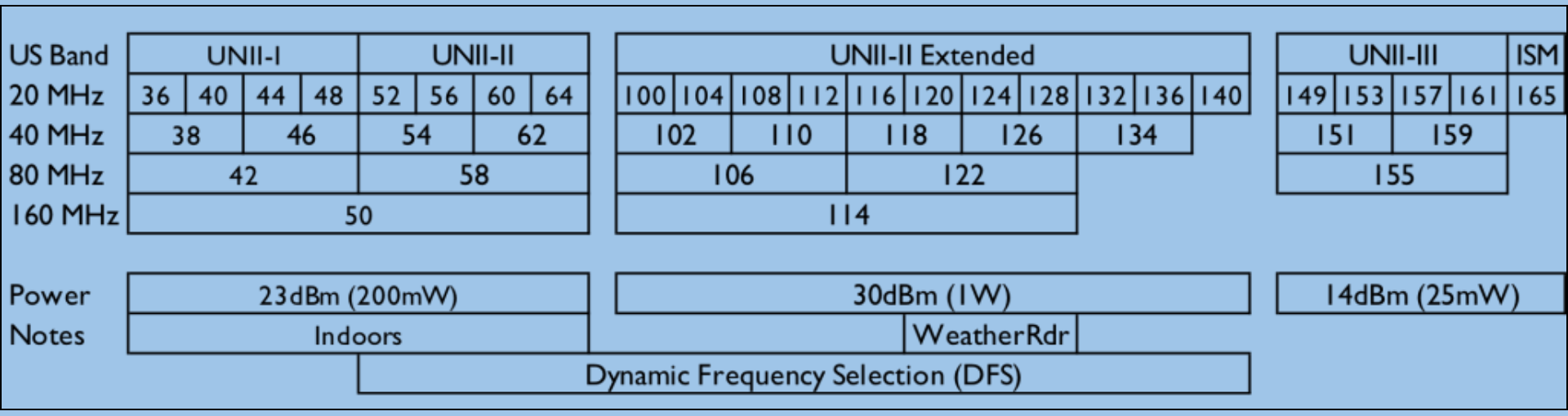
channel interference and open channel



adjacent vs. co-channel congestion



channels on 5 GHz band, 20-160 MHz wide channels



channel numbers vs. channel width

Transmit power control (TPC) is a technical mechanism used within some networking devices in order to prevent too much unwanted interference between different wireless networks (e.g. the owner's network and the neighbour's network).

Dynamic Frequency Selection (**DFS**) is a channel allocation schemes specified for wireless LAN, commonly Wi-Fi. It is designed to prevent electromagnetic interference with other usages of the C band frequency band that had predated Wi-Fi, such as military radar, satellite communication, and weather radar.

