Rapport sécurité
Les algorithmes de cryptographie dans les réseaux Wi-Fi

Delahaye François-Xavier, Chenailler Jean-Christophe

le 2 mars 2003

Table des matières

1 Introduction

1.1 Utilisation des réseaux sans-fil

En raison de leur facilité de déploiement et de leur coût relativement faible, les réseaux sans fil sont de plus en plus utilisés. Les réseaux sans fil se développent très rapidement pour des réseaux temporaires (salons, conférences, ...), pour des points d'accès haut débit dans les lieux publics (aéroports, gares, métros, ...) connus sous le nom de " hotspot " ou des lieux privés accueillant du public (hôtel, restaurant, ...) ; dans de nombreux organismes et sociétés attirés par la souplesse des réseaux sans fil.

1.2 Les différents réseaux sans-fil

Comme pour les réseaux filaires, il existe différents types de réseaux sans fil : les réseaux personnels "WPAN" (Wireless Personal Area Networks), les réseaux locaux " WLAN " (Wireless Local Area Networks), les réseaux métropolitains " WMAN " (Wireless Metropolitan Area Networks) et les reseaux nationaux " WWAN " (Wireless Wide Area Networks).

1.3 Principe et utilisation de la norme 802.11b

Nous allons nous concentrer sur les réseaux " WLAN " de norme 802.11, et plus précisément de norme 802.11b, également appelée Wi-Fi (Wireless Fidelity) ou encore " Airport " chez Apple. La norme IEEE 802.11b a été adoptée en septembre 1999. Grâce à la technologie DSSS (Direct Sequence Spread Spectrum : envoi de l'information en simultané sur plusieurs canaux en parallèle), elle peut atteindre des débits de 11Mb/s sur une portée de 300 mètres et plus. La norme 802.11b utilise la bande des 2,4 Ghz, 14 canaux de transmission différents sont utilisables sur cette bande de fréquence (dont 4 canaux sont autorisés en France), ce qui permet à plusieurs réseaux de cohabiter au même endroit sans interférence. Pour s'identifier auprès d'un réseau, les utilisateurs d'un réseau sans fil 802.11b utilisent un identifiant de réseau (SSID). Le réseau local 802.11b est fondé sur une architecture cellulaire ou chaque cellule appelée BSS (Basic Service Set) est contrôlée par un " AP " (Access Point) également appelé pont, le tout formant un réseau appelé ESS (Extended Service Set). Ce mode de communication est appelé le mode " infrastructure ". Les ponts peuvent être reliés entre eux par des

liaisons radios ou filaires et un terminal peut alors passer d'un pont à un autre en restant sur le même réseau (concept du "roaming ").

1.3.1 Pont

Un pont sur un réseau sans fil équivaut à un concentrateur (hub) sur un réseau filaire. Chaque terminal sans fil reçoit donc tout le trafic circulant sur le réseau. Si ce terminal scrute simultanément plusieurs canaux, il recevra alors le trafic de tous les réseaux qui l'entourent.

1.3.2 Ad-hoc

Le mode de communication " ad-hoc " est également disponible dans la norme 802.11b : il s'agit d'un mode point à point entre des équipements sans fil qui utilise des protocoles de routage proactifs (échange périodique des tables de routage pour la détermination des routes) ou des protocoles de routage réactifs (les routes sont établies à la demande). Il est possible de reconstituer un réseau à partir de ce mode de communication.

1.3.3 CSMA

L'accès au réseau sans fil se fait par un protocole CSMA (Carrier Sense Multiple Access), quand un équipement du réseau veut émettre, il écoute le support de transmission et si celui-ci est libre, alors il émet. Une fonction CRC32 (Cyclical Redundancy Check sur 32 bits) présente sur le protocole 802.11b permet de s'assurer de l'intégrité des données transmises via une liaison sans fil. Cependant même si l'intégrité des données est préservée, l'authenticité n'est pas assurée par le CRC32.

