

Sécurité WIFI

RAPPORT SECURITE



SENNADJ Younes & AMAROUCHE Youcef
2014 |

Table des matières

Introduction :	2
C'est Quoi le WIFI :	2
Sécurité Informatique :	2
Sécurité WIFI :	3
Les étapes à suivre pour sécuriser un réseau WIFI :	4
A. Changer le mot de passe utilisateur de votre routeur Wifi :	4
B. Définir le nom de SSID :	4
C. Filtrer les adresses MAC :	4
D. Activer le cryptage de clef de sécurité de réseau :	4
Les protocoles utilisés pour sécuriser un réseau WIFI :	5
A. WEP (Concept) :	5
B. WEP (Etapes de chiffrement)	5
C. WEP (Tableau de mort)	8
D. WPA (Concept) :	9
E. WPA (Protocole TKIP) :	9
F. WPA2 (Concept) :	11
G. WPA2 (Fonctionnement) :	11
H. Failles du WAP et WPA2 :	11
Les Risques liés aux réseaux sans fil :	13
A. Les Ondes Radioélectriques :	13
B. Interception des données :	13
C. L'intrusion réseau :	13
D. Le brouillage Radio :	14
E. Les Défis de service :	14
Conclusion :	15
Référence :	15

Introduction :

L'information joue un rôle très important et surtout dans l'informatique ou tout est basé sur cette information. Et pour cela il faut bien prendre en compte la sécurité de cette dernière.

De ce fait la sécurité informatique est un domaine très vaste qui sert à assurer la fiabilité et l'intégrité de l'information contre les différentes menaces existantes dans le réseau informatique.

L'un des Technologies qui nécessite une grande sécurité c'est l'internet qui pose en fait un gros problème à cause des différentes failles au niveau des protocoles ou des fonctionnalités implémentés. L'un des protocoles de communication qui pose un problème c'est le WIFI.

C'est Quoi le WIFI :

WIFI (ou Wireless Fidelity) est un protocole de communication permettant de connecter des machines dans un réseau informatique sans la nécessité de câblage ou un réseau sans fil.

Il s'agit en fait de la norme de l'IEEE baptisée 802.11 (Norme ISO/CEI 8802-11) qui est utilisé internationalement pour décrire les caractéristiques d'un réseau local sans fil.

Le débit présenté par le WIFI diffère selon la norme et le matériel utilisé (11 Mbit/s théoriques ou 6 Mbit/s réels en 802.11b à 54 Mbit/s théoriques ou environ 25 Mbit/s réels en 802.11a ou 802.11g et 600 Mbit/s théoriques pour le 802.11n).



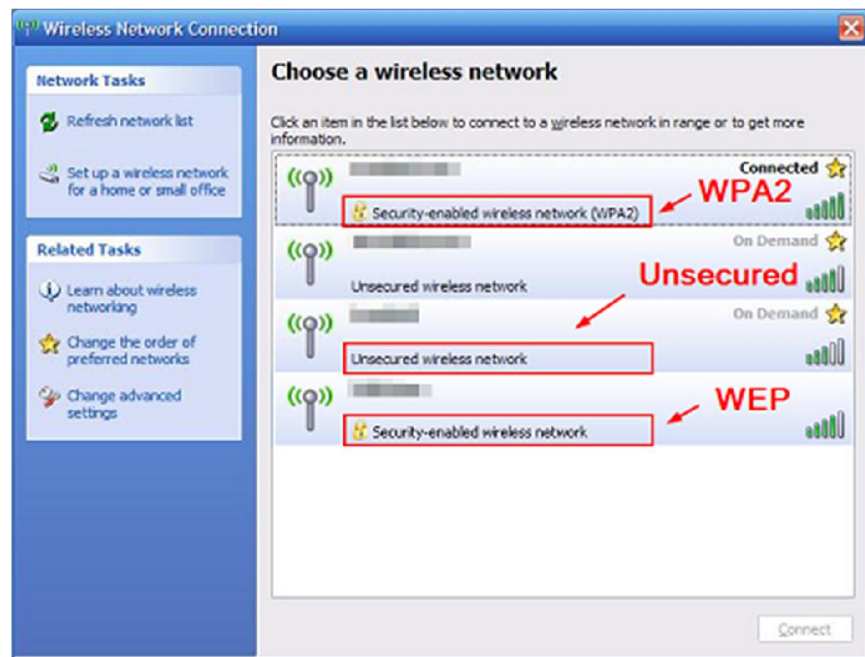
Sécurité Informatique :

La sécurité informatique est l'ensemble des techniques et matériaux mise en place pour assurer que les ressources du système d'information (matérielles ou logicielles) d'une organisation sont utilisées uniquement dans le cadre où il est prévu qu'elles le soient en focalisant sur l'aspect d'intégrité et de fiabilité de données et surtout qu'ils ne tombent pas dans les mains des pirates.

Sécurité WIFI :

La sécurité a toujours été le point faible des réseaux wifi, à cause principalement de sa nature physique : les ondes radio étant un support de transmission partagé quiconque se trouvant dans la zone de couverture peut écouter le support et s'introduire dans le réseau. On peut même, grâce à des antennes amplifiées, se trouver hors de portée de la couverture radio pour pénétrer ce réseau.

