UNIVERSITÉ DU QUÉBEC À MONTRÉAL

SÉCURITÉ DANS LES RÉSEAUX WI-FI : ÉTUDE DÉTAILLÉE DES ATTAQUES ET PROPOSITION D'UNE ARCHITECTURE WI-FI SÉCURISÉE

MÉMOIRE
PRÉSENTÉ
COMME EXIGENCE PARTIELLE
DE LA MAÎTRISE EN INFORMATIQUE

PAR

MAHER GAHA

MARS 2007

«Où peut-on être mieux qu'au sein de sa famille ? »
Marmontel (Jean-François), Lucile -1769

À mes parents,

Recevez de moi l'agrume de mon labeur, de mes nuits blanches, de mon exil. Pour votre soutien inconditionnel, votre patience et votre générosité, pour tous les efforts que vous avez consentis en ma faveur, je vous dédie ce travail en témoignage de ma grande reconnaissance.

À mes frères et sœur,

Je vous dédie ce mémoire en guise de remerciements pour vos encouragements et votre soutien. Je vous souhaite le plus radieux des avenirs.

À tous mes amis pour leurs encouragements et leur soutien, et à tous ceux qui m'ont aidé et soutenu le long de la réalisation de ce projet

Mes pensées vont également à tous ceux qui m'ont aidé de près ou de loin à mener à bien ce travail.

Maher GAHA

REMERCIEMENTS

Je tiens à exprimer ma vive reconnaissance et mes sincères remerciements à Monsieur Guy Bégin, pour avoir accepté de diriger mes recherches. Je le remercie également pour sa bienveillance, ses conseils judicieux et l'encadrement de qualité dont il m'a fait bénéficier aimablement. Je lui adresse, en signe de reconnaissance, toute ma gratitude et tout mon respect pour ses qualités humaines et scientifiques.

Je voudrais également remercier des gens qu'on oublie souvent mais qui ont énormément contribué pour la communauté scientifique en assurant le développement et la distribution de nombreux outils puissants et gratuits et en mettant leurs travaux de recherche à disposition de tous.

TABLE DES MATIÈRES

LISTE DES FIGURES

LISTE DES TABLEAUX

RÉSUMÉ

Nous avons assisté ces dernières années à la montée en puissance des réseaux locaux sans fil ou encore Wi-Fi, qui sont en passe de devenir l'une des principales solutions de connexion pour de nombreuses entreprises. Le marché du sans fil se développe rapidement dès lors que les entreprises constatent les gains de productivité qui découlent de la disparition des câbles.

Avec cette évolution rapide de ce type dématérialisé de réseaux, les exigences en termes de sécurité deviennent de plus en plus sévères. De ce fait, beaucoup de travaux et d'efforts ont été consentis ces dernières années afin d'aboutir à des solutions pour sécuriser ces réseaux. Toutefois, des vulnérabilités persistent encore et il est toujours possible de monter des attaques plus ou moins facilement. Notamment, contre le dernier né des protocoles de sécurité Wi-Fi, à savoir WPA2, qui bien qu'étant plus robuste sur le plan conceptuel que les générations précédentes, fait face à un problème majeur, celui de son incompatibilité matérielle avec les précédents protocoles. En effet, WPA2 exige de nouveaux équipements matériels, ce qui constitue un surcoût économique énorme pour les entreprises ayant déjà déployé des équipements Wi-Fi d'anciennes générations.

Dans ce mémoire, nous élaborons une synthèse exhaustive de toutes les attaques qui ciblent les réseaux Wi-Fi. Cette synthèse comprend une classification des attaques par rapport aux standards de sécurité ainsi que l'illustration des détails de leur mise en œuvre. Outre le volet conceptuel et théorique, nous abordons également le volet pratique et montrons sa richesse. Nous proposons également une nouvelle approche architecturale de sécurisation des réseaux Wi-Fi dans l'entreprise. Notre proposition prend en compte l'hétérogénéité des équipements et des standards de sécurité supportés. Cette nouvelle architecture a le mérite d'offrir une grande flexibilité ainsi qu'une sécurité renforcée par rapport aux approches traditionnelles. Pour élaborer cette solution sécurisée, nous nous sommes basés principalement sur la différenciation à plusieurs niveaux (standard de sécurité supporté, communauté d'utilisateurs, nature de trafic). Ces niveaux de différenciation offrent la granularité nécessaire pour permettre une meilleure gestion du réseau et un meilleur contrôle d'accès aux ressources, ce qui améliore la sécurité du réseau Wi-Fi en particulier et du système d'information de l'entreprise dans son ensemble.

Mots clés : Wi-Fi, sécurité, attaque, architecture sécurisée, différenciation.

CHAPITRE I

INTRODUCTION ET PROBLÉMATIQUE

1.1 Contexte et problématique

Nous assistons aujourd'hui à un fort développement de l'effectif nomade dans les entreprises, dont l'organisation devient de moins en moins hiérarchisée. En effet, les employés sont équipés d'ordinateurs portables et passent plus de temps à travailler au sein d'équipes plurifonctionnelles, trans-organisationnelles et géographiquement dispersées.

De ce fait, nous avons assisté ces dernières années à la montée en puissance des réseaux locaux sans fil ou encore Wi-Fi[1], qui sont en passe de devenir l'une des principales solutions de connexion pour de nombreuses entreprises. Le marché du sans fil se développe rapidement dès lors que les entreprises constatent les gains de productivité qui découlent de la disparition des câbles. Selon les estimations de la Wi-Fi Alliance, l'industrie du LAN sans fil, qui a dépassé 1 milliard de dollars US en 2001, en représentera 10 milliards en 2007, pour quelques 40 millions de périphériques compatibles 802.11 sur le marché.

Ainsi avec cette évolution rapide de ce type dématérialisé de réseaux, les exigences en termes de sécurité deviennent de plus en plus sévères. En effet, pour garantir la pérennité et l'essor de cette technologie, il est primordial de recourir à des méthodes avancées d'authentification, de gestion et de distribution de clés entre les différentes entités communicantes, ceci tout en respectant les contraintes imposées par les réseaux sans fil, telles que la capacité de l'interface radio qui représente le goulot d'étranglement du trafic pour ce

---

[1] Wireless Fidelity

type de réseaux. Ainsi, un protocole de sécurité devrait pouvoir établir des sessions sans altération de la performance globale du réseau, tout en fournissant les différents services de sécurité requis pour chaque type d'application.

Beaucoup de travaux et d'efforts ont été consentis ces dernières années afin d'aboutir à des solutions pour sécuriser les échanges dans ces réseaux. Toutefois, des vulnérabilités persistent encore dans ces solutions et il est toujours possible de monter des attaques plus ou moins facilement. Notamment contre le dernier né des protocoles de sécurité Wi-Fi, à savoir le WPA2, qui bien qu'étant plus robuste sur le plan conceptuel que les générations précédentes, fait face au problème majeur de son incompatibilité matérielle avec les précédents protocoles. En effet, WPA2 exige de nouveaux équipements matériels, ce qui constitue un surcoût économique énorme pour les entreprises ayant déjà déployé des équipements Wi-Fi d'anciennes générations.

Dans ce mémoire, nous nous intéressons à la problématique de sécurité des réseaux Wi-Fi dans l'entreprise. Compte tenu des vulnérabilités des standards de sécurité Wi-Fi, et face à toutes les failles de sécurité et la diversité des attaques qu'il est possible de monter contre les mécanismes de sécurité dans les réseaux 802.11, quelles sont les meilleures pratiques architecturales en matière de sécurisation Wi-Fi ? Comment assurer une sécurité optimale, compte tenu de l'hétérogénéité des équipements Wi-Fi (WEP, WPA, WPA2), existants actuellement dans les entreprises?

Il est à noter que nous nous intéressons dans le cadre de ce mémoire aux réseaux Wi-Fi en mode infrastructure. En effet, nous ne traitons pas le cas des réseaux ad-hoc et dénotons tout au long de ce mémoire par réseaux Wi-Fi, les réseaux de la norme IEEE 802.11 ayant comme élément central un point d'accès.

1.2 Objectifs du mémoire

L'objectif de ce mémoire est dans un premier temps d'apporter une meilleure compréhension du mode de fonctionnement des protocoles de sécurité dans les réseaux Wi-Fi. En effet, nous analysons l'évolution de la normalisation et présentons les principales méthodes d'authentification, ainsi que les mécanismes de chiffrement adoptés par chacun des

protocoles que nous étudions. Le second objectif et non des moindres est l'étude des vulnérabilités des différentes générations de standards de sécurité Wi-Fi et la réalisation d'une synthèse sur les modes opératoires des différentes attaques et leur évolution au fil du temps.

Enfin, nous proposons une nouvelle approche architecturale de sécurisation des réseaux 802.11 dans l'entreprise qui prend en compte l'hétérogénéité des équipements et des standards de sécurité supportés. Cette nouvelle approche a le mérite d'offrir une grande flexibilité ainsi qu'une sécurité renforcée par rapport aux approches traditionnelles.

Par ailleurs, la contribution originale de ce mémoire réside dans deux éléments principaux. La première consiste en l'élaboration d'une synthèse exhaustive de toutes les attaques qui ciblent les réseaux Wi-Fi, leur classification par rapport aux standards de sécurité ainsi que l'illustration des détails de leur mise en œuvre. Outre le volet conceptuel et théorique, nous abordons également le volet pratique et montrons sa richesse. La réalisation de cette étude n'a pas été triviale et a nécessité une documentation approfondie, ainsi que le test de divers outils d'attaques dont la configuration n'a pas toujours été simple. De plus, plusieurs attaques ne sont pas du tout documentées et nous avons eu à les simuler à l'aide d'outils particuliers, afin de comprendre leur mode opératoire.

Cette première contribution nous a permis de cerner les faiblesses des mécanismes de sécurité des réseaux Wi-Fi. D'où la seconde contribution originale et sans doute la plus importante qui consiste en la proposition d'une nouvelle approche architecturale pour sécuriser les réseaux Wi-Fi dans l'entreprise, en fixant un certain nombre d'objectifs, qui parfois sont divergents. Nous sommes parvenus à cette proposition, que nous formulons dans ce mémoire, suite à un cheminement rigoureux et articulé. Le plan de notre mémoire démontre comment nous avons abordé le problème et la méthodologie adoptée (au niveau du chapitre 5 et 6) pour le résoudre.

1.3 Plan du mémoire

Le présent mémoire est structuré comme suit :

Dans le second chapitre, nous nous consacrons à l'étude des technologies employées au niveau de la couche physique et la couche liaison de données, ainsi qu'aux diverses fonctionnalités offertes par la norme Wi-Fi, ou encore IEEE 802.11.

Dans le troisième chapitre, nous focalisons sur les standards de sécurité de la norme IEEE 802.11. Nous nous concentrerons sur l'aspect analyse de cette évolution, montrant à chaque fois, les caractéristiques et les détails de fonctionnement de chaque protocole..

Une fois les différentes générations de protocoles de sécurité Wi-Fi présentées et analysées, nous nous concentrons dans le quatrième chapitre, sur le volet faiblesses et vulnérabilités. En effet, ce chapitre, présente une analyse détaillée des vulnérabilités de chaque génération de protocole de sécurité Wi-Fi, ainsi que les détails de fonctionnement des principales attaques.

Dans le cinquième chapitre, nous proposons une nouvelle approche architecturale de sécurisation des réseaux Wi-Fi et discutons ses caractéristiques.

Dans le sixième chapitre, nous élaborons une évaluation qualitative et quantitative de la nouvelle approche, moyennant une simulation. Cette évaluation permettra de valider notre contribution et de juger de sa pertinence.

Finalement, ce mémoire se termine par une conclusion qui fait la synthèse de ce qui a été vu tout au long de cette étude et donne un aperçu sur les perspectives de travaux de recherche futurs, ainsi que les défis majeurs à relever, en termes de sécurité Wi-Fi.

CHAPITRE II

TECHNOLOGIES DES RÉSEAUX WI-FI

La norme IEEE 802.11 est un standard international décrivant les caractéristiques d'un réseau local sans fil. Le nom Wi-Fi correspond initialement au nom donné à la certification délivrée par la Wi-Fi Alliance, l'organisme chargé de maintenir l'interopérabilité entre les matériels répondant à la norme 802.11. Dans la suite du mémoire, nous utiliserons de façon interchangeable les termes Wi-Fi et 802.11.

Ainsi, à travers ce chapitre nous montrons les différentes topologies de ces réseaux, ainsi que les caractéristiques des couches physiques et liaisons de données. Ensuite, nous présentons les techniques d'accès et de réservation du support employées. Enfin, nous esquissons les diverses orientations de recherche et les problématiques qui restent à résoudre afin de garantir l'essor de cette technologie.

2.1 Architecture Wi-Fi

Un réseaux 802.11 est composé de plusieurs regroupements de terminaux, munis d'une carte d'interface réseau 802.11. Ces regroupements sont des cellules Wi-Fi. Dans ce qui suit, nous montrons qu'ils peuvent être de différentes topologies.

2.1.1 Les topologies de la norme 802.11

A la base, les réseaux sans fil 802.11 peuvent être vus comme un ensemble de technologies permettant d'établir un réseau local sans l'utilisation du câblage pour les liaisons entre les ordinateurs. En effet, le câblage est remplacé par des liaisons hertziennes. Les

principales technologies permettant de développer des réseaux sans fil ou WLAN[2] sont celles appartenant aux normes IEEE 802.11. La norme la plus populaire de WLAN est le 802.11b.

Ainsi, tel que le montre la figure 2.1 la norme Wi-Fi définit deux modes opératoires :

- le mode infrastructure dans lequel les clients sans fil sont connectés à un point d'accès. Il s'agit généralement du mode par défaut des cartes réseaux 802.11.
- le mode ad hoc dans lequel les clients sont connectés les uns aux autres sans aucun point d'accès.

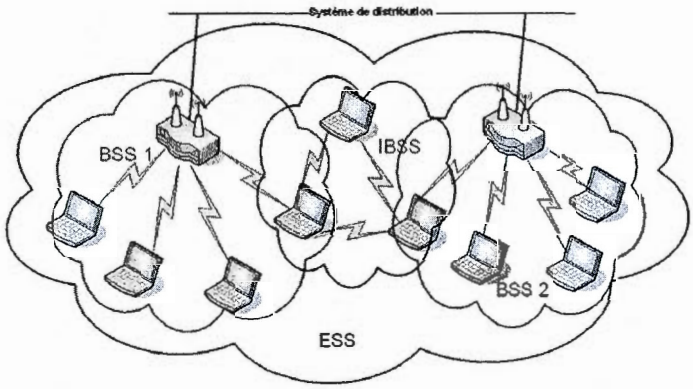


Figure 2.1 : Topologies des réseaux de la norme IEEE 802.11

2.1.1.1 Le mode infrastructure

Un réseau 802.11 est un ensemble de cellules de base (BSS[3]). Chaque cellule BSS comporte un point d'accès matérialisé par un dispositif d'émission/réception. Les cellules sont reliées par une infrastructure de communication fixe et interconnectées par un système de distribution afin de former un ESS[4]. Cette infrastructure incorpore un portail permettant d'assurer l'interface avec un réseau local, tel que le montre la figure 2.2.

---

2 Wireless Local Area Network
3 Basic Service Set
4 Extended Service Set

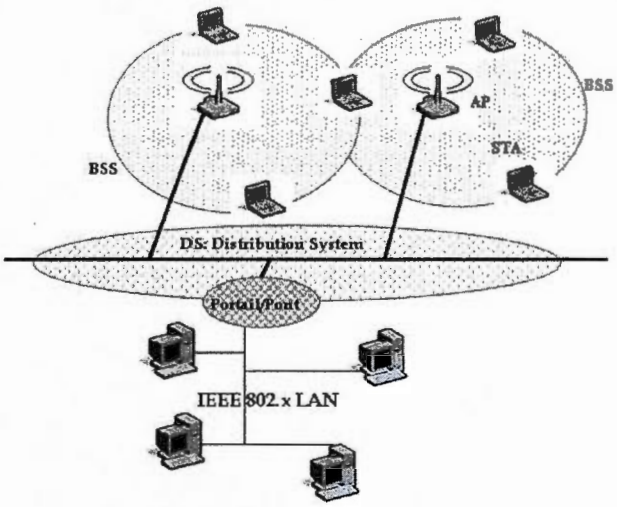


Figure 2.2 : Mode infrastructure

Chaque BSS est identifié par un BSSID. Dans le mode infrastructure, le BSSID correspond à l'adresse physique (adresse MAC) du point d'accès.

2.1.1.2 Le mode ad-hoc

Ce mode représente un ensemble de stations 802.11 qui communiquent entre elles sans avoir recours à un point d'accès. Chaque station peut établir une communication avec n'importe quelle autre station dans la cellule que l'on appelle cellule indépendante IBSS[5], tel qu'illustré dans la figure 2.3.

Dans les deux modes infrastructure et ad hoc, chaque réseau de service est identifié par un identificateur de réseau SSID. Par conséquent, toute station désirant se connecter à un réseau de service particulier doit connaître au préalable la valeur de son SSID [1].

---

5 Independent BSS

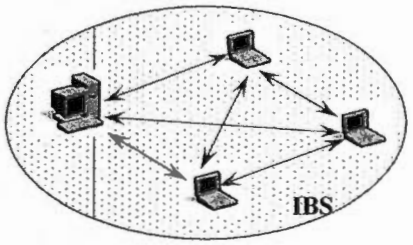


Figure 2.3 : Mode ad-hoc

2.1.2 Les couches de l'IEEE 802.11

L'IEEE 802.11 implémente de nouvelles couches physiques et de nouvelles techniques d'accès au support, au niveau de la couche de liaison de données. Dans ce qui suit, nous donnons un aperçu sur les nouvelles caractéristiques des couches physiques et de liaison de données, relatives à la norme 802.11.

2.1.2.1 La couche physique

Au niveau de la couche physique, les normalisateurs ont opté pour deux sous-couches, à savoir : PLCP (Physical Layer Convergence Protocol) et PMD (Physical Medium Dependent). La sous-couche PLCP concentre les fonctionnalités d'encodage des données, alors que la seconde sous-couche PMD se charge de l'écoute du support et fournit un service de signalisation à la couche MAC, en lui notifiant l'état du support : occupé ou libre [2].

Pour l'encodage des données, la sous-couche PLCP utilise plusieurs techniques de modulation et de codage binaire. Cette diversité de techniques de codage et de modulation a donné naissance à plusieurs sous-normes avec des débits et des portées différentes, telles que 802.11b, 802.11a et 802.11g. Parmi ces techniques, nous citons la CCK (Complementary Code Keying), le codage DSSS (Direct Sequence Spread Spectrum), l'OFDM (Orthogonal Frequency Division Multiplexing) et la FHSS (Frequency Hopping Spread Spectrum).

2.1.2.2 La couche de liaison de données

La couche de liaison de données de la norme 802.11 est subdivisée en deux sous-couches : la sous-couche LLC (Logical Link Control) et la sous-couche MAC. La première sous-couche est commune à tous les standards du groupe 802. Quant à la sous-couche MAC

802.11, son rôle primaire est l'écoute de la porteuse avant l'émission des données. Elle intègre en plus un grand nombre de fonctionnalités que l'on ne trouve pas dans la version 802.3 (Ethernet) de cette même sous-couche.

Les normalisateurs ont en effet défini deux méthodes d'accès différentes au niveau de la couche MAC 802.11. La première est le DCF (Distributed Coordination Function), qui correspond à une méthode supportant le *best-effort*. Le DCF a été conçu principalement pour le transport de données asynchrones. Ainsi, cette méthode garantit à tous les utilisateurs qui veulent transmettre des données la même probabilité d'accès au support.

La seconde méthode d'accès est le PCF (Point Coordination Function). Elle se base sur l'interrogation séquentielle des stations, sous la supervision du point d'accès. Ainsi, la méthode PCF est conçue essentiellement pour la transmission de données sensibles, qui sollicitent une gestion serrée des délais. Cette méthode d'accès est utilisée pour le transport de grosses trames pour lesquelles une retransmission serait trop coûteuse en termes de bande passante.

2.1.3 Les techniques d'accès au support radio

La technique DCF pour l'accès au support de transmission constitue la technique d'accès par défaut. Elle permet la transmission de données en mode asynchrone et best-effort, sans aucune exigence de priorité. La technique DCF s'appuie sur le protocole CSMA/CA[6], qui est la variante sans fil du traditionnel CSMA/CD[7] du monde Ethernet. Dans ce qui suit, nous donnons les caractéristiques principales du protocole CSMA/CA, ainsi que le mécanisme de réservation du support hertzien.

2.1.3.1 Le protocole CSMA/CA

Dans le monde filaire d'Ethernet, le protocole CSMA/CD régule les accès au support et se charge de la détection et du traitement des collisions qui se produisent. Dans les réseaux

---

6 Carrier Sense Multiple Access / Collision Avoidance
7 Carrier Sense Multiple Access / Collision Detection

Wi-Fi, la détection des collisions n'est pas possible, dû à la nature même du support de transmission. En effet, la détection de collision exige de la station la simultanéité de l'émission et de la réception. Or les liaisons radio ne sont jamais en bidirectionnel simultané (*full duplex*) [4]. Ainsi, la station étant incapable d'écouter sa propre transmission, si une collision se produit, la station continuera à transmettre la trame au complet, ce qui entraîne une forte baisse de performance du réseau.

Le protocole CSMA/CA doit donc éviter les collisions, à défaut de pouvoir les détecter. CSMA/CA se base principalement sur les espaces inter trames ou encore IFS[8] pour l'évitement de collisions [2]. Ces IFS sont les intervalles de temps séparant la transmission de trames consécutives et qui correspondent à des périodes d'inactivité sur le support de transmission. Le standard défini trois types d'IFS différents :

1. SIFS (Short IFS): SIFS est utilisé pour séparer les transmissions de trames consécutives au sein d'une même transmission (envoi de données, ACK, etc.). Durant cet intervalle, il n'y a qu'une seule station pouvant transmettre.
2. PIFS (PCF IFS): PIFS est utilisé par le point d'accès pour accéder avec priorité au support.
3. DIFS (DCF IFS): DIFS est utilisé lorsqu'une station veut commencer une nouvelle transmission.

Ainsi, lors de l'envoi d'une trame par la station source, les autres stations entendent cette transmission et pour éviter une collision, incrémentent la valeur d'un compteur, appelé NAV (Network Allocation Vector), qui sert à retarder toutes les transmissions prévues de toutes les stations. La valeur d'incrémentation du NAV est calculée par rapport au champ durée de vie, ou TTL, contenu dans les trames qui passent sur le support. Ensuite, le compteur NAV est décrémenté jusqu'à atteindre la valeur 0, instant signalant à la station l'autorisation de transmettre ses données, après un intervalle DIFS. Le principe de

---

8 Inter-Frame Spacing

fonctionnement de CSMA/CA moyennant les IFS et le compteur NAV est illustré par la figure 2.4.

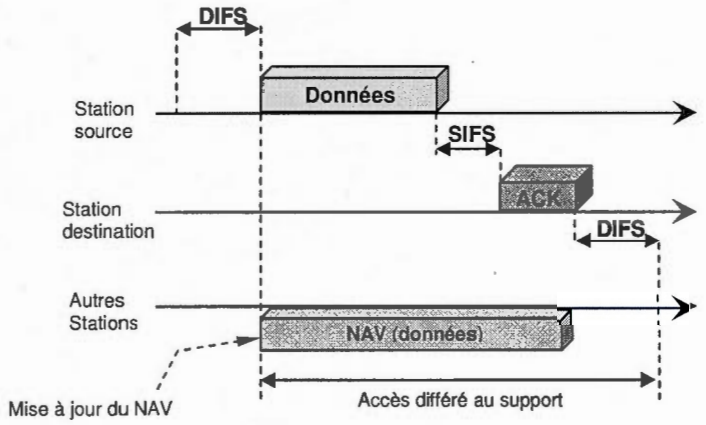


Figure 2.4 : Processus de transmission des trames [2]

Comme le montre la figure 2.4, une station voulant transmettre des données écoute le support. Si aucune activité n'est détectée pendant une période DIFS, elle transmet ses données immédiatement. La station destination attend pendant un intervalle SIFS et émet un ACK pour confirmer la bonne réception des données. Si l'ACK n'a pas été détecté par la station source ou si les données ne sont pas reçues correctement, on suppose qu'une collision s'est produite et la trame est retransmise [4].

2.1.3.2 Mécanisme de réservation du support RTS/CTS

Les normalisateurs ont inclus dans le standard IEEE 802.11 un mécanisme permettant de réserver le support pour une transmission particulière. Ce mécanisme n'est pas actif par défaut dans le standard, mais il est activé optionnellement par la station souhaitant réserver le support exclusivement pour sa transmission. Ce mécanisme n'est autre que VCS[9] localisé au niveau de la couche MAC. VCS se base sur l'émission de trames RTS/CTS[10] entre une station source et une station destination, précédant toute transmission de données.

---

9 Virtual Carrier Sense
10 Request To Send/Clear To Send

Ainsi, une station source voulant transmettre des données émet une trame RTS. Toutes les stations de la cellule BSS détectant le RTS lisent son champ TTL et mettent à jour leur valeur de NAV. La station destination ayant reçu le RTS réplique par un CTS, en temporisant sa transmission pendant un SIFS. Les autres stations détectent le CTS, lisent le champ TTL de celui-ci et mettent à nouveau à jour leur NAV [2].

Après réception du CTS, la station source est assurée que le support est stable et réservé exclusivement pour sa transmission de données. De cette manière, la station source peut transmettre ses données ainsi que recevoir l'ACK sans collision. Ce mécanisme de réservation est surtout utilisé pour l'envoi de grosses trames pour lesquelles une retransmission serait trop coûteuse en bande passante [2].

2.2 Normes associées à l'IEEE 802.11

Les réseaux Wi-Fi ont suscité un engouement incomparable chez la communauté scientifique, ainsi que chez les industriels, vu l'énorme potentiel que représente une telle technologie. D'un autre côté, la technologie Wi-Fi renferme une grande complexité et pose plusieurs problématiques, souvent divergentes.

Dans ce qui suit, nous donnons une description des principales problématiques traitées par les groupes de travail de l'IEEE 802.11.

2.2.1 L'IEEE 802.11e : la qualité de service

L'IEEE a chargé le groupe de travail 802.11e d'améliorer la couche MAC 802.11 pour y inclure des mécanismes de qualité de service, afin de permettre un meilleur support des applications sensibles aux phénomènes de latence, telles que les applications de voix ou vidéo. Le groupe de travail n'a pas encore finalisé le standard 802.11e, mais a réussi à mettre en œuvre quelques solutions intermédiaires intéressantes, tel qu'EDCF[11] qui réalise un contrôle d'admission simple et efficace. Les efforts se poursuivent encore afin d'aboutir à un

---

11 Enhanced DCF

ensemble d'outils pratiques et efficaces qui permettent d'étendre et de développer les applications Wi-Fi.

2.2.2 L'IEEE 802.11f : les handovers

L'objectif du groupe 802.11f est de développer la technologie permettant la mobilité inter-cellules des stations Wi-Fi, tout en préservant les performances du réseau et en maintenant la connectivité des stations lors du déplacement.

Ainsi, la plupart des réseaux sans fil pourront désormais jouer le rôle de réseaux mobiles, en adoptant la norme 802.11f, qui équipe actuellement la plupart des interfaces Wi-Fi. Ces dernières permettent de réaliser des handovers ou relève intercellulaire qui désigne la possibilité de passer d'une cellule à une autre sans interruption de la communication. Le protocole retenu par le groupe de travail 802.11f est IAPP[12], qui fait communiquer les différents points d'accès d'un même réseau ESS, de façon à permettre à un utilisateur mobile de passer d'une cellule à une autre sans perte de connexion.

Toutefois, le standard 802.11f ne garantit pas une mobilité sécurisée et rapide [2]. C'est pourquoi, l'IEEE vient de mettre en place un nouveau groupe de travail, l'IEEE 802.11r, afin de développer une nouvelle norme garantissant la sécurité et la rapidité des handovers.

2.2.3 L'IEEE 802.11n : le haut débit

L'IEEE 802.11n est un groupe de travail au sein de l'IEEE, mis en place en 2003. Les raisons qui ont suscité la création de ce groupe sont les suivantes :

- Les réseaux Wi-Fi (standards 802.11b, g et a) offrent une portée limitée.
- Les réseaux Wi-Fi sont très sensibles aux phénomènes de réflexion d'ondes, ainsi qu'aux interférences ayant comme origine d'autres unités sans fil.
- Les réseaux Wi-Fi sont beaucoup plus lents, en termes de débits, qu'Ethernet.

---

12 Inter Access Point Protocol

Cette unité de recherche travaille sur la mise en œuvre d'une norme devant résoudre les problèmes cités ci-dessus. En effet, 802.11n est sensé permettre d'atteindre un débit minimal de 100Mbps, et un débit théorique utile maximal de 540 Mbps. Ce pré-standard se base sur une technologie radio innovante, nommée MIMO[13], qui se base sur l'utilisation de plusieurs antennes à l'émission et pareillement à la réception. De plus, l'IEEE a mis comme exigence à la mise en œuvre d'une telle technologie la rétrocompatibilité et l'interopérabilité complètes avec les standards actuels (802.11b, g et a). Ce standard devrait voir le jour début 2007 [5].

