



Collège Sciences et Technologies

KRACK : Key Reinstallation Attacks Breaking WPA2 by forcing nonce reuse

Hugo Birginie, Maxime Cerezo, Maxime Moreau

M1 CSI
2024–2025

TER

Table des matières

1 Contexte	3
1.1 Le WEP	3
1.2 WPA	5
1.2.1 MIC	6
1.2.2 Faiblesse	7
1.3 Aircrack-ng	8
2 Introduction	8
3 WPA2	9
3.1 Trames Beacon et Probe Request	9
3.2 Clés de session et 4-Way Handshake	11
3.2.1 PMK	11
3.2.2 PTK	12
3.2.3 GTK et IGTK	12
3.2.4 Keystream	13
3.2.5 MIC	14
3.2.6 4-Way Handshake	15
3.2.7 Wireshark	18
3.3 Group 2-Way Handshake	21
3.4 Canaux et Interférences dans les Réseaux Wi-Fi	21
3.4.1 CRC	21
3.4.2 Techniques d'Interception et de Redirection de Trames	22
4 Faille dans WPA2-PSK	23
4.1 Contexte et normes	23
4.2 KRACK (Key Reinstallation Attack)	24
4.2.1 Vulnérabilité de réinstallation de la PTK : CVE-2017-13077	24
4.2.2 Vulnérabilité de réinstallation de la GTK et IGTK : CVE-2017-13078/CVE-2017-13079	25
4.2.3 Réinitialisation de la clé et exposition des paquets en clair	26
4.2.4 Exploitation du message 4 chiffré et récupération du keystream	27
4.2.5 L'attaque par rejeu de paquets	29
5 Failles dans WPA2-Enterprise	29
5.1 Vulnérabilités du 4-Way Handshake	29
5.2 Faiblesses liées aux certificats et aux méthodes d'authentification	29
6 Un équipement relativement sophistiqué	29
7 Correctif	30
7.1 Correctif coté client	30
7.2 Correctif coté point d'accès	30
7.2.1 Protected management frames	30
7.2.2 Beacons frames protection	31
7.2.3 Channel validation	32
7.3 Mesures supplémentaire	32
8 WPA3	33
8.1 OWE (Opportunistic Wireless Encryption)	33
8.2 SAE (Simultaneous Authentication of Equals)	34
8.3 PMF obligatoires	37
9 Conclusion	38

Résumé

Les attaques par réinstallation de clé exploitent une vulnérabilité du protocole WPA2, permettant à un attaquant d'intercepter et de déchiffrer des communications Wi-Fi supposées sécurisées. En manipulant le processus d'établissement de la connexion, un attaquant peut forcer la réutilisation de paramètres de chiffrement, compromettant ainsi la confidentialité des données transmises. Cette faille a affecté une large gamme de dispositifs, notamment ceux fonctionnant sous Android et Linux. Des correctifs ont été déployés par les principaux fournisseurs pour corriger cette vulnérabilité.

1 Contexte

Les communications sans fil étant transmises par ondes radio, il est essentiel de les chiffrer afin d'empêcher toute personne équipée d'une carte Wi-Fi de les intercepter et d'accéder à nos données.

1.1 Le WEP

Le WEP (Wired Equivalent Privacy) est le premier protocole conçu pour sécuriser les connexions Wi-Fi. Il utilise l'algorithme de chiffrement par flot RC4 avec une clé secrète de 40 ou 104 bits, à laquelle s'ajoute un vecteur d'initialisation (IV) de 24 bits, ce qui donne une longueur totale de 64 ou 128 bits. L'IV est modifié à chaque paquet émis pour éviter l'utilisation répétée de la même clé. La clé est concaténée 16 ou 32 fois pour atteindre les 2048 bits (256 octets) requis en entrée de RC4.

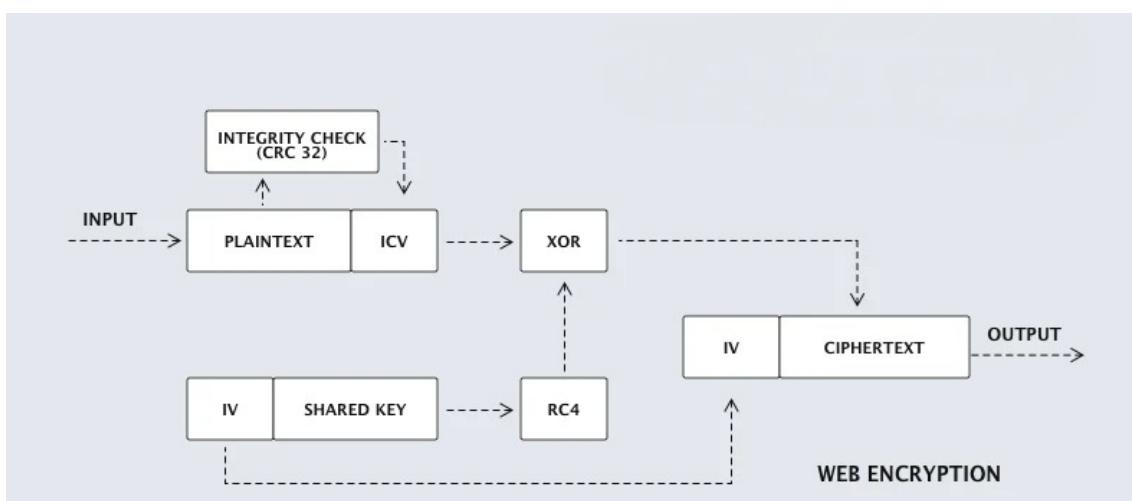


FIGURE 1 – Protocole de chiffrement - WEP

Source : <https://mctt.vn/wep-la-gi>



FIGURE 2 – Trame - WEP
Source : <https://www.youtube.com/watch?v=1JPsKyjzbWw>

Le processus d'authentification repose sur un défi où le point d'accès envoie une phrase à chiffrer, permettant de vérifier si le client dispose de la clé secrète. Pour assurer l'intégrité des données, le WEP utilise une valeur de contrôle d'intégrité (ICV), calculée à l'aide de l'algorithme CRC32. Chaque trame envoyée comprend les données suivies de cette ICV de 32 bits, permettant au récepteur de vérifier l'intégrité des données reçues.

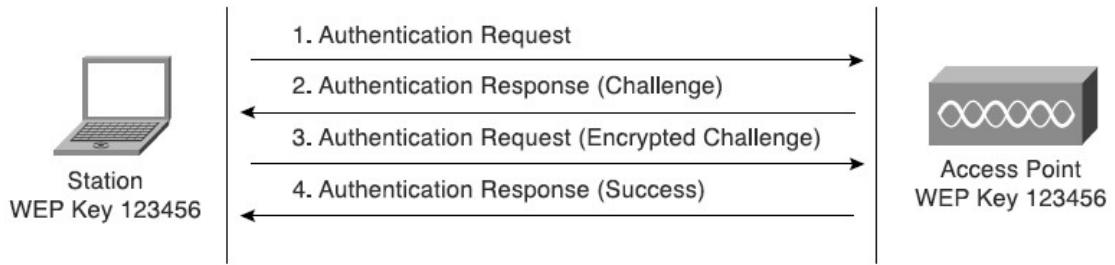


FIGURE 3 – Schéma du processus d'authentification - WEP
Source : <https://youngjun1004.tistory.com/61>

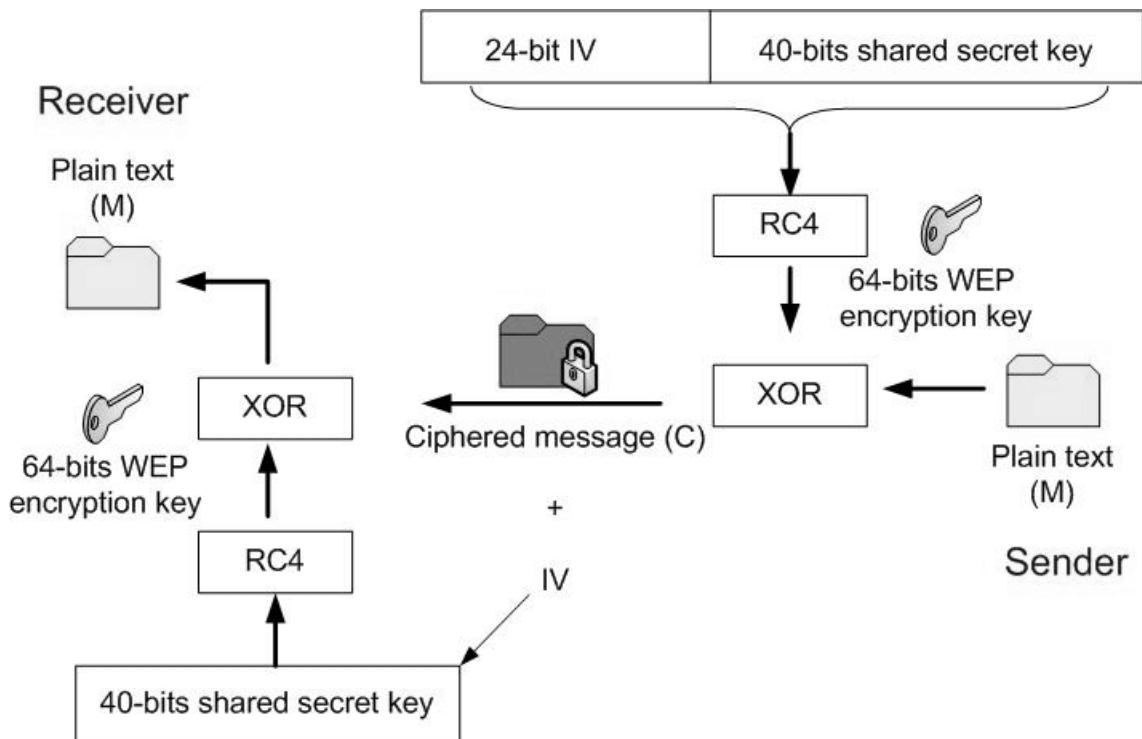


FIGURE 4 – Chiffrement et déchiffrement - WEP

Source : https://www.researchgate.net/figure/Schematics-of-the-Wired-Equivalent-Privacy-WEP-protocol-used-to-control-access-to-the_fig1_250756421

Cependant, WEP présente de nombreuses vulnérabilités. Bien que l'algorithme CRC32 soit efficace pour détecter des erreurs accidentelles lors de la transmission des données, il n'est pas adapté pour résister à des modifications intentionnelles. Il n'utilise pas de clé secrète et il est relativement simple de générer des collisions. Un attaquant peut altérer les données transmises et recalculer facilement l'ICV correspondante, rendant la modification du paquet indétectable pour le récepteur. De plus, l'IV de 24 bits est transmis en clair dans chaque trame. Cette faible longueur entraîne une réutilisation fréquente des mêmes séquences de chiffrement, notamment sur des réseaux très actifs. Les attaquants peuvent exploiter cette faiblesse pour capturer un grand nombre de trames et, en analysant les IV réutilisés, déduire la clé de chiffrement RC4 utilisée.

Avec de bons outils, il est possible de casser la clé en moins de 5 minutes. Ce protocole est donc à bannir.

1.2 WPA

En 2002, le protocole WPA (Wi-Fi Protected Access) a été introduit pour fournir une solution rapide aux failles du WEP. Conçu comme un protocole de transition, il devait rester compatible avec les équipements existants. Il repose sur le protocole de chiffrement TKIP (Temporal Key Integrity Protocol) qui utilise toujours RC4 mais avec une clé secrète et un IV plus grand, respectivement 128 et 64 bits (16 et 8 octets).

TKIP améliore la gestion des clés en les changeant périodiquement. Il ajoute un code d'intégrité de message (Message Integrity Code, MIC) de 64 bits (8 octets) pour vérifier que les paquets n'ont pas été altérés pendant la transmission, ainsi qu'un compteur de séquence pour empêcher les attaques par rejet. Ces attaques se produisent lorsqu'un attaquant intercepte des paquets de données et les retransmet tels quels pour perturber les communications. En attribuant un numéro de séquence unique à chaque paquet, le compteur de séquence permet au récepteur de détecter et de rejeter les paquets dupliqués ou reçus dans le désordre, empêchant ainsi leur réutilisation malveillante.

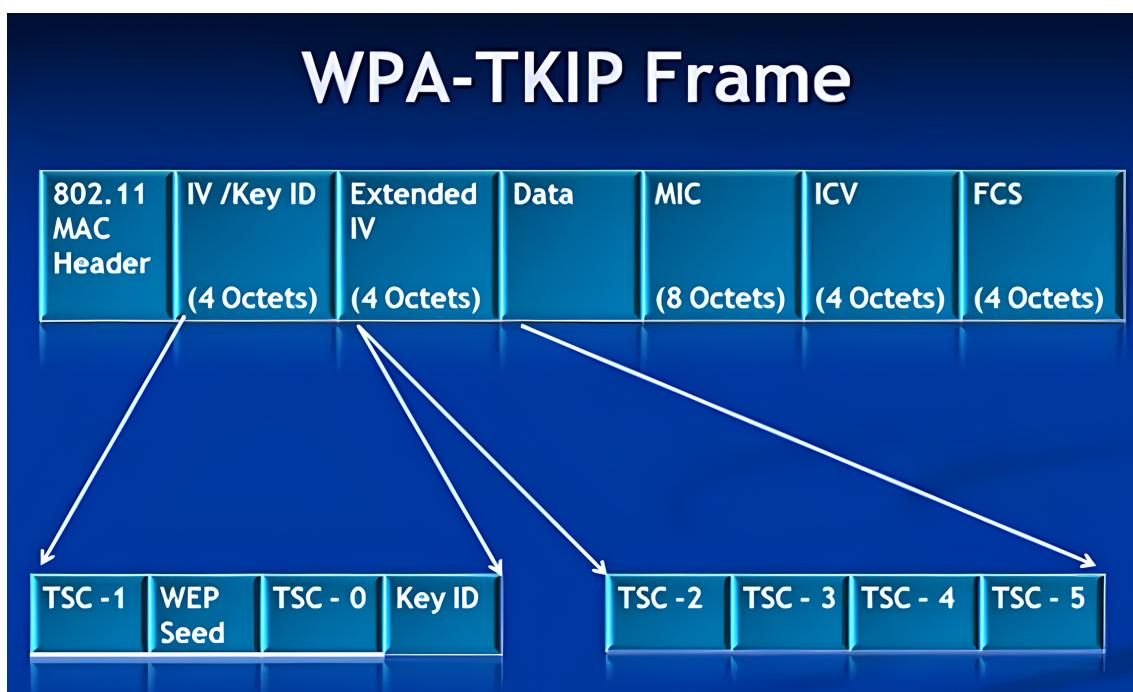


FIGURE 5 – WPA-TKIP Frame - WPA

Source : https://www.youtube.com/watch?v=raU6CeEKM_0

1.2.1 MIC

En mode TKIP, l'intégrité d'une trame est assurée par un MIC (Message Integrity Code) calculé à l'aide de l'algorithme *Michael*. Conçu pour pallier les faiblesses du CRC32 utilisé par WEP, *Michael* effectue une série d'opérations simples (XOR, rotations et additions modulo 2^{32}) sur le message à protéger.

On divise une clé secrète en deux mots de 32 bits, notés :

$$k_0 \text{ et } k_1.$$

On initialise ensuite deux variables internes :

$$L_0 = k_0 \text{ et } R_0 = k_1.$$

Le MIC est calculé sur un segment défini de la trame (par exemple, certains champs d'en-tête et le payload). Ces données, notées M , forment le message sur lequel sera appliqué l'algorithme.

Découpage et Padding : Le message M est découpé en blocs de 32 bits (4 octets) dans l'ordre little-endian. S'il n'est pas multiple de 4 octets, un padding est ajouté :

- Un octet constant `0x5A` est ajouté,
- Suivi d'un nombre suffisant d'octets de padding pour atteindre un multiple de 4.

On note les blocs obtenus :

$$m_0, m_1, \dots, m_{n-1}.$$

Traitement Itératif des Blocs : Pour chaque bloc m_i ($0 \leq i \leq n - 1$), *Michael* effectue les opérations suivantes.

Il mélange le bloc courant avec la variable L par une opération XOR :

$$L \leftarrow L \oplus m_i.$$

La fonction B est une séquence d'opérations qui modifie l'état interne (L, R) . Elle se compose des étapes suivantes (les additions sont effectuées modulo 2^{32}) :

1. $R \leftarrow R \oplus (L17)$ (rotation à gauche de L de 17 bits)
2. $L \leftarrow L + R$
3. $R \leftarrow R \oplus \text{XSWAP}(L)$ (la fonction `XSWAP` échange les deux octets les plus significatifs et les deux moins significatifs de L)
4. $L \leftarrow L + R$
5. $R \leftarrow R \oplus (L3)$ (rotation à gauche de L de 3 bits)
6. $L \leftarrow L + R$
7. $R \leftarrow R \oplus (L2)$ (rotation à droite de L de 2 bits)
8. $L \leftarrow L + R$

Ces étapes sont appliquées pour chaque bloc m_i du message.

Itération sur l'Ensemble des Blocs : Soit (L_0, R_0) l'état initial, pour $i = 0, 1, \dots, n - 1$, on met à jour :

$$\begin{cases} L_{i+1}, R_{i+1} = B(L_i \oplus m_i, R_i) \\ \text{où } B(\cdot, \cdot) \text{ représente la fonction décrite ci-dessus.} \end{cases}$$

Après traitement de tous les blocs, on obtient les valeurs finales L_n et R_n (chacune sur 32 bits). Le MIC final est obtenu en concaténant ces deux valeurs :

$$\text{MIC} = L_n \parallel R_n,$$

ce qui donne un MIC de 64 bits.

Conclusion : En mode TKIP, le MIC d'une trame est généré via l'algorithme *Michael* qui procède de la manière suivante :

1. On initialise (L, R) à partir de la clé MIC de 64 bits, décomposée en k_0 et k_1 .
2. Le message (sélectionné pour calculer l'intégrité) est découpé en blocs de 32 bits avec padding si nécessaire.
3. Pour chaque bloc m_i , on effectue :

$$L \leftarrow L \oplus m_i \quad \text{puis} \quad (L, R) \leftarrow B(L, R)$$

avec la fonction de mélange B définie par une série d'opérations (rotations, XOR, et additions modulo 2^{32}).

