Enseirb-matmeca 2020/2021
Département Informatique / 2A

Faiblesse Wifi

Mémoire

Réalisé par

- Mohammed Boudali
- Saad Margoum

Encadré par

M. Jonathan Durant

Table des matières

1 Introduction

À cause des avantages que le réseau "Wifi" offre, comme la facilité de la connexion, coût d'installation et la mobilité des appareils connectées (pouvoir se déplacer dans un locale puisque le réseau n'exige pas un branchement des appareils), plusieurs entreprises sont passées des technologies filaires aux technologies sans fil. Néanmoins les réseaux filaires sont plus faciles à sécuriser que les réseaux sans file qui présentent plusieurs failles exploités par les cybercriminels. Dans ce mémoire on va voir des mécanismes utilisé par le réseau "Wifi" et les failles qu'ils présentent, des démonstrations de quelques méthodes d'attaques, et des méthodes de protection contre ces attaques.

2 Fonctionnement de Wifi

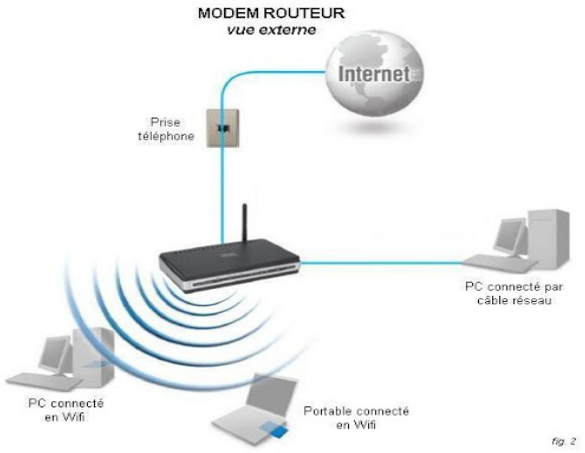
2.1 Définition :

Le mot "Wifi" est une abréviation de "Wireless Fidelity" qui signifie "Fiabilité du sans fil". Le réseau "Wifi" est un réseaux locale inventé en 1999 qui fonctionne à l'aide des ondes radioélectriques. et qui permet de relier plusieurs appareils.

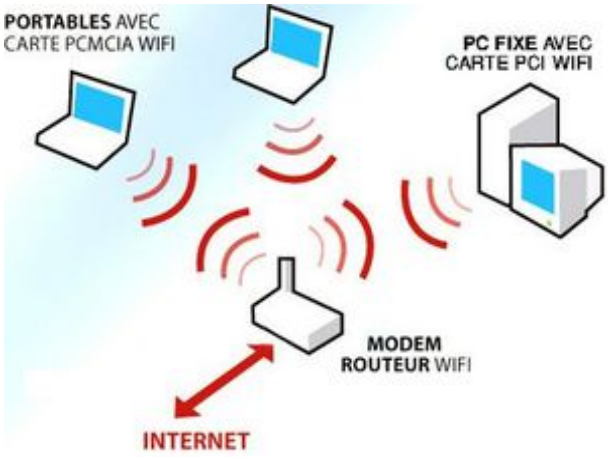
2.2 Comment fonctionne le "Wifi"

Pour que la connexion "Wifi" fonctionne, la machine utilisée (ordinateur, téléphone ...) doit être équipé d'un adaptateur réseau sans fil qui permet la conversion des informations envoyées en un signal radio qui sera communiqué à un routeur qui joue le rôle d'un décodeur via une antenne. Une fois le signal soit décodé, les informations sont transmises à l'internet via une connexion internet filaire.

Le réseau "Wifi" est basé sur un trafic bidirectionnel : les données envoyés par internet sont aussi envoyées vers le routeur pour les transformer en des signaux radios qui seront réceptionnés par l'adaptateur sans fil de l'ordinateur.



utilisation du connexion filaire



la transmission des ondes radioélectriques

3 Mécanismes de sécurité

3.1 WEP

Le mot "WEP" correspond à "Wired Equivalent Privacy", c'est un protocol qui permet la sécurisation des réseaux sans fil de type "Wifi". Ce protocole tient son nom du fait qui est censé armer le réseau d'une sécurité équivalente à celle du réseau filaire. Malheureusement des cryptologues ont identifié plusieurs failles que ce protocole dispose. Ce qui a rendu "WEP" un protocole qui fournit un niveau minimale de sécurité qui peut arrêter des attaquants peut expérimentés.

3.1.1 Description et fonctionnement

Le protocole "WEP" utilise un algorithme de chiffrement par flot **RC4** (catégories de chiffrements modernes en cryptographie symétrique), afin de vérifier la somme de contrôle **CRC-32** pour assurer l'intégrité et la confidentialité lors de transfert de données.

Pour chiffrer les données échangées, "WEP" utilise une clé RC4 de taille 128 bits qui est une combinaison d'une **clé de chiffrement** de 104 bits et un **vecteur d'initialisation (IV)** de 24 bits généré aléatoirement dans chaque échange. cette clé permet de chiffrer les données à l'aide de l'opérateur **XOR (OU exclusif)**.

Pour déchiffrer les données crypté on doit récupérer la clé de chiffrement (KeyID) et le vecteur d'initialisation (IV) qui se trouvent en claire dans la trame, pour construire le **"keystream"** utilisé pour le chiffrement. Ensuite on opére un **XOR** entre le **cryptogramme** et le **"keystream"** pour récupérer les données.