2.2.4 L'IEEE 802.11i : la sécurité

Dans les réseaux Wi-Fi, le support est partagé. Tout ce qui est transmis peut donc être intercepté. L'incapacité de garantir un trafic aussi sécurisé que dans les réseaux fixes constitue un obstacle pour l'essor de la technologie Wi-Fi. C'est pourquoi l'IEEE a mis en place le groupe de travail IEEE 802.11i, dont la mission est la mise au point d'une architecture de sécurité robuste, qui prend en compte les spécificités des réseaux sans fil.

Parmi les groupes de travail de l'IEEE, le 802.11i est certainement le groupe de travail le plus actif et le plus sollicité par les industriels. Les réseaux Wi-Fi dans leur conception originelle n'intégraient pas la sécurité comme contrainte majeure à couvrir, ce qui a eu comme conséquence une grande difficulté à l'intégrer par la suite [2].

Ainsi, ces dernières années nous avons assisté à la production d'une multitude de protocoles de sécurité Wi-Fi, sans pour autant que la sécurité nécessaire à ce type de réseaux s'en trouve vraiment garantie. Dans le prochain chapitre, nous nous concentrons sur cette partie, en montrant l'évolution de la normalisation.

---

13 Multiple Input Multiple Output

CHAPITRE III

ÉTUDE DES STANDARDS DE SÉCURITÉ DANS LES RÉSEAUX WI-FI

Dans ce chapitre, nous allons dresser un bilan de la normalisation IEEE en termes de protocoles de sécurité pour les réseaux Wi-Fi, montrant ainsi l'évolution de la normalisation au cours des dernières années.

Nous commençons par introduire le mécanisme de chiffrement WEP. Nous montrons ses détails de fonctionnement. Ensuite, nous passons au mécanisme d'authentification des réseaux Wi-Fi, à savoir le standard 802.1x, que nous détaillons. Enfin, nous nous attardons sur la norme 802.11i, qui se veut comme norme unificatrice des protocoles de sécurité pour les réseaux Wi-Fi et dont l'objectif est de combler toutes les lacunes de sécurité des standards précédents.

3.1 Le protocole WEP

Le protocole WEP[14] constitue le premier mécanisme de chiffrement implanté dans les réseaux sans fil dans le but de sécuriser les échanges radio. Le protocole WEP se base sur une clé secrète K partagée entre les différentes parties communicantes pour protéger le corps de la trame de données transmise. Le principe du protocole WEP consiste à utiliser l'algorithme RC4[15], un algorithme de chiffrement en mode flux. Ainsi, à partir d'une clé (PSK) de longueur comprise entre 40 et 104 bits (version améliorée de WEP) et un vecteur d'initialisation (IV) de 24 bits transporté en clair dans chaque paquet, WEP génère une suite

---

14 Wireless Encryption Privacy

15 Ron's Code 4

d'octets pseudo aléatoire nommée *KeyStream* (*Ks*). Cette série d'octets est utilisée pour chiffrer un message M, en effectuant un OU exclusif (XOR) bit-à-bit entre *Ks* et M, C = *Ks* XOR M, où C est le message chiffré [6]. La figure 3.1 montre le mécanisme de chiffrement WEP.

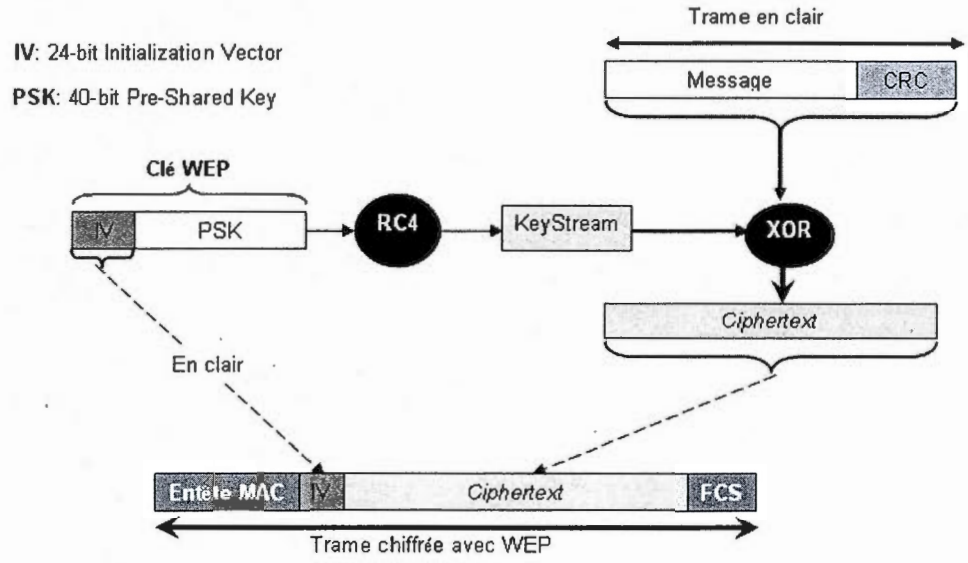


Figure 3.1 : Le chiffrement WEP

Le protocole WEP est destiné à assurer plusieurs objectifs de sécurité tels que le contrôle d'accès, la confidentialité, l'authentification et l'intégrité des données.

Toutefois, tel que démontré dans [6], WEP présente de nombreuses failles de sécurité, notamment au niveau de la gestion des clés (tous les utilisateurs ont la même clé). En effet, WEP ne définit aucun moyen pour gérer les clés de chiffrement de façon dynamique. C'est à l'administrateur du réseau Wi-Fi de créer les clés, de les distribuer, de les archiver d'une manière protégée, de clarifier qui a telle ou telle clé cryptographique et de révoquer les clés compromises. Les spécifications de WEP ne prennent aucunement en charge cette problématique.

C'est pourquoi, la norme IEEE 802.1X a été introduite dans le but de gérer l'authentification via un serveur centralisé. Cette norme, détaillée dans ce qui suit, vient pallier aux insuffisances de WEP, au niveau de la distribution et du renouvellement périodique et automatique des clés. Par ailleurs, les principales faiblesses de WEP et les attaques qu'il est possible d'établir seront détaillées et analysées lors du prochain chapitre.

3.2 Le protocole IEEE 802.1x

Afin de pallier au manque de sécurité du standard 802.11, l'IEEE propose le standard 802.1x comme base pour le contrôle d'accès, l'authentification et la gestion de clés. La mission du 802.1x est de bloquer le flux de données d'un utilisateur non authentifié, c'est-à-dire de permettre une authentification lors de l'accès au réseau et donc un contrôle d'accès aux ressources.

3.2.1 Architecture du 802.1x

Le standard 802.1x utilise un modèle qui s'appuie sur trois entités fonctionnelles :

- Le système à authentifier : c'est un client demandant un accès au réseau. Dans le contexte des réseaux Wi-Fi, le système à authentifier n'est autre que le client 802.11.
- Le certificateur : c'est l'unité qui contrôle et fournit la connexion au réseau. Un port contrôlé par cette unité peut avoir deux états : non autorisé ou autorisé. Lorsque le client n'est pas authentifié, le port est dans l'état non autorisé et seulement le trafic nécessaire à l'authentification est permis entre le terminal et le certificateur. Le certificateur transmet la requête d'authentification au serveur d'authentification en utilisant le protocole EAP[16]. Les autres paquets sont bloqués lorsque le port se trouve dans l'état non autorisé. À la fin de ces échanges, le certificateur analyse le message notifiant l'échec ou le succès de la procédure et filtre les trames de la station Wi-Fi en fonction du résultat. Dans les réseaux Wi-Fi, c'est le point d'accès qui joue le rôle de certificateur.

---

16 Extensible Authentication Protocol

- Le serveur d'authentification : il réalise la procédure d'authentification avec le certificateur, et valide ou rejette la demande d'accès. Durant cette phase, le certificateur (le point d'accès) n'interprète pas le dialogue entre le serveur et le terminal. Il agit comme un simple relais passif. Si la requête d'accès est validée par le serveur, le port est commuté dans l'état autorisé et le client est autorisé à avoir un accès complet au réseau [3]. Généralement, le serveur d'authentification utilisé dans les réseaux Wi-Fi est un serveur RADIUS[17].

3.2.2 Les méthodes d'authentification du 802.1x

Le protocole EAP n'est pas un protocole d'authentification en soit, mais constitue une enveloppe générique pour l'encapsulation de plusieurs méthodes d'authentification. Notons qu'EAP offre deux avantages majeurs par rapport à la sécurité 802.11 de base avec WEP :

- Le premier est la gestion et la distribution centralisées des clés de cryptage. Même si la mise en œuvre WEP de RC4 était sans faille, la distribution des clés statiques à tous les points d'accès et à tous les clients du réseau constituerait encore une sérieuse pénalité administrative.
- Le second avantage est la possibilité de définir un contrôle centralisé des politiques d'accès avec des délais d'expiration de session entraînant une nouvelle authentification et la génération de nouvelles clés.

Le protocole EAP est utilisé avec 802.1X d'une manière transparente entre la station sans fil et le serveur d'authentification au travers du point d'accès. Cependant, 802.1X nécessite la coopération entre un serveur d'authentification et une méthode d'authentification. La méthode d'authentification est une couche située au-dessus d'EAP qui définit des mécanismes de sécurité et de distribution de clés. Néanmoins, 802.11 n'a pas précisé la façon d'implémenter EAP avec 802.1X [7]. Pour cette raison, nous retrouvons une profusion de méthodes d'authentification et plusieurs couches sont définies au-dessus de EAP. Parmi les

---

17 Remote Authentication dial-In User Service

méthodes d'authentification les plus fiables, nous trouvons EAP-TLS, EAP-TTLS[18], LEAP[19] et PEAP[20]. Chacune de ces méthodes d'authentification présente des avantages et des inconvénients et diffère des autres par divers aspects. Pour élaborer une étude comparative, nous avons tenu compte des critères suivants :

- Authentification mutuelle;
- Utilisation de certificats;
- Distribution dynamique de clés;
- Risques de sécurité.

	EAP-TLS	EAP-TTLS	LEAP	PEAP
Authentification du serveur	Oui, par certificat	Oui, par certificat	Oui, par mot de passe	Oui, par certificat
Authentification du client	Oui, par certificat ou carte à puce	Oui, par certificat ou mot de passe ou carte à puce	Oui, par nom d'utilisateur/mot de passe	Oui, par nom d'utilisateur/mot de passe ou mot de passe unique (OTP)
Certificats exigés	Oui	Oui, pour l'authentification côté serveur	Non	Oui
Distribution dynamique des clés	Oui	Oui	Oui	Oui
Risques de sécurité	Obtention de l'identité client	Attaque MitM	Attaque par dictionnaire et obtention du login client	Attaque MitM

Tableau 3.1: Comparaison entre les principales méthodes d'authentification EAP

Ainsi tel que présenté dans le tableau 3.1, toutes les méthodes étudiées assurent une authentification mutuelle entre le client et le serveur (bien que parfois optionnelle), ainsi qu'une distribution dynamique des clés. Toutefois, elles présentent des différences de

---

18 EAP-Tunnelled TLS
19 Lightweight EAP
20 Protected EAP

fonctionnement. En effet, certaines méthodes font appel à des certificats et d'autres pas. De plus, l'authentification du serveur par le client est optionnelle dans certaines méthodes.

Il est vrai que les méthodes d'authentification utilisant les certificats présentent de meilleures garanties de sécurité, sauf que cet avantage s'accompagne d'un inconvénient qui consiste en la lourdeur d'un tel mécanisme, surtout dans un contexte de réseau Wi-Fi, où le support est partagé. Les méthodes d'authentification faisant appel à des certificats exigent le déploiement d'une infrastructure à clé publique. Cette infrastructure ne peut pas être déployée dans plusieurs types d'entreprises. En effet, elle nécessite la distribution des certificats aux clients et la révocation de ceux qui ne sont plus valides. En plus, elle entraîne un surplus important en terme de gestion et de ressources machines et humaines.

Par ailleurs, comme nous pouvons le remarquer, toutes les méthodes d'authentification sont sensibles à des attaques plus ou moins grave. Ceci pourrait nous amener à admettre que l'on ne pourrait pas se contenter d'une méthode d'authentification pour assurer la sécurité des échanges entre le client et le serveur d'authentification dans un réseau sans fil, mais qu'il faudrait ajouter d'autres mécanismes pour pallier à ces faiblesses. Nous évoquerons ces mécanismes dans les sections suivantes.

3.3 La norme 802.11i

Nous avons précédemment donné un aperçu des faiblesses du protocole WEP. Nous avons montré que le protocole 802.1X définit un cadre pour l'authentification mais ne spécifie pas en détails la méthode de distribution des clés. Ainsi, l'authentification 802.1X peut être la cible de plusieurs types d'attaques.

Conscient de ces lacunes de sécurité, le groupe de travail IEEE 802.11i a mis au point une architecture destinée à les combler. Une première évolution sécurisée du Wi-Fi, le WPA[21] apparue en avril 2003, est fondée sur un sous-ensemble du standard IEEE 802.11i. Cette version de WPA peut être considérée comme une norme de deuxième génération pour la sécurité des réseaux sans fil. Implémentée dans les produits depuis le début de l'année

---

[21] Wi-Fi Protected Access

2004, WPA n'a pas vraiment été un succès, principalement du fait de son statut intermédiaire. Il est cependant important de noter que cette deuxième génération est compatible avec les équipements Wi-Fi du marché et qu'il n'y a qu'une minime mise à jour logicielle à opérer.

La norme 802.11i marque une étape plus importante puisqu'elle spécifie la façon de sécuriser un réseau sans fil pour les années à venir. Dans cette norme de troisième génération estampillée WPA2 sur les produits, il y a eu l'introduction de changements fondamentaux comme la séparation de l'authentification utilisateur et le chiffrement/contrôle d'intégrité des messages, donnant une architecture de sécurité robuste passant à l'échelle et convenant tant aux entreprises qu'aux particuliers.

La nouvelle architecture pour les réseaux sans fil utilise l'authentification 802.1X, la rotation et la distribution des clés et de nouveaux mécanismes d'intégrité et de chiffrement tel que le standard américain AES[22] [6]. Toutefois, cette norme n'est pas compatible avec les anciennes générations de standards de sécurité Wi-Fi, ce qui remet en cause tous les investissements en sécurité précédents, qui peuvent être assez lourds. Ainsi, nous pouvons classer les apports de 802.11i en deux catégories principales :

- Définition de multiples protocoles de sécurité radio.
- Nouveau mécanisme de dérivation et de distribution des clés.

Dans ce qui suit, nous discutons chacun des apports du standard 802.11i en détails.

3.3.1 Les protocoles de sécurité Radio

Le protocole WEP ayant montré ses faiblesses et ses limites quant à garantir la sécurité des transmissions de données dans un réseau Wi-Fi, la norme WPA2 a été enrichie de deux protocoles de chiffrement des transmissions radio supplémentaires :

- TKIP[23] qui est le successeur de WEP,
- CCMP qui est un protocole de chiffrement utilisant l'algorithme AES.

---

22 Advanced Encryption Standard
23 Temporal Key Integrity Protocol

Ainsi, dans l'optique d'une meilleure flexibilité et adaptabilité de la norme, TKIP a été maintenu dans le standard 802.11i, afin de permettre la transition des systèmes basés sur WEP vers un protocole plus sécurisé, surtout qu'AES nécessite de nouveaux équipements matériels.

3.3.2 Mécanismes d'échange de clés

Parmi les apports de la norme 802.11i, les mécanismes d'échange et de dérivation des clés sont considérés comme étant les éléments apportant le plus de garanties quant à la manière de sécuriser un réseau Wi-Fi.

En effet, pour la deuxième génération de sécurité Wi-Fi, à savoir WPA, outre l'absence d'un mécanisme de chiffrement robuste tel que CCMP[24], l'absence d'un mécanisme spécifiant la manière d'échanger des clés de façon sécurisée est certainement l'élément crucial qui lui faisait le plus défaut.

Ainsi, tel qu'illustré par la figure 3.2, le standard 802.11i définit un contexte de communication sécurisé qui s'effectue en quatre phases:

- la mise en accord sur la politique de sécurité,
- l'authentification 802.1X,
- la distribution et la hiérarchie des clés,
- le chiffrement et l'intégrité.

---

24 Counter-mode/CBC-MAC Protocol

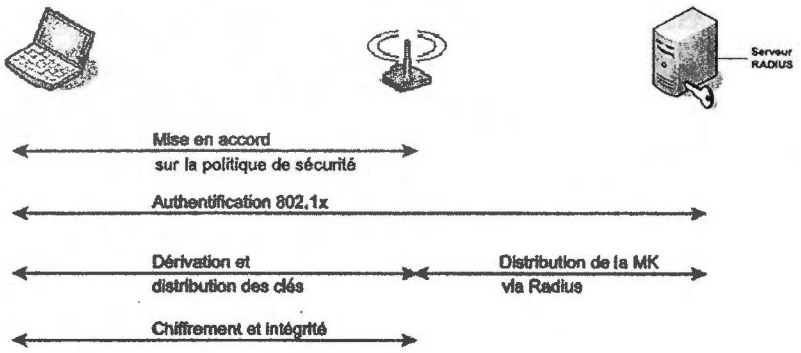


Figure 3.2 : Les phases opérationnelles du 802.11i

3.3.2.1 Phase 1 : Mise en accord sur la politique de sécurité

La norme 802.11i a inclus dans ses spécifications le mécanisme permettant à une station sans fil 802.11i de se rattacher à un point d'accès, avec la négociation de la politique de sécurité à adopter pour la suite de l'échange.

En effet, un point d'accès transmet dans ses trames de sonde (*beacon*) des éléments d'information (IE), afin de signaler aux clients 802.11i la liste des protocoles d'authentification supportées, la liste des protocoles de chiffrement des transmissions radio disponibles et la méthode de chiffrement pour la distribution d'une clé de groupe, ceci en plus de la clé de chiffrement unicast (GTK, PTK). Une station 802.11 notifie son choix en insérant un élément d'information dans sa requête d'association. Cette démarche est illustrée par la figure 3.3.

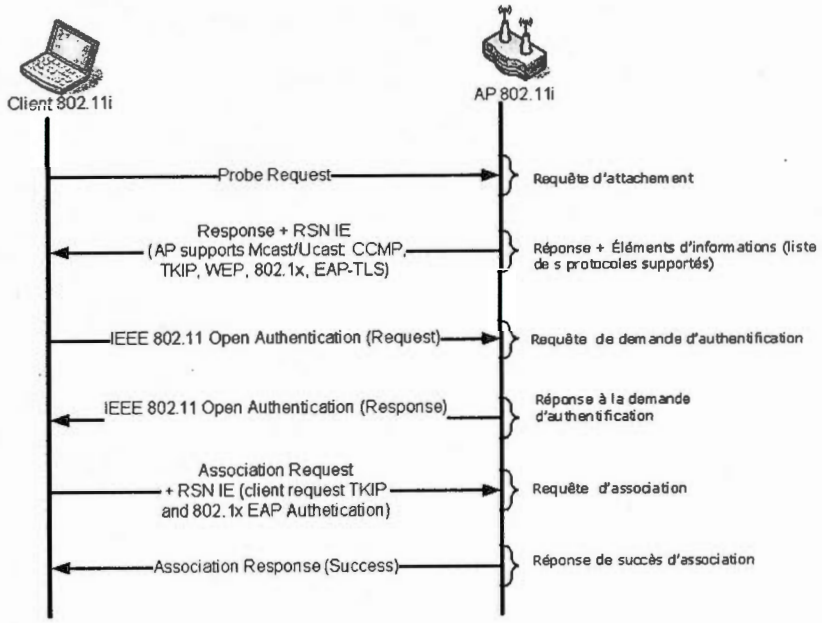


Figure 3.3 : Rattachement au point d'accès [6]

3.3.2.2 Phase 2 : Authentification 802.1x

La seconde phase consiste en l'authentification 802.1X basée sur EAP et la méthode spécifique choisie: EAP-TLS avec certificat client et serveur (nécessitant une infrastructure à clé publique), EAP-TTLS ou PEAP pour des authentifications hybrides (où le certificat est uniquement obligatoire côté serveur).

L'authentification 802.1X est initiée lorsque le point d'accès demande les données d'identification du client, la réponse du client contient alors la méthode d'authentification préférée. Différents messages – dépendant de la méthode spécifique choisie – sont alors échangés par la suite entre le client et le serveur d'authentification afin de générer une clé maîtresse (Master Key – MK). À la fin de l'échange, un message *Radius Accept* est envoyé du serveur d'authentification au point d'accès. Ce message contient la MK ainsi qu'un message final *EAP Success* pour le client.

De plus, à la fin de cette procédure d'authentification mutuelle, le client 802.1x et le serveur d'authentification calculent la clé PMK[25] qui est dérivée de la clé MK. La clé PMK est ensuite transférée du serveur d'authentification vers le point d'accès, par le biais d'un canal sécurisé, établi d'une manière qui dépend encore une fois de la méthode d'authentification choisie.

3.3.2.3 Phase 3 : Distribution et hiérarchie des clés de chiffrement

La sécurité des transmissions repose essentiellement sur des clés secrètes. Avec la norme 802.11i, chaque clé a une durée de vie limitée et de nombreuses clés sont utilisées, organisées selon une hiérarchie. Quand un contexte de sécurité est établi après une authentification réussie, des clés temporaires (de sessions) sont créées et régulièrement mises à jour jusqu'à la fermeture du contexte. La génération et l'échange des clés est le but de cette troisième phase. Deux poignées de main (Handshake) en séquence ont lieu pour dériver les différentes clés:

- le 4-Way Handshake pour la dérivation de la clé PTK (Pairwise Transient Key),
- le Group Key Handshake pour le renouvellement de la clé GTK (Group Transient Key).

Dans ce qui suit, nous donnons plus de détails sur ces deux échanges.

➢ L'échange 4-Way Handshake

Ainsi, une fois la procédure d'authentification mutuelle achevée et la clé PMK calculée et transférée du serveur RADIUS vers le point d'accès, une nouvelle procédure appelée 4-Way Handshake est amorcée entre le client 802.11i et le point d'accès. Le 4-Way Handshake, lancé par le point d'accès, permet :

- la confirmation de la connaissance de la clé PMK par le client,
- la dérivation d'une nouvelle clé PTK,
- l'installation des clés de chiffrement et d'intégrité,
- le transport chiffré de la GTK (après établissement de la nouvelle clé PTK),

---

[25] Pairwise Master Key

À partir de la clé PTK générée, plusieurs autres clés sont dérivées. Ces différentes clés seront utilisées pour assurer différents objectifs de sécurité. Le rôle de chacune des clés est donné dans les sections qui suivent.

La figure 3.4 montre les détails des messages échangés lors de la procédure 4-Way Handshake. Comme son nom l'indique, le 4-Way Handshake comprend quatre messages distincts.

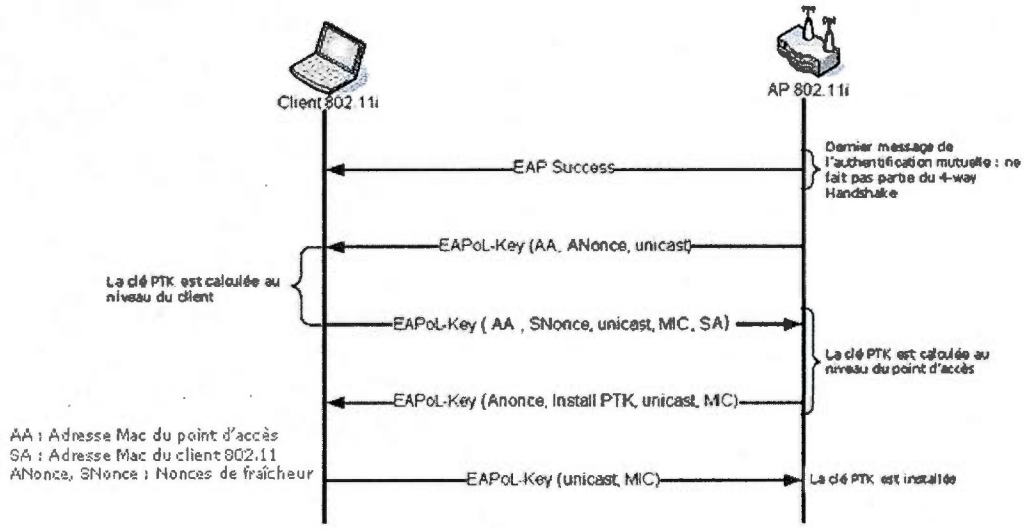


Figure 3.4 : L'échange 4-Way Handshake [6]

Tel qu'illustré à la figure 3.4, une fois la clé PMK générée, la dérivation de la clé PTK se fait en combinant ANonce, SNonce, l'adresse MAC du point d'accès (AA), l'adresse MAC de la station (SA) et la clé PMK, tous fournis comme paramètres à la fonction irréversible PRF (Pseudo-Random Function). La fonction PRF-x( ) retourne, selon les besoins, x bits, x pouvant être égal à 128, 192, 256, 384 ou 512 bits.

Ainsi d'après [9], le calcul de la clé PTK se fait comme suit :

```
PTK = PRF-X (PMK, PAIRWISE KEY EXPANSION, MIN (AA, SA) ||
             MAX (AA, SA) ||
             MIN (ANONCE, SNONCE) ||
             MAX (ANONCE, SNONCE))
                                                    Où
                                                    AA = AUTHENTICATOR ADDRESS
                                                    SA = STATION ADDRESS
                                                    || = Concaténation
```

À la fin du 4-Way Handshake, la clé PTK est générée et un trafic unicast chiffré est établi entre les deux entités. À la suite du 4-Way Handshake, la procédure de génération de la clé de chiffrement multicast GTK est amorcée. Cette procédure est appelée Group Key Handshake ou encore 2-Way Handshake.

➢ L'échange Group Key Handshake

Le point d'accès disposant de la clé de groupe GMK (Group Master Key), un échange à deux passes, ou 2-Way Handshake se déclenche. Ce dernier permet de dériver la valeur de la clé GMK et d'en déduire une clé de groupe temporaire GTK. Ensuite, le point d'accès livre cette clé de manière sécurisée à toutes les cartes réseau des clients authentifiés de la cellule BSS qu'il couvre. Au terme de cette nouvelle procédure de Handshake, illustrée à la figure 3.5, la station peut envoyer du trafic unicast et multicast chiffré.

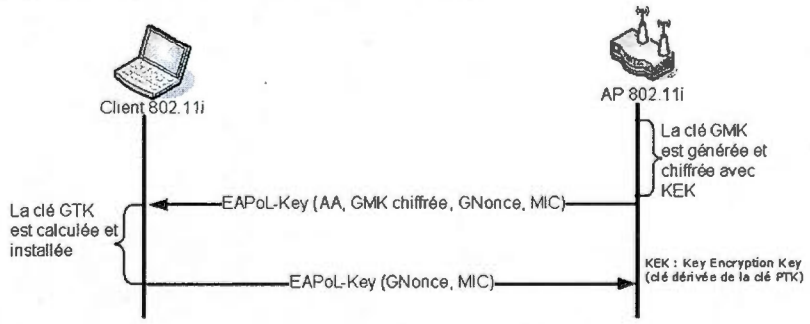


Figure 3.5 : L'échange 2-Way Handshake et la génération de la clé GTK [6]

D'une manière analogue à celle de la dérivation de la clé PTK, la clé GTK s'obtient de la façon suivante : GTK = PRF (GMK, GROUP KEY EXPANSION, MAC_AP, GNONCE)

Les deux phases du Handshake illustré par les figures 3.4 et 3.5 réduisent les chances à tout éventuel attaquant d'usurper la station ou le point d'accès en plus de prévenir les attaques du type homme au milieu [6].

➢ Hiérarchie des clés

Comme indiqué dans les sections précédentes, la norme 802.11i a introduit plusieurs mécanismes d'échanges de clés, engendrant ainsi un grand nombre de clés de chiffrement et d'intégrité, les unes dérivées des autres, créant ainsi une hiérarchie de clés, avec des mécanismes de dérivation différents.

Cette corrélation entre les clés est un atout de la norme 802.11i. En effet, le lien établi entre les différents niveaux (entre les machines à état) empêche les attaques du type détournement de session, homme au milieu, ainsi que les attaques profitant du manque de corrélation et de synchronisation entre les machines à état des entités communicantes dans un réseau sans fil. Dans cette section, nous tentons de dresser un descriptif le plus complet possible de la hiérarchie des clés utilisées et des mécanismes de dérivation utilisés tout au long des étapes d'établissement d'un canal sécurisé entre le client 802.11i et le point d'accès.

Dans les différents échanges prévus par 802.11i, il est nécessaire de chiffrer la plupart des messages au moyen de clés dérivées essentiellement de la clé PMK, elle-même dérivée de la clé MK [6]. La dérivation de la PMK dépend de la méthode d'authentification choisie :

- Si une PSK (Pre-Shared Key) est utilisée, PMK = PSK. La PSK est générée à partir de la phrase secrète (Passphrase composée de 8 à 63 caractères) ou directement à partir d'une chaîne de 256 bits. Cette méthode convient aux particuliers n'ayant pas de serveur d'authentification
- Si un serveur d'authentification est utilisé, la PMK est dérivée de la MK issue de l'authentification 802.1X.

À partir de la clé PMK, on dérive les clés temporaires qui seront utilisées pour le chiffrement radio. La figure 3.6 montre la hiérarchie complète des clés utilisées lors des différents échanges, décrits plus haut dans cette section.

