Master MAIM
Ingénierie du Risque
TER

LE PROTOCOLE WEP :

Mécanismes et Failles

2006 - 2007
Université LYON 1

Vincent HERBERT

Table des matières :

1. INTRODUCTION: 5

2. PRESENTATION GENERALE : 6

2.1. Qu'est ce qu'un réseau Wi-Fi? 6
2.1.1. Les différents types de réseaux: 6
2.1.2. Le Wi-Fi en question: 6

2.2. Qu'est ce que le TCP/IP? 7
2.2.1. Qu'est ce qu'un protocole? 7
2.2.2 Le TCP/IP en question: 7

3. LES MECANISMES DU WEP : 8

3.1. Qu'est ce que le WEP ? 8

3.2. Le chiffrement WEP: 9
3.2.1. Fonctionnement général: 9
3.2.2. Initialisation de la clé: 10
3.2.3. Obtention du keystream: 12
3.2.4. Le contrôle d'intégrité: 13
3.2.5. La constitution du message final et son encapsulation: 13

3.3. Le déchiffrement WEP: 15

3.4. La distribution des clés: 16

3.5. WEP et authentification: 17
3.5.1. Processus d'authentification ouverte: 17
3.5.2. Processus d'authentification à clé partagée: 18

4. LES FAILLES DU WEP : 18

4.1. Premier aperçu des failles: 18

4.2. Les faiblesses du IV: 19
4.2.1. Réutilisation du Keystream : 19
4.2.2. Attaque par clé apparentée: 20
4.2.3. Attaques FMS : 21
4.2.4. Optimisation de FMS: 22
4.2.5. Attaque par fragmentation: 23

4.3. Les problèmes des clés de chiffrement: 25

4.4. L'exploitation du contrôle d'intégrité: 26

4.5. Les failles dans l'authentification: 27

5. LES NOUVELLES PARADES :.....28
6. CONCLUSION:.....30
7. ANNEXES: 31
7.1. Bibliographie: **31**
7.2. Publications: **31**
7.3. Liens: **31**
7.4. Chronologie du protocole WEP: **32**
7.5. Glossaire: **32**

1. INTRODUCTION:

La problématique de la sécurité informatique sera de plus en plus omniprésente dans notre société, dans les années à venir. Nous sommes témoins depuis la fin du XX^{ème} siècle d'une véritable révolution technologique. Aujourd'hui en France, les ordinateurs ainsi qu'Internet sont dans la majorité des foyers et entreprises. On a coutume de dire que les nouvelles technologies évoluent sans cesse. Cette banalité s'applique particulièrement aux réseaux informatiques.

Depuis environ 5 ans, les réseaux sans-fil ont tendance à s'imposer sur le marché, ils présentent à la fois l'avantage de la simplicité et de l'esthétique. Parallèlement au déferlement de nouvelles technologies, la sécurité a souvent été négligé jusqu'ici, entraînant ainsi plusieurs dérives. C'est dans ce contexte général qu'apparut le protocole WEP. Ce dernier vise à protéger un réseau sans fil en s'appuyant sur une technique de chiffrement. Il tente de répondre à lui tout seul à 3 des principaux objectifs de la Cryptographie, à savoir : la confidentialité, l'authentification et l'intégrité des données.

Nous allons ici nous intéresser aux faiblesses du protocole WEP du point de vue sécuritaire. Pour ce faire, nous nous appuierons essentiellement sur les articles « Intercepting Mobile Communications » et « The Final Nail in Wep's Coffin » ainsi que sur d'autres documents dont les références sont fournies en annexe.

Dans la première partie de notre travail, nous aborderons brièvement des notions qui nous semblent essentielles à la compréhension du protocole WEP à savoir les réseaux Wi-Fi et les protocoles TCP/IP. Nous poursuivons le rapport en décrivant en détail les mécanismes de chiffrement et de déchiffrement du WEP. Par la suite, nous tâcherons de présenter et d'expliquer de la façon la plus complète qui soit, les innombrables failles de ce protocole. Pour finir, nous donnerons les différentes parades trouvées pour pallier à ces faiblesses.

2. PRESENTATION GENERALE :

2.1. Qu'est ce qu'un réseau Wi-Fi?

Par définition, un réseau informatique est un ensemble d'ordinateurs reliés entre eux et échangeant des informations.

2.1.1. Les différents types de réseaux:

On distingue différents types de réseaux selon leur taille (en termes de nombre de machines), leur vitesse de transfert des données ainsi que leur étendue. Les réseaux privés sont des réseaux appartenant à une même organisation. On distingue essentiellement trois catégories de réseaux :

- ***LAN*** (Local Area Network) dont la portée est de quelques dizaines de mètres.
- ***MAN*** (Metropolitan Area network) dont la portée est de quelques centaines de mètres.
- ***WAN*** (Wide Area Network) dont la portée est de quelques kilomètres.

2.1.2. Le Wi-Fi en question:

Les ***réseaux sans-fil (WLAN* pour *Wireless Local Area Network)*** sont de plus en plus employés en entreprise. Ils apportent flexibilité et efficacité. Ils échangent les messages par ondes radioélectriques et par conséquent sont très sensibles aux écoutes extérieurs pour 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

Deux standards existent pour les réseaux mobiles : Bluetooth et ***802.11*** (plus communément appelé ***Wi-Fi***, contraction de ***Wireless Fidelity***). Contrairement au Bluetooth, 802.11 permet des débits élevés à de grandes distances (plusieurs centaines de mètres). 802.11 est un protocole réseau sans fil qui est actuellement de plus en plus utilisé pour les réseaux locaux (entreprises, conférences, particuliers, etc.).

La norme Wi-Fi est devenu le symbole de l'informatique et de l'Internet nomades. Dans la pratique, le Wi-Fi permet de relier des ordinateurs portables, des ordinateurs de bureau, des assistants personnels ou tout type de périphérique à une liaison haut débit (11 Mbits/s) sur un rayon de plusieurs dizaines de mètres en intérieur à plusieurs centaines de mètres en environnement ouvert.

Ainsi, des opérateurs commencent à irriguer des zones à fortes concentrations d'utilisateurs (gares, aéroports, hôtels, trains, etc.…) avec des réseaux sans fils. Ces zones d'accès sont appelées «hot spots».

Installer un réseau sans fil sans le sécuriser peut permettre à des personnes non autorisées d'écouter et d'accéder à ce réseau. Il est donc indispensable de sécuriser les réseaux sans fil dès leur installation. Il est possible de sécuriser son réseau de façons plus ou moins forte selon les objectifs de sécurité que l'on se fixe et les ressources dont on dispose. Il existe des moyens de sécurité implantés de base sur le matériel Wi-Fi (carte et point d'accès) permettant un premier niveau de protection, mais ces moyens de sécurisation sont facilement contournables.

2.2. Qu'est ce que le TCP/IP?

2.2.1. Qu'est ce qu'un protocole?

Un protocole est une méthode standard qui permet la communication entre des processus (s'exécutant éventuellement sur différentes machines), c'est-à-dire un ensemble de règles et de procédures à respecter pour émettre et recevoir des données sur un réseau. Il en existe plusieurs selon ce que l'on attend de la communication. Certains protocoles seront par exemple spécialisés dans l'échange de fichiers (le FTP), d'autres pourront servir à gérer simplement l'état de la transmission et des erreurs (c'est le cas du protocole ICMP).

2.2.2. Le TCP/IP en question:

Sur Internet, les protocoles utilisés font partie d'une suite de protocole, c'est-à-dire un ensemble de protocoles reliés entre-eux. Les protocoles TCP/IP ont été conçus pour assurer une connectivité universelle entre les ordinateurs. L'objectif des protocoles de la famille TCP/IP est d'assurer, à tous les équipements terminaux connectés, la possibilité d'échanger des données, sans se soucier de la complexité de l'infrastructure sous-jacente. Les protocoles ont été conçus simplement afin d'autoriser un développement et une diffusion rapide des applications les utilisant, et de faciliter l'interopérabilité.

3. LES MECANISMES DU WEP :

3.1. Qu'est ce que le WEP ?

Le protocole WEP (Wired Equivalent Privacy) fait partie de la norme internationale IEEE 802.11 ratifiée en septembre 1999. Il est très répandu et implémenté dans un grand nombre de cartes réseaux sans fil. Le WEP prétend (comme son l'indique) offrir une solution de confidentialité équivalente à un réseau filaire. En effet, les réseaux câblés sont, par nature, plus sécurisés que les réseaux sans fil car il faut se brancher physiquement sur le réseau. Il ne fut cependant pas créer par des experts en cryptographie. D'un point de vue plus théorique, il protège les communications de la couche liaisons de données (niveau 2 du modèle OSI).

Le WEP est employé dans un WLAN pour rendre inintelligible à un tiers non autorisé les données encapsulées dans des trames. (Un paquet ne peut en effet pas transiter directement sur un réseau.) Le WEP a pour objectif de satisfaire l'association (s'assurer qu'on discute avec les membres du même WLAN), la confidentialité, l'authentification et l'intégrité. Il est défini comme :

« assez fort » (reasonably strong)
La longueur des clés utilisées rend difficile une attaque de type force brute, c'est-à-dire avec l'utilisation de toutes les clés possibles.

« à synchronisation automatique » (self synchronizing)
Chaque paquet contient assez d'informations pour permettre à quiconque possède la clé de déchiffrer son contenu. La connaissance du contenu des paquets précédant n'intervient pas dans le déchiffrement. Autrement dit, les paquets sont autonomes.

« efficace » (efficient)
Sa simplicité fait qu'il peut être implémenté en logiciel aisément. Cela signifie aussi que les opérations de chiffrement et de déchiffrement sont rapides.

« normalement exportable »
Le standard WEP utilise une longueur de clé variable (jusqu'à 2048 bits mais les USA limitent la taille des clés à l'export)

« optionnel »
La mise en place et l'utilisation du WEP dans les équipements sont en effet optionnelles.

3.2. Le chiffrement WEP:

3.2.1. Fonctionnement général:

Le ***WEP (Wired Equivalent Privacy)*** est un protocole qui permet (en théorie, tout du moins) d'éviter le ***eavesdropping*** (écoute clandestine) en chiffrant les communications. Il peut être utilisé pendant la phase d'authentification ou encore pour chacune des trames de données. Il repose sur l'algorithme à clé symétrique RC4. Le mécanisme de distribution des clés n'est pas précisé. Elles doivent dont être saisis manuellement sur les stations et les AP.

C'est dans le champ de contrôle FC (***Frame Control***) des trames de données et d'authentification qu'est précisée l'utilisation du chiffrement WEP. Le bit positionné à 1 signifie que le corps de la trame est chiffré en WEP.

Le chiffrement se décompose en plusieurs phases :

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

Nous avons employé ici des termes que nous tâcherons d'expliciter du mieux possible dans les pages qui viennent. Nous allons ensuite détaillé chacune de ces étapes, pas à pas.

a) Le vecteur d'initialisation:

Le vecteur d'initialisation (IV – ***Initialization Vector***) est une séquence de bits qui change régulièrement (à chaque trame envoyée si l'implémentation est bonne). 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, soit 2^{24} valeurs possibles. 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.