1.3.4 WEP

Constitué d'une communication par voie herzienne, le Wi-Fi n'est pas à l'abris de piratage. En effet, comme toute émission radio, les ondes diffusées par la borne émettrice peuvent être captées par tout autre récepteur. Le 802.11b intègre en option un protocole de sécurité au niveau liaison appelé " WEP " (Wired Equivalent Privacy). Le WEP utilise l'algorithme de chiffrement RC4. La clef résultante de l'algorithme RC4 est d'une longueur de 64 bits ou 128 bits, cette suite d'octets est composée d'un vecteur d'initialisation (IV) sur 24 bits et d'une clef sur 40 ou 104 bits dépendante de ce vecteur

d'initialisation et de la clef WEP initiale. Cette clef permet de générer un " pseudo aléa " d'une longueur égale à la taille maximale d'une trame. Le chiffrement est effectué par un OU EXCLUSIF (XOR) entre ce " pseudo aléa " et le message transmis décomposé en blocs de longueur identique. Nous allons voir plus en détail les algorithmes de cryptographie du Wi-Fi, les limites de ses algorithmes(possibilités d'attaques), puis la future norme 802.11i qui en découle.

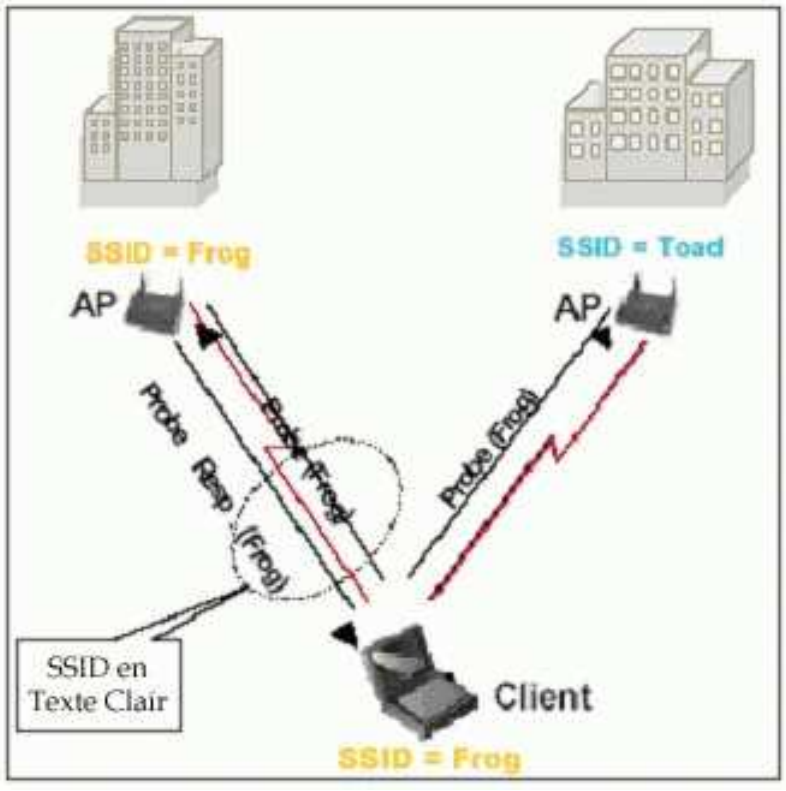
2 Explication des différents mécanismes d'authentification et de sécurité mis en oeuvre dans le WiFi

Les différents mécanismes utilisés en Wi-Fi sont :

1. SSID : Service Set Identifier
2. Open / Shared Authentification
3. WEP : Wired Equivalent Privacy

2.1 SSID : Service Set Identifier

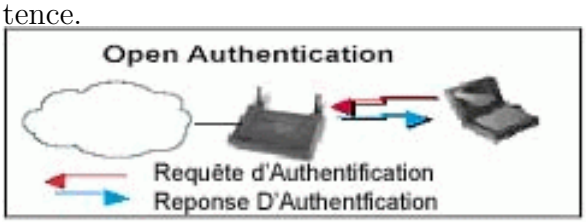
Le SSID est un identifiant unique à 32 caractères attaché à l'entête des paquets envoyés sur les réseaux sans-fil qui agit comme un mot de passe lorsqu'un système mobile essaye de se connecter au réseau. (Aussi appelé ESSID). Le SSID différencie un réseau sans-fil d'un autre, pour que tous les systèmes voulant se connecter à un même réseau utilisent le même SSID. Un système ne pourra pas se connecter au réseau sans-fil s'il ne donne pas le bon SSID. Le SSID n'est pas un mécanisme de sécurité, c'est juste un mécanisme d'authentification, de plus il est transmis en clair dans les requêtes 'probe', et cela même lorsque l'on désactive la fonction 'BroadCast SSID'. Un SSID s'appelle aussi "Nom de réseau" car ce n'est qu'un nom qui identifie un réseau.



