Introduction

Le point crucial lors d'une installation réseau, quelle soit filaire ou sans fil, est la mise en place d'éléments de protection. La sécurité a toujours été le point faible des réseaux Wi-Fi, à cause principalement de sa nature physique : les ondes radio étant un support de transmission partagé quiconque se trouvant dans la zone de couverture peut écouter le support et s'introduire dans le réseau. On peut même, grâce à des antennes amplifiées, se trouver hors de portée de la couverture radio pour pénétrer ce réseau. Ces problèmes de sécurité se posent aussi pour des réseaux câblés mais l'écoute passive nécessite une intrusion physique. Car toute personne possédant quelques notions d'informatique et un peu de matériel peut facilement trouver les informations et les programmes pour écouter et percer des réseaux Wi-Fi. En plus de ces faiblesses intrinsèques aux ondes radio, un réseau Wi-Fi doit se protéger des attaques classiques. Ces failles de sécurité ont porté un préjudice certain à son développement en entreprise, car elles deviennent les points d'accès au réseau interne sur lequel il est connecté. Il existe des moyens de sécurité implantés de base sur le matériel Wi-Fi (carte et point d'accès) permettant un premier niveau de protection, mais ces moyens de sécurisation sont facilement contournable. Dans ce chapitre, on va présenter d'une part une analyse des différentes attaques susceptibles d'atteindre un réseau Wi-Fi, d'autre part une série de notions utilisé qui répondent aux trois principes élémentaires de sécurité qui sont: Codage, Authentification et Intégrité, permettant à leurs administrateurs et usagers de mieux contrôler et si possible réduire les risques.

1. Risques et attaques

1.1. Les risques

Les risques dépendent des paramètres que l'on peut maitriser. Contrairement au réseau câblé, le contrôle des accès physiques au réseau sans fil est difficile, voir impossible.

Il existe deux types de risques :

- **Risque structurel :** dépend de l'organisation de l'entreprise.
- **Risque accidentel :** indépendant de tous les facteurs de l'entreprise.

On peut classifier les risques en quatre niveaux :

a. **Acceptables :** pas des conséquences graves pour les utilisateurs du réseau.

   Exemple : panne éclectique, perte de liaison, engorgement…

b. **Courants :** pas de préjudices graves au réseau, on peut réparer facilement.

Exemple : gestion du réseau, mauvaise configuration, erreur utilisateur…

c. Majeurs : dus à des facteurs graves et qui causent de gros dégâts mais récupérables.

Exemple : foudre qui tombe sur un routeur…

d. Inacceptables : fatals pour l'entreprise, ils peuvent entrainer son dépôt de bilan.

Exemple : perte ou corruption des informations importantes…

1.2. Les attaques

On peut classifier les attaques en deux groupes principaux : les attaques passives et les attaques actives, qui sont bien évidemment plus dangereuses.

1.2.1. Attaques passives

Dans un réseau sans fil l'écoute passive est d'autant plus facile que le média air est difficilement maîtrisable. Bien souvent, la zone de couverture radio d'un point d'accès déborde du domaine privé d'une entreprise ou d'un particulier. L'attaque passive la plus répandue est la recherche de point d'accès. Cette attaque (appelée Wardriving) est devenu le " jeu " favori de nombreux pirates informatique, les points d'accès sont facilement détectables grâce à un scanner (portable équipé d'une carte Wi-Fi et d'un logiciel spécifique de recherche de PA). Ces cartes Wi-Fi sont équipées d'antennes directives (type Yagi) permettant d'écouter le trafic radio à distance hors de la zone de couverture du point d'accès. Il existe deux types de scanners, les passifs (Kismet, Wifiscanner, Prismstumbler…) ne laissant pas de traces (signatures), quasiment indétectables et les actifs (Netstumbler, dstumbler) détectables en cas d'écoute, ils envoient des " probe request ". Seul Netstumbler fonctionne sous Windows, les autres fonctionnent sous Linux. **[15]**

Les sites détectés sont ensuite indiqués par un marquage extérieur (à la craie) suivant un code (warchalking) :

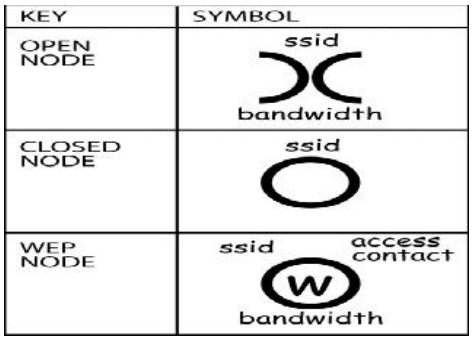

Figure II.1 : Code warchalking

Une première analyse du trafic permet de trouver le SSID (nom du réseau), l'adresse MAC du point d'accès, le débit, l'utilisation du cryptage WEP et la qualité du signal. Associé à un GPS, ces logiciels permettent de localiser (latitude longitude) ces points d'accès.
A un niveau supérieur des logiciels (type Aisnort ou Wepcrack) permettent, en quelques heures (suivant le trafic), de déchiffrer les clés WEP et ainsi avec des outils d'analyse de réseaux conventionnels la recherche d'informations peut aller plus loin. Le pirate peut passer à une attaque dite active.

1.2.2. Attaques actives

Nous allons revoir, assez succinctement, les différentes attaques connues dans les réseaux filaires et qui touchent bien évidemment, le monde du Wi-Fi.

- **DoS (Denial of Service)**

Le déni de service réseau est souvent l'alternative à d'autres formes d'attaques car dans beaucoup de cas il est plus simple à mettre en œuvre, nécessite moins de connaissances et est moins facilement traçable qu'une attaque directe visant à entrer dans un système pour en prendre le contrôle. Cette attaque a pour but d'empêcher des utilisateurs légitimes d'accéder à des services en saturant de fausses requêtes ces services. Elle se base généralement sur des " bugs " logiciel. Dans le milieu Wi-Fi, cela consiste notamment à bloquer des points d'accès soit en l'inondant de requête de désassociassions ou de dés authentification (programme de type Airjack), ou plus simplement en brouillant les signaux hertzien. **[15]**

- **Spoofing (usurpation d'identité)**

Le spoofing IP est une technique permettant à un pirate d'envoyer à une machine des paquets semblant provenir d'une adresse IP autre que celle de la machine du pirate. Le spoofing IP n'est pas pour autant un changement d'adresse IP. Plus exactement il s'agit d'une mascarade (il s'agit du terme technique) de l'adresse IP au niveau des paquets émis, c'est-à-dire que les paquets envoyés sont modifiés afin qu'ils semblent parvenir d'une machine. **[15]**

- **Man in the middle (home au milieu) en milieu Wi-Fi**

Cette attaque consiste, pour un réseau Wi-Fi, à disposer un point d'accès étranger dans à proximité des autres PA légitimes. Les stations désirant se connecter au réseau livreront au PA " félon " leurs informations nécessaires à la connexion. Ces informations pourront être utilisées par une station pirate. Il suffit tout simplement à une station pirate écoutant le trafic, de récupérer l'adresse MAC d'une station légitime et de son PA, et de s'intercaler au milieu. **[15]**

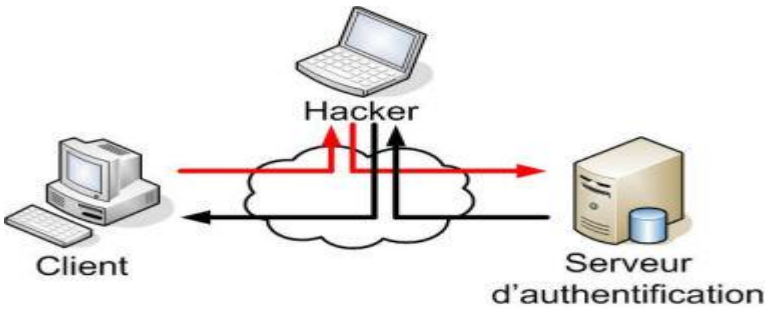

Figure II.2 : Attaque MITM

1.2.3. Autres attaques

- **Craquage de mots de passe**

Cette méthode est souvent le dernier de recours. Il consiste à faire beaucoup d'essais pour déterminer un mot de passe. On distinguera deux grandes méthodes :

- L'utilisation de dictionnaires : la plupart des mots de passes ne sont pas des chaines aléatoires mais des mots ou des phrases faciles à retenir. Cela permet d'écarter une très grande quantité de possibilités.
- La force brute consiste à essayer toutes les combinaisons possibles. Elle est rapidement efficace sur les petites chaînes (moins de 8 caractères) mais devient rapidement trop longue à exécuter quand la longueur du mot de passe augmente (plus de 16 caractères). **[14]**

- **Backdoors**

Quand un pirate arrive à accéder à un système et qu'il veut pouvoir y accéder plus facilement par la suite, il crée une ``Backdoors'' ou porte de derrière. Cela pourra se traduire par : **[14]**

- Le rajout d'un nouveau compte au serveur avec le mot de passe choisi par le pirate.
- La modification du firewall pour qu'il accepte une IP définie (une que le pirate pourra spoofer facilement) ou qu'il ouvre certains ports.
- La création d'un compte FTP.
- L'ouverture de Telnet.
- L'utilisation d'un troyen.

