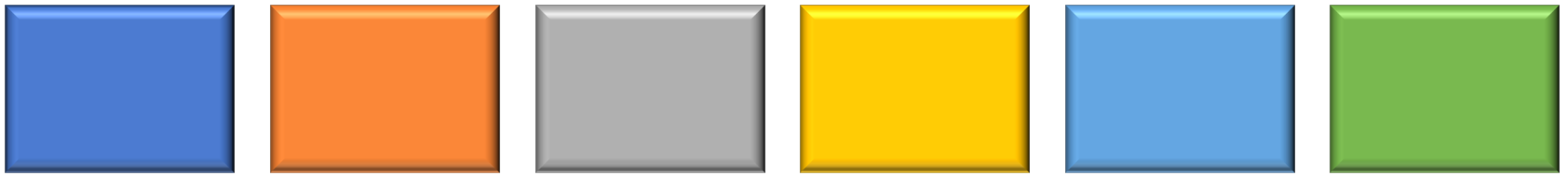
WPA 3

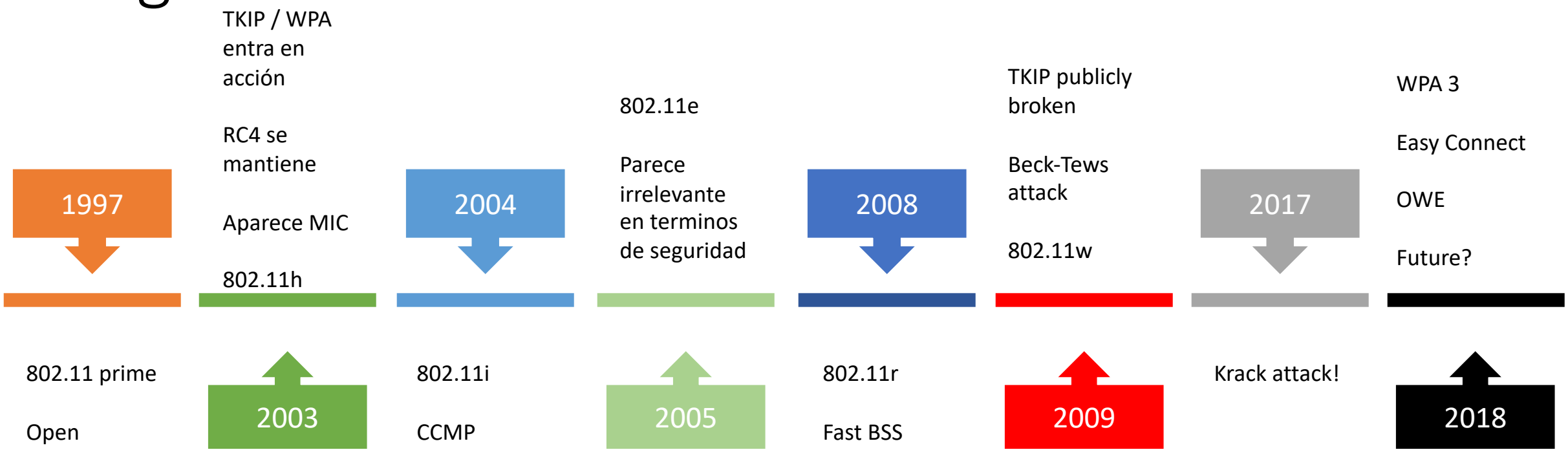
Intro y un poco más…

Victor Tort
CWNE 267 & CWNT

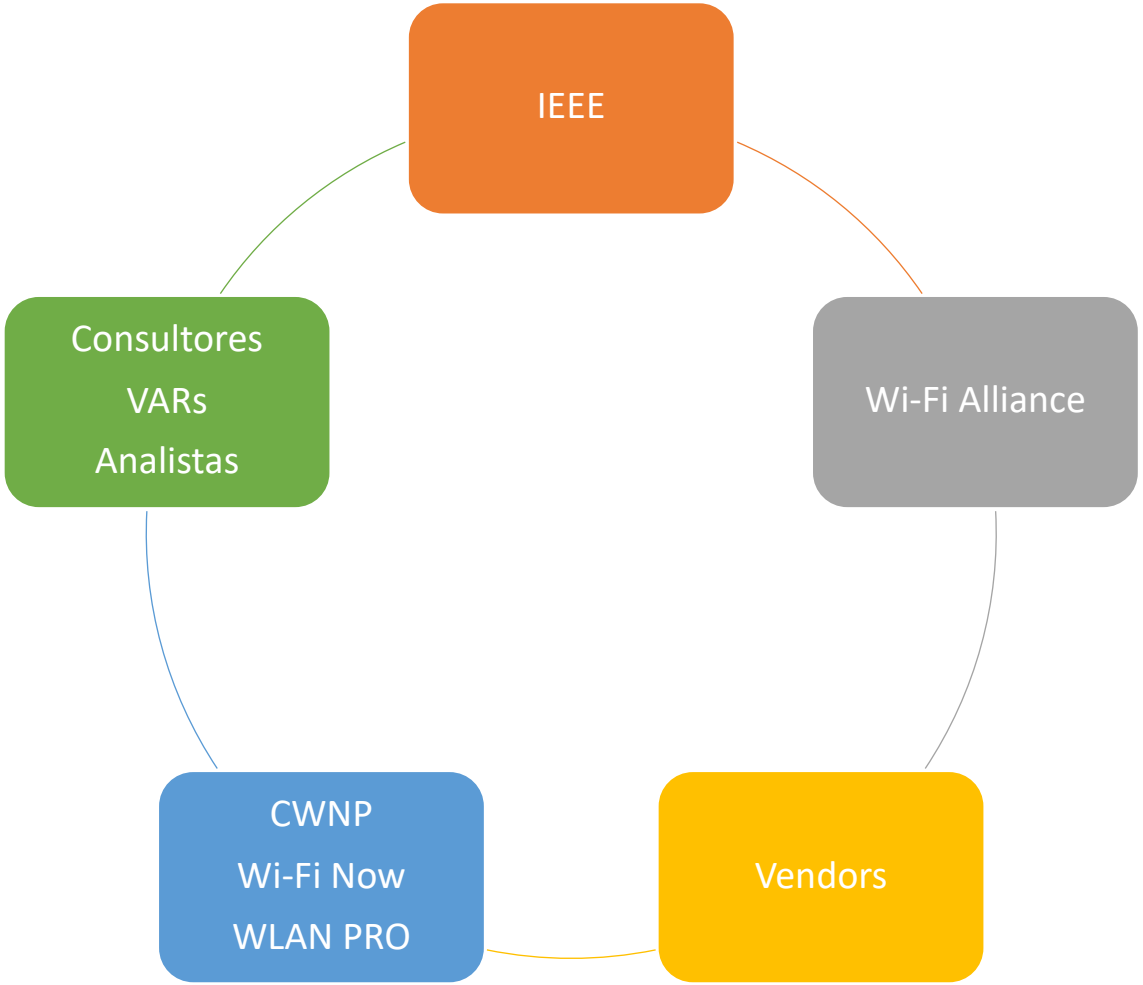


Lo que necesitamos saber

Algo de historia

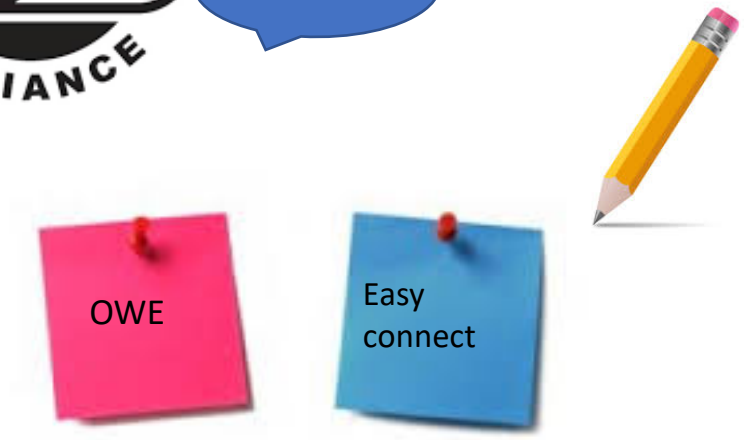


Quiénes son los jugadores?

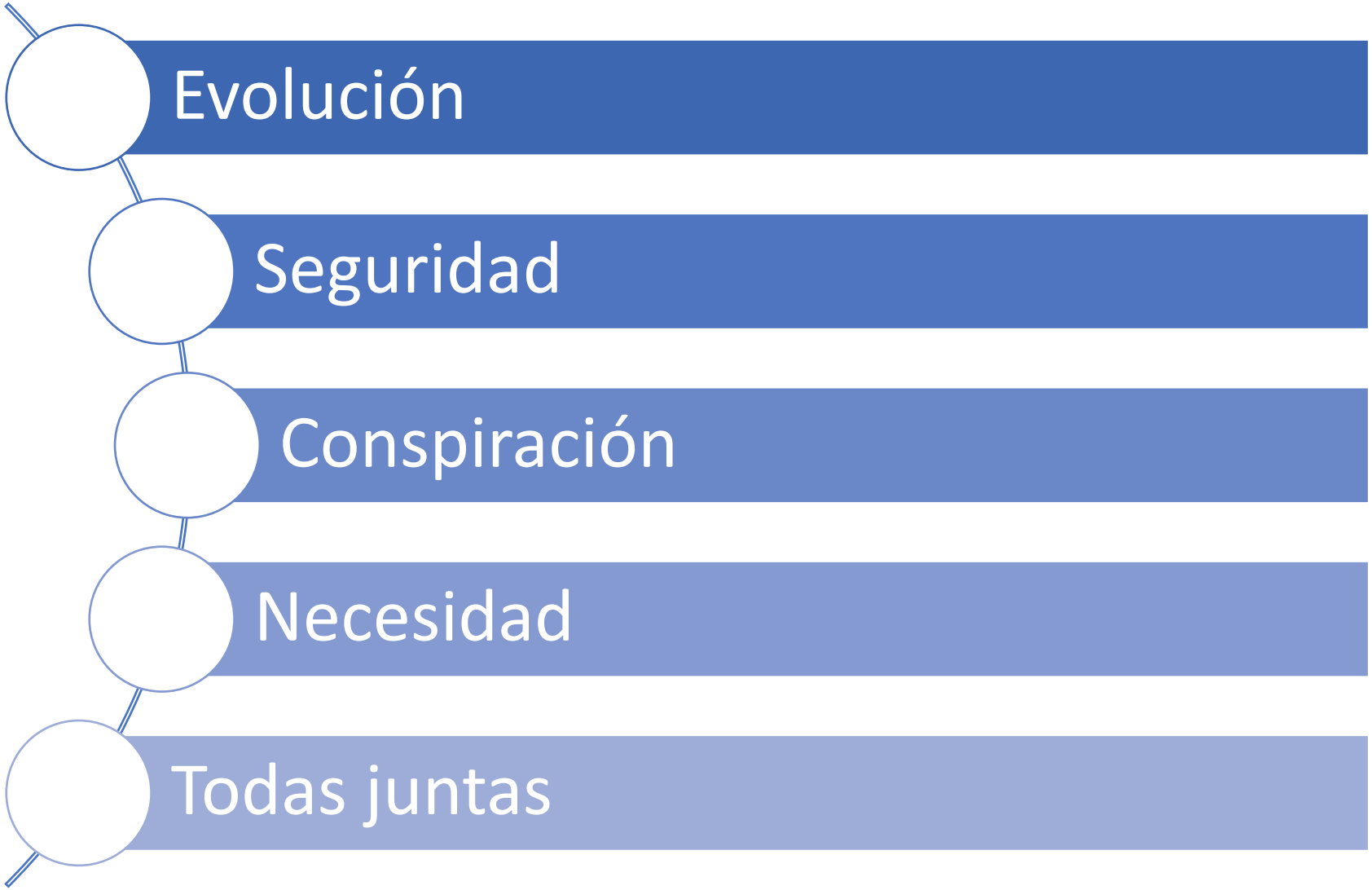


- Investigadores
- Usuarios
- Educadores
- Entusiastas -- Mathy Vanhoef / This amazing group!

Hola, les presento a WPA3!



Por qué estoy aquí?



Matématicas básicas

De la mismisima Wikipedia

- Entropy
  - In information theory, the entropy of a random variable is the average level of "information", "surprise", or "uncertainty" inherent in the variable's possible outcomes

In case of flipping a coin you would expect tails or he
Flipping a coin gives you an entropy of 1 bit

A dice has ~1.80 bits of entropy

Current information technology security best practices state that 96-bits of entropy should be safe for the foreseeable future while 128-bits is definitely safe.