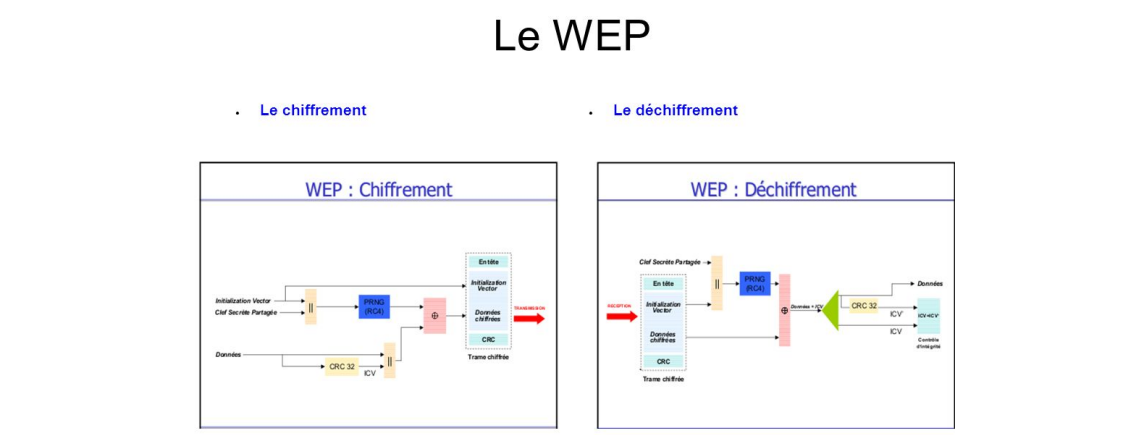


FIGURE 1 – Chiffrement et déchiffrement de données en WEP

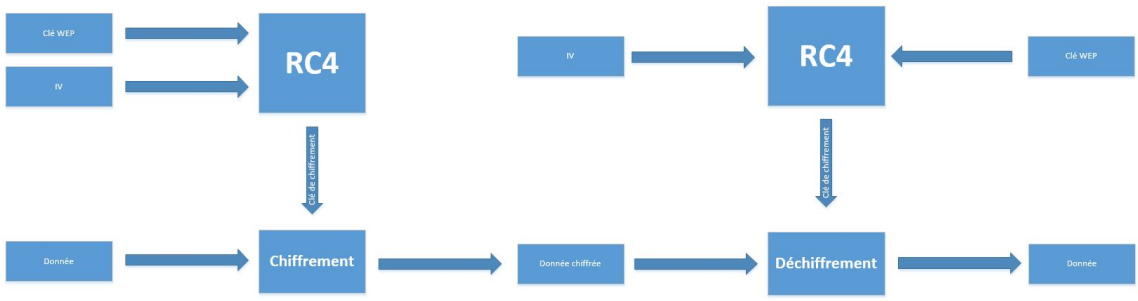


FIGURE 2 – Vue global sur le fonctionnement du WEP

3.1.2 Failles du mécanisme

Le mécanisme **WEP** a présenté nombreuses vulnérabilités autant sur l'intégrité des données échangés ou la confidentialité et ceci est dû a :

- Les faiblesses de l'algorithme de chiffrement **RC4**.
- Les **vecteurs d'initialisation (IV)** ne sont pas assez nombreux : puisque la clé est codée sur 24 bits, il y a une chance de **50%** sur 5000 paquets qu'il y ait un **IV** qui soit utilisé une seconde fois.
- La vérification du **RC32** de l'intégrité des paquets n'est pas fiable.

Un réseau **WI-FI** qui utilise le mécanisme **WEP** peut être attaqué par l'utilisation de l'outil **AIR-CRACK**, doté d'un sniffer **(Airodump)**, d'un injecteur de paquets **(Aireplay)**

et d'un casseur de clés **WEP (Aircrack)**.

La méthode d'attaque en général consiste à identifier les **vecteurs d'initialisation (IV)** singuliers par génération d'un trafic entre l'utilisateur et le point d'accès. Après l'identification des **IV** le déchiffrement de certain données devient assez facile surtout les données à taille limite comme les adresses **IP** et les adresses **MAC**.
Désormais un attaquant peut découvrir la clé de chiffrement en moins d'un minute lorsque le **WEP** est activé.

3.2 L'arrivée de WPA et WPA2

Wi-Fi Protected Access (WPA et WPA2) est un mécanisme de sécurisation des réseaux sans-fil de type **Wi-Fi**. Ils ont été inventés en réponse aux nombreuses faiblesses que le mécanisme **WEP** a présenté.
Les mécanismes **WPA et WPA2** fournissent une bonne sécurité, si les deux points suivants sont respectés :

— Il faut expliciter le choix de **WPA ou WPA2** car le mécanisme **WEP** est le mécanisme de chiffrement par défaut sur la plupart des équipements.

— Il faut choisir des mots de passes **WI-FI** longs et compliqués.

Avant de commencer la description de ces mécanismes de chiffrement on va distinguer deux méthodes d'authentification identiques pour **WPA** et **WPA2** qui concernent deux types d'utilisateurs visés :

— **WPA/WPA2 personnel :** Créé pour les réseaux des particuliers ou des petites entreprises. Chaque machine doit s'identifier auprès du même point d'accès en utilisant une même clé de 256 bits, notée **PSK**.

— **WPA/WPA2 entreprise :** Créé pour les réseaux des entreprises, il exige l'installation d'un serveur d'authentification **RADIUS**, et l'utilisation du protocole **EAP** (Extensible Authentification Protocol) pour l'authentification.

Dans le reste de ce mémoire les mécanismes **WPA** et **WPA2** abordés sont dans le cadre d'un réseau personnel et utilisent la **PSK (Pre-Shared Key)**.

3.3 WPA

Le mécanisme **WPA** respecte la majorité de la norme IEEE802.11i et a été envisagé comme une solution intermédiaire pour remplacer le **WEP** en attendant que la norme 802.11i soit terminée. **WPA** a été conçu pour fonctionner, après mise à jour de leur micro-logiciel, avec toutes les cartes WI-FI, mais pas nécessairement avec la première génération des points

d'accès Wi-Fi.