- **Virus, vers et chevaux de Troie**

Un virus est un programme capable de se cacher dans un autre et qui peut se reproduire en infectant d'autres programmes ou d'autres ordinateurs. Les dégâts pourront aller d'un simple affichage à l'écran à une mise hors service d'un système. On recense plusieurs catégories : **[14]**

- Les vers capables de se propager dans le réseau.
- Les chevaux de Troie ou troyens créant des failles dans un système.
- Les bombes logiques se lançant suite à un événement du système (appel d'une primitive ou date spéciale).
- Les hoax qui sont des canulars envoyés par mail.

- **Le sniffing**

Ce type d'attaque est basé sur l'interception de données émises sans précaution à toutes les parties comme lors des diffusions. Il suffit d'être présent sur le réseau pour intercepter tout le trafic et récupérer n'importe quelles données transitant sur le réseau si celles-ci ne sont pas cryptées. **[14]**

2. Services de sécurité

Les services de sécurité représentent les logiciels et matériels mettant on œuvre les mécanismes dans le but de mettre à la disposition des utilisateurs des fonctions de sécurité dont ils ont besoin.

Il existe cinq notions fondamentales de la sécurité :

2.1. Confidentialité

Le service de confidentialité garantie aux deux entités communicantes à être les seules à pouvoir comprendre les données échangées. Ceci implique la mise en œuvre des algorithmes de chiffrement en mode flux, c'est-à-dire octet par octet, ou en mode bloc.

Un message écrit en clair est transformé en un message chiffré, appelé « cryptogramme » grâce aux algorithmes de chiffrement. Cette transformation est fondée sur une ou plusieurs clés. **[16]**

2.1.1. Chiffrement (la cryptographie)

Le chiffrement consiste à rendre un texte incompréhensible en le codant. On code (crypte ou chiffre) le texte en effectuant une opération sur le texte en clair à partir d'une règle appelée clé de chiffrement. Le texte codé (cryptogramme) peut alors être envoyé à son destinataire. La cryptanalyse consiste à déchiffrer un texte codé en effectuant sur ce texte avec une clé. Il existe trois méthodes de chiffrement : à clé symétrique, à clé asymétrique (ou clé publique), à clé mixte (utilisation des deux précédentes).

2.1.1.1. Clé symétrique

La clé de chiffrement est identique à la clé de déchiffrement. Ainsi c'est la même clé qui va nous permettre à la fois de chiffrer le message et de permettre aux destinataires de le déchiffrer. Cela ne va pas sans poser un problème majeur: l'échange préalable de la clé entre les protagonistes. Or, ceci est particulièrement difficile à réaliser, puisque, tant que la clé n'est pas transmise, il n'existe pas de moyen sûr d'échange d'information, en dehors d'une rencontre physique qui n'est pas forcément possible.

Le deuxième problème est le nombre de clés nécessaire pour sécuriser un ensemble de relations. En effet, si l'on désire que chaque utilisateur d'un réseau puisse communiquer avec un autre utilisateur de manière sécurisée, une clé différente est alors utilisée pour chaque paire d'utilisateurs du réseau. Le nombre total de clés croît alors suivant un polynôme quadratique. Ainsi, un groupe de 10 utilisateurs met en jeu 45 clés différentes et 100 utilisateurs, 4950 clés. **[17]**

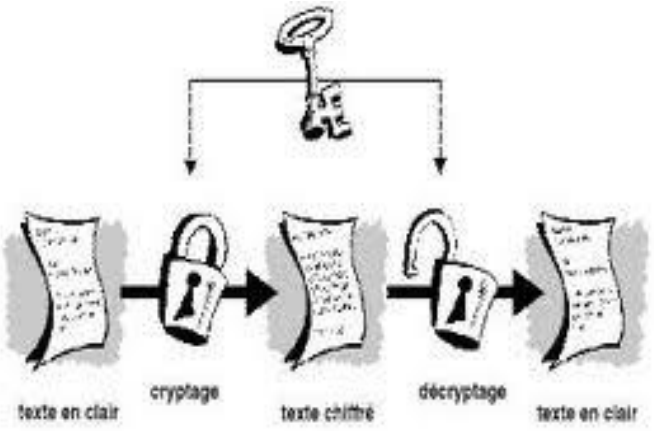

Figure II.3 : Chiffrement symétrique

Les principes algorithmes de chiffrement symétriques sont :

- **DES (Data Encryptions Standard) :** a été le plus utilisé, mais n'est plus utilisé depuis 1998 considéré peu sûr. Clé de 40 à 56 bits.
- **IDEA (International Data Encryptions Algorithm) :** est utilisé par PGP (**P**retty **G**ood **P**rivacy), le logiciel de cryptographie le plus utilisé au monde. Clé de 128 bits.
- **Série RC (Ron's Code) RC2 à RC6 :** algorithme développé par Ron Rivest, la version RC4 est utilisé dans le protocole WEP d'IEEE 802.11.
- **AES (Advanced Encryption Standard) :** remplaçant du DES dans l'administration américaine et du RC4 dans la norme 802.11 avec 802.11i. Fondé sur l'algorithme de Rijndael, est considéré comme étant incassable.

2.1.1.2. Clé Asymétrique

Dans ce cas, les clés de chiffrement et de déchiffrement sont distinctes, et généralement symétriques entres elles: la clé de chiffrement permet de déchiffrer ce qui a été chiffré avec la clé de déchiffrement, et vice versa. Le possesseur d'une telle paire de clés, en rend une (au choix) publique, c'est-à-dire qu'il la donne à tout le monde, dans une sorte d'annuaire. Tout correspondant qui veut envoyer un message, chiffre son message à l'aide de la clé publique du destinataire. Seul le possesseur de la clé secrète correspondant à cette clé publique pourra déchiffrer le message. **[17]**

Les algorithmes de chiffrement à clé publique permettent aussi à l'envoyeur de signer son message. En effet, il lui suffit de chiffrer le message (ou une partie de ce message) avec sa propre clé secrète. Le destinataire déchiffrera cette fonction avec la clé publique de l'envoyeur et sera ainsi certain de l'identité de l'expéditeur, puisqu'il est le seul à posséder la clé secrète qui permet de faire un tel chiffrement. Ainsi cette méthode permet de réaliser une communication confidentielle sans échanger auparavant de code secret.

Le principal inconvénient de ce type d'algorithme est la lenteur à laquelle s'effectuent les opérations de chiffrement et de déchiffrement. **[17]**

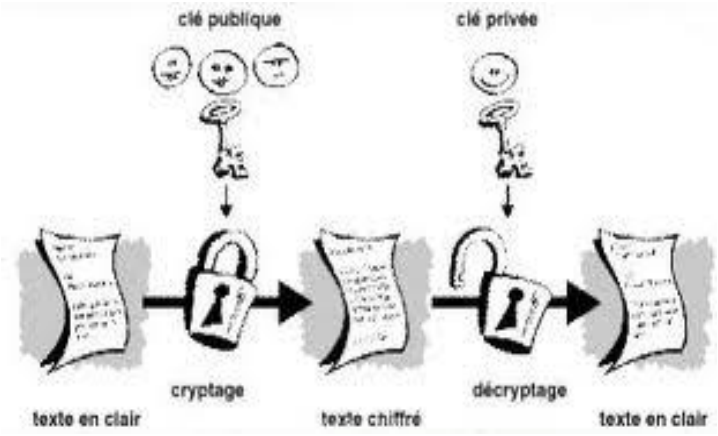

Figure II.4 : Chiffrement asymétrique

- **RSA (Rivest, Shamir, Adelman) :** comme le plus connu de ces algorithmes. La sécurité du RSA réside dans l'impossibilité pratique de factoriser un grand nombre de quelques centaines de chiffres en un temps raisonnable. Qui plus est pour assurer sa pérennité il est toujours possible d'augmenter la longueur de la clé qui varie entre 1024 et 2048 bits.