Block cipher example… An easy one

A	B	C	D	E	F
F	A	B	C	D	E
E	F	A	B	C	D

Decrypt the following message using the table above: EFBD

E = F
F = A
B = C
D = E

Ciphertext = EFBD
Plaintext = FACE

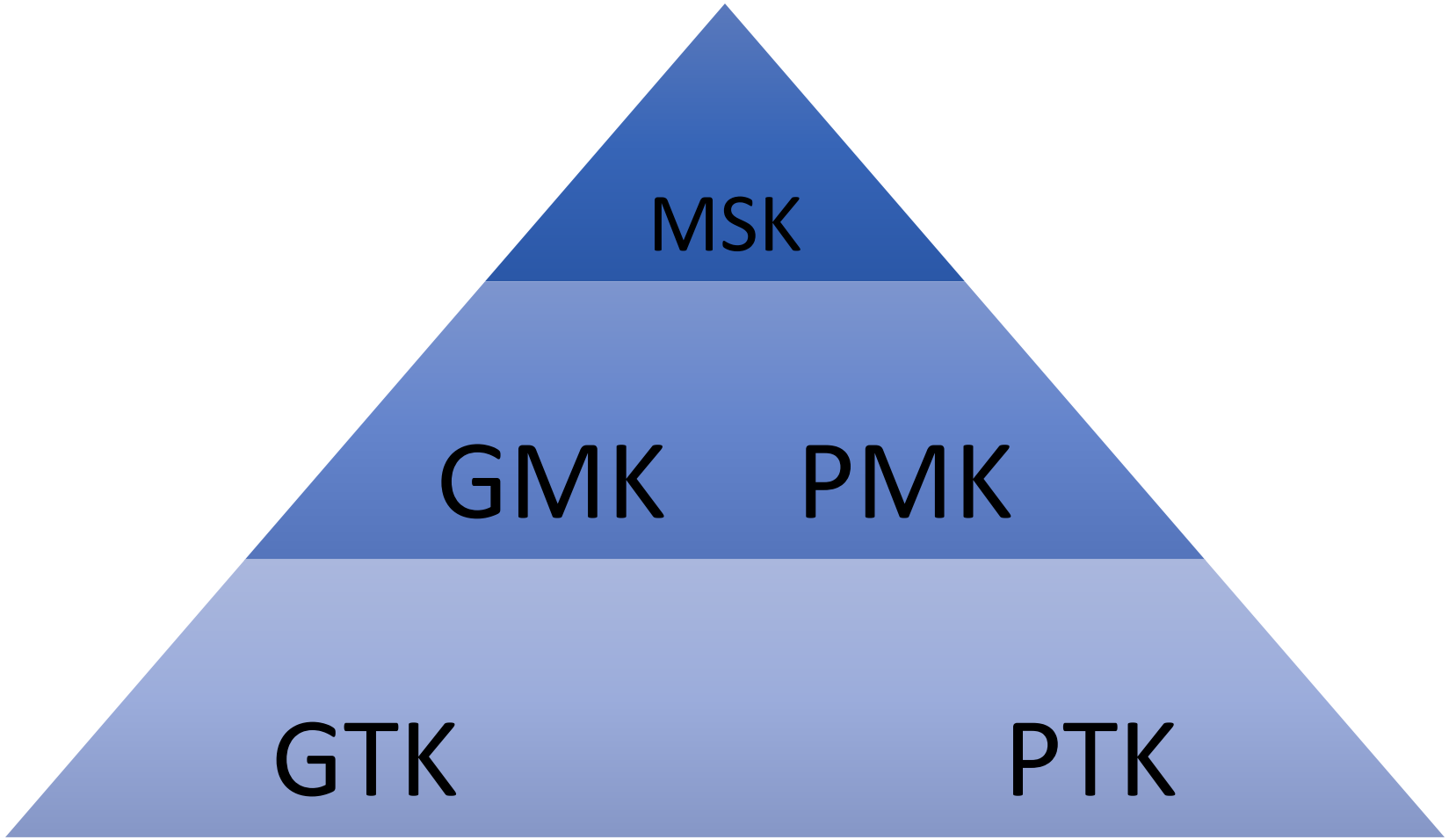
Ciphertext = Plaintext >> 1*

* Represents the Key

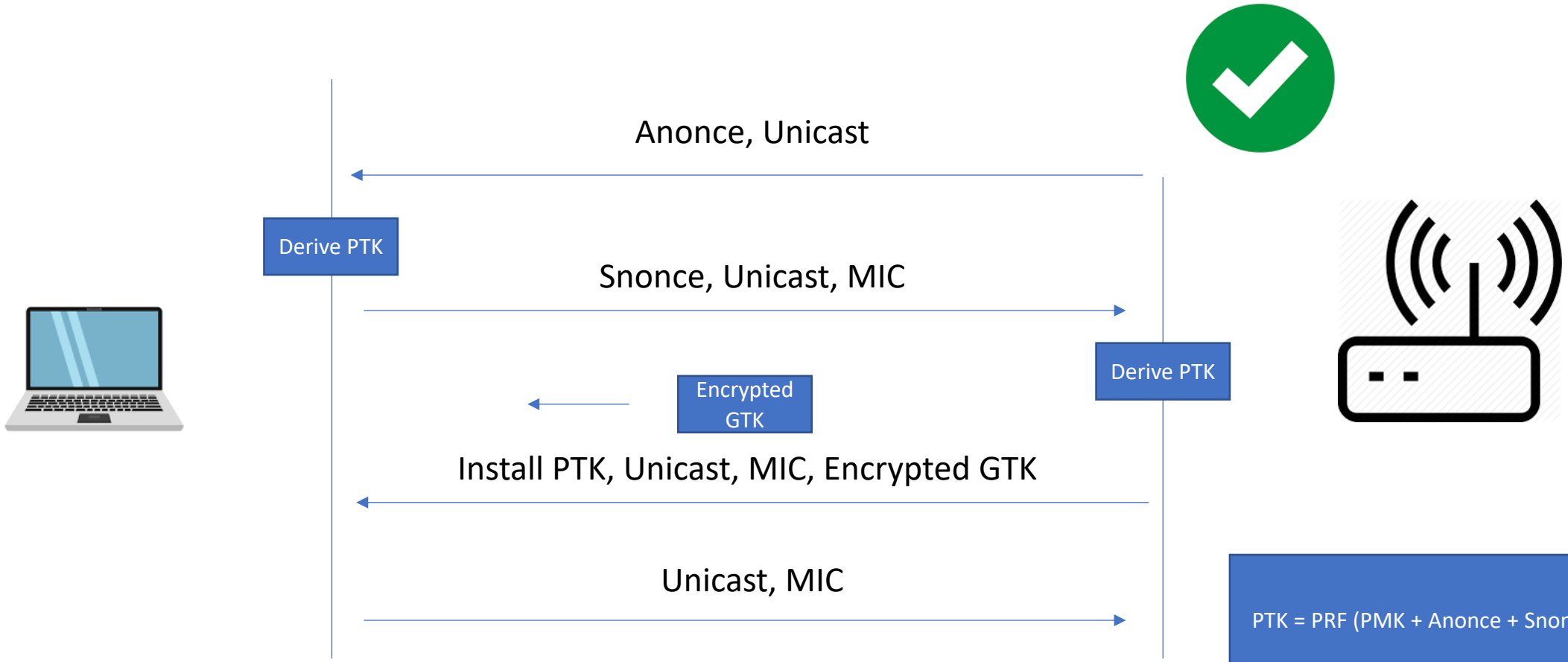
Inputs = Plaintext ^ Key
Output = Ciphertext