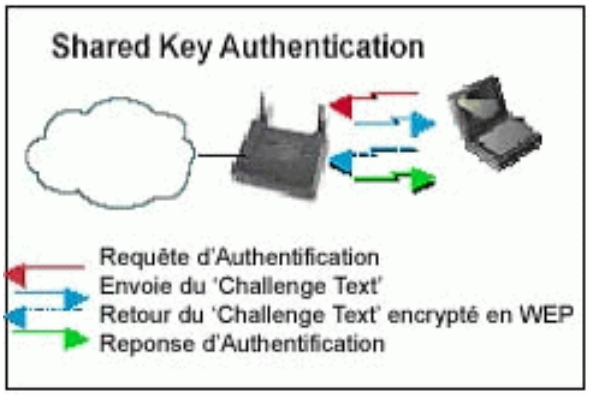
2.2 Open / Shared Authentification

2.2.1 Open Authentification

Aucune authentification n'est effecutée, le client declare juste son existence.



2.2.2 Shared Authentification



Dans le processus partagé d'authentification, le client envoie tout d'abord une demande à l'access point, qui lui renvoie une 'challenge text'. Le client doit encrypter ce texte en utilisant sa clef WEP (configurée au préalable). Le client retourne ensuite le paquet à l'access point et si celui-ci arrive a décrypter correctement ce fichier, l'authentification a réussi.

2.3 WEP : Wired Equivalent Privacy

Afin d'assurer la confidentialité des données transitant sur un réseau 802.11b, le WECA à opté pour le WEP une solution de chiffrement qui se base sur un algorithme RC4 utilisant un chiffrement de 40 bits (voir 128 bits).

Le but principal de WEP est :

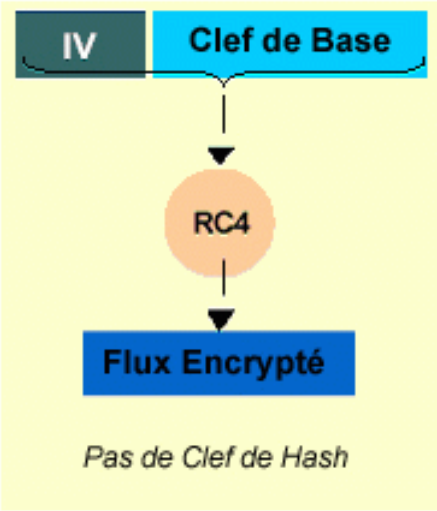
- " Empêcher l'accès au réseau par des utilisateurs qui ne possèdent pas la clef WEP appropriée
- " Empêcher le décryptage des données capturées sur un WLAN sans la possession de la clef WEP adéquate.

WEP est un mécanisme d'encryption symétrique, c'est-à-dire que c'est le même algorithme qui est utilisé pour l'encryptage et le décryptage des données.

L'algorithme RC4 utilisé à été crée par Ron Rivest de RSA Data Security, INC. Cet algorithme permet d'encoder un flux de données en utilisant une clef de longueur variable, jusqu'à 256 octets, mais la norme IEEE impose une longueur de clef de 40 bits, bien que la plupart du matériel supporte des clefs de 128 bits.

Le standard IEEE 802.11 décrit comment utiliser l'algorithme RC4 et les clefs avec WEP, mais la négociation et la distribution des clefs ne sont pas mentionnées. Il en ressort, que chacun peut choisir d'implémenter un système propriétaire pour gérer et configurer les différentes clefs. Cette malencontreuse omission anéantit le travail de création d'un standard, et donc si un fabricant utilise un système qui permet aux clefs d'être compromises, tous les paquets encodés seront aussi compromis.

Fonctionnement de l'algorithme RC4 :



- **RC4 crypte les Flux de Données** *(Utilisé entre autre pas SSL)*
- **Etend une clef** (aussi appelée Graine) **dans un flot de bits pseudo-aléatoire**

Propriétés d'un OU Exclusif (XOR)

- **XOR est facile à Implementer en HardWare**

⊗	0	1
0	0	1
1	1	0

- **Lorsque l'on applique XOR deux fois, cela redonne le resultat d'origine**

If A ⊗ B = C, then C ⊗ B = A

```
  101101        110110
⊗ 011011      ⊗ 011011
  110110        101101
```

