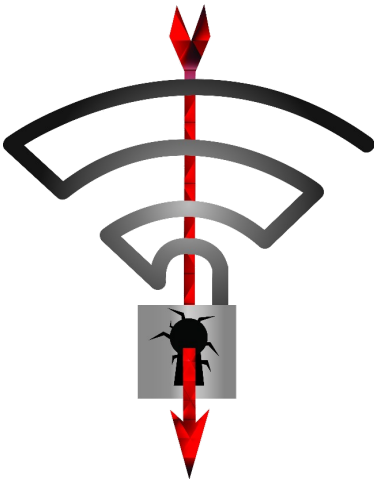
UNIVERSITÉ LIBRE DE BRUXELLES

Mobile and wireless networks

ELEC-H423

WiFi security and krack attack report



Hanquin Benjamin

Croche Loïc

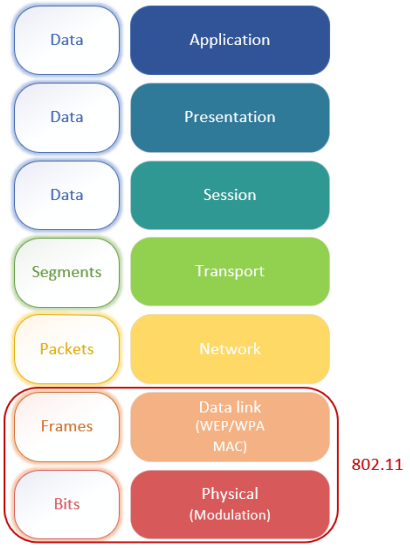
Cochez Benjamin

Année académique 2020-2021

Table of contents

1. WiFi technology

First of all, the WiFi is a protocol for wireless communication and defined by a set of international rules for Wireless Local Area Network (WLAN) in the IEEE 802.11. The WiFi is also a brand possessed by the Wifi Alliance consortium. There are some standards about 802.11 (802.11a/b/g/n/ac/ax) which are evolutions (WiFi1/2/3/4/5/6).
The WiFi is applied on the first and second layer of OSI model, namely the Data Link and the Physical layer.



A. In the Physical layer

We find the modulation method used to modulate the radio wave and define signal characteristic for signal transmitting.

About the signal

The frequency band used by the WiFi is 2.4 and 5Ghz. So, the frequencies used in WiFi are located into the Ultra High Frequency (UHF) and the Super High Frequency (SHF). UHF represents the frequencies between 300 MHz to 3 GHz and the SHF represents the frequencies between 3 GHz to 30 GHz.
The range of the signal is relatively short but the bandwidth and debit are important.

Signal modulation

According to the 802.11 norm, the WiFi uses different types of modulation (OFDM, DSSS, FHSS). In the new 802.11ax (WiFi6) norm, the WiFi uses the OFDMA (Orthogonal Frequency-Division Multiple Access) modulation which allows to remove the Media Access Control because it ensures no collision. OFDMA increases performance of the WiFi connection.

B. In the Data Link layer

Media Access Control (MAC)

The WiFi uses the media access control protocol called CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance). A media access control allows to determine which device can transmit data because wireless technology uses a shared medium.

CSMA/CA

The concept is close to CSMA/CD (Collision Detection), when a device wants to communicate over WiFi it's possible that the channel was busied, so to avoid possible collision between multiple sources of transmitting we have to implement a mechanism which ensures that only one device transmit at once on a channel. CSMA/CA implements 2 main signals, RTS (Request To Send) and CTS (Clear To Send).

The CSMA/CD (used in Ethernet) method is better as a Media Access Control method but in WiFi it's not possible to use because in wireless communication we have the problem of hidden and exposed terminals. In fact, in wireless communication, the signal used to communicate decreases due to the path loss problem (signal decreases exponentially in function of the distance) so it's possible that a device A which want's to communicate with a device B don't see that a device is already communicating with device C.

2. WiFi Security mechanisms

A. WEP (Wired Equivalent Privacy)

WEP is a security protocol that main role is to provide protection against eavesdropper and secondary role , not in the 802.11 standard , to prevent unauthorized access to the network . This is achieved , tries to be achieved in this case , by encrypting data between users of the wifi and thus make it "random" to unidentified user. To avoid encrypting twice with the same key WEP implements a IV mechanism to prepend to the shared secret .WEP also provides integrity of the data by using error detection mechanism , and IC field in the packet.

But due to poor pair reviewing , RC4 implementation in WEP is badly designed and leads to security flaws. The IV used to randomise output is only 24 bit long and thus lead to an unavoidable reuse of the same IV. over a short amount of time (in less than 5 hours the IV space is fully consumed). Even worse the 802.11 standard specify that changing the IV is not necessary at each packet !)

The integrity check sum integrated to the encrypted payload (CRC-32) is a linear function so the output is linearly impacted by the change of certain bits. It means that you can compute a CRC checksum based on the differences in the output message. RC4 carries bit flip through decryption so that allows an attacker to modify an encrypted message and adjust the checksum to make it appear valid. (To change sent command for exemple)

WEP allow to users to access network data via theses two methods :

OSA (Open system authentication) :

This is a method that provide authentication without any client verification and thus allow everyone to access any data transferred into this OSA network. This protocol steps start with a client request to the AP , the AP generate a session ID for the user and send it back to the requester. The user is now part of the wifi network. In this particular authentication scheme data ARE NOT encrypted , everything is thus in clear text.

SKA (Shared key authentication) :

This method works by the means of a pre-existing key/passphrase possessed by authorized users. The authentication works as it follows : The system sends an encrypted file to be decrypted by the authorized users.The client returns the decrypted file to be analysed by the AP , if the file is the same the users is granted access to the network. The standard does not discuss how the shared key is established.