The longest the key, the most secure the protocol

RSNA Key Hierarchy



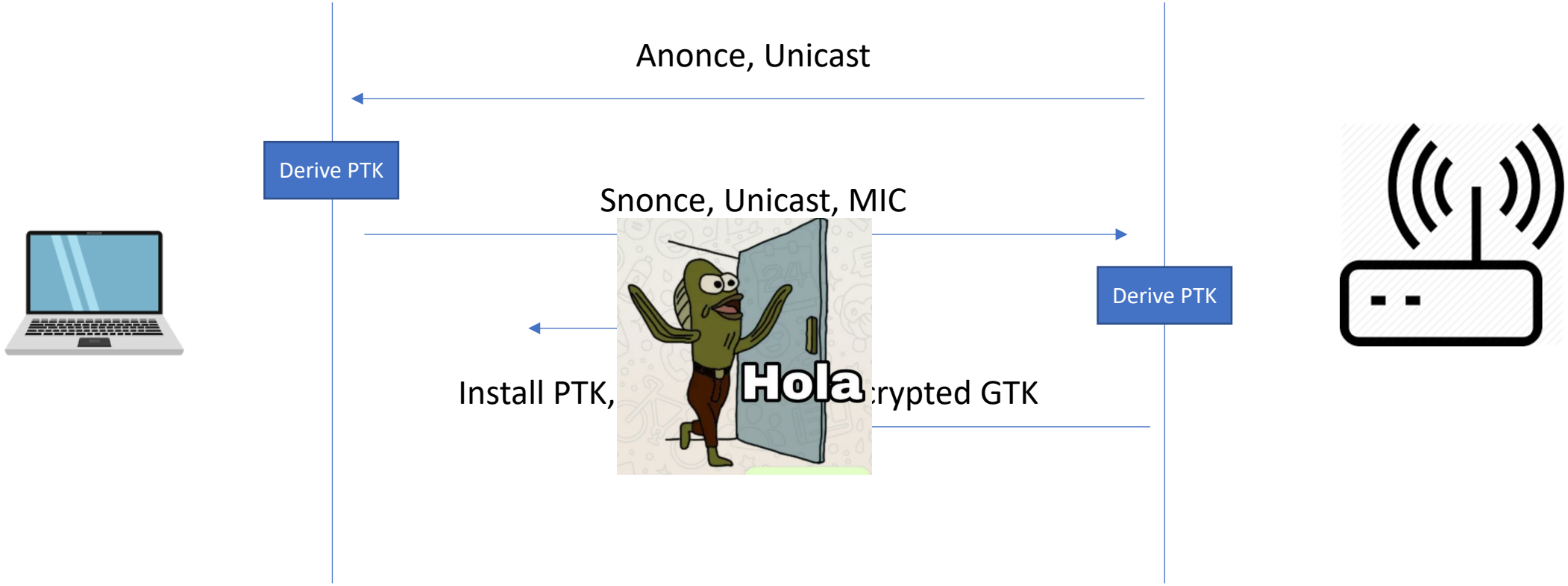
Un viaje al pasado inmediato… WPA2



PTK = PRF (PMK + Anonce + Snonce + AA + SA)

PMK = PBKDF2 HMAC-SHA1, PSK, SSID, 4096,256)

Todo bien hasta que llegó KRACK



Notas esenciales de Krack

- Key Reinstallation Attack
- El ataque funciona al manipular el mensaje 3 del 4 way handshake
  - Each time it receives this message (message 3), it will reinstall the same encryption key, and thereby reset the incremental transmit packet number (nonce) and receive replay counter used by the encryption protocol. **An attacker can force these nonce resets by collecting and replaying retransmissions of message 3 of the 4-way handshake**.
- Remember 802.11w?
- Remember 802.11h?

A little bit of KRACK

- *Message 1: Authenticator → Supplicant: EAPOL-Key (0,0,1,0,P,0,0, Anonce, 0, DataKD_M1) where DataKD_M1 = 0 or PMKID for PTK generation, or PMKID KDE (for sending SMKID) for STK generation*

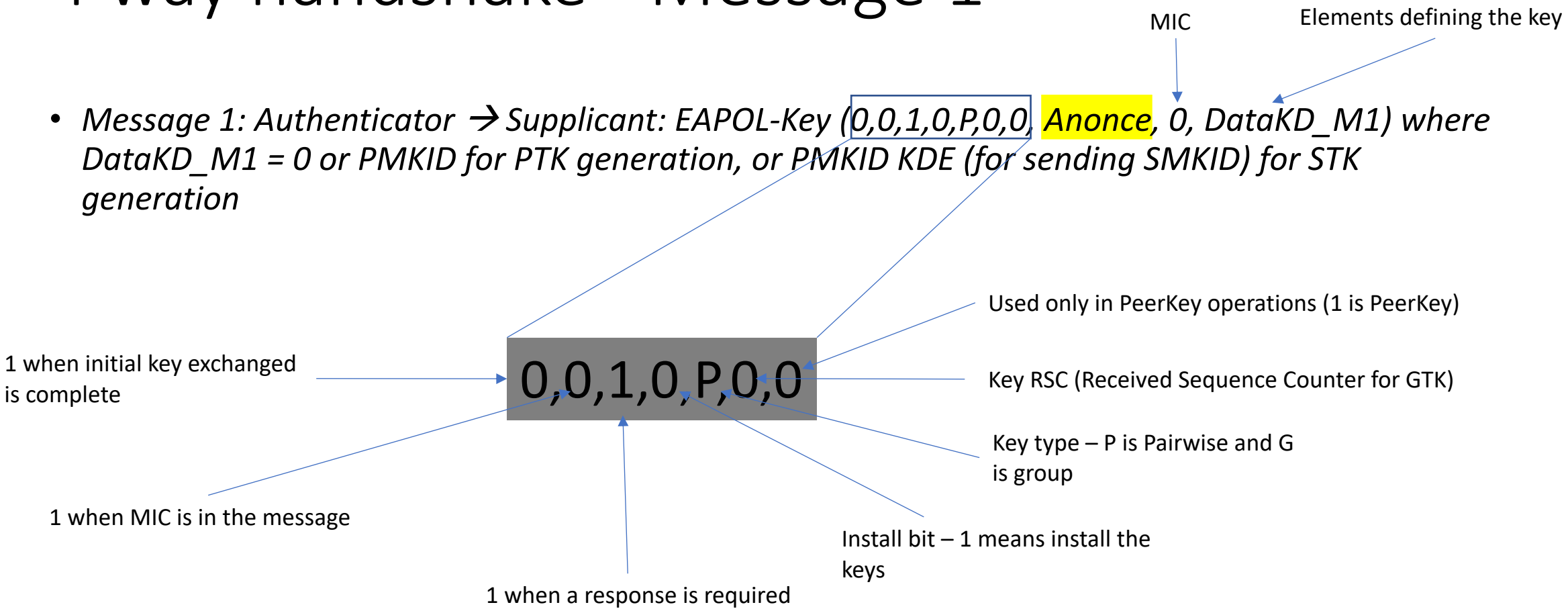
- *Message 2: Supplicant → Authenticator: EAPOL-Key (0,1,0,0,P,0,0, Snonce, MIC, DataKD_M2) where DataKD_M2 = RSNE for creating PTK generation or peer RSNE, lifetime KDE, SMKID KDE (For sending SMKID) for STK generation*