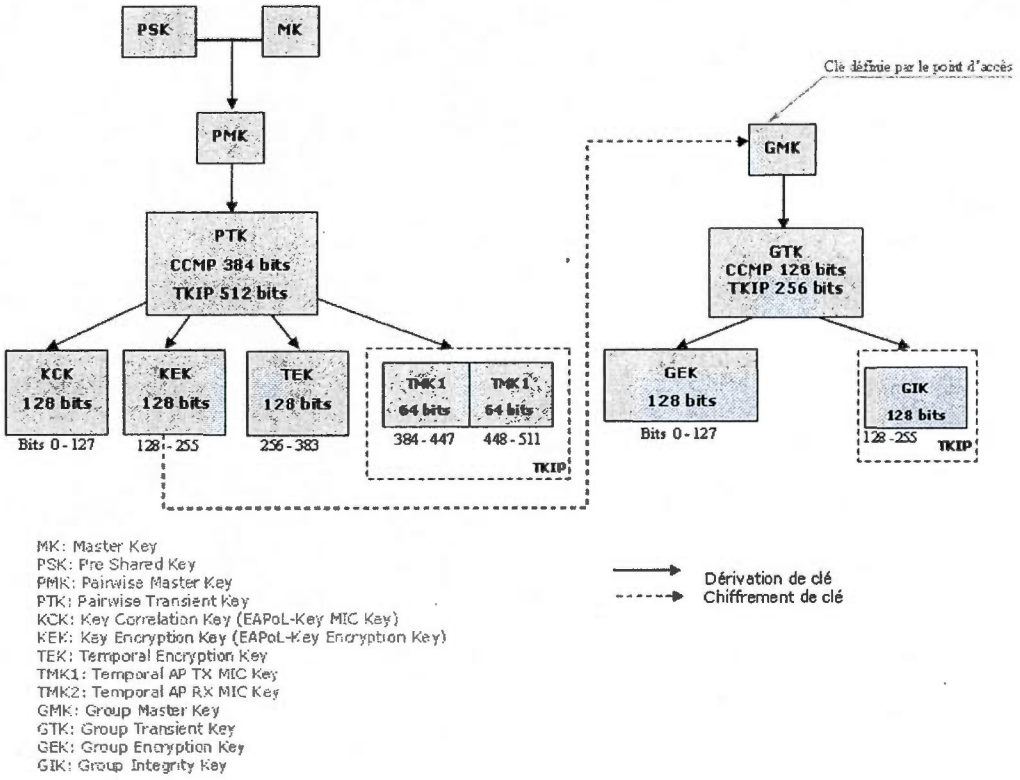


Figure 3.6 : Hiérarchie des clés de chiffrement avec 802.11i

Comme le montre la figure, quasiment toutes les clés sont dérivées à partir de la même clé racine, qui n'est autre que la clé maîtresse MK, ou de la clé PSK, dans le mode ad-hoc. La taille de la PTK dépend du protocole de chiffrement choisi : 512 bits pour TKIP et 384 bits pour CCMP. La PTK se compose de plusieurs clés temporelles dédiées :

- KCK : clé pour authentifier les messages durant le 4-Way Handshake et le Group Key Handshake.
- KEK : clé pour la confidentialité des données durant le 4-Way Handshake et le Group Key Handshake.
- TEK : clé pour le chiffrement des données (utilisée dans TKIP ou CCMP).
- TMK : clé pour l'authentification des données (utilisée seulement dans TKIP). Une clé dédiée est utilisée pour chaque sens de communication.

De même pour la clé GTK, générée à l'aide du protocole à deux passes 2-Way Handshake. La longueur de cette dernière dépend du protocole de chiffrement – 256 bits pour TKIP et 128 bits pour CCMP. La GTK est divisée en des clés temporelles dédiées :

- GEK: clé pour le chiffrement des données (utilisée par CCMP et par TKIP pour l'authentification et le chiffrement).
- GIK: clé pour l'authentification des données (utilisée seulement avec TKIP).

3.3.2.4 Phase 4 : le chiffrement et l'intégrité

Dans cette phase, toutes les clés générées précédemment sont utilisées avec les protocoles tels que TKIP ou CCMP, afin de garantir des échanges sécurisés.

Ainsi dans ce chapitre, nous avons présenté les standards de sécurité pour les réseaux Wi-Fi, en commençant par le mécanisme de chiffrement WEP et en finissant par la toute dernière norme de sécurité Wi-Fi : la 802.11i, en passant par le standard d'authentification 802.1x. Ce que nous pouvons remarquer, c'est que la première génération de standards de sécurité Wi-Fi, avec WEP, était peu sécurisée et que les deuxième (WPA) et troisième générations (802.11i ou WPA2), en cours d'introduction sur le marché, sont susceptibles de mieux satisfaire aux besoins de sécurité des entreprises.

Toutefois, il ne faut pas négliger le fait que pour les entreprises ayant déjà déployé des équipements Wi-Fi, le surcoût engendré par ce renouvellement – dû à l'incompatibilité du 802.11i avec les standards de sécurité préalables – est énorme. Dans le chapitre suivant, nous présentons une étude détaillée sur les attaques que les réseaux Wi-Fi font l'objet.

CHAPITRE IV

ANALYSE DES FAILLES ET DES ATTAQUES DANS LES RÉSEAUX WI-FI

Dans ce chapitre, nous présentons une étude détaillée des vulnérabilités des protocoles de sécurité que nous avons passés en revue au chapitre précédent. Ainsi, ce chapitre se concentre sur les faiblesses de chaque protocole et les types d'attaques qu'il est possible de monter en tirant profit de ces vulnérabilités.

Nous détaillons les attaques relatives à chaque protocole de sécurité Wi-Fi. Nous présentons également un éventail d'outils d'attaques disponibles avec leurs diverses fonctionnalités et exposons les démarches adoptées afin de mettre en œuvre ces attaques. Ce chapitre constitue notre première contribution en avançant une vue d'ensemble originale des attaques contre les réseaux Wi-Fi.

4.1 Faiblesses et contournements des mécanismes préliminaires de sécurité

Avant d'aborder les failles de sécurité des protocoles que nous avons présentés au chapitre 3 (WEP, 802.1x,...), nous présentons dans cette section la première ligne de défense préliminaire des réseaux Wi-Fi, tel que l'utilisation d'ESSID fermés, le filtrage par adresse MAC, ainsi que le filtrage par protocoles.

4.1.1 Utilisation d'ESSID fermés

Afin d'accéder à tout réseau Wi-Fi, il est nécessaire de connaître son identifiant, c'est-à-dire son ESSID. Au début du développement des réseaux Wi-Fi, l'ESSID était transmis en clair périodiquement par le point d'accès dans des trames balises (beacon frames). De cette façon, il était très facile de s'associer avec n'importe quel réseau Wi-Fi, en récupérant

l'ESSID à l'aide d'un renifleur (sniffer) qui permet de récupérer tout le trafic réseau qui circule. De nombreux outils de surveillance et d'analyse de trafic pour les réseaux sont disponibles sur Internet. Parmi les plus célèbres, citons *Kismet*, *AirTraf*, *Mogne* et *WifiScanner* [11].

Afin de parer à cette faiblesse, une nouvelle fonctionnalité a été mise en place. Elle permet d'éviter que l'ESSID ne soit transmis en clair sur le réseau. Ce mécanisme, appelé *Closed Network*, ou réseau fermé, interdit la transmission de l'ESSID par l'intermédiaire de trames balises [6]. Ainsi, pour s'associer à un réseau Wi-Fi implémentant un ESSID fermé, il est indispensable d'entrer l'ESSID à la main. Toutefois, même avec la mise en place d'un tel mécanisme, l'ESSID est transmis quand même en clair durant la phase d'association d'un client légitime à son point d'accès. Ainsi, pour contourner ce mécanisme de défense préliminaire, il suffit d'écouter le trafic réseau durant la phase d'association d'un client légitime et de récupérer l'ESSID en clair.

Outre cette vulnérabilité, l'ESSID est préconfiguré par défaut sur les équipements par les constructeurs de matériels. Par exemple, l'ESSID par défaut est WLAN pour les équipements Dlink, Linksys pour les points d'accès Linksys, Tsunami pour les équipements Cisco, etc.

Cet ESSID par défaut est très rarement modifié par les utilisateurs. Ainsi, il suffit de connaître la marque du point d'accès pour accéder au réseau en utilisant l'ESSID par défaut. Pour trouver la marque du point d'accès, il suffit de lire les trois premiers octets de l'adresse MAC du point d'accès cible (les trois premiers octets de toute adresse MAC sont toujours réservés à la marque de l'équipement).

4.1.2 Filtrage par adresse MAC

Outre l'utilisation de l'ESSID fermé, les points d'accès permettent d'établir un filtrage par adresse MAC, ou encore des listes de contrôle d'accès (ACL). Ainsi, le point d'accès autorise uniquement les stations ayant une adresse MAC qui figure dans la liste ACL.

La première vulnérabilité de ce filtrage est qu'il s'agit d'un mécanisme optionnel, rarement activé dans les faits. Outre cette vulnérabilité, le filtrage par adresse MAC peut être facilement contourné, en usurpant l'adresse MAC d'un hôte légitime du réseau cible.

En effet, il suffit à un attaquant d'écouter le trafic du réseau cible et d'identifier les adresses MAC des hôtes légitimes, car elles transitent en clair. Une fois qu'un client cible est identifié par l'attaquant, il suffit alors d'usurper son adresse MAC (quasiment toutes les cartes sans fil permettent le changement d'adresses MAC) et de s'associer au point d'accès. Avant de pouvoir s'associer au point d'accès, il faut soit attendre que le client légitime se déconnecte du réseau, soit l'obliger à le quitter.

Pour obliger un client légitime à se désassocier du réseau auquel il est rattaché, il suffit d'usurper l'adresse MAC du point d'accès et inonder le client victime de trames de désassociation. Une fois le client légitime désassocié, il est possible de s'associer au réseau à sa place sans problèmes.

Pour réaliser en pratique cette attaque, l'attaquant doit de se doter de deux cartes réseaux sans fil. La première servira à maintenir l'attaque DoS sur le client légitime en le bombardant de trames de désassociation, la seconde interface permet d'usurper l'adresse MAC du client légitime et de s'associer avec le point d'accès. Pour réaliser l'attaque DoS sur le client cible, l'attaquant peut utiliser des outils tels que *Wlan_jack* ou *File2air* sous Linux.

4.1.3 Filtrage par protocoles

Outre le mécanisme d'ESSID fermés et le filtrage par adresse MAC, le filtrage par protocoles constitue un des éléments de la première ligne de défense préliminaire des réseaux Wi-Fi. En effet, ce mécanisme consiste à n'autoriser qu'un ensemble bien défini de protocoles sur le réseau [11].

Certes, il est vrai que le contournement de ce type de filtrage est plus difficile à réaliser que les filtrages précédents. Toutefois, très peu d'équipements sur le marché permettent la mise en œuvre d'un tel mécanisme de filtrage. En fait, il s'agit d'équipements haut de gamme très coûteux, destinés à un usage très spécifique dans lesquels l'activité de l'utilisateur est

limitée à un ensemble d'opérations bien définies à l'avance tel que la navigation via HTTPS sur un site d'entreprise ou l'envoi de courriels, avec une application de courriel bien particulière. Bref, très peu d'équipements permettant la mise en œuvre d'un tel mécanisme de filtrage sont effectivement déployés.

Les attaques contre les réseaux implémentant ce mécanisme de filtrage sont dirigées contre le protocole de sécurité autorisé lui-même. En effet, si les concepteurs du réseau ont opté pour HTTPS et SSH[26] comme protocoles autorisés, les attaquants pourraient monter des attaques contre ces protocoles, en s'aidant des outils tel que *sshow* pour découvrir la longueur des mots de passe ainsi que les commandes utilisées avec le trafic SSHv1 et SSHv2, ou encore les utilitaires *sshmitm* et *Webmitm*, qui permettent de mettre en place des attaques de type homme au milieu pour du trafic SSH et HTTPS.

Les attaquants peuvent également avoir recours à des attaques DoS contre SSH, moyennant des outils tels que *guess-who*, *ssh-crack*, *ssh-brute*, etc. [11].

Nous n'entrerons pas plus dans les détails des attaques sur le mécanisme de filtrage par protocoles, étant donné que c'est un mécanisme qui n'est pas très répandu et est réservé à un usage très spécifique et limité. De plus, les attaques contre ce type de filtrage dépendent étroitement des protocoles autorisés, qui peuvent être assez nombreux. Pour plus de détails relatifs aux attaques sur ce mécanisme de filtrage, le lecteur pourra consulter [11].

4.2 Les failles du protocole WEP

Dans cette section, nous présentons en premier lieu les faiblesses d'ordre conceptuel du protocole WEP. Ensuite, nous passons au volet des attaques, en explicitant les démarches et les techniques utilisées.

---

26 Secure Shell

4.2.1 Les faiblesses conceptuelles du protocole WEP

Le protocole WEP constitue le premier protocole de sécurité des réseaux Wi-Fi. Toutefois, depuis sa sortie ce standard n'a cessé de créer la polémique autour de lui, à cause de plusieurs défaillances et vulnérabilités inhérentes à sa conception.

L'ensemble des mécanismes de sécurité du WEP comportent des faiblesses. Les failles ne sont pas tant liées à l'algorithme de chiffrement RC4 qu'à la façon dont les mécanismes sont mis en œuvre, comme le vecteur d'initialisation ou le contrôle d'intégrité. Chacun de ces mécanismes comporte des défauts, qui ajoutés les uns aux autres, permettent de casser le WEP.

Dans ce qui suit, nous montrons les défaillances de WEP inhérentes à sa conception. Ensuite, nous montrons dans le volet des attaques sur WEP comment ces vulnérabilités conceptuelles ont été exploitées afin de monter des attaques.

4.2.1.1 Mécanisme défaillant de génération des clés WEP : RC4

Le standard comporte une faille profonde, qui est intrinsèquement liée à l'utilisation de l'algorithme de chiffrement RC4. La clé utilisée par RC4 dans WEP est une concaténation de l'IV (Initialization Vector) et de la clé secrète partagée. Il existe des classes de clés RC4 faibles, dans lesquelles un motif dans les trois premiers octets de la clé engendre un motif équivalent décelable dans les premiers octets de la suite chiffrante, ou KeyStream (KS).

En effet, parmi les IVs utilisés pour composer la clé RC4 du WEP, certains ont des valeurs dites résolvantes. Environ 60 IVs ayant des valeurs résolvantes suffisent à retrouver un octet du secret partagé (PSK).

Cette faille facilite la déduction de la clé par des attaques statistiques, en interceptant le maximum de trames chiffrées avec une classe spécifique d'IV. Le KeyStream obtenu avec ces IV révèle des informations sur la clé secrète PSK. En traitant suffisamment de paquets chiffrés, un attaquant peut la déterminer complètement. C'est cette faille qui est exploitée par l'outil AirSnort pour casser des clés WEP.

Il est à noter qu'une minorité d'équipementiers ont corrigé cette défaillance sur leur matériel, en retirant les vecteurs d'initialisation, dits résolvants. Toutefois, dans la majorité des cas, cette faille persiste, à la grande joie des attaquants.

4.2.1.2 Collision de vecteurs d'initialisations

Outre la faiblesse du mécanisme de génération des clés avec RC4, WEP utilise des vecteurs d'initialisations de 24 bits pour réaliser une différenciation de chiffrement (sans IV, toutes les trames seront chiffrées avec la même clé), vu que c'est la même clé secrète de 40 ou 104 bits qui est utilisée par toutes les stations de la même cellule (les clés WEP de 40 bits ne sont quasiment plus employées actuellement).

L'utilisation des vecteurs d'initialisation telle qu'elle est réalisée avec le chiffrement WEP présente deux vulnérabilités. D'abord, la taille de ces vecteurs d'initialisation, qui n'est que de 24 bits.

En effet, la clé secrète partagée (PSK) définie dans le WEP est statique et ne change pratiquement jamais. L'IV est concaténé avec cette clé de façon à créer des flux de chiffrement différents. L'IV étant sur 24 bits, il peut y avoir jusqu'à 2^{24}, soit exactement 16777216 clés différentes. Après les 2^{24} transmissions chiffrées, il y aura une réinitialisation des IVs et la même séquence d'IV sera réutilisée, causant une collision (2 trames chiffrées avec la même clé WEP : même IV et même PSK). Ainsi, il y aura une réutilisation des mêmes flux de chiffrement, puisqu'il s'agit des mêmes IVs et de la même clé secrète partagée qui ne change pas. Selon [6], la probabilité de casser l'algorithme est proportionnelle à l'augmentation du nombre de collisions d'IVs.

Si l'on prend pour hypothèse que le trafic dans un réseau est constant, avec un débit de 11Mbps, et que la taille moyenne d'une trame est de 1500 octets, le simple calcul suivant montre qu'il suffit d'écouter le trafic réseau pendant juste cinq heures pour tomber sur une collision de vecteurs d'initialisation :

Délai moyen d'émission d'une trame: 1500 octets * 8 bits *1/11 Mbps = 0,00109 s
→ Cela signifie qu'une trame est envoyée toutes les 1,09 ms

Délai d'émission de 2^{24} trames : 0,00109 s * 2^{24} = 18287,16544 s ≈ 5 h

La seconde vulnérabilité relative à l'utilisation des vecteurs d'initialisation dans WEP est la transmission en clair du vecteur d'initialisation utilisé pour le chiffrement. En effet, il suffit d'écouter le trafic pendant un certain temps, pour se constituer progressivement un ensemble de trames chiffrées avec le même IV et donc la même suite chiffrante KS.

Ensuite, l'attaquant pourra procéder comme suit :

Réaliser un XOR entre deux trames chiffrées avec le même IV :

$C1 = P1 \oplus KS$, ou $KS = RC4(IV \| K)$

$C2 = P2 \oplus KS$

$C1 \oplus C2 = (P1 \oplus KS) \oplus (P2 \oplus KS) = P1 \oplus P2 \oplus KS \oplus KS$

On obtient : $\mathbf{C1 \oplus C2 = P1 \oplus P2}$

→ Il ne reste plus qu'à dissocier les deux textes en clair

Une première solution qui pourrait venir à l'esprit pour corriger le problème de collision des vecteurs d'initialisions est d'augmenter la taille des IV. Toutefois, cette dernière n'est pas une solution fiable, vu qu'un réseau modérément occupé peut épuiser l'espace des IVs. Une seconde solution serait de changer la clé secrète partagée, à toutes les 2^{24} trames, afin d'éviter la collision. Malheureusement, le protocole WEP tel qu'il a été conçu ne comprend aucun mécanisme central de mise à jour de cette clé secrète.

4.2.1.3 Contrôle d'intégrité inadapté

Généralement en sécurité, un contrôle d'intégrité est assuré par des fonctions non linéaires, à sens unique et sans brèche tel que les fonctions de hachage (MD5, SHA1, etc.). Ces fonctions de hachage très performantes permettent, à partir d'un message donné, de générer une empreinte quasiment irréversible. Une des principales propriétés de ces fonctions est certainement la non-linéarité.

Le contrôle d'intégrité dans WEP est réalisé par la fonction CRC32. Le CRC sert plutôt à la détection d'erreur, mais n'a jamais été considéré cryptographiquement sûr pour le contrôle d'intégrité, principalement à cause de sa linéarité.

Ainsi, un attaquant pourra exploiter cette faiblesse en s'immisçant dans un dialogue entre un client et un point d'accès, intercepter des trames, modifier leur contenu et changer les CRCs correspondants, en y répercutant les modifications opérées et renvoyer ensuite ces trames au récipiendaire légitime. Ce dernier ne pourra détecter ni altération des messages ni tentative d'attaque. Cette attaque sera abordée plus en détail dans la section relative aux attaques WEP.

4.2.1.4 Clé unique : taille faible et gestion statique

Le standard d'origine définit une taille de clé de 40 bits. Cette clé étant d'une taille insuffisante pour contrer les attaques par force brute, les normalisateurs l'ont augmentée à 104 bits, pour ce que l'on appelle WEP2. Toutefois, cela ne résout pas le problème, surtout avec les puissances de calcul de plus en plus grandes, ainsi que les attaques inductives qui injectent du trafic dans le réseau afin de minimiser le temps nécessaire pour casser une clé WEP. Nous nous attarderons sur ce type d'attaque dans les sections qui suivent.

Outre l'insuffisance de la taille de la clé, le protocole WEP ne prévoit pas de mécanisme de mise à jour ou de génération et de distribution dynamique de la clé secrète partagée. En effet, la gestion des clés est statique et manuelle, une seule clé secrète est partagée par toutes les stations du réseau et le point d'accès. Ainsi, cette clé demeure quasiment inchangée, ce qui a pour incidence de débarrasser l'attaquant de la contrainte de temps. En effet, l'attaquant pourrait récupérer les données chiffrées et se constituer jour après jour une base de données des éléments chiffrés et réaliser des analyses sans contrainte de temps, vu que la clé demeure inchangée.

Cette défaillance de WEP ouvre la voie aux attaques par force brute, ainsi que les attaques par rejeux.

4.2.2 Les attaques contre le protocole WEP

Le protocole WEP n'ayant pas été créé par des experts en sécurité ou du monde de la cryptographie, il a montré des faiblesses depuis sa sortie. En effet, WEP était mort avant même sa sortie, vu qu'il se basait sur l'algorithme de chiffrement en mode flux : RC4, qui a

fait l'objet d'une étude montrant ses vulnérabilités en 1995 par *David Wagner* (4 ans avant la sortie du WEP). Depuis cette étude, plusieurs études ont révélés les défaillances du WEP et les cryptanalystes s'en sont donné à cœur joie à monter des attaques contre ce protocole, qui ne satisfait en rien ses objectifs de sécurité [9]. Le tableau 4.1 montre la chronologie de la mort du WEP.

Date	Description
Septembre 1995	Vulnérabilité potentielle dans RC4 (Wagner).
Octobre 2000	Première publication sur les faiblesses du WEP: "Unsafe at any key size: An analysis of the WEP encapsulation" (Walker).
Mai 2001	Attaque inductive: "An inductive chosen plaintext attack against WEP/WEP2" (Arbaugh).
Juillet 2001	Attaque bit flipping sur le CRC32: "Intercepting mobile communications: the Security of the 802.11" (Borisov, Goldberg, and Wagner).
Août 2001	Attaque FMS: "Weakness in the key scheduling Algorithm of RC4" (Fluhrer, Mantin, and Shamir).
Août 2001	Sortie de l'outil AirSnort, implémentant l'attaque FMS.
Février 2002	Optimisation de l'attaque FMS par David Hulton (h1kari).
Août 2004	Attaque de KoreK (IVs uniques) - Sortie de chopchop.
Juillet/Août 2004	Sortie des outils AirCrack (C. Devine) et WepLab (J.I. Sanchez), implémentant l'attaque de KoreK.

Tableau 4.1 : Chronologie de la mort du WEP

Ainsi, chacune des faiblesses conceptuelles présentées dans la sous section précédente a été exploitée afin de bâtir des attaques. Ces attaques ont été améliorées et optimisées au fil du temps, pour donner aujourd'hui une panoplie d'outils très efficaces les implémentant. Dans les sous sections qui suivent, nous allons expliciter les plus importantes classes d'attaques, ainsi que les meilleurs outils les mettant en œuvre.

4.2.2.1 Attaque par force brute

Puisque le protocole WEP base sa sécurité sur le secret de la clé utilisée, une des attaques les plus simples à mettre en œuvre est certainement l'attaque par force brute. En effet, avant de passer à des attaques utilisant des outils sophistiqués d'attaques statistiques, un attaquant peut tenter de casser la clé WEP en opérant des attaques par force brute. Ces

attaques ne sont pas nécessairement moins efficaces que les autres approches exploitant des failles conceptuelles du protocole et mettant en œuvre des techniques statistiques élaborées.

La raison première pour laquelle ce type d'attaques réussit facilement est que la majorité des utilisateurs choisissent des clés de chiffrement WEP faibles d'autant plus que les équipementiers n'intègrent pas dans leurs matériels des fonctions de contrôle de validité et de robustesse des clés choisies par l'utilisateur. Ce manque de rigueur dans le choix de la clé WEP fait qu'un grand nombre de réseaux sans fil sont vulnérables à des attaques par force brute ou des attaques par dictionnaire.

Commençons par les attaques par force brute, dont le principe le plus simple est d'essayer toutes les clés binaires possibles pour une clé WEP donnée. Ce procédé est quasiment impossible pour des clés d'une taille de 128/104bits (2^{104} clés possibles), mais réussit quand même pour des clés WEP de 64/40 bits. Néanmoins, on peut monter une attaque par force brute distribuée, sur plusieurs ordinateurs, afin de multiplier la puissance de calcul et diminuer le temps nécessaire au cassage de la clé. Selon [11], une attaque par force brute contre des clés d'une taille de 40 bits peut nécessiter jusqu'à 50 jours, en se servant d'une seule machine de type Pentium III [12]. Cela nous amène à dire que l'utilisation des clés WEP de 128/104bits, constitue une bonne parade contre ce type d'attaques. L'attaque par force brute serait quasiment impossible si en plus d'une clé de 128 bits, il y avait un mécanisme de mise à jour des clés secrètes PSK, selon une fréquence choisie judicieusement (doit dépendre du temps nécessaire pour casser la clé PSK).

Il existe une panoplie d'outils implémentant des attaques par force brute, les plus performants étant *WepLab* et *dWepCrack* [12].

Pour monter des attaques par dictionnaire, l'attaquant devra avoir une connaissance du matériel déployé dans le réseau cible. En effet, il faut tenir compte de la méthode utilisée pour la transformation de la clé WEP en clé binaire. Ces méthodes sont au nombre de deux : la première et la plus commune se base sur l'utilisation de la fonction de hachage MD5, la seconde, moins fréquente, utilise la méthode « *Null terminated raw ASCII* ».

Les meilleurs outils permettant de mettre en œuvre des attaques par dictionnaires sur WEP sont *WepLab* et *WepAttack* [13]. Ils peuvent être couplés à des utilitaires de génération de dictionnaire tel que l'outil *John the Ripper*, qui en plus de générer des dictionnaires, offre des fonctionnalités de variation (jeu de majuscules/minuscules, ajout de terminaisons et plusieurs combinaisons de chiffres et lettres aux mots du dictionnaire, etc.).

Les attaques par force brute et par dictionnaires sont des attaques purement passives dans le sens où elles n'impliquent ni altération du contenu des messages, ni déni de service, ni de rejeu de paquets dans le réseau cible ou encore de mascarade, comme dans le cas des attaques de l'homme au milieu.

4.2.2.2 Attaque inductive à texte clair connu: injection de trafic

Il s'agit d'une attaque active mise en place par W.Arbaugh [14]. Cette attaque se base sur l'injection de trafic dans le réseau. En effet, elle tire profit des faiblesses de WEP au niveau du chiffrement en mode flux utilisé avec RC4, ainsi que des collisions d'IV et de l'absence d'un mécanisme anti rejeu (deux trames avec le même IV peuvent se trouver sur le réseau). Cette attaque se décompose en trois phases :

Phase 1: Récupération des *n* premiers octets de la suite chiffrante (*KeyStream*)

L'objectif de cette phase est de récupérer les n premiers octets du KeyStream relatif à un IV donné. Pour cela, l'attaquant doit tirer profit des structures de protocoles réseau connus, comme par exemple les messages des protocoles DHCP[27] ou SNAP[28], qui constituent l'entête de la trame 802.11. En effet, l'attaquant peut deviner le texte en clair correspondant à ces structures de protocoles chiffrées, vu qu'elles sont formées de champs prévisibles et facilement identifiables, tel que l'entête IP et une partie de l'entête UDP.

---

27 Dynamic Host Configuration Protocol
28 Sub Network Access Protocol

Ainsi, une fois que l'attaquant dispose d'une partie de la trame 802.11 cryptée et en clair, il peut utiliser la propriété du XOR de RC4 afin de déterminer le KeyStream correspondant. Pour cela, l'attaquant procède comme suit :

Soit
C : données chiffrées
P : données en clair
KS : KeyStream

On sait que $C = KS \oplus P$

En ajoutant P de chaque côté de l'égalité, on obtient :

$C \oplus P = KS \oplus P \oplus P$

$\rightarrow KS = C \oplus P$

Dans notre cas, P correspond aux parties facilement identifiables de la trame 802.11, correspondant aux structures de protocoles. En effet, il ne s'agit pas de toute la trame 802.11. Ainsi, grâce aux propriétés du XOR, il suffit de récupérer les données en clair et les données chiffrées associées pour récupérer le flux de chiffrement KS correspondant.

Au final de cette première phase, l'attaquant dispose d'un pseudo KeyStream, relatif au chiffrement d'une partie d'une trame 802.11 donnée, avec un IV donné.

La séquence logique de cette attaque serait de découvrir la totalité du KeyStream relatif à cet IV, afin de pouvoir déchiffrer n'importe quelle trame chiffrée, employant ce même IV. C'est le but de la seconde phase de cette attaque.

Phase 2: Découverte de la totalité de la suite chiffrante (*KeyStream*)

Dans un réseau sans fil, un point d'accès n'accepte un paquet WEP chiffré que si son ICV[29], réalisé par la fonction de détection d'erreur CRC32, est calculé correctement. La taille du champ ICV est de 4 octets. D'un autre côté, l'attaquant dispose d'un pseudo KeyStream de taille n (résultat de la première phase). Ainsi, l'attaquant procède comme suit :

---

29 Integrity Check Value

1. Générer un message de longueur n-3 octets (ce message doit entraîner une réponse prévisible, s'il est considéré comme valide par le point d'accès, par exemple un DHCP REQUEST).