En résumé, une synthèse de ces deux méthodes de cryptographie est décrite dans le tableau ci-après.

Type de crypto système	Avantages	Inconvénients
Clé Symétrique	- Rapide - Peut être facilement réalisé sur une puce	- Difficultés de distribuer les clés - Ne permet pas de signature électronique
Clé Asymétrique	- Utilise deux clés différents - Fournit des garanties d'intégrité et non répudiation par signature électronique	- Lent et demandant beaucoup de calculs

Tableau II.1 : Comparaison entre les types de chiffrement

Finalement comme nous avons pu le voir précédemment, les deux systèmes de base de la cryptographie (symétrique et asymétrique) souffrent de problèmes complémentaires. Ainsi l'intérêt pour augmenter la sécurité des systèmes de cryptage passe certainement par l'utilisation combinée de ces deux techniques, ce que l'on nomme la cryptographie mixte. **[17]**

2.1.1.3. Clé mixte

Ce principe fait appel aux deux techniques précédentes, à clé symétrique et à clé publique, combinant les avantages des deux touts en évitant leurs inconvénients. Le principe général consiste à effectuer le chiffrement des données avec des clés symétriques, mais en ayant effectué au départ l'envoi de la clé symétrique par un algorithme à clé publique.
L'un de ces algorithmes est PGP**.**

- **PGP (Pretty Good Privacy)**

PGP est un système de cryptographie hybride, utilisant une combinaison des fonctionnalités de la cryptographie à clé publique et de la cryptographie symétrique.
Lorsqu'un utilisateur chiffre un texte avec PGP, les données sont d'abord compressées. Cette compression des données permet de réduire le temps de transmission par tout moyen de communication, d'économiser l'espace disque et, surtout, de renforcer la sécurité cryptographique.
La plupart des cryptanalyses exploitent les modèles trouvés dans le texte en clair pour casser le chiffrement. La compression réduit ces modèles dans le texte en clair, améliorant par conséquent considérablement la résistance à la cryptanalyse.
Ensuite, l'opération de chiffrement se fait principalement en deux étapes :

- PGP crée une clé secrète IDEA de manière aléatoire, et chiffre les données avec cette clé

- PGP crypte la clé secrète IDEA et la transmet au moyen de la clé RSA publique du destinataire.

L'opération de décryptage se fait également en deux étapes :

- PGP déchiffre la clé secrète IDEA au moyen de la clé RSA privée.
- PGP déchiffre les données avec la clé secrète IDEA précédemment obtenue.

Cette méthode de chiffrement associe la facilité d'utilisation du cryptage de clef publique à la vitesse du cryptage conventionnel. Le chiffrement conventionnel est environ 1000 fois plus rapide que les algorithmes de chiffrement à clé publique. Le chiffrement à clé publique résout le problème de la distribution des clés. Utilisées conjointement, ces deux méthodes améliorent la performance et la gestion des clefs, sans pour autant compromettre la sécurité.

2.1.2.Certificats

Un certificat permet d'associer une clé publique à une entité (une personne, une machine, ...) afin d'en assurer la validité. Le certificat est en quelque sorte la carte d'identité de la clé publique, délivré par un organisme appelé autorité de certification (souvent notée CA pour **C**ertification **A**uthority). L'autorité de certification est chargée de délivrer les certificats, de leur assigner une date de validité (équivalent à la date limite de péremption des produits alimentaires), ainsi que de révoquer éventuellement des certificats avant cette date en cas de compromission de la clé (ou du propriétaire).

- **Structure d'un certificat**

Les certificats sont des petits fichiers divisés en deux parties :

- La partie contenant les informations
- La partie contenant la signature de l'autorité de certification

La structure des certificats est normalisée par le standard X.509 de l'UIT (plus exactement X.509v3), qui définit les informations contenues dans le certificat :

- La version de X.509 à laquelle le certificat correspond ;
- Le numéro de série du certificat ;
- L'algorithme de chiffrement utilisé pour signer le certificat ;
- Le nom (DN, pour **D**istinguished **N**ame) de l'autorité de certification émettrice ;
- La date de début de validité du certificat ;
- La date de fin de validité du certificat ;
- L'objet de l'utilisation de la clé publique ;
- La clé publique du propriétaire du certificat ;

- La signature de l'émetteur du certificat.

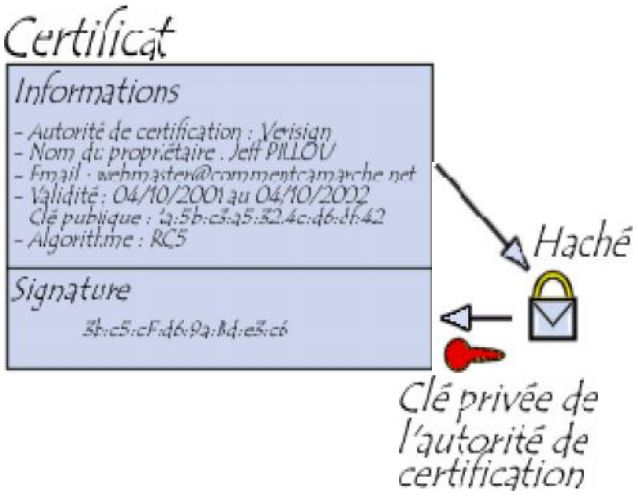

Figure II.5 : Certificat

L'ensemble de ces informations (informations + clé publique du demandeur) est signé par l'autorité de certification, cela signifie qu'une fonction de hachage crée une empreinte de ces informations, puis ce condensé est chiffré à l'aide de la clé privée de l'autorité de certification; la clé publique ayant été préalablement largement diffusée afin de permettre aux utilisateurs de vérifier la signature avec la clé publique de l'autorité de certification.

Lorsqu'un utilisateur désire communiquer avec une autre personne, il lui suffit de se procurer le certificat du destinataire. Ce certificat contient le nom du destinataire, ainsi que sa clé publique est signé par l'autorité de certification. Il est donc possible de vérifier la validité du message en appliquant d'une part la fonction de hachage aux informations contenues dans le certificat, en déchiffrant d'autre part la signature de l'autorité de certification avec la clé publique de cette dernière, et en comparant ces deux résultats. **[18]**

2.2. Service d'authentification

L'authentification a pour but de garantir l'identité des correspondantes. Parmi les solutions simples qui existent, l'utilisation d'un identificateur et d'un mot de passe, une méthode de défi basé sur une fonction cryptographique et un secret, l'authentification peut s'effectuer par un numéro d'identification personnel, comme le numéro inscrit dans une carte à puce, ou code PIN.

L'authentification peut être simple ou mutuelle. Elle consiste surtout à comparer les données provenant de l'utilisateur qui se connecte à des informations, stockées dans un site protégé et susceptibles de piratage. Les sites mémorisant les mots de passe. **[16]**

- **Les protocoles**

Un protocole d'authentification est un moyen de contrôle d'accès caractérisé par les 3 A (AAA) qui signifient **A**uthentication, **A**uthorization, **A**ccounting, soit authentication, autorisation et compte en français. La signification de ces termes est la suivante :

- Authentication : consiste à vérifier qu'une personne/équipement est bien celle qu'elle prétend être.
- Autorisation : consiste à permettre l'accès à certains services ou ressources.
- Accounting : le serveur AAA a la possibilité de collecter des informations sur l'utilisation des ressources.