NB : Certains systèmes sophistiqués offrent des mécanismes de synchronisation qui dérivent des clés de façon automatique et sûre.

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).Son nom

signifie : Ron's Code #4 ou encore Rivest Cipher #4. Il utilise différentes tailles de clé, couramment jusqu'à 256 bits. Le RC4 est la propriété de la RSA Security, mais la version allégée ARC4 peut être utilisée légalement. 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 mais une mauvaise implémentation peut entraîner des failles. 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.

Le procédé mathématique est né d'un vide technique laissé par d'autres procédés de chiffrement extrêmement efficaces mais très gourmands en puissance de calcul. Le gros avantage de RC4 est qu'il fournit un niveau de sécurisation assez élevé, tout en étant implantable de façon logicielle, donc à faible coût. RC4 est l'un des protocoles de chiffrement les plus utilisés dans le monde.

Deux étapes sont nécessaires pour l'opération de chiffrement :

- L'initialisation de la clé
- La réalisation du ***cryptogramme* (*texte chiffré* ou *cyphertext*)**

3.2.2. Initialisation de la clé:

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

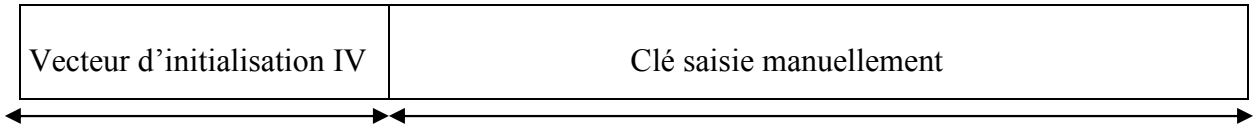
- 40 bits, soit 5 octets
- 104 bits, soit 13 octets

Parfois, les constructeurs ont mis en place des tailles de clé supérieures. Ces valeurs n'étant pas normalisées, il faut veiller à l'interopérabilité des équipements.

La clé K est concaténée à l'IV en position de poids faible généralement. On trouve parfois l'inverse. On notera par la suite : || l'opérateur de concaténation. On obtient alors une clé de 64 bits (8 octets) ou 128 bits (16 octets) que l'on appelle graine, germe, plaintext ou encore seed : IV || K

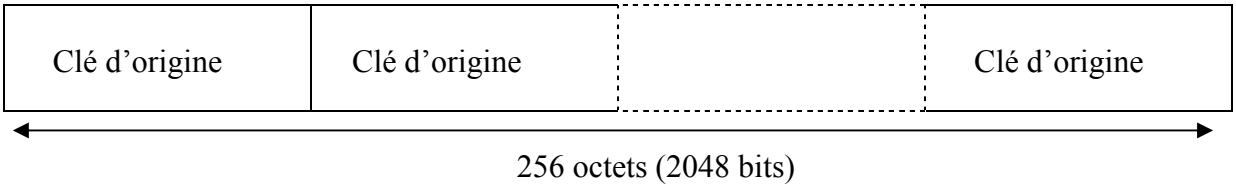
NB : Les constructeurs parlent souvent de clés de 64 bits ou de 128 bits. En réalité, la taille effective de la clé est, comme nous l'avons vu, de 40 bits ou 104 bits. Un mécanisme utilisant des clés WEP de 232 bits est parfois disponible.

Clé d'origine :



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) par la suite.

Table initialisée :



Par permutation et autres manipulations, les cellules sont ensuite mélangées. On initialise une table d'états T (qui sera le masque appliqué sur le texte clair) avec T[i]=i pour $0 \leq i \leq$ longueur(T)-1. Ce procédé porte le nom de Key Scheduling Algorithm (KSA) ou encore ***module de mise à la clé***. A son issue, tous les éléments de la table auront été permutés.

L'algorithme KSA, pour une clé WEP K de taille t est :

KSA(K,t) :

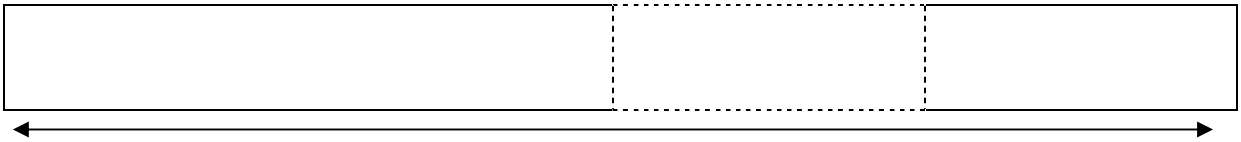
/* S est défini comme vu précédemment.
S et T contiennent des nombres entre 0 et t (une fois convertis en base 10).
Les additions se font modulo t.
On va prendre ici t=256 (taille usuelle) : */

pour i de 0 à 255 faire
T[i]=i
fin pour
y ← 0

pour x de 0 à 255 faire
    y ← y + T[x] + S[x] (modulo 256)
    T[x] ↔ T[y]
fin pour

L'entropie (mesure de l'aléa) de cette technique est assez importante puisque l'un des indices (à savoir « y ») est déduit de la valeur contenue dans la table qui est elle-même en cours de modification.

Table aléatoire résultante:



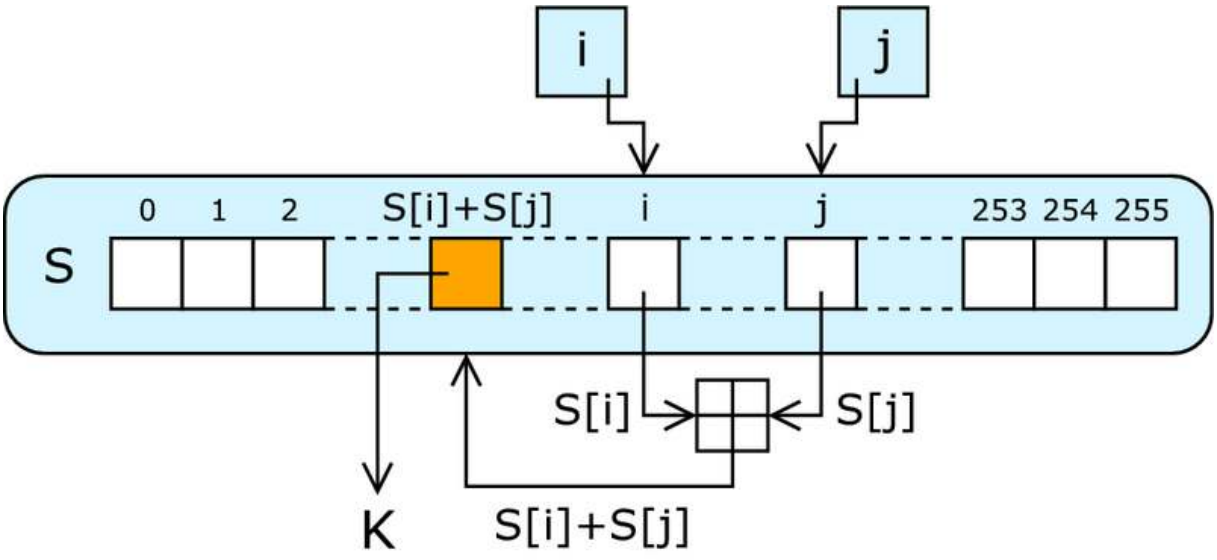
256 octets (2048 bits)

Une fois la table T mélangée, on peut fabriquer des PRNs ou « Pseudo Random Numbers » à l'aide d'un générateur PRGA ou « Pseudo Random Generator Algorithm » qui fonctionne sur le même principe que le module KSA mais sans faire appel à la clé K. L'algorithme est comme suit :

PRGA(T) :
x ← 0
y ← 0
x ← x+1
y ← y+T[x]
T[x] ↔ T[y]
z ← T[x] + T[y] (modulo 256)
renvoie T[z]

La clé de chiffrement utilisée est une séquence de bits extraite de cette table à partir du PRGA. On appelle cette ***séquence pseudo aléatoire, suites-clé, masque*** ou encore ***keystream***.

3.2.3. Obtention du keystream:



Comme le temps de génération de celle-ci est très court, elle peut évoluer en cours de chiffrement, par exemple en utilisant un autre IV. Ainsi la cryptanalyse en recherche de clé devient plus ardue.

3.2.4. Le contrôle d'intégrité:

Un contrôle de redondance cyclique (CRC Cyclic Redundancy Check) dans le cas d'un code des trames MAC est prévu pour pallier les erreurs de transmission par ajout de redondance. La redondance ajoutée, communément appelée (à tort) somme de contrôle (checksum), est obtenue par un type de hachage sur l'ensemble des données. Les propriétés du CRC sont telles que le niveau de sécurité atteint est très faible. Un pirate pourrait en effet modifier le contenu de la trame et insérer le CRC correspondant.

En réalité le CRC a été initialement conçu pour la détection d'erreurs et non des tests d'intégrité. Ces derniers reposent sur des fonctions de hachage cryptographiques. Elles sont construites pour récupérer pour satisfaire certaines propriétés, par exemple : impossibilité de reconstruire le haché lorsqu'on modifie le message. Pour cela, les fonctions sont généralement non linéaires, ce qui n'est pas le cas du CRC. On verra que cela ne sera pas sans conséquence…

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.

3.2.5. La constitution du message final et son encapsulation:

Il a été mathématiquement démontré par Claude Shannon dans les années 40, qu'un chiffrement n'est fiable que si la longueur de la clé est au moins égale à celle du message à chiffrer.

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.

On définit une suite aléatoire comme étant une suite de variables aléatoires (Xi) de Bernoulli indépendantes et identiquement distribuées (i.e. P[Xi=1]= P[Xi=0]= 0.5 pour tout i)

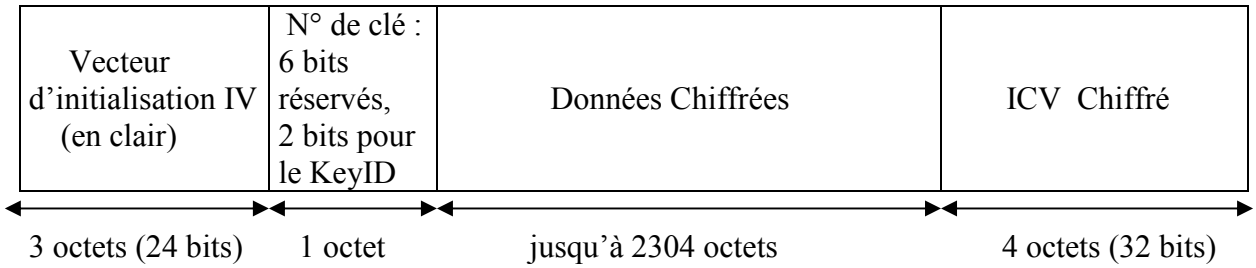
NB : On oppose le chiffrement par flux au chiffrement par blocs (DES, AES, Blowfish…). Le chiffrement par flux permet de traiter des données de n'importe quelle longueur sans rien découper.