4. Après traitement de tous les blocs, on concatène les valeurs finales L et R pour obtenir un MIC de 64 bits.

Ce mécanisme permet de garantir une intégrité minimale des trames, empêchant ainsi certaines modifications non autorisées lors de la transmission.

1.2.2 Faiblesse

Malheureusement, WPA présente aussi plusieurs vulnérabilités. La dépendance de TKIP à RC4 expose le réseau aux faiblesses intrinsèques de cet algorithme.

- **Attaques par analyse statistique** : RC4 ne produit pas un flux de sortie assez aléatoire, ce qui permet d'identifier des motifs répétitifs et d'exploiter ces irrégularités pour reconstruire des parties du message en clair.
- **Attaques basées sur les clés faibles** : Certaines valeurs de clés secrètes produisent des sorties avec des structures prévisibles, facilitant la cryptanalyse.
- **Attaques de type key recovery** : Des attaques comme celles de Mantin et Shamir (2001) exploitent des biais dans la distribution des premiers octets du flux RC4 pour deviner progressivement les bits de la clé de chiffrement.

L'algorithme *Michael* a été conçu pour offrir une protection minimale contre les attaques de type *bit-flip* (où un attaquant modifie quelques bits du message sans se faire détecter). Toutefois, il est considéré comme faible par rapport aux standards cryptographiques modernes et a fait l'objet d'attaques exploitant ses faiblesses, par exemple, les attaques de Beck et Tews.

Le flux aléatoire généré par RC4 est légèrement biaisé en faveur de certaines séquences d'octets. La meilleure attaque utilisant cette faiblesse a été publiée par Scott Fluhrer et David McGrew. Leur attaque arrive à distinguer un flux pseudo-aléatoire RC4 d'un flux aléatoire, moyennant des données de l'ordre du gigaoctet.

Bart Preneel et Souradyuti Paul ont montré en 2004 que la distinction entre un flot aléatoire et un flot de RC4 ne nécessitait que 225 octets produits par RC4. Ils ont entre autres montré que le biais ne disparaît pas même si les 256 premiers octets sont éliminés.

En 2008, une attaque démontrée par Martin Beck et Erik Tews permettant à un attaquant de décoder des requêtes ARP et d'injecter jusqu'à 7 paquets de 28 octets maximum. L'attaquant pouvait identifier des paquets ARP chiffrés grâce à leur taille et à la connaissance préalable de certaines données, comme les adresses MAC et les plages IPv4. Sans rentrer trop dans les détails, il pouvait exploiter des canaux de qualité de service peu utilisés pour contourner les mécanismes de protection et injecter des paquets malveillants.

En 2013, Mathy Vanhoef et Frank Piessens ont amélioré cette attaque, permettant l'injection d'un nombre arbitraire de paquets avec une charge utile maximale de 112 octets chacun, sans nécessiter l'activation des fonctionnalités de qualité de service. Ils ont également démontré la possibilité de déchiffrer des paquets arbitraires envoyés à un client, ouvrant la voie à des attaques plus sophistiquées, telles que le détournement de connexions TCP et l'injection de code malveillant lors de la visite de sites web.

Ces vulnérabilités ont conduit à l'abandon progressif de WPA au profit de WPA2.

1.3 Aircrack-ng

Aircrack-ng est une suite d'outils dédiée à l'audit de la sécurité des réseaux Wi-Fi. Il permet de surveiller, tester, attaquer et casser les protections WEP et WPA en capturant et en analysant les paquets de données transmis sur le réseau. Cet outil est couramment utilisé pour mettre en évidence les failles de ces protocoles.

2 Introduction

C'est en 2004 avec la norme IEEE 802.11i que le protocole WPA2 va pousser encore plus loin la sécurité. Il introduit le protocole de chiffrement CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) qui remplace RC4 par l'algorithme de chiffrement AES en mode CTR qui transforme le chiffrement par blocs AES en un chiffrement par flot.

Dans ce mode, chaque bloc de texte en clair est combiné avec un bloc du keystream, généré en chiffrant une valeur de compteur unique à l'aide de l'algorithme de chiffrement par bloc AES en utilisant la clé secrète partagée. Cette opération utilise le XOR pour produire le texte chiffré. De même, lors du déchiffrement, le même processus est appliqué : le bloc du keystream est XORé avec le texte chiffré pour retrouver le texte en clair. Il est essentiel de garantir que chaque valeur de compteur (souvent constituée d'un nonce et d'un compteur incrémental) soit unique et ne soit jamais réutilisée avec la même clé, afin d'assurer la sécurité du chiffrement en mode CTR.

CCMP Encryption

Encryption method: AES in Counter mode (AES-CTR)

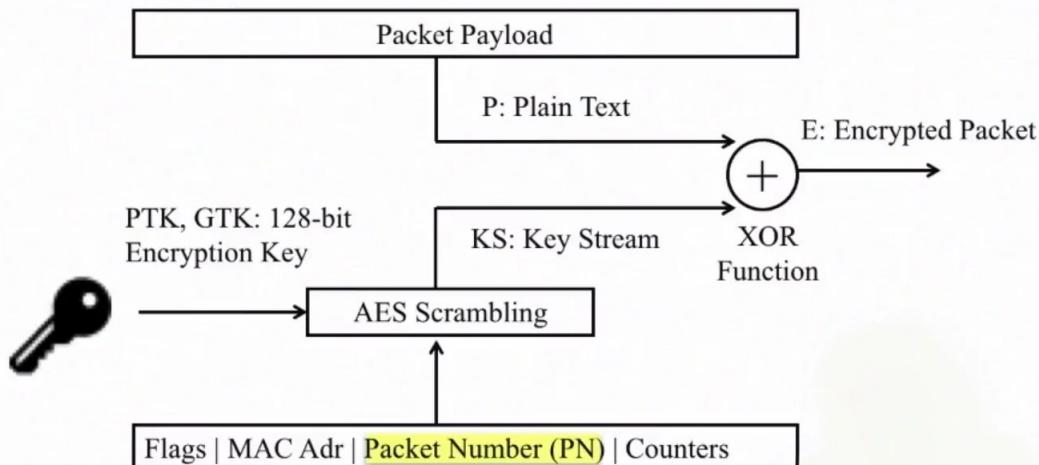


FIGURE 6 – Protocole de chiffrement CCMP - WPA2

Source : <https://www.youtube.com/watch?v=QeDn7bgIpIU&list=PLzKIBgD3ky20pBEZKz6o7X0gNBQPLIrBi>

Ces algorithmes, plus robustes, nécessitent plus de puissance de calcul pour le codage et le décodage. Cela rend WPA2 incompatible avec certains appareils existants. C'est pourquoi une version mixte WPA/WPA2 existe. Cette version utilise WPA pour les appareils non compatibles et WPA2 pour les autres. À noter qu'aujourd'hui, il est possible d'utiliser AES avec WPA.

Chiffrement Wifi invité

The screenshot shows a configuration interface for a WiFi network. It has three main sections: 'Système' (System) set to 'WPA/WPA2 Personnel', 'Type de clé' (Key Type) set to 'AES', and 'Clé' (Key) containing the value 'M3-ap2hjHOV-1WQCDK7M'. A purple 'Valider' (Validate) button is at the bottom left, and a small circular icon with a checkmark is at the top right.

FIGURE 7 – AES - WPA/WPA2

WPA2 existe en deux variantes, dont le choix dépend de la taille du réseau et des besoins en sécurité :

- **WPA2-PSK (Pre-Shared Key)** : Destiné aux réseaux domestiques et aux petites entreprises. Il repose sur une clé secrète partagée entre tous les utilisateurs du réseau. Cette méthode est simple à mettre en place mais si la clé est compromise, l'ensemble du réseau est vulnérable.
- **WPA2-Entreprise** : Destiné aux grandes organisations. Il utilise un serveur d'authentification centralisé (généralement basé sur le protocole RADIUS ou TACACS+) pour la gestion des identités des utilisateurs. Chaque utilisateur dispose d'un identifiant unique.

Malgré les améliorations apportées par WPA2, Mathy Vanhoef a découvert des vulnérabilités critiques en 2017. Ces attaques permettent d'exploiter une faille du protocole qui met en péril la confidentialité des communications. Elles ont affecté un grand nombre d'appareils et ont obligé les fabricants à publier des correctifs pour protéger les utilisateurs.

Dans la suite de ce document, nous allons examiner en détail le fonctionnement de WPA2, puis expliquer comment l'attaque compromet la sécurité d'un réseau. Nous verrons également les mesures mises en place pour ce protéger et assurer la sécurité des communications sans fil.

3 WPA2

Un point d'accès (Access Point, AP) est un appareil de mise en réseau qui permet aux autres appareils (clients) de se connecter à un réseau sans fil. Pour annoncer sa présence aux périphériques potentiels, le point d'accès émet des trames de gestion appelées balises (beacons).

3.1 Trames Beacon et Probe Request

Ces trames sont diffusées en clair périodiquement (généralement toutes les 100 ms) et contiennent plusieurs éléments essentiels, dont le RSN IE (Robust Security Network Information Element) :

1. L'identifiant du réseau (SSID).
2. Les protocoles supportées (WEP, WPA2, WPA3, WPA4).
3. Les protocoles de chiffrement pris en charge (TKIP, CCMP, GCMP).
4. Les méthodes d'authentification (PSK, 802.1X/EAP).
5. Les paramètres temporels de synchronisation (ex : timestamp).

6. Les informations sur les canaux et débits supportés (ex : 2,4 ou 5 GHz).
7. La plage de bits prise en charges .
8. ...

Les paramètres temporels de synchronisation : Ce champ contient des informations permettant aux appareils du réseau de se synchroniser avec l'AP. Il permet de garantir que les appareils communiquent sur un même rythme, évitant ainsi les collisions et optimisant la gestion du temps pour l'envoi et la réception des données. Par exemple, la timestamp (horodatage) indique l'heure précise à laquelle la trame a été émise, ce qui aide les appareils à se synchroniser correctement avec l'AP.

Les informations sur les canaux et débits supportés : Ce champ fournit des détails sur les canaux Wi-Fi disponibles (canal de fréquence) et les débits de données maximums que le point d'accès peut supporter. Ces informations permettent aux appareils de connaître les options de transmission possibles pour établir une connexion optimale. Cela inclut des informations comme les modes de modulation, les vitesses maximales de transmission (par exemple, 54 Mbps pour 802.11g), et les canaux radio utilisés (par exemple, canal 1, 6, 11 en 2.4 GHz).

Beacons are not protected

```

· Tag: SSID parameter set: cisco
· Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 6, 9, 12, 18, [Mbit/sec]
· Tag: DS Parameter set: Current Channel: 1
· Tag: Traffic Indication Map (TIM): DTIM 0 of 0 bitmap
· Tag: Country Information: Country Code GB, Environment Unknown (0x04)
· Tag: Power Constraint: 3
· Tag: ERP Information
· Tag: Extended Supported Rates 24, 36, 48, 54, [Mbit/sec]
· Tag: QBSS Load Element 802.11e CCA Version
· Tag: RM Enabled Capabilities (5 octets)
· Tag: HT Capabilities (802.11n D1.10)
· Tag: RSN Information
· Tag: Mobility Domain
· Tag: HT Information (802.11n D1.10)
· Tag: Extended Capabilities (10 octets)
· Ext Tag: HE Capabilities (IEEE Std 802.11ax/D3.0)
· Ext Tag: HE Operation (IEEE Std 802.11ax/D3.0)
· Ext Tag: Spatial Reuse Parameter Set

```

FIGURE 8 – Beacons trames - WPA
Source : <https://www.youtube.com/watch?v=KtYjX8xWcOU>

En plus des trames balises, lorsqu'un client souhaite découvrir les réseaux disponibles, il envoie une trame de probe request. Un point d'accès qui reçoit cette requête répond par une probe réponse, dans laquelle il inclut les informations qu'il gère.

Dans le cas où le client décide de se connecter, il commence par s'authentifier et s'associer au point d'accès. Lors de la première connexion, aucune authentification réelle n'a lieu directement. Une authentification par système ouvert (Open System) est utilisée, permettant à tout client de s'authentifier. La véritable authentification sera effectuée par un mécanisme appelé la poignée de main en 4 étapes (4-Way Handshake).

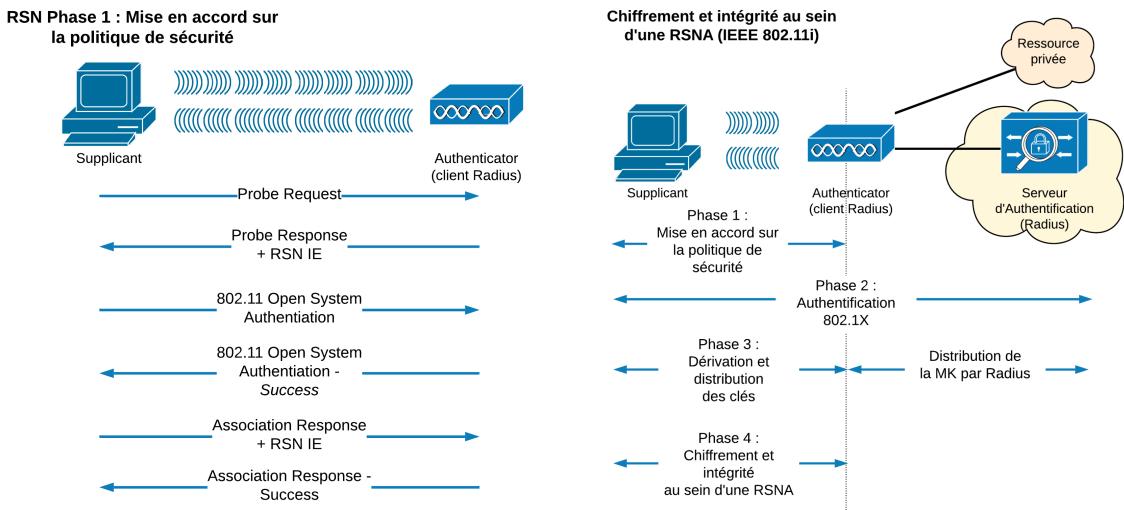


FIGURE 9 – Authentification - WPA/WPA2

Source : <https://cisco.goffinet.org/ccna/wlan/protocoles-securite-sans-fil-wpa-wpa2-wpa3>

3.2 Clés de session et 4-Way Handshake

Cette poignée de main est un processus permettant une authentification mutuelle basée sur un secret partagé appelé clé maître pair-à-pair (Pairwise Master Key, PMK). Le client doit prouver qu'il connaît la clé, tout comme le point d'accès. Son rôle principal est d'établir de nouvelles clés de session appelées PTK (Pairwise Transient Key) pour sécuriser les communications unicast et un couple GTK, IGTK (Group Temporal Key, Integrity Group Temporal Key) pour les communications broadcast et multicast.

PTK : Pairwise Temporel Key

- Protège les communications unicast entre le client et le point d'accès.
- Elle est générée à l'aide de la 4-Way Handshake

$$\text{PTK} = F(\text{PMK}, \text{ANonce}, \text{SNonce}, \text{MAC_1}, \text{MAC_2})$$

GTK : Group Temporal Key

- Protège les communications broadcast/multicast du point d'accès vers les clients.
- Transporté du point d'accès au client dans une trame EAPOL durant la 4-Way Handshake (message 3) ou la Group 2-Way Handshake (message 1).

IGTK : Integrity Group Temporal Key

- Protège les trames de gestion broadcast/multicast
- Transporté du point d'accès au client dans une trame EAPOL durant la 4-Way Handshake (message 3) ou la Group 2-Way Handshake (message 1).

FIGURE 10 – Temporal Keys - WPA2

3.2.1 PMK

Dans un réseau WPA2-PSK, la PMK est dérivée du mot de passe, du SSID et d'un peu de sel via une fonction de hachage PBKDF2 (Password-Based Key Derivation Function 2). Le processus

implique l'application répétée de HMAC-SHA1 sur le mot de passe et le SSID, avec un nombre élevé d'itérations (généralement 4096), ce qui renforce la sécurité en ralentissant les attaques par force brute.

Dans un réseau WPA2-Entreprise, elle est générée lors de l'authentification entre le client et le serveur d'authentification à l'aide du protocole EAP (Extensible Authentication Protocol) qui établit un canal sécurisé avec le client, tel que EAP-TLS, EAP-PEAP ou EAP-PWD (Transport Layer Security, Protected EAP, Password). Une fois l'authentification réussie, la PMK est fournie au point d'accès et au client.

3.2.2 PTK

La PTK est calculée à partir de la PMK, des deux adresses MAC, ainsi que deux nombres aléatoires (ANonce et SNonce) générés respectivement par le point d'accès et le client. Une fois calculée, la PTK est divisée en trois parties :

- **KCK (Key Confirmation Key)** : Assure l'intégrité des messages, elle est utilisée pour générer les MIC.
- **KEK (Key Encryption Key)** : Protège la poignée de main en chiffrant les clés de session.
- **TK (Temporal Key)** : Utilisée pour chiffrer les trames de données unicast après la poignée de main.