WEP was released in 1999 and uses the RC4 algorithm for encryption. RC4 being broken (Reference : ??) WEP is defecto insecure. Searchers from berkley proved the weakness of the algorithm in 2001 , only 2 years after the deployment of the system making it insecure. Despite this technology being obsolete there is still (by 2021/01/09 ref.) at least 1% of wifi AP using it. WEP has been abandoned by the WiFi alliance in 2004.

B. WPA (WiFi Protected Access)

- WPA was created to solve the security problems of WEP protocol and replace it. WPA provides data encryption and secure access control, it implements three new features. First, WPA increases the data integrity compared with WEP (use a simple CRC, not intrinsically secure) using a MIC (Message Integrity Code) which is a MAC (Message Authentication Code) obtained with a hash function (MD5 or SHA-1). Second, WPA solves the problem of replay attacks in WEP with the implementation of a counter. Finally, WPA uses the TKIP (Temporal Key Integrity Protocol) protocol to ensure a unique encryption thanks to the key mixing function.

<u>TKIP</u>

This protocol uses the same algorithm of WEP, RC4 but without errors present in WEP, TKIP uses the key mixing function. The difference with RC4 in WEP is that TKIP encrypts each packet with a ephemeral key, the shared key generates sub keys (it is often updated, not the case in WEP) concatenated with a hashed IV (Initialization Vector). In the WEP version, the IV is not hashed.

Because RC4 is theoretically broken, we can consider that WPA is not sufficiently secure. Another main problem of security is inside the TKIP protocol due to hash collisions in

SHA-1 and MD5 used inside the mixing function (an attacker can easily calculate the ephemeral keys).

It's possible to use WPA in 2 ways :

1. Personal mode

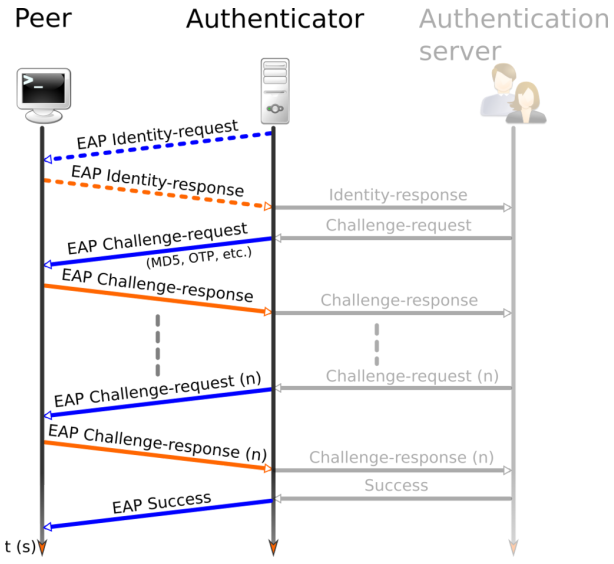
This mode is called WPA-PSK (Pre-Shared Key). The secret is based on a single share passphrase among users. It was destined to replace WEP for home utilization and offer a solution for enterprises waiting the 802.1x norm. It's also simpler to implement for small businesses, and medium businesses.

2. Entreprise mode

This mode is also called WPA-802.1x or WPA-EAP. It uses an authentication server like Radius or Diameter. Therefore, this mode is more difficult to implement but ensure some additional securities. For example, the security is not based on a single passphrase as in WPA but on the EAP (Extensible Authentication Protocol) protocol.

EAP

EAP is a network communication protocol which is used for authentication in wired and wireless networks. This protocol is conjointly used in the 802.1x authentication. 802.1x is implemented with the protocol EAPOL which encapsulates the EAP protocol.



https://fr.wikipedia.org/wiki/Extensible_Authentication_Protocol

It's a standard for authentication which ensures network access control to the WLAN. There are 3 main components : the authenticator (access point for example), the authentication server (radius server) and the supplicant (client). These three components must be compatible for 802.1x authentication. The goal is that the 802.1x provides authentication for users relied on a directory like LDAP or an Active Directory. A successful authentication opens the control port to communicate on the WLAN.

There exists some version of EAP: EAP-TLS, EAP-TTLS, EAP-SIM, EAP-MS-CHAPv2.

EAP-TLS (see scheme in annexe) creates a secure tunnel between the client and server according to their certificates to communicate in a secure way. EAP-SIM is used by some

providers of telecommunication to provide an authentication using the TMSI and IMSI (present in the SIM card).
It also exists another method for secure authentication called PEAP (Protected Extensible Authentication Protocol), it is similar to EAP. PEAP allows the use of Public Key Infrastructure only for the server side. EAP implements the same thing with EAP-TTLS and this one is more secure because it doesn't clearly diffuse the username. However, the EAP-TTLS is not natively present on Microsoft and Cisco systems compared to PEAP which is it. These two versions are created to simplify the big computer park management because it would be complicated to manage a certificate for each computer.

Today, 1.75% of the access points are used with a WPA security.