En fait c'est facile de mettre en place un réseau avec les différentes configurations mais il ne faut jamais oublier de fermer la porte de votre appartement. Donc de cette façon qu'on peut voir la sécurité d'un WIFI.



Les étapes à suivre pour sécuriser un réseau WIFI :

A. Changer le mot de passe utilisateur de votre routeur Wifi :

A la création d'un nouveau réseau WIFI il faut changer le mot de passe utilisé et ceci en se basant soit sur la ligne de commande (« nets wlan sethostednetwork ... »), l'utilitaire de configuration de réseau sur votre système d'exploitation et enfin le navigateur web en tapant l'adresse de votre routeur (par exemple : 192.168.1.1).

B. Définir le nom de SSID :

Chaque réseau WIFI a un nom SSID que l'utilisateur peut éventuellement le changer d'un nom simple vers un autre qui est plus compliqué toujours soit via l'invité de commande de l'utilitaire de configuration ou bien le navigateur. L'option la plus pertinente est de cacher ce réseau dans la liste des connexions possibles pour les voisins et celle-ci est faisable en cochant juste une case à partir de notre utilitaire.

C. Filtrer les adresses MAC :

Le Mac est une adresse unique identifiant chaque machine. Sur le routeur qui permet la connexion Internet on peut découcher l'option de filtrage des adresses IP qui peuvent accéder au réseau et comme ça on peut limiter les risques d'être attaquer par un intrus dans le réseau.

D. Activer le cryptage de clef de sécurité de réseau :

Avant d'utiliser un réseau WIFI vaut mieux chiffrer la clé de sécurité et pour ça deux types de cryptages existent le WEP et le WPA qu'on va les présenter après dans ce document. Il faut juste noter si le matériel utilisé entre le routeur et les machines supportent le WPA alors vaut mieux l'utiliser car il est plus sécurisé.

Les protocoles utilisés pour sécuriser un réseau WIFI :

Le développement au fil de temps :

A. WEP (Concept) :

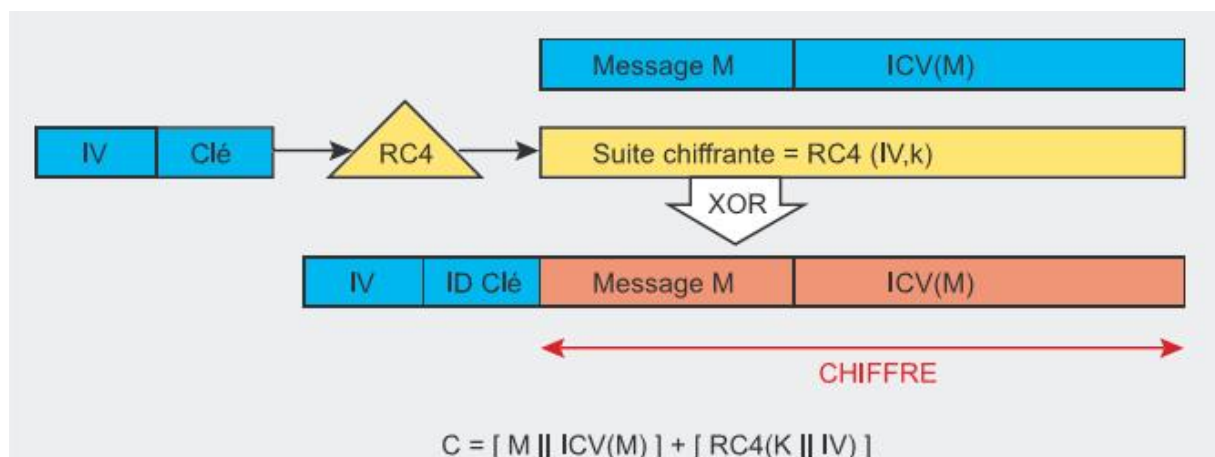
Protocole de sécurité spécifié dans le standard IEEE 802.11 permettant de fournir aux utilisateurs de réseaux locaux sans fil une protection contre le piratage. WEP cherche à fournir à ces derniers une confidentialité similaire à celle que les réseaux filaires peuvent offrir.

B. WEP (Etapas de chiffrement)

Donc le WEP est un protocole de chiffrement qui est utilisé pour chiffrer les paquets circulant dans le réseau sans fil (WIFI).

Ce chiffrement se décompose en plusieurs phases :

- La création de la graine
- La création du key Stream
- Le calcul ICV
- La constitution du message final et son encapsulation dans une trame



a) Le vecteur d'initialisation :

Le vecteur d'initialisation (IV – Initialization Vector) est une séquence de bits qui change régulièrement. Combiné à la clé statique, il introduit une notion aléatoire au chiffrement.

Ainsi, deux messages identiques ne donneront pas le même contenu chiffré, puisque l'IV est dynamique.