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 :

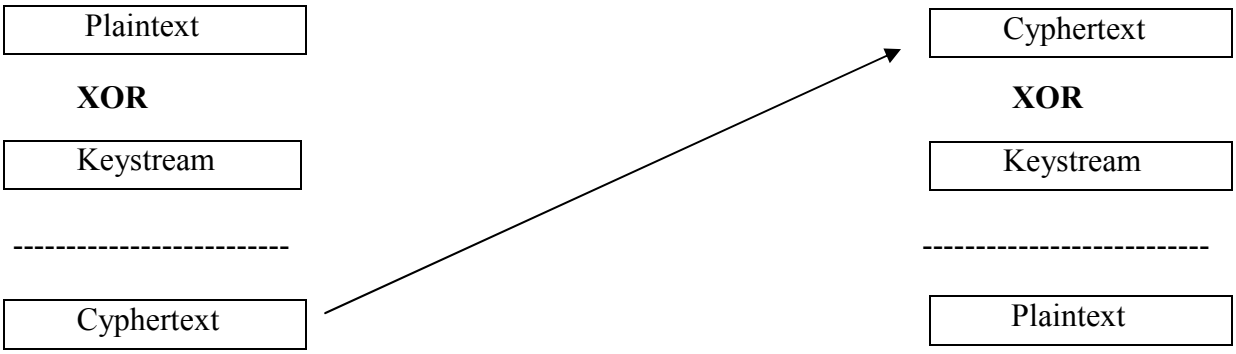
C= (M||ICV(M)) xor RC4(IV||K)

Encapsulation d'une trame chiffrée :



La trame envoyée contient un ***en-tête (MAC header)*** qui contient entre autres la nature de la trame et les adresses de la source et de la destination. La trame contient également l'IV (en clair),un certain nombre de bits réservés, l'identifiant de la clé (KeyID), le message à chiffrer (***payload*** ou ***charge***) est lui contenue dans le ***corps de la trame (frame body)*** et l'ICV (mécanisme d'intégrité sur lequel nous reviendrons) tous deux chiffrées.

Opérations de chiffrement et de déchiffrement (schéma simplifié):



3.3. Le déchiffrement WEP:

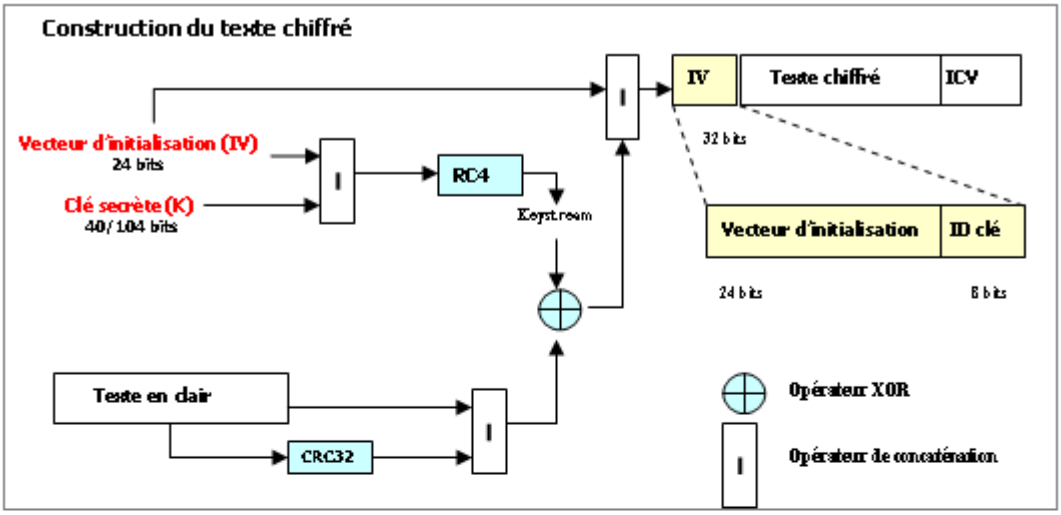
On détient dans la trame deux informations en clair : le KeyID et l'IV. On récupère la graine en concaténant la clé WEP indiquée par le Key ID avec l'IV qui se trouve en clair dans la trame. On peut retrouver alors le keystream utilisé pour le chiffrement.

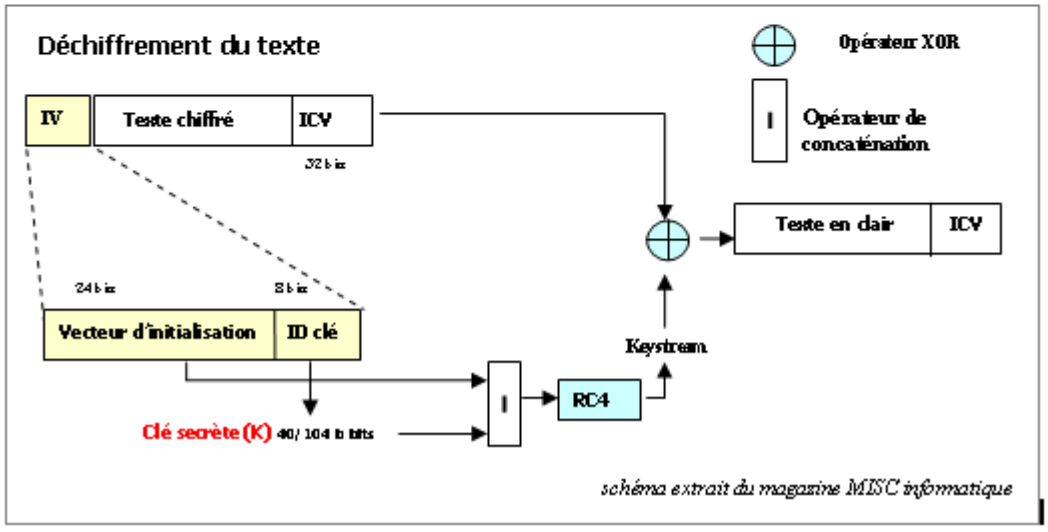
On opère un XOR entre le cryptogramme et le keystream et on récupère ainsi le payload et le CRC. Prenons un message chiffré C, un plaintext P et une graine G, on a :

C + RC4(G) = (P + RC4(G)) + RC4(G) = P

On applique alors l'algorithme de contrôle d'intégrité et on peut dès lors comparer les résultats. Si les résultats coïncident, la trame est acceptée, sinon elle est rejetée et supprimée. La probabilité qu'un contrôle d'intégrité se révèle positif alors que la clé utilisée serait invalide est considérée comme nulle.

Opérations de chiffrement et de déchiffrement (schéma complet):





3.4. La distribution des clés:

La clé WEP utilisée par le ***point d'accès (Access Point* – AP ou *carte de communication*)** et tous ses clients est généralement la même sur un WLAN donné. On parle de *Shared Key (clé partagée)*. Elle est statique contrairement à l'IV qui est incrémenté de manière régulière.Elle peut être saisie sous forme hexadécimale ou sous forme de caractères ASCII.

NB : Un caractère hexadécimal est codé sur 4 bits. Un caractère ASCII est codé sur un octet.

Certains AP permettent de saisir une ***phrase de passe (passphrase*)** qui initialisera un générateur avec une graine de 32 bits. A partir de là, le programme générera une ou plusieurs clés WEP en hexadécimal. Dans ce cas, il faut conserver une copie de la clé fabriquée puisque les procédés de génération de clé d'une marque à l'autre diffèrent. Toutefois, ces générateurs sont biaisés puisque la passphrase est composé uniquement de caractères tapés au clavier, c'est à dire de caractères ASCII dont le bit de poids fort sera toujours nul. Ainsi chaque octet de la graine appartient à l'ensemble {0x00, …, 0x7F} et non {0x00, …, 0xFF}. L'espace décrivant la graine du générateur aléatoire va donc de 00 :00 :00 :00 à 7F :7F :7F :7F . En fonction du générateur, d'autres attaques sont possibles.

L'utilisation d'une clé WEP de 104 bits est donc vivement recommandé. Da génération repose toujours sur une passphrase, mais cette fois, la fonction MD5 (Message Digest #5) est utilisée et seule les 104 premiers bits de la sortie sont conservés

Sinon, des freewares disponibles sur Internet permettent de générer une clé WEP. On citera par exemple: Wireless Key Generator.

Elle est stockée en clair sur un équipement mobile (fichier ou adaptateur suivant les constructeurs), donc exposé. Il est donc recommandé de modifier la clé WEP régulièrement. En effet, celle-ci peut-être retrouvée ou divulguée. Cela nécessite la ressaisie des informations sur toutes les entités qui communiquent en chiffré sur le WLAN. On spécifie alors dans la trame, le numéro de la clé utilisée. Ces manipulations sont d'autant recommandées (et contraignantes) que le réseau est de grande taille.

Certains constructeurs proposant d'introduire non pas une seule clé, mais plusieurs (4 dans le cas des clés 40 bits), en indiquant simplement l'index de la clé (KeyID) actuellement utilisée pour faciliter la gestion des clés. Autrement dit, l'administrateur pourra configurer les différents nœuds du réseau avec un ensemble de plusieurs clés en indiquant quelle est actuellement la clé utilisée. C'est un complément de protection que ne vaut que si la clé active est souvent changée, et de façon aléatoire, autant que possible. Mais cette procédure de changement de clé active reste manuelle et doit être exécutée sur tous les nœuds du réseau.

Il existe deux types de clé WEP. Lorsqu'une seule clé est employée, elle est dite commune et sert pour l'ensemble des communications au sein de l'infrastructure.

Une deuxième clé, qualifiée d'individuelle, peut être utilisée. Elle permet de minimiser l'emploi de la première dans les communications de type unicast, depuis les stations vers les AP.

Un équipement permet de stocker plusieurs clés. Une seule clé (par station) sert pour le chiffrement, on l'appelle la clé active. Les autres servent au déchiffrement des trames reçues. L'AP doit connaître toutes les clés actives si les stations n'emploient pas les mêmes.

Les trafics de type multicast ou broadcast sont généralement émis par les AP. Une clé commune doit dont être connue sur tous les équipements.

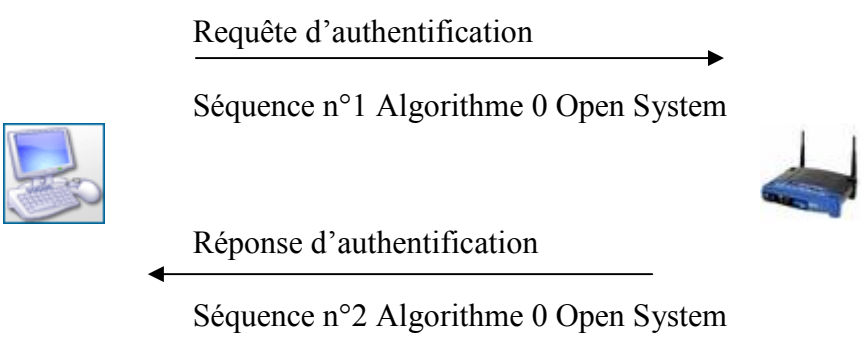
3.5. WEP et authentification:

Le WEP intervient dans deux solutions d'authentification offertes par la norme 802.11.