PTK Details

The PTK is comprised of three keys: KCK, KEK and TK

KCK used for key integrity

KEK used to encrypt and send keys (GTK)

The TK is used to encrypt data payloads

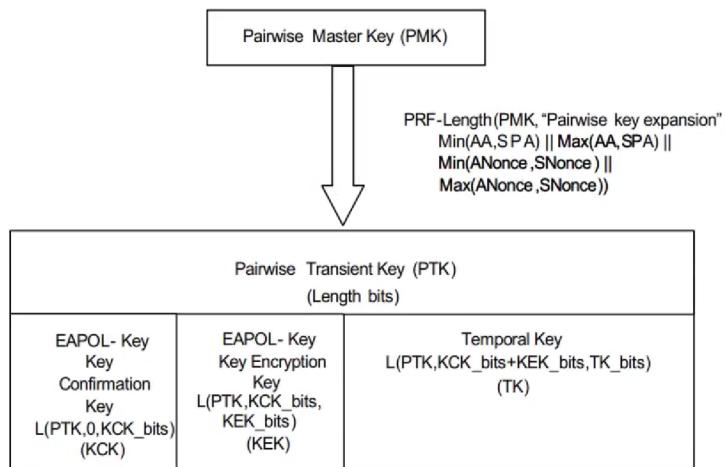


FIGURE 11 – Pairwise Transient Key - WPA2

Source : <https://www.youtube.com/watch?v=pjTTG2nZax0>

La KCK et la KEK protègent la poignée de main, tandis que la TK sert au chiffrement des trames de données unicast. Si le client est déjà connecté au réseau, la PTK peut nécessiter d'être actualisée en initiant une nouvelle poignée de main à 4 étapes. Cela peut se produire, par exemple, lorsque le compteur de paquets atteint sa limite. Cette mise à jour évite que le compteur déborde et revienne à zéro, ce qui entraînerait la réutilisation des mêmes paramètres de chiffrement. L'idée est d'apprendre des erreurs passées et donc de changer les clés de temps en temps. Lors de ce renouvellement, tous les messages sont authentifiés avec la PTK actuelle.

3.2.3 GTK et IGTK

La GTK est employée pour chiffrer les trames de données broadcast et multicast. Quant à elle, l'IGTK permet d'authentifier certaines trames de gestion diffusées en broadcast et multicast. Par ailleurs, quand un client souhaite transmettre une trame broadcast ou multicast sur le réseau, il l'envoie d'abord sous forme de trame unicast chiffrée au point d'accès. C'est le point d'accès qui chiffre ensuite la trame en utilisant la GTK pour la retransmettre en broadcast à tous les clients connectés.

3.2.4 Keystream

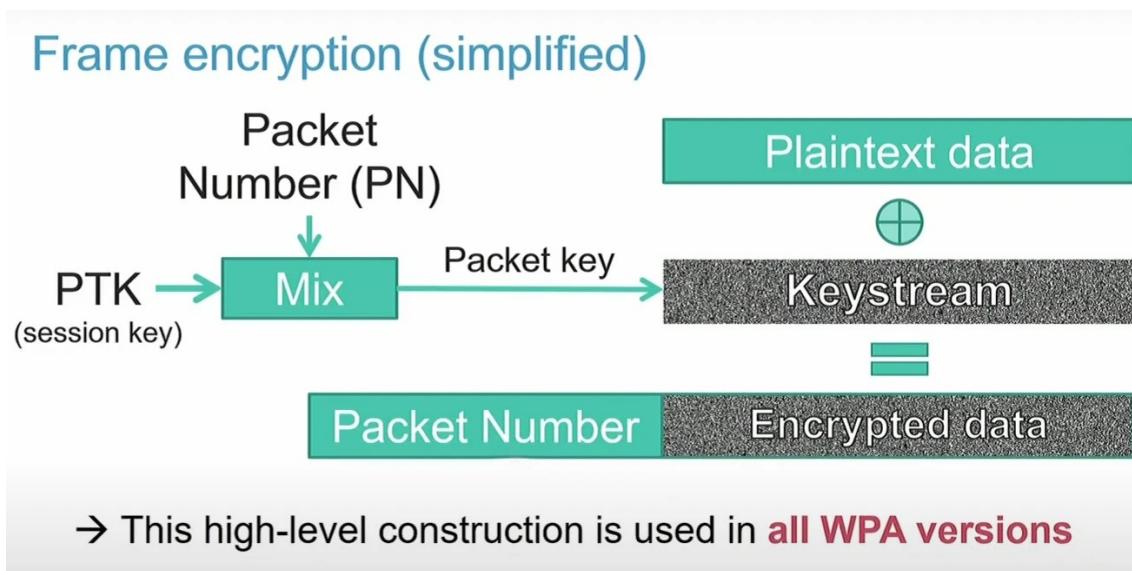


FIGURE 12 – Frame encryption (simplified) - WPA
Source : <https://www.youtube.com/watch?v=KtYjX8xWcOU>

Le chiffrement des paquets dans WPA2 repose sur un mécanisme qui utilise un numéro de paquet unique pour chaque paquet envoyé. Ce numéro est crucial pour générer une clé de chiffrement (**Keystream**) distincte pour chaque paquet. Cette clé est ensuite utilisée pour chiffrer le contenu du paquet via une opération de type **XOR**, garantissant ainsi la confidentialité des données échangées.

La clé de chiffrement ou Keystream est générée à partir de la combinaison du **Temporal Key** (TK), qui est une clé partagée entre le client et le point d'accès, et du **Packet Number** (PN), un numéro qui est unique et incrémenté pour chaque paquet. Plus précisément, dans WPA2-CCMP, le chiffrement repose sur l'algorithme AES utilisé en mode compteur (**AES-CTR**), qui transforme AES en un générateur de flux pseudo-aléatoire.

Au lieu de chiffrer directement les données, AES est utilisé pour chiffrer un compteur (Nonce + Counter), et la sortie est ensuite combinée avec les données via une opération **XOR**. Ce mode permet de chiffrer efficacement de grandes quantités de données tout en assurant que chaque bloc chiffré utilise une Keystream différente, tant que le couple clé/nonce est unique.

La formule utilisée pour générer la Keystream peut être représentée comme suit :

$$\text{Keystream} = \text{AES}_{\text{CTR}}(\text{TK}, \text{Nonce})$$

Où :

- **TK** est la clé temporaire partagée (Temporal Key), issue du 4-Way Handshake.
- **Nonce** est une valeur unique dérivée du **Packet Number** (PN), de l'adresse MAC du point d'accès, et d'un identifiant de priorité (Packet Number + MAC + Priority).

Le **Nonce** est utilisé comme compteur d'entrée pour AES, ce qui garantit que chaque invocation produit une Keystream différente, même si le TK reste le même. Cette Keystream est ensuite utilisée pour chiffrer chaque paquet individuellement via une opération **XOR** avec les données en clair.

Cependant, le numéro de paquet (PN) est crucial pour la création du Nonce et donc du Keystream. Comme les réseaux sans fil sont sujets à des pertes de paquets, le destinataire peut ne pas savoir avec précision combien de paquets ont été effectivement reçus. Pour pallier cela, le PN est transmis en clair dans l'en-tête du paquet, ce qui permet au récepteur de reconstituer correctement la séquence et de générer le bon keystream pour le déchiffrement.

Dans le cas où le PN serait perdu ou mal synchronisé, cela pourrait entraîner une incohérence du keystream, rendant les données illisibles ou facilitant certaines attaques. La rigueur dans la

gestion du PN est donc essentielle à la sécurité du chiffrement dans WPA2-CCMP.

3.2.5 MIC

Dans WPA2 configuré en mode CCMP, l'intégrité et l'authenticité d'une trame sont assurées par un mécanisme d'authentification reposant sur CBC-MAC associé à l'algorithme AES-128. Pour chaque trame, un **nonce** unique est généré à partir d'éléments tels que l'adresse MAC du transmetteur et le numéro de ce paquet (PN). Ce nonce, souvent de longueur 13 octets, est utilisé à la fois dans AES-CTR pour le chiffrement et dans CBC-MAC pour le calcul du MIC.

Bloc Initial B_0 : Le premier bloc de 16 octets, noté B_0 , est construit comme suit :

- **Flags** : Un octet de flags indiquant, par exemple, la longueur du tag (typiquement 8 octets) et la présence d'Additional Authenticated Data (AAD).
- **Nonce** : Les 13 octets du nonce.
- **Longueur du message** : 2 octets indiquant la longueur (en octets) du message à authentifier.

Ainsi, on a :

$$B_0 = \text{Flags} \parallel \text{Nonce (13 octets)} \parallel \text{Longueur (2 octets)}$$

Additional Authenticated Data : Certaines parties de l'en-tête de la trame, comme les adresses MAC et le numéro de séquence, doivent être protégées sans être chiffrées. L'AAD est formaté de la manière suivante :

- Préfixé par sa longueur sur 2 octets.
- Complété par les champs concernés, puis éventuellement paddé pour obtenir un multiple de 16 octets.

Le corps de la trame est découpé en blocs de 16 octets. Si le dernier bloc n'est pas complet, un *padding* est ajouté pour atteindre la taille de 16 octets.

Calcul du CBC-MAC : On commence par chiffrer le bloc initial B_0 avec AES-128 en mode chiffrement classique :

$$X_0 = \text{AES_Encrypt}(K, B_0)$$

Pour chaque bloc B_i , $i = 1, 2, \dots, N$ (où B_1, \dots, B_{N_A} représentent les blocs constituant l'AAD et B_{N_A+1}, \dots, B_N les blocs du message), le CBC-MAC se calcule de manière itérative :

$$X_i = \text{AES_Encrypt}(K, X_{i-1} \oplus B_i)$$

où \oplus représente l'opération XOR.

Après avoir traité tous les blocs, le dernier bloc X_N est obtenu. Le MIC est alors extrait en tronquant X_N .

Extraction et Utilisation du MIC : Dans le cadre de CCMP, le MIC est généralement obtenu en prenant les 8 premiers octets du bloc final X_N , c'est-à-dire :

$$\text{MIC} = \text{Tronc}(X_N, 8) \quad (8 \text{ octets})$$

Le MIC est ensuite inséré dans le champ réservé de la trame CCMP. À la réception, le destinataire recalcule le CBC-MAC avec la même clé (KCK + nonce + AAD), et compare le MIC obtenu avec celui reçu. Si les deux concordent, la trame est considérée comme authentique et intacte.

Conclusion : Le processus de calcul du MIC en mode CCMP dans WPA2 repose sur :

- La construction d'un bloc initial B_0 à partir de flags, du nonce et de la longueur du message.
- Paddé correctement l'AAD et le message.
- Le calcul itératif du CBC-MAC à l'aide de l'opération XOR et du chiffrement AES-CTR.
- L'extraction d'un MIC de 8 octets à partir du dernier bloc.

Le CBC-MAC offre une sécurité robuste tant que le nonce et l'AAD sont correctement choisis et ne se répètent pas pour une même clé puis que le padding est réalisé correctement. Toute altération d'un bloc B_i modifie la valeur de X_i , et par conséquent le MIC final, ce qui permet de détecter toute modification de la trame. Ce mécanisme garantit l'intégrité et l'authenticité des trames transmises dans un réseau WPA2 utilisant CCMP.

3.2.6 4-Way Handshake

La poignée de main intervient juste après l'échange initial de messages d'association entre le client et le point d'accès, comprenant les requêtes et réponses d'Authentication et d'Association. Elle se compose de quatre messages définis à l'aide de trames EAPOL (Extensible Authentication Protocol Over LAN), chacun contenant des champs spécifiques :

- **Compteur de relecture (Replay Counter)** : Détecte les trames rejouées. Les deux appareils incrémentent leur compteur après chaque transmission.
- **Champ nonce** : Transporte les nonces aléatoires générés par le supplicant et l'authentificateur pour dériver une clé de session.
- **Champ RSC (Receive Sequence Counter)** : Contient le numéro de séquence de départ d'une clé de groupe si elle est transportée dans la trame.
- **Données de clé (Key Data)** : Contient les clés de groupe chiffrée.
- **MIC (Message Integrity Check)** : Assure l'intégrité des messages et protège contre les modifications malveillantes.

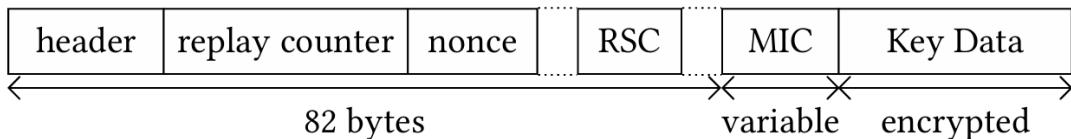


FIGURE 13 – Contenu d'une trame EAPOL simplifié
Source : <https://papers.mathyvanhoef.com/ccs2017.pdf>

Les messages de cette poignée de main sont les suivants :

- **Message 1** : Le point d'accès envoie un premier message contenant un nonce aléatoire (**ANonce**) au client. Ce message est non protégé par un MIC.
- **Message 2** : Le client génère son propre nonce (**SNonce**), dérive la PTK de la PMK, de ces nonces et des deux adresses MAC, puis envoie le **SNonce** au point d'accès avec un MIC pour vérifier l'intégrité de la communication.
- **Message 3** : Une fois le **SNonce** reçu, le point d'accès dérive également la PTK, chiffre la GTK et l'IGTK à l'aide de la KEK et l'envoie au client, accompagnée d'un MIC et du RSC.
- **Message 4** : Le client confirme la réception du message 3 avec un MIC, indiquant qu'il a installé les clés de sessions.

Les deux premiers messages permettent d'échanger les nonces pour générer une clé de session unique, tandis que les deux derniers messages servent à distribuer et confirmer la mise en place des clés. Cette séquence permet d'assurer l'authenticité mutuelle des participants grâce aux MIC du message 3 et 4.

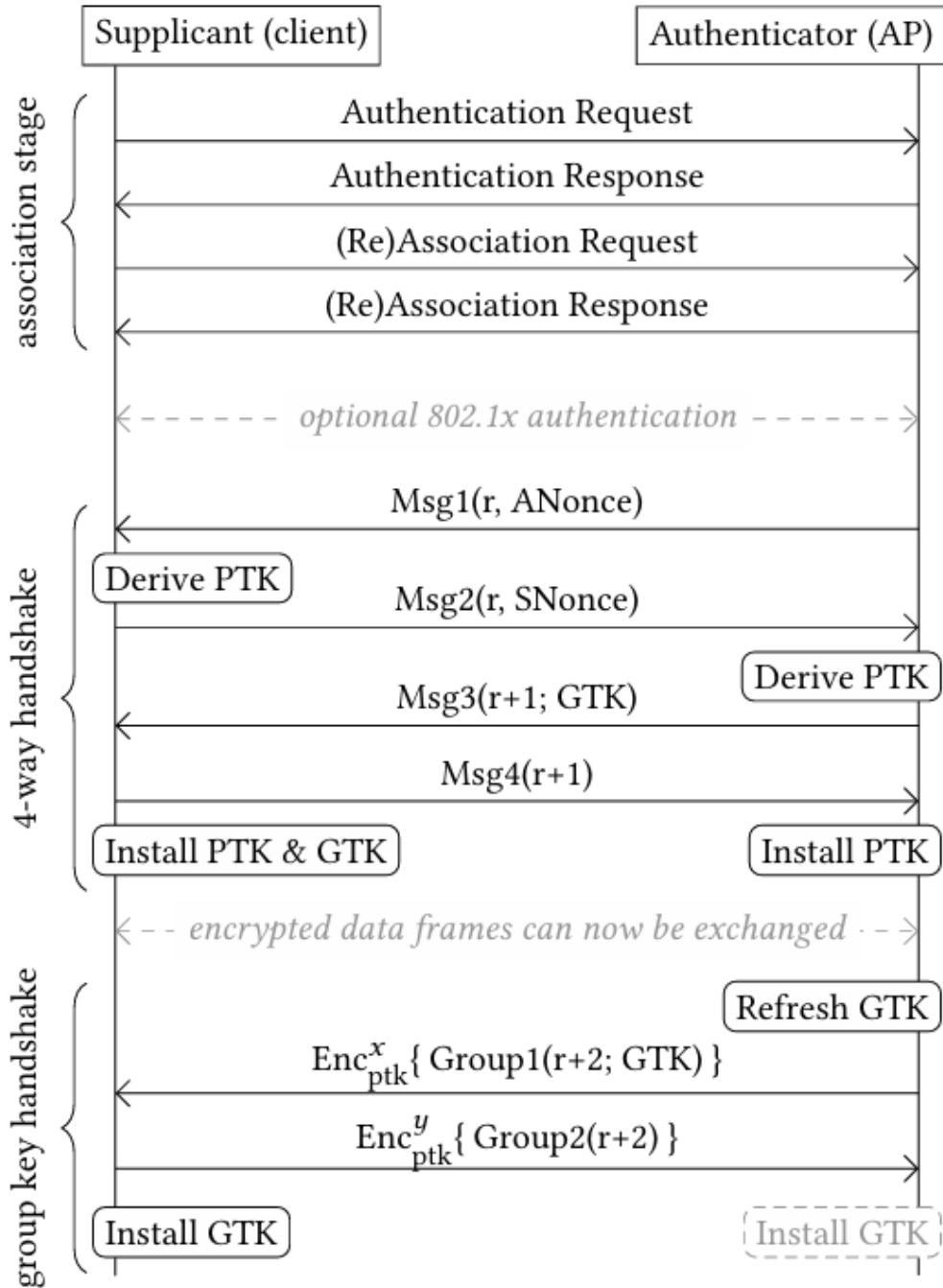


Figure 2: Messages exchanged when a supplicant (client) connects with an authenticator (AP), performs the 4-way handshake, and periodically executes the group key handshake.