3.3.1 Description et fonctionnement

Ce mécanisme utilise le même algorithme de chiffrement que **WEP (RC4)** car il est un peut gourmand en ressources. Cependant il implémente des sécurités supplémentaires comme :

- La longueur du **Vecteur d'initialisation (IV)** a passé de **24 bits à 48 bits**.
- La longueur de la clé **PSK (Pre-Shared Key)** a passé à 124 bits.
- Le **vecteur d'initialisation (IV)** est envoyé hashé (il n'est plus envoyé en clair).
- Le mécanisme **CRC-32** qui n'est pas fiable à vérifier l'intégrité des paquets est remplacé par le mécanisme **MIC (Message Integrity Code)**.
- La clé de chiffrement des données est modifiée à chaque fois que 10ko des données sera envoyé, il s'agit de l'algorithme **TKIP(Temporal Key Integrity Protocol)**.

Le mécanisme **WPA** utilise un algorithme **TKIP** qui est basé sur la génération des clés de chiffrement temporaires à l'aide du **4-Way Handshake**. Le **4-Way Handshake** permet l'établissement d'une connexion entre les utilisateurs et le point d'accès. Le mécanisme d'authentification utilise une clé appelée **PMK (Pair Wise Master Key)** qui est de taille fixe et réversible. Cette clé est générée à l'aide du **PSK (Pre-Shared Key)** et le **SSID** du point d'accès.
La clé **PMK** n'est pas utilisée pour crypter les données mais pour générer une clé temporaire nommée **PTK (Pairwise Transient Key)**, au travers d'une suite de 4 étapes principales :

1. L'AP envoie un nombre pseudo aléatoire nommée **ANonce** à l'utilisateur.
2. De son tour l'utilisateur génère un nombre pseudo aléatoire nommé **SNonce**, puis il génère la clé **PTK** par concaténation du **PMK**, **ANonce, SNonce**, son adresse **MAC** et celle de **l'AP**. ensuite il envoie le **SNonce** à l'AP avec un **MIC**.
3. L'AP génère aussi la **PTK** et valide le **MIC**. Cela permet de savoir si l'utilisateur connait bien la **PMK**, sinon il crée une nouvelle clé, puis il envoie une clé nommée **GTK** à l'utilisateur accompagné d'un **MIC**, comme sa il informe le client qu'il peut installer la **PTK** et eventuellement la **GTK**.
4. L'utilisateur répond par acquittement pour dire qu'il a bien installé la **PTK** et la **GTK**.

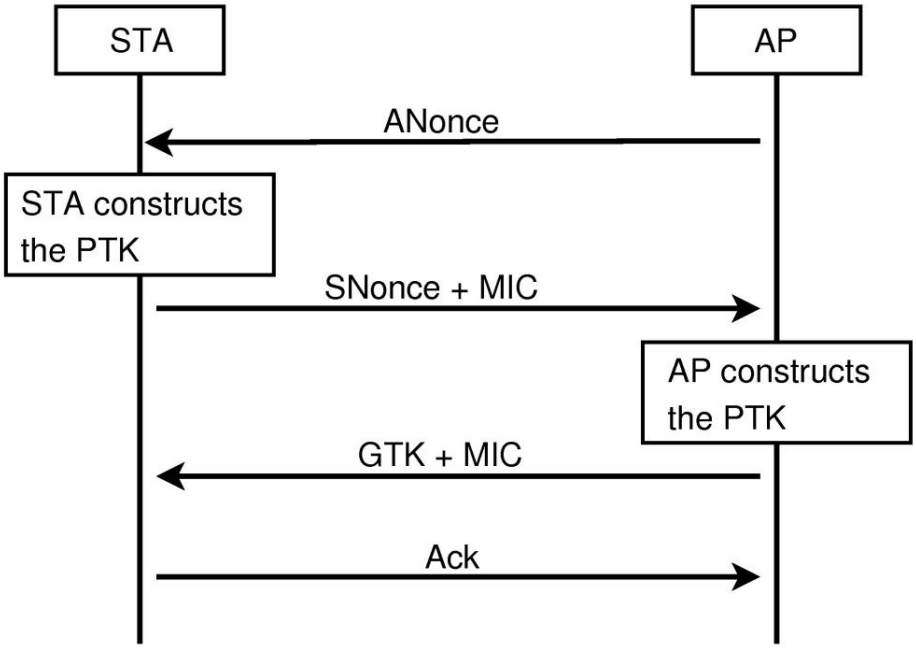


FIGURE 3 – 4-Way Handshake

Il faut savoir qu'il y a une différence entre la clé **PTK et GTK** :

— **PTK (Pairwise Transient Key) :** Cette clé est utilisée pour chiffrer les données envoyés en **unicast** entre deux appareils (par exemple : communication entre un client et un point d'accès). Cette clé est décomposé en 4 sous clés.

— **GTK (group Transient Key) :** Cette clé est utilisée pour transmettre des données en **multicast** entres plusieurs appareils. Ainsi cette clé est utilisé dans les réseaux d'entreprises.

La clé **PTK** est découpée en 4 clés :

1. **TK (Temporary Key)** : c'est une clé de **128 bits** qui permet de chiffrer les flux de données (utilisé par **TKIP**).
2. **KEK (Key Encription Key)** : c'est clé de **128 bits**, elle permet de chiffre les données du **4-WAY Handshake.**
3. **KCK (Key Confirmation Key)** : c'est une clé de 128 bits, elle permet d'authentifier les messages (MIC) dans le **4-WAY Handshake**.
4. **TMK (Temporary MIC Key)** : c'est une clé de **128 bits**, elle est utilisé pour l'authentification du flux de données.

3.3.2 Failles du mécanisme

Pour attaquer un réseau qui utilise un mécanisme **WPA** il faut deviner la clé **PSK** par utilisation du **BRUTE-FORCE ATTACK**. Ceci ce fait par capturation des deux premiers échanges du **ANonce et SNonce** par faire déconnecter le client de sont point d'accès (grâce a des requêtes de dés-authentification) afin qu'il refait le **4-WAY Handshake**.