2. Calculer l'ICV (4 octets) relatif à ce message et ne considérer que les 3 premiers octets.

3. Concaténer le message de longueur n-3 et les 3 premiers octets de l'ICV calculé (on aura un message d'une taille de n octets, qui est la taille de notre pseudo KeyStream).

4. Transmission d'un message d'une taille de n+1 octets : les n octets de l'étape précédente, suivis d'un octet supplémentaire construit par recherche exhaustive. L'attaquant répétera cette étape en balayant toutes les 255 valeurs possibles pour ce dernier octet, jusqu'à l'obtention d'une réponse du réseau, indiquant la validité de l'ICV ainsi construit.

5. Réaliser l'opération XOR entre le $4^{ème}$ octet de l'ICV calculé à l'étape 2 et le $(n+1)^{ème}$ octet transmis à l'étape 4. la valeur résultante est le $(n+1)^{ème}$ octet du KeyStream.

   Par analogie à $KS = C \oplus P$

   On a:

   $KS[n+1] = Message[n+1] \oplus ICV[4]$

6. Répéter les étapes de 1 à 5, en incrémentant de 1 octet la taille du message généré à l'étape 1, jusqu'à trouver le KeyStream au complet.

La figure 4.1 résume les étapes décrites ci-dessus.

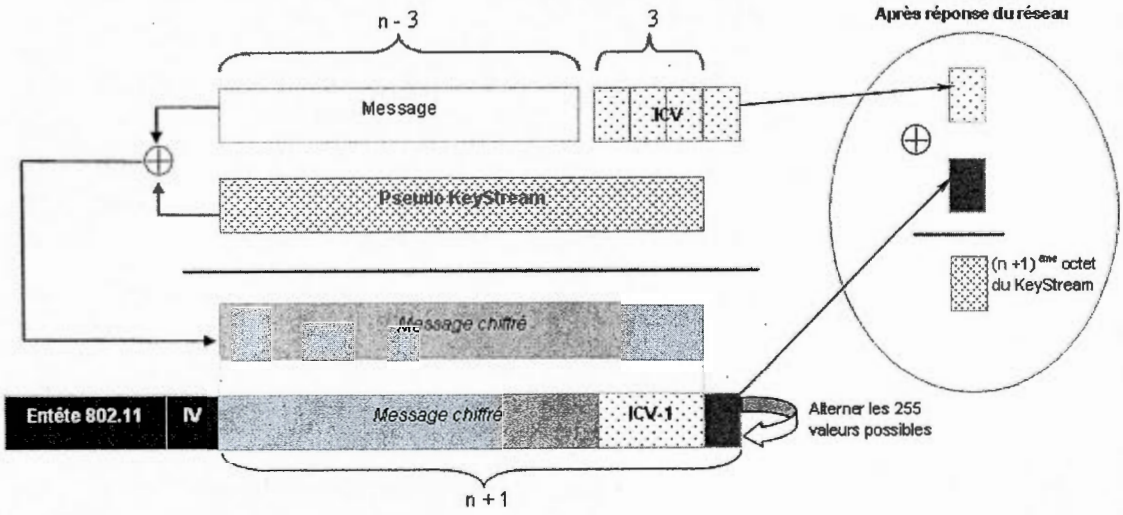


Figure 4.1 : Processus de découverte du KeyStream

Phase 3: Construction de la table de correspondance

Une fois que l'attaquant dispose d'un KeyStream complet pour un IV particulier, il devient possible d'injecter au réseau des paquets chiffrés en utilisant ce même IV. Au bout de cette dernière phase, l'attaquant disposera d'une table de correspondance complète, entre IV et KeyStream correspondant.

Pour ce faire, l'attaquant pourra envoyer des requêtes chiffrées avec le KeyStream dont il dispose, engendrant des réponses prévisibles de la part du réseau [14]. En récupérant les réponses à ses requêtes, l'attaquant utilisera la propriété de l'opérateur XOR, utilisé auparavant lors de la phase 2, à savoir : $KS = C \oplus P$ (l'attaquant reçoit C du réseau et devine P, car réponse prévisible à sa requête). Ceci permet de trouver de nouveaux KeyStream, relatifs à d'autres IVs.

À la fin de cette attaque, l'attaquant sera dans la possibilité de déchiffrer tous les paquets transitant sur le réseau, vu qu'il dispose de tous les KeyStream (2^{24} KeyStream). La seule condition pour empêcher cette attaque est la mise en place d'un mécanisme de

changement de clés secrètes PSK permettant de mettre à jour la clé au plus à tous les 2^{24} paquets.

4.2.2.3 Attaque bit flipping sur le CRC

L'attaque bit flipping tire profit de la faille conceptuelle de WEP inhérente au contrôle d'intégrité qui se fait au moyen de la fonction CRC32. Il s'agit d'une attaque active, vu qu'elle vise à apporter des modifications illicites dans les trames 802.11 du réseau Wi-Fi cible.

C'est en Juillet 2001, que *Borisov*, *Goldberg* et *Wagner* publient leur attaque dans [15], intitulée *«Bit Flip»*, qui permet de modifier des parties d'un message chiffré avec le WEP sans que le récepteur ne décèle d'erreur. En effet, cette attaque se base sur la propriété de linéarité du CRC, avec l'opérateur XOR. Du fait que RC4 utilise l'opérateur XOR, un attaquant peut modifier arbitrairement le message chiffré tout en maintenant un CRC valide.

Ainsi, d'après [15] le principe de l'attaque est comme suit :

On sait que :

$C = (M \| ICV(M)) \oplus RC4(K \| IV)$

Soit C' les données chiffrées, C' s'écrit : $C' = (M' \| ICV(M')) \oplus RC4(K \| IV)$

Avec M' : les données modifiées par l'attaquant de la façon qui suit

$M' = M \oplus \Delta$

On ajoute par un XOR à C la modification Δ, que l'on souhaite apporter aux données concaténées et à leur ICV. On obtient :

$C \oplus (\Delta \| ICV(\Delta)) = (M \| ICV(M)) \oplus (\Delta \| ICV(\Delta)) \oplus RC4(K \| IV)$

Ce qui équivaut à :

$C \oplus (\Delta \| ICV(\Delta)) = (M \oplus \Delta) \| (ICV(M) \oplus ICV(\Delta)) \oplus RC4(K \| IV)$

De par les propriétés du CRC, cela équivaut à :

$C \oplus (\Delta \| ICV(\Delta)) = (M \oplus \Delta) \| (ICV(M \oplus \Delta)) \oplus RC4(K \| IV)$

Soit :

$C \oplus (\Delta \| ICV(\Delta)) = (M' \| (ICV(M')) \oplus RC4(K \| IV)$

$\rightarrow C \oplus (\Delta \| ICV(\Delta)) = C'$

Comme le montre l'attaque, il est assez facile de modifier le contenu d'une trame tout en validant son intégrité. Ainsi, au lieu d'écouter passivement le réseau, il est possible de modifier les données afin de rediriger le trafic vers une autre machine, ceci juste en modifiant l'adresse IP de destination. Toutefois, pour réussir cette attaque, l'attaquant devra avoir une certaine connaissance des données chiffrées.

4.2.2.4 Attaque FMS

Une des attaques les plus célèbres pour craquer la clé WEP est certainement l'attaque FMS, du non de ses créateurs *Fluhrer*, *Mantin* et *Shamir*. L'attaque FMS est une attaque passive dans le sens où elle n'influe pas sur le comportement du réseau cible. En effet, FMS est une attaque cryptanalytique statistique apparue en 2001. FMS a d'abord été mise en œuvre dans l'outil *Wep_Crack*, puis dans *AirSnort*.

Cette attaque exploite deux failles majeures :

- Faiblesses RC4 : l'utilisation de certains IVs, dits faibles, permettent de révéler quelques bits de la clé secrète partagée. Ceci en plus d'une faiblesse au niveau de l'algorithme KSA[30], implémenté dans RC4. Cette dernière, dite faiblesse d'invariance, permet de déterminer les octets de clé les plus probables, parmi les octets du flux de sortie de RC4.

- Les quatre premiers octets du flux de sortie de RC4 sont toujours prévisibles, car ils contiennent l'entête du protocole SNAP.

Il est à signaler que nous n'allons pas aborder les détails cryptographiques et statistiques de cette attaque, vu leurs relatives complexité et abondance. De plus, les détails cryptographiques dépassent largement le contexte de ce mémoire. Toutefois, nous allons expliciter les principes sur lesquels est fondée cette attaque. Nous montrons également le degré de son efficacité et les conditions de succès.

---

30 Key Scheduling Algorithm

L'algorithme de chiffrement RC4 est en réalité composé de deux algorithmes qui travaillent en séquence (voir figure 4.2) : KSA et PRGA[31].

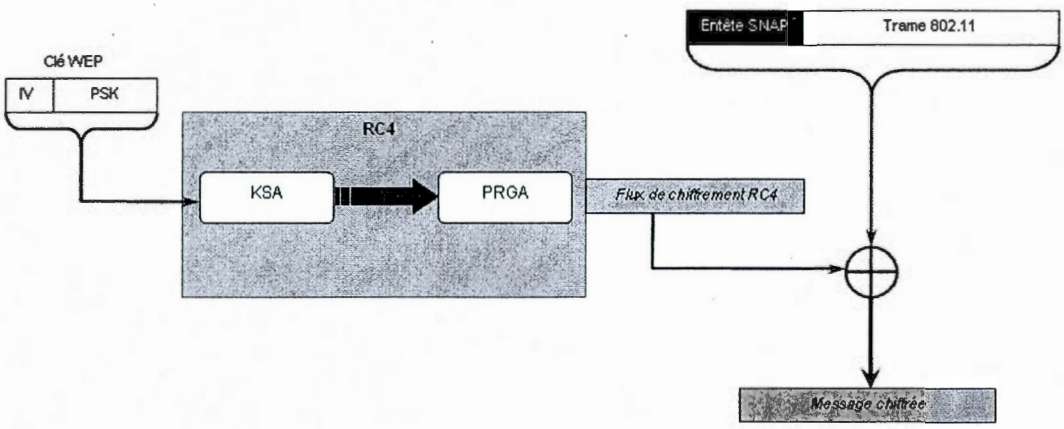


Figure 4.2 : Chiffrement RC4

L'algorithme KSA réalise une opération de brouillage de la clé WEP, qui une fois brouillée sera donnée en entrée à l'algorithme PRGA, qui réalise une suite d'opérations de permutations et génère une séquence pseudo-aléatoire, qui n'est autre que le flux de chiffrement RC4 (*KeyStream*). L'attaque FMS exploite une faiblesse dans l'algorithme KSA.

Cette faiblesse est que certains IVs faibles initialisent la fonction de brouillage de KSA de façon à générer une séquence de bits qui comprend plusieurs bits de la clé secrète PSK. Ensuite, cette même séquence sera relayée à l'algorithme PRGA, qui donnera un flux de chiffrement (*KeyStream*), dont le premier octet est celui de la clé PSK. Ce dernier est ensuite transformé par un OU-exclusif (XOR) avec une donnée prévisible (l'entête SNAP). De cette manière, il est assez facile d'extraire le premier octet du flux de chiffrement, afin d'obtenir l'octet de la clé PSK.

---

31 Pseudo Random Generation Algorithm

Remarque :

Un IV faible est de la forme, dite résolvante, suivante : **(A+3, N-1, X)**
où
A : Octet quelconque de la clé secrète PSK.
N : Taille de la boite de permutation (S-box) utilisée au niveau de KSA et PRGA.
X : Un nombre aléatoire.

L'attaque FMS permet de détecter les IV faibles, ayant une forme résolvante. Une fois ces IVs détectés, une série d'analyses statistiques sont effectuées sur le flux de chiffrement correspondant afin de déterminer si le premier octet appartient à la clé secrète. Pour casser une clé WEP à l'aide de l'attaque FMS, il est nécessaire d'analyser un grand nombre de paquets (selon [16], environ huit millions de paquets) pour déterminer la clé WEP.

Cette même attaque a été améliorée par David Hulton en 2002, qui a analysé la forme des IV faibles et leur relation avec les octets de la clé secrète [17]. L'étude réalisée a permis d'améliorer la performance de l'attaque FMS, qui en plus du premier octet du flux de chiffrement généré par PRGA, analyse les octets suivants. Une telle méthode réduit considérablement le temps de recherche, vu qu'il n'est plus nécessaire d'analyser huit millions de paquets, un demi-million étant amplement suffisant avec la nouvelle méthode [11]. Cette attaque FMS améliorée a été implémentée dans les outils *dWepCrack* et *AirCrack* [13].

Toutefois, il est important de signaler que cette attaque n'est désormais plus possible avec les nouveaux équipements Wi-Fi, vu que les industriels ont éliminé la majorité des IV faibles transmis par les points d'accès [11]. Néanmoins, au bonheur des pirates, les réseaux Wi-Fi existants ne sont pas tous munis de ces nouveaux équipements.

Pour plus de détails sur l'attaque FMS et son optimisation, voir [16] et [17].

4.2.2.6 Attaque ChopChop de KoreK

Cette attaque est basée sur la preuve de concept publiée par un pirate informatique surnommé KoreK. Cette attaque appelée *ChopChop*, ou encore *Chopper* (Découpeur) peut décrypter un paquet chiffré avec le protocole WEP sans avoir connaissance de la clé.

Il s'agit d'une attaque cryptanalytique statistique, qui contrairement à l'attaque FMS, permet de casser une clé WEP avec quelques centaines de milliers de paquets et non pas des millions (environ 200.000 paquets pour une clé de 64 bits et 500.000 paquets pour une clé de 128 bits).

Ainsi, ChopChop utilise la faiblesse du contrôle d'intégrité avec CRC32, qui comme on l'a vu dans l'attaque Bit Flip permet à un attaquant d'injecter une modification à un message chiffré, en reflétant cette modification sur le champ de contrôle d'intégrité.

Cette modification se fait comme suit :

$$M' = M \oplus (modif \| CRC(modif))$$

où

M : Le message chiffré à modifier

M' : Le message M modifié

modif : La modification à opérer sur le message chiffré M

Outre cette faiblesse de contrôle d'intégrité, l'attaque KoreK s'inspire fortement de l'attaque inductive d'Arbaugh [14], mais en empruntant le raisonnement inverse. C'est pourquoi on l'appelle également l'attaque inductive inverse. Dans son approche, l'attaque KoreK, à l'encontre de l'attaque inductive d'Arbaugh, part du message chiffré pour trouver son correspondant en clair.

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. De ce fait, en coupant le message chiffré de son dernier octet (d'où le nom de l'attaque Chopper, *Découpeur* en français), 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. Cette correction se fait à l'aide du principe de l'attaque Bit Flip, afin d'injecter la modification au message chiffré.

Ensuite, le paquet corrigé est réinjecté dans le réseau. Il sera supprimé par le point d'accès si le choix fait est incorrect (dans ce cas un nouveau choix doit être fait : de 0 à 255). Si la correction est bonne, le paquet sera relayé sans problèmes, ce qui permet de constater le succès de cette correction. En répétant l'attaque sur chacun des octets du message chiffré, il est possible de décrypter l'intégralité du paquet et de retrouver la suite chiffrante associée.

Pour résumer, l'attaque se déroule comme suit :

1. Récupérer un message M chiffré transitant sur le réseau cible;
2. Tronquer le message chiffré M de son dernier octet;
3. Faire un choix sur la valeur en clair du dernier octet du message M (valeurs possible de 0 à 255);
4. Trouver la modification *modif* à affecter au message M, de façon que le dernier octet de l'ICV soit égal à la valeur qu'on a choisie lors de l'étape précédente;
5. Appliquer cette modification au message M, selon le principe de l'attaque Bit Flip;
6. Envoyer le message modifié au point d'accès;
7. Si le message n'est pas accepté, refaire les étapes 3 à 6, avec une autre valeur pour le dernier octet;
8. Si par contre, le message est accepté, l'attaquant connaît alors la valeur en clair du dernier octet du message;
9. Refaire toutes les étapes précédentes pour un autre octet, jusqu'au déchiffrement du paquet crypté en totalité.

Contrairement à l'attaque FMS et l'attaque inductive d'Arbaugh, l'attaque ChopChop de KoreK ne dépend pas des IV faibles et est plus performante, vu qu'elle permet de déchiffrer n'importe quel paquet indépendamment de la classe d'IV employée pour son chiffrement.

Ainsi, avec cette attaque il n'est plus nécessaire d'analyser des millions de paquets, ni de détecter les IVs faible, afin de casser la clé WEP. D'ailleurs, c'est ce qui fait de ChopChop, l'attaque la plus innovante et la plus performante du moment, vu qu'elle tire profit de quasiment toutes les attaques précédentes. Tous les experts de la sécurité des

réseaux sans fil sont unanimes sur la mort de WEP depuis la sortie de cette attaque en août 2004.

4.3 Les failles du protocole 802.1x

Tout comme nous avons procédé pour présenter les failles du protocole WEP, nous commençons cette section en présentant les faiblesses d'ordre conceptuel du protocole 802.1x. Ensuite, nous passons au volet des attaques, en explicitant les démarches, les techniques et outils utilisés pour leur mise en œuvre.

4.3.1 Les faiblesses conceptuelles du protocole IEEE 802.1x

Le protocole 802.1x est un protocole d'authentification utilisé au départ dans les réseaux filaires commutés qui a été ensuite intégré au mécanisme de sécurité des réseaux Wi-Fi. L'utilisation de ce protocole vient répondre principalement à la problématique d'authentification centralisée et de distribution dynamique des clés de chiffrement dans ce type de réseaux. Ainsi, 802.1x vient encadrer l'authentification dans les réseaux Wi-Fi. Toutefois, certaines spécificités des réseaux Wi-Fi ne sont pas prises en compte par ce protocole tel que l'association d'un client à un point d'accès selon la puissance du signal qu'il émet. De plus, 802.1x vient s'intégrer dans les réseaux 802.11, sans pour autant qu'il y ait une synchronisation avec les machines à état de ces derniers.

4.3.1.1 Authentification à sens unique

Dans l'architecture 802.1x, les points d'accès sont considérés à tort comme des entités de confiance. Cette façon de faire provient de l'origine d'utilisation de ce protocole dans les réseaux filaires, où les commutateurs étaient l'équivalent des points d'accès dans les réseaux Wi-Fi [18]. Toutefois, les commutateurs étaient enfermés dans des salles informatiques sécurisées et pour y accéder il fallait s'y connecter physiquement, alors que dans les réseaux Wi-Fi, les points d'accès peuvent être localisés n'importe où.

De ce fait, le protocole 802.1x ne fournissait pas une authentification mutuelle entre les clients et le point d'accès. Toute la sémantique du protocole se basait sur une authentification

unilatérale allant du point d'accès vers le client. Ce traitement asymétrique de l'authentification dans un contexte Wi-Fi rend le protocole 802.1x sujet à plusieurs attaques.

4.3.1.2 Absence de synchronisation entre les machines à état

Les machines à état de 802.11 et 802.1x ne sont pas corrélées, vu qu'elles ont été conçues de façon complètement indépendante [19]. Ce manque de synchronisation laisse la porte ouverte à bon nombre d'attaques qui utilisent cette défaillance afin de détourner des sessions.

La combinaison des deux machines à état (du client et du point d'accès) détermine l'état d'authentification. Du fait du manque de communication entre les deux machines à état, il est possible de réaliser une attaque par détournement de session en tirant profit de la faille de synchronisation.

En effet, il est possible que le client soit dissocié du point d'accès, alors que ce dernier garde le port relatif au client à l'état contrôlé authentifié. Nous montrons les détails de cette attaque dans la section relative aux attaques.

4.3.1.3 Manque d'intégrité dans les messages de contrôle 802.1x

Outre l'authentification mutuelle et l'absence de synchronisation entre les machines à état du client et du point d'accès, plusieurs messages de signalisation de 802.1x sont dépourvus de mécanismes de vérification d'intégrité. En particulier, les messages *Disassociate*, *Deauthenticate*, *EAP Success* et *EAP failure* ne sont pas protégés. De ce fait, il est possible de dissocier et désauthentifier les clients légitimes ou même de monter des attaques DoS contre eux en les inondant de ces messages.

4.3.2 Les attaques sur le protocole 802.1x

Les attaques sur le standard 802.1x sont toutes des attaques du type homme au milieu, mais qui s'opèrent à des niveaux différents. Le but ultime de ces attaques est de s'intercaler dans les connexions entre les clients 802.11 et le point d'accès et donc de subtiliser la session sécurisée établie entre les pairs légitimes.

Il est en effet possible d'effectuer ce type d'attaque aussi bien au niveau physique qu'au niveau liaison de données. Il est également possible de mettre en œuvre cette attaque contre les réseaux Wi-Fi dans lesquels l'authentification se fait par le biais d'interface Web au moyen de SSL [11].

Dans ce qui suit, nous donnons plus de détails quant au déroulement et la mise en œuvre de ces différentes attaques.

4.3.2.1 Attaque de l'homme au milieu sur la couche physique

Cette attaque consiste à mettre en place un point d'accès pirate, dont le rôle est de brouiller le signal émis par un point d'accès légitime, en émettant un signal fort et clair. Ce signal devrait être bien supérieur à la puissance de rayonnement autorisée sur la majorité des réseaux sans fil déployés, soit 1 Watt. Le brouillage peut être réalisé à l'aide d'un dispositif de brouillage spécifique ou en inondant de trafic factice le canal du point d'accès de trafic factice. Il existe une panoplie d'utilitaires permettant de générer un tel trafic, citons *FakeAP*, *Void11* ou *File2air* [11].

Le brouillage aura pour incidence de forcer les hôtes du point d'accès victime de se dissocier de leur WLAN, pour s'associer avec le point d'accès pirate, dont la puissance de rayonnement est relativement élevée. La figure 4.3 illustre le déroulement de cette attaque.

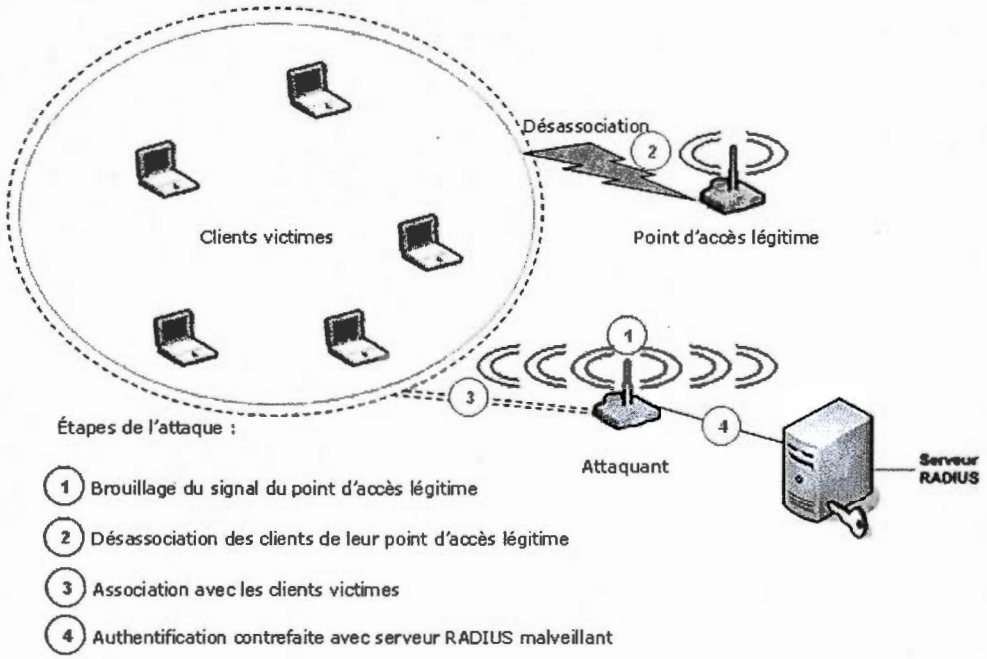


Figure 4.3 : Attaque de l'homme au milieu sur la couche physique

Toutefois, pour garantir la réussite d'une telle attaque, le point d'accès malveillant devra également être associé à un serveur RADIUS pirate et fournir des éléments d'identification contrefaits sous la forme de réponses d'authentification (toujours positives) aux hôtes clients dupés.

Il est à signaler que ce type d'attaques n'est faisable que contre les systèmes d'authentification 802.1x unilatéraux, utilisant une méthode d'authentification unilatérale, notamment, EAP-MD5. Ce qui explique la portée limitée de ce type d'attaques et leur manque de fiabilité pour les attaquants. Néanmoins, les attaques de l'homme au milieu sur la couche physique sont surtout utilisées pour provoquer un dérèglement du point d'accès légitime en brouillant son signal. De ce fait, ces attaques sont combinées avec d'autres approches telles que l'attaque de l'homme au milieu au niveau de la couche de liaison de données, dont les détails sont donnés dans la sous section qui suit, afin d'accroître les chances de réussite du piratage de la session sécurisée établie.

4.3.2.2 Attaque de l'homme au milieu sur la couche de liaison de données

Cette attaque, également appelée détournement de sessions (*Session Hijacking*), consiste à détourner une session sécurisée établie entre un point d'accès et un client. Elle se déroule comme le montre la figure 4.4 :

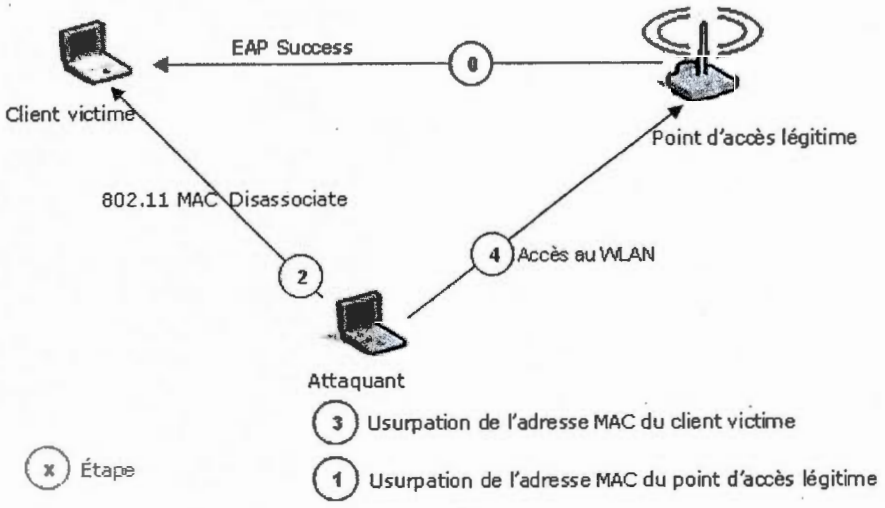


Figure 4.4 : Attaque de l'homme au milieu sur la couche liaison de données

Remarque: Nous avons assignés le numéro zéro au message *EAP Success* pour montrer que l'attaque vient à la suite d'une authentification réussie du client cible.

Cette attaque est possible principalement à cause des éléments suivants :

- Absence de mécanisme d'intégrité dans les messages de signalisation 802.11, tel que le message *MAC 802.11 Disassociate*. Ceci a pour incidence de permettre à l'attaquant de forger son propre message *Disassociate* et l'envoyer à l'hôte victime de son choix. La faiblesse du mécanisme d'intégrité est valable également pour les messages de contrôle 802.1x tels que les messages *EAP SUCCESS* et *EAP FAILURE* qui viennent conclure toute procédure d'authentification EAP.

- Absence de synchronisation entre les machines à état du client et du point d'accès : en effet, comme le montre cette attaque le client victime bascule à l'état désassocié, alors que le point d'accès garde le port relatif au client à l'état connecté authentifié. D'ailleurs, c'est ce qui permet à l'attaquant de se substituer au client légitime et d'accéder au WLAN.

Cette attaque est redoutable car elle contourne tous les mécanismes d'authentification de niveau supérieur et les rend inefficaces. À défaut d'une synchronisation entre les deux machines à état, cette attaque reste possible.

4.3.2.3 Attaque de l'homme au milieu sur SSL : Phishing

Cette attaque concerne le cas où le réseau sans fil a recours à une authentification utilisateur 802.1x fondée sur une interface Web (page de login Web), comme le font classiquement les points d'accès publics sans fil (exemple : UQAM sans fil), au moyen du protocole de sécurité SSL.

Cette attaque se base sur la technique du *Phishing*, qui par ailleurs n'est pas spécifique au protocole 802.1x. L'attaquant contrefait la page Web d'ouverture de session de manière à inspirer la confiance aux utilisateurs dupés, qui livrent leurs éléments d'identification, pour apprendre ensuite qu'une simple erreur réseau est survenue et que la connexion est perdue. Pendant ce temps, l'attaquant aura récupéré les éléments lui permettant d'accéder au réseau sans fil, sans éveiller de soupçons.

Il est très facile de monter ce genre d'attaques, en s'aidant d'outils comme *AirSnarf*, qui permet de créer des séquences de pages Web d'ouverture de session classiques (par exemple eBay, Paypal, Hotmail, etc.) [11].Peu importe que la connexion emploie SSL ou des clés PGP[32], l'utilisateur final ne détectera aucune attaque et s'associera inévitablement avec le point d'accès malveillant en lui livrant tous ses éléments d'identification.