La longueur du IV est de 24 bits. Cela laisse à penser que l'IV ne sera pas réutilisé plusieurs fois. Comme la clé, le IV doit être connu à la fois de l'émetteur et du récepteur. La solution d'un mécanisme de génération automatique qui devrait être présent sur tous les équipements n'a pas été retenue car elle est difficile à mettre en place. Le IV est donc transporté en clair dans les trames.

b) L'algorithme RC4 dans WEP :

RC4 est un algorithme de chiffrement par flux (par flot ou encore sans état) à clé symétrique développé en 1987 par Ronald Rivest (l'un des créateurs du RSA). Il utilise différentes tailles de clé, couramment jusqu'à 256 bits. Le RC4 est la propriété de la RSA Security. Il est utilisé dans de nombreuses applications, l'une des plus connues étant SSL (Secure Socket Layer).

RC4 ne nécessite pas trop de puissance de calcul. Il est extrêmement rapide (environ dix fois plus rapide que le DES). Il est considéré comme fiable. Cet algorithme reprend le principe du masque jetable (OTP – One Time Pad ou masque de Vernam). En effet, on génère un flux de données de taille identique au flux de données claires et on fait un XOR entre les deux, le déchiffrement se fait par XOR entre le chiffré et le même flux pseudo-aléatoire.

c) La création de la graine

Deux longueurs de clé WEP peuvent être choisies sur les équipements Wi-Fi :

- 40 bits, soit 5 octets
- 104 bits, soit 13 octets

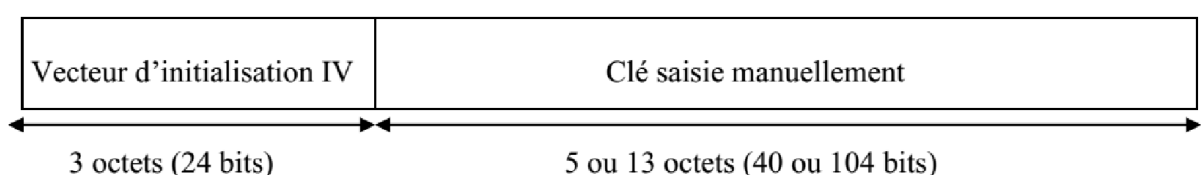
La génération de la graine est l'étape où on génère le IV et on le concatène à notre clé statique ce qui nous donne une clé de 64 bits (8 octets) ou 128 bits (16 octets) que l'on appelle graine.

d) La création de la graine

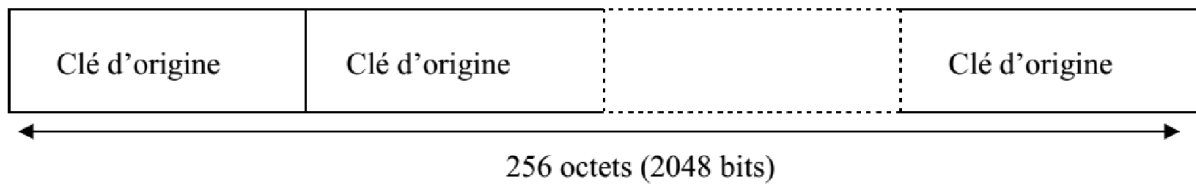
Deux longueurs de clé WEP peuvent être choisies sur les équipements Wi-Fi :

- 40 bits, soit 5 octets
- 104 bits, soit 13 octets

La génération de la graine est l'étape où on génère le IV et on le concatène à notre clé statique ce qui nous donne une clé de 64 bits (8 octets) ou 128 bits (16 octets) que l'on appelle graine.