Encryptions de stream en WEP

- **Pour Encrypter: on XOR la clef avec le Text Clair**

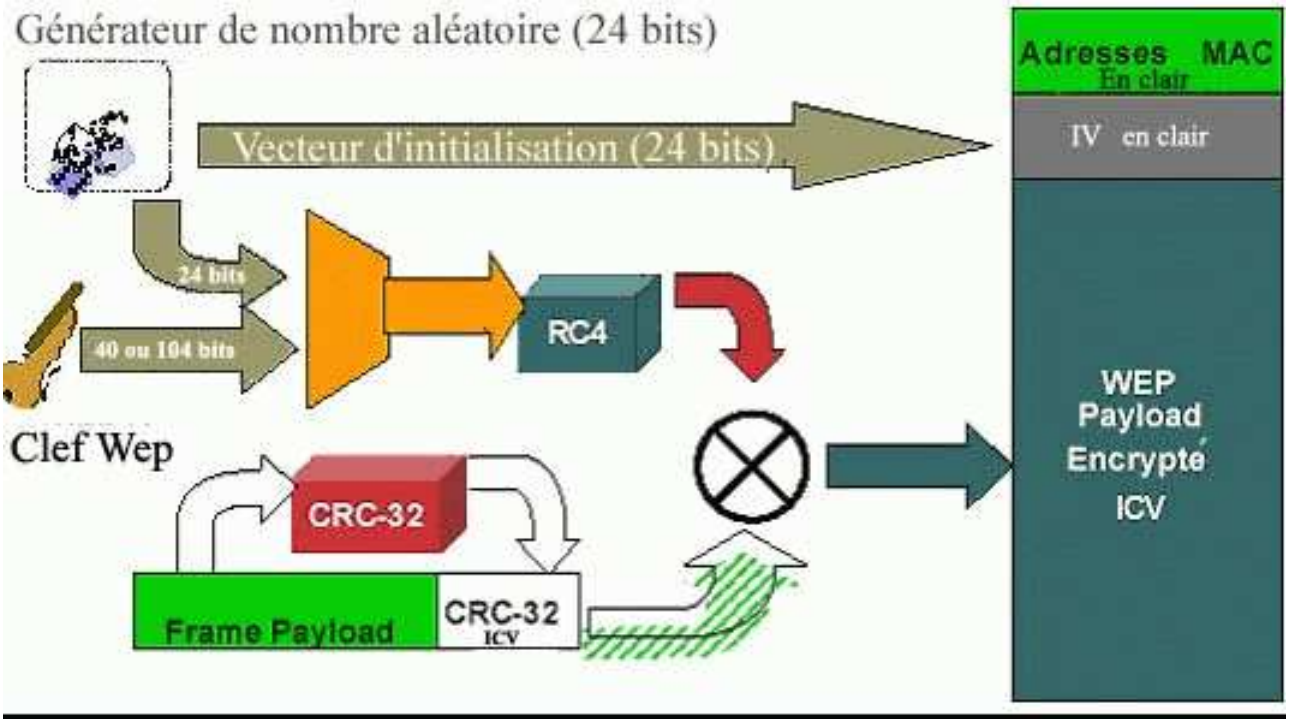
  Clef ⊗ Text Clair => Text Crypté

- **Pour Decypter: On XOR la Clef avec le Text Crypté**

  Clef ⊗ Text Crypté => Text Clair

```
"WIRELESS"  = 58495245C455353
Clef        = 123456789ABCDEF   XOR
              4A7D043D6FBE9C
Clef        = 123456789ABCDEF   XOR
"WIRELESS"  = 58495245C455353
```

Mécanisme d'encryption du WEP



Le standard IEEE 802.11 fournit 2 mécanismes qui permettent de sélectionner une clef lorsque l'on crypte ou décrypte les données.

Le premier mécanisme consiste en un jeu de plusieurs clefs par défaut. Les clefs par défaut sont partagées par toutes les stations utilisant le sous-système sans fil. L'avantage de ce système est qu'une fois qu'une station possède les clefs par défaut elle peut communiquer de façon sécurisée avec l'ensemble des stations du sous-système. Le problème est qu'une fois que les clefs par défaut sont distribuées largement elles sont plus faciles à compromettre.