---

32 Pretty Good Privacy

Finalement, un attaquant peut combiner les attaques de l'homme au milieu explicitées ci-dessus (de la couche physique, liaison de données et sur le protocole SSL), afin de maximiser les chances de réussite de son attaque.

En guise de conclusion sur les failles du protocole 802.1x, nous pouvons dire qu'outre les problèmes d'authentification mutuelle, de manque de synchronisation des machines à état et d'absence de mécanisme d'intégrité des messages de contrôle, le protocole 802.1x ne résout pas les problèmes de confidentialité liés au WEP. Ainsi, il ya eu un empilement de protocoles malheureusement accompagné d'un empilement de failles, avec pour résultat que les réseaux Wi-Fi ne sont pas plus sécurisés.

Toutefois, nous tenons à signaler que suite à ces graves défaillances de sécurité, il y a eu des modifications au standard. Parmi ces modifications, la plus importante est certainement l'incorporation de l'authentification mutuelle [18]. Le protocole 802.1x corrigé a été ensuite repris dans les normes WPA et WPA2, dont les défaillances vont être présentées dans ce qui suit.

4.4 Les failles de la norme WPA/WPA2

Depuis la sortie de WPA puis de WPA2, il y a eu découverte de trois failles sur trois mécanismes de sécurité. Aucune des ces trois failles n'est critique si des recommandations simples de sécurité sont suivies.

4.4.1 Attaque par dictionnaire sur la clé PSK

Cette attaque cible la clé PSK qui, nous le rappelons est l'un des modes de génération des clés de chiffrement et d'intégrité introduits par WPA. En effet, la clé PSK est la clé pré-partagée à partir de laquelle toutes les autres clés sont dérivées (voir figure 3.11 dans le chapitre 3). La clé PSK est utilisée comme alternative à l'établissement de clés de chiffrement et d'intégrité avec le protocole 802.1x.

L'attaque par dictionnaire sur la clé PSK a été découverte en novembre 2003. Une clé PSK est d'une taille de 256 bits, une longueur relativement importante. Toutefois, vu que personne ne pourra retenir une chaîne de mot de passe de cette taille, la clé PSK est générée à

partir d'une phrase de passe (*Passphrase*) ASCII, d'une taille acceptable (du point de vue de l'utilisateur). Cette phrase de passe est entrée par l'utilisateur.

Ainsi, l'attaquant peut tenter une attaque par dictionnaire sur la valeur de cette clé PSK. Une fois la clé PSK connue, l'attaquant peut dériver la clé PTK et toutes les clés qui en découlent (Rappelons qu'à partir de la clé PTK seront générées les différentes clés de chiffrement TKIP et d'autres clés d'intégrité, voir figure 3.11).

En effet, pour calculer la clé PTK, il suffit de connaître les adresses MAC des stations en communication et de capturer les nonces de fraîcheur générés par ces derniers, en plus de la clé PMK. Rappelons d'abord que la clé PTK s'obtient selon la formule suivante :

$$PTK = PRF\{PMK, AA||SPA||ANonce||SNonce\}$$

AA : Adresse du point d'accès
SPA : Adresse du client 802.11
ANonce, SNonce : Nonces de fraîcheur

La clé PMK est dérivée de la clé PSK selon la formule suivante :

$$PMK = PBKDF2\ (PSK\_\ passphrase, ssid, ssidLength, 4096, 256)$$

PBKDF2 : fonction cryptographique de hachage du standard PKCS #5 v2.0
4096 : Nombre de fois qu'on calcule un haché de (PSK_ passphrase‖ssid‖ssidLength)
256 : taille de la clé PMK à calculer

Cette attaque est d'autant plus redoutable que la clé PSK est valable pour un réseau Wi-Fi étendu (ESS). Ainsi, l'attaquant devient membre de l'ESS et la sécurité du réseau entier est compromise. L'utilitaire *cowpatty* a été crée pour exploiter cette faiblesse et son code source a été repris et améliorée par Christophe Devine dans AirCrack afin de réaliser des attaques par force brute ou par dictionnaire sur la PSK. Toutefois, le protocole tel qu'il fonctionne implique que les attaques de type force brute soient très lentes (4096 hachage pour chaque phrase de passe tentée) [20].

La solution recommandée par les normalisateurs pour contrer cette défaillance est de choisir une phrase de passe (*Passphrase*) de plus de 20 caractères ou entrer la PSK en hexadécimal. En effet, selon les normalisateurs une phrase de passe typique possède environ

2,5 bits de sécurité par caractère. La phrase de passe à n bits doit produire une clé avec 2,5 * n + 12 bits de sécurité (formule adoptée par le standard 802.11i) [20]. Selon cette formule, une clé générée avec une phrase de passe comprenant moins de 20 caractères n'est pas assez sécuritaire et peut être cassée.

Certes, il est vrai que cette solution (selon la formule adoptée) garantit une plus grande sécurité pour la clé PSK. Toutefois, une question se pose : combien d'utilisateurs (ou même d'administrateurs) choisissent et mémorisent habituellement des mots de passe d'au moins 20 caractères ?

4.4.2 Attaques DoS sur l'échange 4-Way Handshake

L'attaque DoS sur l'échange 4-Way Handshake est l'attaque la plus célèbre et la plus percutante que WPA2 ait connu depuis sa sortie. En effet, le premier message de l'échange 4-Way Handshake n'est pas authentifié. De plus, le client conserve chaque premier message jusqu'à réception du troisième message (signé), laissant le client vulnérable à une saturation de mémoire. L'attaque exploite cette faille en inondant le client avec des messages 1 contrefaits (ouverture de plusieurs sessions simultanées), en usurpant l'identité d'un point d'accès légitime. Cela aura pour incidence la saturation de l'espace mémoire du client et le blocage du protocole [9]. Ceci en plus du blocage de l'échange avec le point d'accès légitime : impossible d'établir la clé PTK.

Dans ce qui suit, nous rappelons le déroulement normal d'un échange 4-Way Handshake. Puis nous illustrons le mode opératoire de l'attaque DoS contre ce mécanisme.

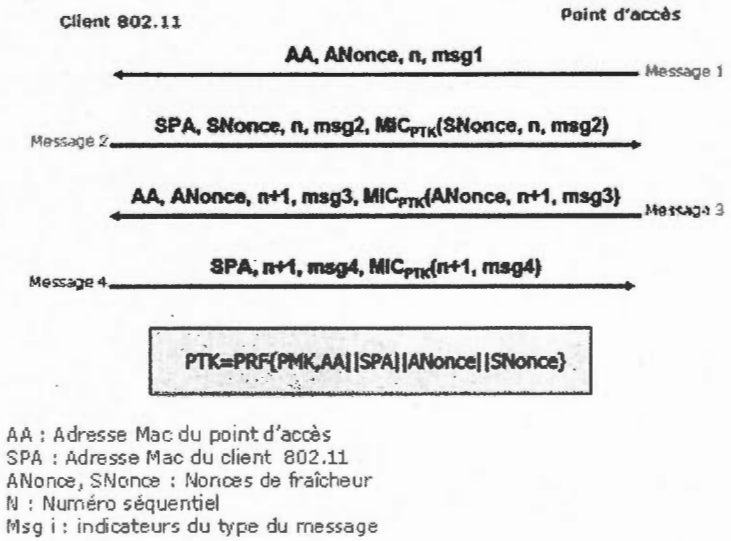


Figure 4.5 : Échange 4-Way Handshake simplifié [9]

Comme nous l'avons mentionné dans le chapitre précédent, l'échange 4-Way Handshake vient à la suite de l'authentification mutuelle entre le client et le point d'accès. Le but de cet échange est d'établir la clé PTK (pour plus de détails sur l'échange 4-Way Handshake, voir le chapitre 3). La faiblesse de cet échange vient de l'absence d'un mécanisme d'authentification du premier message (Message 1). De ce fait, il est très facile d'usurper l'identité d'un point d'accès et d'envoyer des messages 1 contrefaits. Le mode opératoire de l'attaque est illustré dans la figure 4.6.

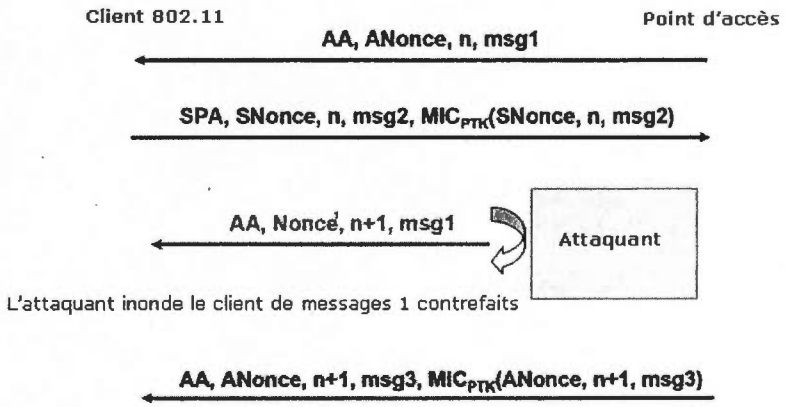


Figure 4.6 : Attaque Dos sur l'échange 4-Way Handshake

Après les deux premiers messages du Handshake, l'attaquant envoie un nouveau message 1 du Handshake en usurpant l'adresse MAC du point d'accès. Le client croyant recevoir ce message d'un point d'accès légitime, permet l'ouverture d'une nouvelle session.

De son côté, l'attaquant continue d'envoyer des messages, afin d'inonder le client par des messages 1 contrefaits, de manière à obliger le client victime à ouvrir en permanence de nouvelles sessions et saturant son tampon.

La faille exploitée par cette attaque a été corrigée et la correction a été intégrée au standard WPA2. Toutefois, il est à signaler que cette attaque n'a jamais été mise en œuvre concrètement. La difficulté de l'élaboration de cette attaque sur un plan pratique vient du fait qu'il est nécessaire à l'attaquant de synchroniser l'envoi de ses messages 1 contrefaits avant l'émission du message 3 du point d'accès.

4.4.3 Attaque sur la clé TEK de WPA

L'attaque sur la clé temporaire TEK de la norme WPA a été publiée en 2004. TEK (Temporal Encryption Key) est une clé dérivée de la clé PTK (voir figure 3.11 du chapitre précédent), d'une taille de 128 bits. Cette clé sert principalement au chiffrement des paquets selon le nouveau protocole de chiffrement introduit par WPA, à savoir, TKIP. L'attaque

décrite dans [21] est une attaque cryptanalytique statistique, d'une complexité de l'ordre de O (2^{105}) au lieu de O (2^{128}) d'une attaque par force brute.

Le problème de cette attaque est qu'elle nécessite la connaissance d'au moins deux clés RC4 générées à partir d'IV identiques. Les auteurs de l'attaque l'ont implémentée avec quatre clés RC4 connues. À la fin de leur expérimentation, ils ont pu récupérer la clé TEK en moins de 7 minutes de calcul (sur Pentium IV de 2,5GHz). Une fois la clé TEK récupérée, il est possible à l'attaquant de déchiffrer toutes les trames qui transitent sur le réseau, utilisant cette même clé TEK.

Toutefois, avec le nouveau mode opératoire de chiffrement introduit par TKIP, cette condition devient très improbable, voire impossible (avec TKIP, un même IV n'est utilisé qu'une seule fois, plus de problème de collision d'IV). De ce fait, le risque induit par cette attaque est quasiment nul, d'autant plus que la clé TEK a une durée d'utilisation limitée. C'est pourquoi il n'y a pas eu trop d'échos créés par cette attaque, vu la faible probabilité d'application pratique.

4.5 Attaques DoS sans fil

Dans cette section, nous regroupons toutes les variétés d'attaques DoS qu'il est possible de mettre en ouvre sur les réseaux Wi-Fi au niveau des couches 1 et 2 du modèle OSI. Ce genre d'attaques est certainement parmi les plus graves dangers qui guettent les réseaux 802.11. En effet, un assaillant pourrait être tenté d'utiliser les attaques DoS comme dernier recours sur des réseaux Wi-Fi contre lesquels il a tenté sans succès des attaques plus élaborées afin d'y accéder.

Le but ultime de ces attaques est de dévier le réseau cible de son comportement normal et de causer des disfonctionnements graves. Pour ce faire, il existe plusieurs approches pour réaliser ce type d'attaques. Dans ce qui suit, nous explicitons le mode opératoire de chaque approche d'attaque. Le facteur en commun de ces attaques est leur efficacité et la facilité de leur mise en œuvre.

4.5.1 Attaque par brouillage radio sur la couche physique

Cette attaque, bien qu'étant d'un principe très simple, est tout à fait redoutable pour tout réseau Wi-Fi et quasiment imparable. En effet, l'assaillant aura à se munir d'un brouilleur de fréquences comprises entre 2,4 GHz et 2,5 GHz (plage de fréquence des réseaux Wi-Fi 802.11 b et g) et de se placer le plus proche possible du réseau sans fil cible. Le dispositif de brouillage pourra être un émetteur-récepteur fait maison, une carte client à haute puissance d'émission ou même un point d'accès inondant le ou les canaux sélectionnés de trafic factice, en s'aidant d'utilitaires comme FakeAP, void11 ou File2air [11].

Il est également relativement facile de construire un brouilleur de fréquence personnalisé très puissant, en utilisant le magnétron d'un four à micro-ondes, en guise de noyau du brouilleur. Sur Internet, il existe plusieurs sites donnant des descriptions détaillées sur la construction de brouilleur de fréquences, ainsi que des antennes de tout type pour amplifier l'émission du signal de brouillage.

Tout ceci montre la facilité de la mise en ouvre d'une telle attaque, qui bien qu'étant simple, provoque de graves disfonctionnements dans le réseau victime. Comme conséquences à cette attaque, notons le dérèglement de la puissance émise par le point d'accès et la désassociation de toutes les stations clientes.

De plus, il est quasiment impossible de contrer cette attaque. En effet, bien qu'il existe des équipements radio qui par triangulation permettent de localiser l'emplacement du signal parasite de brouillage, rien n'empêche le pirate de changer fréquemment de position. On peut imaginer un attaquant qui circule en voiture avec un ordinateur portable muni d'une carte client Wi-Fi à haute puissance d'émission raccordée à un amplificateur et une antenne. Dans ce cas de figure, il est quasiment impossible de localiser l'assaillant.

4.5.2 Attaque par inondation RTS

Cette attaque est fondée sur l'exploitation du mécanisme de réservation prioritaire RTS/CTS implanté dans les réseaux Wi-Fi, que nous avons décrit dans le chapitre II. Ainsi, l'attaque consiste à inonder continuellement le support de transmission par des trames RTS

(*Request To Send*), en fixant le champ *Durée* de la trame RTS à un grand intervalle de transmission. La figure 4.7, montre le déroulement de l'attaque, ainsi que les champs composants une trame RTS.

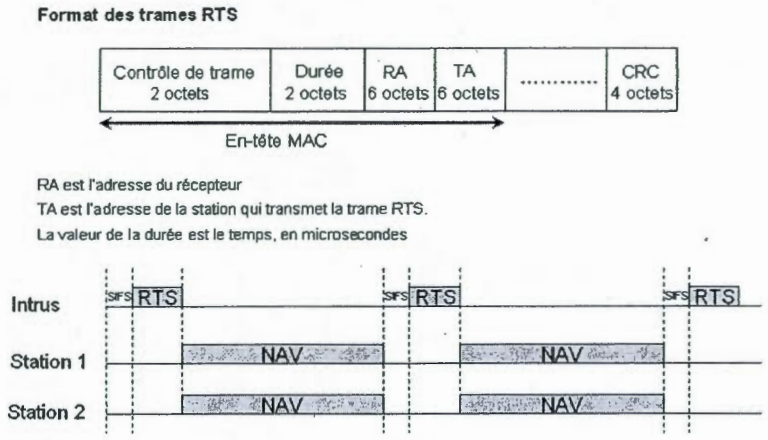


Figure 4.7 : Attaque par inondation RTS

Comme le montre la figure, l'intrus émet continuellement des trames RTS, en modifiant l'adresse de l'émetteur à chaque fois pour ne pas éveiller les soupçons. De cette manière, l'intrus garde le support réservé en permanence pour ses transmissions, en interdisant aux autres stations d'accéder au canal de communication. Le réseau sera surchargé de messages RTS et des réponses CTS (*Clear to Send*). Les clients victimes sont obligés de cesser de transmettre et d'incrémenter la valeur du compteur NAV au passage de chaque trame RTS.

4.5.3 Attaque contre le mode économie d'énergie

Cette attaque exploite le mécanisme d'économie d'énergie implanté dans les réseaux Wi-Fi. Ce mécanisme stipule que les clients associées à un point d'accès et qui n'ont pas d'activité (pas de données à émettre, ni à recevoir) peuvent basculer en mode veille ou économie d'énergie (ces stations sont généralement des terminaux avec une capacité d'énergie limitée). Pendant que les stations sont en veille, le point d'accès se charge

d'envoyer des trames Beacon aux stations en veille pour leur signaler qu'il a reçu des données qui leur sont destinées [2].

Ainsi, l'attaquant pourra se faire passer pour le client en veille (en usurpant son adresse MAC, par exemple) et récupérer toutes les trames accumulées pour sa cible depuis le point d'accès. Une fois les trames reçues par l'attaquant (vu que le destinataire légitime est en mode veille), le point d'accès vide le contenu du tampon. Dans ce cas, le client légitime ne recevra jamais les trames qui lui étaient destinées.

L'attaquant peut également obliger les stations d'un réseau sans fil à rester éveillées et ne jamais basculer en mode économie d'énergie. Pour ce faire, il suffit de contrefaire les trames Beacon et les envoyer aux clients cibles [11]. De cette manière, les stations vont sortir du mode veille, en croyant que des données vont leur être transmises du point d'accès. Cela aura pour effet d'augmenter la consommation d'énergie des stations cibles et provoquer ultimement un déni de service par épuisement des ressources (piles).

4.5.4 Inondation de trames de désassociation et de désauthentification

Cette attaque est probablement la plus employées et la plus connue des attaques DoS contre des réseaux 802.11. De plus, comme pour le brouillage radio, cette attaque est quasiment imparable. Ce qui rend cette attaque possible est l'absence de mécanisme de vérification d'intégrité et surtout d'authentification des trames de désassociation et de désauthentification.

Les normalisateurs du 802.11i ont étudié la possibilité de corriger cette défaillance, mais leurs intentions n'ont jamais été traduites en pratique. Pour réaliser cette attaque, il existe de nombreux outils permettant de lancer de telles inondations, tels que *dinject*, *wlan_jack*, *File2air* et *void11* [11].

L'attaque se base sur l'inondation d'un hôte cible par des trames de désassociation et de désauthentification, afin de le mettre hors du réseau. Une fois que le client cible est désassocié de son réseau, il est possible d'usurper son adresse Mac afin de monter d'autres attaques d'intrusion plus élaborées.

4.5.5 Attaque par dépassement de capacité sur le point d'accès

Un grand nombre de points d'accès sont dépourvus de protection contre un dépassement de capacité de leurs tampons et montrent des défaillances après l'établissement d'un nombre excessif de connexions ou d'envois de requêtes d'authentification.

Il existe plusieurs utilitaires qui permettent de réaliser ce type d'attaque, en inondant le point d'accès cible de requêtes d'association avec différentes adresses MAC. Parmi ces outils, citons *void11* qui met en œuvre à la fois des inondations de trames d'association et d'authentification avec une inondation aléatoire des adresses MAC de l'interface hôte. *Void11* permet également d'associer une seule station avec une adresse MAC contrefaite, puis il lance des modifications rapides d'adresse MAC à l'interface associée [11]. Ces deux méthodes aboutissent au même résultat qui est le blocage du point d'accès.

Ainsi, le point d'accès sera associé à de plus en plus de stations contrefaites jusqu'à ce que cela provoque un blocage suite au dépassement de capacité de ses tampons. De ce fait, il primordial pour les équipementiers d'intégrer dans leurs matériels des mécanismes de protection contre le dépassement de capacité des tampons des points d'accès.

4.5.6 Attaque par suppression de trames

Cette attaque repose sur la corruption du CRC32 d'une trame envoyée par un client donné d'un réseau Wi-Fi cible. Ainsi, l'attaquant devra modifier le CRC d'une trame en transit, de façon à ce qu'elle soit rejetée par son destinataire (car CRC non valide). En même temps, l'attaquant envoie un message d'acquittement ACK contrefait à l'émetteur de la trame modifiée.

Ainsi, la trame corrompue est supprimée par le destinataire, sans pour autant qu'elle soit renvoyée par le destinataire. Cette attaque est possible vu que les trames CSMA/CA ne sont pas toutes authentifiées et ce pour des raisons de ressources et de la capacité limitée du support hertzien.

Pour corrompre le CRC de la trame, l'attaquant devra émettre un signal de brouillage au moment de l'émission des quatre derniers octets de la trame, correspondants aux quatre

octets du CRC. D'un point de vue théorique, cette attaque est valable, toutefois il n'existe actuellement aucun utilitaire la mettant en pratique, vu la difficulté de faire coïncider l'émission du signal de brouillage avec l'émission des quatre derniers octets de la trame. Une chose est certaine, mise en œuvre correctement, une telle attaque est aussi difficile à détecter qu'à repousser.

4.6 Attaques Wi-Fi : mise en œuvre

Le fait qu'il existe une panoplie d'attaques qui fonctionnement admirablement bien sur le plan théorique ne fait pas qu'elles soient simples à mettre en œuvre sur le plan pratique. En effet, le degré d'efficacité et de réussite d'une attaque donnée dépend étroitement des équipements matériels et des utilitaires logiciels utilisés.

Dans cette section, nous nous intéresserons à l'aspect matériel et logiciel de la mise en œuvre de toute attaque Wi-Fi. Nous verrons qu'une attaque qui semble redoutable sur le plan théorique, ne l'est pas forcément sur le plan pratique. Ainsi, nous commencerons par le volet matériel en présentant les spécificités des cartes sans fil 802.11. Ensuite, nous explicitons le volet pilotes et utilitaires logiciels nécessaires aux attaques. Nous finirons cette section en présentant l'utilitaire d'attaques AirCrack, qui est l'outil d'attaque Wi-Fi le plus complet pour le moment.

4.6.1 Équipements Wi-Fi

Le volet matériel est crucial pour toute attaque Wi-Fi. En effet, la carte client sans fil est l'élément le plus important dans la boîte à outils de tout attaquant Wi-Fi. Du point de vue de l'attaquant, les critères de choix d'une carte Wi-Fi sont les suivants :

- le jeu de puces (*Chipset*).
- la puissance de sortie et ses possibilités de réglage.
- la sensibilité de réception.
- la présence et le nombre de connexions d'antennes extérieures.

Parmi les chipsets 802.11 les plus adaptés à des attaques Wi-Fi, citons : Prism, Cisco Aironet, Hermes/Orinoco, Symbol, Atheros et ADMtek [11]. Les cartes clients sans fil avec

ces chipsets offrent la possibilité de configurer le mode de fonctionnement. En effet, les cartes Wi-Fi peuvent être configurées dans les modes suivants :

- Mode Ad-hoc : la carte peut se connecter à un réseau ad-hoc d'une seule cellule sans point d'accès.
- Mode Managed : la carte peut se connecter à un réseau d'une ou plusieurs cellules avec point d'accès, c'est le mode par défaut de toute carte sans fil 802.11.
- Mode Master : la carte joue le rôle d'un point d'accès maître.
- Mode Repeater : la carte joue le rôle d'un répéteur entre différents noeuds. Cette méthode peut être utilisée pour relayer une connexion Wi-Fi sur de longues distances.
- Mode Secondary : la carte joue le rôle d'un backup pour Master ou Repeater.
- Mode RFMON[33] : c'est l'équivalent du mode promiscuité pour les cartes réseaux Ethernet. La carte est passive et ne fait que recevoir les messages. Un client avec une carte sans fil qui est configurée en mode de RFMON pourra capturer tous les signaux des canaux sur lesquels il est configuré pour écouter. RFMON est un mode récepteur uniquement.

Toutefois, toutes les cartes n'offrent pas tous les modes listés ci-dessus. En effet, les équipementiers ont tendance à inhiber certains modes notamment le mode RFMON sur leurs cartes. Pour établir la plupart des attaques, il est nécessaire de pouvoir écouter le trafic Wi-Fi, en capturant les trames qui transitent sur le support hertzien. De ce fait, l'activation du mode RFMON est indispensable.

En effet, la quasi-totalité des attaques contre des réseaux Wi-Fi nécessitent l'activation du mode RFMON. D'un autre côté, pour monter certaines attaques telles que les attaques de l'homme au milieu, il est nécessaire d'activer le mode Master. Ce dernier permettra de jouer

---

33 Radio Frequency Monitoring

le rôle de point d'accès pirate vis-à-vis des clients victimes. C'est pourquoi, il est nécessaire de choisir une carte sans fil avec le chipset adéquat.

Outre le fait de choisir une carte avec l'un des chipsets permettant de changer de mode de fonctionnement, il est nécessaire de trouver le pilote adéquat pour gérer le fonctionnement de l'interface 802.11. Les pilotes fournis par les constructeurs sont très limités du point de vue des fonctionnalités de configuration offertes. Afin d'augmenter les chances de réussite d'une attaque donnée, un pilote d'une carte sans fil devrait permettre le réglage de la puissance de sortie et la sensibilité de réception de l'interface 802.11. C'est pourquoi les attaquants ont tendance à recourir à des pilotes à code source ouvert (open source) qu'ils modifient afin de les adapter à leurs besoins spécifiques. Dans la section qui suit, nous nous attarderons sur les pilotes de cartes Wi-Fi.

Une des qualités d'une carte Wi-Fi est également la présence et le nombre de connexions d'antennes extérieures. L'utilisation d'antennes pour mettre en œuvre une attaque peut s'avérer très utile et accroit sensiblement la probabilité de réussite de l'attaque. En effet, les capacités d'émission et de réception de l'attaquant se verront multipliées en utilisant des cartes Wi-Fi couplées à des antennes hautement directionnelles tel que celles de type parabole ou grille.

4.6.2 Pilotes et utilitaires Wi-Fi

Outre le fait de s'équiper avec une carte client sans fil avec un chipset adéquat et offrant les meilleures caractéristiques matérielles (haute puissance d'émission, grande sensibilité de réception, présence de connecteurs d'antennes externes, etc.), il est nécessaire d'utiliser un pilote adapté à l'usage spécifique de la carte. De plus, il est primordial pour un attaquant Wi-Fi de s'équiper avec un ensemble d'utilitaires logiciels de capture, d'injection de trafic 802.11, ou encore des outils d'attaques statistiques qui permettent le cassage de clés de chiffrement.

Tous les pilotes et utilitaires adaptés à la mise en œuvre d'attaques Wi-Fi sont à code source ouvert. Cela s'explique pour plusieurs raisons. L'élaboration d'une attaque sur un réseau Wi-Fi nécessite la modification et l'adaptation du comportement de l'interface 802.11

aux spécificités de l'attaque. Contrairement aux pilotes propriétaires, les pilotes à code source ouvert se prêtent à merveille à ces manipulations et modifications de la configuration.

Ainsi, le système d'exploitation Linux s'impose naturellement comme plate-forme privilégiée pour l'exécution, la modification et le développement de pilotes 802.11 spécifiques, d'utilitaires d'analyse et d'injection de trafic réseau. Le système BSD vient en seconde position (essentiellement en raison de la taille inférieure de la communauté des développeurs et d'une liste de matériels pris en charge moins développée).

Par ailleurs, une connaissance pointue des pilotes de cartes sans fil et des détails de leur fonctionnement s'impose pour tout attaquant Wi-Fi.

Ainsi, une fois que l'attaquant s'est équipé d'une carte sans fil en ayant adapté et configuré le pilote, il doit se constituer une sorte de boîte à outils dont les éléments principaux sont les suivants :

1. Outils de découverte ou de cartographie réseau. Exemples : *Kismet, AirTraf, Mognet,* etc.
2. Outils de surveillance de la force du signal radio. Exemples: *wavemon, wlanmeter, Wireless Power Meter, XnetworkStrength, etc.*
3. Outils d'analyse et de journalisation de trafic. Exemples: *Wellenreiter, Gtkskan, etc.*
4. Outils de génération et d'injection de trafic 802.11. Exemples: *WEPWedgie, AirJack, File2Air, etc.*
5. Outils de déchiffrement (WEP, 802.1x). Exemples: *AirSnort, Wep_Crack, DwepUtils, Asleap-imp, LeapCrack, etc.*

Remarque : La quasi majorité de ces outils sont réalisés par des pirates informatiques et sont très rarement accompagnés d'une documentation ou de guides de configuration. Ils sont généralement publiés dans des forums dédiés au piratage des réseaux Wi-Fi.

Pour chaque groupe de fonctions, il existe une liste impressionnante d'outils avec une efficacité et une complexité de mise en place variables. Toutefois, en 2004, il y a eu la sortie de deux utilitaires qui intègrent quasiment toutes les catégories d'outils listées ci-dessus en un

seul logiciel. Ces deux outils sont WepLab de J.I. Sanchez et AirCrack de C. Devine. Ce dernier outil a connu beaucoup de succès surtout par sa relative facilité d'installation et de configuration. Dans ce qui suit, nous présentons l'utilitaire AirCrack et les types d'attaques qu'il permet de monter.