FIGURE 14 – 4-Way Handshake - WPA2-Personnel
 Source : <https://papers.mathyvanhoef.com/ccs2017.pdf>

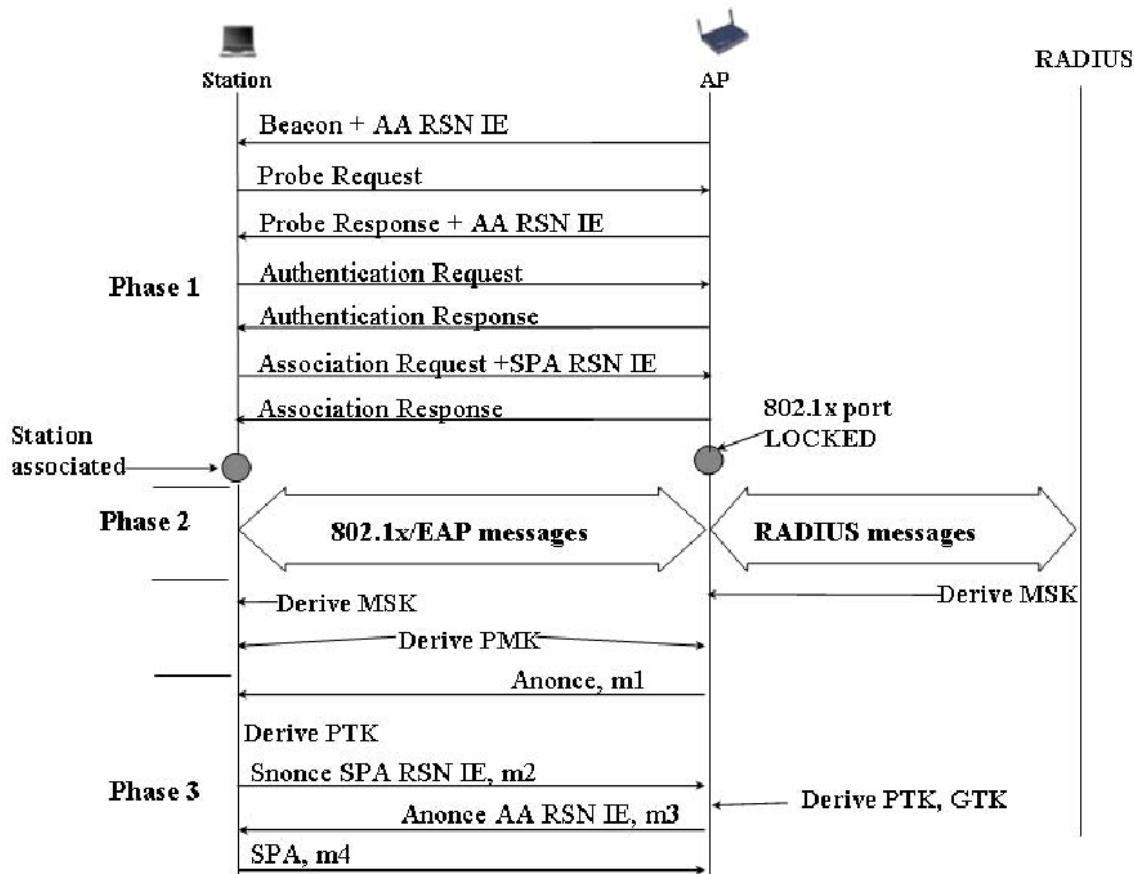


FIGURE 15 – 4-Way Handshake - WPA2-Entreprise

Source : <https://doiserbia.nb.rs/img/doi/1820-0214/2006/1820-02140602097P.pdf>

4-Way Handshake

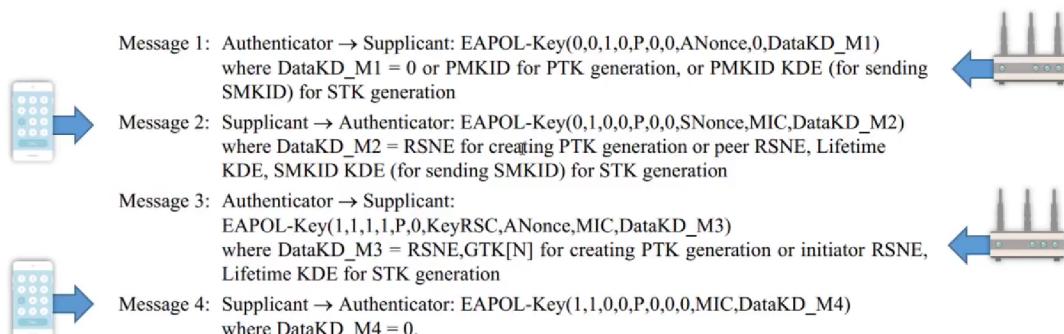


FIGURE 16 – Contenu des messages de la 4-Way Handshake - WPA2

Source : <https://www.youtube.com/watch?v=KtYjX8xWcOU>

4-Way Handshake – Message 1

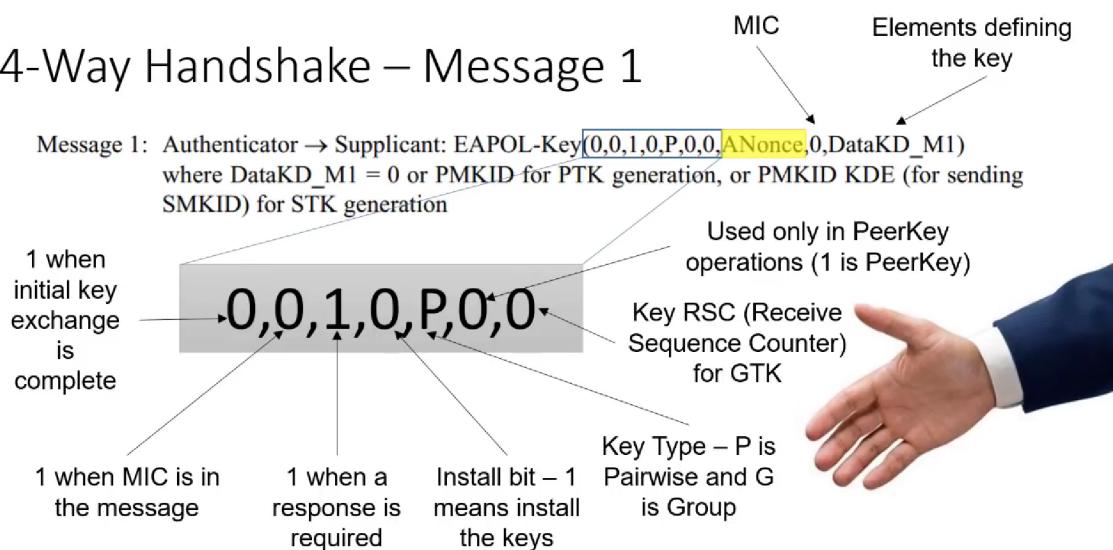


FIGURE 17 – Détail du message 1 - WPA2

Source : <https://www.youtube.com/watch?v=KtYjX8xWcOU>

3.2.7 Wireshark

Sur les captures d'écran de Wireshark, on peut observer les quatre messages de la 4-Way Handshake échangés entre le client et le point d'accès. Chaque message contient des informations clés telles que le WPA KeyNonce, le WPA Key MIC et d'autres paramètres du protocole WPA2. Ces informations sont visibles dans les champs des paquets échangés, permettant de suivre l'évolution du processus de négociation des clés.

En particulier, on peut voir le nonce généré dans le premier et le second message, ainsi que la validation de l'intégrité des messages grâce au WPA Key MIC. À partir du troisième message, les captures montrent que les clés de session sont bien installées sur les deux côtés, ce qui marque la fin de la 4-Way Handshake.