Puis il est possible de deviner la clé PSK, ensuite calculer les clés **PMK** et **PTK**. Après avoir la clé **PTK** on peut trouver la clé **KCK** qui permet d'obtenir le **MIC** du second message du **4-WAY HandShake**. Si la clé n'est pas la bonne (le **MIC** calculé ne correspond pas à celui du second message), un autre est testé et ainsi de suite.

3.4 WPA2

3.4.1 Description et fonctionnement

WPA2 : Le successeur de **WPA** respecte la norme **802.11i** entière. L'amélioration plus importante de WPA2 sur WPA était l'usage de l'**AES** (Advanced Encryption Standard). Ce protocole n'est pas fonctionnel sur l'ancien matériel vu qu'il nécessite plus de software à cause de la nouvelle méthode de cryptage.

CCMP(Counter-Mode/CBC-Mac protocol) est imposé par les normes de la **WPA2**. Ce protocole utilise le chiffrement par bloc AES dans un mode d'opération de type "compteur" couplé à code d'authentification MAC (CBC-MAC) ; le compteur garantie que les block n'ont pas le même vecteur d'initialisation et le code d'authentification vérifie que le message n'a pas été modifié.

Déroulement de CCMP :

— **Authentification** :La première étape consiste à générer un code d'authentification pour le paquet 802.11. Ce code, le MIC (message integrity code) est produit avec les étapes dans la figure qui hachent le message selon une clé d'authentification

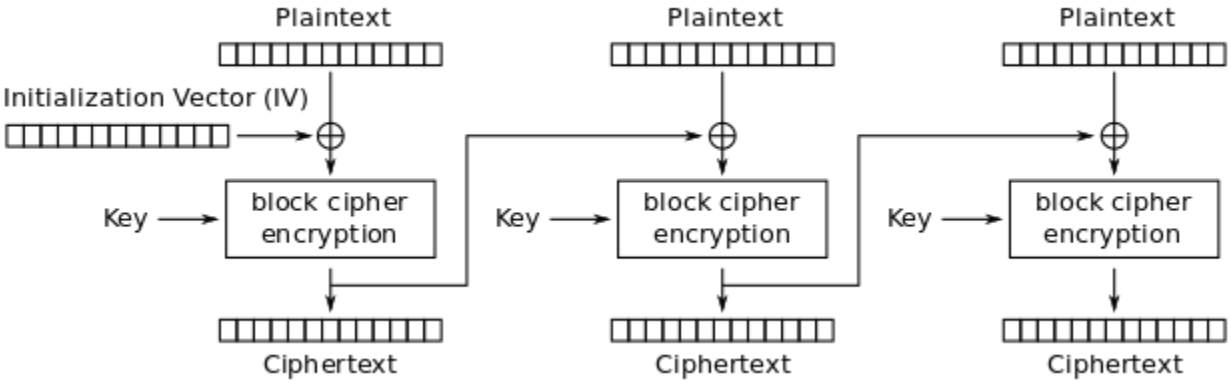


FIGURE 4 – CBC en mode encryption

— **Chiffrement** :L'en-tête du paquet CCMP contient la valeur initiale du compteur (128 bits) utilisé pour le mode d'opération. Le chiffrement se fait bloc par bloc selon la procédure suivante :

1. chiffrer de la valeur initiale du compteur avec **AES** et la clé de chiffrement.
2. Effectuer un XOR entre ce compteur chiffré et les 128 bits de données, on obtient le premier bloc chiffré.
3. Incrémenter le compteur et le chiffrer avec AES.
4. effectuer un XOR entre ce compteur chiffré et les 128 bits suivants de données, on obtient un autre bloc chiffré.

On répète cette opération pour toutes les blocs.

3.4.2 Failles du mécanisme

Même avec la nouvelle méthode d'encryption, WPA2 est encore vulnérable à la plupart des failles de sécurité de la WPA.
En addition à la faille précédente qui a besoin d'un dictionnaire pour trouver le mot de passe,il existe d'autre failles qui nécessite pas de Wordlist comme l'attaque Krack.
La faille **Krack** profite su **4-way handshake**, vu qu'en bloquant le $4^{éme}$ message du handshake provenant du client, le point d'accès va ré-émettre le $3^{éme}$ message et par la suite l'attaquant génère des transmissions successives par le client avec la même clé **PTK** dérivée avec le même compteur r, dont la valeur est réinitialisée à chaque réception du $3^{éme}$ message et vu que l'attaquant a une idée du contenu des paquets il peut finir par décrypter les messages(texte chiffré connu et choisis).

3.5 Outils d'attaque

Nous allons exploité les failles des mécanismes WPA/WPA2 pour récupérer le mot de passe d'un point d'accès en WPA2 qu'on a crée avec un mot de passe relativement faible.Pour réaliser les attacks suivant nous avons utilisé un adaptateur RT5370 qui supporte le mode monitoring qui permet d'injecter des paquets.

— Avec **Aircrack** :