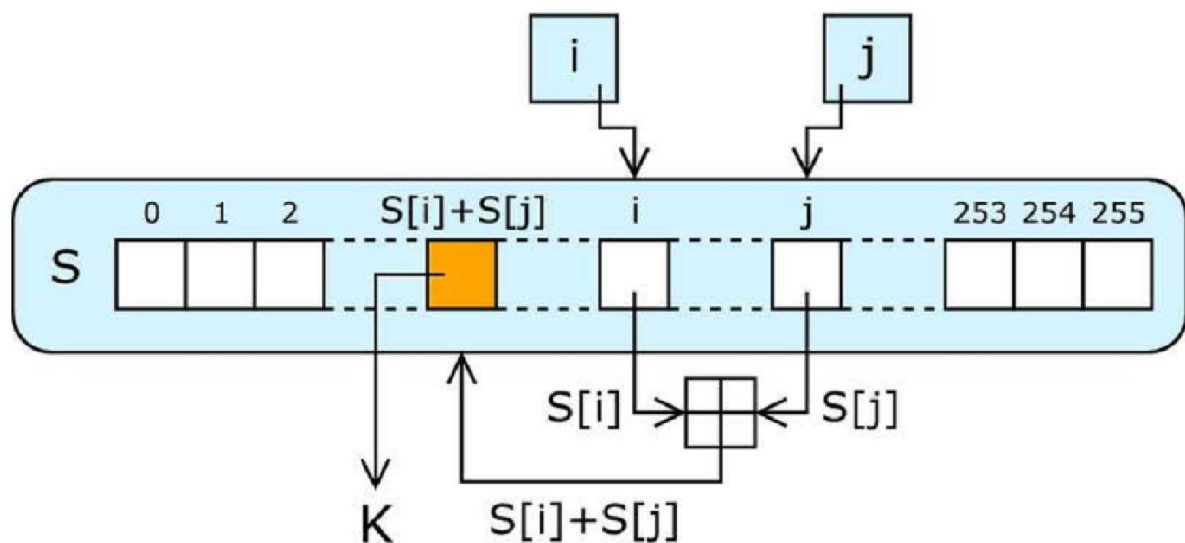


Une table de 256 octets (généralement) est formée. Elle est initialisée en reportant la graine autant de fois que nécessaire. A partir de la même clé, on obtient donc la même table à l'issue de la phase d'initialisation. On appellera ce tableau S (comme seed).



NB : les 256 octets sont générés à partir de la graine en appliquant l'algorithme KSA

e) La création de Key Stream :



A partir de la matrice S obtenue dans la phase de création de gaine on applique un ensemble de modifications qui permet de mettre le déchiffrement de ce paquet plus difficile.

f) Le contrôle d'intégrité :

Le WEP prévoit un mécanisme nommé Integrity Check Value (ICV), destiné à contrôler l'intégrité des séquences WEP dites trames (frames en anglais). Pour cela, un code équivalent au CRC32 (i.e. sur 32 bits) est calculé. Il résulte du message en clair M et non du contenu chiffré. Le CRC32 correspond en fait au reste dans la division en binaire du message par un diviseur fixé à l'avance.

NB : Le CRC32 est parfois désigné sous l'appellation de FCS (Frame Check Sequence).

Le résultat du calcul d'intégrité : $ICV(M)$ est ensuite concaténé au payload M : $M || ICV(M)$, puis chiffré avec la clé. La clé WEP est donc indispensable pour l'interpréter.

La modification de la trame chiffrée semble inconcevable sans la clé puisque le résultat de l'ICV changerait.

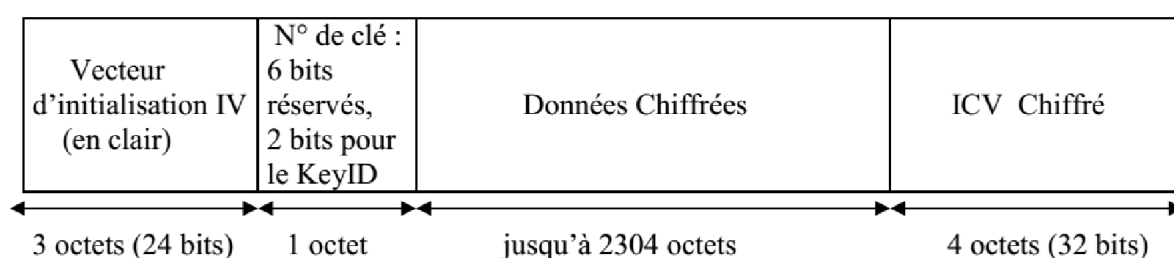
g) La constitution du message final et son encapsulation :

Dans le chiffrement RC4, chaque bit du texte clair est chiffré, en flux continu, par un bit de la table. On réalise un XOR (OU exclusif ou addition modulo 2) bit à bit entre l'une des clés aléatoires, générées précédemment et le payload. Cette opération produit une suite aléatoire non exploitable par l'attaquant.

L'opérateur XOR est adéquat pour employer le mécanisme de clé symétrique. La clé pour chiffrer est ainsi la même que celle pour déchiffrer puisqu'en l'appliquant deux fois de suite, on retrouve la valeur initiale.

Le résultat est la séquence chiffrée C donnée par :

$$C = (M \parallel \text{ICV}(M)) \text{ xor } \text{RC4}(\text{IV} \parallel K)$$



C. WEP (Tableau de mort)

Tableau 1. Chronologie de la mort du WEP

Date	Description
Septembre 1995	Vulnérabilité potentielle dans RC4 (Wagner)
Octobre 2000	Première publication sur les faiblesses du WEP : <i>Unsafe at any key size; An analysis of the WEP encapsulation</i> (Walker)
Mai 2001	<i>An inductive chosen plaintext attack against WEP/ WEP2</i> (Arbaugh)
Juillet 2001	Attaque <i>bit flipping</i> sur le CRC – <i>Intercepting Mobile Communications : The Insecurity of 802.11</i> (Borisov, Goldberg, Wagner)
Août 2001	Attaques FMS – <i>Weaknesses in the Key Scheduling Algorithm of RC4</i> (Fluhrer, Mantin, Shamir)
Août 2001	Sortie de AirSnort
Février 2002	Optimisation de l'attaque FMS par h1kari
Août 2004	Attaque de KoreK (IVs uniques) – sortie de chopchop et chopper
Juillet/Août 2004	Sortie d'Aircrack (Devine) et WepLab (Sanchez) implémentant l'attaque de KoreK.

Voilà quelques failles dans le protocole WEP qui diminuent l'utilisation de ce protocole aujourd'hui :

Vulnérabilité dans l'algorithme RC64 utilisé pour le chiffrement.