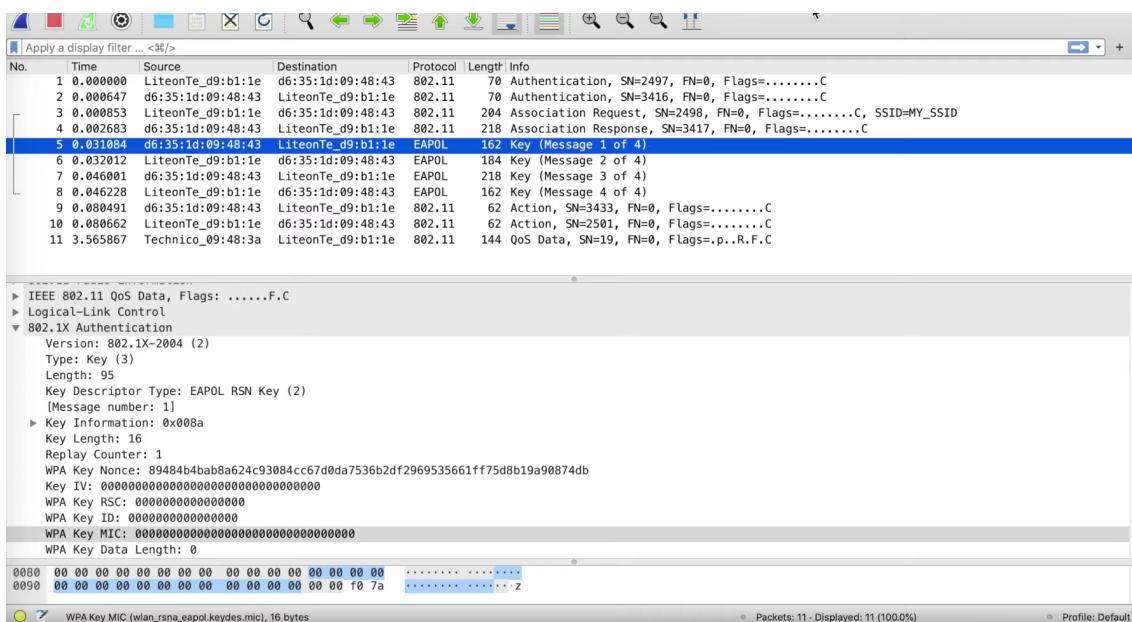


FIGURE 18 – Message 1 - WPA2

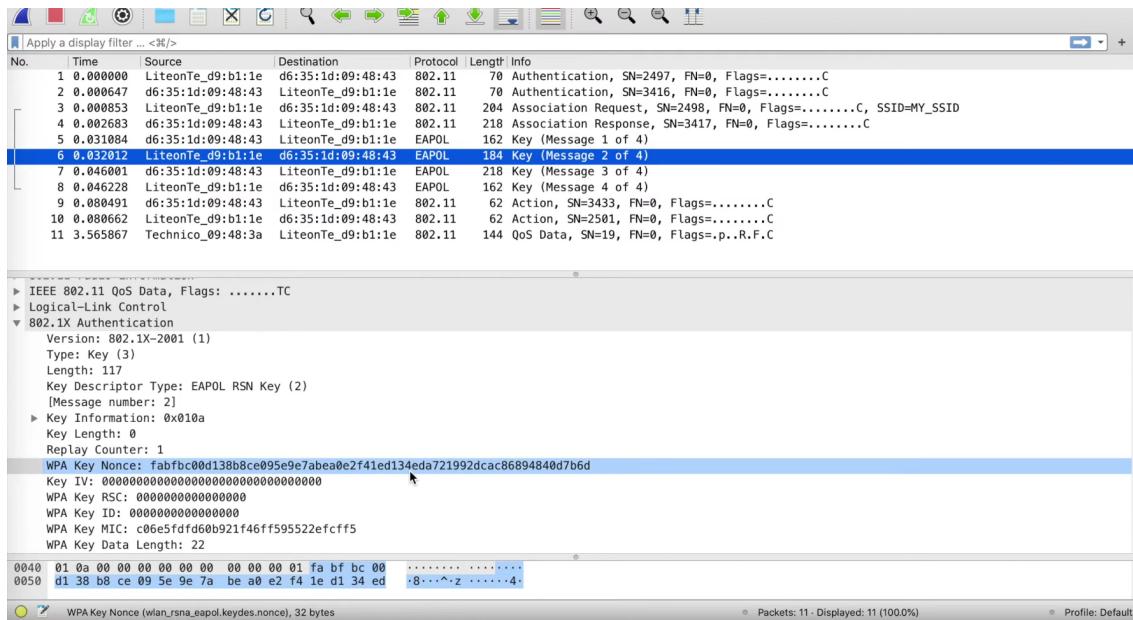


FIGURE 19 – Message 2 - WPA2

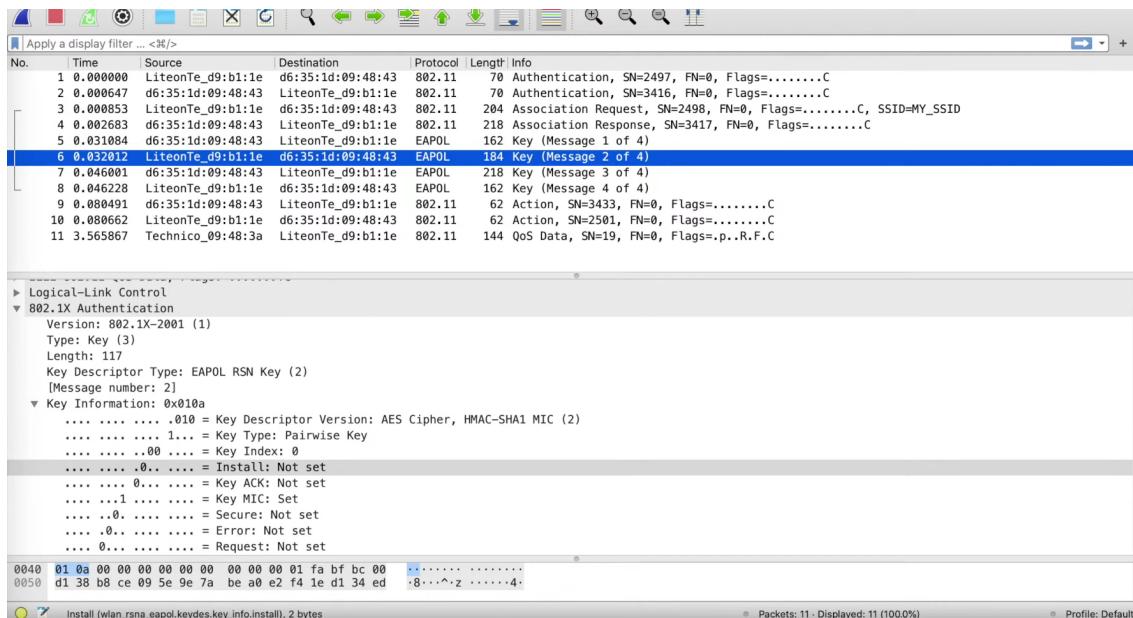


FIGURE 20 – Message 2, zoom sur les flags - WPA2

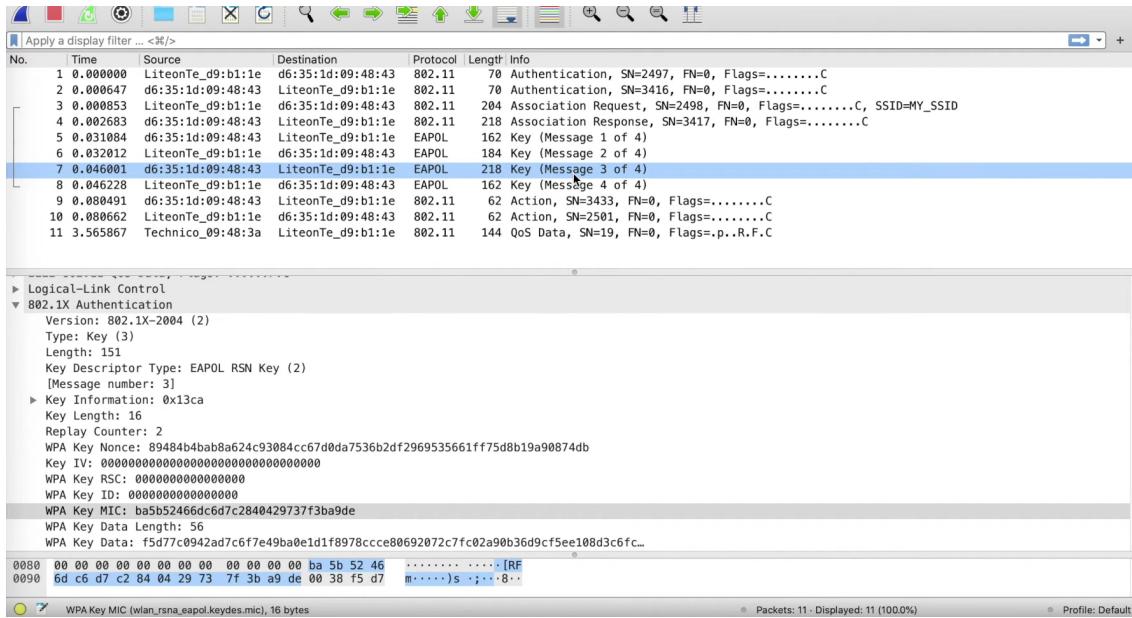


FIGURE 21 – Message 3 - WPA2

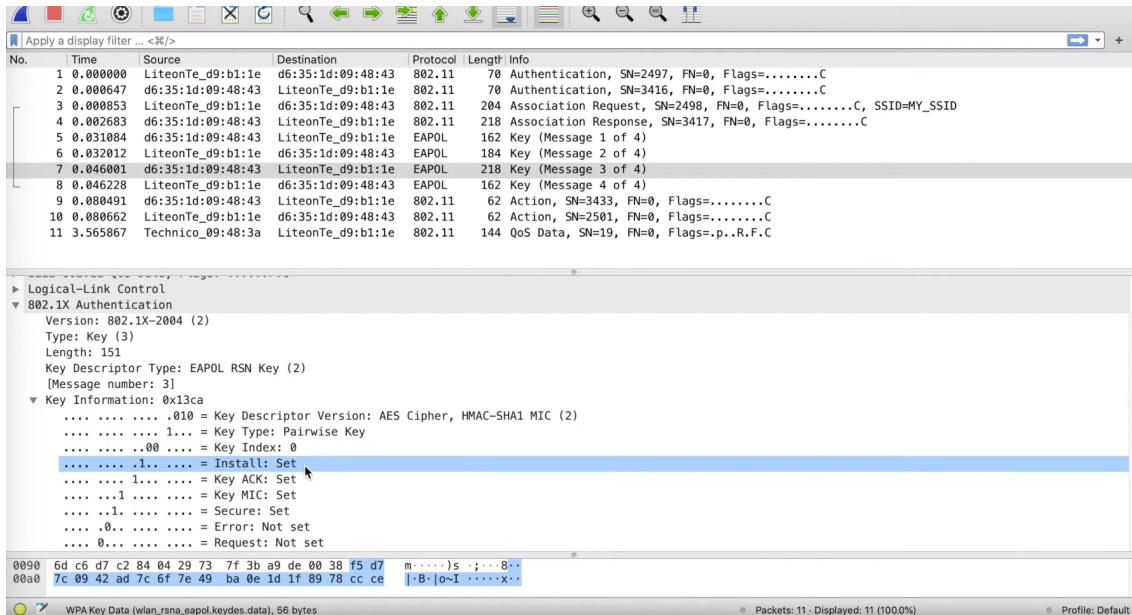


FIGURE 22 – Message 3, zoom sur les flags - WPA2

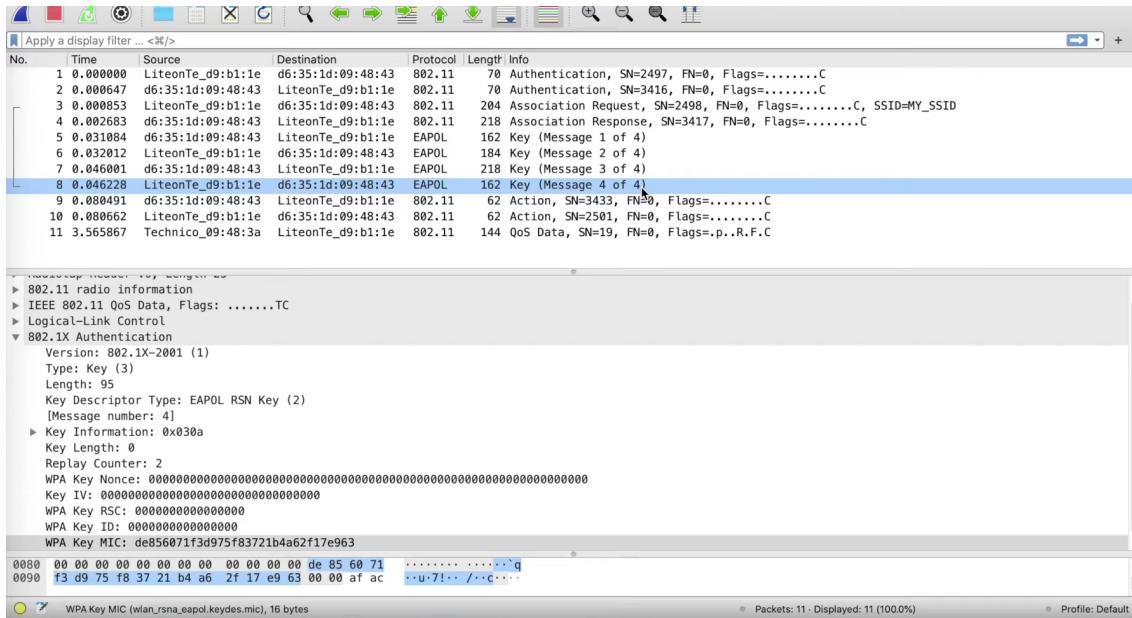


FIGURE 23 – Message 4 - WPA2

3.3 Group 2-Way Handshake

Les clés de groupe sont aussi renouvelées périodiquement par le point d'accès. Ces clés doivent être partagées avec l'ensemble des clients connectés au réseau. Lorsqu'un client se déconnecte du réseau, le point d'accès les renouvelle afin de garantir qu'elles ne restent accessibles qu'aux appareils encore connectés. Si ces clés sont mises à jour, le point d'accès les redistribue à tous les clients en initiant une poignée de main à 2 étapes (Group 2-Way Handshake) avec chacun d'entre eux. Ce processus similaire à la 4-Way Handshake, s'effectue en deux messages :

1. **Message 1** : Contient les nouvelles clés chiffrée avec la KEK, toujours accompagné d'un MIC.
2. **Message 2** : Une confirmation de réception, également protégée par un MIC.

Les deux messages utilisent des trames EAPOL. Ces trames sont chiffrées, puisque à ce stade la PTK est déjà installée. Elles utilisent le numéro de paquet actuel. Selon l'implémentation, le point d'accès installe les clés de groupe soit après avoir envoyé le message 1, soit après avoir reçu les réponses de tous les clients connectés.

3.4 Canaux et Interférences dans les Réseaux Wi-Fi

Dans les réseaux Wi-Fi, les canaux correspondent aux bandes de fréquences sur lesquelles les appareils communiquent. Chaque canal offre un environnement particulier, où la qualité de la transmission peut varier en fonction des interférences et des conditions du milieu. Comme plusieurs dispositifs peuvent chercher à communiquer simultanément sur une même bande, cela peut engendrer des interférences affectant la transmission des bits. Si le degré de perturbation excède la capacité de correction d'erreurs, trop de bits seront altérés et le contrôle par redondance cyclique (CRC) ne pourra plus valider la trame.

Pour minimiser ce risque, la plage de fréquence est divisée en plusieurs sous-ensembles, appelés canaux. Un point d'accès indique dans ses Beacon Frames ou Probe Responses le canal qu'il souhaite utiliser, permettant ainsi aux clients de se synchroniser précisément sur cette fréquence. Cette segmentation permet d'optimiser la gestion du spectre. Contrairement à des technologies comme le Bluetooth, le Wi-Fi ne procède pas à une alternance de canaux (channel hopping) durant la communication. Le choix du canal est donc fondamental pour limiter les interférences.

3.4.1 CRC

Il convient de préciser que le CRC, souvent implémenté sous la forme d'un champ FCS (Frame Check Sequence), est une méthode de détection d'erreurs appliquée à la couche MAC. Il permet

de vérifier qu'une trame n'a pas subi de modifications accidentelles durant sa transmission (par exemple, en raison de bruit ou d'interférences électromagnétiques). Ce mécanisme diffère toutefois du MIC. Tandis que le CRC garantit l'intégrité physique de la trame, le MIC assure l'intégrité et l'authenticité cryptographique des données, permettant de détecter toute modification malveillante dans les trames chiffrées.

3.4.2 Techniques d'Interception et de Redirection de Trames

Pour effectuer KRACK, l'attaquant doit pouvoir intercepter, bloquer, rejouer et potentiellement modifier certaines trames. Cependant, du fait de la nature du support utilisé (sans-fil), cela semble compliqué, rien ne garantit qu'il pourra le faire avant que le destinataire n'en reçoive l'original. Pour le réaliser de manière fiable en Wi-Fi, une astuce très simple exploite les canaux. Ce type d'attaque était bien connu sous le nom de Multi-Channel Machine-in-the-Middle.

L'attaquant doit appliquer un brouillage continu. Cette méthode, appelée jamming, consiste à générer un bruit suffisamment important pour invalider la réception correcte des trames. Le « Selective Jamming » se distingue d'un jamming classique par sa capacité à cibler précisément certaines trames plutôt que de saturer l'ensemble du canal. Pour cela, l'appareil attaquant doit être capable de deux choses :

1. D'abord, il doit écouter en continu le canal afin de repérer en temps réel la trame spécifique à jammer.
2. Ensuite, dès que cette trame est identifiée, l'appareil doit passer du mode réception (RX) au mode transmission (TX) très rapidement, et envoyer une impulsion ou un signal perturbateur destiné à corrompre le CRC de la trame, de façon à ce que le destinataire la considère comme invalide et interprète le canal comme trop perturbé pour communiquer.

Les trames Wi-Fi, qu'elles soient transmises sur la bande 2.4 GHz ou sur les bandes 5/6 GHz, circulent à une vitesse très élevée, ce qui rend le timing crucial. Si l'appareil attaquant n'est pas suffisamment performant pour passer rapidement du mode réception (RX) au mode transmission (TX) et émettre un signal perturbateur avant que le client ne reçoive et valide la trame, il peut être nécessaire d'utiliser deux interfaces Wi-Fi complémentaires (l'une dédiée à la réception et l'autre à la transmission) pour obtenir une réactivité suffisante permettant au selective jamming de fonctionner efficacement. Si l'attaque est bien synchronisée, elle peut altérer la trame de manière à ce que le CRC calculé par le récepteur ne corresponde pas au CRC reçu, entraînant le rejet de la trame.

Cette technique s'appuie sur l'analyse en temps réel des caractéristiques des paquets, telles que les adresses MAC et éventuellement d'autres marqueurs présents dans les MPDU (MAC Protocol Data Unit). C'est l'unité de données de base utilisée dans la couche MAC du standard IEEE 802.11, qui définit la structure et les règles de transmission des trames en Wi-Fi. Un MPDU englobe généralement plusieurs éléments : un en-tête (contenant des informations de contrôle et d'adressage telles que l'adresse MAC de destination et de source), une charge utile (le contenu utile ou les données utilisateur), et un champ de contrôle tel que le CRC qui permet de vérifier l'intégrité des données reçues. Dans le cadre d'une attaque par selective jamming, l'analyse de ces MPDU permet à l'attaquant d'identifier rapidement les trames critiques à bloquer, en se basant sur des informations telles que l'adresse MAC ou d'autres marqueurs spécifiques inclus dans l'en-tête.

L'attaquant peut cloner le point d'accès sur un canal alternatif. Concrètement, l'attaquant copie les Beacon Frames de l'AP (celles-ci n'étant pas protégées) en modifiant le champ du canal pour orienter le client vers un autre canal. Parallèlement, en brouillant en continu le canal initial, l'attaquant perturbe la communication sur ce dernier. Face à l'absence de Beacon Frames cohérentes et à une saturation provoquée par le jamming, le client perd la connexion avec l'AP légitime et cherche automatiquement à rétablir une communication stable, ce qui le conduit à s'orienter vers le canal alternatif proposé par l'attaquant. Dès que la trame d'authentification du client est reçue sur ce canal, le brouillage du canal original est arrêté, puisque, comme nous l'avons vu, il n'y a pas d'alternance de canaux en cours de communication. Cela permet alors de rediriger l'ensemble des échanges du client vers ce canal.

Prenons un exemple : si l'AP légitime opère sur le canal 6, l'attaquant réplique ce réseau sur le canal 1 et pousse le client à s'y connecter. Il se retrouve alors en position de *Man-in-the-Middle*. Même si la plupart des trames sont chiffrées et authentifiées, l'attaquant peut contrôler leur ordre

et leur timing. Il est ainsi capable de bloquer certaines transmissions et de rejouer des trames interceptées dans l'ordre d'origine, pour tromper les équipements légitimes.

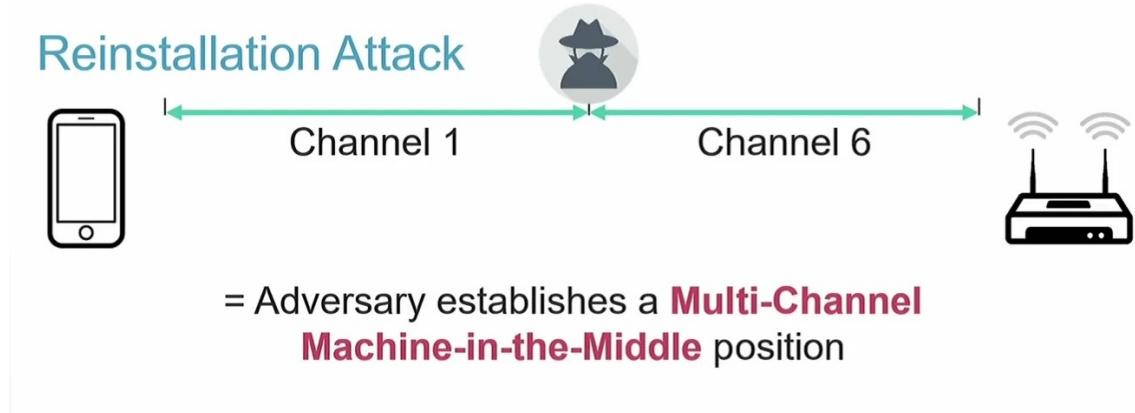


FIGURE 24 – Multi-Channel Machine-in-the-Middle - WPA
Source : <https://www.youtube.com/watch?v=KtYjX8xWcOU>

Where KRACK Operates

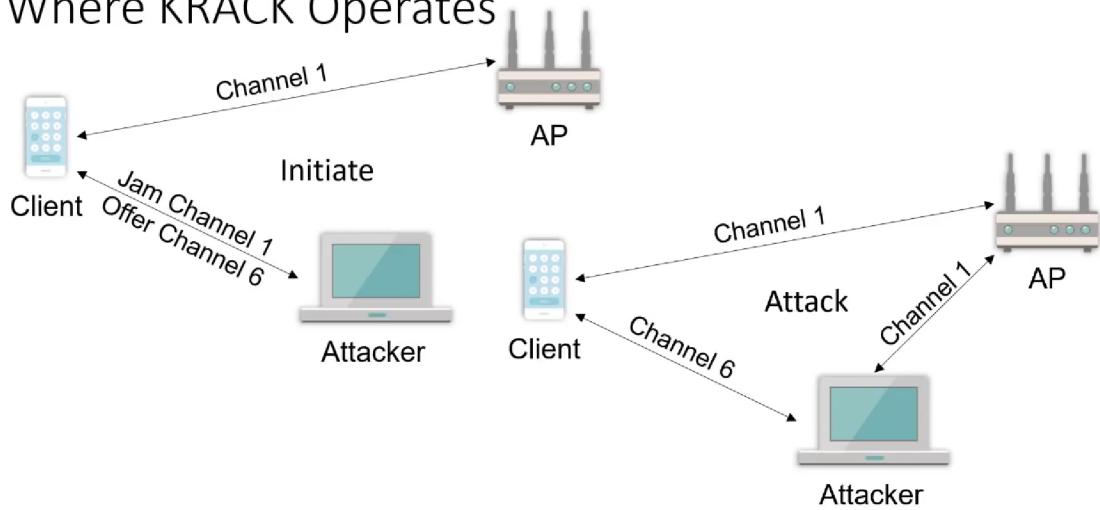


FIGURE 25 – Multi-Channel Machine-in-the-Middle 2 - WPA
Source : <https://www.youtube.com/watch?v=KtYjX8xWcOU>

Bien que l'attaquant puisse rejouer les trames sur le canal légitime, cette opération n'est pas exempte de contraintes. La présence du chiffrement et des mécanismes d'authentification rend toute manipulation délicate, l'attaquant devant respecter à la fois l'ordre chronologique et le timing précis des trames pour éviter des incohérences détectables par les dispositifs légitimes, pouvant entraîner une perte de synchronisation ou une alerte de sécurité.

4 Faille dans WPA2-PSK

Malgré sa robustesse apparente, le protocole WPA2-PSK présente plusieurs vulnérabilités ciblant la 4-Way Handshake qui peuvent être exploitées par des attaquants pour compromettre la sécurité du réseau sans fil.

4.1 Contexte et normes

Différents protocoles sont utilisés pour le chiffrement et l'intégrité des données une fois la clé partagée établie. Parmi eux, on retrouve TKIP (Temporal Key Integrity Protocol), aujourd'hui obsolète, CCMP (Counter-mode/CBC-MAC Protocol), qui est le standard largement adopté, et

GCMP (Galois/Counter Mode Protocol), également répandu.

Les protocoles CCMP et GCMP sont robustes, à condition que des règles strictes soient respectées, notamment l'unicité des valeurs utilisées pour le chiffrement, comme le nonce. Cette exigence est précisément celle qui est exploitée dans l'attaque KRACK.

Lors du 4-Way Handshake, nous avons vu que le nonce utilisé pour chiffrer les communications est le Packet Number (PN), qui est incrémenté à chaque message envoyé. Ce mécanisme garantit normalement l'unicité du nonce et, par conséquent, la sécurité du chiffrement. En cas de perte d'un message nécessitant une retransmission, le client le renvoie avec un PN incrémenté, assurant ainsi la continuité de cette unicité.

Une ambiguïté dans la norme IEEE 802.11 concerne la gestion des retransmissions des messages lors du 4-Way Handshake. En effet, la norme autorise la retransmission d'un message du handshake en l'absence de confirmation, mais elle ne précise pas explicitement que la clé de chiffrement ne doit être installée qu'une seule fois.

Ainsi, certaines implémentations de WPA2 réinstallent la clé de chiffrement lorsqu'elles reçoivent une retransmission du troisième message du handshake, ce qui entraîne la réinitialisation du compteur de nonce, essentiel pour garantir l'unicité des clés de chiffrement.

L'ambiguïté réside dans l'interprétation du comportement à adopter lorsqu'un client reçoit à nouveau un message M_3 alors qu'une clé est déjà installée. Celui-ci doit alors renvoyer un message M_4 , mais la norme ne précise pas explicitement que ce message doit être envoyé en clair. Comme les prochaines poignées de main sont protégé (normalement juste authentifié) à l'aide de l'ancienne clé, certaines implémentations l'ont donc renvoyé chiffré, ce qui constitue un écart critique par rapport à l'intention initiale. En effet, M_4 désigne un message spécifique, et non sa version chiffrée C_4 , car $C_4 \neq M_4$. Le renvoyer signifie transmettre à nouveau le même message en clair, comme lors du premier envoi. Cette confusion devient d'autant plus problématique lorsque le compteur de paquet à zéro est réinitialisé. Supposons que la clé soit K_0 . Le premier paquet réellement chiffré sera alors $P_1 = M_5 + K_0$. Si le client renvoie M_4 mais cette fois chiffré, on obtient $C_4 = M_4 + K_0$. Un attaquant, ayant intercepté M_4 en clair lors de la première poignée de main, peut alors calculer $P_1 + C_4 + M_4 = M_5$, ce qui lui permet de déchiffrer P_1 . Il s'agit ici d'une attaque par texte clair connu. Pire encore, en combinant $C_4 + M_4 = K_0$, l'attaquant peut directement obtenir la clé de chiffrement utilisée. Si le protocole repose sur un algorithme faible pour le calcul des MIC, comme dans le cas de TKIP qui ne résiste pas aux collisions, l'attaquant peut bloquer la transmission de P_1 , injecter un paquet forgé chiffré avec K_0 et doté d'un MIC valide via collision, usurpant ainsi l'identité du client pour introduire des trames malveillantes dans le réseau.

C'est précisément cette gestion des retransmissions qui est exploitée par KRACK pour forcer la réinstallation d'une clé déjà utilisée, compromettant ainsi la confidentialité et l'intégrité des communications.

4.2 KRACK (Key Reinstallation Attack)

Découverte en 2017, l'attaque KRACK exploite une faille dans la gestion du 4-Way Handshake. L'attaquant peut manipuler les messages échangés entre le point d'accès et le client pour forcer la réinstallation d'une clé déjà utilisée. Cela permet de décrypter les communications, voire d'injecter des paquets malveillants dans le réseau.