4.6.3 Présentation de l'outil AirCrack

AirCrack est une suite d'outils composée de trois principaux éléments utilisés conjointement pour monter une attaque contre un réseau Wi-Fi [9]. Les composantes d'AirCrack sont les suivantes :

- Airodump : outil de capture réseau utilisé pour découvrir les réseaux WEP environnants,
- Aireplay : outil pour injecter artificiellement du trafic,
- Aircrack : casseur de clé WEP utilisant les trames collectées préalablement.

L'injection de trafic utilisant Aireplay n'est supportée que sur un certain nombre de cartes client Wi-Fi, le support pour l'injection en mode RFMON nécessite la dernière version des pilotes modifiés. Avec des pilotes modifiés, il est possible d'injecter et de capturer simultanément le trafic en utilisant une seule carte sans fil.

L'outil AirCrack permet de mettre en œuvre plusieurs attaques sur différents protocoles de sécurité Wi-Fi, principalement sur le protocole WEP. En effet, AirCrack implémente une panoplie d'attaques sur ce protocole (FMS, FMS optimisé, attaque inductive d'Arbaugh, attaque ChopChop de KoreK). De ce fait, il est possible de casser une clé WEP de 128 bits en moins de 10 minutes en utilisant AirCrack. L'injection de trafic avec aireplay a certainement été pour beaucoup dans cette performance. Les attaques possibles avec AirCrack sont les suivantes :

- Cassage de clé WEP (64/128 bits);
- Décrypter un paquet chiffré avec WEP sans connaître la clé;
- Dé-authentification et désassociation;
- Fausse authentification ;

- DoS par inondation de trafic.

En guise d'exemple d'attaque réalisée avec AirCrack, nous montrons dans ce qui suit les étapes à suivre afin de casser une clé WEP.

Étape 1 : Activation du mode RFMON de la carte Wi-Fi

Cette étape permet de capturer le trafic. Ici une carte 802.11 basée sur un chipset Atheros est utilisée

```
# airmon.sh start ath0
Interface       Chipset         Driver
ath0            Atheros         madwifi (monitor mode enabled)
```

Étape 2 : Découverte des réseaux environnants et des stations Wi-Fi associées

```
# airodump ath0 wep-crk 0

BSSID              PWR  Beacons    # Data   CH  MB  ENC   ESSID
00:13:10:1F:9A:72   62      305       16    1  48  WEP    demo

BSSID              STATION            PWR  Packets  ESSID
00:13:10:1F:9A:72  00:0C:F1:19:77:5C   56        1  demo
```

Le résultat du Listing ci dessous peut être interprété de la façon suivante : un point d'accès avec le BSSID 00:13:10:1F:9A:72 utilise le protocole WEP sur le canal 1 avec le SSID demo, un client identifié par la MAC 00:0C:F1:19:77:5C est associé et authentifié sur ce réseau sans fil.

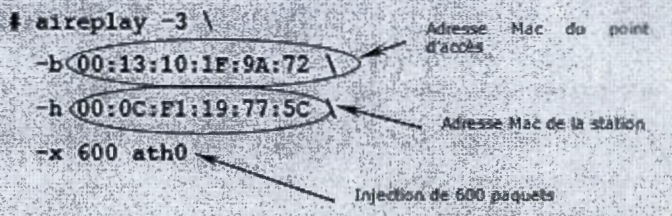
Étape 3 : Capture et journalisation du trafic 802.11

Une fois le réseau cible de l'attaque repéré, la capture doit être réalisée sur le canal adéquat pour éviter de perdre des paquets lors du passage sur les autres canaux. Cette étape fournit un fichier de journalisation de trafic, nommé wep-crk.

```
# airodump ath0 wep-crk 1
```

Étape 4: Injection de trafic avec aireplay

Ensuite, il est possible de lancer l'injection de trafic avec aireplay en utilisant les informations précédemment découvertes. L'injection de trafic se fait par la commande qui suit :



Étape 5 : Cassage de la clé WEP

L'étape finale consiste à utiliser AirCrack pour casser la clé WEP. Il est possible de lancer cette étape sur le fichier pcap alors qu'airodump capture toujours le trafic.

```
# aircrack -x -0 wep-crk.cap
```

Ainsi, avec cette dernière section, nous avons donné un aperçu des détails techniques (matériels et logiciels) à prendre en considération pour la mise en œuvre d'attaques sur des réseaux 802.11. Nous pouvons remarquer une grande complexité des plates-formes matérielles et logicielles à mettre en place afin de monter des attaques. Ceci d'autant plus que l'élaboration de telles attaques exige des connaissances pointues en équipements Wi-Fi, fonctionnement et configuration des pilotes, détails de fonctionnements des protocoles de sécurité, ainsi que les spécificités de la couche 802.11.

Ce chapitre constitue une étude des failles des protocoles de sécurité Wi-Fi. Nous avons ainsi parcouru, protocole par protocole, la quasi-totalité des attaques qu'il est possible de monter en tirant profit des failles conceptuelles de ces protocoles. Nous avons donné un aperçu sur le volet matériel et logiciel pour la mise en œuvre des attaques Wi-Fi, en mettant en évidence la complexité et la multitude des détails à prendre en considération pour la mise en place de plates-formes pour des attaques 802.11.

En guise de synthèse, nous pouvons dire que WEP est définitivement à éviter. En effet, la durée de vie d'une clé de 128 bits est inférieure à 1h avec les nouveaux outils, tel qu'AirCrack.

Les points d'accès ne supportant pas WPA doivent impérativement implémenter un mécanisme de rotation des clés au moins à toutes les heures, afin de minimiser les risques liés à WEP. La norme de transition WPA s'impose comme solution pour les points d'accès ne supportant pas le standard WPA2 (mise à jour logicielle possible).

Finalement, nous pouvons affirmer que WPA2 est certainement la solution la plus robuste et la plus pérenne. Toutefois, le mode PSK ne garantit pas la confidentialité entre utilisateurs d'une même cellule BSS. De plus, les attaques DoS de bas niveau sont toujours possibles.

Il est à signaler que l'étude présentée dans ce chapitre constitue une contribution originale. En effet, il est vrai que les failles et attaques traitées sont présentes dans la littérature. Toutefois, à notre connaissance aucun ouvrage ou article à date ne fait un recensement exhaustif et ne présente un degré de détail tel que nous l'avons fait.

Outre le volet conceptuel et théorique, nous avons également présenté le volet pratique avec la profusion d'outils et techniques qu'il renferme. Ainsi, nous avons scruté l'environnement du pirate et avons dégagé les grandes lignes des méthodes adoptées. La réalisation de cette étude n'a pas été triviale et a nécessité une documentation approfondie, ainsi que le test de divers outils d'attaques dont la configuration n'a pas toujours été simple. De plus, la majorité des attaques ne sont pas du tout documentées et nous avons eu à les simuler à l'aide d'outils particuliers, afin de comprendre leur mode opératoire.

Le prochain chapitre s'inscrit dans la suite logique des chapitres précédents en abordant les différentes architectures de sécurité Wi-Fi et proposant une nouvelle approche dans la sécurisation de l'architecture Wi-Fi dans l'entreprise.

CHAPITRE V

NOUVELLE ARCHITECTURE WI-FI SÉCURISÉE ET FLEXIBLE

Le chapitre précédent met en évidence le manque de sécurité dans les réseaux Wi-Fi, la profusion des attaques qu'il est possible de monter et leur relative simplicité de mise en œuvre. Toutefois, ce manque de sécurité ne devrait pas constituer un obstacle à la mise en place et au déploiement de réseaux Wi-Fi dans l'entreprise. En effet, dans de nombreux cas (nouveau bâtiment non câblé, installation temporaire, etc.), il est économiquement plus intéressant de mettre en place un réseau local sans fil qu'un réseau local filaire. Un réseau Wi-Fi est beaucoup plus flexible qu'un réseau filaire et peut être désinstallé facilement. Il peut également compléter ou remplacer un réseau local filaire lors d'un contexte de mobilité.

Ce chapitre vient répondre aux questions suivantes : face à toutes les failles de sécurité et à la diversité des attaques qu'il est possible de monter contre les mécanismes de sécurité dans les réseaux Wi-Fi, quelles sont les meilleures pratiques en matière de sécurité Wi-Fi ? Faut-il abandonner complètement le protocole WEP? Comment assurer une sécurité optimale, compte tenu de l'hétérogénéité des équipements/standards Wi-Fi (WEP, WPA, WPA2) existants actuellement dans les entreprises?

Cette dernière question, plus particulièrement, fera l'objet d'étude principal de ce dernier chapitre. En effet, nous proposons une nouvelle approche de sécurisation de l'architecture Wi-Fi de l'entreprise qui prend en considération l'hétérogénéité des équipements et des standards de sécurité supportés.

Il est important de signaler que dans le cadre de ce mémoire, nous nous attaquons principalement à un problème d'ordre architectural qui a suscité des travaux de recherche

surtout dans le milieu industriel. En effet, le panorama actuel des parcs informatiques dans les entreprises se caractérise par la diversité des équipements Wi-Fi avec différents standards supportés, qui ne sont pas toujours compatibles. Cette situation a crée un besoin urgent d'une approche architecturale qui permette d'assurer une sécurité optimale tout en tenant compte de l'hétérogénéité de l'environnement Wi-Fi existant.

Ce chapitre se compose de deux sections principales : la première s'intéresse aux principales approches de sécurisation d'un réseau Wi-Fi. Cette section nous permettra de prendre conscience de l'étendue et envergure des travaux réalisés jusqu'alors dans ce domaine. La seconde section présente les objectifs et la méthodologie adoptée pour aboutir à l'architecture que nous proposons, ainsi que ses principes fondateurs.

5.1 Approches principales de sécurisation des architectures Wi-Fi

Le manque de sécurité des réseaux Wi-Fi et l'absence de standards de sécurité 802.11 robuste a obligé les entreprises à faire appel à d'autres technologies afin de renforcer la sécurité de l'extension Wi-Fi de leurs systèmes d'information.

Les technologies employées visaient principalement deux objectifs. D'abord, isoler le trafic Wi-Fi du reste du trafic filaire, ce qui peut être réalisé par le biais des réseaux locaux virtuels (VLAN). Ensuite, sécuriser les liens radio établis entre les clients Wi-Fi et le serveur d'authentification, ce qui peut se mettre en place en utilisant la technologie des réseaux virtuels privés (VPN).

Dans ce qui suit, nous abordons les caractéristiques de ces deux approches de sécurisation des architectures Wi-Fi dans l'entreprise.

5.1.1 Approche VLAN

Cette approche consiste à mettre en place un VLAN pour tous les clients 802.11 qui se connectent au réseau de l'entreprise. À défaut de sécuriser les liens radio des réseaux Wi-Fi, les architectes réseaux de l'entreprise ont opté pour l'isolation de ce trafic non sécurisé du reste du trafic qui transite dans le système d'information, ceci afin de minimiser les risques liés à l'insécurité des réseaux Wi-Fi.

Rappelons qu'un VLAN est un réseau local regroupant un ensemble de machines de façon logique et non physique. En effet dans un réseau local, la communication entre les différentes machines est régie par l'architecture physique. Grâce aux réseaux locaux virtuels, il est possible de s'affranchir des limitations de l'architecture physique (contraintes géographiques, contraintes d'adressage, etc.) en définissant une segmentation logique (logicielle) basée sur un regroupement de machines grâce à des critères logiques (adresses MAC, numéros de port, protocole, etc.) [22].

Ainsi, l'allocation d'un VLAN particulier aux clients Wi-Fi permet de définir un nouveau réseau au-dessus du réseau physique, ce qui offre les avantages suivants :

- plus de souplesse pour l'administration et les modifications du réseau car toute l'architecture peut être modifiée par simple paramétrage des commutateurs;
- gain en sécurité car les informations sont isolées logiquement du reste du trafic et peuvent éventuellement être analysées;
- réduction de la diffusion du trafic sur le réseau.

Toutefois, compte tenu de l'hétérogénéité des équipements et standards Wi-Fi utilisés et de la différence des profils des utilisateurs 802.11 qui se connectent au système d'information de l'entreprise, cette solution n'est pas flexible et ne s'adapte pas vraiment aux besoins spécifiques de sécurité. En effet, les utilisateurs Wi-Fi qui se connectent au système d'information n'ont pas tous le même profil et n'ont pas tous les mêmes privilèges d'accès aux ressources du système d'information. De plus, l'isolation des clients Wi-Fi à travers un VLAN ne garantit pas l'absence d'attaques radio qui pourraient avoir comme incidence d'empêcher les clients Wi-Fi légitimes d'avoir accès aux ressources du système d'information.

5.1.2 Approche VPN

La seconde approche de sécurisation des réseaux Wi-Fi consiste à déployer des réseaux virtuels privés entre les clients 802.11 et le réseau filaire de l'entreprise. En effet, afin de faire face au manque de sécurité des liens radios des réseaux Wi-Fi, les responsables de sécurité ont opté pour la mise en place de tunnels sécurisés pour protéger le flux d'information qui

transite du client sans fil vers le système d'information de l'entreprise. Dans la majorité des cas, cette mise en place de VPN se fait moyennant le protocole de tunnelisation IPSec[34].

Cette solution a le mérite de renforcer la sécurité des liens radio et de pallier ainsi aux faiblesses des standards de sécurité, notamment le protocole WEP. Ceci d'autant que le protocole IPSec a fait ses preuves et peut être considéré comme étant le meilleur protocole de tunnelisation, en offrant simultanément sécurité et flexibilité (il est possible de privilégier l'authentification ou la confidentialité, en activant AH ou ESP) [6]. Toutefois, il ne faut pas négliger l'importance de la charge qu'ajoutent les VPN à chaque paquet envoyé qui a pour incidence de gaspiller les ressources des liens radio. Ceci est particulièrement vrai dans le cas d'IPSec. En effet, ce dernier bien qu'offrant de bonnes garanties de sécurité, présente l'inconvénient d'alourdir chaque paquet en ajoutant plusieurs entêtes supplémentaires, ce qui a pour effet de surcharger et d'affecter sensiblement les performances globales du réseau Wi-Fi.

Outre l'aspect de surcharge des liens radio du réseau Wi-Fi, l'approche de sécurisation par VPN présente l'inconvénient de centraliser l'accès des clients sans fils au système d'information de l'entreprise. En effet, tous les clients Wi-Fi devront passer par un concentrateur VPN pour avoir accès aux ressources du système d'information, ce qui aura pour incidence de créer un goulot d'étranglement à ce niveau.

De plus, dans le contexte actuel avec un paysage Wi-Fi qui se caractérise par la diversité des équipements et des standards, le recours systématique à une tunnelisation VPN n'est pas toujours justifié. En effet, dans le cas des équipements supportant les standards WPA/WPA2, il n'est nullement nécessaire de mettre en place une connexion VPN. En effet, WPA/WPA2 permet de sécuriser les liens radio et ajouter un VPN à cela, ne ferait qu'encombrer les liens radio et diminuer sensiblement les performances du réseau.

---

34 IP Security (http://www.ietf.org/rfc/rfc2411.txt)

5.1.3 Autres solutions de sécurisation des architectures Wi-Fi

Il est à signaler qu'il n'existe pas un grand nombre de travaux sur la problématique que nous traitons. Ceci n'est pas dû au manque d'intérêt de celle-ci mais c'est surtout à cause du facteur d'instabilité des standards du monde Wi-Fi et la sortie rapide de nouveaux protocoles de sécurité. Parmi les travaux que nous commentons ci-dessous, aucun ne prend vraiment en considération le facteur d'hétérogénéité des équipements et standards existants. En effet, la plupart des travaux ont tendance à se focaliser sur un seul standard de sécurité (généralement WPA2 et WPA) et dénigrer WEP.

La compagnie Cisco a énormément travaillé sur cette problématique architecturale afin de répondre au mieux aux besoins des entreprises. En effet, dans [7] nous trouvons une documentation très riche sur les solutions proposées par Cisco pour résoudre la problématique de sécurisation de l'extension Wi-Fi des systèmes d'information dans l'entreprise. Ainsi, plusieurs architectures et approches de sécurisation ont été proposées selon la taille et la nature du réseau à protéger. Quatre cas de figure ont été distingués : grand réseau WLAN, réseau WLAN de taille moyenne, petit réseau WLAN et réseau WLAN pour utilisateurs distants.

Pour chacun de ces cas, Cisco propose une solution qui s'adapte aux exigences de sécurité. Toutefois, trois critiques majeures peuvent être faites vis-à-vis des solutions Cisco. Toutes les approches proposées se basent sur des plates-formes propriétaires Cisco qui implémentent des protocoles de sécurité version maison, qui ne sont pas toujours compatibles avec les standards. En effet, les différentes solutions proposées dans [7] se basent sur une version améliorée de WEP qui n'est pas compatible avec le standard, ainsi que Cisco TKIP pour les architectures avec WPA et surtout Cisco LEAP en guise de méthode d'authentification.

La seconde critique que l'on peut exprimer vis-à-vis des solutions Cisco est sa focalisation sur la technologie VPN. En effet, Cisco base toute la sécurité du WLAN sur la mise en place de VPN avec selon la taille et la nature du réseau à protéger des VPN logiciels ou matériels, ceci s'accompagnant toujours d'une plate-forme d'administration et un paramétrage très précis à suivre scrupuleusement. Finalement, dans les solutions de Cisco

peu d'égard à été fait au facteur d'hétérogénéité des équipements et standards des clients qui se connectent au WLAN de l'entreprise, ainsi que des équipements Wi-Fi existants dans l'entreprise. En effet, une tendance à homogénéiser les clients et les équipements utilisés est très présente dans les architectures sécurisées proposées par Cisco.

Outre les architectures Cisco, nous trouvons la solution d'Ucopia, documentée dans [6] qui est une solution très complète et assez robuste. Contrairement aux solutions Cisco, Ucopia s'appuie sur les standards existants, donc pas de problème d'incompatibilité. Toutefois, l'architecture Ucopia se distingue par sa complexité et sa difficulté de mise en place dans l'entreprise. En effet, plusieurs bases de données doivent être mises en place pour la gestion des clients Wi-Fi qui se connectent au WLAN de l'entreprise, ceci en plus d'une plate-forme d'administration dont le paramétrage est fastidieux. De plus, tout comme les solutions Cisco, l'approche Ucopia se base sur les VPN et ne réalise pas une différenciation des clients Wi-Fi qui se connectent au WLAN de l'entreprise, selon leurs équipements et les standards de sécurité supportés.

Les auteurs de [22] figurent parmi ceux qui ont le plus traité la problématique qui fait l'objet de notre étude. En effet, dans [22] une approche rigoureuse de sécurisation des réseaux Wi-Fi est proposée. Cette dernière se base sur la différenciation des clients Wi-Fi selon deux catégories principales, à savoir les permanents et les visiteurs. Pour chacun de ces profils un VLAN particulier est attribué. Ainsi, une segmentation logique des clients est opérée au dessus du même réseau physique. Cette approche est rigoureuse et s'adapte bien (quoique partiellement) aux besoins de sécurité et de facilité d'administration exprimés actuellement. Il reste qu'on n'accorde que peu d'attention aux clients Wi-Fi ne pouvant compter que sur le protocole WEP comme mécanisme de sécurité. De plus, nous trouvons que la différenciation réalisée n'est pas suffisante et ne couvre que partiellement la réalité des besoins actuels en termes d'administration et de sécurité. Toutefois, l'usage des VLAN pour établir une différenciation est un élément important sur lequel nous nous sommes d'ailleurs basés pour élaborer notre nouvelle approche.

Au final, nous pouvons dire qu'aucune des solutions proposées ci-dessus ne permet, à elle seule de répondre aux exigences de nombreux administrateurs et responsables de sécurité

Wi-Fi qui souhaitent avoir une différenciation logique d'une part entre l'extension Wi-Fi et le réseau cœur de l'entreprise, ainsi qu'entre les clients Wi-Fi selon leurs profils et les spécificités de leurs équipements. Dans la suite, nous présentons l'approche architecturale de sécurisation Wi-Fi retenue et qui répond aux besoins actuels en termes de sécurité et d'administration.

5.2 Nouvelle approche de sécurisation des architectures Wi-Fi

Il est vrai qu'il existe actuellement une profusion de solutions propriétaires de sécurisation Wi-Fi très robuste telles que celles offertes par Cisco ou Ucopia, qui offrent de très bonnes garanties de sécurité. Toutefois, dans un contexte technologique en perpétuelle mouvance et des sorties de standards en chaîne, les solutions propriétaires devraient être évitées, en raison du manque, voire l'absence, d'interopérabilité entre les diverses solutions proposées sur le marché et surtout avec les standards.

De plus, la démarche de sécurisation de l'architecture doit s'intégrer et utiliser au maximum le parc matériel existant de l'entreprise et non pas ajouter d'autres contraintes liées aux équipements et aux standards de sécurité supportés. L'approche de sécurisation que nous proposons intègre toutes les contraintes et limitations du système d'information de l'entreprise et tire profit de l'hétérogénéité des souches d'équipements/standards (WEP, WPA, WPA2).

Dans ce qui suit, nous présentons les objectifs de l'approche de sécurisation architecturale que nous proposons dans le contexte des réseaux Wi-Fi. Ensuite, nous présentons la démarche suivie et passons en revue les principes sur lesquels nous avons conçu cette nouvelle architecture sécurisée et flexible. Enfin, nous illustrons notre solution en mettant en évidence ses caractéristiques.

5.2.1 Objectifs et méthodologie adoptée

En élaborant cette architecture, nous visons plusieurs objectifs, le plus urgent étant d'assurer une sécurité optimale compte tenu de la vulnérabilité des standards de sécurité Wi-Fi et des menaces qui planent au dessus de tout réseau 802.11. Notre second objectif est de

mettre en place une architecture flexible qui s'adapte au mieux aux besoins spécifiques de sécurité.

Pour cela, nous introduisons une séparation logique entre les différentes catégories de trafic qui transitent sur le système d'information et ce au sein de la même architecture physique. Nous pouvons qualifier notre méthodologie d'analytique, étant donné que nous nous sommes basés sur une analyse approfondie des différentes approches existantes. En effet, en cernant les besoins en sécurité et l'hétérogénéité des équipements et des standards existants, la différenciation des trafics moyennant des VLAN nous semble un impératif. Toutefois, nous faisons un usage plus élaboré des VLAN que celui des approches décrites précédemment. Une fois cette segmentation établie, nous pouvons adapter les mécanismes de sécurité en fonction des spécificités de chaque segment ou niveau de différenciation. Ainsi, nous nous sommes inspirés des différentes approches existantes et proposons une approche architecturale qui englobe la plupart des problématiques soulevées. Dans ce qui suit nous décrivons sur quels principes notre approche a été élaborée.

5.2.2 Principes

Pour élaborer notre solution de sécurisation Wi-Fi, nous avons fait appel aux approches traditionnelles mais que nous employons de façon plus élaborée, afin de satisfaire au mieux les besoins spécifiques de sécurité. En effet, nous nous sommes basés sur le principe de différenciation entre les différentes catégories de trafics qui passent sur le réseau de l'entreprise. Pour matérialiser cette différenciation, nous avons fait appel aux réseaux locaux virtuels afin d'établir trois niveaux de séparation logique. Le premier niveau est relatif aux types d'équipements utilisés par les utilisateurs qui se connectent au réseau 802.11 et aux standards de sécurité Wi-Fi supportés (par exemple : WEP, WPA avec TKIP, WPA2 avec AES). Ainsi, nous opérons une première différenciation des utilisateurs selon la catégorie de leurs équipements/standards. Cette différenciation permet d'adapter les mécanismes de sécurité et d'authentification en fonction des vulnérabilités des standards implantés sur le matériel.

Ensuite, nous opérons un second niveau de différenciation qui vient à la suite de l'authentification des clients 802.11. Ce second niveau de différenciation vient établir un

VLAN par profil d'utilisateur. Finalement, nous mettons en place un troisième niveau de différenciation relatif au trafic de gestion et d'administration du système d'information.

Outre cet aspect de différenciation de trafic, nous faisons appel au protocole TLS[35], afin de mettre en place des canaux de communication sécurisés pour les transmissions des clients 802.11 ayant le protocole WEP comme seul mécanisme de sécurité. Dans ce qui suit, nous explicitons tous ces éléments avec plus de détails.

5.2.3 Présentation de l'architecture

Comme décrit plus haut, l'approche que nous proposons repose sur l'utilisation d'un canal sécurisé et de réseaux locaux virtuels (VLAN) avec trois niveaux de différenciation. En effet, en étudiant de près les besoins des entreprises en termes de connectivité Wi-Fi, et prenant en compte les différentes souches d'équipements existantes (WEP, WPA, WPA2), nous avons choisi d'établir trois niveaux de différenciation matérialisés par des réseaux locaux virtuels. Ces niveaux de différenciation sont les suivants :

- Premier niveau : différenciation selon le type d'équipement Wi-Fi utilisé, ou encore selon le standard de sécurité supporté (WEP, WPA, WPA2);
- Second niveau : différenciation selon le profil de l'utilisateur de l'extension Wi-Fi du réseau de l'entreprise.
- Troisième niveau : permet d'isoler le trafic relatif à la gestion et l'administration du système d'information.

Ainsi, pour le premier niveau de différenciation nous avons choisi de le matérialiser avec deux VLAN : un premier VLAN pour les utilisateurs avec des équipements Wi-Fi basé sur le chiffrement WEP et ne supportant pas une migration vers des standards de sécurité plus évolué. En effet, la plupart des responsables de sécurité et de systèmes d'informations ont tendance à oublier cette catégorie d'utilisateurs et insistent sur le manque de sécurité et la nécessité de migrer vers les nouveaux standards de sécurité Wi-Fi. Toutefois, dans notre

---

35 Transport Layer Security (http://www.ietf.org/rfc/rfc2246.txt)

approche nous privilégions la flexibilité et mettons cette hétérogénéité d'équipements et de standards comme contrainte de base à satisfaire impérativement dans l'élaboration de notre architecture. Le second VLAN sera réservé à la communauté des utilisateurs avec des équipements compatibles WPA/WPA2. De cette manière le premier niveau de filtrage et d'isolation est basé sur un critère d'équipements et de standards supportés.

Quant au second niveau de différenciation qui se base sur le profil de l'utilisateur, nous avons supposé l'existence de trois types d'utilisateurs du système d'information de l'entreprise. Ces trois types d'utilisateurs sont les suivants :

- Les permanents : ce sont les employés de l'entreprise qui ont un accès total au système d'information et qui doivent bénéficier d'une authentification forte pour assurer la sécurité de leur accès aux ressources du système d'information.

- Les partenaires : il s'agit d'employés d'autres entreprises partenaires. Cette famille d'utilisateurs aura un accès restreint aux ressources du système d'information.

- Les visiteurs : il s'agit des visiteurs de l'entreprise et qui requièrent un accès à Internet. Cette dernière communauté d'utilisateurs devrait avoir un accès simplifié mais contrôlé à l'internet.

Le troisième niveau permet de séparer le trafic d'administration et d'authentification du reste des trafics. Ceci convient aux administrateurs réseaux en facilitant la gestion du système d'information et en permettant d'avoir un meilleur contrôle des accès aux diverses ressources. Dans le tableau 5.1, nous récapitulons les différents VLAN associés à chaque niveau de différentiation.

Niveau de différenciation	Standard de sécurité WI-Fi	Profil du client Wi-Fi	Nature du trafic
VLAN associés	VLAN WEP	VLAN Permanents	VLAN d'authentification et de gestion
	VLAN WPA/WPA2	VLAN Partenaires	
		VLAN Visiteurs	

Tableau 5.1 : Niveaux de différenciation et VLAN associés

Outre cette différenciation, nous avons choisi d'utiliser le protocole TLS pour sécuriser les échanges avec la communauté des clients 802.11 ayant le protocole WEP comme mécanisme de sécurité (communauté WEP), ceci afin de pallier au manque de sécurité de cette dernière. En effet, compte tenu de la facilité de cassage des clés WEP avec des logiciels disponibles sur Internet, il est primordial d'ajouter un niveau de sécurité supplémentaire afin de faire transiter le trafic WEP. Pour ce faire, nous avons choisi d'utiliser TLS et non pas IPSec, essentiellement à cause de la grande charge que ce dernier impose aux liens radio, de manière à affecter le moins possible les performances globales du réseau sans fil.

À part les mécanismes de VLAN et de sessions sécurisées avec TLS, nous mettons en place des zones démilitarisées en se servant de coupe-feu (voir figure 5.1).

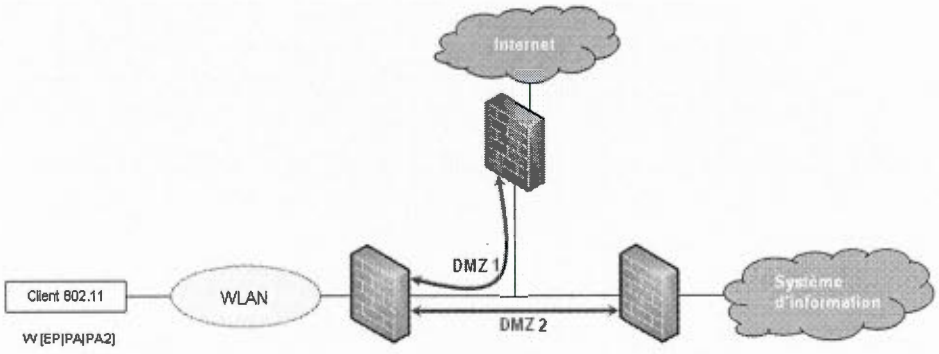


Figure 5.1 : Mise en place de zones démilitarisées

En effet, nous protégeons l'accès depuis le monde Wi-Fi aux serveurs d'authentifications de l'entreprise (voir la figure 5.2), à l'aide d'un premier coupe-feu, pour constituer la première zone démilitarisée, qui donne accès à Internet pour les clients Wi-Fi authentifiés en tant que visiteurs. Quant aux permanents et partenaires, ces derniers seront réacheminés vers une seconde zone démilitarisée. Ainsi, l'accès aux ressources depuis le WLAN est renforcé.