➢ **DIAMETER**

Diameter est un protocole d'Authentication conçu pour servir de support à l'architecture AAA, successeur du protocole Radius. Ce protocole est défini par la RFC 3588. Il a repris les principales fonctions de Radius (Diameter est compatible avec Radius) et en a rajouté de nouvelles pour s'adapter aux nouvelles technologies (IPv4 Mobile, NASREQ ...) et plus particulièrement offrir des services aux applications mobiles. Ce protocole se situe au niveau de la couche transport. Il utilise le port 3868 via le protocole TCP ou bien SCTP. **[19]**

➢ **TACACS+**

TACACS+ (**T**erminal **A**ccess **C**ontroller **A**ccess **C**ontrol **S**ystem **P**lus) est un protocole de sécurité inventé à la fin des années 90 par CISCO Systems. Même s'il a fini par remplacer les protocoles TACACS et XTACACS, TACACS+ n'est pas basé sur ces derniers. Ce protocole se situe au niveau de la couche transport. Il utilise le port 46 via le protocole TCP.

TACACS+ permet de vérifier l'identité des utilisateurs distants mais aussi, grâce au modèle AAA, d'autoriser et de contrôler leurs actions. **[19]**

➢ **PAP**

Le protocole PAP (**P**assword **A**uthentication **P**rotocol) utilise des mots de passe en texte brut et constitue le protocole d'authentification le moins sécurisé. Il est généralement négocié lorsque le client d'accès distant et le serveur d'accès distant ne disposent d'aucun moyen de validation plus sûr.

➢ **CHAP**

Le protocole CHAP (**C**hallenge **H**andshake **A**uthentication **P**rotocol) est un protocole

d'authentification par stimulation-réponse, qui utilise le modèle de hachage MD5 (**M**essage **D**igest 5) standard pour crypter la réponse. CHAP est utilisé par de nombreux fournisseurs de clients et de serveurs d'accès réseau. Un serveur exécutant routage et accès distant prend en charge CHAP pour que les clients d'accès distant exigeant CHAP soient authentifiés. Dans la mesure où CHAP exige l'utilisation d'un mot de passe crypté à l'envers, vous devez envisager un autre protocole d'authentification comme MSCHAP version 2.

- **Kerberos**

Kerberos est un protocole de sécurité originaire de monde Unix, il a pris un nouveau départ lorsqu'il a été choisi par Microsoft pour remplacer NTLM (**NT L**an **M**anager) dans Windows 2000. Kerberos a pour objectif :

- D'authentifier les utilisateurs ;
- De leur allouer des droits d'accès à des applications (sur un serveur) sur le réseau sous forme de ticket ou jetons d'accès périssables dans le temps ;
- D'assurer la transmission sécurisée de ces tickets ou jetons d'accès vers les applications et ressources demandées ;
- De protéger les échanges entre les utilisateurs et les applications. **[19]**

2.3. L'intégrité des données

Dans certaines cas, il peut être nécessaire d'assurer simplement que les données sont intégrés, c'est-à-dire qu'elles n'ont pas été au passage falsifiées par un intrus. Ces données restent claires, au sens ou elles ne sont pas secrètes.

2.4. Non répudiation

Elle fournit au récepteur/émetteur une preuve qui empêche l'émetteur/récepteur de l'envoi de message.

2.5. Contrôle d'accès

De nos jours, toutes les entreprises possédant un réseau local et aussi un accès à internet, afin d'accéder à la manne d'information disponible sur le réseau, et pouvoir communiquer avec l'extérieur. Cette ouverture vers l'extérieur est indispensable…et dangereuse en même temps.

Ouvrir l'entreprise vers le monde signifie aussi laisser place ouverte aux étrangers pour essayer de pénétrer le réseau local de l'entreprise, et y accomplir des actions douteuse, pour cela une architecture sécurisée est nécessaire.

Le cœur d'une telle architecture est basé sur un firewall (un pare-feu).

Cet outil a pour but de sécuriser au maximum le réseau local de l'entreprise, de détecter les

tentatives d'intrusion. Cela représente une sécurité supplémentaires rendant le réseau ouvert sur internet beaucoup plus sur. De plus, il peut permettre de restreindre l'accès interne de l'extérieur et l'accès vers l'extérieur de l'intérieur.

En effet, des employés peuvent s'adonner à des activités (exemple : les jeux en ligne) que l'entreprise ne cautionne pas. En plaçant un firewall, on peut limiter ou interdire l'accès à ces services, l'entreprise peut donc avoir un contrôle sur les activités se déroulant dans son enceinte.

Le firewall propose donc un véritable contrôle sur le trafic réseau de l'entreprise. Il permet d'analyser, de sécurisé et de gérer le trafic réseau, et ainsi d'utiliser le réseau de la façon pour laquelle il a été prévu et sans l'encombrer avec des activités inutiles, et d'empêcher une personne sans autorisation d'accéder à ce réseau de données. Mais il ne fournit pas les services de sécurité tels que (authentification, intégrité, confidentialité, etc.).**[20]**

Sécurisation du Wi-Fi

Installer un réseau sans fil sans le sécuriser peut permettre à des personnes non autorisées d'écouter, de modifier et d'accéder à ce réseau. Il est donc indispensable de sécuriser les réseaux sans fil dès leur installation. Il est possible de sécuriser son réseau de façon plus ou moins forte selon les objectifs de sécurité et les ressources que l'on y accorde. La sécurité d'un réseau sans fil peut être réalisée à différents niveaux : configuration des équipements et choix des protocoles. **[4]**

1. Sécurité des points d'accès

La première chose à faire lors de la mise en place d'un réseau sans fil consiste à positionner intelligemment les points d'accès selon la zone que l'on souhaite couvrir. Eviter les murs extérieurs mais choisir plutôt un emplacement central. En se promenant autour de l'immeuble, on peut établir le périmètre à l'intérieur duquel la borne est accessible. Il n'est toutefois pas rare que la zone effectivement couverte soit largement plus grande que souhaitée, auquel cas il est possible de réduire la puissance de la borne d'accès afin d'adapter sa portée à la zone à couvrir. **[2]**

1.1. Eviter les valeurs par défaut

Lors de la première installation d'un point d'accès, celui-ci est configuré avec des valeurs par défaut, y compris en ce qui concerne le mot de passe de l'administrateur. Un grand nombre d'administrateurs en herbe considèrent qu'à partir du moment où le réseau fonctionne

il est inutile de modifier la configuration du point d'accès. Toutefois les paramètres par défaut sont tels que la sécurité est minimale. Il est donc impératif de se connecter à l'interface d'administration notamment pour définir un mot de passe d'administration.

D'autre part, afin de se connecter à un point d'accès il est indispensable de connaître l'identifiant du réseau (SSID). Ainsi il est vivement conseillé de modifier le nom du réseau par défaut et de désactiver la diffusion (broadcast) de ce dernier sur le réseau. Le changement de l'identifiant réseau par défaut est d'autant plus important qu'il peut donner aux pirates des éléments d'information sur la marque ou le modèle du point d'accès utilisé. L'idéal est même de modifiez régulièrement le nom SSID, Il faudrait même éviter de choisir des mots reprenant l'identité de l'entreprise ou sa localisation, qui sont susceptibles d'être plus facilement devinés. **[2]**

1.2. Filtrage des adresses MAC

Chaque adaptateur réseau possède une adresse physique qui lui est propre. Les points d'accès permettent généralement dans leur interface de configuration de gérer une liste de droits d'accès (appelée ACL) basée sur les adresses MAC des équipements autorisés à se connecter au réseau sans fil. Cette précaution un peu contraignante permet de limiter l'accès au réseau à un certain nombre de machines. En contrepartie cela ne résout pas le problème de la confidentialité des échanges. **[2]**

Remarque : certains adaptateurs permettent de modifier leurs adresses et donc de se faire passer pour d'autres adaptateurs se trouvant sur d'autres postes.

2. Sécurité des protocoles liés aux Wi-Fi

De nombreuses évolutions protocolaires ont rythmé la sécurité des réseaux Wi-Fi. Les objectifs sont les suivants :

- Garantir la confidentialité des données ;
- Permettre l'authentification des clients ;
- Garantir l'intégrité des données ;

Les différents protocoles sont :

2.1. WEP (Wired Equivalent Privacy)

Le WEP est un protocole pour sécuriser les réseaux sans fil de type Wi-Fi. Les réseaux sans fil diffusant les messages échangés par ondes radioélectriques, sont particulièrement

sensibles aux écoutes clandestines. Le WEP tient son nom du fait qu'il devait fournir aux réseaux sans fil une confidentialité comparable à celle d'un réseau local filaire classique.