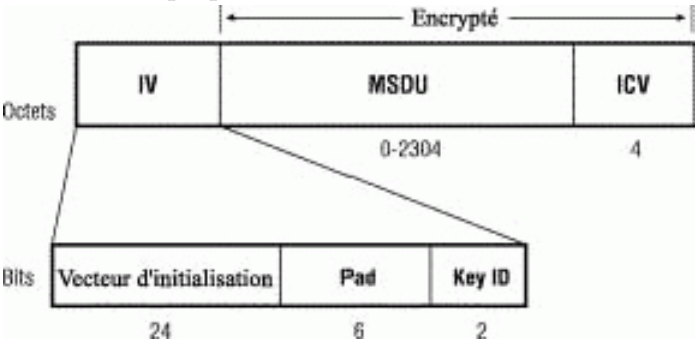
Le second mécanisme autorise une station à établir une table de clefs en relation avec les autres stations. Ce système est beaucoup plus securisé puisque peu de stations possèdent les clefs, mais cela pose problème lorsque le nombre de stations augmente.

Voici un exemple de paquet WEP

Les Headers et Trailer sont ajoutés au corps encrypté du paquet, la clef qui à été utilisée pour encoder le corps est indiquée dans la partie KeyID du Header ainsi qu'un vecteur d'initialisation, une valeur de contrôle d'intégrité est incluse dans le trailer.

La longueur de la clef varie en fonction de la longueur de la clef établie avec WEP plus un vecteur d'initialisation. Par exemple, une clef WEP de 64 bits comprend 40 bits pour la clef et 24 bits pour le vecteur d'initialisation. Ceci pose souvent des problèmes de compréhension a propos de la longueur des clefs.

Détail d'un paquet WEP



3 Les attaques sur les normes existantes

3.1 Le Wardriving

Le Wardriving est une nouvelle forme de piratage, qui fait fureur actuellement(surtout aux Etats-Unis) et qui consiste à rechercher les réseaux sans fils détectables sur la voie publique. Pour cela, un "wardriver" est équipé d'un terminal mobile, avec une antenne et éventuellement un mobile GPS. Il n'a alors plus qu'à se balader tranquillement pour capter les réseaux sans fils existants dans les parages et les cartographier. Il pourra alors pratiquer deux sortes d'attaques :

- Détourner une connexion réseau à son avantage, et éventuellement pouvoir surfer sur Internet gratuitement.
- Ecouter ce qui se passe sur le réseau pour notammant voler des informations.

Le plus simple pour appliquer ce genre d'attaque est encore d'utiliser un script automatique qui va assigner à votre périphérique le premier noeud accessible. Voir : http ://reseaucitoyen.be/index.php ?ScriptWarDriving.

Le war driving peut aussi se pratiquer sous windows grâce à "network Stumbler". Il a l'avantage de donner l'adresse mac, le ssid le nom de la machine, le canal utilisé, le type de reseau (ap , per to per...), il notifie si wep est activé, donne le niveau de bruit et le niveau du signal, peut se connecter avec un gps et ainsi donner la latitude et la longitude (les résultats sont importables sur Microsoft map), l'heure de début et de fin de captage du signal. Pour chaque ssid trouvé, il donne aussi un graphique des connections (nombre de dB, bruit et signal sur ligne de temps). Voir http ://www.wifi-montauban.net/communaute/index.php/TrebucherSansFil

Le War driving est surtout utilisé sur les réseaux non sécurisés (utilisateurs n'activant pas le wep ou ne changeant pas les mots de passe par défaut). Néanmoins il peut se pratiquer via les failles de sécurité du Wep.

3.2 Attaque du Wep

De façon très succincte, le chiffrement utilisé par WEP peut être décrit comme suit : la clé partagée est notée K. Au moment de la transmission des données M, celles-ci sont d'abord concaténées avec leur checksum c(M). Parallèlement à cela le vecteur d'initialisation est concaténé à la clé K, et passé en entrée à la fonction de chiffrement RC4. Le résultat subit un XOR

avec les données, ce qui nous donne pour résumer :

$$C = (M||c(M))XORRC4(IV||K)$$

La structure du RC4 se compose de 2 parties distinctes ; la première, ou key scheduling algorithm, génère une table d'état S à partir des données secrètes, à savoir soit 64 bits (40 bits de clé secrète et 24 bits d'IV) ou 128 bits (104 bits de clé secrète et 24 bits d'IV). La deuxième partie de l'algorithme RC4 est le générateur de données en sortie, qui utilise la table S et 2 compteurs. Ces données en sortie forment une séquence pseudo-aléatoire.