La première s'appelle ***Open System Authentification***. Elle est utilisée par défaut et se déroule en deux étapes. Un des parties envoie une trame dite de gestion, de sous-type authentification précisant le n° d'algorithme souhaité (ici ce sera 0). En retour, il lui est fourni une réponse positive ou négative dans une trame de même type. Cette méthode ne nécessite aucun pré-requis et peut-être considérée comme une authentification nulle. Elle est utilisée pour mettre en place des points d'accès publics

Si le WEP est utilisé, le corps de la trame est chiffré. Il est alors nécessaire que la clé utilisée par le AP et le client soit la même.

3.5.1. Processus d'authentification ouverte:

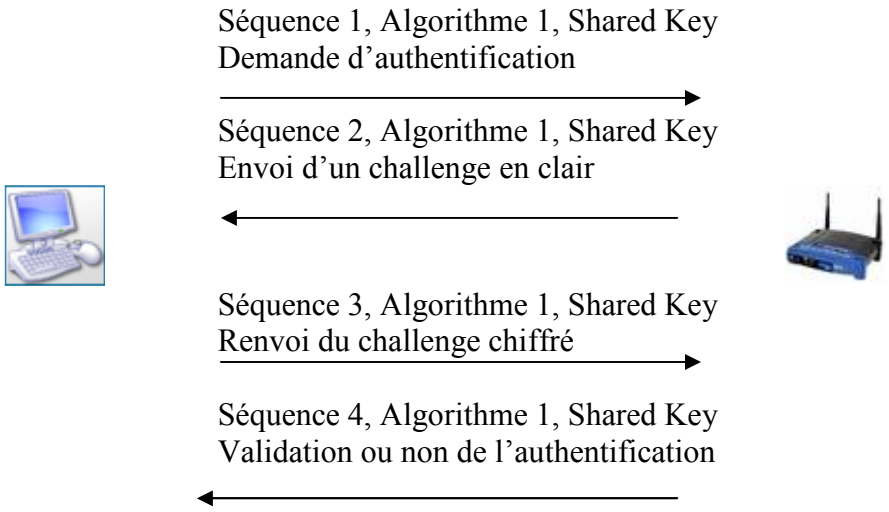


La seconde s'intitule ***Shared Key Authentification***. Elle nécessite la possession d'une clé de chiffrement partagée par les 2 entités. L'objectif est de vérifier que l'autre entité dispose la même clé de chiffrement. Aucun échange de clé n'a lieu durant le processus. Un programme nommé ***WEP Pseudo-Random Number Generation (PRNG)*** produit une suite de 128 octets aléatoires qui constitue ce que l'on appelle un ***texte de défi*** ou ***challenge*** .On s'assure alors que la station est capable de chiffrer la ***séquence de probation*** qui lui est

soumise. On se retrouve en fait dans ce que l'on appelle en cryptographie une situation de ***preuve à divulgation nulle de connaissance (ZKIP* pour *Zero Knowledge Interactive proof)***.

Le processus d'authentification (entre des entités A et B) se déroule alors en 4 étapes où 4 trames sont échangées. La 1ère trame indique le mode d'authentification souhaité par A. Dans le cas où B ne serait pas configuré pour ce mode, le processus s'arrête. Sinon B émet une seconde trame dans lequel se trouve le challenge en clair. A doit alors répondre en chiffrant le challenge avec sa clé WEP. B déchiffre la trame envoyée par A et compare le résultat avec le challenge. S'ils sont identiques, B confirme à A l'authentification dans une dernière trame.

3.5.2. Processus d'authentification à clé partagée:



4. LES FAILLES DU WEP :

Il existe mille manières d'aborder les failles du WEP, on a tenté ici de privilégier une approche à la fois historique (cf. la chronologie en annexe) et technique tout en essayant de rester le plus cohérent possible. On a ainsi répertorié de nombreuses méthodes pour mettre à mal le protocole WEP.

4.1. Premier aperçu des failles:

Un intrus qui dispose du SSID (identifiant réseau) et qui usurpe une des adresses MAC autorisées, ne pourra pas se connecter au réseau tant qu'il ne disposera pas de la clé WEP. Le pirate pourra la récupérer soit par ***Ingénierie Sociale* (*Social-Engineering*)** soit par cryptanalyse.

L'Ingénierie Sociale consiste à obtenir l'information par un membre quelconque de l'organisation, qui partage le secret. Elle peut également être volée… Nous ne nous étalerons pas davantage sur le sujet. Ce qui nous intéresse dans le cadre de ce travail, ce sont les faiblesses du point de vue cryptographique du protocole WEP.

Il y eut un temps où le protocole WEP fut considéré comme sûr. La diffusion dans le domaine public de l'algorithme RC4 a complètement modifié la donne.

En 1995, Wagner met en évidence les vulnérabilités du protocole RC4 sur le newsgroup sci.crypt. Il fallait alors 10 millions de paquets pour trouver la clé. Cela mettait beaucoup de temps à l'époque. En l'an 2000, plusieurs publications démontrent la faiblesse des clés WEP.

En 2005, une équipe du FBI des États-Unis d'Amérique fit la démonstration qu'il est possible de pénétrer un réseau protégé par du WEP en 3 minutes en utilisant des outils disponibles publiquement.

Depuis le 1er avril 2007, elles peuvent être retrouvées en une minute. Leur utilisation en entreprise est donc formellement déconseillée.

Le fait que le WLAN ne soit pas borné ''géographiquement'' rend aisé l'***intrusion*** d'une station. On appelle intrusion, l'insertion d'un nœud non autorisé au sein d'un réseau.

Les principales failles du WEP sont essentiellement les suivantes :

- Les algorithmes de vérification d'intégrité et d'authentification sont très facilement contournables.
- Possibilité de construire des dictionnaires fournissant en fonction d'un IV, le keystream.
- L'algorithme de chiffrement RC4 présente des clés faibles et l'espace disponible pour les IV est trop petit.
- Une même clé est utilisée pour tout le réseau et les clés de chiffrement sont statiques .
- Clés courtes 40 bits (5 caractères !!!) ou 104 bits et/ou trop simples (attaque par dictionnaire)
- Gestion des clés

4.2. Les faiblesses du IV:

4.2.1. Réutilisation du Keystream :

En 2001, Borisov, Goldberg et Wagner (Intercepting Mobile Communications : the insecurity of 802.11) montrèrent que les utilisateurs se servent parfois des mêmes keystreams du fait que la clé est statique.

En effet, le IV est sensé fournir une information aléatoire qui rend une clé unique dans le temps. Sa longueur de 24 bits, soit moins de 17 millions de combinaisons est trop courte. Le paradoxe des anniversaires nous dit qu'il y a une forte probabilité (50% pour 5000 trames, 99% pour 12000 trames) de trouver dans un nombre raisonnable de trames cryptées 2 trames cryptées ayant le même IV. Dans le même ordre d'idées, certaines implémentations initialisent le IV à zéro au redémarrage, ce qui facilite l'attaque sur les trames chiffrées avec le même IV. D'autres utilisent un générateur aléatoire pour constituer le IV.

Dans un réseau d'entreprise, 5 à 8 heures de trafic peuvent suffire à transmettre un tel nombre de trames. En effet pour un AP qui envoie des paquets de 1500 octets à un débit de 11 Mbps, le calcul est simple, il suffit approximativement de : ***1500*8/ (11*10^6)*2^{24} = 18000 secondes*** soit bien 5 heures en moyenne avant qu'un IV soit rejoué. L'information de chiffrement perd son caractère aléatoire et des cryptogrammes chiffrés avec une même clé circulent à intervalles réguliers. On parle alors de ***collisions***. Les collisions sont facilement détectables, étant donné que l'IV circule en clair.

Le principe employé afin de trouver la clé WEP, est basé sur l'analyse des trames chiffrées. Une écoute passive des communications permet de capturer les trames. On peut utiliser pour cela le logiciel KISMET (on appelle ce type de logiciel : un analyseur de protocoles) ou encore ETHEREAL, WIRESHARK. Lorsqu'on ***sniffe*** (écoute) le réseau, on doit mettre la carte Wi-Fi en mode ***monitor***, dans ce mode, la carte ne se comporte plus comme une interface réseau normal mais capture tout le trafic dans le voisinage. La phase d'écoute doit donc nous permettre de récupérer un nombre important de trames cryptées avec la même clé. Lorsqu'une collision survient, on obtient de l'information sur la différence entre les clairs. La connaissance de cette attaque permet des attaques statistiques qui donne accès au clair.

4.2.2. Attaque par clé apparentée:

Imaginons que pour une clé WEP K, nous avons deux messages clairs, M1 et M2, et leurs versions chiffrées C1 et C2. On a alors les identités suivantes :

M1 xor K= C1'
M2 xor K= C2'

On en déduit que:
M1 xor M2 = C1 xor C2

Cette donnée apporte des informations que l'on peut utiliser dans certains conditions. S'il l'on connaît l'un des deux textes en clair, par exemple, mais pas ce n'est pas là l'unique possibilité. En effet, il faut savoir qu'on connaît souvent le début des trames en clair car elles contiennent des informations redondantes (les adresses des stations qui communiquent notamment) la plupart du temps. On sait par exemple que la majorité du trafic d'un réseau Wi-Fi est constitué de trafic IP et à partir de cela, on en déduit ce que contiennent les headers des trames. On identifie par exemple les paquets ARP par leur taille et leur adresse de destination qui est l'adresse ***broadcast*** Ethernet (FF :FF :FF :FF). On connaît ensuite la structure et les valeurs courantes de certains champs des paquets ARP (8 octets d'en-tête LLC/SNAP, 8 octets d'en-tête ARP, 6 octets d'adresse MAC de la source). On parle d'***attaque par clé apparentée*** ou encore d'***attaque active des extrémités***. Le fait de disposer de toutes ces informations nous permet de retrouver avec une forte probabilité avec les premiers octets du keystream (22 pour un paquet ARP, 8 pour un paquet IP) et progressivement la clé WEP et ainsi de déchiffrer tous les autres messages chiffrés avec cette clé. Notre progression est liée, rappelons le, au nombre de trames capturées. Si on dispose de n messages chiffrés, on parle de ***problème de profondeur n***.