2.1.1. Clé WEP

La clé de session partagée par toutes les stations est statique, c'est-à-dire que pour déployer un grand nombre de stations Wi-Fi, il est nécessaire de les configurer en utilisant la même clé de session. Ainsi la connaissance de la clé est suffisante pour déchiffrer les communications. De plus, 24 bits de la clé servent uniquement pour l'initialisation, ce qui signifie que seuls 40 bits de la clé de 64 bits servent réellement à chiffrer et 104 bits pour la clé de 128 bits.

2.1.2. Principe du WEP

Le principe du WEP consiste à définir dans un premier temps la clé secrète. Cette clé doit être déclarée au niveau du point d'accès et des clients. Elle sert à créer un nombre pseudo-aléatoire d'une longueur égale à la longueur de la trame. Chaque transmission de donnée est ainsi chiffrée en utilisant le nombre pseudo-aléatoire comme masque grâce à un OU Exclusif entre ce nombre et la trame.

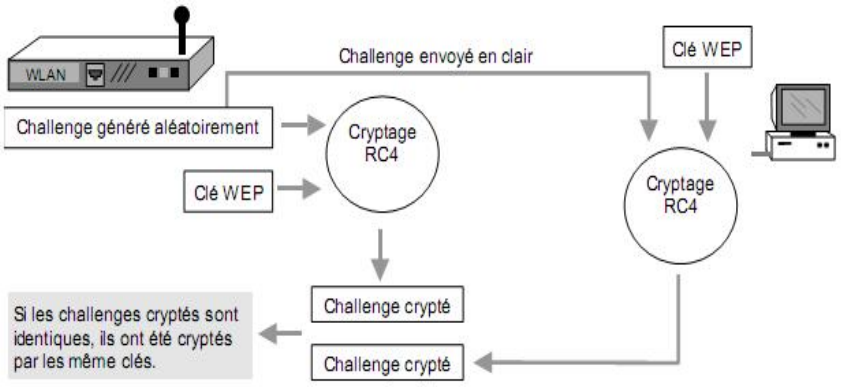

Figure II.6 : Principe du WEP

2.1.3. Failles du WEP

La faiblesse de WEP se situe dans son vecteur d'initialisation IV. Le IV est un nombre 24 bits qui est combiné avec la clef que l'administrateur réseau entre dans la configuration de son point d'accès. Un nouveau IV est utilisé pour chaque paquet transmis, il n'y a pas de problème ici. Par contre, le nombre IV n'est pas réellement un numéro aléatoire et peut être prédit par un panel. Ce qui est plus grave, le nombre IV se recycle lui même au bout d'un certain temps mais avec le même IV et la même clef avec un payload (contenu du message) différent. Si un

intrus collecte suffisamment de paquets (100 Mo à 1 Go), il sera capable de compromettre votre réseau.

Le WEP n'est donc pas suffisant pour garantir une réelle confidentialité des données. Pour autant, il est vivement conseillé de mettre au moins en œuvre une protection WEP 128 bits afin d'assurer un niveau de confidentialité minimum et d'éviter de cette façon 90% des risques d'intrusion.

2.2. WPA (Wi-Fi Protected Access)

Le WPA, développé par l'IEEE, est un autre protocole de sécurisation des réseaux sans fil offrant une meilleure sécurité que le WEP car il est destiné à en combler les faiblesses. En effet, le WPA permet un meilleur cryptage de données qu'avec le WEP car il utilise des clés TKIP (**T**emporal **K**ey Integrity **P**rotocol) - dites dynamiques - et permet l'authentification des utilisateurs. Ainsi, le WPA permet d'utiliser une clé par station connectée à un réseau sans fil, alors que le WEP lui utilisait la même clé pour tout le réseau sans fil. Les clés WPA sont en effet générées et distribuées de façon automatique par le point d'accès sans fil qui doit être compatible avec le WPA.

De plus, un vérificateur de données permet de vérifier l'intégrité des informations reçues pour être sûr que personne ne les a modifiées. **[9]**

2.2.1. Fonctionnement du WPA

WPA, lui est plus évolué avec un nombre IV de 48 bits: ce qui veut dire qu'il prendra beaucoup plus de temps avant que le nombre IV ne soit recyclé. Il faut également noter que dans la manière, WPA est supérieur dans sa méthode de connexion lorsque des utilisateurs sont connectés, ils sont authentifiés par des clefs pré-partagées, ou bien par des configurations plus sophistiquées, par une authentification (LDAP, RADIUS).

Une fois qu'un utilisateur est membre d'un réseau, une clef WPA est crée. Périodiquement, WPA va générer une nouvelle clef par utilisateur. Combiné à la longueur du nombre IV, ceci rend très difficile le piratage. Sur la transmission de chaque paquet, WPA ajoute un code de vérification d'intégrité de 4 bit (ICV) afin de les vérifier (injection de paquets, forge etc.). On peut donc conclure que l'utilisation de WPA est renforcée par rapport à la vérification WEP. Néanmoins un problème ici reste évident : Un attaquant peut intercepter la transmission, modifier le payload, recalculer le code d'intégrité, et le retransmettre sans que personne ne s'en aperçoive. WPA résout ce problème avec un message d'intégrité 8 bit : un payload crypté

et des facteurs dans le calcul de l'ICV réduise fortement les possibilités de forge de paquets (l'usurpation d'adresses IP sources).

2.2.2.TKIP (Temporal Key Integrity Protocol)

Protocole permettant le cryptage et le contrôle d'intégrité des données. Ce protocole utilise toujours le RC4 (d'où sa comptabilité avec le WEP) comme algorithme de cryptage avec une clé de 128 bits, par contre l'IV passe à 48 bits. De plus il y a une clé par station (et non une pour tout le réseau avec WEP), cette clé est générée et changer automatiquement de façon périodique. Le contrôle d'intégrité des données s'effectue par un code de hachage de 8 octets appelé MIC (**M**essage **I**ntegrity **C**ode) ou Michael. Ce code porte aussi les adresses MAC, ce qui évite de modifier ou forger des trames. De plus, il utilise un numéro de séquence sur les paquets, permettant un contrôle de bon séquencément.

2.3. WPA 2/ 802.11i

La dernière évolution en juin 2004, est la ratification de la norme IEEE 802.11i, aussi appelé WPA2 dans la documentation grand public. Ce standard reprend la grande majorité des principes et protocoles apportés par WPA, avec une différence notoire dans le cas du chiffrement : l'intégration de l'algorithme AES. Les protocoles de chiffrement WEP et TKIP sont toujours présents. Deux autres méthodes de chiffrement sont aussi inclus dans IEEE 802.11i en plus des chiffrements WEP et TKIP :

WRAP (**W**ireless **R**obust **A**uthenticated **P**rotocol) s'appuyant sur le mode opératoire OCB (**O**ffset **C**ode **B**ook) de AES ; CCMP (**C**ounter with **C**BC **M**AC **P**rotocol) : s'appuyant sur le mode opératoire CCM (**C**ounter with **C**BC-**M**AC) de AES ; Le chiffrement CCMP est le chiffrement recommandé dans le cadre de la norme IEEE 802.11i. Ce chiffrement, s'appuyant sur AES, utilise des clefs de 128 bits avec un vecteur d'initialisation de 48 bits. Ces mécanismes cryptographiques sont assez récents et peu de produits disponibles sont certifiés WPA2. Le recul est donc faible quant aux vulnérabilités potentielles de cette norme. Même si ce recul existe pour l'algorithme AES, le niveau de sécurité dépend fortement de l'utilisation et de la mise en œuvre d'AES.

La norme IEEE 802.11i définit deux modes de fonctionnement :

- **WPA Personal :** le mode « WPA personnel » permet de mettre en œuvre une infrastructure sécurisée basée sur le WPA sans mettre en œuvre de serveur d'authentification. Le WPA personnel repose sur l'utilisation d'une clé partagée, appelées PSK pour **P**ré-**S**hared **K**ey, renseignée dans le point d'accès ainsi que dans les postes clients. Contrairement au

WEP, il n'est pas nécessaire de saisir une clé de longueur prédéfinie. En effet, le WPA permet de saisir une phrase secrète, traduite en PSK par un algorithme de hachage. **[9]**

- **WPA Enterprise :** le mode entreprise impose l'utilisation d'une infrastructure d'authentification 802.1x basée sur l'utilisation d'un serveur d'authentification, généralement un serveur RADIUS, et d'un contrôleur réseau (le point d'accès). Cette solution est actuellement ce qu'il y a de plus sûr en termes de sécurité d'authentification forte. Mais attention, toutefois, rien n'est acquis et il y a fort à parier que cette solution ne restera pas à l'abri des hackers très longtemps. **[9]**

2.4. VPN (réseau privé virtuel)

Pour toutes les communications nécessitant un haut niveau de sécurisation, il est préférable de recourir à un chiffrement fort des données en mettant en place un réseau privé virtuel.