Clefs de trop faibles tailles :

- pour le WEP 64 bits, une clef de 40 bits ;
- possible à trouver par force brute ;
- des IV de 24 bits, cyclent en quelques heures.

Induite des textes en clair :

- Capture de paquets C1 et C2 avec le même IV ;
- ils s'écrivent : $C1 = F(+) P1$, $C2 = F(+) P2$;
- on obtient $P1 (+) P2 = C1 (+) C2$;
- on induit un texte en clair (e.g. ARP), on obtient les autres.

Aujourd'hui le logiciel aircrack-ng présent sur le système d'exploitation Linux est l'un des logiciels les plus efficaces pour obtenir la clé WIFI, et pour cela il est conseillé d'utiliser la technologie WPA ou WPA 2.

D. WPA (Concept) :

WIFI Protected Access est un protocole d'authentification développé par la WIFI Alliance pour remédier aux faiblesses de WEP et servir d'intermédiaire avant le WPA2 conçu pour fonctionner avec le même matériel que le WEP mais avec un logiciel mis à jour.

Par rapport au WEP il utilise une clé RC4 avec une clé 128 bits + 48 bits pour le vecteur d'initialisation. Il implémente le protocole TKIP pour contre certaines faiblesses de WEP.

E. WPA (Protocole TKIP) :

Temporal Key Integrity Protocol est un protocole de sécurité qui intègre des mécanismes additionnels pour contrer les problèmes rencontrés en WEP en pratique.

- Fonction de mélange de clé** : combine à la fois une clé secrète temporelle dérivée de la clé secrète racine, un vecteur d'initialisation et l'adresse MAC de transmission avant de passer le résultat obtenu à RC4. (Voir Figure 1)
- Mécanisme de compteur pour séquence** : chaque paquet envoyé contient un compteur. Les paquets qui ne sont pas reçus dans le bon ordre sont rejetés.
- Michael** : CAM utilisé pour la vérification de l'intégrité des messages (sur 64 bits). Il utilise le RC4 comme une méthode de chiffrement et il met à jour la clé de chiffrement d'une façon à ce que chaque paquet envoyé est encrypté avec une clé de chiffrement unique.