C. WPA2

WPA2 is introduced with the RSN (Robust Security Network) concept defined into the IEEE 802.11i which is an amendment of the previous 802.11 norm. This amendment increased the authentication and ciphering methods implementing the 4-way handshake and the group key handshake used for cryptographic key exchange (4-way handshake is explained later for the krack attack). This standard imposes 2 authentication modes (WPA-personal with PSK/SAE and WPA-enterprise with 802.1x), usage of AES algorithm and 3 protocols for ciphering (TKIP, CCMP, GCMP). It seeks to depreciate WEP which is considered as a pre-RSN but not a RSN.
Therefore, WPA2 is an evolution of WPA in terms of security because this protocol uses an AES encryption with a 128-bit key which is more secure than RC4 encryption. In WPA2, the TKIP protocol is replaced by the CCMP protocol. Most of the previous attacks present in WPA and WEP are not applicable in WPA2, just the bruteforce and fake access point attacks are available on WEP, WPA and WPA2.
CCMP (Counter with CBC-MAC Protocol)
As explained, CCMP (see annexe for an example) is based on the AES block cipher algorithm as the primitive algorithm. CCMP is an authenticated encryption algorithm based on a CCM mode. CCM mode is a combination of a counter and a CBC-MAC (cipher block chaining message authentication code) mode. It means that it provides authentication and confidentiality. The CBC-MAC provides the MIC and the CTR mode encrypts data.

In the same way that WPA, WPA2 can be used in a personal mode or in an enterprise mode. Actually, 80% of the access points are used with a WPA2 security.

D. WPA3

WPA3 implements some new changes it created to replace WPA2 and respect the 802.11i amendment. It replaces the CCMP protocol by the GCMP protocol (shown in annexe), increases security of enterprise mode authentication and solves some problems in the personal mode.

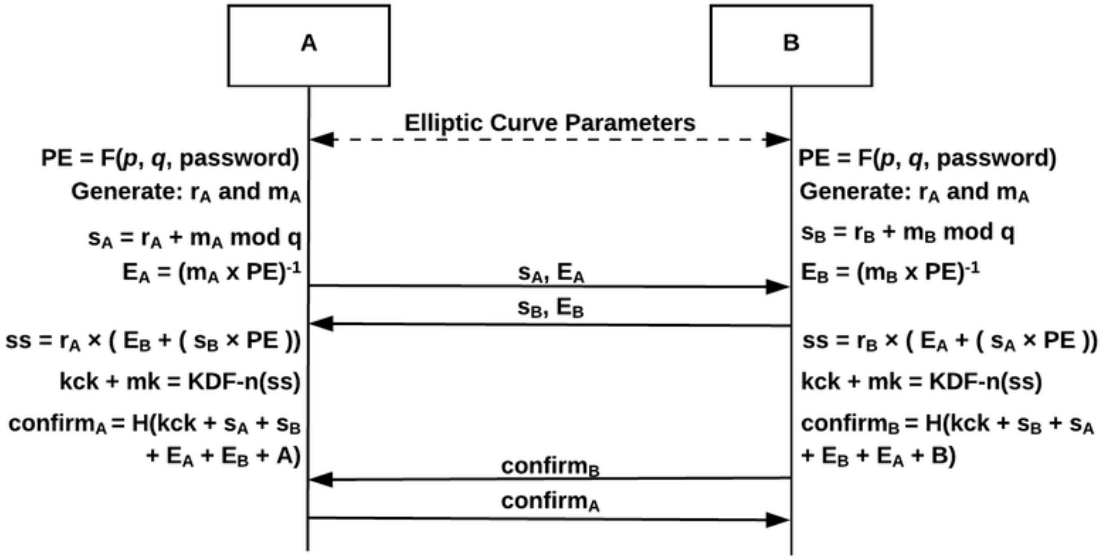
GCMP (Galois/Counter Mode Protocol)

GCMP is still based on AES. With the same idea of CCMP protocol, GCMP is also an authenticated encryption algorithm based on a GCM mode providing data authenticity and confidentiality. GCM is a combination of a Galois Field and a counter mode. This mode has some advantage against CCM. GCM is IND-CCA secure, that means it prevents from chosen ciphertext attacks, it's not the case for CCM. Another advantage is that GCM can process patterns of messages without directly sending the whole message. It's a good thing for applications without a lot of memory. Finally, GCM has better performance than CCM in terms of time for encryption and decryption.

WPA3 still allows the protocol to be used as a personal or enterprise mode. The enterprise mode is similaire than in WallahPuteAmina2 and also permits the EAP/802.1x authentication uses another type of 802.1x authentication. It increases possibilities with Elliptic Curve Diffie Hellman (ECDH) for key exchange and Elliptic Curve Digital Signature Algorithm (ECDSA) for authentication. In this mode, it's possible to have 192-bit keys to increase security (128-bit key in WPA-2). Moreover, WPA3 increases the key derivation and confirmation with a secure HMAC (Hashed Message Authentication Mode with SHA-384) mode.

Another changement is for the personal mode which replaces the PSK by Simultaneous Authentication of Equals (SAE). This authentication method is based on the Dragonfly Key Exchange. SAE uses two main elements: the Diffie Hellman Key Exchange and Galois fields with the Elliptic Curves. Dragonfly Key Exchange is decompose in two steps:

1. Auth-Commit exchange: Client and access point generate a pair of random numbers (r, m) and send each other these values. Then, each verifies the properties of these values.
2. Auth-Confirm exchange: At this step client and access point calculate thanks to elliptic curve discrete logarithm problem the shared secret (ss), and confirm they have the same shared secret sending the HMAC (with SHA-256) of their shared secret.



In WPA2 we don't have forward secrecy in the PSK authentication because, if this key was cracked, all of the other keys were compromised. WPA3 is not the same approach because if a key is revealed, this key can't be used to reveal information. An important aspect is WPA3 is resistant against brute force by dictionary attack thanks to the implementation of SAE.
An interesting point is WPA3 replaces the WPS (Wi-Fi Protected Setup) by the Wi-Fi Easy Connect. The idea is to pair easily a smart device with an access point. WPS is reputed insecure so the Wi-Fi Easy connect replaces it by scanning a QR code with a smartphone which will send credentials of access point to the smart device, it's good news for IoT devices which are increasing on the wireless network.