1. on active le monitoring mode avec **airmon-ng**

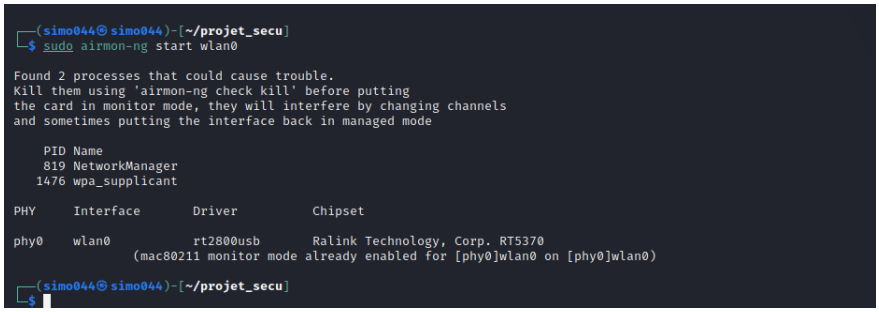
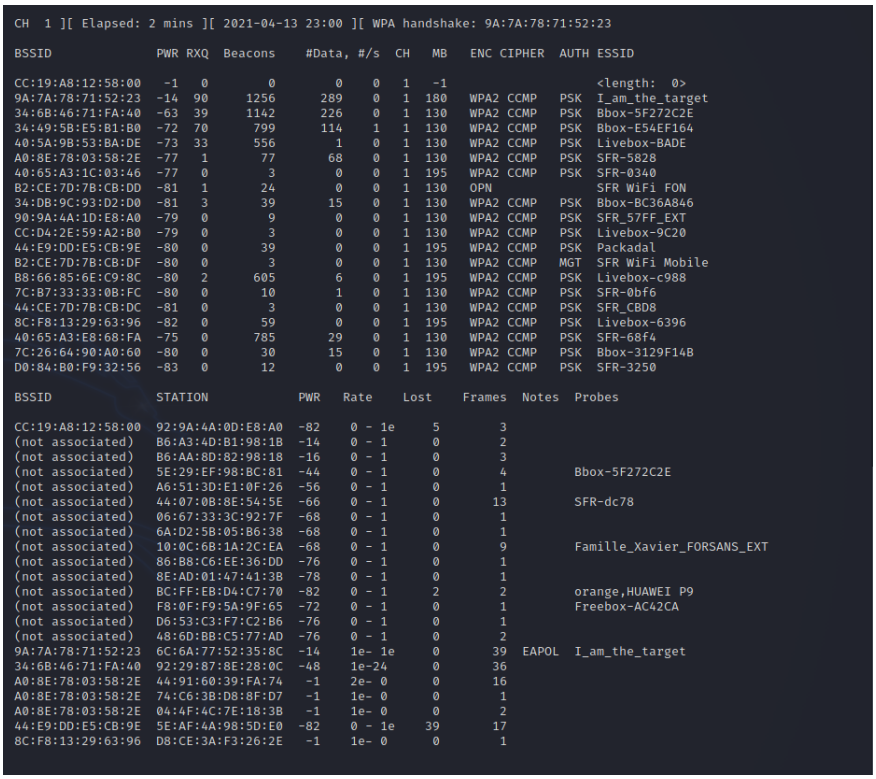


FIGURE 5 – monitoring mode

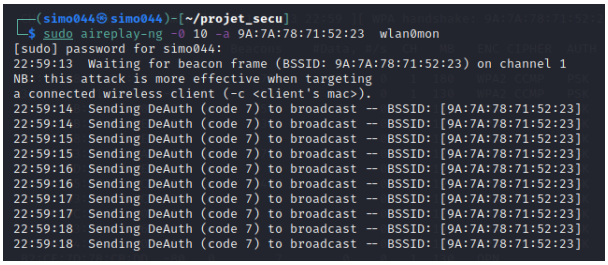
2. On scan notre réseau à l'aide de **Airodump** toute en gardant un log au cas ou on effectue des handshakes.



```
CH  1 ][ Elapsed: 2 mins ][ 2021-04-13 23:00 ][ WPA handshake: 9A:7A:78:71:52:23

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

CC:19:A8:12:58:00   -1   0        0        0    0   1   -1                    <length:  0>
9A:7A:78:71:52:23  -14  90     1256      289    0   1  180   WPA2 CCMP   PSK  I_am_the_target
34:6B:46:71:FA:40  -63  39     1142      226    0   1  130   WPA2 CCMP   PSK  Bbox-5F272C2E
34:49:5B:E5:B1:B0  -72  70      799      114    1   1  130   WPA2 CCMP   PSK  Bbox-E54EF164
40:5A:9B:53:BA:DE  -73  33      556        1    0   1  130   WPA2 CCMP   PSK  Livebox-BADE
A0:8E:78:03:58:2E  -77   1       77       68    0   1  130   WPA2 CCMP   PSK  SFR-5828
40:65:A3:1C:03:46  -77   0        3        0    0   1  195   WPA2 CCMP   PSK  SFR-0340
B2:CE:7D:7B:CB:DD  -81   1       24        0    0   1  130   OPN              SFR WiFi FON
34:DB:9C:93:D2:D0  -81   3       39       15    0   1  130   WPA2 CCMP   PSK  Bbox-BC36A846
90:9A:4A:1D:E8:A0  -79   0        9        0    0   1  130   WPA2 CCMP   PSK  SFR_57FF_EXT
CC:D4:2E:59:A2:B0  -79   0        3        0    0   1  130   WPA2 CCMP   PSK  Livebox-9C20
44:E9:DD:E5:CB:9E  -80   0       39        0    0   1  195   WPA2 CCMP   PSK  Packadal
B2:CE:7D:7B:CB:DF  -80   0        3        0    0   1  130   WPA2 CCMP   MGT  SFR WiFi Mobile
B8:66:85:6E:C9:8C  -80   2      605        6    0   1  195   WPA2 CCMP   PSK  Livebox-c988
7C:B7:33:33:0B:FC  -80   0       10        1    0   1  130   WPA2 CCMP   PSK  SFR-0bf6
44:CE:7D:7B:CB:DC  -81   0        3        0    0   1  130   WPA2 CCMP   PSK  SFR_CBD8
8C:F8:13:29:63:96  -82   0       59        0    0   1  195   WPA2 CCMP   PSK  Livebox-6396
40:65:A3:E8:68:FA  -75   0      785       29    0   1  130   WPA2 CCMP   PSK  SFR-68f4
7C:26:64:90:A0:60  -80   0       30       15    0   1  130   WPA2 CCMP   PSK  Bbox-3129F14B
D0:84:B0:F9:32:56  -83   0       12        0    0   1  195   WPA2 CCMP   PSK  SFR-3250

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

CC:19:A8:12:58:00  92:9A:4A:0D:E8:A0  -82    0 - 1e     5         3
(not associated)   B6:A3:4D:B1:98:1B  -14    0 - 1      0         2
(not associated)   B6:AA:8D:82:98:18  -16    0 - 1      0         3
(not associated)   5E:29:EF:98:BC:81  -44    0 - 1      0         4         Bbox-5F272C2E
(not associated)   A6:51:3D:E1:0F:26  -56    0 - 1      0         1
(not associated)   44:07:0B:8E:54:5E  -66    0 - 1      0        13         SFR-dc78
(not associated)   06:67:33:3C:92:7F  -68    0 - 1      0         1
(not associated)   6A:D2:5B:05:B6:38  -68    0 - 1      0         1
(not associated)   10:0C:6B:1A:2C:EA  -68    0 - 1      0         9         Famille_Xavier_FORSANS_EXT
(not associated)   86:B8:C6:EE:36:DD  -76    0 - 1      0         1
(not associated)   8E:AD:01:47:41:3B  -78    0 - 1      0         1
(not associated)   BC:FF:EB:D4:C7:70  -82    0 - 1      2         2         orange,HUAWEI P9
(not associated)   F8:0F:F9:5A:9F:65  -72    0 - 1      0         1         Freebox-AC42CA
(not associated)   D6:53:C3:F7:C2:B6  -76    0 - 1      0         1
(not associated)   48:6D:BB:C5:77:AD  -76    0 - 1      0         2
9A:7A:78:71:52:23  6C:6A:77:52:35:8C  -14    1e- 1e     0        39  EAPOL  I_am_the_target
34:6B:46:71:FA:40  92:29:87:8E:28:0C  -48    1e-24      0        36
A0:8E:78:03:58:2E  44:91:60:39:FA:74   -1    2e- 0      0        16
A0:8E:78:03:58:2E  74:C6:3B:D8:8F:D7   -1    1e- 0      0         1
A0:8E:78:03:58:2E  04:4F:4C:7E:18:3B   -1    1e- 0      0         2
44:E9:DD:E5:CB:9E  5E:AF:4A:98:5D:E0  -82    0 - 1e    39        17
8C:F8:13:29:63:96  D8:CE:3A:F3:26:2E   -1    1e- 0      0         1
```