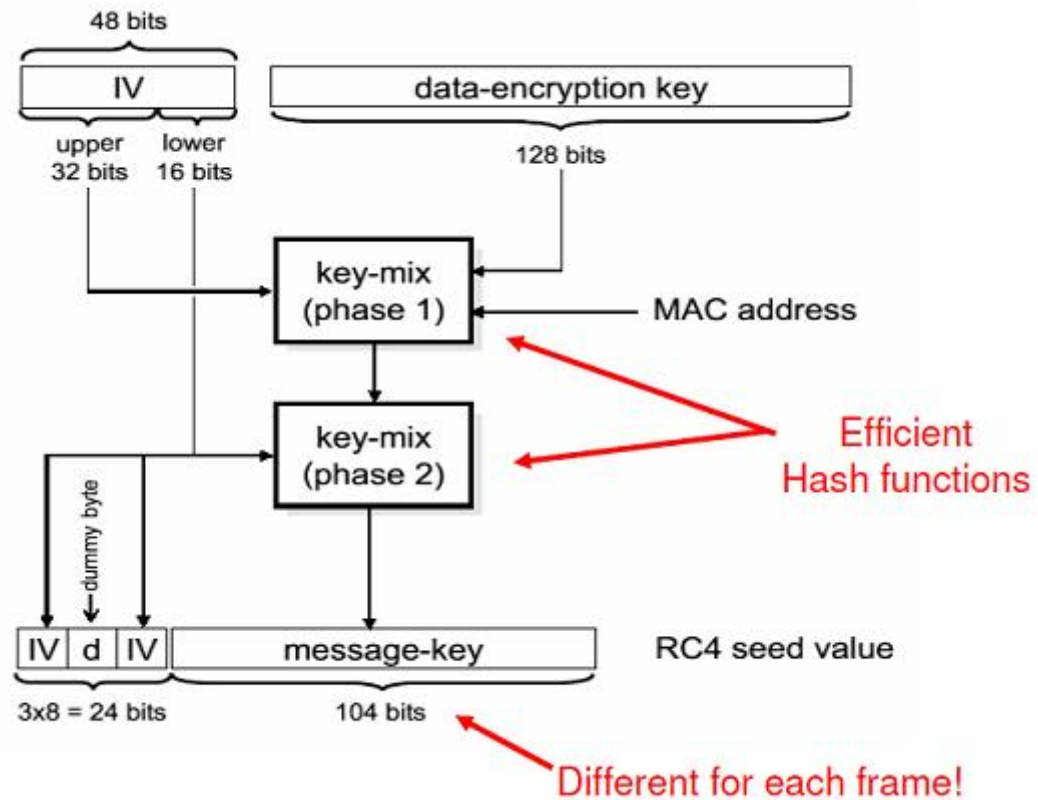


Figure 1 : Illustration de mélange des clés

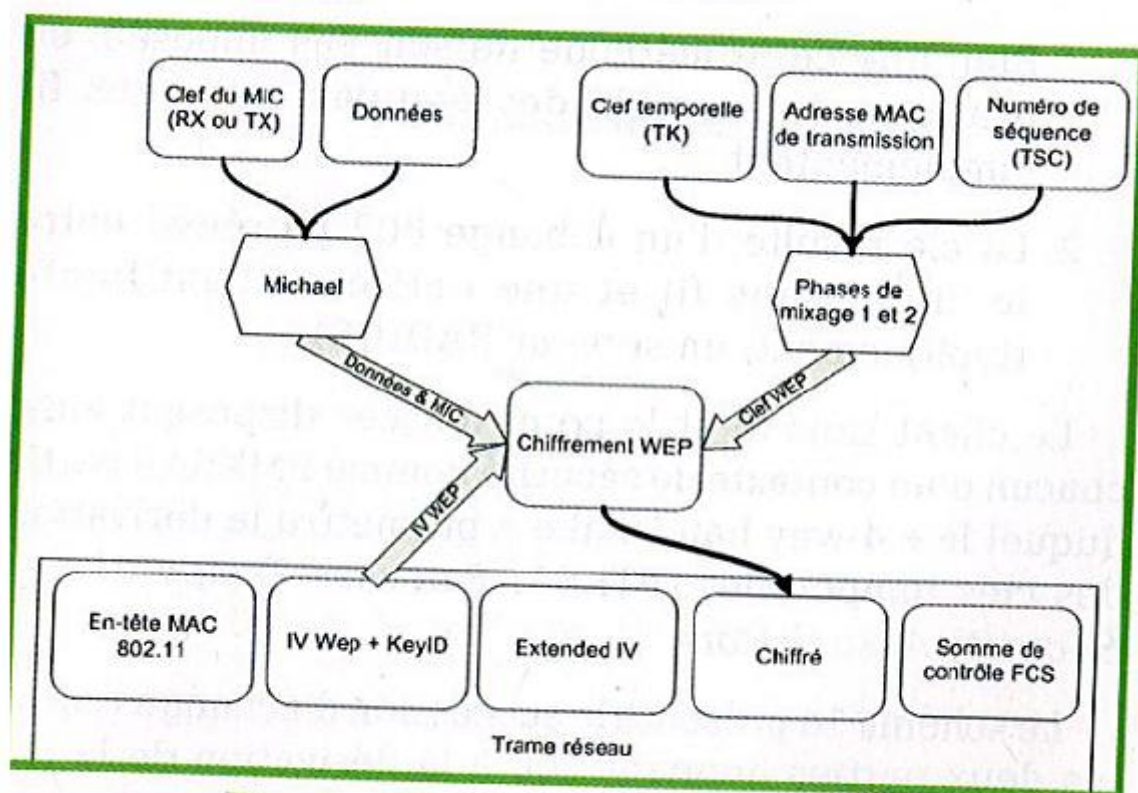


Fig. 1 : Trame chiffrée avec TKIP

F. WPA2 (Concept) :

Protocole d'authentification de WPA et actuellement implémenté dans la norme WIFI.

Il utilise le protocole CCMP qui est un protocole de chiffrement par blocs de types AES pour assurer la confidentialité et l'intégrité des données.

G. WPA2 (Fonctionnement) :

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 suivantes qui hachent le message selon une clé d'authentification :

- chiffrer un premier bloc de données de 128 bits avec AES grâce à une clé d'authentification
- faire un XOR entre ce résultat et les 128 bits suivants de données
- chiffrer ce nouveau résultat avec AES (toujours avec la même clé d'authentification)
- Faire un XOR entre ce résultat et les 128 bits suivants de données

On répète les deux dernières opérations pour traiter tous les blocs. On tronque ensuite le résultat final de 128 bits pour extraire les 64 bits de poids fort. C'est le MIC. L'intégrité se fait également sur les champs fixes de l'en-tête du paquet (contrairement à WEP et à WPA).

La 2eme étape représente le chiffrement en se basant sur le protocole CCMP.

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 :

- chiffrer la valeur initiale du compteur avec AES et la clé de chiffrement
- procéder à un XOR entre ce compteur chiffré et les 128 bits de données, on obtient le premier bloc chiffré
- incrémenter le compteur et le chiffrer avec AES (toujours avec la même clé)
- procéder à un XOR entre ce compteur chiffré et les 128 bits suivants de données, on obtient un autre bloc chiffré

On continue avec les deux dernières étapes jusqu'à avoir traité tous les blocs. Pour le dernier bloc, on conserve le résultat d'un XOR entre le compteur et les derniers bits de données.

