



Les réseaux WiFi: La sécurité



A. Introduction

1. Le risque lié aux ondes radio électrique

Les ondes radio électriques ont intrinsèquement une grande capacité à se propager dans toutes les directions avec une portée relativement grande. Il est ainsi très difficile d'arriver à confiner leurs émissions dans un périmètre restreint. La propagation des ondes radio doit également être pensée en trois dimensions. Ainsi les ondes se propagent également d'un étage à un autre (avec de plus grandes atténuations).

La principale conséquence de cette "propagation sauvage" des ondes radio est la facilité que peut avoir une personne non autorisée d'écouter le réseau, éventuellement en dehors de l'enceinte du bâtiment où le réseau sans fil est déployé.

Là où le bât blesse c'est qu'un réseau sans fil peut très bien être installé dans une entreprise sans que le service informatique ne soit au courant ! Il suffit en effet à un employé de brancher un point d'accès sur une prise réseau pour que toutes les communications du réseau soient rendues "publiques" dans le rayon de couverture du point d'accès !



2. Le War-driving

Étant donné qu'il est très facile d'"écouter" des réseaux sans fils, une pratique venue tout droit des États Unis consiste à circuler dans la ville avec un ordinateur portable (voire un assistant personnel) équipé d'une carte réseau sans fil à la recherche de réseaux sans fils, il s'agit du war-driving (parfois noté wardriving ou war-Xing pour "war crossing"). Des logiciels spécialisés dans ce type d'activité permettent même d'établir une cartographie très précise en exploitant un matériel de géo localisation (GPS, Global Positionning System).

Les cartes établies permettent ainsi de mettre en évidence les réseaux sans fil déployés non sécurisés, offrant même parfois un accès à Internet ! De nombreux sites capitalisant ces informations ont vu le jour sur Internet, si bien que des étudiants londoniens ont eu l'idée d'inventer un "langage des signes" dont le but est de rendre visible les réseaux sans fils en dessinant à même le trottoir des symboles à la craie indiquant la présence d'un réseau wireless, il s'agit du « war-chalking » (francisé en craieFiti ou craie-fiti).

Deux demi-cercles opposés désignent ainsi un réseau ouvert offrant un accès à Internet	Un rond signale la présence d'un réseau sans fil ouvert sans accès à un réseau filaire	Un W encerclé met en évidence la présence d'un réseau sans fil correctement sécurisé



B. Les risques en matière de sécurité

Les risques liés à la mauvaise protection d'un réseau sans fil sont multiples :

- L'interception de données consistant à écouter les transmissions des différents utilisateurs du réseau sans fil.
- Le détournement de connexion dont le but est d'obtenir l'accès à un réseau local ou à Internet.
- Le brouillage des transmissions consistant à émettre des signaux radio de telle manière à produire des interférences.
- Les dénis de service rendant le réseau inutilisable en envoyant des commandes factices.