FIGURE 6 – Scan des APs

3. Avec **Aireplay**on envoi des paquets de dés-authentifications pour obliger les client de se déconnecter et reconnecter tout en effectuant 4-way Hanshake



```
┌──(simo044㉿simo044)-[~/projet_secu]
└─$ sudo aireplay-ng -0 10 -a 9A:7A:78:71:52:23  wlan0mon
[sudo] password for simo044:
22:59:13  Waiting for beacon frame (BSSID: 9A:7A:78:71:52:23) on channel 1
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
22:59:14  Sending DeAuth (code 7) to broadcast -- BSSID: [9A:7A:78:71:52:23]
22:59:14  Sending DeAuth (code 7) to broadcast -- BSSID: [9A:7A:78:71:52:23]
22:59:15  Sending DeAuth (code 7) to broadcast -- BSSID: [9A:7A:78:71:52:23]
22:59:15  Sending DeAuth (code 7) to broadcast -- BSSID: [9A:7A:78:71:52:23]
22:59:16  Sending DeAuth (code 7) to broadcast -- BSSID: [9A:7A:78:71:52:23]
22:59:16  Sending DeAuth (code 7) to broadcast -- BSSID: [9A:7A:78:71:52:23]
22:59:17  Sending DeAuth (code 7) to broadcast -- BSSID: [9A:7A:78:71:52:23]
22:59:17  Sending DeAuth (code 7) to broadcast -- BSSID: [9A:7A:78:71:52:23]
22:59:18  Sending DeAuth (code 7) to broadcast -- BSSID: [9A:7A:78:71:52:23]
22:59:18  Sending DeAuth (code 7) to broadcast -- BSSID: [9A:7A:78:71:52:23]
```

FIGURE 7 – handshake

4. finalement, **Aircrack** va calculer le MIC et le comparer avec celui capturer avec Airodump

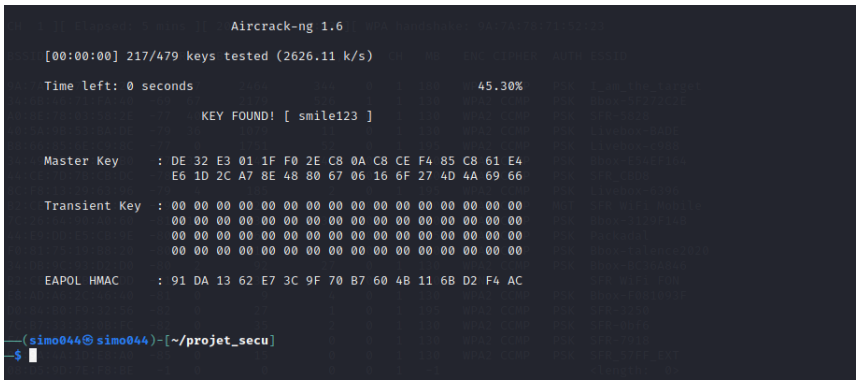


FIGURE 8 – dec

— Avec **Fern wifi cracker** :
Fern wifi cracker est un outil disponible sur kali qui permet étant donné un dictionnaire d'automatiser toutes les étapes de l'outil précédant.