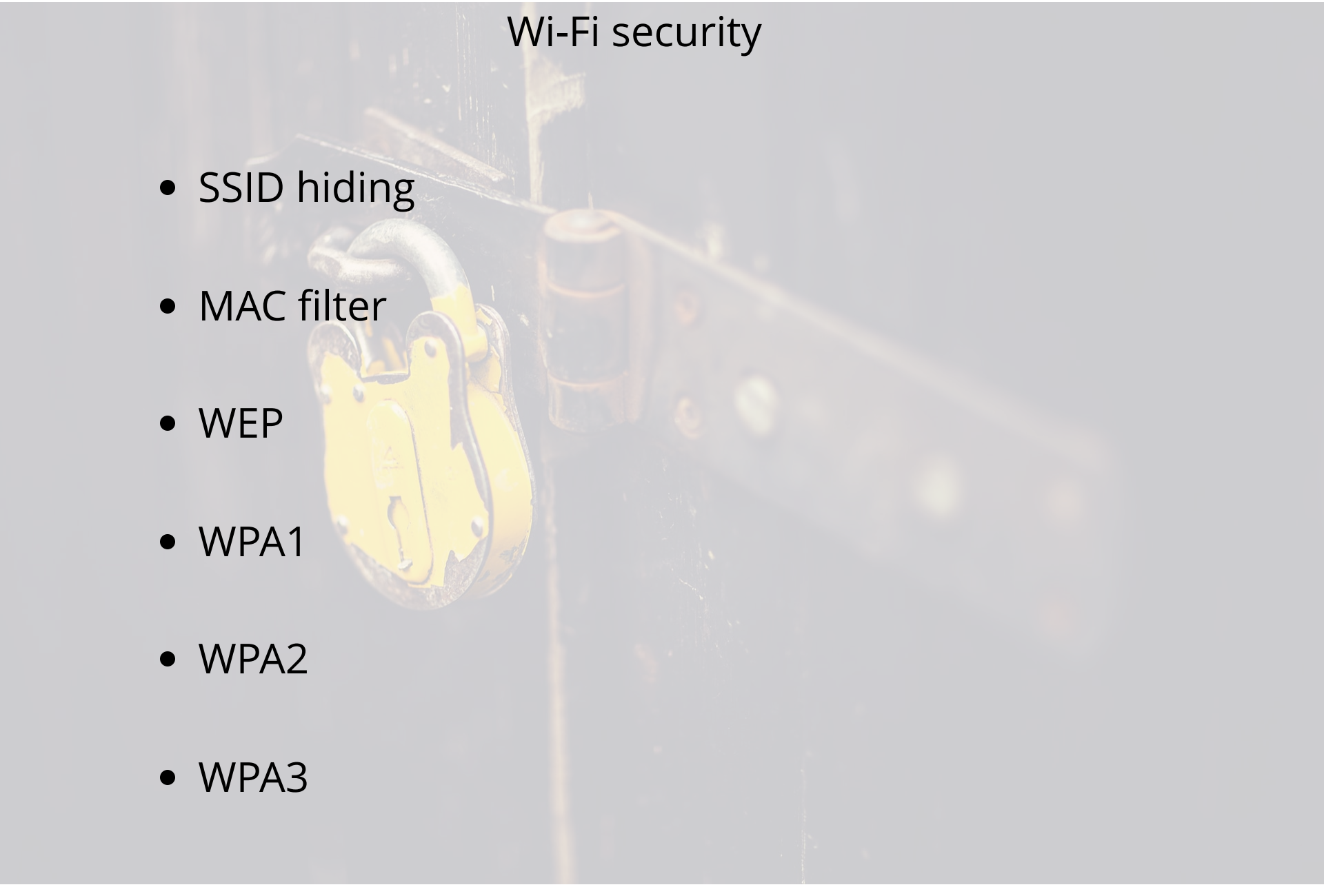
Signal Strength	TL;DR	
-30 dBm	Amazing	Max achievable signal strength. The client can only be a few feet from the AP to achieve this. Not typical or desirable in the real world.
-67 dBm	Very Good	Minimum signal strength for applications that require very reliable, timely delivery of data packets.
-70 dBm	Okay	Minimum signal strength for reliable packet delivery.
-80 dBm	Not Good	Minimum signal strength for basic connectivity. Packet delivery may be unreliable.
-90 dBm	Unusable	Approaching or drowning in the noise floor. Any functionality is highly unlikely.

The Common Interference Culprits

Several household electronics can be sabotaging your Wi-Fi performance:

- Microwave oven
- Cordless phone
- Baby monitor
- Wireless video camera
- Wireless game controller
- Older Bluetooth devices

Wi-Fi security



- SSID hiding
- MAC filter
- WEP
- WPA1
- WPA2
- WPA3

Wi-Fi security

- SSID hiding 
- MAC filter
- WEP
- WPA1
- WPA2
- WPA3

Wi-Fi security

- SSID hiding ☹
- MAC filter ☹
- WEP
- WPA1
- WPA2
- WPA3

Wi-Fi security

- SSID hiding ☹
- MAC filter ☹
- WEP ☹
- WPA1
- WPA2
- WPA3

Wi-Fi security

- SSID hiding ☹
- MAC filter ☹
- WEP ☹
- WPA1 ☹
- WPA2
- WPA3

Wi-Fi security

- SSID hiding 
- MAC filter 
- WEP 
- WPA1 
- WPA2 
- WPA3

Wi-Fi security

- SSID hiding 
- MAC filter 
- WEP 
- WPA1 
- WPA2 
- WPA3 

Wi-Fi security

- SSID hiding 
- MAC filter 
- WEP 
- WPA1 
- WPA2 
- WPA3 

Wi-Fi security

- SSID hiding 
- MAC filter 
- WEP 
- WPA1 
- WPA2 
- WPA3 

 IEEE 802.1X

Wi-Fi security

- SSID hiding 
- MAC filter 
- WEP 
- WPA1 
- WPA2 
- WPA3 

 IEEE 802.1X 

WPA:

- Personal - Pre-shared Key (PSK)
- Enterprise

In cryptography, a **pre-shared key** (**PSK**) is a shared secret which was previously shared between the two parties using some secure channel before it needs to be used.