3.2.1 Attaque par la méthode de Fluhrer, Mantin et Shamir

Fluhrer, Mantin et Shamir présentent 2 faiblesses dans la spécification de l'algorithme RC4. La première repose sur le fait qu'il existe de larges ensembles de clés dites faibles, c'est-à-dire des clés dont quelques bits seulement suffisent à déterminer de nombreux bits dans la table d'état S (avec une forte probabilité), ce qui affecte directement les données produites en sortie ; c'est l'attaque nommée ńinvariance weaknessż.

La deuxième attaque de Fluhrer, Mantin et Shamir est la ńknown IV attack ż. Elle nécessite la connaissance de l'IV ce qui est le cas puisqu'il circule en clair sur le réseau, et la connaissance du premier octet de M (à deviner). Dans un certain nombre de cas (" les cas résolus ", suivant l'expression de Fluhrer, Mantin et Shamir) , la connaissance de ces 2 éléments permet de déduire des informations sur la clé K.

Selon les auteurs, ces 2 attaques sont applicables et peuvent permettre une récupération complète de la clé avec une efficacité bien supérieure à l'attaque par recherche exhaustive.

3.2.2 Conséquences

Le but n'est pas ici de présenter une liste exhaustive de toutes les attaques possibles sur le Wep, mais de montrer qu'il existe de nombreuses failles de sécurité. En conséquence de ses failles, il est nécessaire de faire évoluer la norme 802.11b vers quelque chose de plus sécurisé. C'est le but de la norme 802.11i que nous allons voir maintenant.

4 La future norme 802.11i

Pour contrer les différentes erreurs présentes dans la norme 802.11b, une nouvelle version est en cours d'élaboration : IEEE 802.11i. Ces principales améliorations sont les suivantes :

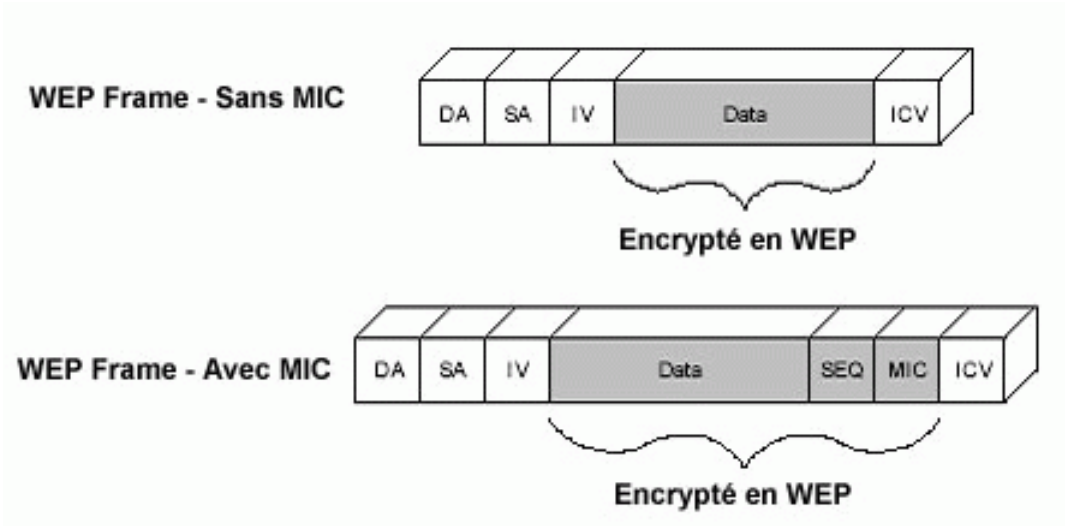
1. MIC (Message Integrity Check) & Sequencer Number
2. TKIP
3. Rotation de la Clef de Broadcast (Broadcast Key Rotation)

4.1 Message Integrity Check (MIC)

Contrairement à CRC32, MIC utilise un algorithme de hash pour encrypter les données d'un paquet WEP.

Le MIC est basé sur une valeur aléatoire, l'adresse MAC de destination, l'adresse MAC de source et playload. N'importe quel changement sur l'une de ces valeurs implique un changement de la valeur MIC

La valeur MIC est incluse dans le playload comme indiqué par le schéma suivant :