H. Failles du WAP et WPA2 :

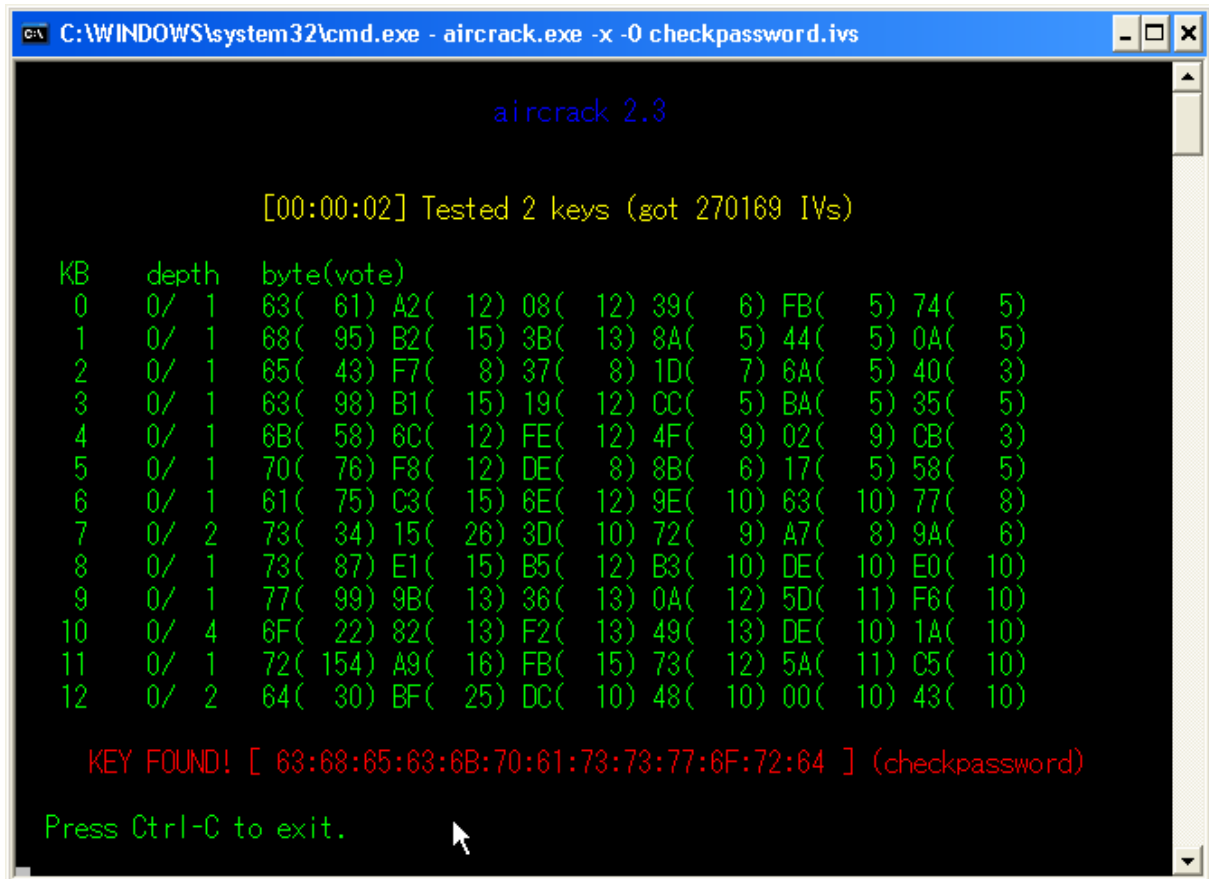
Le WPA aussi possède des failles, et une des failles du WPA est dans le mode WPA-PSK. En effet si on utilise un mot de passe usuelle, un pirate peut utiliser une attaque par dictionnaire. Une attaque par dictionnaire est une attaque dans laquelle on va tester une série de mot existant que l'on a répertorié dans un dictionnaire.

Dans le cas du WPA en mode « Enterprise », il est possible au moment de l'authentification de tenter une attaque de « Man in the Middle », c'est à dire que l'on a tenté de prendre la place de l'ordinateur qui essaye de s'authentifier au réseau (et qui possède des identifiants pour le faire !). On va donc pouvoir se faire passer pour lui auprès du point d'accès, et ainsi pouvoir s'authentifier à sa place. Un pirate peut aussi attendre que

la session soit établit, puis attaquer cette même session. En effet EAP qui est utilisé pour radius, le serveur d'authentification ne protège pas la session, elle peut donc être attaquée.

Il est aussi possible de faire un forçage brutal d'identifiants utilisateurs, mais cette technique peut s'avérer très longue. Mise à part cela, les techniques de WPA et WPA2 sont relativement sûr si elles sont bien utilisées, à savoir si notre clé WPA-PSK est complexe. En effet la seule façon de trouver la clé serait de l'attaque par brute force, c'est à dire, essayer toutes les combinaisons possibles, mais il faudrait des ressources de calculs énormes et un temps quasi infini afin de pouvoir trouver un mot de passe compliqué avec WPA et WPA2.