To build a key from shared secret, the key derivation function is typically used. Such systems almost always use symmetric key cryptographic algorithms. The term PSK is used in Wi-Fi encryption such as Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), where the method is called WPA-PSK or WPA2-PSK.

In all these cases, both the wireless access points (AP) and all clients *share* the same key.

WPA2 (IEEE 802.11i)

- TKIP
- AES (CCMP)

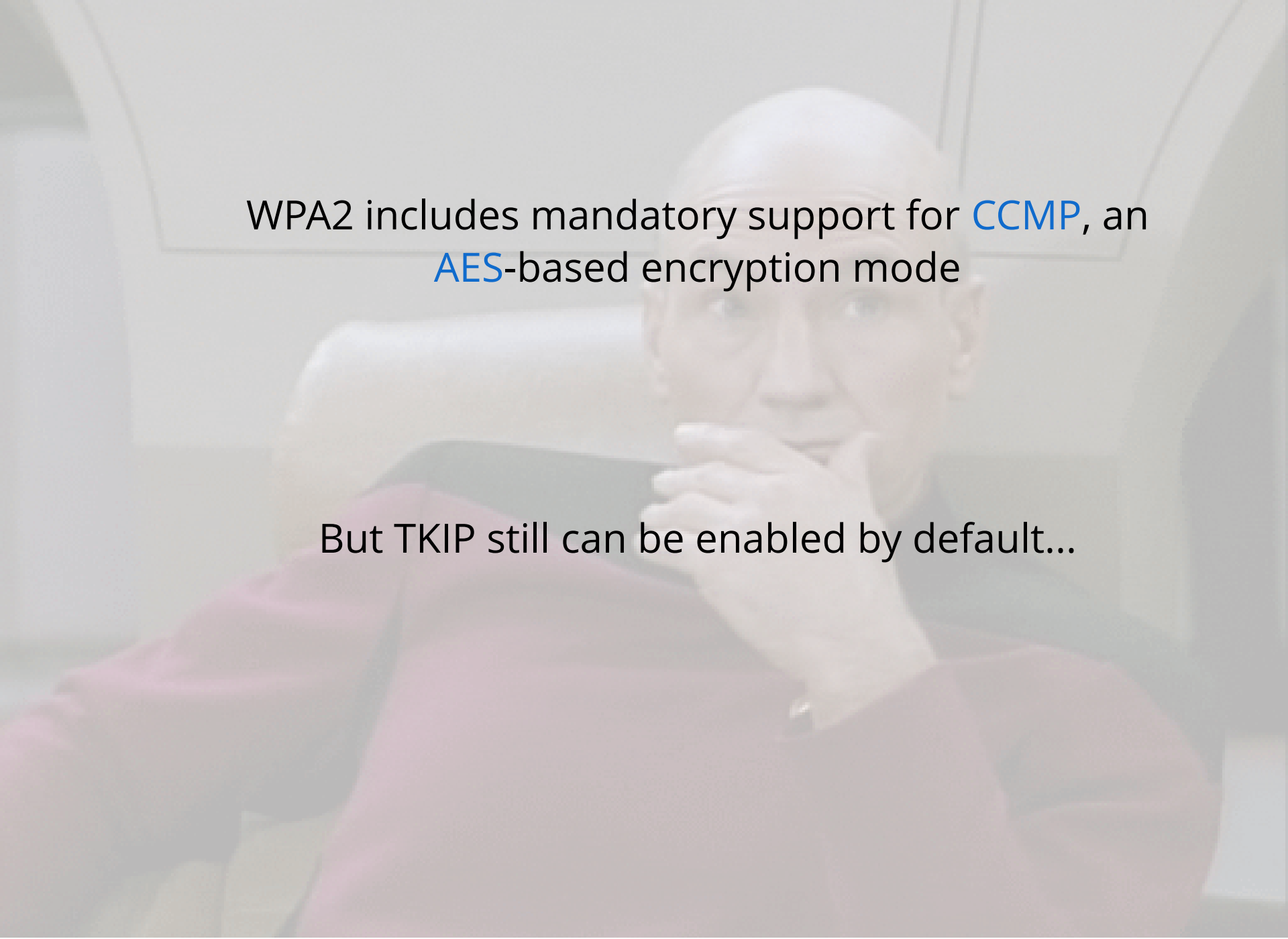
The standard also provides two RSNA data confidentiality and integrity protocols, TKIP and CCMP, with implementation of CCMP being mandatory since the confidentiality and integrity mechanisms of TKIP are not as robust as those of CCMP. The main purpose to implement TKIP was that the algorithm should be implementable within the capabilities of most of the old devices supporting only WEP.