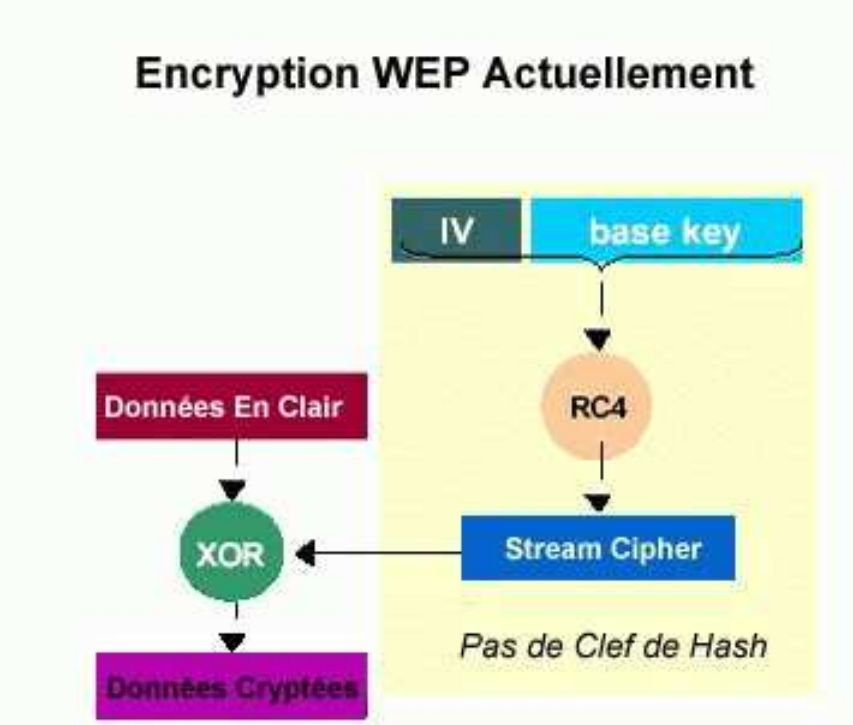
4.2 TKIP

La fonction de Hash de TKIP inclus l'AID (Association ID) dans la génération du hash de la clef, et s'assure que la clef générée est différente pour chaque connection (pour éviter les collisions des Vecteurs d'Initialisation, IV).

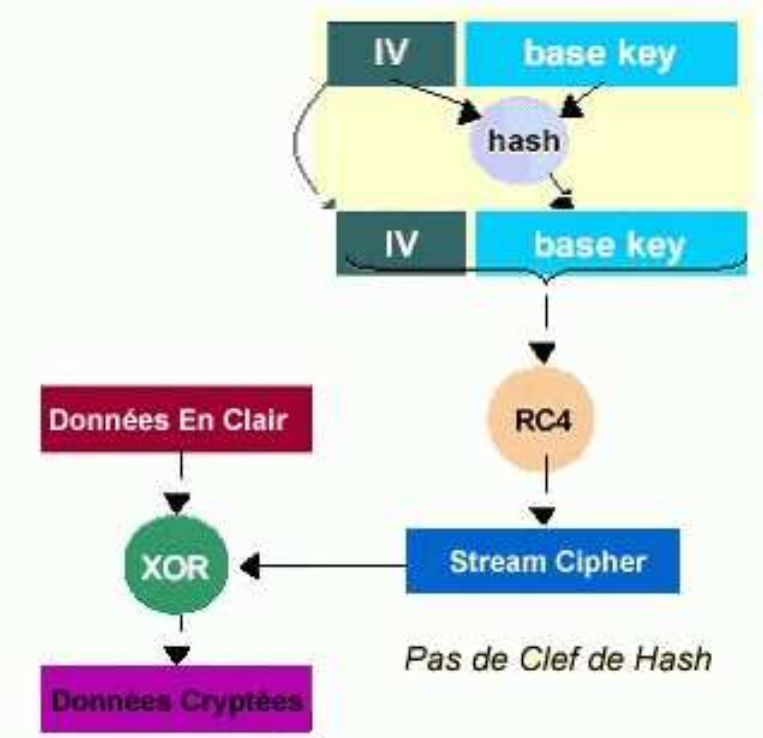
Les paquets en flux montant (vers l'access point) utilisent un IV pair et les paquets en flux descendant (venant de l'Access Point) utilisent des IV impairs.

Les IV s'incrémentent lors des transmissions et l'Anti-Replay s'assure que les paquets reçus avec un ancien IV sont bien rejetés.

Voici un schéma montrant la création d'un paquet WEP dans la norme 802.11b



Avec une implémentation de TKIP voici le fonctionnement :



4.3 Rotation de la clef de Broadcast

Comme nous l'avons vu, une clef de broadcast statique est vulnérable à une Weak IV attack, en utilisant un système de rotation de cette clef, on peut donc prévenir ce genre d'attaque.