4.2.1 Vulnérabilité de réinstallation de la PTK : CVE-2017-13077

Pour exploiter cette faille, l'attaquant doit se positionner en tant qu'intermédiaire malveillant (Man-in-the-Middle) entre le client et le point d'accès. L'attaque suit le déroulement suivant :

CVE-2017-13077
PTK Reinstallation Vulnerability (Decryption)

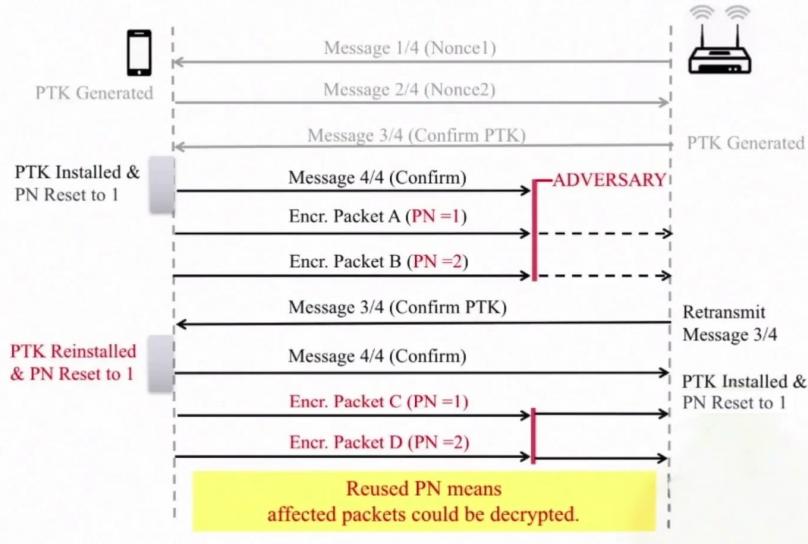


FIGURE 26 – Schéma de la vulnérabilité de réinstallation de la PTK
Source : <https://www.youtube.com/watch?v=g3i-rFq8TlI>

- Les trois premiers messages du 4-Way Handshake sont échangés normalement entre le client et l'AP.
- L'attaquant intercepte et bloque le quatrième message avant qu'il n'atteigne le point d'accès.
- Le client, ayant reçu le message 3 et envoyé sa réponse (message 4), croit que la session est correctement établie et commence à envoyer des paquets de données.
- Ces paquets ont un numéro de paquet (Packet Number, PN) qui commence à 1.
- L'AP, n'ayant jamais reçu le message 4, considère que la poignée de main est incomplète et retransmet le message 3 au client.
- Le client reçoit de nouveau le message 3 et réinstalle la même PTK, ce qui entraîne la réinitialisation du PN.
- Les paquets envoyés par le client après cette réinstallation auront le même PN que ceux envoyés précédemment, ce qui permet à l'attaquant de décrypter les communications.

Cette vulnérabilité compromet la sécurité des réseaux WPA2-PSK en permettant le déchiffrement des paquets. Le fait de réutiliser les PN casse la sécurité des protocoles CCMP et GCMP qui sont deux protocoles très robustes tant que les règles sont suivies, notamment le fait de ne jamais réutiliser un même Nonce pour chiffrer deux messages.

4.2.2 Vulnérabilité de réinstallation de la GTK et IGTK : CVE-2017-13078/CVE-2017-13079

Contrairement à la réinstallation de la PTK, cette attaque vise les clés de groupe (GTK/IGTK), utilisées pour chiffrer le trafic multicast et broadcast. En réinstallant ces clés, un attaquant peut intercepter et manipuler le trafic partagé dans un réseau WPA2.

CVE-2017-13080/81/87
GTK/IGTK Reinstallation Vulnerability (Replay)

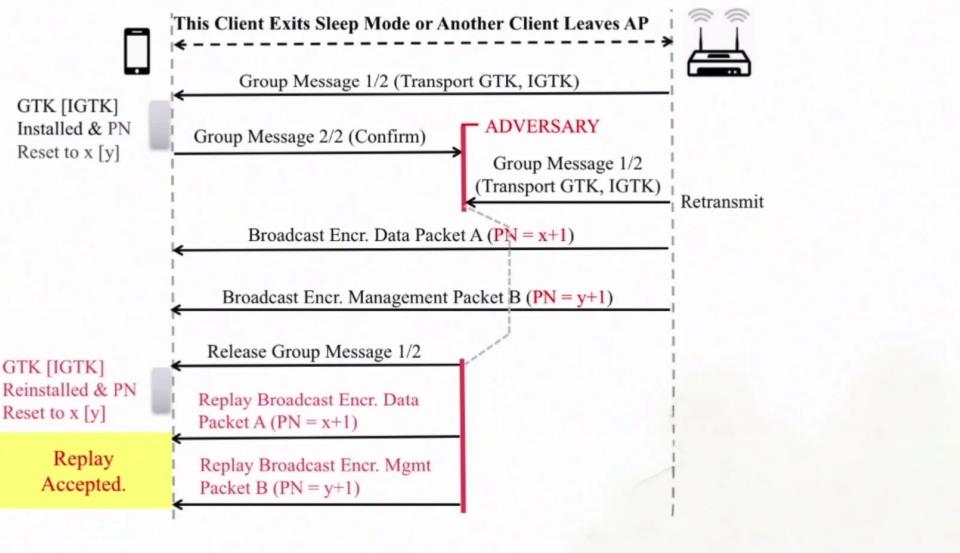


FIGURE 27 – Schéma de la vulnérabilité de réinstallation de la GTK et IGTK

Source : <https://www.youtube.com/watch?v=Zv64XXRx4zc>

- Les trois premiers messages du 4-Way Handshake sont échangés normalement entre le client et l'AP.
- L'attaquant intercepte et bloque le quatrième message avant qu'il n'atteigne le point d'accès.
- L'AP commence à broadcaster des paquets de données que l'attaquant intercepte.
- Ces paquets ont un numéro de paquet (Packet Number, PN) qui commence ($x+1$) et ($y+1$).
- L'AP, n'ayant jamais reçu le message 4, considère que la poignée de main est incomplète et retransmet le message 3 au client.
- Le client reçoit de nouveau le message 3 et réinstalle la GTK et IGTK avec le même packet number.
- L'AP reçoit le message 4.
- L'attaquant peut rejouer les paquets interceptés, entraînant la manipulation du trafic multicast/broadcast et l'injection de fausses informations.

L'attaquant peut bloquer le message de confirmation et la retransmission du message 1. Ainsi l'AP, pour ne pas faire attendre les autres clients injustement, commence à envoyer des paquets chiffré aux clients. L'attaquant peut alors rejouer le message 1 pour que notre client réinstalle ses clés et rejouer les paquets qui ont été envoyés avant la réinstallation.

En exploitant ces vulnérabilités, un attaquant peut forcer des utilisateurs à se reconnecter à un réseau compromis, récupérer des données sensibles, ou encore perturber le fonctionnement du réseau en injectant de faux paquets. Ces failles soulignent la nécessité de correctifs de sécurité.

4.2.3 Réinitialisation de la clé et exposition des paquets en clair

L'attaque KRACK exploite une faille dans le protocole WPA2 en forçant la réinstallation des clés de chiffrement (PTK et GTK). Certaines implémentations, notamment sous Linux et Android 6.0+, réinitialisaient ces clés à zéro lorsqu'une telle réinstallation était déclenchée. Cette erreur critique exposait directement le trafic réseau en clair, permettant à un attaquant d'intercepter et de lire les communications sans effort supplémentaire.

En revanche, d'autres systèmes comme Windows, macOS, iOS et OpenBSD conservaient l'ancienne clé après une réinstallation forcée. Bien que cela n'empêchât pas totalement l'exploitation de KRACK (notamment en permettant le rejet de paquets), l'impact restait moindre comparé aux systèmes où la clé était remise à zéro.

Le tableau suivant illustre les comportements des différentes plateformes avant l'application des correctifs de sécurité :

Système d'exploitation	Valeur de réinitialisation de la clé (avant patch)
Linux	Clé réinitialisée à zéro
Android 6.0+	Clé réinitialisée à zéro
Windows	Ancienne clé conservée
macOS	Ancienne clé conservée
OpenBSD	Ancienne clé conservée
iOS	Ancienne clé conservée

TABLE 1 – Réinitialisation de la clé avant les patchs KRACK

Dans le cas particulier de l'implémentation `wpa_supplicant` 2.4, utilisée notamment sous Linux et Android 6.0+, la seconde installation de la clé PTK aboutit à la configuration d'une clé entièrement nulle (tous les bits à zéro). Or, puisque la PTK sert à dériver plusieurs clés (dont la KCK utilisée pour le calcul du MIC), cette vulnérabilité offre une surface d'attaque critique. En effet, un attaquant à proximité peut non seulement intercepter et déchiffrer les paquets (ceux-ci n'étant plus chiffrés, dû à une clé nulle), mais également injecter ou forger librement des paquets. Si la PTK est fixée à zéro, le calcul du MIC devient trivial : l'attaquant peut générer un MIC approprié pour toute trame forgée en utilisant cette même clé nulle, contournant ainsi les mécanismes d'authenticité. En pratique, l'absence de clé fonctionnelle équivaut à établir une communication en clair, compromettant simultanément la confidentialité, l'intégrité et l'authenticité des échanges.

4.2.4 Exploitation du message 4 chiffré et récupération du keystream

Certaines implémentations envoyait un premier message 4 en clair avant l'installation de la clé de session (PTK & GTK), puis un second message 4, cette fois chiffré, après son installation. Ce comportement, bien qu'il puisse sembler anodin, introduisait une vulnérabilité critique exploitable par un attaquant. Cette particularité, bien que présente dans certaines implémentations, entre en contradiction avec la norme WPA2, qui stipule que le message 4 doit toujours être transmis en clair.

Un attaquant pouvait alors intercepter le message 4 en clair avant l'installation de la clé, puis capturer le message 4 chiffré envoyé après l'installation. En effectuant un XOR entre les deux versions du message 4, il obtenait directement le keystream utilisé pour chiffrer les paquets :

$$\text{Keystream} = \text{Message 4 clair} \oplus \text{Message 4 chiffré}$$

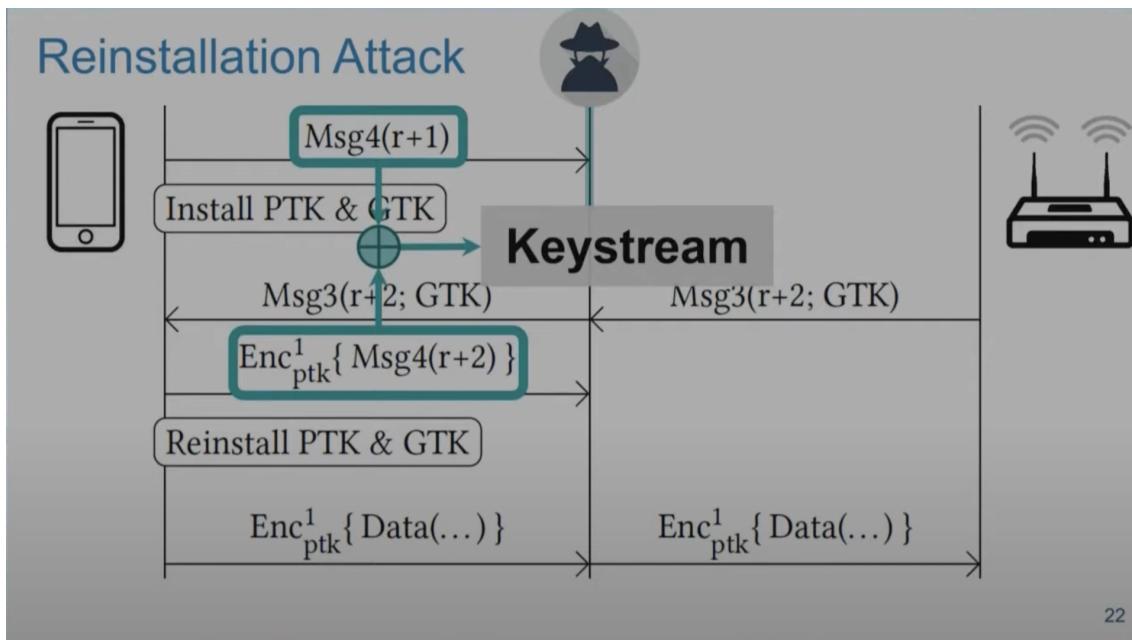
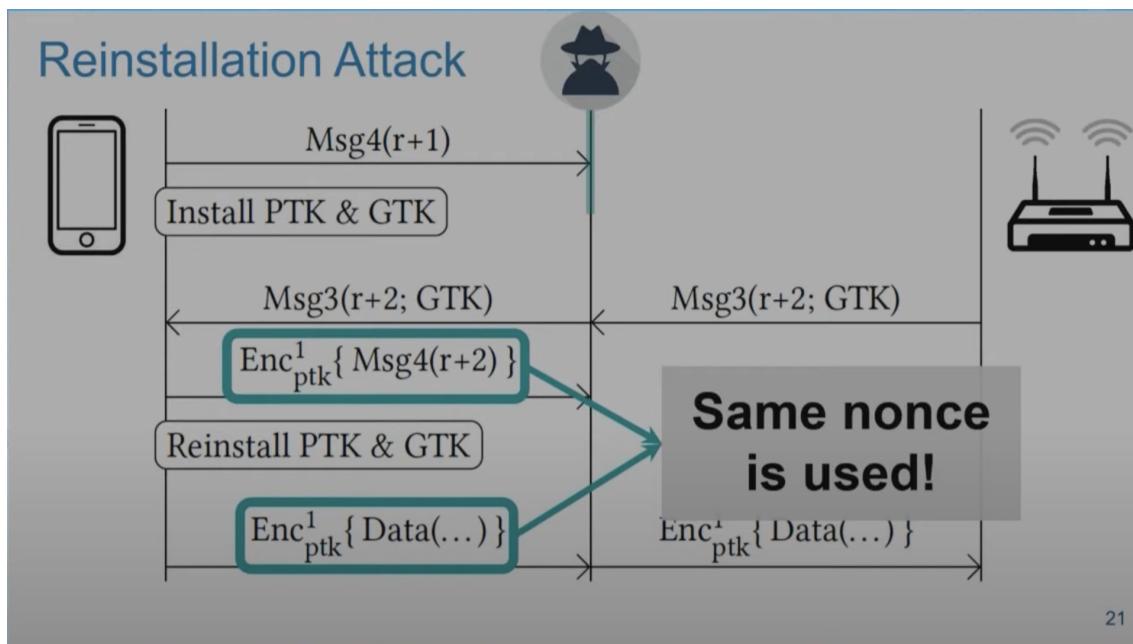


FIGURE 28 – Récupération du keystream - WPA2
Source : <https://www.youtube.com/watch?v=KtYjX8xWcOU>

Une fois le keystream récupéré, il est important de noter que le message 4 chiffré, tout comme les autres paquets qui seront envoyés par la suite, utilise le même nonce pour la génération du

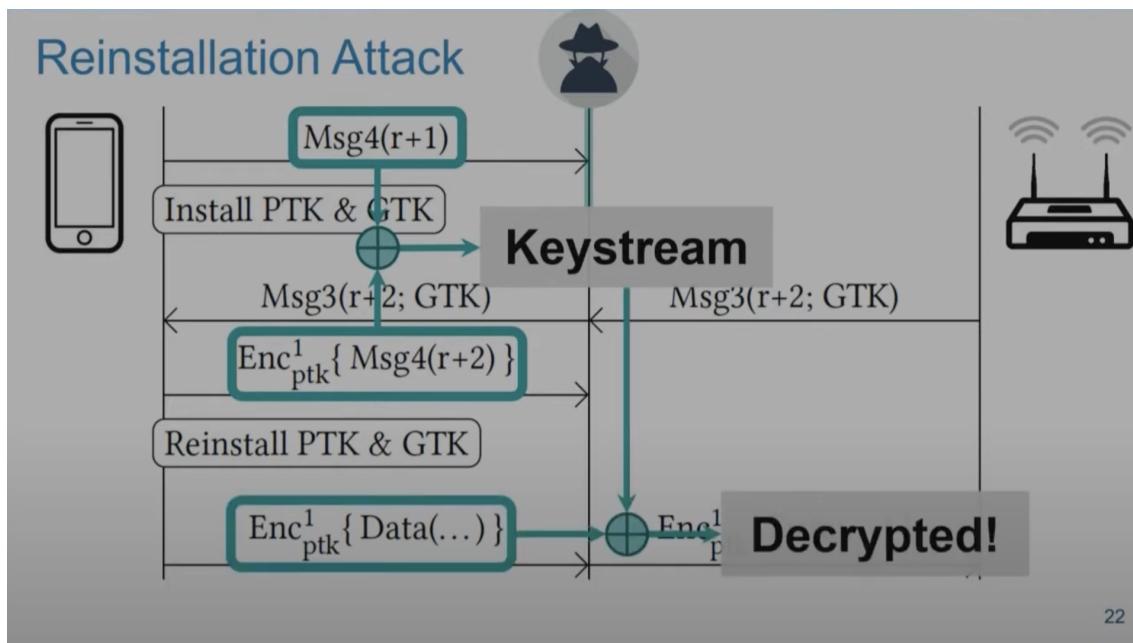
keystream. Cependant, dans ce cas précis, la réutilisation du nonce pour plusieurs paquets, y compris le message 4, compromet la sécurité de l'ensemble du système de chiffrement.



21

FIGURE 29 – Réutilisation du nonce pour chiffrer plusieurs paquets - WPA2
Source : <https://www.youtube.com/watch?v=KtYjX8xWcOU>

Puisque le message 4 et les autres paquets envoyés après utilisent le même nonce, un attaquant peut utiliser le keystream précédemment récupéré pour déchiffrer d'autres paquets. Cela rend l'attaque particulièrement efficace, car l'attaquant dispose désormais d'un moyen de déchiffrer les communications en continu.



22

FIGURE 30 – Extraction du keystream et déchiffrement des paquets - WPA2
Source : <https://www.youtube.com/watch?v=KtYjX8xWcOU>

Maintenant que nous avons la capacité de déchiffrer n'importe quel paquet échangé dans un réseau WPA2, cela signifie que la sécurité du protocole WPA2 est désormais compromise.