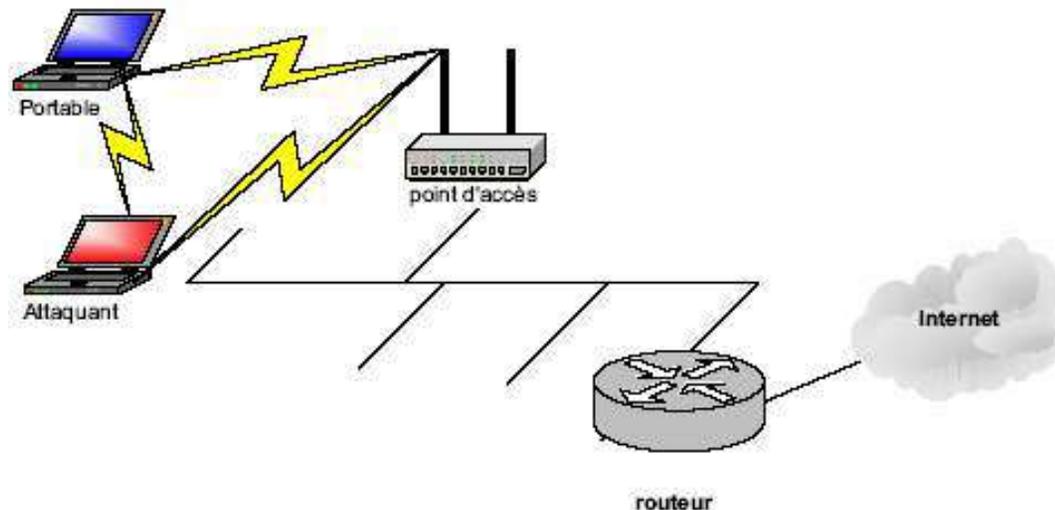
1. L'interception de données

Par défaut un réseau sans fil est non sécurisé, c'est-à-dire qu'il est ouvert à tous et que toute personne se trouvant dans le rayon de portée d'un point d'accès peut potentiellement écouter toutes les communications circulant sur le réseau. Pour un particulier la menace est faible car les données sont rarement confidentielles, si ce n'est les données à caractère personnel. Pour une entreprise en revanche l'enjeu stratégique peut être très important.

2. L'intrusion réseau

Lorsqu'un point d'accès est installé sur le réseau local, il permet aux stations d'accéder au réseau filaire et éventuellement à Internet si le réseau local y est relié. Un réseau sans fil non sécurisé représente de cette façon un point d'entrée royal pour le pirate au réseau interne d'une entreprise ou une organisation.

Outre le vol ou la destruction d'informations présentes sur le réseau et l'accès à Internet gratuit pour le pirate, le réseau sans fil peut également représenter une aubaine pour ce dernier dans le but de mener des attaques sur Internet. En effet étant donné qu'il n'y a aucun moyen d'identifier le pirate sur le réseau, l'entreprise ayant installé le réseau sans fil risque d'être tenue responsable de l'attaque.





3. Les dénis de service

La méthode d'accès au réseau de la norme 802.11 est basée sur le protocole CSMA/CA, consistant à attendre que le réseau soit libre avant d'émettre. Une fois la connexion établie, une station doit s'associer à un point d'accès afin de pouvoir lui envoyer des paquets. Ainsi, les méthodes d'accès au réseau et d'association étant connus, il est simple pour un pirate d'envoyer des paquets demandant la désassociation de la station. Il s'agit d'un déni de service, c'est-à-dire d'envoyer des informations de telle manière à perturber volontairement le fonctionnement du réseau sans fil.

D'autre part, la connexion à des réseaux sans fils est consommatrice d'énergie. Même si les périphériques sans fils sont dotés de fonctionnalités leur permettant d'économiser le maximum d'énergie, un pirate peut éventuellement envoyer un grand nombre de données (chiffrées) à une machine de telle manière à la surcharger. En effet, un grand nombre de périphériques portables (assistant digital personnel, ordinateur portable, ...) possèdent une autonomie limitée, c'est pourquoi un pirate peut vouloir provoquer une surconsommation d'énergie de telle manière à rendre l'appareil temporairement inutilisable, c'est ce que l'on appelle un déni de service sur batterie.