- *Message 3: Authenticator → Supplicant: EAPOL-Key (1,1,1,1,P,0,KeyRSC, Anonce, MIC, DataKD_M3) where DataKD_M3 = RSNE, GTK[N] for creating PTK generation or initiator RSNE, Lifetime KDE for STK generation*

- *Message 4: Supplicant → Authenticator: EAPOL-Key(1,1,0,0,P,0,0,0,MIC,DataKD_M4) where DataKD_M4 = 0*

4 way handshake - Message 1

- *Message 1: Authenticator → Supplicant: EAPOL-Key (0,0,1,0,P,0,0, Anonce, 0, DataKD_M1) where DataKD_M1 = 0 or PMKID for PTK generation, or PMKID KDE (for sending SMKID) for STK generation*



4 way handshake – Message 3

- *Message 3: Authenticator → Supplicant: EAPOL-Key (1,1,1,1,P,0,KeyRSC, Anonce, MIC, DataKD_M3) where DataKD_M3 = RSNE, GTK[N] for creating PTK generation or initiator RSNE, Lifetime KDE for STK generation*

The AP or controller can now send the GTK to the client and the install bit (bit 4) is set to 1

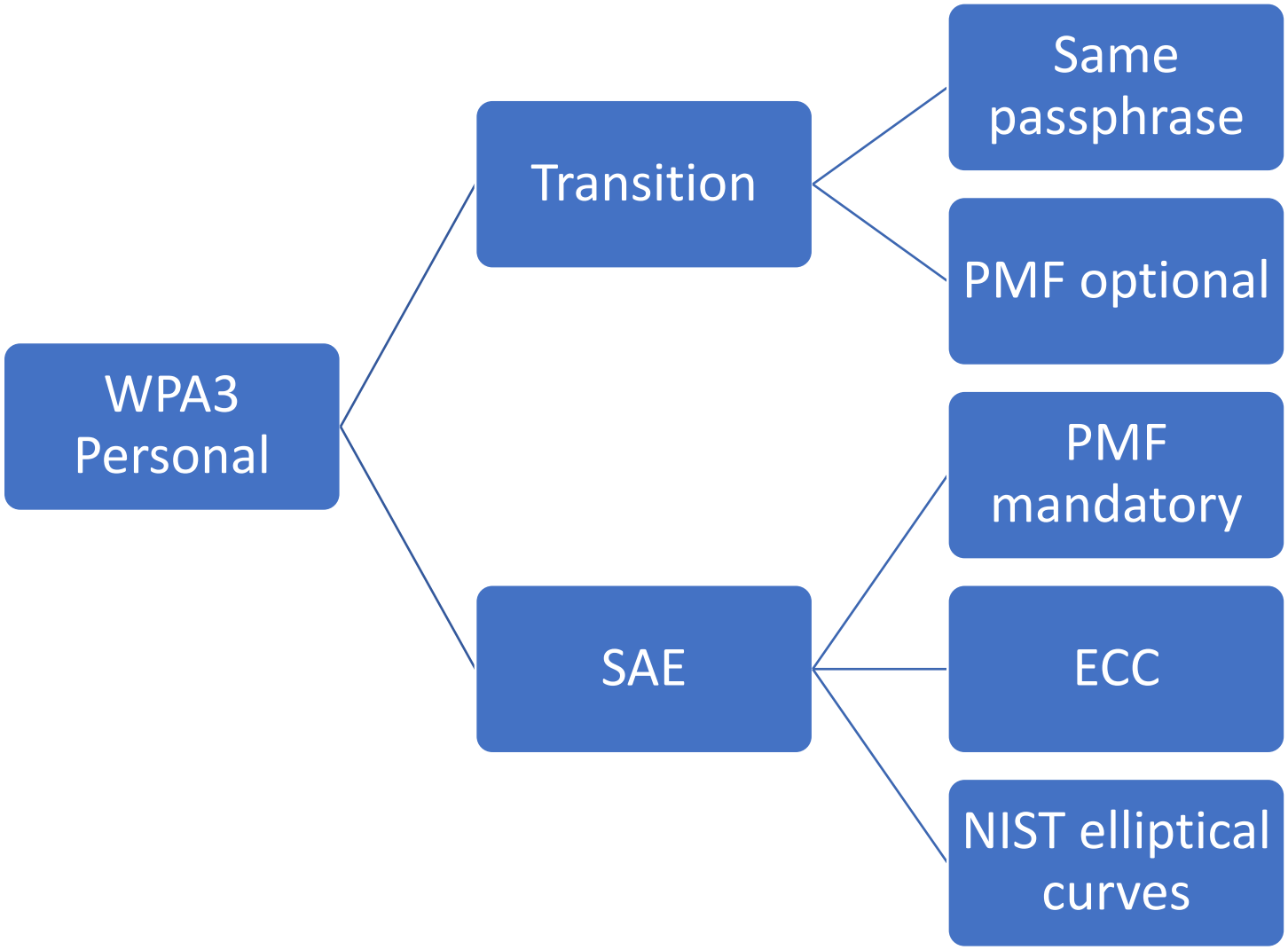
This is the point where KRACK attack operates

Más detalles (~~Victimas~~)