2.4.1. Concept de VPN

Une solution consiste à utiliser le réseau Wi-Fi comme support de transmission en utilisant un protocole d'encapsulation (en anglais tunneling, d'où l'utilisation impropre parfois du terme "tunnelisation"), c'est-à-dire encapsulant les données à transmettre de façon chiffrée. On parle alors de réseau privé virtuel (noté RPV ou VPN, acronyme de **V**irtual **P**rivate **N**etwork) pour désigner le réseau ainsi artificiellement créé. Le système de VPN permet donc d'obtenir une liaison sécurisée à moindre coût, si ce n'est la mise en œuvre des équipements terminaux.

2.4.2. Fonctionnement

Un réseau privé virtuel repose sur un protocole, appelé protocole de tunnelisation (tunneling), c'est-à-dire un protocole permettant aux données passant d'une extrémité du VPN à l'autre d'être sécurisées par des algorithmes de cryptographie. Le terme de "tunnel" est utilisé pour symboliser le fait qu'entre l'entrée et la sortie du VPN les données sont chiffrées (cryptées) et donc incompréhensible pour toute personne située entre les deux extrémités du VPN, comme si les données passaient dans un tunnel. Dans le cas d'un VPN établi entre deux machines, on appelle client VPN l'élément permettant de chiffrer et de déchiffrer les données du côté utilisateur (client) et serveur VPN, l'élément chiffrant et déchiffrant les données du côté de l'organisation.

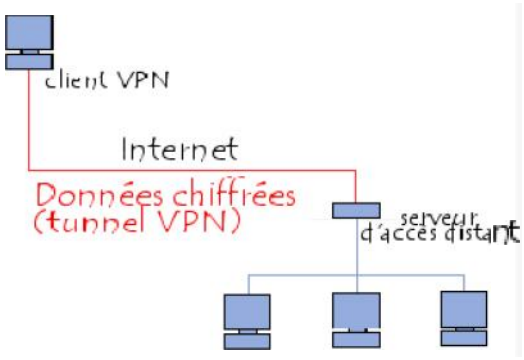

Figure II.7 : Principe de VPN

2.5. 802.1x

Le protocole 802.1x est une solution de sécurisation d'un réseau mis au point par l'organisme de standardisation IEEE en 2001. Il a pour but de contrôler l'accès à un réseau filaire ou sans fil grâce à un serveur d'authentification. Le standard permet de mettre en relation le serveur d'authentification et le système à authentifier par des séquences par des échanges EAP. Le protocole 802.1x va donc unifier les différents méthodes d'authentification sous la même bannière : le protocole EAP.

La principale innovation amenée par le standard 802.1x consiste à scinder le port logique, qui est connectés en parallèle sur le port physique. Le premier port logique est dit "contrôle", et peut prendre deux états "ouvert" ou "fermé". Le deuxième port logique est lui toujours accessible mais il ne gère que les trames spécifique à 802.1x. Cela permet de gérer le dialogue nécessaire à l'authentification au préalable à une connexion réseau. La connexion initiale est donc limitée à un usage de sécurité qui ouvre ultérieurement le canal des données en cas d'authentification réussie. **[19]**

802.1x est aussi appelé Port-based Network Access Control, c'est-à-dire qu'il introduit une notion de port contrôlé par l'authentification. Une station ne pourra accéder aux ressources d'un LAN que si elle a été auparavant authentifiée.

Le protocole fonctionne à partir de trois éléments :

- **Le client (supplicant) :** c'est le système à authentifier c'est-à-dire l'élément qui désire se connecter sur le réseau ;
- **Le contrôleur (point d'accès) :** ou système authentificateur c'est-à-dire l'élément qui va demander l'authentification;
- **Le serveur d'authentification :** Ce serveur d'authentification est en général un serveur Radius. Selon la requête du supplicant, ce serveur détermine les services auxquels le demandeur a accès (serveur placé sur le LAN).

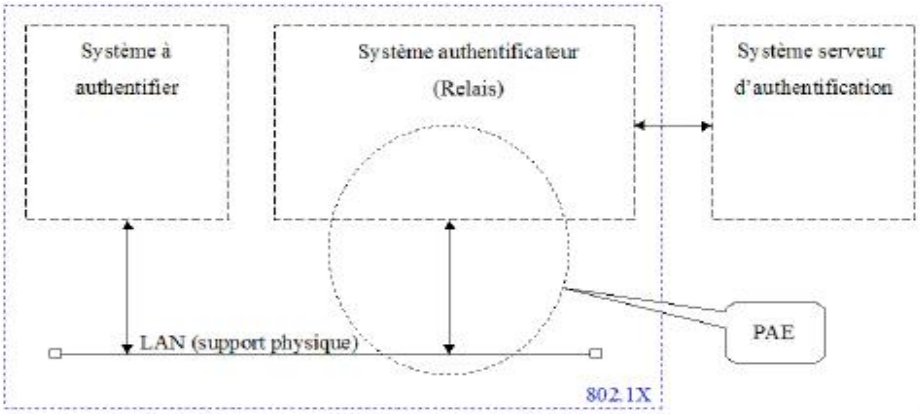

Figure II.8 : Les trois entités qui interagissent dans le 802.1x

La communication entre ces éléments fait intervenir différents protocoles suivant un principe de fonctionnement spécifique.

2.5.1.Mécanisme générale

Le supplicant souhaite accéder aux ressources du réseau, mais pour cela il va devoir s'authentifier. Le système authentificateur gère cet accès via le PAE (**P**ort **A**ccess **E**ntity) ; ce PAE est divisé en deux ports, un port contrôlé (connexion ouverte ou fermée) donnant accès à la ressource en cas de succès de l'authentification, et un port non contrôlé (connexion toujours ouverte) servant à l'authentification où tout autre trafic est rejeté.

Le port contrôlé peut être ouvert ou fermé suivant le contrôle qui a été défini au moyen d'une variable (Auth Controlled Port Control). Cette variable peut prendre trois états :

- **ForceUnauthorized :** l'accès au port contrôlé est interdit (connexion toujours ouverte).
- **ForceAuthorized :** l'accès au port contrôlé est autorisé (connexion toujours fermée).
- **Auto (par défaut) :** l'accès dépend du résultat de l'authentification.

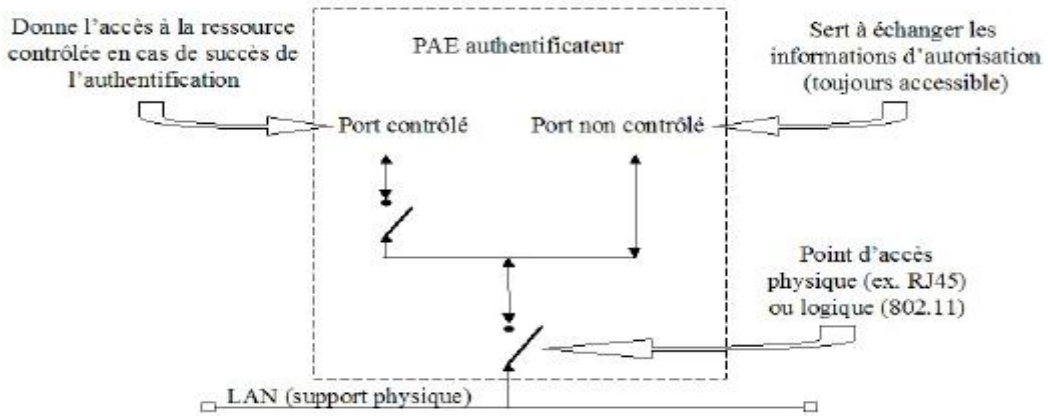

Figure II.9 : PAE

L'utilisation du 802.1x en Wi-Fi permettra l'authentification du demandeur, le contrôle d'accès aux bornes et la distribution des clés WEP. Mais attention, il faut que le 802.1x soit bien implémenté sur les différentes machines. Si les implémentations sur les bornes et serveurs sont disponibles, il n'en est pas de même chez les postes clients. Le 802.1x est maintenant de plus en plus intégré avec le système d'exploitation. **[21]**

2.5.2.EAP (Extensible Authentification Protocol)

EAP est une extension de PPP définie par la RFC 2284. Il permet l'authentification des utilisateurs du lien selon de nombreuses méthodes possibles. En somme, on peut dire que l'EAP est une sorte de protocole "parapluie" pour l'authentification : il détermine un schéma d'authentification (Kerberos, mot de passe jetable, PKA, etc.). **[14]**

Une extension d'EAP s'appelle EAPOL pour "**EAP O**ver **L**an". Celle-ci permet de faire transiter des requêtes EAP à travers un réseau LAN en direction d'un serveur compétent qui se chargera de passer la requête EAPOL en EAP.