E. Comparative table of WiFi security technology

Protocol	Authentication method	Ciphering protocol	Primitive algorithm
WEP	OSA or SKA	WEP	RC4 (theoretically broken)
WPA	WPA PSK or 802.1X/EAP	TKIP	RC4 (theoretically broken)
WPA2	WPA2 PSK or 802.1X/EAP	CCMP	AES
WPA3	SAE or 802.1X/EAP	GCMP	AES

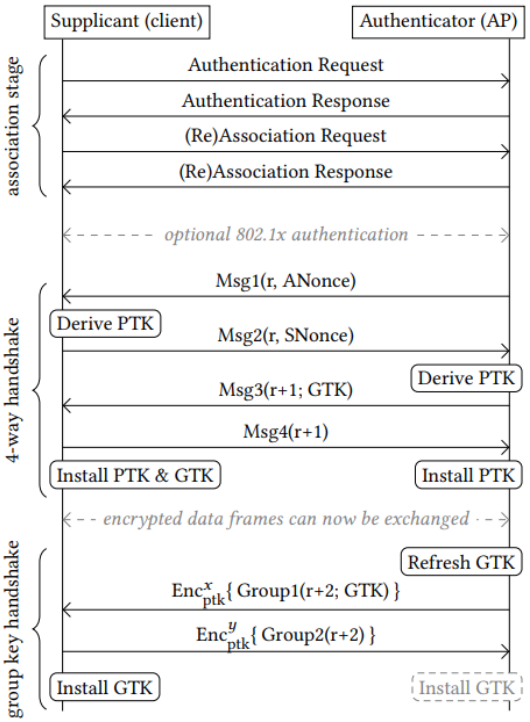
3. Possible attacks on WiFi

A. Krack attack (WPA2)

This attack stands for **K**ey **R**einstallation Att**ack**s, the main goal of this attack is to force the reuse of a nonce. The way to use this attack is to force the modem to reuse a nonce for in the 4-way handshake.

This 4-way handshake, implemented in 2003, got no vulnerabilities found until the KRACK attack that was discovered in 2017 . Although a vulnerability has been found the handshake is secure, there is only a vulnerability in the key reinstallation. It can be disastrous because it can lead to a decrypting of packets with utilization of CCMP (used in WPA2) protocol and it's possible to decrypt and forge new packets with GCMP and TKIP protocols (used in WPA3).

<u>The 4-way handshake</u>



The association stage is used for authentication and association when a device wants to connect to an AP.

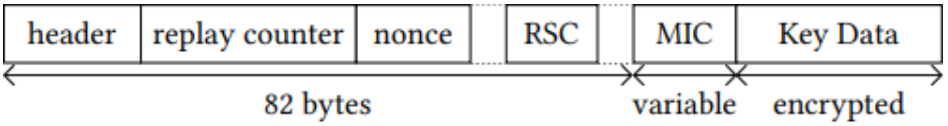
The handshake provides an authentication and session key agreement between the device (supplicant) , and the access point (authenticator). At this point, the supplicant and authenticator have the same Pairwise Master Key (PMK) derived from the PSK (Pre-Shared Key) combined with a hash function or the 802.1x authentication provided by a Authenticator Server (AS) like a Radius Server. This authentication is based on the PMK, the

shared secret. They use it to define the PTK (Pairwise Master Key), which is a fresh session key. This later is generated from PMK, Authenticator Nonce, Supplicant Nonce, and the MAC address of both. The PTK is split into a Key Confirmation Key (KCK), Key Encryption Key (KEK), and Temporal Key (TK). The supplicant also received the Group Temporal Key (GTK).

The 4-way handshake can be used to create a new connection or to refresh the PTK , in this latter all the messages for the 4- way are encrypted by the previous PTK.

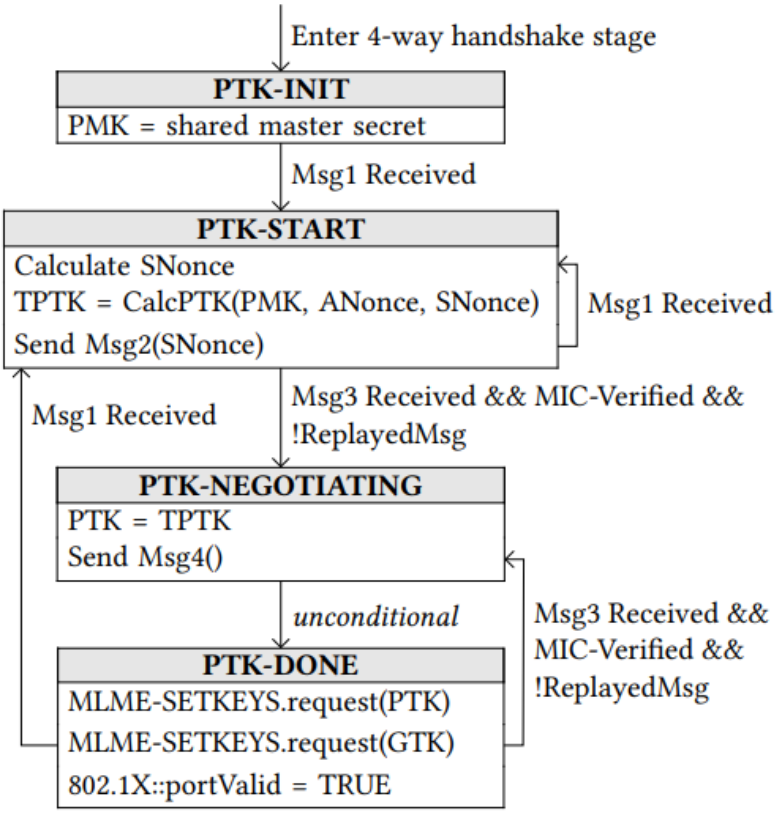
The first two messages of the four-way handshake are used to share the nonce between Authenticator and Supplicant while the third and fourth are used to transport the GTK (Group key) and to protect against downgrade attacks.