4.2.5 L'attaque par rejet de paquets

Bien que certaines implémentations conservent la clé après réinitialisation, permettant ainsi de limiter les effets de l'attaque KRACK, l'attaque présente une autre faiblesse critique : le rejet de paquets.

En effet, même dans les systèmes où la réinitialisation des clés ne pose pas de problème, l'attaque KRACK permet toujours de rejouer des paquets chiffrés. Le principe de l'attaque par rejet est de capturer des paquets légitimes envoyés sur le réseau, puis de les réinjecter dans le réseau. Étant donné que WPA2 n'inclut pas de mécanisme efficace pour vérifier que les paquets sont envoyés dans le bon ordre ou pour empêcher le rejet de paquets, un attaquant peut alors rejouer ces paquets pour provoquer des erreurs ou intercepter des données sensibles.

L'attaque par rejet est rendue particulièrement efficace par la possibilité de réutiliser le nonce, déjà compromis par l'attaque KRACK. Cette faille permet de rejouer des paquets avec les mêmes clés, rendant ainsi l'attaque plus menaçante et difficile à détecter.

5 Failles dans WPA2-Enterprise

Dans WPA2-Enterprise, l'authentification via un serveur RADIUS utilisant un protocole EAP pour négocier une clé secrète partagée avant d'entamer la 4-Way handshake pour obtenir des clés de sessions. Ce modèle offre une sécurité renforcée par rapport à WPA2-PSK en attribuant des identifiants uniques à chaque utilisateur. Fondamentalement, au lieu de commencer la 4-Way handshake avec un secret partagé (PMK) toujours identique, ici on le négocie à l'aide du protocole EAP. Cette clé secrète, nommée MK (Master Key), remplace le secret pré-partager (mot de passe) de WPA2-PSK. Toutefois, KRACK fonctionne exactement pareil et peut être exploitées pour compromettre la confidentialité des communications.

5.1 Vulnérabilités du 4-Way Handshake

Comme pour WPA2-PSK, l'attaque KRACK affecte WPA2-Enterprise en exploitant la réinstallation de la clé de session pendant la 4-Way Handshake. Un attaquant positionné en tant que Man-in-the-Middle peut intercepter toutes les communication entre le client et le point d'accès de la même manière. Il commence par retransmettre entièrement la phase d'authentification. Ensuite, il peut forcer la réinstallation des clés et entraînant la réutilisation des paramètres de chiffrement.

5.2 Faiblesses liées aux certificats et aux méthodes d'authentification

De nombreuses implémentations de WPA2-Enterprise utilisent des certificats pour authentifier le client auprès du serveur RADIUS. Cependant, des erreurs de configuration ou une validation insuffisante des certificats peuvent exposer le réseau aux attaques suivantes :

- **Attaques sur EAP** : Certains types d'EAP, comme EAP-MD5, sont vulnérables aux attaques qui peuvent exposer les mots de passe des utilisateurs.
- **Attaque de type rogue AP** : Un attaquant peut déployer un faux point d'accès imitant un réseau légitime, incitant les clients à s'y connecter et à divulguer leurs identifiants.

6 Un équipement relativement sophistiqué

L'attaque KRACK nécessite un équipement relativement sophistiqué. En effet, elle implique la capture et la retransmission de paquets (mode monitoring). L'attaquant doit pouvoir simultanément les transmettre (potentiellement modifié) et perturber les échanges sur le même canal, ce qui requiert d'un environnement contrôlé et d'une synchronisation extrêmement précise. La mise en œuvre du selective jamming demande des ressources importantes, car l'attaquant doit constamment surveiller le flux de données pour déterminer quelles communications interrompre. Pour réussir cette attaque, il est préférable d'être à proximité de la cible, idéalement à l'intérieur du bâtiment, ou d'utiliser des antennes performantes (permettant de transmettre un signal plus puissant que celui de l'AP). Un système avancé, comprenant du matériel et des logiciels spécialisés, est requis pour exécuter ces attaques efficacement.

7 Correctif

Face à la vulnérabilité KRACK, plusieurs mesures ont été mises en place afin de pousser la sécurité des communications Wi-Fi et d'empêcher les attaques par réinstallation de clé. Ces mesures concernent aussi bien les clients que les points d'accès.

7.1 Correctif coté client

Le problème principal de KRACK est l'implémentation de la 4-Way Handshake coté client. Il réinstalle une clé de chiffrement déjà utilisée. Un correctif simple, ne pas réinitialiser les paramètres de chiffrement (PN) si le client reçoit à nouveau un message 3. Il pourrait suspecter une activité malveillante et demander au point d'accès d'établir de nouvelles clés de session en renvoyer une nouvelle poignée de main. Il peut aussi respecter la norme en retransmettant le message 4 en clair et pas chiffré. En dehors de KRACK, pour WPA2-Entreprise, l'utilisation de certificats soigneusement vérifiés du serveur RADIUS est essentielle.

7.2 Correctif coté point d'accès

Bien que l'attaque cible principalement les clients, les points d'accès peuvent également être mis à jour pour atténuer les risques. Un correctif consiste à annuler la retransmission du message 3. Cependant, cela pose des problèmes de connectivité pour des clients légitimes qui pourraient ne pas recevoir ce message par des phénomènes physiques. Ce n'est donc pas la bonne solution.

7.2.1 Protected management frames

Les trames de gestion jouent un rôle clé dans l'établissement et la gestion des connexions sans fil. Avant l'introduction de la norme IEEE 802.11w, ces trames étaient transmises sans protection. Comme on a vu, KRACK exploite cette faiblesse en forçant un client à se reconnecter de manière contrôlée.

Les trames de gestion assurent plusieurs fonctions :

- **Association/désassociation et Authentification/ désauthentification** des clients avec un point d'accès.
- **Balises (beacons frames)** pour annoncer la présence d'un réseau.
- Demandes et réponses de sonde (**probe request/response**) utilisées lors de la recherche de réseaux.

Avec IEEE 802.11w, les trames de gestion critiques sont protégées. Les Protected Management Frames (PMF) protègent ces trames en les authentifiant avec un MIC à l'aide de la IGTK. Contrairement aux trames de données, ces trames étaient auparavant envoyées sans protection, ce qui les rendait vulnérables à des attaques comme la désauthentification forcée où l'attaquant envoie des trames de déconnexion à un client pour le forcer à quitter le réseau (Denial of Service) ou à KRACK.

Les trames concernées sont :

- Trames de désauthentification (**Deauthentication**).
- Trames de désassociation (**Disassociation**)
- Trames d'action robustes (**Robust Action Frames**), telles que : Gestion du spectre (**Spectrum Management**), qualité de service (**Quality of Service - QoS**), accusés de réception groupés (**Block Ack**).

En réalité, les PMF sont déjà disponibles dans WPA2 mais elles sont supportées en trois modes :

- **Désactivé** : Aucune protection des trames de gestion.
- **Optionnel** : Le point d'accès active les PMF avec les clients compatibles.
- **Obligatoire** : Tous les clients doivent utiliser les PMF, sinon ils ne peuvent pas se connecter au réseau.

Une fois la connexion établie, l'IGTK est distribuée aux clients par le point d'accès pour protéger les trames multicast et broadcast, tandis que les trames unicast utilisent la KCK.

La norme à également apporté des modifications aux capacités RSN. Les bits 6 et 7 sont maintenant utilisés pour indiquer des paramètres différents pour 802.11w.

Bit 6 : MFPR (Management Frame Protection Required) Ce bit est défini à 1 par le client pour indiquer que la protection des trames de gestion robustes est obligatoire. Cela signifie que le client n'acceptera de s'associer qu'à un point d'accès prenant en charge cette protection.

Bit 7 : MFPC (Management Frame Protection Capable) Ce bit est défini à 1 par le client pour signaler qu'il est capable de prendre en charge la protection des trames de gestion robustes. Lorsqu'un point d'accès définit également ce bit à 1, il informe les clients qu'il prend en charge cette fonctionnalité.

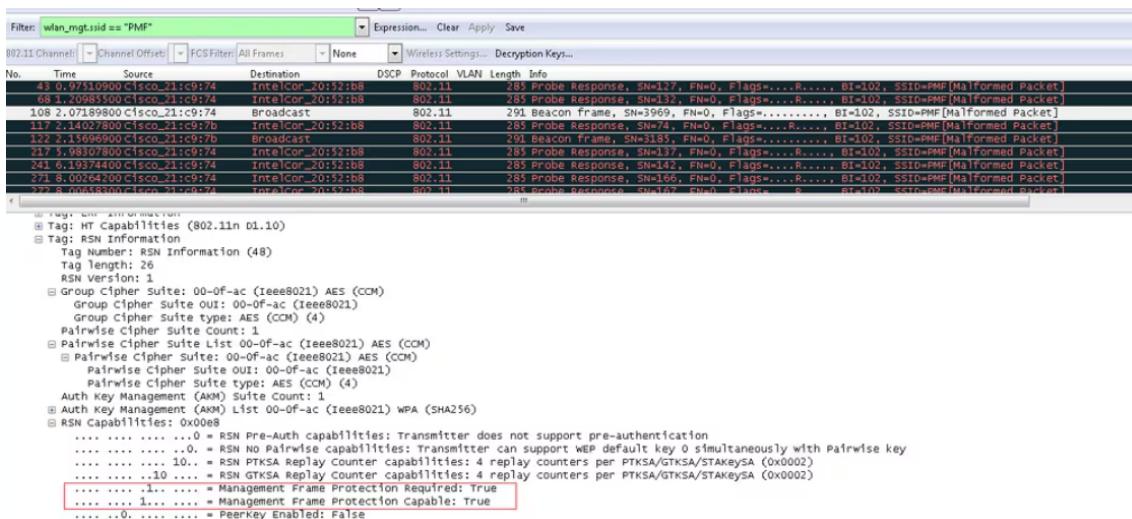


FIGURE 31 – Les bits 6 et 7 dans 802.11w - WPA2

Bien que les PMF ne corrigent pas directement la vulnérabilité KRACK, ils offrent une protection supplémentaire en empêchant certaines manipulations de trames de gestion. Ainsi, un attaquant ne peut pas utiliser des trames de désauthentification/désassociation pour forcer un client à se reconnecter à un réseau malveillant. L'attaquant devrait être présent au moment de la première connexion, ce qui complique l'exploitation de KRACK.

7.2.2 Beacons frames protection

Il est également possible de protéger la trame de gestion beacons à l'aide d'un MIC. Cette mesure est obligatoire dans le Wi-Fi 7. Le point d'accès génère une clé symétrique spécifiquement pour authentifier ces trames. Lorsqu'un client tente de se connecter au réseau, le point d'accès lui transmet cette clé dans un message protéger de la poignée de main. Le client peut alors tout abandonner si la clé est incorrecte, avant de commencer à envoyer des paquets chiffré. Le client doit alors mémoriser certaines informations du beacon avant de finaliser la poignée de main.

Beacon protection: new element

We add a **new type-length-value element** to beacons:

Element ID	Length	Key ID	Nonce	MIC
------------	--------	--------	-------	-----

- › Clients that do not recognize this element will ignore it
- › Nonce: incremental number to **prevent replay attacks**
- › Message Integrity Check: **C MAC or G MAC** over the beacon
 - » Existing crypto primitive of management frame protection
 - » All WPA3-capable devices already support it

FIGURE 32 – Beacons frames protection - WPA

Source : <https://www.youtube.com/watch?v=KtYjX8xWcOU>

En voyant l'Element ID, si un client ne supporte pas ce correctif, il ignorerá simplement cette trame et la clé symétrique qu'il reçoit. Le nonce est incrémenté de 1 à chaque envoi de celle-ci. Il est utilisé dans le calcul du MIC afin d'éviter les attaques par rejet. Les algorithmes CMAC et GMAC qui génèrent ces MIC ont été choisis pour rester rétrocompatibles. Cette méthode atténue aussi les attaques de rétrogradation mais à quand même un problème. Un client connecté au réseau connaît la clé symétrique et peut donc usurper cette trame en l'authentifiant avec la bonne clé. Elle ne doit donc surtout pas fuité.

Un fonctionnalité permet de signaler les beacons falsifiées. Si un client légitime détecte qu'il existe un réseau imitant le sien dont les trames beacons sont invalides. Il peut le signaler au point d'accès légitime. Cela peut être utile pour les administrateurs.

7.2.3 Channel validation

Même si le canal est communiquer dans la trame beacon qui est maintenant protégée. Une autre défense obligatoire dans le Wi-Fi 7, nommée validation de canal (Channel validation) complique la méthode Multi-Channel Machine-in-the-Middle. Lorsque le client se connecte au point d'accès, celui-ci authentifie le canal de communication qu'il souhaite utiliser. Il devient alors plus difficile pour un attaquant de bloquer de manière fiable les trames.

7.3 Mesures supplémentaires

Outre ces correctifs, d'autres mesures permettent de renforcer la sécurité des réseaux Wi-Fi :

- **Utilisation de TLS (Transport Layer Security)** : TLS chiffre les communications de bout en bout envoyées entre le client et le serveur (Client-to-site). C'est une couche de chiffrement supplémentaire.
- **Utilisation d'un VPN (Virtual Private Network)** : A la différence de TLS, un VPN chiffre l'ensemble du trafic réseau. C'est aussi une couche de chiffrement supplémentaire.
- **Détection des intrusions et comportements suspects (MAC Spoofing)** : Des solutions comme les WIPS (Wireless Intrusion Prevention Systems) et WIDS (Wireless Intrusion Detection Systems) surveillent le trafic réseau et détectent les comportements suspects. Ils peuvent détecter un nombre anormal de reassociation requests provenant d'un même client, bloquer un client ciblé par une attaque en l'isolant temporairement du réseau ou bien encore désactiver automatiquement un point d'accès s'il présente un comportement suspect.

- **Surveillance des points d'accès frauduleux (Rogue AP Detection)** : Les points d'accès peuvent surveiller les canaux afin de détecter des réseaux clones ou des SSID imités par un attaquant. On a vu que les clients peuvent aussi le faire.
- **Analyse avancée des signatures des appareils** : Certains contrôleurs Wi-Fi peuvent identifier les clients non seulement par leur adresse MAC, mais aussi par des caractéristiques comme le modèle ou fabricant de la carte réseau, la fréquence des connexions et les empreintes des signaux radio.

8 WPA3

Bien que les correctifs apportés à WPA2 corrigent KRACK, la meilleure solution reste la transition vers WPA3. Dès 2018, ce nouveau protocole introduit des améliorations majeures. Il augmente la longueur des clés à 192 bits et perfectionne le processus d'authentification grâce au protocole SAE (Simultaneous Authentication of Equals), une variante de Dragonfly Key Exchange, basé sur l'échange de clés Diffie-Hellman avec un secret partagé pour établir une session sécurisée.

8.1 OWE (Opportunistic Wireless Encryption)

OWE est une amélioration significative de la sécurité pour les réseaux ouverts. Traditionnellement, les communications y étaient transmises en clair. OWE assure un chiffrement entre le point d'accès et chaque client, sans nécessiter de mot de passe.

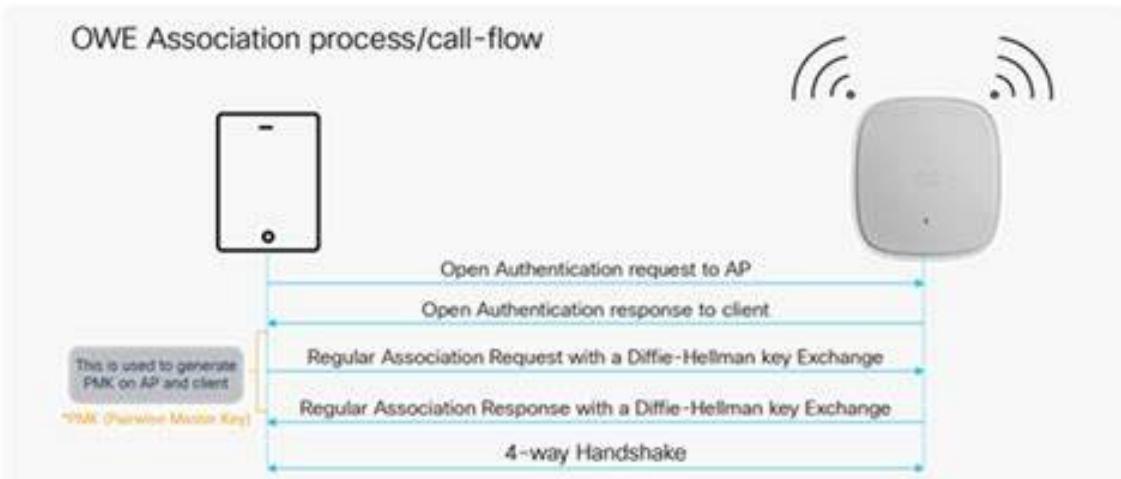


FIGURE 33 – Opportunistic Wireless Encryption - WPA3
Source : <https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/technical-reference/wpa3-dg.html>

OWE COMPARED TO OPEN SYSTEM AUTHENTICATION

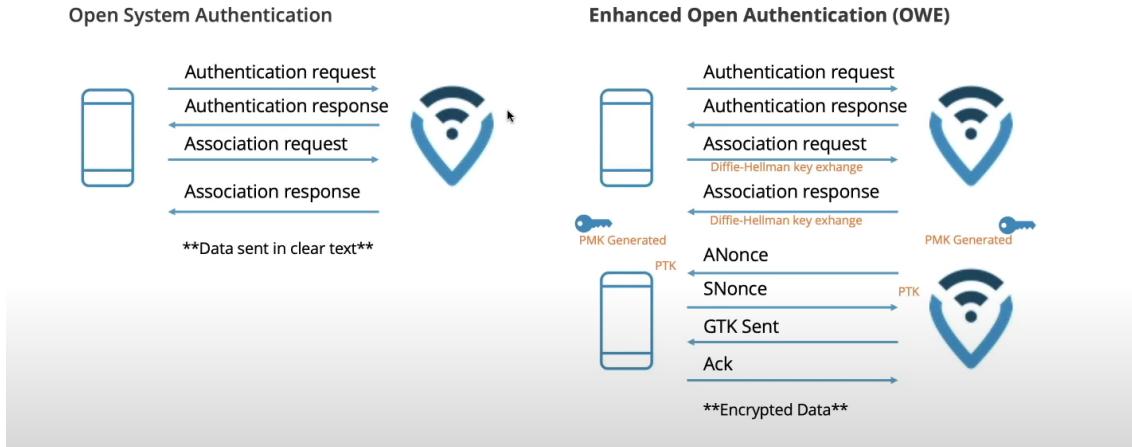


FIGURE 34 – Opportunistic Wireless Encryption - WPA3

Ce processus permet la création d'une clé secrète partagée. Dérivée d'un échange Diffie-Hellman, la méthode s'appuie sur des opérations dans un groupe cyclique fini, qui peut être un groupe modulo ou formé par certains points d'une courbe elliptique (MODP groups, Elliptic curves). Elle permet à chaque partie de générer une valeur publique à partir d'un choix secret (généralement aléatoire), puis de combiner ces valeurs pour obtenir une clé secrète commune. Ainsi, même si un attaquant intercepte toutes les trames échangées, il ne pourra pas récupérer la clé de session de l'utilisateur. OWE renforce donc la confidentialité des communications tout en maintenant la simplicité des connexions ouvertes.