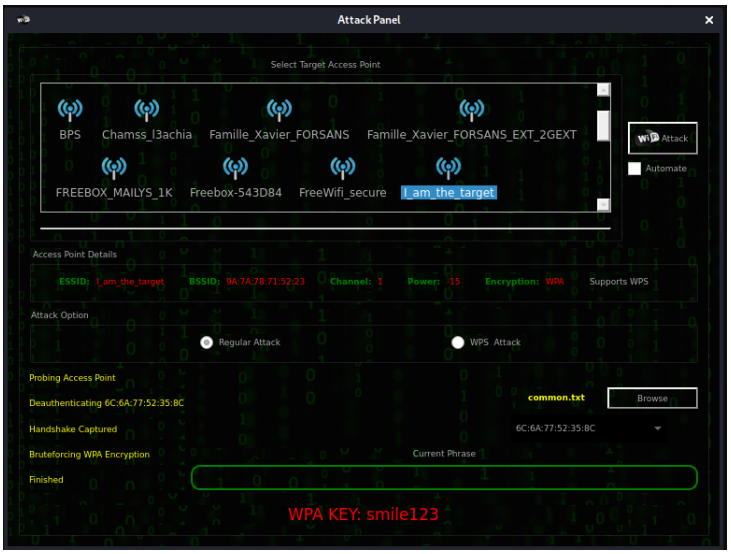


FIGURE 9 – monitoring mode

3.6 WPA3

3.6.1 Description et fonctionnement

WPA3, le successeur de tout les protocoles Wi-Fi était annoncé par WiFi Alliance en 2018 et supposé enter en phase d'industrialisation pendant l'année courante. on remarque des produits comme Nest Wifi et Google Wifi(des produits Google) qui recommandent la transition vers ce nouveau protocole.

— Protocole plus robuste aux attack brute force vu que la WPA3 remplace la clé pré-partagée WPA2 (PSK) par l'authentification simultanée d'égaux (SAE) pour éviter les attaques de réinstallation de clés comme le KRACK
— Meilleur cryptage pour une meilleur protection fiable par mot de passe
— Connexion plus sûre dans l'espace public.Même avec les clés de chiffrement du trafic, il est difficile de calculer l'utilisation du trafic et les données transmises avec WPA3-Personal

3.7 Failles du mécanisme

Même si WPA3 est une protocole très récent des faille ont été découvertes par des chercheurs en Avril 2019.
Dragonfly Handshake, censé être parmi les points forts de ce protocole, peut connaître des fuites, ces fuites soumis a des traitement mathématique, peut donner une idée sur le mot de passe.Cette faille a été présenté pour la première fois lors de **Real World Crypto conference 2020**

4 Social engineering

Le but de tout ces attacks est d'arriver à **men in the middle** situation. Une fois on arrive à établir une telle situation, l'attaquant peut poursuivre son attaque par une rederiction HTTP ou autre.

4.1 Evil Twin

Principe d'attaque :
cette attaque consiste en premier lieu à déconnecter la victime du point d'acces par envoi d'un seginal de dés-authentification . Ensuite il faut créer un jumeau maléfique ; un point d'accès qui porte le même nom du point accès légitime et puisque la victime à uniquement accès à l' **SSID** du réseau, elle est porté à se connecter à notre point d'accès maléfique. Finalment, l'attaquant peut effectuer une **MIM** attaque ou récupérer le mot de passe du point d'accès initial en dirigeant la victime vers une page qui parait légitime et le demander son login et mot de passe.

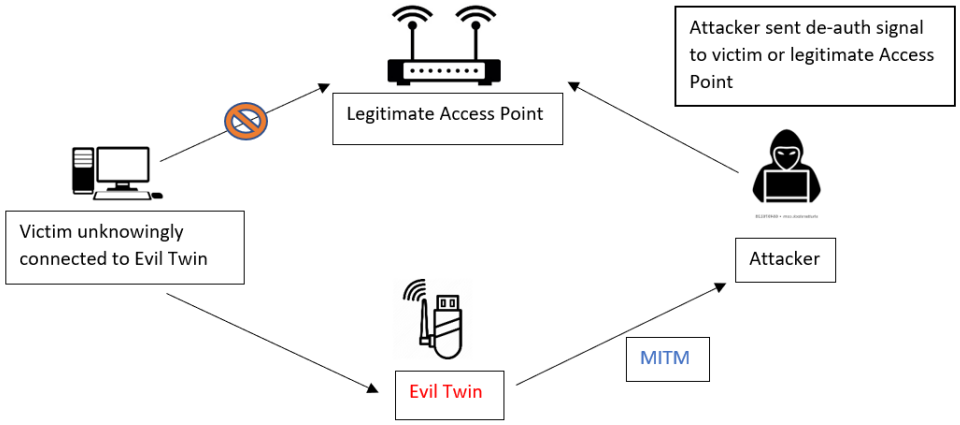


FIGURE 10 – evil twin attack

Outils informatiques :il existe plusieurs outils qui puissent exécuter toutes les étapes de cette attack comme **Airgeddon**

Protection contre cette attaque :

- Se méfier quand il y a un doublon du point d'accès.
- Se méfier des pages http d'authentification.
- En cas de doute, taper un mot de passe erroné si vous arriver à vous connecter cela vaut dire que c'est un **evil twin**.

4.2 Known Beacons

Principe d'attaque :
cette attaque est crée comme exploite le flag Auto-connect. en supposant que le target s'est connecté au moins une fois à un WIFI appelé :"ANDROID", "Airport Free WiFi","Public wifi" ou "FreeWifi_secure". Ce qui est 99% le cas. La plupart de système opérationnel ayant le **auto_connect** flag activé même si ils sont en mode passive vont essayer de se connecter au **AP**.
Donc en basant sur un dictionnaire contenant les ssid les plus utilisé,la victime va éventuellement se connecté à de ces point d'accèset on se trouvera par la suite dans une situation **MIM**.