The initial authentication process is carried out either using a pre-shared key (PSK), or following an EAP exchange through 802.1X (WPA-Enterprise), which requires the presence of an authentication server.

WPA2 includes mandatory support for CCMP, an AES-based encryption mode

WPA2 includes mandatory support for CCMP, an AES-based encryption mode

But TKIP still can be enabled by default...



WPA2 includes mandatory support for CCMP, an AES-based encryption mode

But TKIP still can be enabled by default...

WPA-Enterprise ~=

EAP

The WPA-improvement over the IEEE 802.1X standard already improved the authentication and authorization for access of wireless and wired LANs.

New, improved version of EAP is called Extended EAP and is available in several versions; these include: EAP-MD5, PEAPv0, PEAPv1, EAP-MSCHAPv2, LEAP, EAP-FAST, EAP-TLS, EAP-TTLS, MSCHAPv2, and EAP-SIM

The **Protected Extensible Authentication Protocol**, also known as **Protected EAP** or simply **PEAP**, is a protocol that encapsulates the Extensible Authentication Protocol (EAP) within an encrypted and authenticated Transport Layer Security (TLS) tunnel. The purpose was to correct deficiencies in EAP.

First EAP assumed a protected communication channel, such as that provided by physical security, so facilities for protection of the EAP conversation were not provided.

The IEEE 802.11 (Wi-Fi) protocol contains the provision for a deauthentication frame. Sending the frame from the access point to a station is called a "sanctioned technique to inform a rogue station that they have been disconnected from the network".

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, even when the session was established with Wired Equivalent Privacy (WEP) for data privacy, and the attacker only needs to know the victim's MAC address, which is available in the clear through wireless network sniffing.

Usage

Evil twin access points

One of the main purposes of deauthentication used in the hacking community is to force clients to connect to an Evil twin access point which then can be used to capture network packets transferred between the client and the AP.

The attacker conducts a deauthentication attack to the target client, disconnecting it from its current network, thus allowing the client to automatically connect to the Evil twin access point.

Usage

Password attacks

In order to mount a brute-force or dictionary based WPA password cracking attack on a WiFi user with WPA or WPA2 enabled, a hacker must first sniff the WPA 4-way handshake. The user can be elicited to provide this sequence by first forcing them offline with the deauthentication attack.

Protected management frames (PMF)

Current 802.11 standard defines "frame" types for use in management and control of wireless links. IEEE 802.11w is the Protected Management Frames standard for the IEEE 802.11 family of standards. Task Group w worked on improving the IEEE 802.11 Medium Access Control layer (MAC). Its objective was to increase security by providing data confidentiality of management frames, mechanisms that enable data integrity, data origin authenticity, and replay protection.

WPA3

In January 2018, the Wi-Fi Alliance announced WPA3 as a replacement to WPA2.

192-bit cryptographic strength in WPA3-Enterprise mode (AES-256 in GCM mode with SHA-384 as HMAC), and still mandates the use of CCMP-128 (AES-128 in CCM mode) as the minimum encryption algorithm in WPA3-Personal mode.

The WPA3 standard also **replaces** the Pre-Shared Key exchange with Simultaneous Authentication of Equals (SAE) as defined in IEEE 802.11-2016 resulting in a more secure initial key exchange in personal mode and forward secrecy.

Protection of management frames as specified in the IEEE 802.11w amendment is **enforced** by the WPA3 specifications.

SAE is a variant of the Dragonfly Key Exchange defined in RFC 7664, based on **Diffie–Hellman (DH)** key exchange using finite cyclic groups which can be a primary cyclic group or an elliptic curve. The problem of using Diffie–Hellman key exchange is that it does not have an authentication mechanism. So the resulting key is influenced by a pre-shared key and the MAC addresses of both peers to solve the authentication problem.

In cryptography, **forward secrecy** (**FS**), also known as **perfect forward secrecy** (**PFS**), is a feature of specific key agreement protocols that gives assurances that session keys will not be compromised even if the private key of the server is compromised.

Opportunistic Wireless Encryption (**OWE**) is an extension to IEEE 802.11 which adds a standard for opportunistic encryption for use with an open Wi-Fi network. OWE is an encryption technique similar to that of Simultaneous Authentication of Equals (SAE) and is specified by Internet Engineering Task Force (IETF) in RFC 8110 with devices certified as **Wi-Fi Certified Enhanced Open** by the Wi-Fi Alliance.

questions?