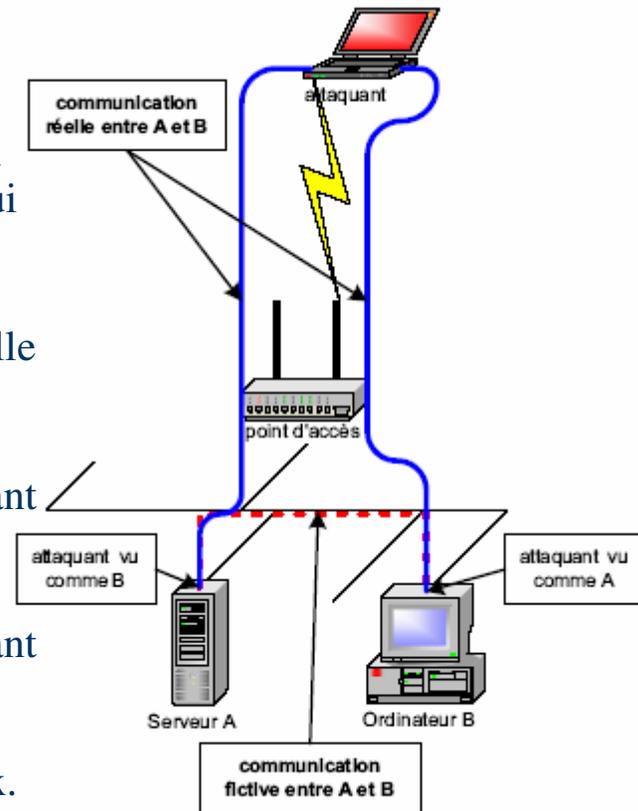
4. L'usurpations d'identité

L'usurpation d'identité, revêt un caractère actif puisque l'agent malveillant cherche à pénétrer le réseau en usurpant l'identité d'une personne autorisée, ceci pouvant parfois se faire de manière transparente. Une fois l'opération réussie, il a toute liberté d'action pour porter atteinte à l'intégrité du réseau en modifiant ou en supprimant les informations qui y circulent.

Pour ce faire, l'agent malveillant a la possibilité d'usurper soit l'identité d'un point d'accès, soit celle d'un client.

Dans la première hypothèse, l'attaquant se place entre le client et le véritable point d'accès tout en feignant d'être légitime ; il peut alors à loisir enregistrer et modifier les données transmises.

Dans la seconde , il se fait passer pour un client pouvant légitimement accéder à l'ensemble du réseau (sans fil et/ou filaire). L'aspect immatériel du réseau ne permet pas de distinguer le véritable client du faux. Dans ce cas, les informations qui normalement transitaient uniquement par le réseau filaire, peuvent être déroutées et passer désormais sur le réseau radio.





5. Le brouillage radio

Les ondes radio sont très sensibles aux interférences, c'est la raison pour laquelle un signal peut facilement être brouillé par une émission radio ayant une fréquence proche de celle utilisée dans le réseau sans fil. Un simple four à micro-ondes peut ainsi rendre totalement inopérable un réseau sans fil lorsqu'il fonctionne dans le rayon d'action d'un point d'accès.

6. Le danger des postes nomades

Un poste nomade présente 2 niveaux de faiblesse :

lors de l'utilisation d'un hot spot, les cryptages de type WEP ou WPA sont généralement déconnectés. Le poste client est alors une cible potentielle pour un pirate situé à proximité,

lorsqu'un ordinateur portable a été piraté, il devient un excellent relais pour une attaque du site central, puisqu'il sera reconnu par celui-ci comme un ami.

Les postes nomades requièrent donc une protection soigneuse, aussi bien pour eux mêmes, que pour le danger potentiel qu'il représente pour le site central (mise en place de firewalls individuels, communications en mode VPN...).



C. La sécurisation d'un réseau WiFi

1. Une infrastructure adaptée

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. 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. Éviter 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.



3. Le 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.

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

4. WEP - Wired Equivalent Privacy

a. Introduction

Pour remédier aux problèmes de confidentialité des échanges sur les réseaux sans fils, le standard 802.11 intègre un mécanisme simple de chiffrement des données, il s'agit du WEP, Wired equivalent privacy.

Le WEP est un protocole chargé du chiffrement des trames 802.11 utilisant l'algorithme symétrique RC4 avec des clés d'une longueur de 64 ou 128 bits..



b. La clé WEP

La clé de session partagé par toutes les stations est statique, c'est-à-dire que pour déployer un grand nombre de stations WiFi 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