Il est important d'obtenir est l'adresse IP de destination. L'attaquant va alors pouvoir modifier les bits appropriés pour changer l'adresse de destination et envoyer le paquet vers un ***hôte (*****une *station*****)*** sous son contrôle. Si l'installation dispose d'une connexion Internet, l'AP

va déchiffrer le contenu des paquets pour les envoyer à la passerelle reliée à Internet, qui à son tour les renverra vers l'attaquant. Cela s'appelle l'***IP Redirection (*ou *IP Forwarding)***.En modifiant le message, on change également le ***contrôle d'intégrité (contrôle de conformité*)**. Pour que la trame forgée soit valide, on peut utiliser les propriétés du CRC (détaillées plus loin), des attaques statistiques ou alors compenser la modification du champ de l'adresse de destination (par exemple avec l'IP source) de manière à ce que le CRC reste identique.

Il existe une autre méthode appelée ***attaque avec test de validité* (*Reaction Attack* ou *attaque par réaction)*** qui utilise l'AP pour déchiffrer la trame. Contrairement à l'IP Redirection, elle fonctionne même si le réseau n'est pas relié à Internet. En revanche, elle ne déchiffre que le trafic TCP/IP. Elle consiste à forger des messages et à tester les réactions du destinataire selon qu'il l'accepte en renvoyant un ***accusé de réception (ACK* pour *acknowledgement*)** ou non, en la rejetant. Le destinataire est qualifiée d'***oracle***. Selon la réaction (qui dépend de la validité du TCP Checksum), on peut déduire des octets du plaintext.

4.2.3. Attaques FMS :

En 2001, une attaque passive sur les IVs est publié par Scott FLURHER, Itsik MANTIN, Adi Shamir (le S de RSA). Son nom correspond d'ailleurs à leurs initiales : FMS. Cette attaque exploite le fait que l'algorithme RC4 présente des IVs dits ***faibles*** (ou encore ***favorables***) qui permettent de prédire avec une probabilité raisonnable de nombreux bits dans la table d'état S. Cette attaque est connue sous le nom de «invariance weakness». Il faut donc identifier les circonstances dans lesquelles des IVs faibles peuvent apparaître et éviter de les utiliser.

La deuxième attaque de Fluhrer, Mantin et Shamir est la «known IV attack ». 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. Pour cela, on travaille avec un IV faible. Chaque IV faible fournit une information sur le premier octet. Il faut correctement deviner chaque octet avant de pouvoir déterminer le suivant. Cela est dû à la nature des deux modules de RC4 : KSA et PRGA. La détermination de chaque octet à partir d'un seul IV favorable est statistique et donne une probabilité de succès de 5%. En cas de succès, on parle de ***cas résolu***. C'est pourquoi l'on cherche à capturer un maximum de trame avec des IVs faibles.

Toutefois cette attaque théorique n'avait pas été testée par ses auteurs. La validité de cette attaque a été montrée par un étudiant américain, Adam Stubblefield, associé à deux spécialistes de la sécurité des laboratoires d'AT&T, John Ionnadis et Aviel Rubin. Leur principale difficulté a été de deviner le premier octet des données brutes. Malgré les différents types de protocoles utilisés (notamment ARP et IP), il s'est avéré que 802.11 rajoute une couche supplémentaire en encapsulant tous ses paquets (header SNAP). Ainsi, tous les

paquets capturés commençaient par le même octet 0xAA. Selon les auteurs, 256 cas «résolus» suffisent pour retrouver l'intégralité de la clé de 128 bits.

Peu de temps après, des développeurs ont mis à disposition sur Internet les logiciels WEPCRACK et AIRSNORT capables de casser une clé WEP selon la technique FMS.

4.2.4. Optimisation de FMS:

Récupérer l'échantillon représentatif peut prendre un "certain temps", qui dépend principalement du trafic généré sur le réseau. La technique étant ***passive***, si le réseau est peu utilisé (cas par exemple d'un réseau sans fil personnel, qui ne sert qu'à partager une connexion Internet pour deux ou trois clients), l'opération peut durer plusieurs semaines. L'expérience a montré que cette seule attaque nécessite la capture d'entre 5 et 6 millions de trames pour retrouver la clé. En 2002, ce nombre fut réduit à 1 million par David Hulton (h1kari) qui ne prit pas en considération uniquement le 1er octet du keystream mais aussi les suivants.

Afin d'accélérer la recherche, des outils apparaissent, permettant la réinjection des paquets capturés, pour augmenter artificiellement le trafic et ainsi diminuer le temps pour casser la clé WEP. L'attaque devient alors ***active*** puisqu'on modifie le trafic sur le WLAN. Elle devient donc aussi plus facilement repérable pour l'administrateur.

Les constructeurs ont alors pensé à intégrer directement sur leurs nouveaux ***firmwares*** des mécanismes pour détecter les clés faibles et ne pas les utiliser. Airsnort devint dès lors inutilisable.

Le 8 août 2004, Korek, un hacker, diffuse sur le forum de Netstumbler l'outil CHOPPER (celui-ci n'est plus disponible) qui permet de casser la clé WEP, en capturant un nombre réduit d'IVs, faibles ou non. Il suffit d'environ 150000 trames pour retrouver une clé de 64 bits et de 500000 pour une clé de 128 bits. Il s'agit d'une attaque par cryptanalyse statistique des données chiffrées.

Des développeurs entreprirent de continuer le travail de Korek. Rapidement, la suite AIRCRACK (développé par le Français Christophe Devine) apparaît, combinant l'attaque FMS et celle de Korek. Il est le premier d'une longue série de logiciels (on peut citer WepLab, Aircrack-ng) démontrant les failles dues aux collisions des IVs.
Une dizaine de minutes suffisent alors pour retrouver une clé WEP par ces moyens.

La suite d'outils Aircrack est constituée de 3 outils principaux :

- Airodump (équivalent de Kismet) qui collecte les trames sur le WLAN.
- Aircrack qui casse les clés WEP.
- Aireplay qui génère du trafic artificiel afin de diminuer le temps de collecte des trames chiffrées avec un même IV.

Aireplay exécute une attaque par rejeu, il essaie d'identifier les requêtes ARP (Adress Resolution Protocol) et les renvoie tels quels sur le réseau. Les autres clients répondront, générant ainsi du trafic.

Une fois que les trames sont collectées, la clé WEP est déterminée en quelques secondes. Le seul paramètre sur lequel il est nécessaire de travailler est le ***fudge factor*** qui détermine l'espace de recherche des clés.

Aircrack permet un autre type d'attaque. Autre création de Korek, elle s'appelle CHOPCHOP. Elle permet de décrypter un paquet chiffré avec le protocole WEP sans avoir connaissance de la clé. Le contrôle d'intégrité implémenté dans le protocole WEP permet à un attaquant de modifier à la fois le contenu chiffré du paquet et le CRC correspondant. On le verra plus en détail, plus loin. De plus, l'utilisation de l'opérateur XOR au sein du protocole WEP implique qu'un octet dans le message chiffré dépend toujours du même octet du texte en clair. En coupant le message chiffré de son dernier octet, le message devient corrompu mais il est possible de faire un choix sur la valeur de l'octet correspondant du texte en clair et de corriger le texte chiffré. On construit donc 256 trames modifiées, une pour chaque valeur possible de l'octet, et on les soumet à l'AP pour voir s'il les relaie ou non. Si c'est le cas, on a la bonne valeur, sinon la trame sera supprimée. On transforme donc l'AP en oracle. En répétant l'attaque sur tous les octets du message chiffré, il est possible de décrypter l'intégralité du paquet et de retrouver le keystream. Il est important de noter que l'incrémentation de l'IV n'est pas obligatoire dans le protocole WEP, il est donc possible de réutiliser le keystream pour forger d'autres paquets (en ré-utilisant le même IV).

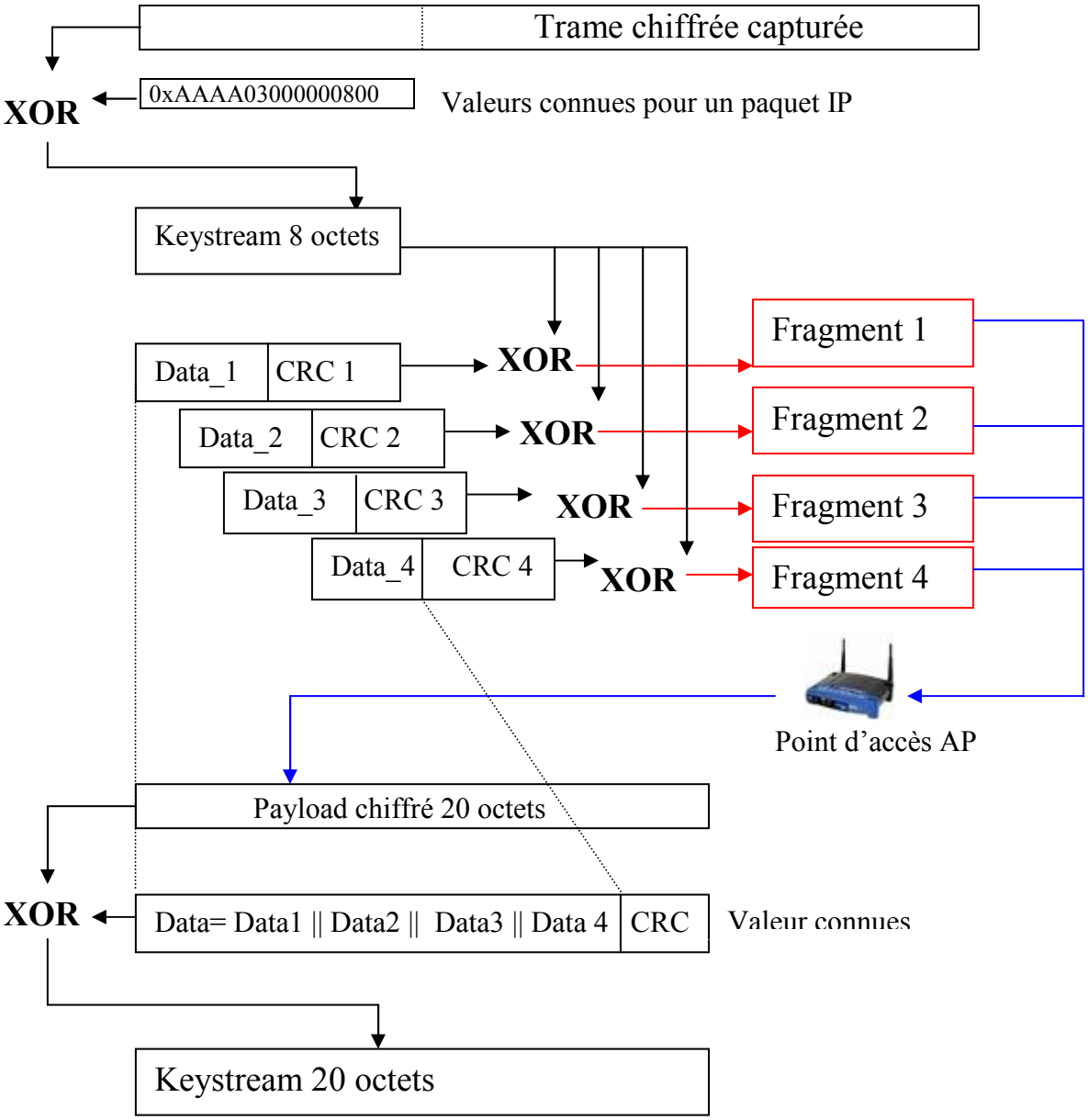
4.2.5. Attaque par fragmentation:

En 2004, encore, dans un contexte où le WEP prédomine toujours (et ce malgré sa vulnérabilité), Andrea BITTAU, Mark HANDLEY du collège of London et Joshua LACKEY de chez Microsoft publièrent un article (The Final Nail in WEP's Coffin – Le clou final au cercueil du WEP) sur une nouvelle attaque : ***l'attaque par fragmentation*** qui se base sur la réutilisation des keystreams. L'attaque a été implémentée sur le logiciel Wesside disponible à l'origine uniquement sur l'OS FreeBSD. On a vu que l'on pouvait par ***attaque à clés apparentées*** récupérer des keystreams de 8 ou 22 octets. Cela permet de chiffrer des messages très courts. En soit ce n'est pas très intéressant, il nous faudrait des keystreams ayant la taille maximum d'une trame (***MTU* ou *maximum transmission unit***). Le standard 802.11 prévoit un mécanisme qui permet de fragmenter une trame en 16 fragments au plus, chiffrés indépendamment les uns des autres (chacune a donc un CRC distinct). On peut dès lors augmenter la portée du keystream. Prenons un keystream de 22 octets. On chiffre 16 fragments avec ces 22 octets. A chaque fois, 4 octets sont réservés pour le CRC32, on chiffre donc de manière effective (22-4)*16=288 octets de données avec seulement 22 octets de keystream. Mieux encore, lorsqu'un AP reçoit une trame 802.11 fragmentée qu'il doit relayer, il la défragmente (il déchiffre chaque fragment et rassemble tout en une trame). On se retrouve alors en situation de clair connu et on peut de cette manière récupérer un keystream plus long.

En itérant ce processus, on récupère un keystream qui permet de chiffrer n'importe quelle trame (et de déchiffrer toutes celles associés au IV). On appelle cette phase : ***« le bootstrap »***, elle dure environ 30 secondes. De manière générale, si on dispose d'un keystream de N octets de X fragments, on obtient un keystream de longueur L=(N-4)*X+4.

Dans le schéma qui suit, on a pris un exemple simplifié où à partir de 8 octets de keystream et 4 fragments, on récupère un keystream de 20 octets.

Augmentation du keystream par fragmentation :



Il existe plusieurs façons d'exploiter cette attaque :

- On peut dans un premier temps faire du ***mapping*** (dresser une carte du plan d'adressage et l'adresse de passerelle) du réseau. Pour cela, il nous suffit d'émettre des requêtes ARP, cela prend environ 5 minutes. On pourra alors émettre des requêtes vers Internet et faire de l'IP Forwarding (vu précédemment).
- On peut générer du trafic avec n'importe quel paquet IP (contrairement à Aireplay qui nécessite des paquets ARP) et le fournir à Aircrack. Cette méthode est implémentée dans Aircrack-ng.
- On peut constituer une table IV/Keystream (la clé étant statique) qui permettra de chiffrer de déchiffrer n'importe quel message. La taille de cette table de keystream devrait être de 25 Gigaoctets . Cela prend 17 heures alors qu'Aircrack permet de casser la clé WEP en quelques minutes. L'attaque par fragmentation n'est donc pas une révolution mais une nouvelle faiblesse WEP.

Une autre méthode pour l'attaquant de constituer une table de décryptage est d'envoyer un message de type « ping » en clair, l'attaquant peut voir comment celui est chiffré. En confrontant les 2 versions, il obtient le keystream. Il suffit alors d'associer chaque keystream avec chaque IV.

4.3. Les problèmes des clés de chiffrement:

L'IV présente une telle faille que la quasi-totalité des attaques le sollicitent.

La première des faiblesses de la clé WEP reste son caractère statique. Il est très facile de la compromettre, puisqu'elle est présente sur de nombreux postes de travail ainsi que sur tous les points d'accès. De plus, il s'avère souvent que de nombreux utilisateurs la connaissent.

Certains clés choisies sont très simples. Les attaques par dictionnaire peuvent, comme pour les mots de passe, retrouver l'information. Des outils comme WepLab et WepAttack proposent ce type d'attaque. WepLab propose une attaque par dictionnaire fondée sur les techniques courantes de hash MD5 employées par les AP pour passer d'une passphrase une clé WEP hexadécimale. WepAttack se base quant à lui sur les clés WEP ASCII. On peut les combiner à un outil appelé John The Ripper qui augmentera la taille du dictionnaire.

La connaissance d'une trame cryptée C avec une graine G et de sa version en clair M (attaque à texte clair connu) permet de construire le keystream pour un IV donné.

$M + C = M + (M + RC4(G)) = RC4(G)$

Il est alors possible d'injecter dans le trafic un nouveau message valide (utilisant le même IV) sans avoir d'information sur la clé K. Mieux encore, dans le WEP, on peut également retrouver la clé K initiale à partir du keystream (on ne peut pas avec SSL). Il est donc facile de déduire le keystream pour un autre IV en exploitant les identités suivantes :
On notera la clé WEP K, les vecteurs d'initialisation IV_1 et IV_2, l'opérateur OU exclusif + et l'opérateur de concaténation ||.

$X = IV_1||K$
$Y = IV_2||K$
$RC4(Y) = RC4(X) + X + Y$

La connaissance d'un keystream permet, on le voit, de retrouver aisément le keystream pour un autre IV sans pour autant avoir à connaître/calculer la clé K. En effet K+K s'annule.

4.4. L'exploitation du contrôle d'intégrité:

Le calcul du type CRC, utilisé par Integrity Check Value (ICV) ne devrait servir qu'à vérifier si la trame reçue n'a pas été altérée lors de la communication. Une telle technique est en fait facile à contourner du fait des propriétés du CRC.

L'algorithme de contrôle d'intégrité ICV est linéaire. Supposons que nous disposions par eavesdropping d'une trame chiffrée valide RC4(K) + X||CRC(X), le payload étant noté X et la clé K. Si nous modifions une partie de cette trame (appelons cette modification Y), il nous suffit (du fait des propriétés du CRC) de calculer le champ ICV correspondant aux modifications : CRC (Y) et de l'ajouter au champ ICV initiale pour obtenir une trame forgée valide. On peut donc modifier le contenu d'une trame capturée puis la réinjecter dans le trafic, de manière transparente. La modification de certains bits s'appelle le ***bit flipping***. On peut ainsi faire une ***attaque par mascarade*** ou ***spoofing (usurpation d'identité)***.

On notera + plutôt que XOR (rappelons que XOR est l'addition modulo 2).

La propriété de linéarité s'écrit : $CRC(X+Y) = CRC(X)+CRC(Y)$.
Et voilà, la faille qui en découle :

$$\begin{aligned}\text{trame forgée} &= RC4(K) + (X+Y||CRC(X+Y)) \\ &= RC4(K) + (X+Y||CRC(X)+CRC(Y)) \quad \text{(linéarité du CRC)} \\ &= RC4(K) + (X||CRC(X) + Y||CRC(Y)) \\ &= (RC4(K) + X||CRC(X))+ Y||CRC(Y) \\ &= \text{trame capturée} + \text{modification}||CRC(\text{modification})\end{aligned}$$

On peut remarquer que cette attaque ne nécessite même pas la connaissance du payload (i.e. du message en clair, rappelons le) correspondant à la trame capturée mais seulement de la modification apportée. Les paquets étant chiffrés, on peut penser que cette attaque ne sert à rien. On verra en fait que l'on peut se servir de cette faille lors de l'authentification.

Il existe une autre faille pour peu que l'on puisse écouter le trafic sur le réseau Ethernet derrière le AP, on a vu qu'il était facile de tromper le mécanisme de contrôle d'intégrité. Lorsque des trames forgées sont envoyées à un AP, ce dernier relaye ces trames déchiffrées sur le réseau Ethernet câblé. Il est alors facile de lancer une attaque de type texte à clair connu, puisque la version chiffrée d'un paquet et sa version en clair, espionnées sur le réseau Ethernet sont connues.

4.5. Les failles dans l'authentification:

La méthode ***Shared Key Authentification*** peut-être considérée comme moins sécurisée que l' ***Open System Authentification*** contrairement à ce que l'on pourrait penser.

Ce processus ne protège pas d'une attaque ***Man In the Middle (MiM).*** L'authentification étant unilatérale, la station n'a aucun moyen d'authentifier l'AP auquel elle s'associe. Si la station pirate est configurée comme AP (on parle d'***APs malicieux,*** de ***points d'accès voyous*** ou encore ***Rogue APs***) avec le même SSID (identifiant du réseau) que l'entreprise, elle peut intercepter le challenge. Celle-ci est ensuite prolongée jusqu'à la borne de l'entreprise qui authentifie le pirate. Le processus initial avec la station est interrompue, on parle de ***désassociation***. La station reprendra une recherche d'AP ce qui conduit à l'envoi d'un nouveau challenge et tout cela se passe de manière transparente pour l'utilisateur. Il est donc recommandé d'utiliser des méthodes d'authentifications plus solides. Un AP malicieux pourrait en outre transformer un client en oracle en lui fournissant des messages à chiffrer sous forme de challenge.

De plus, si l'on connaît la clé de chiffrement ou un dictionnaire des keystreams associés à cette clé l'authentification est immédiate à obtenir. Il y a là un défaut grossier de conception, authentification et chiffrement reposant sur la même protection.

Mais surtout, le transit du même message en clair et chiffré facilite le travail du cryptanalyste pour découvrir la clé WEP. On avait dit plus haut que le CRC interviendrait dans une faille lors de l'authentification. Il est temps d'en parler. Supposons que l'on dispose d'un message en clair X et de son cryptogramme RC4(X) + X||CRC(X) on se trouve donc dans une situation d'attaque à texte clair connu. On récupère aisément le keystream :

RC4(X) = (RC4(X) + X||CRC(X)) + X||CRC(X)

On fait alors une demande d'authentification auprès de l'AP, celui ci envoie le challenge Y. Il est à noter que les réponses d'authentification sont toutes de mêmes longueur (celles du keystream calculé). On peut donc dès lors chiffrer le challenge sans pour autant disposer de la clé K. On procède comme suit :

Y chiffré= RC4(K)+ Y||CRC(Y)
= RC4(K)+ Y||CRC(Y) + X||CRC(X) + X||CRC(X)
= (RC4(K) + X||CRC(X)) + Y||CRC(Y) + X||CRC(X)
= X en chiffré + challenge Y + X en clair

Cela fonctionne pour 2 raisons: le CRC ne dépend pas de la clé et surtout le fait que l'AP nous permettent de choisir l'IV. On prend évidemment le même IV (qui circule en clair, rappelons le) que celui de la trame capturée.