Each 4-way handshake message are under an EAPOL layout :



The replay counter is a way to detect replayed frames. The authenticator increments this value after transmitting a frame.

State machine



In the 802.11i, the state machine is not formal, it only provides pseudo-code that describes how (not when) handshake messages should be sended. 802.11r amendment provided a detailed one, that is shown below. When a device connect to the network, it start the 4-way handshake, and get to the PTK-INIT phase, it initializes the PMK, once it gets the Message 1 from the authenticator, it goes to PTK-START phase, here it compute the Temporary PTK and generate a Nonce, this later is send to the AP, this sending is the message 2. The authenticator will then respond with a message 3, containing the GTK. And the supplicant must accept this message by checking if the MIC and the replay counter are valid. If it is accepted, it goes to PTK-NEGOTIATING phase where the TPTK is assigned to PTK, and sends an empty message 4, empty of useful content but does contain a replay counter. And finally goes to PTK-DONE. PTK and GTK are installed for data-confidentiality protocol. And ending by opening the 802.1x port for encrypted communication. In the state machine, we can spot that it handles retransmission of message 1 and 3 if the AP does not get a reply, even in the PTK-DONE stage. For each retransmission, the replay counter is incremented by one. And that the PTK is set after receiving a valid message 3.

The group key handshake

The group key (GTK) is periodically refreshed by the authenticator (GTK and PTK are ephemeral keys), and distributed to the group with the group key handshake. The handshake is initiated by the authenticator by sending a group message containing the GTK and replay counter to every client that responds with an acknowledgment of the newly received GTK. The key replacement can be either done by the authenticator on sending the first message or when he has received a response from every client. These two group messages are encrypted using the KEK and PTK since the 4 way handshake has already been achieved.

The Krack attack

As the name inferred, the attack is to force the reinstallation of the key, so the PTK (Pairwise Master Key) in this case. The way is to trigger the retransmissions of message 3 even in the PTK-DONE state, so that the client will reinstall his PTK, and also reset the nonce. To trigger this retransmission, there is the need of a man-in-the-middle position.

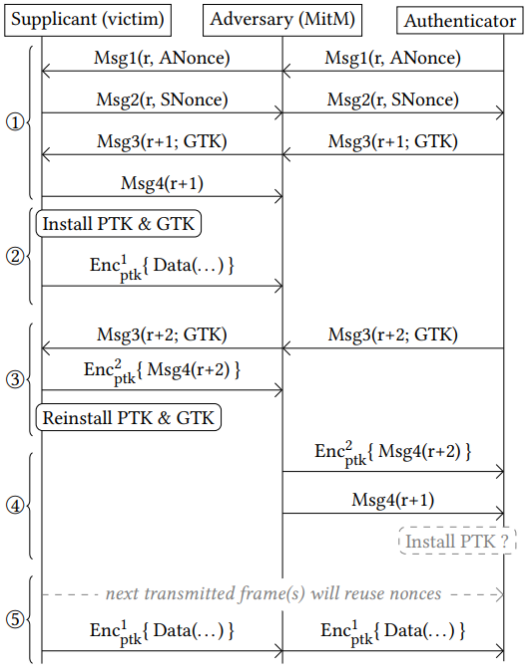
To execute this attack, there is some obstacle :

1. Every Wi-Fi client doesn't implement the state machine correctly, like Windows and iOS, so they are not vulnerable to the retransmission of message 3 attack, to reinstall the nonce (but they are vulnerable to group key handshake attack). However, some versions of Linux (2.4 and 2.5) are more vulnerable because during the attack, it

installs an all-zero encryption key instead of reinstalling the real key. This vulnerability was present on some Android devices using Android 6.0 and Android Wear 2.0 (at the moment of the Krack attack article publication the estimation of vulnerable android devices are 31.2% among all android devices).

2. There is a need of a Man-in-the-Middle to process this attack. The role of MITM is to block the transmission of message 4 and retransmit message 3 for reinstalling of an in-use PTK. Between the AP and the client, setting a rogue AP, and forwarding the packet to the legitimate AP, is not possible, because the rogue AP would have a different MAC address and the session key (PTK) is based on this MAC. So the attack employs a channel-based MitM, the AP is cloned on a different channel, which has the same MAC of the legitimate AP.
3. Some implementations need an encrypted frame once the PTK has been installed for the first time. But if the attack forces the authenticator to refresh the PTK by stopping the Message4, this latter will retry an unprotected frame. Thus the supplicant would ignore the retransmission of the message. so the simple retransmission of message 3 wouldn't work.

Plaintext Retransmission of message 3



Once the MitM is up and running, the attacker blocks the message 4 before that the authenticator gets it. The supplicant will pass in PTK-DONE state, and starts sending normal data frames using the session key to encrypt them. The authenticator didn't receive message 4, so it believes that the client did not get message 3, it will resend it. The client

must refresh the PTK. To finish this handshake, the MitM must resend the message 4 to the authenticator, since the client has already a PTK he encrypts the “new” message 4. The weakness is at the 802.11 standard, because it accepts a message if its Key Replay Counter is valid (the last one or a previous one). So the first message 4 saved by the MitM is transmitted to the authenticator. And from now, the device will reuse exactly the same nonces for the x firsts frames. So the attacker can “pause” the retransmission of message 3 to gather the amount of nonces needed.
This attack can be repeated with the deauthentication attack, which will have for effect to restart a 4-way handshake on the client device.