Les Risques liés aux réseaux sans fil :



```
C:\WINDOWS\system32\cmd.exe - aircrack.exe -x -0 checkpassword.ivs

aircrack 2.3

[00:00:02] Tested 2 keys (got 270169 IVs)

KB    depth  byte(vote)
0     0/ 1    63( 61) A2( 12) 08( 12) 39( 6) FB( 5) 74( 5)
1     0/ 1    68( 95) B2( 15) 3B( 13) 8A( 5) 44( 5) 0A( 5)
2     0/ 1    65( 43) F7( 8) 37( 8) 1D( 7) 6A( 5) 40( 3)
3     0/ 1    63( 98) B1( 15) 19( 12) CC( 5) BA( 5) 35( 5)
4     0/ 1    6B( 58) 6C( 12) FE( 12) 4F( 9) 02( 9) CB( 3)
5     0/ 1    70( 76) F8( 12) DE( 8) 8B( 6) 17( 5) 58( 5)
6     0/ 1    61( 75) C3( 15) 6E( 12) 9E( 10) 63( 10) 77( 8)
7     0/ 2    73( 34) 15( 26) 3D( 10) 72( 9) A7( 8) 9A( 6)
8     0/ 1    73( 87) E1( 15) B5( 12) B3( 10) DE( 10) E0( 10)
9     0/ 1    77( 99) 9B( 13) 36( 13) 0A( 12) 5D( 11) F6( 10)
10    0/ 4    6F( 22) 82( 13) F2( 13) 49( 13) DE( 10) 1A( 10)
11    0/ 1    72( 154) A9( 16) FB( 15) 73( 12) 5A( 11) C5( 10)
12    0/ 2    64( 30) BF( 25) DC( 10) 48( 10) 00( 10) 43( 10)

KEY FOUND! [ 63:68:65:63:6B:70:61:73:73:77:6F:72:64 ] (checkpassword)

Press Ctrl-C to exit.
```

A. Les Ondes Radioélectriques :

Les ondes radioélectriques utilisées dans les réseaux WIFI pour transporter l'information ont une grande capacité à se propager dans toutes les directions. En plus il est difficile d'arriver à confiner les émissions d'ondes radio dans un périmètre restreint. Donc le principal problème avec les ondes radio est la facilité que peut avoir une personne non autorisée d'écouter le réseau.

B. Interception des données :

Par défaut un réseau sans fil est non sécurisé et ouvert à n'importe quelle personne trouvant dans un dans le rayon de portée d'un point d'accès. Pour une personne particulière y a pas un gros risque surtout s'il s'agit de données personnels mais si c'est le cas d'une entreprise l'enjeu stratégique peut être très important.

C. L'intrusion réseau :

Dans le cas où on aura un réseau local (WIFI dans notre cas) installé sur une machine et cette dernière est dotée d'un réseau Internet on aura un grand risque à être infecté par un pirate qui va subir des attaques à partir de ce réseau local vu que ce dernier

donne l'accès au réseau Internet trouvant sur la machine et à la fin la personne ayant installé le réseau sans fil sera tenue responsable de l'attaque.

D. Le brouillage Radio :

La sécurité ce n'est pas seulement assure l'intégrité des données mais aussi assurer le bon fonctionnement de réseau. Dans le cas d'un réseau fil qui utilise les ondes radio on peut facilement brouiller ce dernier en juste envoyant un signal qui est proche des messages circulant dans le réseau.

E. Les Déni de service :

La méthode d'accès au réseau de la norme 802.11 est basée sur le protocole CSMA/CA, consistant à attendre que le réseau soit libre avant d'émettre. Une fois la connexion établie, une station doit s'associer à un point d'accès afin de pouvoir lui envoyer des paquets. Ainsi, les méthodes d'accès au réseau et d'association étant connus, il est simple pour un pirate d'envoyer des paquets demandant la désassociation de la station. Il s'agit d'un déni de service, c'est-à-dire d'envoyer des informations de telle manière à perturber volontairement le fonctionnement du réseau sans fil.

D'autre part, la connexion à des réseaux sans fils est consommatrice d'énergie. Même si les périphériques sans fils sont dotés de fonctionnalités leur permettant d'économiser le maximum d'énergie, un pirate peut éventuellement envoyer un grand nombre de données (chiffrées) à une machine de telle manière à la surcharger. En effet, un grand nombre de périphériques portables (assistant digital personnel, ordinateur portable, ...) possèdent une autonomie limitée, c'est pourquoi un pirate peut vouloir provoquer une surconsommation d'énergie de telle manière à rendre l'appareil temporairement inutilisable, c'est ce que l'on appelle un déni de service sur batterie.²

² <http://www.commentcamarche.net/contents/1283-les-risques-lies-aux-reseaux-sans-fil-wifi-802-11-ou-wi-fi>

Conclusion :

Pour finir le réseau WIFI est l'une des technologies les plus utilisées dans le monde entier et surtout dans les entreprises et pour cela il faut prendre en considération le facteur sécurité qui a un grand poids sur le niveau de l'information.

Après toutes les failles détectées dans le protocole WEP ou même WPA il est conseillé d'utiliser aujourd'hui WPA2 ainsi que limitez les adresses IP accédant au réseau.

Référence :

<http://www.commentcamarche.net/contents/1283-les-risques-lies-aux-reseaux-sans-fil-wifi-802-11-ou-wi-fi>

<http://www.linternaute.com/hightech/wifi/05-wifi/securite.shtml>