En revanche, l'attaquant ne peut pas communiquer sur le WLAN puisqu'il ne dispose pas de la clé WEP, il est seulement authentifié et associé sur ce WLAN.

Cependant, cette faille ne s'arrête pas là. La sortie RC4(IV||K) qu'il récupère est en effet longue de 140 octets, ce qui est largement suffisant pour chiffrer quelques requêtes, comme un requête ARP ou HTTP par exemple. L'attaquant est donc en mesure, à partir de l'observation d'une authentification, d'injecter des paquets cohérents dans le réseau. Il sera

également en mesure de déchiffrer les 144 premiers octets de tout paquet chiffré avec l'IV en question.

Il apparaît donc que WEP présentent plusieurs vulnérabilités, dont certaines sont structurelles. S'il est par exemple simple de modifier le générateur d'IV pour supprimer les clés faibles, les problèmes du mécanisme d'authentification, de l'utilisation du CRC32 ou encore les possibilités de rejeu/injection ne peuvent pas être corrigées sans modifier le protocole lui-même.

5. LES NOUVELLES PARADES :

Le protocole WEP ne peut raisonnablement être utilisé que dans des cas très limitatifs et avec de fortes contraintes administratives :

- L'intrusion du réseau ne doit présenter que peu d'intérêt, c'est un élément important qui détermine la motivation de l'intrus. Le réseau domestique ne sera probablement pas la proie la plus intéressante, ce qui sera certainement moins vrai pour le réseau d'entreprise.
- Le trafic généré naturellement doit être le plus faible possible.
- L'administrateur doit surveiller avec attention le trafic sur le réseau.
- Il faudrait mettre à disposition les clés par moyens confidentiel (ex : en Intranet)
- La clé partagée doit être modifiée le plus souvent possible, puisque dans le pire des cas, on peut estimer que la durée de vie d'une clé à 64 bits n'est que d'environ une journée. Utilisez donc de préférence une clé 128 bits.
- Le nombre de nœuds doit être le plus faible possible (moins un secret est partagé, moins il risque de fuir).
- Il est recommandé d'associer des mécanismes complémentaires pour une sécurisation plus performante (IPSec, SSH,VPMN, SSL,…).

De nouvelles normes et de nouveaux protocoles sont en passe de supplanter le WEP et le 802.11b. Ils se développent progressivement et s'appellent : 802.1x, WPA et WPA2 (802.11i).

Ils ont pour vocation de corriger les erreurs commises par le passé en matière de sécurité.

On peut évoquer brièvement la norme IEEE 802.1x (***Port-Based Network Access Control*** - 2001) qui est une extension pour 802.11 et qui permet la fourniture de clé WEP par un serveur d'authentification (RADIUS). Cela évite de devoir paramétrer les clients et les AP. Elle utilise le protocole ***EAP (Extensible Authentication Protocol, RFC 2284)*** qui permet de distribuer des clés WEP en cours de session, autrement dit, la clé WEP devient dynamique alors qu'elle était à la base statique. On parle alors de *clés rotatives*. Une nouvelle clé WEP est générée pour chaque utilisateur et chaque session. En limitant la quantité de données chiffrées avec une même clé, la sécurité est quelque peu renforcée.

Le WPA (Wi-Fi Protected Access) est une version « allégée » du protocole 802.11i. Le WPA emploie des solutions techniques proches de WEP (il est basé sur RC4) mais sans les erreurs de conception de ce dernier. Le WPA permet de surcroît de conserver le matériel supportant WEP. En revanche, ce n'est pas le cas de WPA2 (802.11i).

Le 802.11i (2004) fournit plusieurs améliorations regroupées sous le terme de ***TKIP (Temporary Key Integrity Protocol)*** parmi lesquelles :

- ***MIC (Message Integrity Check* ou *Michael*)** basé sur SHA-1: Il s'agit d'une partie calculée pour chaque message et ajoutée à la fin de celui-ci afin de réduire la possibilité de construire/modifier des trames à partir d'informations dérivées du réseau.
- Utilisation d'un autre mécanisme d'authentification.
- Modification de la fonction permettant de dériver de la clé de chiffrement et du IV la graine pour l'algorithme RC4 permettant ainsi la lutte contre les clés faibles.
- Assignation d'une clé de chiffrement différente par station associée à un AP et modification régulière de cette clé de chiffrement
- L'augmentation de la taille de l'IV de 24 à 48 bits.
- Le WPA2 s'appuie sur AES en tant que primitive de cryptage plutôt que sur RC4.
- L'IV ne peut plus reprendre une ancienne valeur si la clé n'est pas changée.
- L'IV n'est pas envoyé en clair comme pour le WEP mais haché.
- etc.…

On constate en lisant cette liste les lacunes initiales du protocole WEP.

On peut schématiser la progression de la sécurité Wi-Fi comme suit :

Aucune Protection➔WEP➔802.1x➔WPA➔802.11i (WPA2)

6. CONCLUSION:

Le WEP avait à sa création pour but avoué (prétention) de proposer une solution de confidentialité équivalente au réseau filaire en s'appuyant uniquement sur un algorithme réputé sûr: RC4. A partir de cette certitude infondée, la simplicité d'utilisation a alors été privilégiée pour promouvoir le développement de ce protocole. Cette « négligence » de la sécurité n'a pas été sans conséquence. Sa conception n'a - on l'a constaté- pas été exempte de failles.

Le développement exponentiel de l'Internet a chamboulé les donnes du point de vue de la sécurité des réseaux. La découverte constante, au cours de ces dernières années, de ces nombreuses failles devrait mettre un terme à l'utilisation du protocole WEP qui est tout bonnement à proscrire en entreprise et à utiliser avec parcimonie en environnement domestique. C'est pour cela qu'il est progressivement remplacé par des solutions plus performantes telles que WPA et WPA2.

Le WEP nous prouve que la sécurité cryptographique d'un protocole ne repose pas que sur un algorithme réputé fort mais aussi sur son implémentation. Le WEP nous rappelle ainsi un principe fondamental : « La solidité d'une chaîne est celle de son maillon le plus faible ».

Le WEP est – on l'a bien compris - devenu obsolète; cependant, pour prendre une autre métaphore, rappelons que : « Mieux vaut une serrure en mauvais état que pas de serrure du tout ».

Les attaques sur le WEP sont pour la plupart connues depuis longtemps mais appliquées à d'autres protocoles. Autrement dit, on a répété des erreurs déjà commises par le passé. La mise en œuvre d'un protocole cryptographique nécessite donc la présence d'experts en la matière, chose qui a cruellement manqué au WEP. Fort des erreurs du passé, la sécurité devrait ainsi être privilégiée à l'avenir.

7. ANNEXES:

7.1. Bibliographie:

- 802 .11 et les réseaux sans fil – Paul MUHLETHALER
- Wi-Fi Réseaux sans fils 802.11 – Philippe ATELIN
- Wi-Fi Maîtriser le réseau sans-fil – Alexandre CHAUVIN-HAMEAU

7.2. Publications:

- Intercepting Mobile Communications : The Insecurity of 802.11 - Nikita BORISOV, David WAGNER, Ian Goldberg (2001)
- The Final Nail in Wep's Coffin – Andrea BITTAU, Mark HANDLEY, Joshua LACKEY (2004)
- Revues sur la sécurité informatique : MISC

7.3. Liens:

1. http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html
2. http://users.info.unicaen.fr/~fsy/reseau/wep.html
3. http://www.uqtr.ca/~delisle/Crypto/
4. http://www.cs.berkeley.edu/~daw/my-posts/my-rc4-weak-keys
5. http://www.securityfocus.com/infocus/1814
6. http://www.securityfocus.com/infocus/1824
7. http://wiki.caensansfil.org/index.php/La_s%C3%A9curit%C3%A9
8. http://fr.wikipedia.org/wiki/Wep
9. http://www.commentcamarche.net/wifi/wifi-wep.php3
10. http://www.lapagedujour.com/articles/hack-cle-wep.html
11. http://ethneo.free.fr/casser_cle_wep.php

7.4. Chronologie du protocole WEP:

Date	Description
Septembre 1995	Vulnérabilité potentielle dans RC4 (Wagner)
Octobre 2000	Premières publications sur les faiblesses du WEP : *Unsafe at any key size,…*
Juillet 2001	Attaque bit flipping sur le CRC- *Intercepting Mobile Communications : The Insecurity of 802.11* (Borisov, Goldberg, Wagner)
Août 2001	Attaques FMS – *Weaknesses in the Key Scheduling Algorithm of RC4* (Fluhrer, Martin, Shamir)
Août 2001	Sortie du logiciel Airsnort
Février 2002	Optimisation de l'attaque FMS par David Hulton (h1kari)
Août 2004	Attaque de KoreK (IVs uniques) – sortie de chopchop et chopper
Juillet/août 2004	Sortie de la suite Aircrack (Devine) et WepLab implémentant l'attaque de KoreK
2004	Attaque par fragmentation (Bittau, Handley, Lackey) – The Final Nail in WEP's coffin
Avril 2005	Démonstration de cassage d'une clé WEP (128 bits) en 3 minutes par le FBI.
1er Avril 2007	Sortie de Aircrack-ptw qui permet de casser une clé WEP en 1 minute!

7.5. Glossaire:

Ad-hoc :
Groupe de périphériques sans fil qui communiquent directement entre eux (d'égal à égal) sans utiliser de point d'accès.

Attaque : opération qui tente de violer les *objectifs de sécurité* d'un *cryptosystème* .

Authentification : preuve d'identité ou preuve de l'origine des données. Ce terme regroupe l'*identification* , les *signatures* et les *MAC* .

Broadcast : Terme anglais (en français on utilise le terme **diffusion**) définissant une diffusion de données depuis une source unique à un ensemble de récepteurs

Cassage (total) : calcul de la *clé secrète* d'un utilisateur.

Checksum (Somme de contrôle): Mot contenant une valeur calculée à partir des bits d'un message ou d'un bloc pour détecter les erreurs de transmission.

Chiffrement : Technique permettant de rendre illisible tout message à un tiers qui ne possède pas la clé de codage. Le chiffrement n'est pas un service de sécurité, c'est une technique qui sert à mettre en place les services de sécurité. Il peut être déterministe ou probabiliste.

Clé : valeur qui paramètre un *cryptosystème* . Si elle est confidentielle, on parle alors de clé secrète ou privée, sinon on parle de clé publique.

Client/serveur :
La formule « client/serveur » décrit la relation entre deux programmes informatiques, telle que l'un d'eux, le client, envoie une demande de service à l'autre, le serveur, qui répond à cette demande.

Confidentialité : Prévention d'une divulgation non autorisée de l'information (définition Itsec). Propriété qui assure que seuls les utilisateurs habilités ont accès aux informations.

Contrefaçon : fabrication d'un objet sans en avoir le pouvoir légitime (connaissance de la *clé secrète*). Contrefaire une *signature* ou un *MAC* .