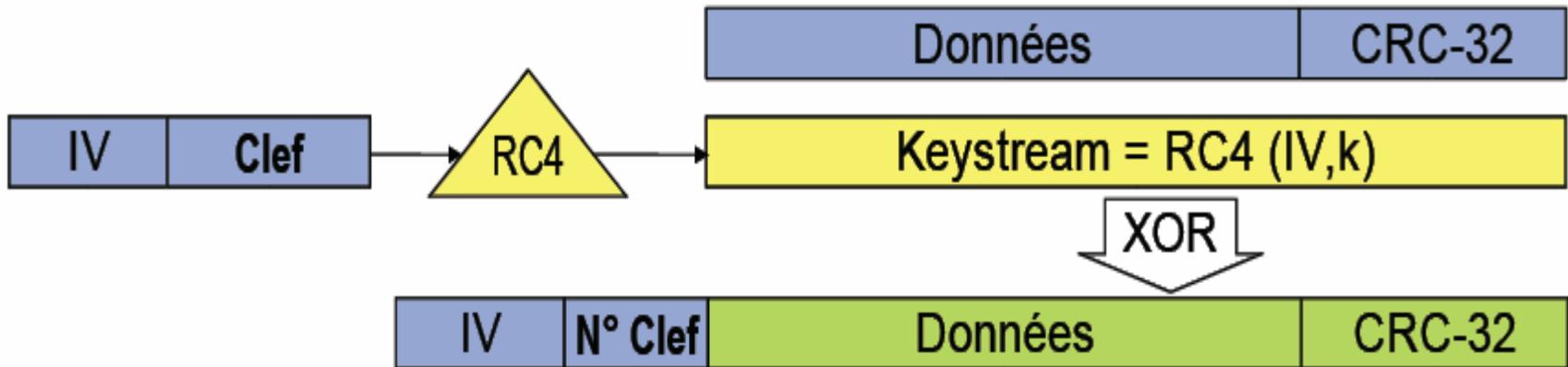
De plus, 24 bits de la clé servent uniquement pour l'initialisation, ce qui signifie que seuls 40 bits de la clé de 64 bits servent réellement à chiffrer et 104 bits pour la clé de 128 bits.

	Vecteur d'initialisation (IV)	Clef partagée	Clef RC4 $K=IV,k$
WEP	24 bits	40 bits (x4)	64 bits (4x)
WEP2	24 bits	104 bits	128 bits

c. Le 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.





d. La faiblesse de 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. Secondo, 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 oeuvre une protection WEP 128 bits afin d'assurer un niveau de confidentialité minimum et d'éviter de cette façon 90% des risques d'intrusion.



5. Le 802.1X

a. Présentation

La norme IEEE 802.1X (Port-Based Network Access Control, juin 2003 web) propose un moyen d'authentifier les équipements connectés sur un port avant de leur donner l'accès au réseau. Elle utilise EAP (Extensible Authentication Protocol, RFC 2284 txt).

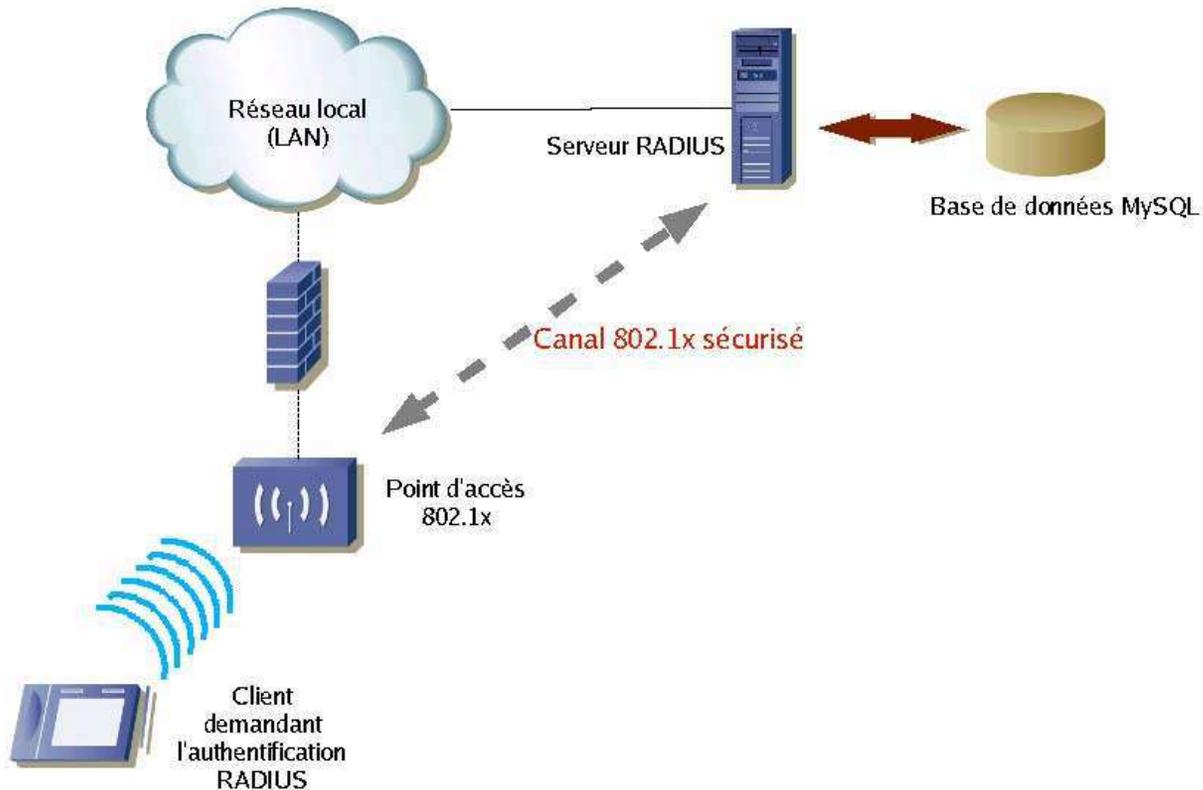
EAP est un protocole générique qui permet de transporter divers protocoles d'authentification, l'encapsulation de chaque protocole d'authentification dans EAP étant défini à part. Parmi les protocoles qu'on peut transporter dans EAP : TLS (EAP-TLS), PEAP (EAP-PEAP), TTLS (EAP-TTLS).