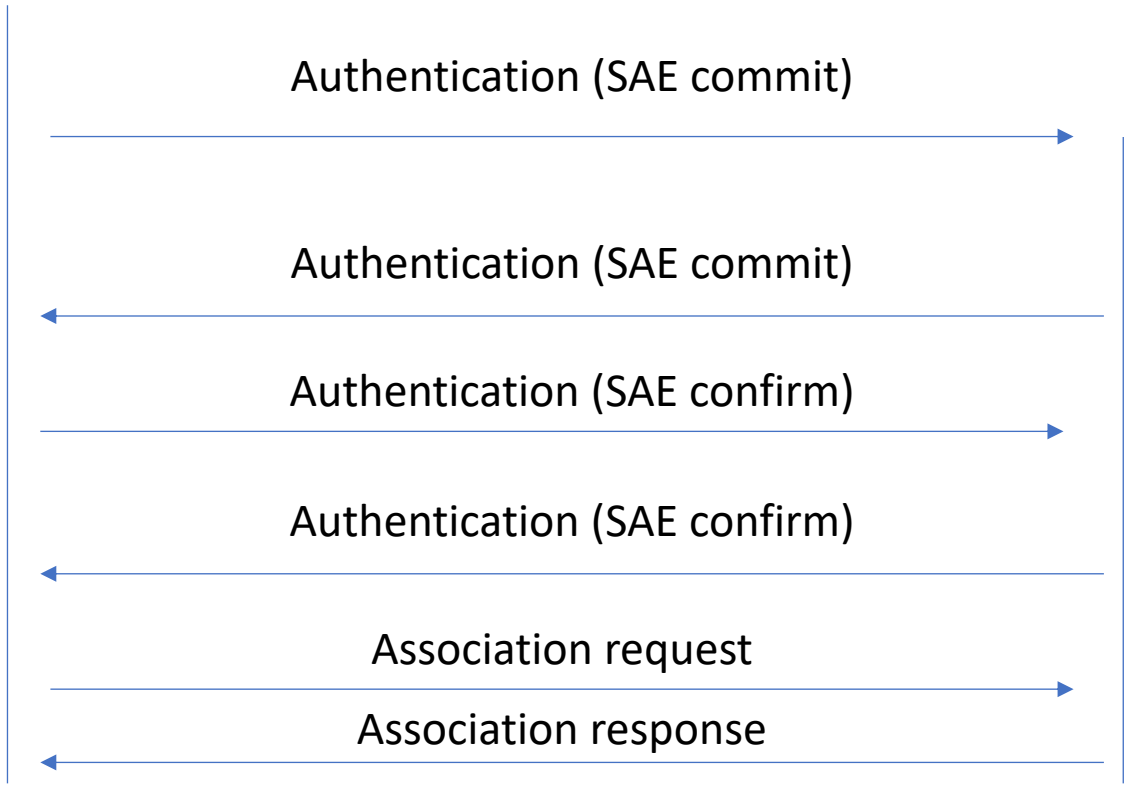
- Typical PTK 4 way handshake
- Peerkey 4-way handshake
- Group key handshake
- Fast BSS Transition (FT) handshake

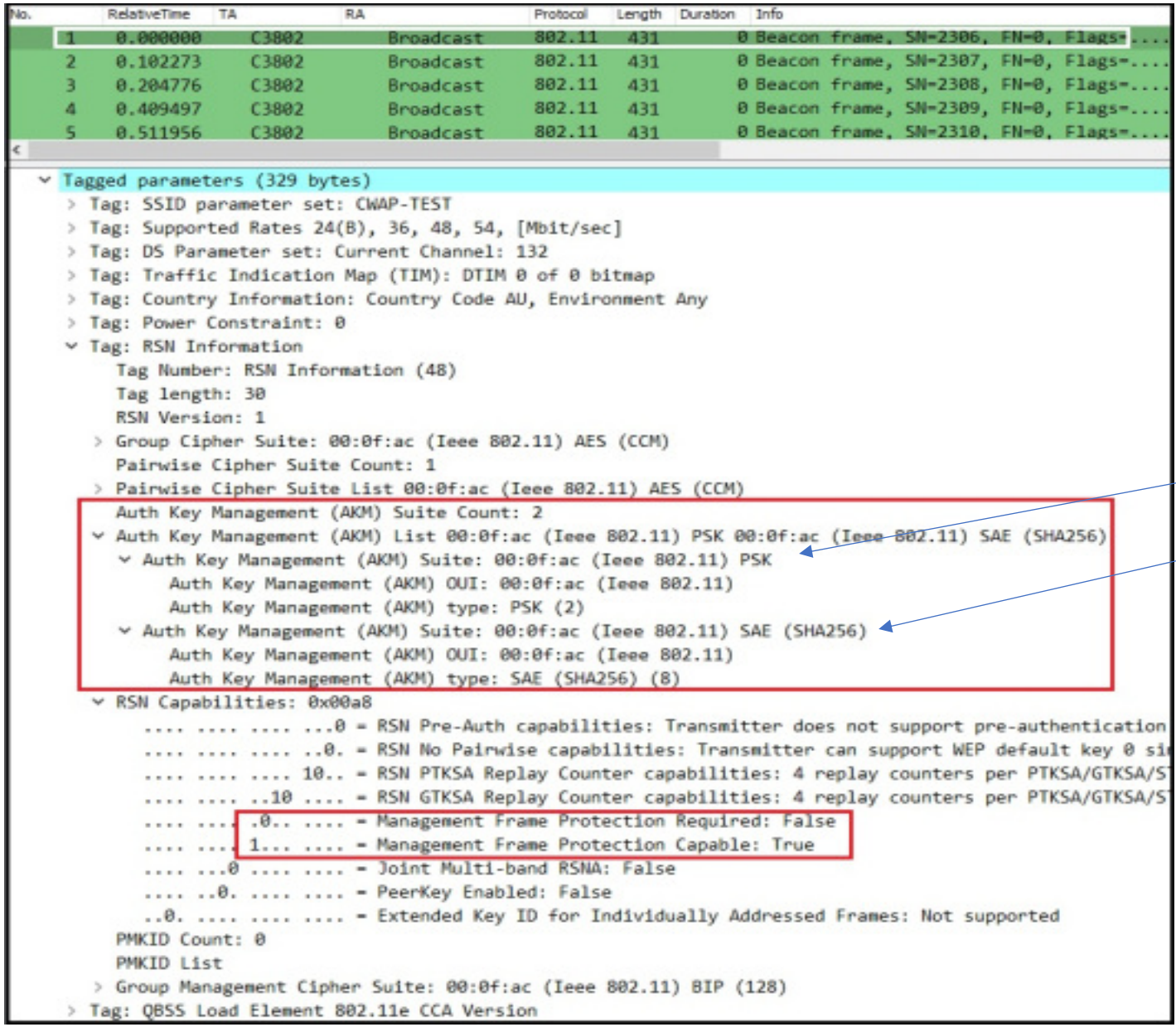
CVE-2017-13077: Reinstallation of the pairwise encryption key (PTK-TK) in the 4-way handshake.
CVE-2017-13078: Reinstallation of the group key (GTK) in the 4-way handshake.
CVE-2017-13079: Reinstallation of the integrity group key (IGTK) in the 4-way handshake.
CVE-2017-13080: Reinstallation of the group key (GTK) in the group key handshake.
CVE-2017-13081: Reinstallation of the integrity group key (IGTK) in the group key handshake.
CVE-2017-13082: Accepting a retransmitted Fast BSS Transition (FT) Reassociation Request and reinstalling the pairwise encryption key (PTK-TK) while processing it.
CVE-2017-13084: Reinstallation of the STK key in the PeerKey handshake.
CVE-2017-13086: reinstallation of the Tunneled Direct-Link Setup (TDLS) PeerKey (TPK) key in the TDLS handshake.
CVE-2017-13087: reinstallation of the group key (GTK) when processing a Wireless Network Management (WNM) Sleep Mode Response frame.
CVE-2017-13088: reinstallation of the integrity group key (IGTK) when processing a Wireless Network Management (WNM) Sleep Mode Response frame.