Contrôle d'accès : service consistant à contrôler l'accès d'utilisateurs identifiées à des applications

CRC (Cyclic Redundancy Check): Mécanisme de contrôle appliqué régulièrement à des blocs fixes de données dans une communication. Le "mot" de contrôle (ou le CRC) est ajouté à la fin de chaque bloc et permet au récepteur de constater que le bloc a été corrigée.

Cryptanalyse : étude des procédés de *décryptage* , ou plus généralement de la sécurité des *cryptosystèmes* .

Cryptographie : étude des procédés permettant d'assurer la *confidentialité* , l'*intégrité* et l'*authentification* .

Cryptosystème (mécanisme cryptographique) : *système de chiffrement* et plus généralement tout *schéma de signature* , de *MAC* ou de *générateur pseudo-aléatoire* .

Déchiffrement : transformation inverse du *chiffrement* qui consiste à retrouver, à l'aide d'une *clé secrète* , l'information initiale contenue dans le message chiffré.

Décryptage : action de « casser » le *chiffrement* , et donc de retrouver le texte clair d'un chiffré, sans connaître la *clé secrète* .

Fonction à sens unique : fonction simple à calculer mais difficile à inverser.

Fonction à sens unique à trappe : *fonction à sens unique* pour laquelle une information supplémentaire, appelée « trappe », facilite l'inversion.

Fonction de hachage : transformation déterministe d'une chaîne de bits de taille variable en une chaîne de bits de taille fixe, telle que toute modification de la valeur d'entrée modifie la valeur de sortie.

Fragmentation
Scission en paquets d'unités plus petites lors de la transmission sur un support réseau qui n'est pas en mesure de prendre en charge la taille initiale du paquet.

Frame (Trame): Suite définie d'informations constituant une entité logique de base pour la transmission dans un réseau. Une trame comporte les informations à transmettre proprement dites et des informations de contrôle qui les précèdent et les suivent.

Générateur pseudo-aléatoire : transformation déterministe permettant de produire une chaîne de bits apparaissant aléatoire à partir d'une entrée de petite taille.

Hot Spot (ou point d'accès public)
Site d'où il est possible d'accéder à Internet avec des périphériques compatibles Wi-Fi tels que des ordinateurs portables ou des PDA. L'accès peut être gratuit ou payant. On trouve généralement des points d'accès dans les cybercafés, les aéroports, les gares, les stations d'essence et d'autres lieux publics.

Hub : Equipement matériel permettant l'interconnexion réseau de plusieurs machines. Le mot Hub, qui veut dire moyeu, provient de la représentation en étoile que l'on fait de cette interconnexion.

Identification : preuve d'identité lors d'un contrôle d'accès.

IEEE (Institute of Electrical and Electronics Engineers, institut des ingénieurs électriques et électroniciens)
Institut indépendant qui développe des normes de mise en réseau.

IEEE 802.11 : Est un standard international décrivant les caractéristiques d'un réseau local sans fil (*WLAN*)

IEEE 802.11i : est un complément à la couche réseau (normes 802.11b ou g); elle a été homologuée de 24 juin 2004. Elle repose sur le standard de chiffrement AES (Advanced Encryption Standart) en reprenant les principes de gestion des clés du WPA. L'AES prévoit des clés de 128, 192 et 256 bits. L'AES fonctionne au-dessus du WEP, qui ne disparaît pas.

IEEE 802.1x : Normalisation d'authentification. Pendant la phase d'authentification, la station ne peut accéder qu'au serveur d'authentification (serveur Radius par exemple). Une fois l'authentification acceptée, les communications vers le réseau sont permises en fonction des accès accordés. Chaque client a une clé spécifique, les clés peuvent être renouvelées.

Infrastructure
Matériel informatique et de mise en réseau actuellement installé.

Intégrité : Prévention d'une modification non autorisée de l'information (définition Itsec). Propriété qui garantit la présence et la conservation sans altération d'une information ou d'un processus.

IP Spoofing : Usurpation d'adresse IP. Technique utilisée afin de tenter d'obtenir un accès non autorisé sur une machine. L'intrus envoit des messages à un ordinateur cible en utilisant une adresse IP semblant indiquer que le message provient d'une machine de confiance.

LAN (réseau local)
Ordinateurs et produits de mise en réseau qui constituent le réseau à votre domicile ou votre bureau.

MAC : donnée de taille fixe jointe à un message qui prouve l'identité de l'émetteur et qui garantit l'*intégrité* du message. Contrairement aux *signatures* , seules les personnes possédant la *clé secrète* peuvent vérifier un MAC.

Mode Infrastructure
Configuration dans laquelle un pont est établi entre un réseau sans fil et un réseau câblé via un point d'accès.

Objectifs de sécurité : les services assurés par les *systèmes cryptographiques* sont la *confidentialité* , l'*intégrité* et l'*authentification* .

Paquets
Petit bloc de données transmis dans un réseau d'échange de paquets.

Passerelle
Point de réseau faisant office d'entrée sur un autre réseau.

Payload : Partie utile d'un message, par opposition à la partie servant pour assurer la transmission.

Point d'accès
Périphérique qui émet et reçoit des données sur un réseau local sans fil (WLAN). également appelé « station de base » ou « concentrateur sans fil », il connecte les utilisateurs au sein du réseau local et peut servir de point d'interconnexion entre le WLAN et un réseau câblé fixe (Ethernet).

Point d'accès pirate
Point d'accès non autorisé installé sur le réseau local sans fil d'une entreprise, généralement par un utilisateur. Les points d'accès pirates posent un risque de sécurité car ils respectent rarement les politiques de sécurité de la société et n'ont, dans la plupart des cas, aucun mécanisme de sécurité activé. Ils forment une interface ouverte non sécurisée avec le réseau de l'entreprise.

Primitive : opération mathématique de base à partir de laquelle des *cryptosystèmes* pourront être construits. Par exemple, la primitive de chiffrement RSA consiste à calculer $c = me \mod N$ où $pk = (e , N)$ est la *clé publique* .

Protocole : ensemble de messages échangés entre plusieurs entités.

RADIUS (Remote Authentication Dial-In User Service)
Protocole qui utilise un serveur d'authentification pour contrôler l'accès au réseau.

RC4 : 'Rivest Cypher 4' ou ‘Ron’s Code #4’. Algorithme à clé symétriques de longueur variable (de 1 à 256 octets). Cependant la clée a souvent une longueur fixe de 40 bits.

Réseau
Série d'ordinateurs ou de périphériques connectés dans le but de partager des données, de les stocker et/ou de les transmettre entre utilisateurs.

Routeur
Désigne un équipement qui assure la fonction d'acheminement (routage) d'une communication à travers un réseau (niveau 3 du modèle OSI). Périphérique de mise en réseau qui connecte plusieurs réseaux ensemble, comme un réseau local et Internet.

Scellement : Méthode par laquelle l'intégrité de données peut être prouvée grâce à un «sceau» (parfois appelé «empreinte numérique») qui permet de détecter toute modification.

Serveur : Tout ordinateur dont la fonction dans un réseau consiste notamment à permettre à l'utilisateur d'accéder aux fichiers, d'imprimer et de communiquer.

Système (ou schéma) : ensemble d'opérations reliées combinant une ou plusieurs *primitives* entre elles avec d'autres techniques afin d'augmenter la sécurité et éventuellement traiter des messages de taille variable. Le système de chiffrement RSA consiste à rajouter un *padding* puis à utiliser la primitive de chiffrement RSA. Il est d'usage de parler de *schéma de signature* et de *système de chiffrement* .

Signature : donnée de taille fixe jointe à un message et qui prouve l'identité de l'émetteur, garantit l'*intégrité* du message et assure la non-répudiation. Tout le monde ayant accès à la *clé publique* peut vérifier la signature

Sniffing : attaque passive qui consiste à analyser le trafic réseau. Lorsque deux ordinateurs communiquent entre eux, il y a un échange d'informations (trafic). Mais, il est toujours possible qu'une personne malveillante récupère ce trafic. Elle peut alors l'analyser et y trouver des informations sensibles

SSID (Service Set Identifier, identificateur de jeu de service)
Nom permettant d’identifier un réseau sans fil. L’identifiant SSID est une entrée alphanumérique de 32 caractères maximum. L’identifiant SSID est également appelé nom réseau, réseau préféré, ESSID ou zone de service de réseau local sans fil.

TCP/IP (Transmission Control Protocol/Internet Protocol)
Protocole réseau de transmission de données qui exige un accusé de réception du destinataire des données envoyées.

TKIP : "Temporal Key Integrity Protocol" Protocole permettant le chiffrement et le contrôle d'intégrité des données par un renouvellement automatique des clefs de chiffrement. Il est compatible avec WEP.

War Chalking
Activité consistant à tracer des marques à la craie sur des surfaces extérieures (murs, sols, immeubles, arbres) pour indiquer la présence d'une connexion sans fil offrant un accès gratuit à Internet. Le symbole à la craie représente le type de point d'accès disponible à cet emplacement : deux demi-cercles dos à dos désignent un nœud ouvert, un cercle fermé indique un nœud fermé, un cercle fermé avec un « W » à l'intérieur signale un nœud équipé du protocole WEP.

War Driving
Activité consistant à se déplacer à l'aide d'un système GPS et d'un portable équipé d'un adaptateur sans fil et/ou d'une antenne pour repérer les réseaux locaux sans fil sécurisés et non sécurisés. La portée d'un réseau local sans fil peut dépasser l'immeuble dans lequel il est installé, ce qui permet à un utilisateur extérieur de pénétrer sur le réseau et d'exploiter une connexion Internet gratuite, voire d'accéder aux données et aux autres ressources de la société. Ce nom s'inspire du film « War Games », où des pirates tentent d'accéder aux réseaux traditionnels en composant des numéros de téléphones au hasard, jusqu'à ce qu'un modem réponde.

WEP (Wired Equivalent Privacy)
WEP est un protocole de sécurité pour les réseaux sans fil. WEP assure la sécurité en cryptant les données sur les ondes radio de sorte à les protéger lors de leur transfert d'un point final à un autre. Une clé partagée (semblable à un mot de passe) est utilisée pour autoriser la communication entre les ordinateurs et le routeur.

Wi-Fi (Wireless Fidelity, fidélité sans fil)
Ce terme désigne des produits de réseau local sans fil reposant sur les normes IEEE 802.11.

Wi-Fi Alliance (précédemment WECA - Wireless Ethernet Compatibility Alliance)
Organisation internationale à but non lucratif créée en 1999 pour tester et certifier la compatibilité des produits Wi-Fi avec les spécifications IEEE 802.11. **En 2006, l'alliance compte plus de 250 membres et a certifié l'interopérabilité de plus de 2 800 produits.**

WLAN (Wireless LAN, réseau local sans fil)
Type de réseau local (LAN) utilisant des ondes radio haute fréquence au lieu de câbles pour communiquer d'un nœud à l'autre.
Groupe d'ordinateurs et de périphériques associés qui communiquent sans fil entre eux.