L'utilisation de l'authentification 802.1X avec le chiffrement WEP permet de pallier certains des problèmes du WEP tel qu'il est défini dans 802.11:

- L'authentification du client n'est plus effectuée par le point d'accès avec la clé pré-partagée, mais par un serveur RADIUS à l'aide d'un protocole d'authentification tel que TLS, TTLS ou PEAP.
- La clé de chiffrement n'est plus statique et commune à tous les clients : une nouvelle clé WEP est générée pour chaque utilisateur et chaque session.

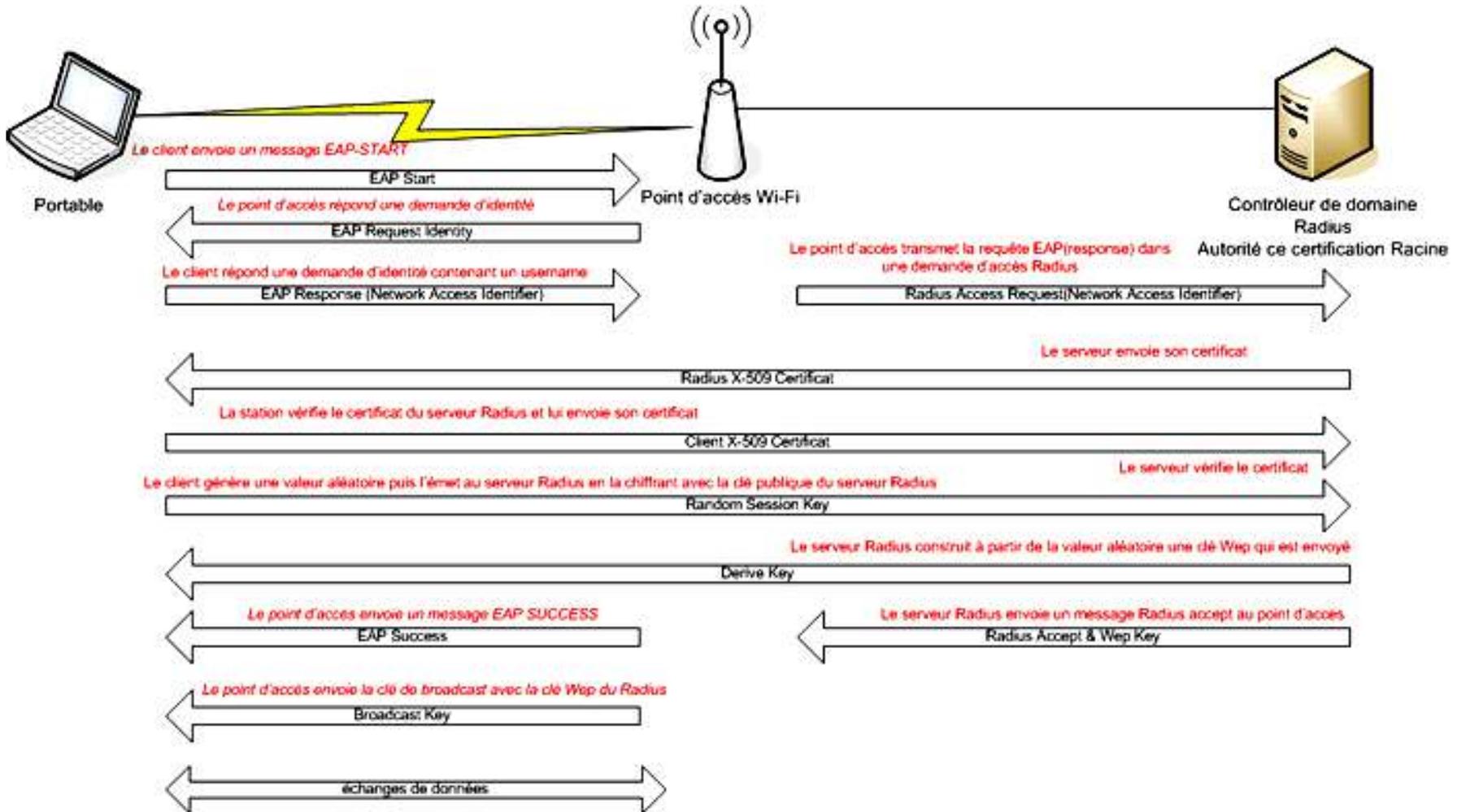
b. Le principe

Le principe de l'authentification 802.1X consiste en ce que l'équipement d'accès au réseau (commutateur filaire ou point d'accès sans fil) ne relaie que les trames EAP entre le poste client et un serveur d'authentification (qui, dans la pratique, est un serveur RADIUS), sans avoir à connaître le protocole d'authentification utilisé. Si le protocole d'authentification comprend la génération de clés de session, qui est unique, celles-ci sont transmises à l'équipement d'accès et utilisées pour le chiffrement de la session.





c. Principe de l'échange d'authentification





d. Inconvénient

L'usage de 802.1X, outre le serveur d'authentification, impose un service de gestion des utilisateurs comme pour tout système gérant une authentification, des bornes adéquates, et le logiciel client déployé sur les postes clients. Seul les toutes dernières versions de Windows, MacOS ou Linux intègrent EAP-TLS en standard. Il y a quelques effets induits : le temps de connexion au réseau est plus lent pour les utilisateurs, et l'ensemble de ce mécanisme, de l'authentification au chiffrement WEP, est incompatible avec le handover qui permet la mobilité de borne à borne. L'IEEE a récemment lancé la normalisation d'un protocole pour pallier à ce problème.