8.2 SAE (Simultaneous Authentication of Equals)

SAE s'appuie sur la poignée de main Dragonfly (Dragonfly Handshake), conçue pour résister aux attaques par dictionnaire hors ligne. Cette poignée de main existait déjà depuis un certain temps, elle est utilisée dans le protocole EAP-PWD pour authentifier les utilisateurs (identifiant/-mot de passe) dans un réseau WPA2-Entreprise.

Essentiellement, si un attaquant capture l'intégralité du trafic réseau pendant un an et que la clé secrète finit par être compromise, il ne pourra toujours pas déchiffrer les données capturées. Cette poignée de main assure toujours une authentification mutuelle.

Lorsqu'un client cherche à se connecter à un point d'accès utilisant WPA3-SAE, plusieurs étapes ont lieu. Tout d'abord, le client propose un groupe à utiliser. Les deux appareils convertissent la clé secrète pré-partagé en un élément du groupe. Ici, le choix de l'élément n'est donc pas aléatoire. Ensuite, une phase de commit permet de négocier une clé secrète partagée entre eux. Elle est suivie d'une phase de confirmation où chacun vérifie qu'il possède bien la même clé. A noté que si le point d'accès ne supporte pas ce groupe il répond par un message de rejet qui est facile à usurper. Un attaquant peut alors faire une attaque par déclassement de groupe (group downgrade attacks) pour forcer les appareils à utiliser un groupe spécifique, idéalement faible. Cela à forcer, les chercheurs à définir une liste de groupe reconnu comme robuste à utilisé dans les implémentations.

Pendant la phase de commit, le client envoie son élément $x \bmod p$ ou un point $P = (x, y)$ suivant le groupe négocié. Le point d'accès ignore ce message si ce point P n'est pas sur la courbe ou si x ne se situe pas entre 1 et $q - 1$, où q est l'ordre du sous-groupe engendré par le générateur.

Dragonfly

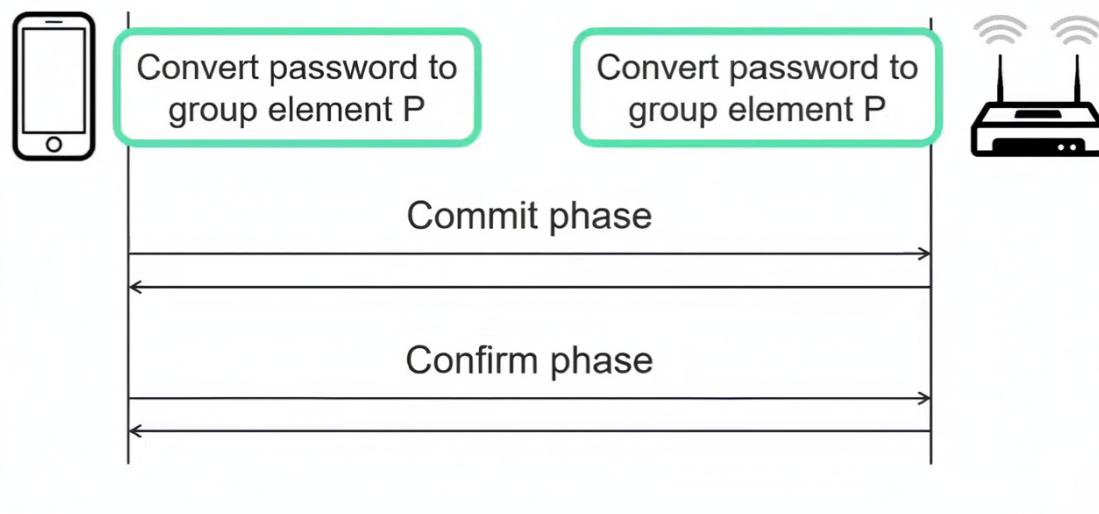


FIGURE 35 – Dragonfly - WPA3
Source : <https://www.youtube.com/watch?v=uzN7twQbEdQ>

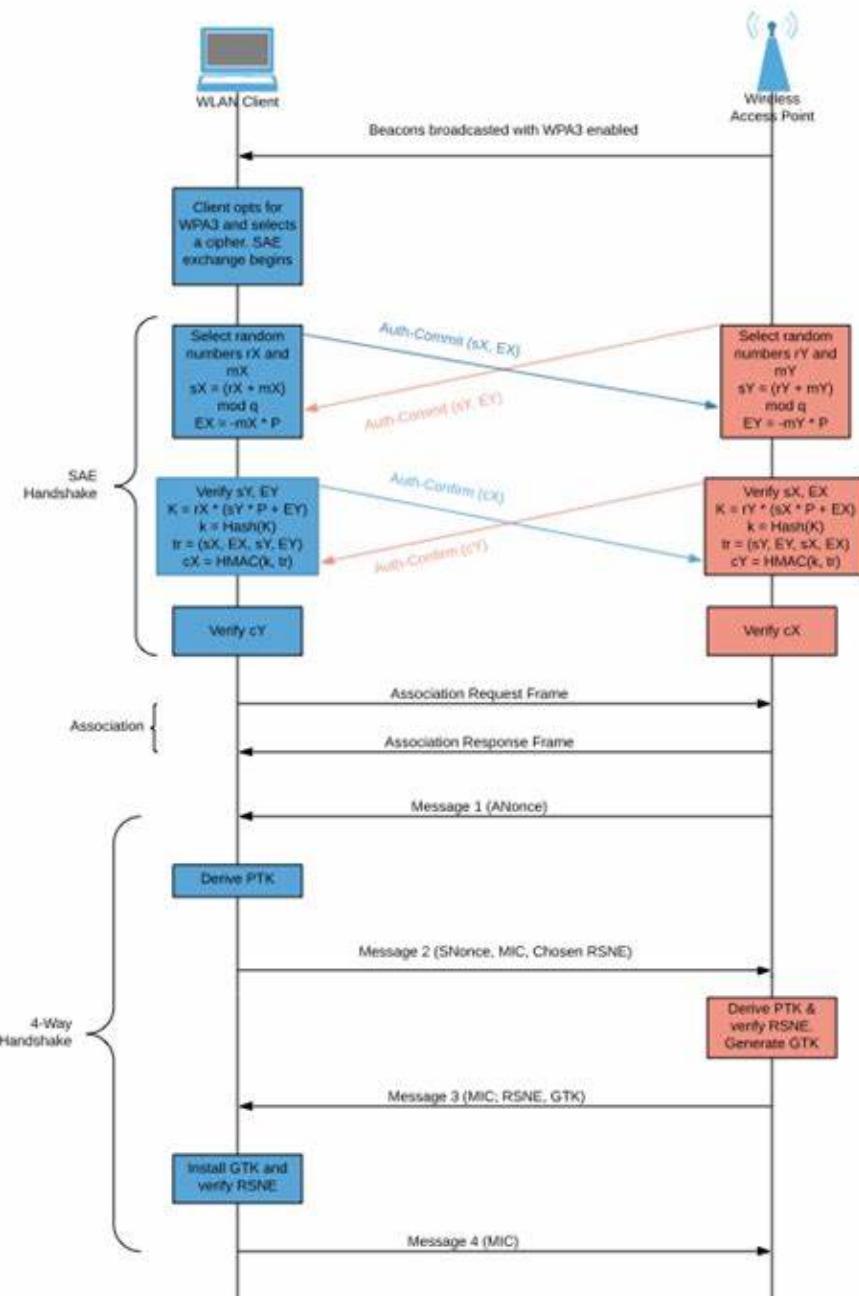


FIGURE 36 – Dragonfly - WPA3

Source : <https://wenzwu.com/2021/12/29/cissp-practice-questions-20211229/>

Le 11 octobre 2019, Mathy Vanhoef et Eyal Ronen ont publié une analyse critique du Dragonfly Handshake, identifiant des vulnérabilités dans WPA3 et EAP-PWD. Leur présentation à la conférence Black Hat USA a été reconnue par les Boney Awards comme la meilleure attaque cryptographique de l'année.

L'algorithme de conversion de la clé secrète pré-partagée (mot de passe) en un élément du groupe repose sur une fonction de hachage appliquée au mot de passe en clair combinées aux adresses MAC. Toutefois, pour certains groupes, il existe une forte probabilité que la valeur obtenue ne remplisse pas toutes les conditions requises pour garantir facilement l'obtention d'un élément du groupe. Il est donc nécessaire de s'assurer que la valeur de retour respecte certaines conditions. Pour cela, un compteur est ajouté en entrée de la fonction de hachage. Il est incrémenté à chaque fois que la valeur de retour ne satisfait pas les critères requis, permettant ainsi de recalculer un hachage avec des paramètres toujours différents jusqu'à remplir les conditions pour générer facilement un élément du groupe.

En fonction du mot de passe choisi, il se peut alors que l'algorithme calcul plus ou moins de

fois la fonction de hachage. Le mot de passe à donc une influence sur le temps de connexion, c'est une mauvaise chose.

Convert password to MODP element

```
for (counter = 1; counter < 256; counter++)
    value = hash(pw, counter, addr1, addr2)
    if value >= p: continue
    P = value(p-1)/q
return P
```

Hash-to-curve: WPA3 (simplified)

```
for (counter = 1; counter < 40; counter++)
    x = hash(pw, counter, addr1, addr2)
    if x >= p: continue
    if square_root_exists(x) and not P:
        P = (x, √x3 + ax + b)
return P
```

Code may be skipped!

FIGURE 37 – Covert password to element - WPA3

Source : <https://www.youtube.com/watch?v=uzN7twQbEdQ>

En effet, pour les groupes modulo p , si $value \geq p$ la formule $value^{\frac{p-1}{q}}$ ne donne pas forcément un élément du groupe engendré par le générateur. Dans les courbes elliptiques, il se peut que la racine carré n'a pas de solution ou bien que dans certains types de courbe (Bainpool curves), si $x \geq p$ cela peut aussi poser un problème.

Si on considère un mot de passe A qui demande un seul itération et un mot de passe B qui en demande plusieurs. Alors, un attaquant peut initier une poignée de main avec le point d'accès, observer le temps d'exécution de l'algorithme et donc différencier l'utilisation de A ou de B. On les appelle des attaques temporel (timing attacks).

Un détail à souligner est qu'avec les courbes elliptiques l'algorithme effectue toujours 40 itérations pour masquer cette information. Ce nombre 40 a été choisi de telle sorte que la probabilité d'avoir besoin de plus de 40 itérations est extrêmement faible. Mais cela ne suffit pas, l'attaquant peut contraindre quels blocs sont exécutés (Flush + Reload en mode monitoring) et toujours différencier l'utilisation de A ou de B. De plus, sachant que les opérations dans ces groupes sont assez gourmande cela utilise des ressources inutilement si notre mot de passe n'a besoin d'une seule itération. Comme l'élément du groupe dépend aussi de l'adresse MAC du client, le point d'accès ne peut pas le prédire. Il doit le recalculer à chaque poignée de main initiée. On pourrait alors congestionner le réseau, voire réaliser un déni de service, en initiant simultanément plusieurs poignées de main avec le point d'accès, ce qui aurait pour effet d'utiliser toutes ses ressources. Pour atténuer ce cas, il est possible de limiter le nombre de poignées de main simultanées.

Cette attaque reste extrêmement sophistiquée et coûteuse pour l'attaquant. Il doit être capable d'exécuter du code avec les bons priviléges sur l'appareil de la victime. Mais elle existe et reste praticable avec des moyens plus ou moins raisonnables. Un algorithme de cryptographie moderne se doit d'être résistant à ce type d'attaque.

Heureusement la norme a été mise à jour pour empêcher certaines de ces attaques. L'algorithme pour convertir les mots de passe a été changé pour avoir un temps constant. Il est différent suivant le type de groupe que l'on choisit.

Contrairement à WPA2-CCMP, WPA3-SAE rend impraticable la récupération du mot de passe à partir d'une capture de trames. Même si un attaquant enregistre tous les processus d'authentification, il est impraticable de faire une attaque par dictionnaire hors ligne. La vérification du mot de passe nécessite une interaction en direct avec le réseau. SAE intègre des mécanismes modernes pour résister aux attaques par rejet et aux tentatives de forçage par canal auxiliaire.

8.3 PMF obligatoires

L'une des faiblesses majeures des versions précédentes de WPA2 résidait dans l'absence de protection des trames de gestion. WPA3 impose l'utilisation obligatoire des PMF, garantissant ainsi l'authenticité et l'intégrité de ces trames critiques.

Avec les PMF, les attaques de type désauthentification forcée, utilisées pour déconnecter un client et tenter une attaque de type rogue AP ou KRACK, deviennent inefficaces. Toutes les trames

de gestion sensibles sont protéger et ne peuvent pas être falsifiées par un attaquant.

9 Conclusion

L'adoption de WPA3-SAE marque une avancée majeure dans la sécurisation des réseaux Wi-Fi contre les attaques modernes.

Il faudra un certain temps pour que WPA3 soit implémenter dans tout les appareils en circulation. Nous avons donc besoin d'un point d'accès qui supporte à la fois WPA2 et WPA3 avec le même mot de passe. Sans rentré trop dans les détails, pour empêcher une attaque par rétrogradation le client doit se souvenir si le point d'accès utilise WPA3. Si c'est le cas le client ne doit jamais revenir à WPA2. Sinon, encore une fois, on pourrait obtenir des informations supplémentaire sur le mot de passe pour effectuer notre attaque par dictionnaire. Cette méthode est similaire à la confiance sur la première utilisation utilisé dans SSH ou bien HTTPS.

Un autre point, WPA3 à besoin de stocker une version brut du mot de passe ce qui signifie que si notre point d'accès est compromis l'attaquant peut récupérer la clé secrète. L'idéal serait de stocker une version salé de la clé mais WPA3 ne le permet pas.

WPA3 offre une sécurité renforcée par rapport à WPA2.

Références

- [1] M. Vanhoef, F. Piessens. *Key Reinstallation Attacks : Forcing Nonce Reuse in WPA2*, 2017. [En ligne]. Disponible : <https://papers.mathyvanhoef.com/ccs2017.pdf>
- [2] Mathy Vanhoef. *KRACK Attacks - Breaking WPA2 by forcing nonce reuse*. [En ligne]. Disponible : <https://www.krackattacks.com/>
- [3] CERT-FR. *Alerte CERTFR-2017-ALE-014 – Vulnérabilités WPA2 (KRACK)*. [En ligne]. Disponible : <https://www.cert.ssi.gouv.fr/alerte/CERTFR-2017-ALE-014/>
- [4] Cisco. *WPA3 Deployment Guide*, 2023. [En ligne]. Disponible : <https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/technical-reference/wpa3-dg.html>
- [5] Abdou Guermouche. *Cours Sécurité Réseaux - Chapitre 5 : Sécurité WiFi*. [En ligne]. Disponible : <https://dept-info.labri.u-bordeaux.fr/~guermouc/SR/SR/cours/cours5.pdf>
- [6] Hackndo. *KRACK - Key Reinstallation Attacks*. [En ligne]. Disponible : <https://beta.hackndo.com/krack/>
- [7] Newbie Contest. *Comprendre le WEP - Forum*. [En ligne]. Disponible : <https://www.newbiecontest.org/forums/index.php?topic=4651.msg61609#msg61609>
- [8] w1.fi. *wpa_supplicant - Wi-Fi Protected Access supplicant*. [En ligne]. Disponible : https://w1.fi/wpa_supplicant/
- [9] YouTube. *Injection ARP - WEP Hack*. [En ligne]. Disponible : https://www.youtube.com/watch?v=bxJgYl_4gUU&t
- [10] YouTube. *Attaques Replay sur WPA*. [En ligne]. Disponible : <https://www.youtube.com/watch?v=L-ohPuPBle4>
- [11] YouTube. *KRACK Attacks : Breaking WPA2 (détail)*. [En ligne]. Disponible : <https://www.youtube.com/watch?v=KtYjX8xWcOU&t>
- [12] YouTube. *KRACK - Vulnérabilité WiFi*. [En ligne]. Disponible : <https://youtu.be/fZ1R9RliM1w?si=TRP6L04g8cqniyKO>
- [13] YouTube. *Playlist sécurité WiFi – KRACK, WPA, etc..* [En ligne]. Disponible : <https://www.youtube.com/watch?v=LWz2DNUHp0Y&list=PLzKIBgD3ky20pBEZKz6o7X0gNBQPLIrBi>
- [14] YouTube. *Playlist Sécurité WLAN – WEP, WPA, WPA2.* [En ligne]. Disponible : <https://www.youtube.com/playlist?list=PLzKIBgD3ky20pBEZKz6o7X0gNBQPLIrBi>
- [15] YouTube. *Comprendre le chiffrement WEP*. [En ligne]. Disponible : <https://youtu.be/uzN7twQbEdQ?si=ZU-x1msXS08LRhTJ>
- [16] YouTube. *Histoire des protocoles WPA/WPA2*. [En ligne]. Disponible : https://youtu.be/Z4946fE-FiQ?si=FIuBvVqt9_RGYCxk