Entonces qué hay con WPA3?



Flujos


Authentication (SAE commit)
Authentication (SAE commit)
Authentication (SAE confirm)
Authentication (SAE confirm)
Association request
Association response
4 way
handshake



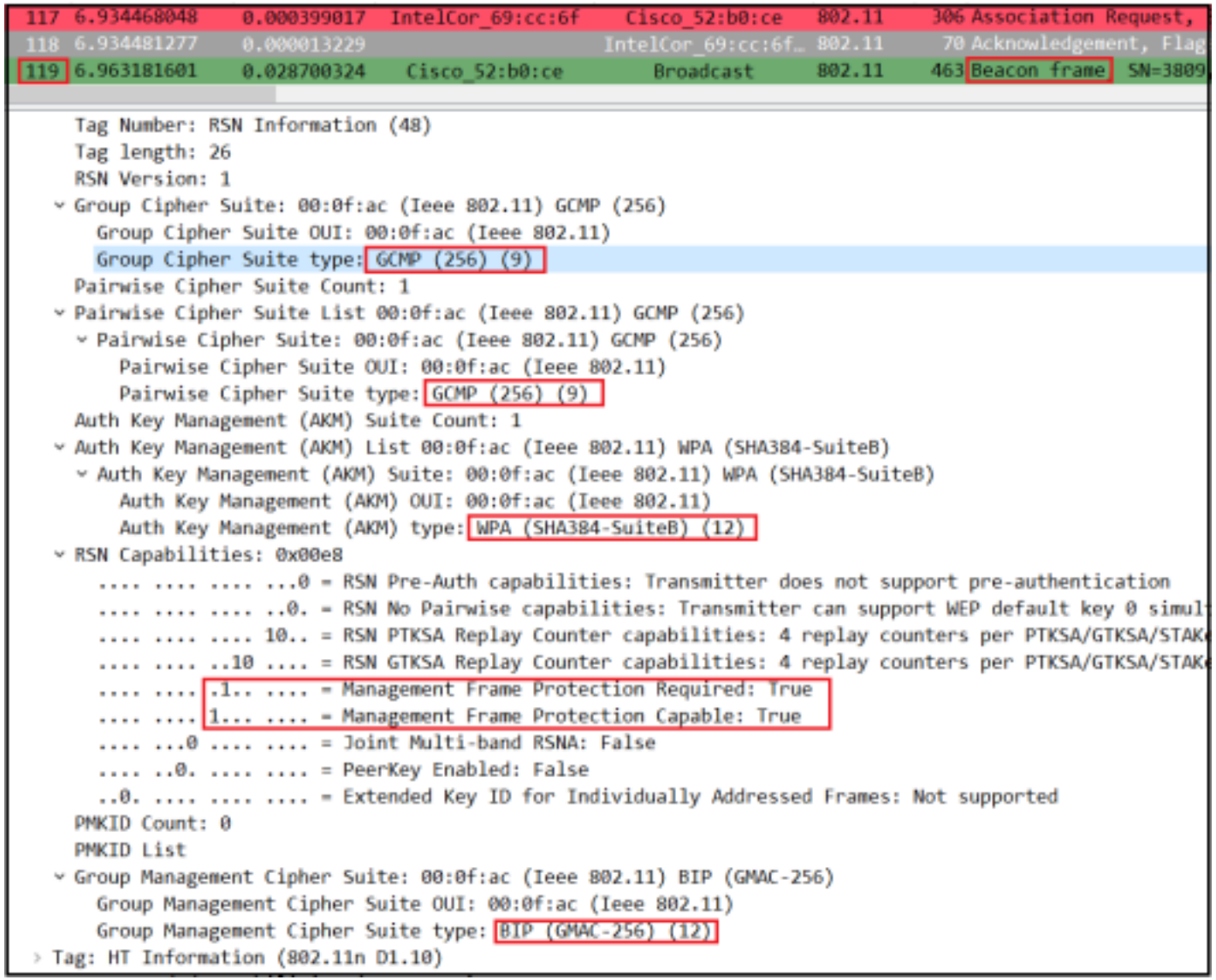
WPA2-PSK

WPA3-SAE

Entreprise

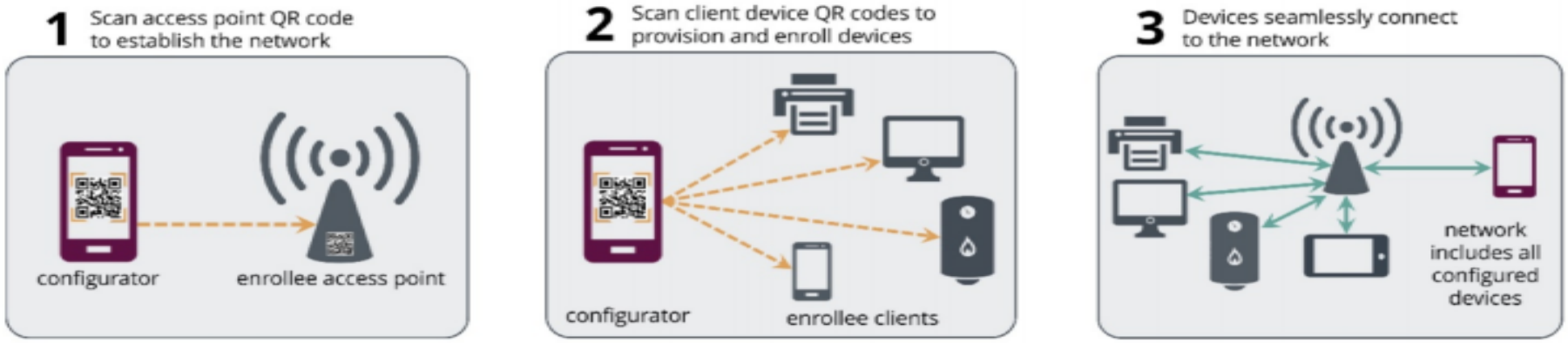
- 802.11w requerido
- EAP sigue en uso
- Viene en dos sabores. 128 bits y 192 bits
- Para 192 bits es necesario utilizar AES-256-GCM
  - Hashing
  - Key establishments
  - Digital signatures