2.5.2.1. Composition du paquet EAP

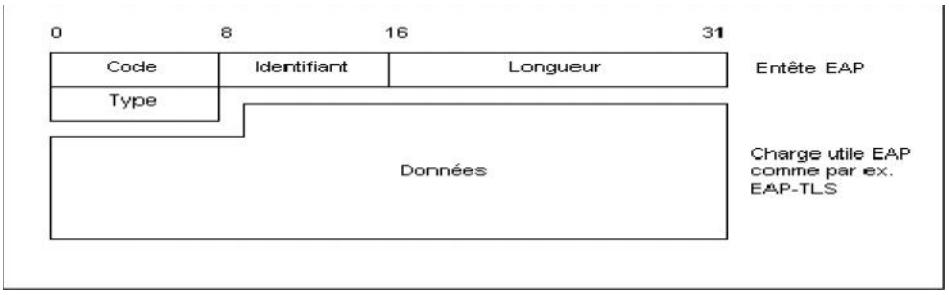

Figure II.10 : Paquet EAP

- **Champ code**

Dans l 'en-tête du paquet EAP, le champ code correspond au premier octet.

Il en existe 4 types : **[22]**

- Request : le système authentificateur émet une requête d'information auprès du supplicant.
- Response : le supplicant répond à la requête du système authentificateur.
- Success : le système authentificateur informe le supplicant du succès de la demande d'authentification.
- Failure : le système authentificateur informe le supplicant de l'échec de la demande d'authentification.

- **Champ identifiant**

Codé sur un octet également, il sert à identifier une session d'authentification. Ce champ change pour chaque nouvelle requête ou réponse. Si une duplication d'une requête doit être faite, l'identifiant ne change pas. **[22]**

- **Champ longueur**

Codé sur 2 octets, il indique la longueur de l'ensemble du paquet EAP, il prend donc en compte la longueur des données mais aussi des longueurs des autres champs de l'entête comme le type, le code...

Ainsi on connaîtra la taille des données utiles même en cas de bourrage par la couche liaison. **[22]**

- **Champ type**

Ce champ est codé sur un octet et définit le type de données que contient le paquet EAP. Logiquement, requête et réponse possèdent des trames de même type.

Nous allons particulièrement nous intéresser au champ type lors des communications requête / réponse. **[22]**

2.5.2.2. Méthodes d'authentification associés a EAP

Le standard 802.1x ne propose pas une seule méthode d'authentification mais un canevas sur lequel sont basés plusieurs types d'authentification. Ainsi, une méthode d'authentification EAP utilise différents éléments pour identifier un client :

- Login / mot de passe ;
- Certificats ;
- Carte à puce ou calculette ;

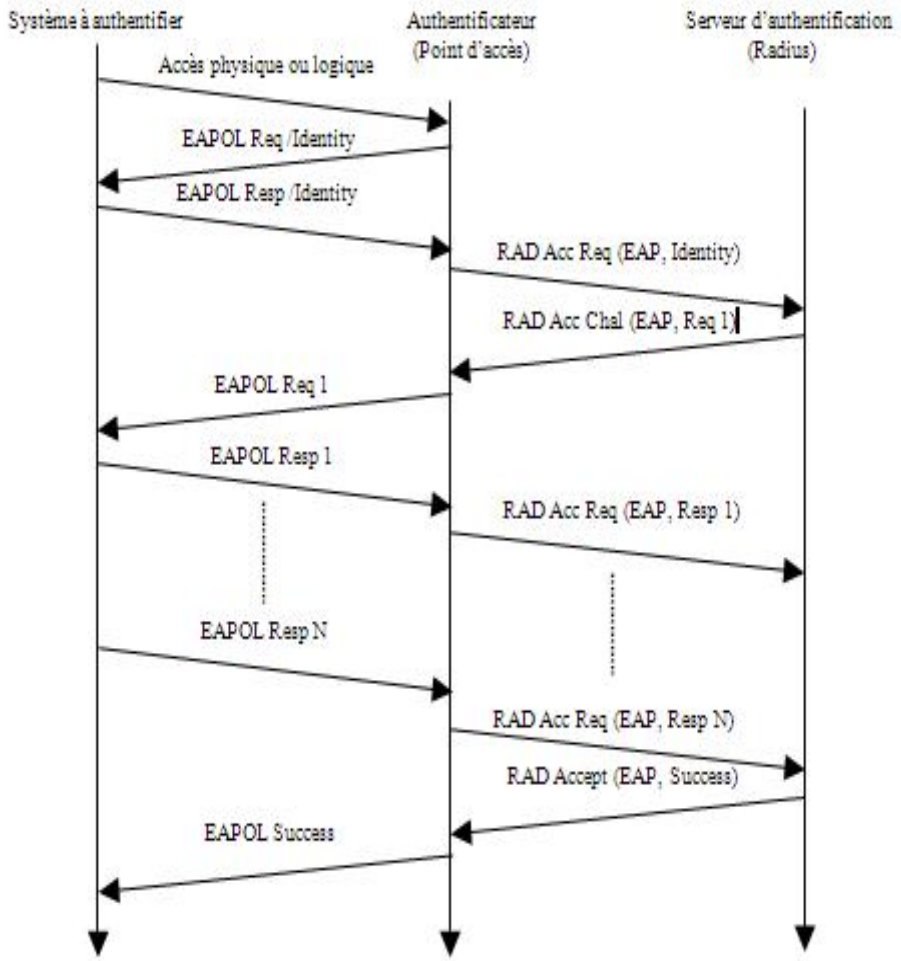

Figure II.11 : Séquence d'authentification 802.1x

a. Méthodes basées sur les mots de passes [22]

- **LEAP:** (**L**ightweight **E**xtensible **A**uthentification **P**rotocol) c'est la méthode la plus utilisée pour les points d'accès. Il gère la distribution dynamique de clés WEP. C'est aussi à la base une solution propriétaire de Cisco (CISCO-EAP) mais qui a aussi été implémentée par la suite par d'autres constructeurs.
- **EAP-MD5:** (**EAP-M**essage **D**igest **5**) il est souvent utilisé pour les informations d'authentification des clients, par un système basé sur le nom d'utilisateur et le mot de passe. Il n'existe pas d'authentification du serveur. Une machine qui se fait passer pour un serveur peut ainsi facilement récupérer les authentifiants (login, mot de passe) de la machine qui cherche à s'authentifier.
- **EAP-SKE:** (**EAP-S**hared **K**ey **E**xchange) il permet une authentification mutuelle ainsi qu'une itinérance entre les réseaux de plusieurs fournisseurs d'accès Internet.
- **EAP-SRP:** Il s'agit de l'adaptation du protocole SRP (RFC2945) à l'EAP.

b. Méthodes basées sur les certificats

- **EAP-TLS:** utilise le mécanisme d'authentification à clé publique de TLS. Client et serveur doivent posséder un certificat. Permet l'authentification mutuelle, l'échange des clés (WEP dynamique ou TKIP), la fragmentation et le réassemblage, la reconnexion rapide.
- **EAP-TTLS:** méthode du tunnel TLS. Fournit une séquence d'attributs inclus dans le message. En incluant un attribut de type RADIUS, EAP peut fournit les mêmes fonctionnalités que PEAP. Cependant, si un mot de passe RADIUS ou CHAP est encapsulé, il est chiffré par TLS. Cette méthode est moins utilisée que PEAP qui rend les mêmes services.
- **PEAP:** (**P**rotected **EAP)** authentification sans certificat. Ajoute une couche TLS sur EAP (comme EAP-TTLS), permet d'authentifier le serveur au client mais pas l'inverse, c'est la méthode protégée par PEAP qui doit authentifier le client. Offre les services d'authentification (impossible de falsifier ou insérer des messages EAP), de chiffrement, d'échange de clé (WEP dynamique ou TKIP), fragmentation et réassemblage, reconnexion rapide.
- **PEAP Microsoft:** supporte l'authentification du client via MS-CHAP v2 uniquement réduisant ainsi le champ d'utilisation au domaine NT et ADS.

c. Méthodes basées sur les cartes à puces

- **EAP-SIM:** (**EAP** - **S**ubsciber **I**dentity **M**odule) utilisé pour les points d'accès public (hot spot), utilise la carte à puce SIM du GSM, permet la mise en place de facturation.
- **EAP-AKA:** (**EAP** - **A**uthentification and **K**ey **A**greement) utilise le système d'authentification de la carte SIM de l'UMTS, il est compatible avec le GSM.