Obviously there is not only the retransmission of the message 3 in plaintext. There is the encrypted retransmission of message 3 (with acceptance of a plaintext message 3 or not), but it is the same kind of reasoning, so it will not be explained in this report.
Just for information, the difference between both ideas (when the transmitting of the message 3 is encrypted and the basic retransmitting) resides into the fact that, when the message 3 is encrypted the adversary can’t forward directly the message 3, it must wait that the AP retransmits the message 3. In some implementations of 802.11 standard is possible to force the retransmission with a Pairwise bit set request, but often there is a delay.

Impact on reuse of the nonce

The impact differs between the data-confidentiality protocol used. In TKIP, CCMP and GCMP, since they use stream cipher, the reuse of the nonce corresponds to a reuse of the keystream, and thus the decryption of the frame.
The replay counters are also restarted so it allows replay attacks.

- In TKIP, the MIC can be retrieved by attacking the Michael algorithm, this weakness allows forging a packet in a specific direction.
- In CCMP there is no practical way to forge arbitrary packets.
- In GCMP, it is possible to retrieve the authentication key (which should be kept secret). Which allows forging packets in both directions. It is also possible to reconstruct the authentication key to recover the GHASH.

To be clearer, here is a summary table of possible impact on the 4-way handshake in function of the protocol used for ensure confidentiality :

	Replay [c]	Decrypt [a]	Forge
4-way impact			
TKIP	AP → client	client→ AP	client→ AP [b]
CCMP	AP → client	client→ AP	
GCMP	AP → client	client→ AP	client↔ AP [b]

Countermeasures

The data-confidentiality protocol should verify if a PTK is already installed and in-use when a client receives a new one, if this is the case, it should just replay message 4 and not reset nonces and replay counters.

B. Evil Twinning (WEP / WPA /WPA2 / WPA3)

This attack is performed by setting up a fake access-point (also called Rogue AP) that appears legitimate to the user by setting the same SSID and BSSID of the network targeted. Whenever the victim connects unexpectedly (or is forced to connect to it, when a DOS attack (e.g : jamming attack) is occuring). All the traffic goes in the fake-AP, which eavesdrops on all their communication. So if a user is connecting to a non-https site (unciphered), the attacker intercepts the credentials. Since there is a lot of uncertainty (user must connect to fake access-point and use non-https sites) in this kind of attack, attacker will force user to leak data.

Common usage

The most commonly used evil twin method is the *Captive portal* attack, once the rogue AP has been set up, the attacker will DOS the legitimate access-point of the targeted network. Once the AP is down, the user is going to connect to the Rogue AP, on this AP, the connection will be limited, and using a DNS server, any web page is redirected to a fake page saying : “Your wifi hotspot needs an update, enter your WiFi password to continue”. The web page can obviously be configured to look-like your real IPS template. For example when the real SSID looks like “Orange-CX8B”, the attacker knows that he has to display an Orange template. If the victim enters his AP-password, it is sent to the hacker. And he will be able to access, monitor, and play a man-in-the-middle attack on the legitimate AP.

KARMA Attack : Alternative to classic evil twin

The Karma attack is using the Preferred network list (PNL) as a vulnerability. The PNL list is a list in certain types of devices like phone or laptop, which contains the SSIDs of access points to which the device has already been connected. This is the process allowing the device to automatically connect to the home WiFi, when the network is reachable. The vulnerability is on the behaviour of this list. The device will try for each preferred network if the first SSID is reachable, connect to it, if not, try the second, until the end of the list, and

restart at the first SSID of the list. And these probes are openly broadcasted, and unencrypted. So if a fake access point is reachable with an SSID existing in the PNL, the device will connect to it without the user intervention. So the KARMA attack, will listen to PNL of a user, and will set up an evil twin, as a Rogue AP of an SSID contained in this PNL. The device of the victim is connecting automatically to it, and the user is at the mercy of the attacker.

How to prevent against this kind of attack

The evil twin attack is more an social engineering attack than a vulnerability on the Wifi technology. However, detecting a Rogue AP, is easily done by scanning and comparing available AP. But it needs some extra infrastructure, so the easier way is, as for every social engineering attack, training users !

Concerning karma attack, a user should deactivate his wifi connection, unless he wants to connect to one. And the PNL discovery disclosure on some devices got updated, but it is not the case for every one.

C. Denial-of-service

a. Deauthentication attack

This kind of attack targets the communication between a user and an access point, the goal of this attack is to send a deauthentication packet to the access point as if the user had sent it. So the AP thinks that the user wants to disconnect, and process the deauthentication.

Why is it working

The problem of the 802.11 protocol is that the encryption is only on data payloads, and does not apply to the frame headers. Since a lot of management frames use the 802.11 headers, it is easy to spoof them.

So anyone, knowing the MAC address of an AP's user, can craft deauthentication frames.

Field	Frame control	Duration, id	Address 1	Address 2	Address 3	Sequence control	Address 4	QoS control	HT control	Frame body	Frame check sequence
Length (Bytes)	2	2	6	6	6	0, or 2	6	0, or 2	0, or 4	*Variable*	4

This is a classical 802.11 frame. The frame control two bytes are used for the configuration of a frame.

Two firsts bits are for protocol version, the two following are for the Type (00 for management frames, 01 for Control frames, 10 for Data frames), and the four following are for the subtypes. In the management frame, deauthentication subtype is *1100, 0xC*. So to craft the frame, the frame control bytes must be set as a deauthentication frame, and the three MAC addresses must be set as the one of the victim network as the AP MAC, source MAC, destination MAC.