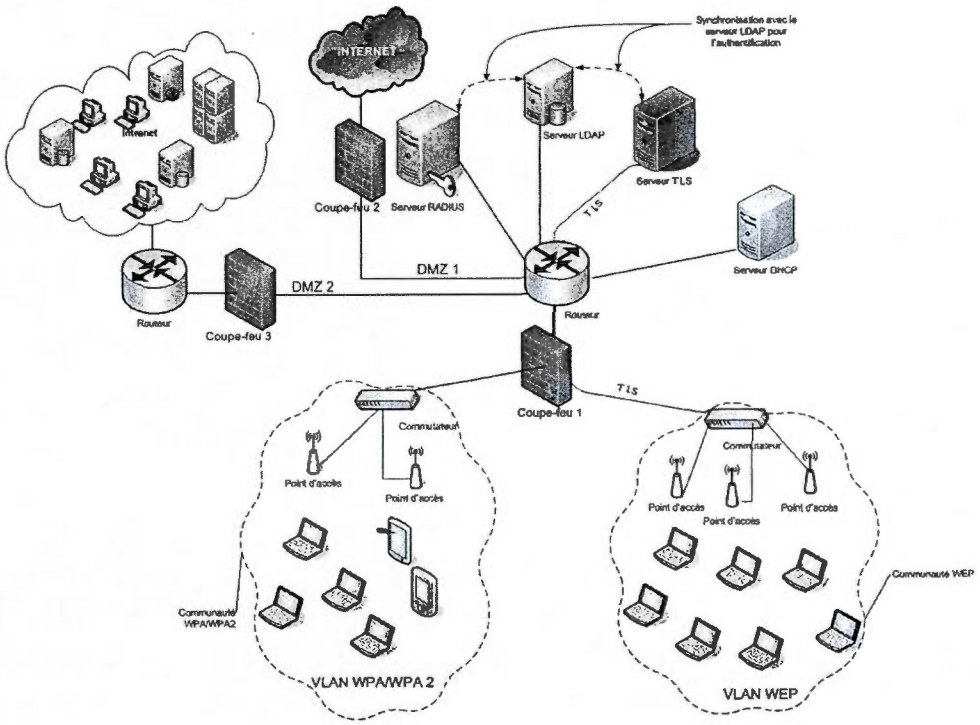


Figure 5.2 : Architecture Wi-Fi sécurisée

Comme illustré dans la figure 5.2, nous avons choisi de placer le serveur d'authentification TLS pour l'établissement du canal TLS sécurisé avec les clients de la communauté WEP derrière le premier coupe-feu. Ceci en plus d'un serveur RADIUS pour l'authentification des clients de la communauté WPA/WPA2. Ces deux derniers serveurs,

sont en communication avec le serveur LDAP[36] de l'entreprise qui comporte les profils de tous les utilisateurs autorisés à avoir accès aux ressources du système d'information. En effet, dans la grande majorité des cas, les entreprises utilisent LDAP ou Active Directory afin de stocker les profils avec les droits d'accès des utilisateurs. De plus, pour pouvoir authentifier les utilisateurs de la communauté WPA/WPA2, il est impératif d'utiliser un serveur RADIUS et pas n'importe lequel : il doit être compatible EAP-RADIUS, ce qui n'est pas le cas de tous les produits de commerce. Il est ensuite nécessaire de gérer les connecteurs vers l'annuaire LDAP ou Active Directory de l'entreprise. Ainsi, il faut savoir adapter le mappage RADIUS-LDAP, qui n'est pas une mince affaire.

Nous avons également choisi de mettre en place un serveur DHCP pour l'attribution d'adresses IP aux clients 802.11. Ce serveur DHCP permettra de mettre en place un adressage IP dynamique et privé, selon des règles d'adressage par VLAN, de façon à permettre l'identification de chaque client 802.11 par la classe de son adresse IP.

En élaborant cette approche de sécurisation Wi-Fi, nous avions comme objectif de pouvoir supporter plusieurs architectures logiques, sur la même architecture physique. Cela a pu être possible grâce au déploiement de plusieurs VLAN. En observant ces différents niveaux de différenciation, on pourrait se poser les questions suivantes : comment gérer la différenciation ? Comment définir l'appartenance à un groupe de manière automatique ? La réponse à ces questions est très simple : tout est géré au niveau des commutateurs.

En effet, pour la mise en place du premier niveau de différenciation, c'est-à-dire VLAN par famille d'équipements (WEP, WPA/WPA2), il suffit d'associer un nom de réseau (SSID) à un VLAN. Ainsi, chaque SSID/VLAN peut bénéficier d'une authentification spécifique. Un client Wi-Fi se connectant à un point d'accès avec un SSID particulier se trouvera automatiquement membre d'un VLAN particulier. Il est à rappeler que la majorité des points d'accès supportent les SSID multiples et la correspondance SSID/VLAN. Un point d'accès peut comporter plusieurs SSID, chacun associé à un VLAN particulier.

---

36 Lightweight Directory Access Protocol

Ainsi, un client 802.11 associé à un point d'accès appartiendra à un VLAN particulier (VLAN WEP ou VLAN WPA/WPA2) dès le départ. Une fois authentifié, par exemple en tant que visiteur, le client sera affecté à un nouveau VLAN, celui relatif à la communauté des visiteurs. Cette réaffectation d'un VLAN à un autre se fait en changeant le marquage des paquets émis ou reçus par le client 802.11 en question. Pour cela, les commutateurs utilisés devraient supporter l'étiquetage (*tagging*) IEEE 802.1Q. Ce sont les mêmes commutateurs utilisés pour l'établissement des VLAN du premier niveau de différenciation, qui seront utilisés pour le déploiement des VLAN du second niveau de différenciation (visiteurs, partenaires, permanents). Ainsi, nous pourrons aboutir à une configuration logique tel que montrée par la figure 5.3.

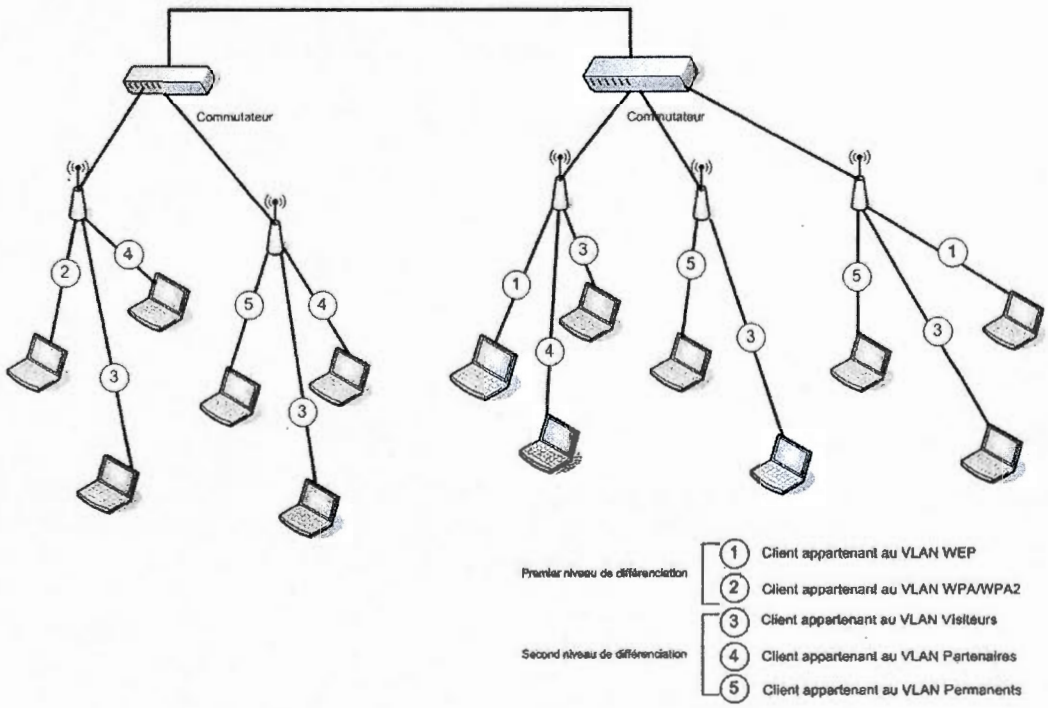


Figure 5.3 : Niveaux de différenciation et VLAN associés

La différenciation du premier niveau selon le standard de sécurité Wi-Fi supporté sert à réaliser une séparation logique entre les différentes communautés d'utilisateurs (WEP,

WPA/WPA2) afin de leur appliquer le niveau de sécurité adéquat. Une fois authentifiés, les clients 802.11 seront réaffectés aux VLAN du second niveau de différenciation. Ainsi, au fur et à mesure que les clients 802.11 sont authentifiés, il y aura de moins en moins de clients appartenant aux VLAN du premier niveau de différenciation, au profit des VLAN du second niveau de différenciation (visiteurs, partenaires, permanents).

Il est à noter que tout le trafic relatif à l'authentification des clients, la gestion et les flux entre les différents serveurs (DHCP, LDAP, RADIUS, TLS) est isolé du reste du trafic en utilisant un VLAN spécifique à ces fonctions.

Ce découpage en plusieurs VLAN répond aux exigences de nombreux administrateurs de réseaux qui souhaitent bénéficier d'infrastructures logiques différentes afin de pouvoir exercer une meilleure gestion ainsi qu'un un meilleur contrôle des différents flux qui transitent envers et à partir du système d'information filaire de l'entreprise [7].

Dans le chapitre suivant, nous procédons à l'évaluation de l'approche que nous proposons et sa validation par le biais d'évaluation de performance et d'étude comparative avec d'autres alternatives de sécurisation de réseau Wi-Fi.

CHAPITRE VI

ÉVALUATION DE LA NOUVELLE ARCHITECTURE WI-FI SÉCURISÉE

Dans le chapitre précédent, nous avons présenté la nouvelle architecture de sécurisation Wi-Fi que nous proposons et qui favorise principalement la sécurité et la flexibilité. Comme dans toute démarche scientifique rigoureuse, nous allons dans ce chapitre valider notre contribution en établissant une évaluation de performance ainsi qu'une étude comparative avec d'autres architectures Wi-Fi dans l'entreprise, ceci selon les critères les plus pertinents.

Ainsi, la suite de ce chapitre s'articule comme suit : une première section qui présente une évaluation d'un point de vue qualitatif qui met en évidence les caractéristiques principales de notre architecture. Ensuite, nous établissons l'évaluation quantitative qui illustre la valeur ajoutée de notre solution par rapport à d'autres solutions.

6.1 Évaluation qualitative

Pour évaluer qualitativement l'approche que nous proposons, nous pouvons mettre en évidence ses apports par rapport aux approches architecturales conventionnelles et propriétaires pour la sécurisation du Wi-Fi dans l'entreprise. En effet, si on devait résumer les apports de notre solution, nous pourrions énumérer les éléments suivants :

- Différenciation logique sur plusieurs niveaux :

Contrairement aux approches conventionnelles par VPN simple ou par VLAN pour les clients Wi-Fi, notre approche met une séparation logique très élaborée entre les clients 802.11 du réseau Wi-Fi de l'entreprise. En effet, outre l'isolation du trafic de gestion du système

d'information, nous mettons en place deux niveaux de différenciation: le premier relatif à l'équipement du client sans fil, qui permet d'adapter le niveau de sécurité et la méthode d'authentification aux standards de sécurité supportés par le client. Le second niveau de différenciation est relatif aux profils des clients 802.11. Cette dernière différenciation permet aux administrateurs d'avoir un meilleur contrôle de l'accès aux ressources du système d'information. De plus, la séparation en plusieurs VLAN sur plusieurs niveaux est totalement transparente pour le client 802.11 qui se connecte au réseau Wi-Fi de l'entreprise.

- Utilisation de TLS au lieu d'IPSec :

Contrairement aux approches traditionnelles de sécurisation Wi-Fi qui font appel à IPSec, nous avons choisi d'utiliser le protocole TLS pour l'établissement d'un canal de communication sécurisé entre le serveur TLS et les clients sans fil de la communauté WEP, ceci compte tenu de la faiblesse du mécanisme de sécurité WEP. La technologie VPN vise la sécurisation des données de l'utilisateur et suppose l'insécurité des liens utilisés (ce qui est le cas des liens Wi-Fi chiffrés avec WEP). Toutefois, les VPN ajoutent une charge considérable à chaque paquet envoyé et gaspillent les ressources des liens radio. Ceci est particulièrement vrai dans le cas de l'utilisation d'IPSec. En effet, le protocole IPSec bien qu'offrant de bonnes garanties de sécurité et est bien adapté à la tunnelisation, a le défaut d'ajouter des entêtes à chaque paquet, surchargeant ainsi le lien de transmission de données. Ceci est particulièrement pénalisant dans un contexte de lien radio tel que les réseaux Wi-Fi. C'est pourquoi, nous avons opté pour l'utilisation de TLS qui en offrant un bon niveau de sécurité, ne charge pas le lien de transmission et est léger relativement à IPSec.

- Mise en place de deux zones démilitarisées :

Nous avons choisi de mettre en place deux zones démilitarisées pour protéger l'accès aux ressources du système d'information. La première zone démilitarisée protège l'accès aux divers serveurs (TLS, DHCP, RADIUS, LDAP), ainsi que l'accès à Internet par la communauté des visiteurs. Une seconde zone démilitarisée vient renforcer la sécurité pour l'accès à l'intranet et aux ressources délicates du système d'information. Cette double barrière ne fait que renforcer la sécurité, en facilitant le contrôle et le filtrage des différents

flux, ainsi que l'audit des opérations d'accès aux ressources : fonction qui fait terriblement défaut aux administrateurs dans le contexte d'accès Wi-Fi aux systèmes d'information.

6.2 Évaluation quantitative

Comme nous l'avons dit précédemment, la validation de toute contribution scientifique est une étape importante dans tout cheminement scientifique expérimental qui se respecte.

Il est vrai que dans notre cas, la meilleure manière d'évaluer la performance de notre solution serait de mettre en œuvre l'architecture que nous proposons avec tous les équipements matériels nécessaires, ceci en plus de l'établissement d'un banc d'essai permettant de mesurer les performances de la solution proposée pour les comparer à d'autres. Toutefois, nous ne disposons pas de moyens et de laboratoires expérimentaux pour considérer cette option.

La seconde option serait de recourir à une simulation. Ainsi, nous avons réalisé une simulation à l'aide du logiciel QualNet[37]. Cette simulation nous a permis de comparer les performances de notre solution vis-à-vis d'autres approches. L'élément le plus pertinent à évaluer est certainement l'impact de la surcharge appliquée sur l'ensemble des communications transitant sur le réseau Wi-Fi. En effet, nous n'évaluons pas la sécurité de notre architecture, d'une part car il n'existe pas de méthodologie de validation pour la sécurité à un niveau architectural. D'autre part, nos choix pour la sécurité dans notre approche se sont basés sur des protocoles ayant fait leurs preuves en matière de robustesse et de résistance aux attaques. Dans notre processus d'élaboration de l'architecture que nous proposons, le défi majeur que nous avons essayé de remporter est d'allier sécurité, flexibilité et utilisation optimale des ressources du réseau.

Ainsi, pour montrer l'intérêt de notre approche, nous allons dans ce qui suit démontrer ses avantages et justifier nos choix par rapport aux approches traditionnelles par une analyse quantitative de la surcharge appliquée sur chaque paquet.

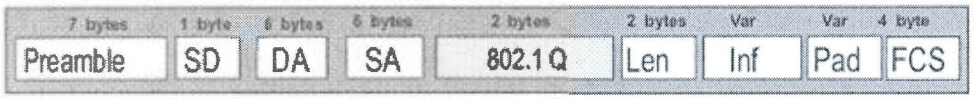
---

37 http://www.scalable-networks.com/

6.2.1 Surcharge appliquée par l'association à un VLAN

Certains pourront penser qu'avec l'utilisation de plusieurs VLAN conjugués à l'utilisation du protocole TLS, constitue une grande charge pour le support hertzien des réseaux Wi-Fi. Toutefois, ce point de vue n'est pas tout à fait fondé, vu que l'utilisation des VLAN n'ajoute que deux octets supplémentaires et ne se fait pas moyennant une encapsulation des paquets dans d'autres enveloppes.

En fait, il s'agit de réaliser un marquage 802.1Q des paquets pour les identifier par rapport au VLAN sur lequel ils doivent transiter. Ce marquage se fait en ajoutant un entête de deux octets à la trame. La figure 5.4 montre le positionnement et la taille du marquage 802.1Q dans une trame IEEE 802.3.



SD : Start Frame Delimitor
DA : Destination Address
SA : Source Address
Len : Taille de la zone de données
Inf : Données
Pad : Bourrage
FCS : Séquence de contrôle pour la détection d'erreur

802.1Q :

TPI : Tag Protocol Identifier
VI : VLAN Identifier

Figure 6.1 : Trame IEEE 802.3 avec marquage 802.1Q [2]

En transitant d'un VLAN à un autre, il y a juste un changement au niveau du champ 802.1Q qui s'opère. De plus, l'association d'un client à un VLAN en particulier, se fait automatiquement sans aucun message de signalisation. Le client 802.11 en s'associant à un point d'accès avec un SSID particulier s'associe automatiquement au VLAN correspondant. Comme nous l'avons mentionné dans le chapitre précédent, chaque SSID est relatif à un VLAN particulier.

De ce fait, nous pouvons affirmer que la surcharge relative à l'association et la transition d'un VLAN à un autre est minime (deux octets) et ne constitue en aucun cas une lourdeur pour le réseau Wi-Fi.

6.2.2 Surcharge et signalisation pour la mise en place de TLS

Outre l'utilisation des VLAN, nous adoptons dans notre solution l'établissement d'un canal de communication sécurisé au moyen du protocole TLS.

Pour justifier le choix du protocole TLS, nous allons dans ce qui suit montrer la différence de charge appliquée par TLS et un VPN IPSec. En effet, en établissant un VPN à base du protocole IPSec, nous allons avoir une surcharge sur chaque paquet transmis, qui varie selon le mode (transport ou tunnel) et le sous-protocole utilisé (AH ou ESP). Le tableau 5.2 montre la surcharge (*overhead*) appliquée à chaque paquet en fonction des différents modes et sous-protocoles d'IPSec.

Protocole	Mode	Taille surcharge (en bits)
IPSec mode transport	ESP	32
	ESP et AH	44
IPSec mode tunnel	ESP	36
	ESP et AH	48

Tableau 6.1 : Taille de la surcharge du protocole IPSec

Ainsi, tel qu'illustré par le tableau 6.1, l'établissement d'un VPN au moyen du protocole IPSec, implique une surcharge de 4 à 6 octets sur chaque paquet. Contrairement à IPSec qui opère au niveau de la couche réseau du modèle de référence, TLS est un protocole du niveau session, tout juste au dessus de la couche de transport. L'entête du protocole TLS est de quatre octets sur chaque paquet [10]. Elle se décompose comme suit :

- *Content-Type* (1 octet) : Indique le type de paquet TLS:

0x20 - Paquet de type *Change Cipher Spec*
0x21 - Paquet de type *Alert*
0x22 - Paquet de type *Handshake*
0x23 - Paquet de type *Application Data* : ce type correspond aux données effectives de la session SSL.

- *Major Version* (1 octet), *Minor Version* (1 octet) - Numéros de versions principal et secondaire du protocole TLS utilisé.
- (Compressed) Length (1 octet) - Taille (compressée s'il y a lieu) du fragment SSL et TLS.

Toutefois, il ne faut pas négliger le fait que cette diminution de charge avec TLS se fait au dépend d'un certain manque de sécurité, comparativement à IPSec en mode tunnel qui en encapsulant les adresses IP source et destination offre de meilleures garanties de sécurité. En mode transport, IPSec n'offre pas plus de sécurité que TLS, vu que les adresses IP sources et destinations transitent en clair sur le réseau.

Par ailleurs, avec TLS il n'est pas nécessaire d'installer de logiciel spécifique sur le client pour atteindre le réseau de l'entreprise, contrairement au VPN IPSec. Ceci est dû au fait qu'aujourd'hui TLS est supporté par la majorité des systèmes d'exploitation.

6.2.3 Évaluation de performance de la nouvelle architecture

La sécurité est une arme à deux tranchants. En effet, il est bien possible de mettre en place une architecture avec une sécurité renforcée, moyennant les protocoles et algorithmes cryptographiques des plus solides. Toutefois, le revers de la médaille de cette sécurité renforcée est souvent la surcharge du support de transmission, ainsi que le manque de flexibilité qui vient du caractère limitatif et inhibiteur intrinsèque à tout mécanisme de sécurité. C'est pourquoi, tout architecte systèmes tente d'aboutir au savant dosage entre sécurité, facilité d'utilisation et surtout utilisation optimale des ressources du réseau. Ainsi, pour évaluer la performance de notre solution, nous nous concentrons dans cette section à l'évaluation de l'impact de la surcharge de signalisation par l'empilement de VLAN, de VPN, WEP et WPA/WPA2 sur la bande passante utile du réseau Wi-Fi. Ainsi, nous entendons par évaluation de performance dans notre contexte, l'évaluation de l'impact des mécanismes de sécurité présents dans l'architecture que nous proposons sur le débit utile de chaque client. Pour ce faire, nous considérons trois solutions différentes :

1. La première solution que nous intitulons *sécurité nulle*, permet aux clients 802.11 de se connecter au réseau Wi-Fi de l'entreprise, sans aucune considération de sécurité. En d'autres termes, aucun mécanisme de sécurité n'est utilisé, pas même le protocole WEP.

2. La seconde solution se base sur la mise en place d'un tunnel IPSec pour permettre la connexion des clients 802.11 au réseau Wi-Fi, indépendamment du type de l'équipement et du standard de sécurité supporté (WEP ou WPA/WPA2). Il est à noter que nous distinguons deux cas pour cette solution : *IPSec-WEP* pour la communauté WEP et *IPSec-WPA/WPA2* pour la communauté WPA/WPA2. Dans la suite, nous dénotons cette solution par *solution IPSec.*

3. La troisième solution n'est autre que l'architecture que nous proposons qui se base sur la différenciation de trafic moyennant des VLAN et la mise en place de TLS pour la communauté WEP. Comme pour la solution 2, nous considérons deux cas relatifs aux communautés WEP et WPA/WPA2. Dans la suite, nous faisons référence à cette solution par *AWSF* (Architecture Wi-Fi Sécurisée et Flexible).

Dans ce qui suit, nous décrivons plus en détail chacune des solutions considérées avec les scénarios de simulation que nous avons mis en place.

6.2.3.1 Scénario 1 : solution avec sécurité nulle

Comme décrit précédemment, dans cette solution nous ne considérons aucun mécanisme de sécurité. Il est bien évident qu'une telle option n'est pas envisageable dans un contexte réel. Toutefois, dans une optique d'évaluation de performance, cette solution nous servira comme une base de référence pour comparer les autres solutions qui intègrent des mécanismes de sécurité.

Ainsi, en utilisant l'outil de simulation QualNet, nous avons mis en place le réseau Wi-Fi matérialisé par un point d'accès *Linksys WAP55AG* capable de gérer les trois normes 802.11a, b et g offrant un débit théorique de 54 Mbps et des clients 802.11. Ainsi, dans notre processus de simulation, nous faisons varier le nombre de clients Wi-Fi et observons

l'évolution du débit utile pour chaque client. Dans notre simulation, nous avons fixés un taux d'atténuation d'environ 15%, qui correspond à une atténuation minimale dans un environnement dégagé, présentant très peu d'obstacles.

Il est à noter que physiquement la plupart des points d'accès Wi-Fi gèrent un maximum théorique de 128 clients. Dans la pratique, une limite d'environ 15 à 25 clients (selon l'atténuation du signal par les obstacles et la distance) doit être respectée pour tirer un usage acceptable de la bande passante. La figure 6.2 montre l'évolution du débit utile par client en fonction de l'augmentation du nombre de clients se connectant au même point d'accès.

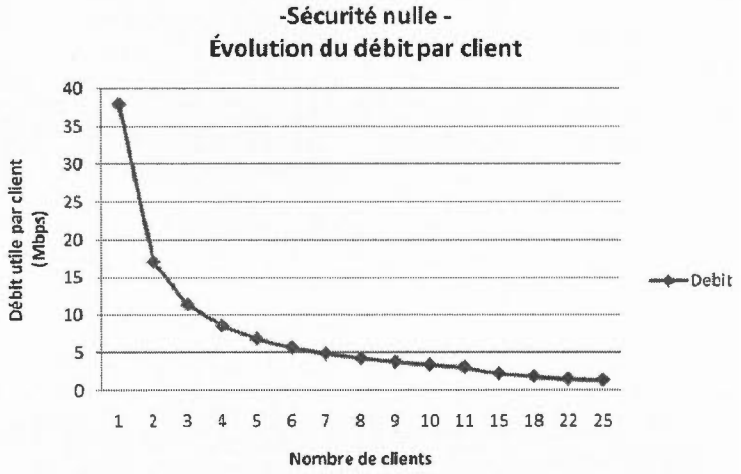


Figure 6.2 : solution avec sécurité nulle

Tel que nous le prévoyons, le débit utile par client diminue au fur et à mesure que le nombre de clients 802.11 augmente. Ainsi, le point d'accès permet de connecter près de 25 clients, avec un débit utile par client d'environ 1,5 Mbps. Ce scénario constituera pour nous le point de référence avec lequel nous pourrons comparer la performance des autres solutions considérées, vu qu'il y a très peu de signalisation.

6.2.3.2 Scénario 2 : solution IPSec

Dans ce scénario, tous les clients Wi-Fi se connectent au point d'accès moyennant la mise en place d'un VPN IPSec. Ceci en plus des mécanismes de sécurité Wi-Fi à savoir WEP, WPA et WPA2. Ainsi, tous les clients 802.11 qu'ils utilisent WEP ou WPA/WPA2 comme mécanismes de sécurité Wi-Fi devront tout d'abord établir un tunnel IPSec pour se connecter au point d'accès. C'est pourquoi, nous distinguons deux cas dans ce même scénario :

Cas 1 : Clients 802.11 avec le mécanisme de sécurité WEP

Dans ce premier cas, les clients 802.11 devront en premier lieu établir le tunnel IPSec avec le point d'accès. Suite à cela, le client amorce l'authentification WEP. Ainsi, en réalisant la simulation, en utilisant le même point d'accès que celui utilisé lors du scénario 1, nous obtenons la figure 6.3, qui montre l'impact du nombre de clients 802.11 qui se connectent sur le débit utile par client.

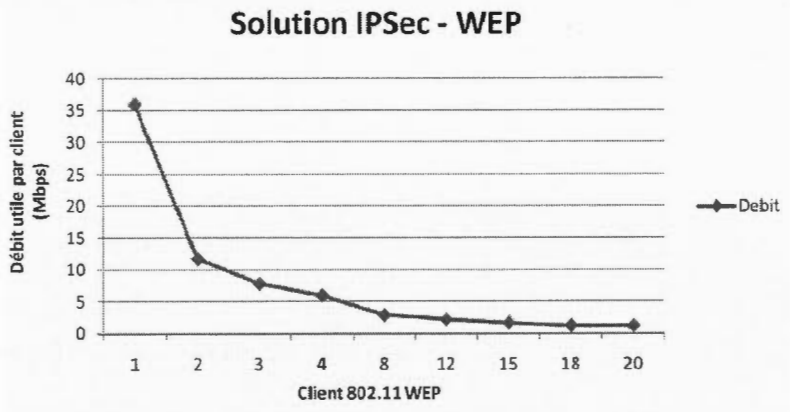


Figure 6.3 : solution IPSec avec des clients 802.11 utilisant WEP

Comme nous pouvons le remarquer, le débit utile par client diminue plus rapidement que dans le cas du scénario 1 présenté préalablement, ceci est dû principalement au poids de la signalisation plus important dans ce scénario. En effet, après la connexion d'un vingtième client 802.11 au point d'accès, le débit utile par client descend vers 1,29 Mbps.

Cas 2 : Clients 802.11 avec les mécanismes de sécurité WPA/WPA2

Comme dans le cas 1, les clients Wi-Fi supportant les mécanismes de sécurité WPA ou WPA2 devront en premier lieu établir un tunnel IPSec avec le point d'accès, suite à quoi les échanges WPA2 ou WPA ont lieu. Les résultats de la simulation sont donnés dans la figure 6.4.