2.5.3.Faiblesses 802.1x

La principale faiblesse de 802.1x vient de ce qu'il a été conçu au départ dans un contexte de connexion physique (type accès PPP sur RTC). Rien n'empêche en effet un utilisateur d'insérer un hub (transparent à 802.1x) et de faire bénéficier d'autres utilisateurs de l'ouverture du port Ethernet d'un commutateur. La plupart des implémentations d'équipementiers permettent de surmonter cette difficulté en permettant de configurer un blocage du port Ethernet si l'adresse MAC du système authentifié change. Les attaques par écoute et rejeu sont aussi possibles, ainsi que le vol de session des faiblesses de 802.1x. Les attaques sur 802.1x sont, de plus, facilitées dans le cas de l'Ethernet sans fil.

2.6. Protocole Radius

2.6.1. Présentation

RADIUS (**R**emote **A**uthentification **D**ial **I**n **U**ser **S**ervice) est un protocole d'authentification client/serveur habituellement utilisé pour l'accès à distance, défini par la RFC 2865. Ce protocole permet de sécuriser les réseaux contre des accès à distance non autorisés. Ce protocole est indépendant du type de support utilisé. **[14]**

Le protocole Radius repose principalement sur un serveur (serveur Radius), relié a une base d'identification (fichier local, base de données, annuaire LDAP, etc.) et un client Radius, appelé NAS (**N**etwork **A**ccess **S**erver), faisant office d'intermédiaire entre l'utilisateur final et le serveur. Le mot de passe servant à authentifier les transactions entre le client Radius et le serveur Radius est chiffré et authentifier grâce a un secret partagé.

Il est à noter que le serveur Radius peut faire office de proxy, c'est-à-dire transmettre les requêtes du client a d'autres serveurs Radius.

2.6.2. Principe de fonctionnement

Le fonctionnement de Radius est basé sur un scénario proche de celui-ci :

1. Un utilisateur envoie une requête au NAS afin d'autoriser une connexion à distance ;
2. Le NAS achemine la demande au serveur Radius ;
3. Le serveur Radius consulte la base de données d'identification afin de connaître le type de scénario d'identification demandé pour l'utilisateur. Soit le scénario actuel convient, soit une autre méthode d'identification est demandée à l'utilisateur. Le serveur Radius retourne ainsi une des quatre réponses suivantes :

- **ACCEPT :** l'identification a réussi ;
- **REJECT :** l'identification a échoué ;
- **CHALLENGE :** le serveur RADIUS souhaite des informations supplémentaires de la part de l'utilisateur et propose un « défi » (en anglais « *challenge* ») ;
- **CHANGE PASSWORD :** le serveur Radius demande à l'utilisateur un nouveau mot de passe.

Suite à cette phase d'authentification débute une phase d'autorisation ou le serveur retourne les autorisations aux utilisateurs.

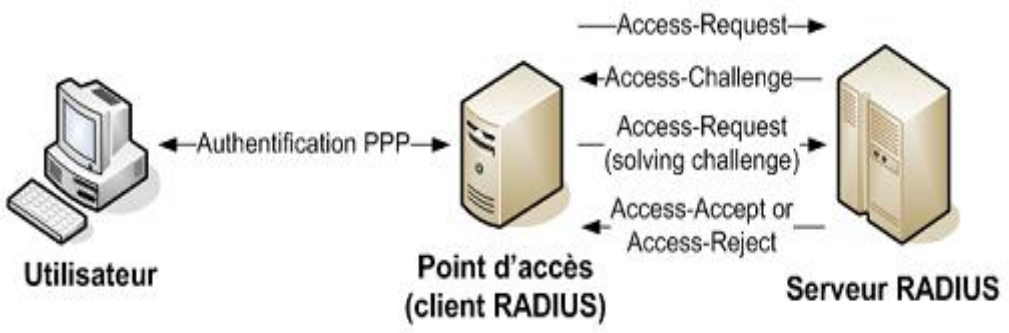

Figure II.12 : Principe de fonctionnement de Radius

- **Paquets Radius**

Un paquet Radius est inclus dans un et un seul paquet UDP. Le schéma suivant représente un paquet Radius standard, les unités étant exprimées en octets :

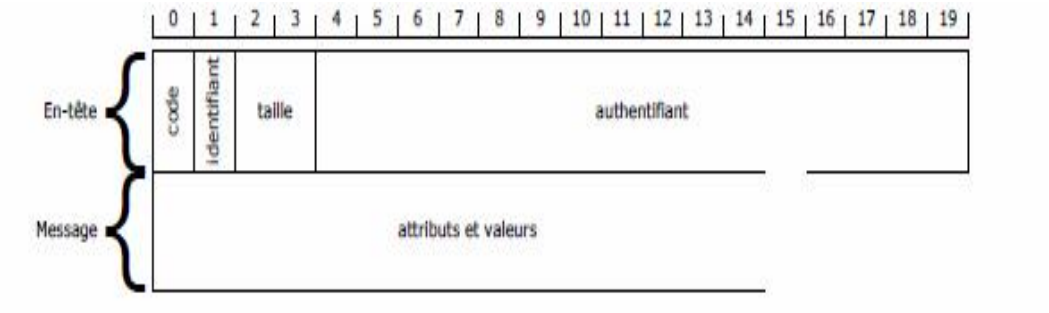

Figure II.13 : Paquets Radius

- **Code :** identifie le type de message

Code	Description
Access - Request	Demande accès à un service
Access -Accept	Réponse favorable à la demande du client
Access - Reject	Réponse négative au client
Accounting - Request	Demande les informations d'authentification
Accounting - Response	Informations d'authentification
Access - challenge	Sollicite des informations supplémentaires pour l'autorisation du client

Tableau II.2 : Description du champ code

- **Identifiant :** permet de reconnaitre les messages (requêtes et réponses) d'une même session d'authentification.
- **Longueur (taille) :** définie la longueur de la trame.
- **Authentificateur :** permet au client d'authentifier la réponse de serveur Radius et de protégé les mots de passe (évite le phénomène « man in the middle » par exemple). Il contient également la méthode d'authentification à utiliser avec le client.
- **Attributs :** ce champ est utilisé pour véhiculer toutes les informations nécessaires, il a pour format :

Type	Longueur	Valeur

Figure II.14 : Format des attributs Radius

Conclusion

En prenant connaissance des faiblesses de sécurité des réseaux de type Wi-Fi et au vu de l'essor important de ce type de matériel, il est probable que le marché des serveurs d'authentification va prendre de l'importance. Ainsi, depuis les tests, certains produits ont déjà beaucoup évolué pour prendre en charge davantage de méthodes d'authentification et de plateformes. Cependant, sur le segment de la sécurité des réseaux Wi-Fi, d'autres solutions restent envisageables notamment celles basées sur les VPN.

Le niveau de sécurité proposé par 802.1x est correct mais il ne permet pas de résoudre les problèmes liés aux faiblesses de WEP. Ainsi, pour proposer une architecture vraiment sûre il faudra utiliser d'autres techniques de chiffrement comme WPA et attendre les avancées proposées par 802.11i. La relative jeunesse de tous ces protocoles, et des réseaux Wi-Fi en général, ne permettent pas encore de garantir une pérennité de la solution retenue. Malgré tout, il est nécessaire de prendre le risque d'opter pour une solution plutôt que d'attendre et de laisser son réseau sans fil sans protection.