How to prevent

The 802.11w update of the standard, in September 2009, increased the security of these management frames. Although it is impossible to protect frames sent before the key establishment (4-ways handshake), all the management ones sended after are protected.
This is an optional feature of the 802.11, both client and infrastructure must support it and enable it. However, it is a mandatory feature for the use of TKIP and CCMP.

D. WEP attacks and weaknesses

1) Passive attacks to decrypt traffic based on statistical analysis.

In the case of no chosen plaintext or ciphertext , An eavesdropper can listen to the Wifi traffic until an IV collision occurs (likely). The attacker can then XOR the two packets with the same IV that give a XOR of the two plaintexts. This leads to an information leak about the plaintext and thus makes the scheme insecure. In the context of an IP network data is often redundant and predictable making the guess of the XORed plaintexts much more easy. It is often , with statistical methods , possible to recover the exact content of the message.
The attacker can use multiple collision packets using the same IV (Possible in a few hours due to the poor IV space). If the attacker manages to find one of the XORed plain text all the XORed plaintext obtained by collisions with the same IV will be found.

In the case of chosen plaintext , an attacker can use an outside host to send data to an inside host. The attacker knows what he sends to the inside host and when he catches IV collision with his encrypted data he can XOR them and get all the plaintexts.

2) Active attack to inject new traffic from unauthorized mobile stations, based on known plaintext.

If an attacker knows the exact plaintext (X) for one ciphertext (RC4(X)) , he can forge correct encrypted packets (RC4(Y)) . This involves the weak CRC-32 by constructing a new message (Y) , producing his CRC and bit flipping the original encrypted message to change his plaintext (X) to the new message (Y) . This is because a property of RC4 (RC4(X) * X * Y = RC4(Y)).

3) Active attacks to decrypt traffic, based on tricking the access point from Both Ends

An attacker can make guesses about header of the packets instead of the content itself. The user can , with a bitflip operation described earlier to change the IP destination of the packet to his own IP address rogue station on the internet . The data will escape the Wifi network to the internet and thus be decrypted. The attacker can also change the port of the packet and avoid firewall detection.

4) Dictionary-building attack that, after analysis of about a day's worth of traffic, allows real-time automated decryption of all traffic.

Using the aboves technique an attacker can build up a table of IV-KeyStream for every IV possible (Takes up to 15GB due to the low IV space). Once built this table can help the attacker to decrypt every packet flowing through the wireless network. The attacker can build the RC4 keystream for the IV once he has the plaintext of several packets.

The FMS Attack, The KoreK Attack, The PTW Attack, Beck and Tews', Chopchop Attack, Fragmentation Attack,

F. Conclusion

As a conclusion, through these technologies we can see that there are a lot of possible attack vectors and consequently the security is a serious challenge for further implementations, especially with the explosion of IoT devices. A main challenge will be to ensure a certain level of security in cryptographic protocols through future norms against potential threats. These threats are in a constant evolution so it's important to keep up to date the security updates of devices and constantly have peer-reviews protocols.