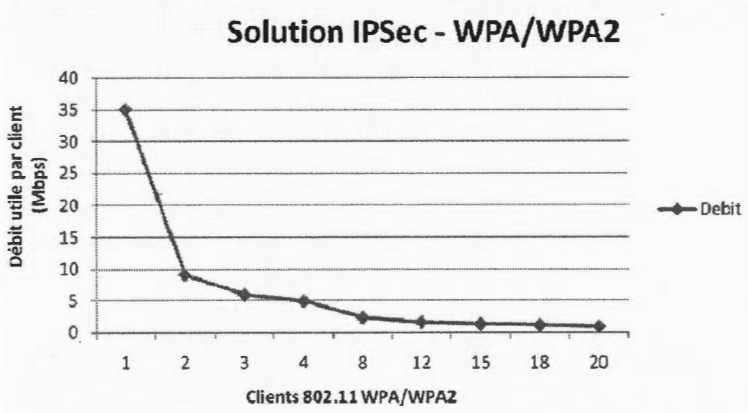


Figure 6.4 : solution IPSec avec des clients 802.11 utilisant WPA/WPA2

La courbe présentée dans la figure 6.4 montre l'impact du nombre de clients Wi-Fi connectés sur le débit utile alloué par client. Nous pouvons remarquer que la bande passante utile par client s'atténue plus rapidement que dans le cas 1 de ce même scénario (le vingtième client a un débit utile de 0,98 ≈ 1 Mbps). Ceci s'explique par le fait que les mécanismes WPA/WPA2 imposent plus de signalisation que le protocole WEP. Il est à signaler que la courbe présentée ci-dessus, illustre la moyenne des débits obtenus respectivement pour les clients WPA et les clients WPA2.

Ce scénario démontre l'impact de la mise en place d'un VPN IPSec pour toutes les catégories de clients 802.11, indépendamment du fait qu'ils supportent WEP ou WPA/WPA2.

6.2.3.3 Scénario 3 : solution AWSF

Ce dernier scénario s'intéresse à l'approche que nous proposons dans le cadre de ce mémoire. Ainsi, dans notre simulation, nous prenons en considération la mis en place de TLS pour la communauté WEP et la différenciation de trafic moyennant des VLAN. Toutefois, dans notre simulation nous considérons uniquement les VLAN du premier niveau (VLAN WEP et VLAN WPA/WPA2). En effet, à cause des limitations que nous impose l'outil de simulation QualNet, nous ne pouvons matérialiser le changement des clients d'un VLAN à un autre. Toutefois, cela n'altère en rien les résultats que nous avons obtenus, vu qu'un client 802.11, selon notre architecture ne peut appartenir à deux VLAN à la fois. Comme dans le cas du scénario 2, nous distinguons pour ce scénario 3 les deux cas suivants :

Cas 1 : Clients 802.11 avec le mécanisme de sécurité WEP

Dans ce premier cas, les clients 802.11 supportant le protocole WEP appartiennent tous au VLAN de la communauté WEP. Suite à cela il y a établissement d'une session TLS, dans laquelle se déroulera l'authentification WEP. La figure 6.5 illustre les résultats obtenus par la simulation.

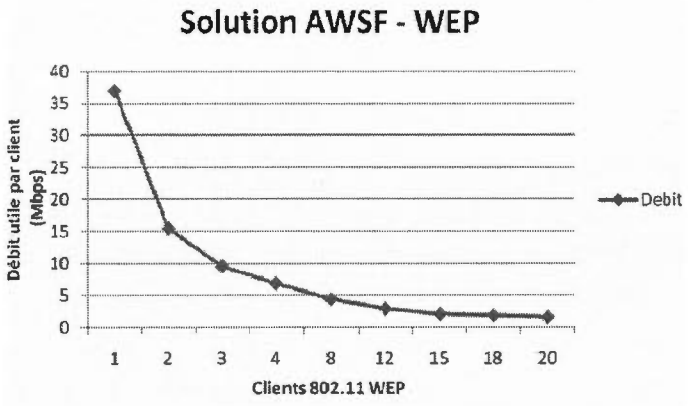


Figure 6.5 : solution AWSF avec des clients 802.11 utilisant WEP

Comme nous pouvons le remarquer, le débit utile par client diminue moins rapidement et avec une moindre amplitude que dans le cas 1 du scénario 2, avec IPSec (le vingtième

client qui se connecte dispose d'un débit utile de 1,58 Mbps, soit une amélioration d'environ 22% par rapport à IPSec-WEP).

Cas 2 : Clients 802.11 avec les mécanismes de sécurité WPA/WPA2

Cette catégorie de clients appartient au VLAN de la communauté WPA/WPA2. Suite aux rattachements au point d'accès et l'association au VLAN WPA/WPA2, les échanges WPA/WPA2 ont lieu afin d'établir le canal de communication sécurisé, sans avoir recours à un VPN.

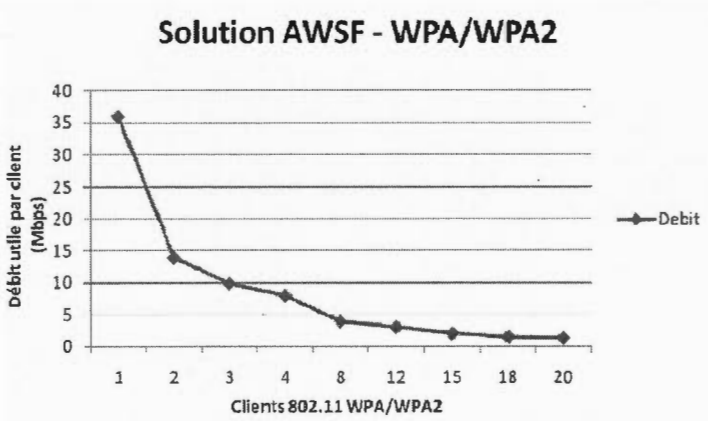


Figure 6.6 : solution AWSF avec des clients 802.11 utilisant WPA/WPA2

La courbe présentée dans la figure 6.6 illustre les résultats obtenus par simulation. Nous pouvons remarquer que le débit utile par client s'atténue moins rapidement que dans le cas 2 du scénario 2, qui implique la mise en place d'un VPN IPSec. Il est à signaler que la courbe présentée ci-dessus, illustre la moyenne des débits obtenus respectivement pour les clients WPA et les clients WPA2.

La figure 6.7 illustre l'évolution du débit utile par client en fonction du nombre de clients connectés, pour la solution IPSec et la solution AWSF, relativement à la communauté WEP.

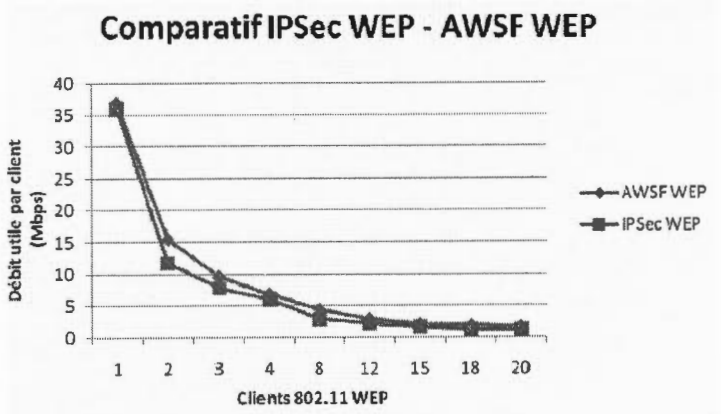


Figure 6.7 : comparatif IPSec - AWSF pour la communauté WEP

Ainsi, nous pouvons remarquer que la solution AWSF que nous proposons donne une meilleure performance que la solution IPSec (pour la communauté WEP, AWSF donne un débit utile par client supérieur de 22% à celui fourni avec la solution IPSec, pour 20 clients). Ceci est également valable pour les clients 802.11 supportant les standards de sécurité WPA/WPA2, tel que le montre la figure 6.8.

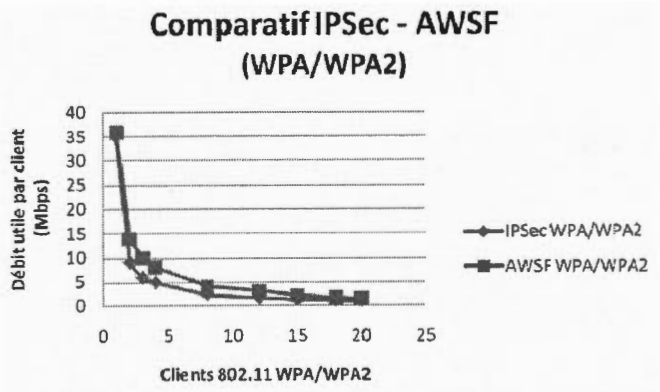


Figure 6.8 : comparatif IPSec - AWSF pour la communauté WPA/WPA2

Ainsi, pour la communauté WPA/WPA2 la solution AWSF donne un débit utile par client supérieur d'environ 34% à celui avec IPSec (pour 20 clients). Dans la figure 6.9, nous illustrons le comportement des trois solutions considérées face à la charge de signalisation qu'ils imposent au réseau. Ainsi comme le montre le graphique, la solution AWSF que nous

proposons a une moindre performance en termes de charge de signalisation par rapport à la solution avec sécurité nulle, ce qui est très prévisible. D'un autre côté, la solution AWSF présente une relative meilleure performance que la solution IPSec. En effet, cette dernière surcharge le réseau très rapidement, ceci à cause de la charge cryptographique et de signalisation relativement importante d'IPSec.

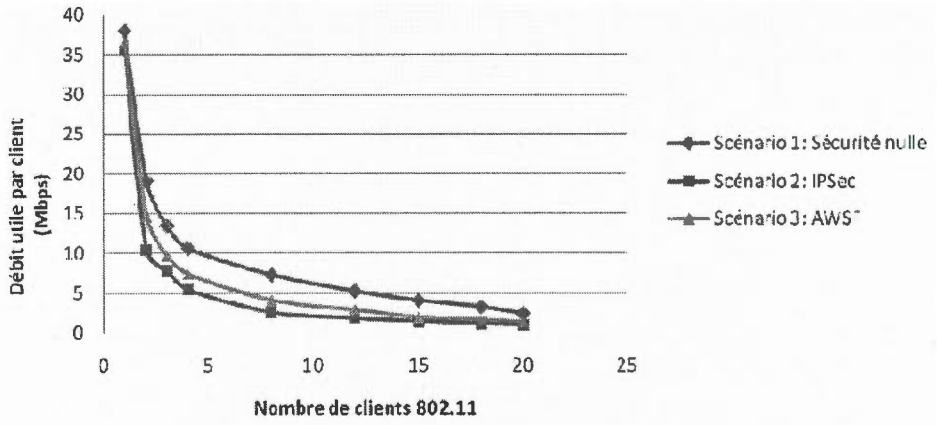


Figure 6.9 : comparatif *Sécurité nulle - AWSF - IPSec*

Ainsi, outre le fait de présenter une flexibilité indéniable (à cause de la différenciation du trafic moyennant les VLAN), la solution AWSF constitue également une solution légère qui permet d'optimiser l'utilisation de la bande passante dans le réseau : élément d'une importance capitale et à ne pas négliger surtout dans un contexte de réseaux Wi-Fi.

Quant à la vérification de l'atteinte de l'objectif de sécurité, il faut savoir qu'il n'existe pas de méthodologie d'évaluation de la sécurité à un niveau architectural. En effet, il est bien possible de vérifier la sécurité au niveau protocolaire moyennant une approche formelle. Toutefois, dans le cas d'un empilement de protocoles tel que nous l'avons proposé dans notre approche, il devient très difficile d'évaluer quantitativement le niveau de sécurité atteint. Par ailleurs, il faut noter que nous avons bâti notre architecture sur des protocoles et méthodes réputés pour leur robustesse. De plus, avec notre approche à aucun moment nous n'ajoutons de risques supplémentaires de sécurité. Au contraire, par notre cheminement nous avons

essayé d'adapter la sécurité aux risques réels existants. En effet, selon l'avis de plusieurs experts une sécurité renforcée est surtout une sécurité adaptée et non pas exagérée.

D'un autre côté, les résultats de la simulation réalisée confortent notre idée, selon laquelle le fait d'adopter IPSec pour tous les clients 802.11, indépendamment du standard de sécurité Wi-Fi, en considérant les clients comme un groupe homogène n'est pas un choix adéquat pour les réseaux Wi-Fi. En effet, il est primordial de tenir compte des spécificités des différents standards de sécurité supportés par les clients et mettre en place une architecture adaptative et flexible telle que celle présentée dans le cadre de ce mémoire.

Dans la section qui suit, nous présentons une analyse de la signalisation appliquée aux communautés WEP et WPA/WPA2 tel que nous l'avons définie dans l'architecture que nous proposons.

6.2.4 Signalisation appliquée aux communautés WEP et WPA/WPA2

Dans l'architecture que nous proposons, deux communautés avec deux modes d'accès différents au système d'information se dégagent : la communauté WEP et la communauté WPA/WPA2. Pour avoir accès aux ressources du système d'information depuis le réseau Wi-Fi, les clients 802.11 de la communauté WEP doivent passer par les étapes suivantes :

- ✓ Rattachement au point d'accès
- ✓ Association au VLAN de la communauté WEP
- ✓ Établissement d'une session TLS
- ✓ Authentification WEP
- ✓ Établissement d'un canal WEP sécurisé

Quant aux clients 802.11 de la communauté WPA/WPA2, ces derniers devront passer par les étapes suivantes :

- ✓ Rattachement au point d'accès
- ✓ Association au VLAN de la communauté WPA/WPA 2
- ✓ Échanges WPA/WPA 2
- ✓ Établissement d'un canal WPA/WPA2 sécurisé

À première vue, nous pourrions penser que notre architecture favorise la communauté WPA/WPA2 et que l'accès aux ressources du système d'information par les clients 802.11 de la communauté WEP se trouve alourdi et passe par plusieurs étapes avant de pouvoir envoyer ou recevoir le premier paquet de données effectives et non de signalisation. Toutefois, notre étude montre que ce n'est pas le cas. En effet, nous avons regardé en détail chacune des étapes par lesquelles passe un client des deux communautés et avons dégagés les résultats illustrés par le tableau 6.2.

<table>
<tr><th colspan="2">Communauté WEP</th><th colspan="3">Communauté WPA/WPA2</th></tr>
<tr><th>Étape</th><th>Nombre de messages</th><th colspan="2">Étape</th><th>Nombre de messages</th></tr>
<tr><td>Rattachement au point d'accès</td><td>2</td><td colspan="2">Rattachement au point d'accès</td><td>2</td></tr>
<tr><td>Association au VLAN WEP</td><td>0</td><td colspan="2">Association au VLAN WPA/WPA2</td><td>0</td></tr>
<tr><td rowspan="2">Établissement d'une session TLS</td><td rowspan="2">4</td><td rowspan="4">Échanges WPA2</td><td>Mise en accord sur la politique de sécurité</td><td>6</td></tr>
<tr><td>Authentification 802.1x</td><td>6</td></tr>
<tr><td rowspan="2">Authentification WEP</td><td rowspan="2">6</td><td>4-Way Handshake</td><td>4</td></tr>
<tr><td>2-Way Handshake (optionnelle)</td><td>0-2</td></tr>
<tr><td colspan="2">Total: 12</td><td colspan="3">Total: 18-20</td></tr>
</table>

Tableau 6.2 : Signalisation appliquée aux communautés WEP et WPA/WPA2

Nous avons assigné zéro messages à l'étape d'association au VLAN pour les deux communautés, étant donné que comme on l'a vu précédemment, cette association se fait de façon transparente lors du rattachement au point d'accès. Tout client se rattachant à un point d'accès avec un SSID particulier se trouve du même coup associé au VLAN correspondant à ce SSID.

Ainsi, un client 802.11 de la communauté WEP devra passer par un échange de 12 messages avant de pouvoir émettre son premier paquet de données, contre 18 ou 20 paquets pour le client WPA2, selon que l'on fasse appel à un échange 2-Way Handshake pour la génération de la clé de groupe GTK ou pas. De ce fait, nous pouvons affirmer que la

communauté WEP n'est pas pénalisée en termes de poids de signalisation avant l'accès aux ressources, par rapport à la communauté WPA/WPA2.

6.3 Autres considérations de sécurité

Le fait de sécuriser un réseau Wi-Fi sur le plan logique ne signifie pas qu'il offrira pour autant le même niveau de sécurité que son homologue filaire au cœur de l'entreprise. En effet, pour les réseaux Wi-Fi, outre les considérations architecturales, il est primordial de prendre en considération le volet de sécurisation radio.

Dans les réseaux Wi-Fi d'aujourd'hui, le seul risque qui ne peut pas être totalement paré est celui du déni de service volontaire. Comme précédemment montré dans le chapitre 4, des attaques radio ou logiques existent et sont imparables si elles sont bien exécutées. Ainsi, faire reposer la sécurité d'un réseau WLAN sur des éléments intrinsèques de sécurité n'est pas suffisant. C'est pourquoi nous préconisons d'utiliser des compléments de sécurité tels qu'illustré par les points suivants :

- Implantation des systèmes de détection d'intrusion spécifiques aux réseaux Wi-Fi. Pour cela, il faudra consolider la cohérence de l'information de tout le réseau Wi-Fi pour corréler les événements et détecter des attaques ou comportements à risque : un vrai travail de vérification et de correspondance des configurations des points d'accès s'impose. Les systèmes de détection d'intrusion Wi-Fi sont généralement composés d'un module logiciel de collecte d'informations distribué sur les points d'accès déployés, ainsi qu'un module central de traitement des données pour la détection de toute éventuelle anomalie du réseau [11]. Il est à noter qu'il n'est pas nécessaire de se procurer une solution de détection d'intrusion commerciale, qui selon l'avis de tous les experts est d'une efficacité minimale [23]. En effet, il serait plus intéressant de se procurer une version à code source ouvert, afin de la modifier et l'adapter aux besoins réels de l'entreprise.

- Détection des points d'accès pirates, permettre une localisation de l'élément en cause et opérer une contre-attaque radio. Ces fonctionnalités sont disponibles sur certains points d'accès modernes. Ainsi, il serait utile de mettre en place des points d'accès dédiés à la

défense du réseau Wi-Fi qui ne font que détecter les points d'accès pirates, les tentatives de brouillage radio et riposter à ces attaques. Il est à noter qu'il existe actuellement sur le marché des outils performants qui permettent la localisation par triangulation des points d'accès pirates.

- L'ingénierie radio est un élément crucial pour la sécurité de tout réseau Wi-Fi. En effet, il est préférable que les signaux émis par le réseau Wi-Fi de l'entreprise ne dépassent pas le périmètre du bâtiment où sont localisés les points d'accès. C'est pourquoi la disposition physique des points d'accès est importante, voire primordiale. Selon les experts radio, pour limiter les propagations en dehors du périmètre autorisé, il faudra privilégier l'utilisation d'antennes à rayonnement directif et placer les points d'accès en hauteur (pour contrer le *wardriving* qui s'opère au niveau de la rue) [11].

- La mise en place d'outils qui permettent de vérifier le niveau de sécurité et la conformité des postes clients 802.11 avec les exigences de sécurité de l'entreprise. En effet, n'importe quel utilisateur peut activer la connexion ad hoc sur sa machine. De cette façon, n'importe qui peut accéder aux ressources du système d'information via le client légitime ayant activé un lien ad hoc, sans que ce dernier ne se rende compte de rien. C'est pour cela qu'il est nécessaire de développer des outils qui permettent de vérifier la configuration de sécurité du client.

Dans ce chapitre, nous avons évalué notre nouvelle approche de sécurisation des réseaux Wi-Fi dans l'entreprise. Ainsi, les résultats montrent que notre solution en plus d'offrir une sécurité renforcée, compte tenu des faiblesses de WEP et des menaces d'attaques qu'on a passées en revue dans le chapitre 4, constitue une architecture flexible qui prend en considération les spécificités du support hertzien dans les réseaux Wi-Fi

Bien que nous n'ayons pas mis en pratique notre proposition pour des raisons matérielles évidentes, la suite logique de ce travail consisterait à développer des outils pour faciliter l'administration du réseau et le contrôle de sécurité, par exemple :

- vérification du niveau de sécurité et la conformité de la configuration des postes clients 802.11 avec les exigences de sécurité de l'entreprise.

- Détection et suivi du comportement de chaque client 802.11 (activation de la connexion ad hoc, déconnexion du point d'accès,...).
- Détection si un point d'accès est déconnecté du réseau.
- Mise à jour automatique de la configuration des points d'accès.

CHAPITRE VII

CONCLUSION ET PERSPECTIVES

Dans cette étude, nous avons présenté une synthèse de l'état de l'art des réseaux Wi-Fi. Ensuite, nous sommes passés au volet des standards de sécurité qui a fait l'objet du troisième chapitre. Ainsi, nous avons montré l'évolution de la normalisation en termes de standards de sécurité 802.11. Nous avons également présenté une étude détaillée sur les vulnérabilités des standards de sécurité et les modes opératoires des différentes attaques qui exploitent ces faiblesses. Cette étude nous a permis de prendre conscience de l'étendue des dégâts qu'il est possible de provoquer sur un réseau Wi-Fi. Finalement, nous avons proposé une nouvelle approche architecturale qui permet d'allier sécurité renforcée, flexibilité et optimisation de l'utilisation des ressources du réseau.

Notre proposition a le mérite de favoriser principalement la flexibilité et de répondre aux besoins spécifiques exprimés aujourd'hui par les administrateurs des réseaux Wi-Fi. Ceci en plus de la prise en compte de l'hétérogénéité des équipements Wi-Fi et des standards de sécurité supportés. L'architecture Wi-Fi sécurisée que nous proposons se base sur une différenciation à plusieurs niveaux. En effet, nous établissons un premier niveau de différenciation relatif au standard de sécurité employé (WEP, WPA, WPA2). Le second niveau de différenciation permet de distinguer les différentes communautés d'utilisateurs Wi-Fi, ainsi nous avons distingués trois communautés d'utilisateurs (visiteurs, partenaires et permanents), dont l'accès aux ressources et les niveaux de sécurité à appliquer sont différents d'une communauté à une autre.

Finalement, nous établissons un troisième niveau de différenciation relatif au trafic d'authentification et de gestion des accès. Ces niveaux de différenciation offrent la granularité nécessaire pour permettre une meilleure gestion du réseau et un meilleur contrôle d'accès aux ressources, ce qui améliore la sécurité du réseau Wi-Fi en particulier et du système d'information de l'entreprise dans son ensemble.

Outre ces niveaux de différenciation, nous avons opté pour l'établissement de sessions sécurisées via le protocole TLS, afin de sécuriser les liens radios des clients 802.11, ayant le protocole WEP comme seul mécanisme sécuritaire. Ce choix s'explique par la défaillance du protocole WEP et ses vulnérabilités flagrantes.

Il est utile de signaler que notre proposition s'inscrit pleinement dans le contexte actuel qui se caractérise par l'instabilité des standards de sécurité Wi-Fi et la rapidité de leur obsolescence. Cette mouvance rapide entre les différents standards et les diverses technologies inhérentes à la sécurité Wi-Fi, a créé une méfiance vis-à-vis de cette technologie malgré son grand potentiel. Notre solution vient intégrer toutes ces problématiques et propose une nouvelle approche de sécurisation de la technologie Wi-Fi dans l'entreprise.

Les résultats des simulations que nous avons réalisées appuient notre contribution et montrent clairement l'apport de notre approche en termes de surcharge du réseau. En effet, en comparant notre approche avec une solution basée sur IPSec, nous trouvons que notre solution garantie un débit utile par client supérieur de 22% à 34%, selon qu'il s'agisse de la communauté WEP ou WPA/WPA2.

Nous pouvons dire que ce travail a constitué pour nous, un très bon exercice d'analyse et de conception architecturale dans le contexte de la sécurité des réseaux Wi-Fi. Cela nous a également permis de prendre conscience de l'étendue des potentialités de cette technologie et en même temps, la difficulté d'assurer une sécurité optimale. Le plus difficile étant d'atteindre un compromis entre facilité d'accès et sécurité optimale.

En guise de conclusion, nous pouvons affirmer que les réseaux Wi-Fi présentent de grands potentiels. Toutefois, les services fournis par ces réseaux sont confrontés à de graves problèmes de sécurité, au point de mettre en péril leur développement. Ces risques de sécurité

ont tendance à s'atténuer, surtout avec le standard WPA2 qui semble répondre à la majorité des exigences actuelles de sécurité dans les réseaux Wi-Fi. Mis à part cet aspect de sécurité, les réseaux Wi-Fi font face à d'autres défis, parmi lesquels on peut citer la qualité de service et le transfert entre cellules (*handover*), ou encore la mobilité Wi-Fi.

En effet, selon [6], le service de confidentialité assuré par le WEP fait perdre en moyenne 25% de performances, en induisant de graves failles de sécurité. Quant à TKIP et WPA, étant plus sécuritaires que WEP, ils induisent 30% de baisses de performances. WPA2, le nec plus ultra en matière de sécurité Wi-Fi, améliore un peu les performances mais engendre une perte de 25% de bande passante. De ce fait, il est primordial de trouver un compromis entre les exigences de sécurité et ceux de la qualité de service.

Outre l'aspect qualité de service, les réseaux Wi-Fi se doivent de remporter le défi de la mobilité sécurisée, en assurant un transfert entre cellules Wi-Fi le plus sécuritaire et le plus rapide possible.

Une fois, tous ces défis relevés, la technologie Wi-Fi sera certainement un pilier majeur pour l'établissement de l'Internet ambiant de demain, offrant sécurité, mobilité, qualité de service et haut débit.

BIBLIOGRAPHIE

[1] K. Al Agha, G. Pujolle et G. Vivier. « Réseaux de mobiles & réseaux sans fil ». Paris: Édition Eyrolles, 2001, 475p.

[2] G. Pujolle, O. Salvatori et J. Nozick. « Les Réseaux, Édition 2005 ». Paris : Édition Eyrolles, 2004, 1094p.

[3] M. Gast « 802.11 Wireless Networks: The Definitive Guide ». O'Reilly. April 2002.

[4] P. Roshan, et J. Leary « Réseaux WiFi: notions fondamentales ». Paris: CampusPress, Cisco Press, 2004, 291p.

[5] J. M. Wilson « The Next Generation of Wireless LAN Emerges with 802.11n ». *Technology@Intel Magazine*, Août 2004, 8p.

[6] G. Pujolle. « Sécurité Wi-Fi ». Paris : Édition Eyrolles, 2004, 237p.

[7] S. Convery, et D. Miller « Cisco SAFE : Description détaillée de la sécurité pour les réseaux locaux sans fil ». Cisco Safe white paper, 2003.

[8] G. Lehembre « Sécurité Wi-Fi: WEP, WPA, WPA2 ». *Hakin9 Magazine*, no 1 (Janvier 2006), 15p.

[9] H. Changhua, et J. C. Mitchell « Analysis of the 802.11i 4-Way Handshake ». Stanford University, *ceci a été publié dans le Workshop WiSe'04 (Philadelphia: 1 octobre 2004).*

[10] E. Rescorla « SSL and TLS: Designing and Building Secure Systems ». Addison-Wesley Professional, 2001, 528 p.

[11] A. A. Vladimirov, K. V. Gavrilenko et A. A. Mkhailovsky. « Wi-Foo: Piratage et défense des réseaux sans fil ». Paris: CampusPress, 2005, 557p.

[12] M. Ossman « WEP: Dead Again, Part 1 ». *Ceci a été publié dans le forum SecurityFocus en décembre 2004.* [http://www.securityfocus.com/infocus/1814].

[13] M. Ossman « WEP: Dead Again, Part 2 ». *Ceci a été publié dans le forum SecurityFocus en Mars 2005.* [http://www.securityfocus.com/infocus/1824].

[14] W. A. Arbaugh « An inductive chosen plaintext Attack against WEP/WEP2 ». University of Maryland, *ceci est un document IEEE 802.11-02/230, Mai 2001, grouper.ieee.org/groups/802/11.*

[15] Borisov, Goldberg, et Wagner « Intercepting Mobile Communications: The Insecurity of 802.11 ». *Ceci a été publié dans la 7ème conférence internationale "Mobile Computing and Networking"*, 2001.

[16] S. R. Fluhrer, I. Mantin, et A. Shamir « Weaknesses in the Key Scheduling Algorithm of RC4 ». Cisco Systems, Computer Science Department, The Weizmann Institute, *ceci a été publié dans le 8ème Workshop international annuel "Selected Areas in Cryptography"*, 2001.

[17] D. Hulton « Practical Exploitation of RC4 Weaknesses in WEP Environments ». Dasb0den Labs, 2002. [http://www.dachb0den.com/projects/bsd-airtools/wepexp.txt].

[18] L. Saccavini « 802.1X et la sécurisation de l'accès au réseau local ». INRIA, *ceci a été publié lors des 5ème journées Réseaux au pôle universitaire de Lille, France*, 2003. [http://2003.jres.org/actes/paper.111.pdf].

[19] A. Mishra, W. A. Arbaugh « An initial security analysis of the 802.1x standard ». Rapport technique CS-TR-4328 UMIACS-TR-2002-10, University of Maryland, 2002. [http://www.cs.umd.edu/~waa/1x.pdf 2002].

[20] G. Fleishmann, et R. Moskowitz « Weakness in Passphrase choice in WPA Interface ». ICSA Labs, TrueSecure Corp, 2003.

[21] V. Moen, H. Raddum, et K. J. Hole « Weaknesses in the Temporal Key Hash of WPA ». Department of Informatics, University of Bergen, 2004.

[22] G. Le Grand, A. Hecker, F. Springfield « Architecture Flexible de Réseau sans fil WiFi sécurisé ». GET/Télécom Paris - LTCI-UMR 5141 CNRS, *ceci a été publié dans la 3ème conférence sur la sécurité et architecture réseaux (SAR'04)*, 2004.

[23] W. A. Arbaugh, N. Shankar, et J. Wang « Your 802.11 Networks has no Clothes ». University of Maryland, December 2001.