5 Conclusion

En conclusion nous pouvons dire que la norme actuelle 802.11b est très peu sécurisée, pour ne pas dire non sécurisée. La norme actuelle peut en effet subir différentes attaques et permettre à n'importe quel hacker débutant de s'introduire sur un réseau Wi-Fi. En conséquence les algorithmes de cryptographie associés au Wi-Fi doivent subir quelques modifications pour être plus efficaces (MIC, TKIP). La norme 802.11i devrait répondre à la demande de sécurisation de plus en plus forte.

6 Glossaire

- **WPAN :** (Wireless Personal Area Networks) réseaux de taille locale
- **WLAN :** (Wireless Local Area Networks) réseaux de taille métropolitaine
- **WMAN :** (Wireless Metropolitan Area Networks) reseaux de taille nationale
- **AP ou Access Point :** Point du réseau à partir duquel le fournisseur de services permet à l'utilisateur de se relier au réseau.
- **Wi-Fi ou Wireless Fidelity :** c'est le nom de la technologie IEEE 802.11b de réseau local ethernet sans fil (WLAN), basé sur la fréquence 2.4 Ghz. La technologie de réseau sans fil Wi-fi est autrement appelée 802.11 b.
- **SSID :** identifiant de réseau pour le Wi-Fi.
- **Pont :** Un pont sur un réseau sans fil équivaut à un concentrateur (hub) sur un réseau filaire. Chaque terminal sans fil reçoit donc tout le trafic circulant sur le réseau. Si ce terminal scrute simultanément plusieurs canaux, il recevra alors le trafic de tous les réseaux qui l'entourent.
- **Ad-hoc :** Le mode de communication " ad-hoc " est disponible dans la norme 802.11b : il s'agit d'un mode point à point entre des équipements sans fil qui utilise des protocoles de routage proactifs (échange périodique des tables de routage pour la détermination des routes) ou des protocoles de routage réactifs (les routes sont établies à la demande). Il est possible de reconstituer un réseau à partir de ce mode de communication.
- **CSMA :** L'accès au réseau sans fil se fait par un protocole CSMA (Carrier Sense Multiple Access), quand un équipement du réseau veut émettre, il écoute le support de transmission et si celui-ci est libre, alors il émet. Une fonction CRC32 (Cyclical Redundancy Check sur 32 bits) présente sur le protocole 802.11b permet de s'assurer de l'intégrité des

données transmises via une liaison sans fil. Cependant même si l'intégrité des données est préservée, l'authenticité n'est pas assurée par le CRC32.

- **WEP :** C'est le nom donné au protocole de sécurité utilisé dans la technologie Wi-Fi. Le Wep utilise l'algorithme de sécurité RC4

- **RC4 :** Algorithme de sécurité utilisé par le WEP.

- **Le Wardriving :** technique qui consiste à s'introduire sur un réseau Wi-Fi en se promenant à proximité d'un réseau non protégé.

- **WECA :** Organisme indépendant en charge d'assurer l'interopérabilité des réseaux sans fils basé sur la norme IEEE 802.11

7 Liens

- http ://www.securiteinfo.com/crypto/802_11.shtml
- http ://www.isaac.cs.berkeley.edu/isaac/wep-faq.html
- http ://www.rsasecurity.com/newsletter/wireless/2002_winter/feature.html
- http ://jtr2002.unilim.fr/fichiers-presentation/aironet-security-2002-10-08.pdf
- http ://reseaucitoyen.be/index.php ?ScriptWarDriving
- Plein de liens sur le protocole 802.11
  et autres http ://www.paris-sansfil.net/index.php/TechniLinks
- Les différentes attaques : http ://www.guill.net/index.php3 ?cat=4
- Document cisco sur LEAP et les nouvelles générations de WLAN :
  http ://www.cisco.com/warp/public/102/wlan/nextgen.html
- Le site officiel du WECA : http ://www.weca.net
- Article très complet sur la sécurité des Réseaux WLAN :
  http ://www.hsc.fr/ressources/presentations/clusif802.11b/

8 Bibliographie

- FLUHRER, MANTIN et SHAMIR, Weaknesses in the key scheduling algorithm of RC4, English Annual Workshop on Selected Areas in Cryptography (08/2001).
- STUBBLEFIELD, IOANNIDIS et RUBIN, Using the Fuhrer, Mantin and Shamir Attack to Break WEP, AT&T Labs Technical Report TD-4ZCPZZ (08/2001).