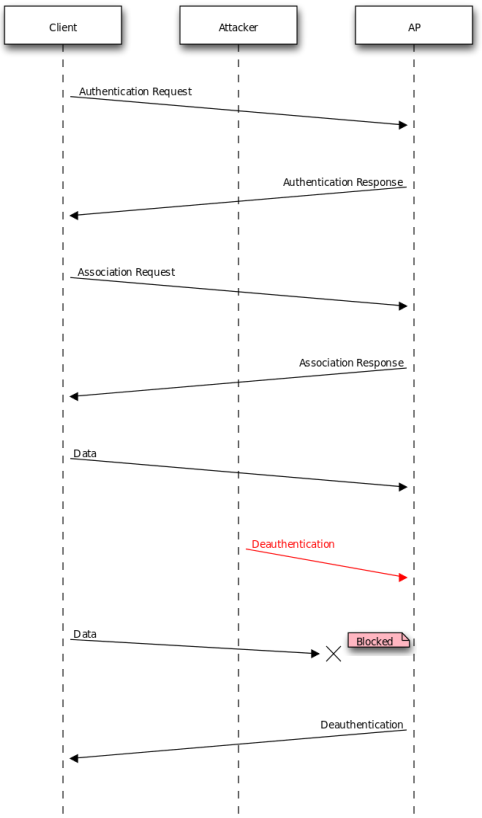
Annexe

EAP-TLS handshake

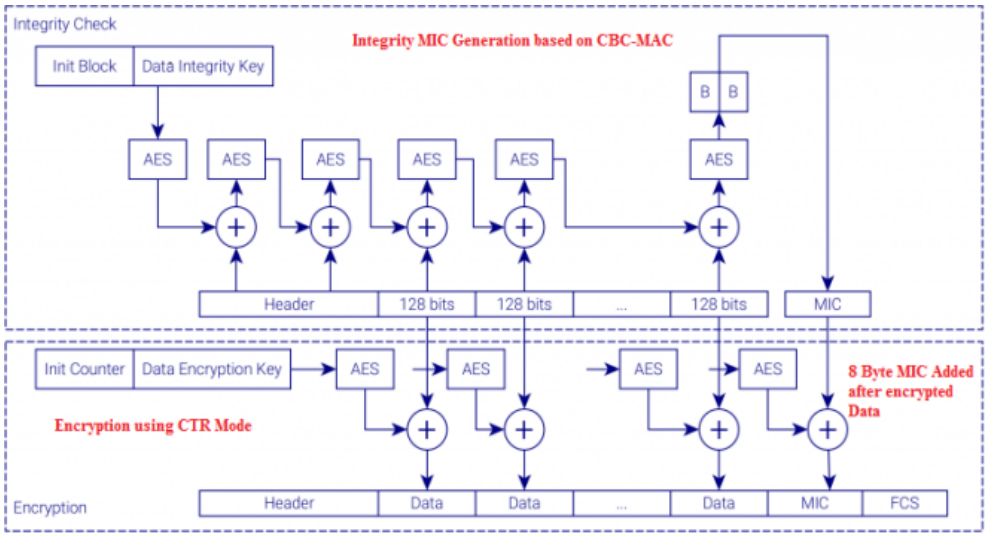
```
Authenticating Peer     Authenticator
-------------------     -------------
                        <- EAP-Request/
                        Identity
EAP-Response/
Identity (MyID) ->
                        <- EAP-Request/
                        EAP-Type=EAP-TLS
                        (TLS Start)
EAP-Response/
EAP-Type=EAP-TLS
(TLS client_hello)->
                        <- EAP-Request/
                        EAP-Type=EAP-TLS
                        (TLS server_hello,
                          TLS certificate,
                  [TLS server_key_exchange,]
                   TLS certificate_request,
                      TLS server_hello_done)
EAP-Response/
EAP-Type=EAP-TLS
(TLS certificate,
 TLS client_key_exchange,
 TLS certificate_verify,
 TLS change_cipher_spec,
 TLS finished) ->
                        <- EAP-Request/
                        EAP-Type=EAP-TLS
                        (TLS change_cipher_spec,
                         TLS finished)
EAP-Response/
EAP-Type=EAP-TLS ->
                        <- EAP-Success
```

https://tools.ietf.org/html/rfc5216

Wifi Deauthentication

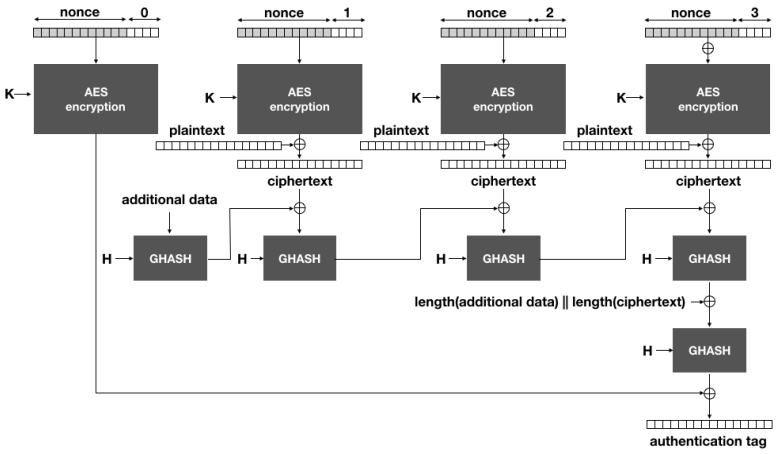


CCMP Encryption/MIC generation



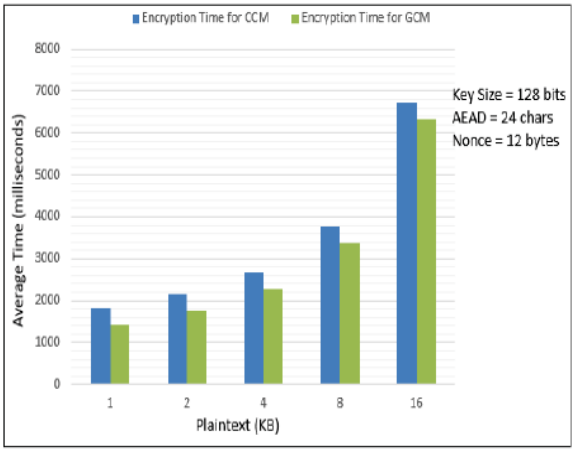
https://praneethwifi.in/2020/05/02/ctr-with-cbc-mac-protocol-ccmp-aes-ccmp/

GCMP Encryption/GHASH generation



https://livebook.manning.com/concept/cryptography/aes-gcm

CCMP/GCMP time comparaison



Levent Ertaul, Anup Mudan, Nausheen Sarfaraz: Performance Comparison of AES-CCM and AES-GCM Authenticated Encryption Modes

Sources

https://tools.ietf.org/html/rfc5216

https://www-sciencedirect-com.ezproxy.ulb.ac.be/science/article/pii/S092552731500451X

https://scotthelme.co.uk/wifi-pineapple-karma-dnsspoof/

https://blog.dinosec.com/2015/02/why-do-wi-fi-clients-disclose-their-pnl.html

https://www.krackattacks.com/

https://papers.mathyvanhoef.com/ccs2017.pdf

https://en.wikipedia.org/wiki/CCMP_(cryptography)

https://tools.ietf.org/html/rfc4186

https://tools.ietf.org/html/rfc3748

https://www.wi-fi.org/discover-wi-fi/security

https://tools.ietf.org/html/rfc7664

https://www.speedcheck.org/wiki/wep/

https://www.dummies.com/programming/networking/understanding-wep-weaknesses/

http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html

https://en.wikipedia.org/wiki/Wired_Equivalent_Privacy

https://smallbusiness.chron.com/wep-shared-key-authentication-69537.html

https://wigle.net/enc-large2y.html

Levent Ertaul, Anup Mudan, Nausheen Sarfaraz: Performance Comparison of AES-CCM and AES-GCM Authenticated Encryption Modes.

Finn Michael Halvorsen, Olav Haugen : Cryptanalysis of IEEE 802.11i TKIP

Mathy Vanhoef, Eyal Ronen: Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd

WPA3™ Security Considerations November 2019 : www.wi-fi.org

Nelson, Sharon D; Simek, John W : New WPA3 WiFi Standard Released

Rahul N1, Roopa J : Comparison between CCM and GCM Modes of Encryption