AES-256-GCM Encryption and data authentication	SHA-384 Hashing	ECDH-P384 Establishment of keys	ECDSA-P384 Digital signatures


117 6.934468048 0.000399017 IntelCor_69:cc:6f Cisco_52:b0:ce 802.11 306 Association Request,
118 6.934481277 0.000013229 IntelCor_69:cc:6f… 802.11 70 Acknowledgement, Flag
119 6.963181601 0.028700324 Cisco_52:b0:ce Broadcast 802.11 463 Beacon frame SN=3809
Tag Number: RSN Information (48)
Tag length: 26
RSN Version: 1
Group Cipher Suite: 00:0f:ac (Ieee 802.11) GCMP (256)
Group Cipher Suite OUI: 00:0f:ac (Ieee 802.11)
Group Cipher Suite type: GCMP (256) (9)
Pairwise Cipher Suite Count: 1
Pairwise Cipher Suite List 00:0f:ac (Ieee 802.11) GCMP (256)
Pairwise Cipher Suite: 00:0f:ac (Ieee 802.11) GCMP (256)
Pairwise Cipher Suite OUI: 00:0f:ac (Ieee 802.11)
Pairwise Cipher Suite type: GCMP (256) (9)
Auth Key Management (AKM) Suite Count: 1
Auth Key Management (AKM) List 00:0f:ac (Ieee 802.11) WPA (SHA384-SuiteB)
Auth Key Management (AKM) Suite: 00:0f:ac (Ieee 802.11) WPA (SHA384-SuiteB)
Auth Key Management (AKM) OUI: 00:0f:ac (Ieee 802.11)
Auth Key Management (AKM) type: WPA (SHA384-SuiteB) (12)
RSN Capabilities: 0x00e8
....0 = RSN Pre-Auth capabilities: Transmitter does not support pre-authentication
....0. = RSN No Pairwise capabilities: Transmitter can support WEP default key 0 simul
.... 10.. = RSN PTKSA Replay Counter capabilities: 4 replay counters per PTKSA/GTKSA/STAK
....10 .... = RSN GTKSA Replay Counter capabilities: 4 replay counters per PTKSA/GTKSA/STAK
.... .1.. .... = Management Frame Protection Required: True
.... 1... .... = Management Frame Protection Capable: True
....0 .... = Joint Multi-band RSNA: False
.... ..0. .... = PeerKey Enabled: False
..0. .... = Extended Key ID for Individually Addressed Frames: Not supported
PMKID Count: 0
PMKID List
Group Management Cipher Suite: 00:0f:ac (Ieee 802.11) BIP (GMAC-256)
Group Management Cipher Suite OUI: 00:0f:ac (Ieee 802.11)
Group Management Cipher Suite type: BIP (GMAC-256) (12)
Tag: HT Information (802.11n D1.10)

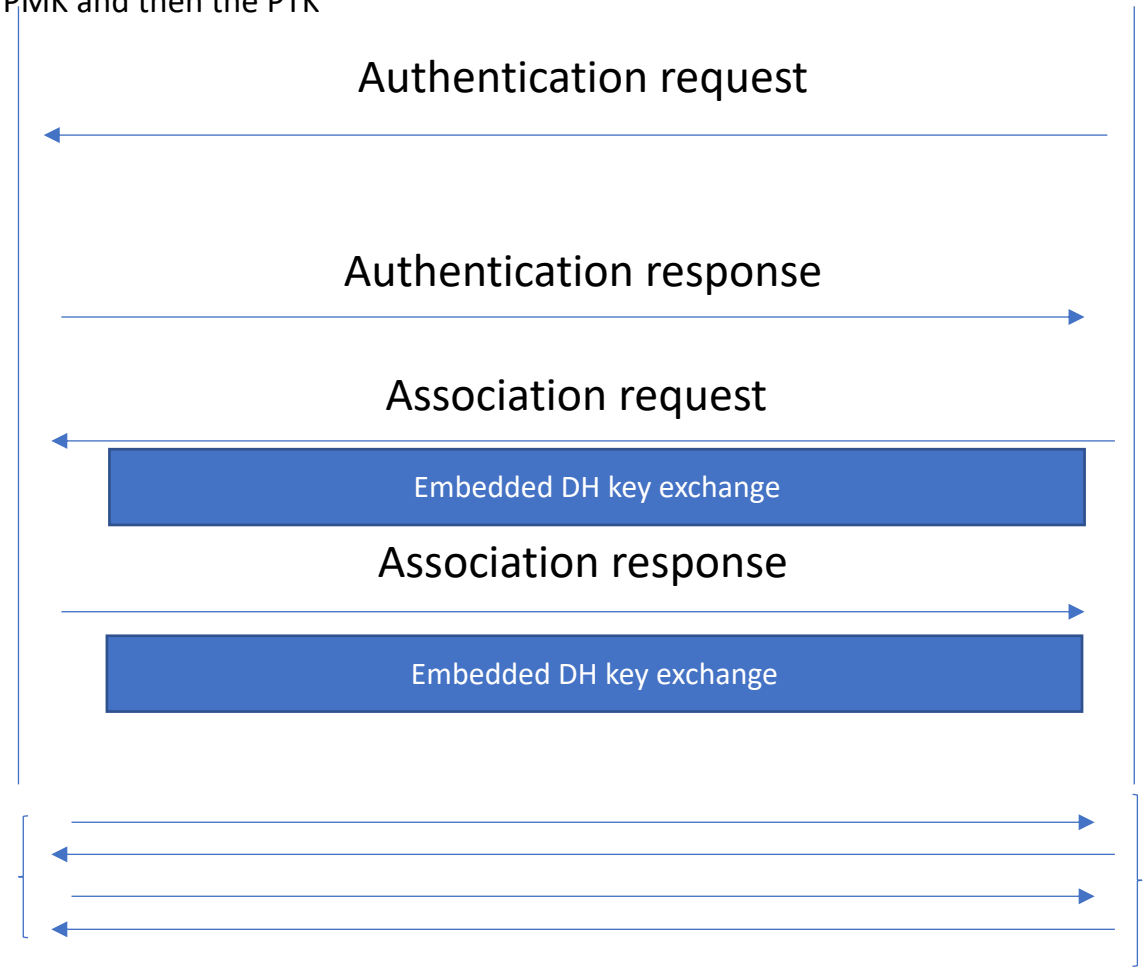
Wi-Fi Easy connect

- Aprovisionamiento a través de códigos QR
- Utiliza el protocolo DPP (device Provisioning protocol)
- Mas inteligente, mas fuerte que WPS
- Aprovisionamiento sencillo de dispositivos IoT
- Utiliza PKI
- Dispositivos sin interfaz grafica



OWE

- Opportunistic Wireless Encryption
- Short-term public keys
- Diffie-Helman to derive a PMK and then the PTK



Preguntas…