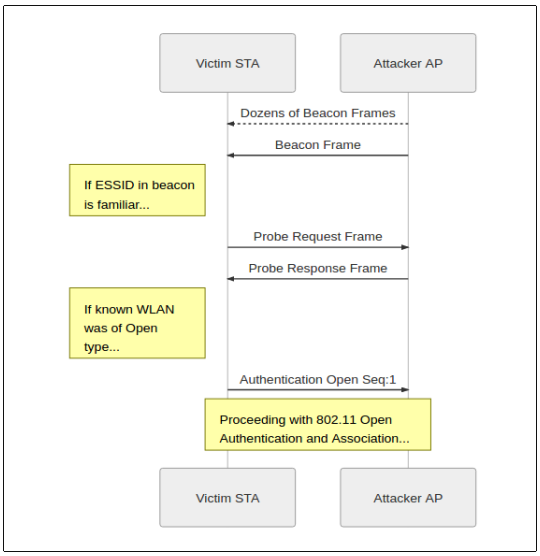


FIGURE 11 – Known beacon attack attack

Outils informatiques :
MDK3 est outil très puissant qui fait partie du projet **aircrack-ng** et qui peut s'occuper de génerer des **beacons** étant donné une liste de **SSID**. simplement à travers la commande suivant :
mdk3 mon0 b -f <ssid.list>-g -a -c <canal>

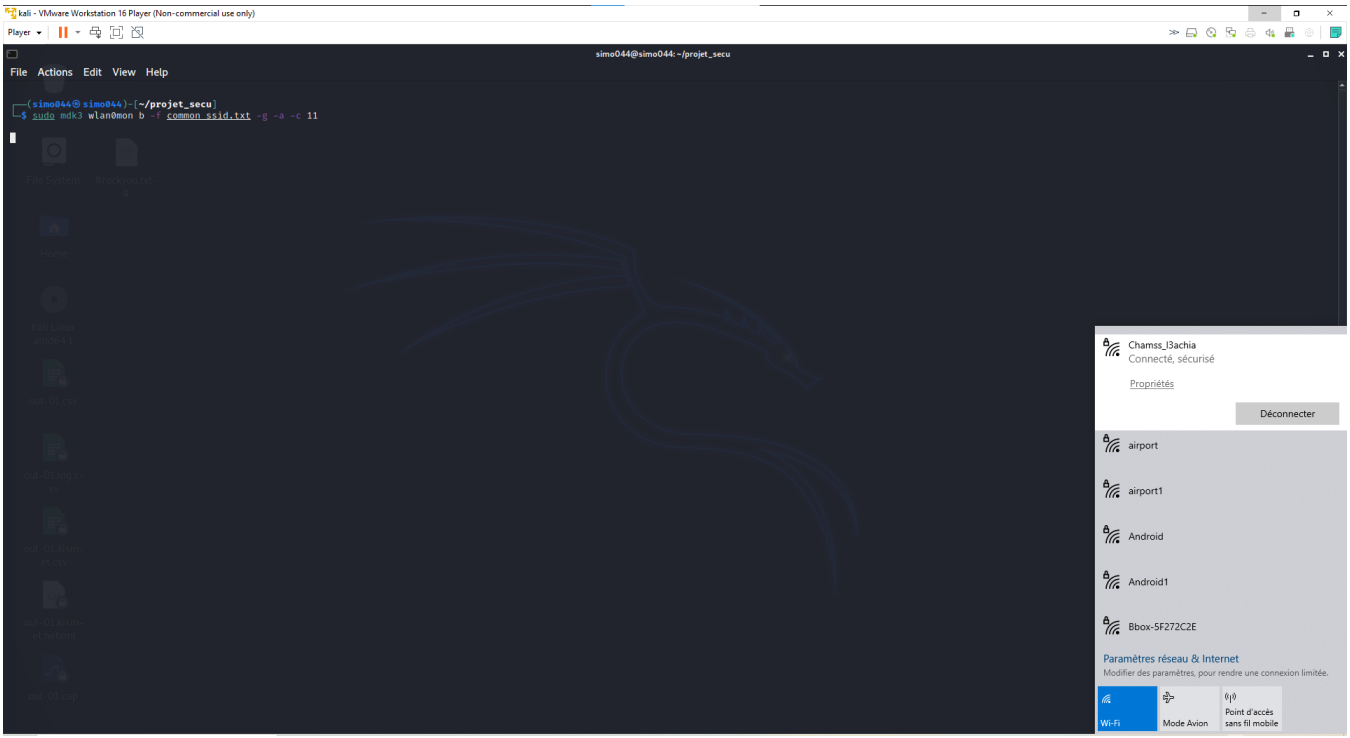


FIGURE 12 – mdk3 beacon flood

Protection contre cette attaque :
La façon la plus simple pour ce protéger contre ce type d'attaque est d'effacer les **SSID** des points d'accès public de la liste du **network manager**.

5 Méthodes de protection

Afin de naviguer sur internet à travers un réseau **WI-FI** en toute sécurité il faut adopter les bonnes pratiques suivantes :

- Dans le cas de l'utilisation du mécanisme **WPA2** dans un réseau **WI-FI** personnel vaut mieux utiliser le l'algorithme de chiffrement **AES-CCMP**, et choisir un long mot de passe.
- Ne pas se connecter à n'importe quel réseaux **WI-FI**.
- Utiliser un **VPN** qui permet de chiffrer les échanges sans-fil et empêchera les tentatives de **SNIFFING**.
- Privilégier les sites qui utilise un protocole de sécurité **HTTPS**.
- Changer le nom de réseau **SSID** générique qui est proposé par défaut.
- Limiter la puissance du signal du réseau **WI-FI** pour diminuer le risque potentiel de craquer la clé **WPA**.

— Filtrage des équipements qui peuvent se connecter au réseau **WI-FI**.

6 Conclusion

D'après ce que on a vu précédemment tous les mécanismes de sécurité des réseaux sans fils présentent des lacunes en terme de sécurité, et cela signifie que pour avoir une sécurité prometteuse lors de la navigation sur le web, il ne faut pas compter seulement sur les mécanismes **WEP/WPA/WPA2/WPA3** pour protéger les données échangées sur le réseau, il faut absolument accompagner l'un de ces mécanismes de sécurité par des méthodes de protection mentionnées précédemment ou privilégier une connexion filaire si c'est possible.

7 références bibliographiques

https ://census-labs.com/news/2018/02/01/known-beacons-attack-34c3/
https ://fr.wikipedia.org/wiki/Wi-Fi_Protected_Access
https ://wpa3.mathyvanhoef.com/
https ://www.asus.com/fr/support/FAQ/1042478/
https ://fr.wikipedia.org/wiki/Counter-Mode/CBC-Mac_protocol