En entreprise, en plus de l'authentification 802.1X, il faut segmenter son infrastructure sans fil du réseau interne de l'entreprise par un routeur filtrant ou firewall.



6. WPA (wifi protected access)

beaucoup de points d'accès 802.11g utilisent le wifi protected access (WPA).

WPA utilise une clé pré - partagée afin de chiffrer les transmissions. Pour le moment il n'y a pas de d'outils pour cracker le WPA. Cependant, il restera à l'attaquant déterminé une attaque par dictionnaire, ce qui signifie qu'il peut essayer toute les combinaisons de mots possibles et les expressions communes jusqu'a ce qu'il parvienne à ses fins. Comme vous pouvez aisément l'imaginer, cela prend beaucoup plus de temps que de casser du WEP avec un outil automatisé. WPA est donc plus sécurisé.

Fonctionnement du WPA

WPA, lui est plus évolué avec un nombre IV 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 créée. 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 en conclure que l'utilisation de WPA est renforcée par rapport à la vérification WEP.

Néanmoins le problème ici est 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 réduisent fortement les possibilités de forge de paquets (l'usurpation d'adresses IP sources).



7. IEEE802.11i ou WPA2

La dernière évolution en date de 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 notable dans le cas du chiffrement : l'intégration de l'algorithme AES (Advanced Encryption Standard). Les protocoles de chiffrement WEP et TKIP sont toujours présents.

Deux autres méthodes de chiffrement sont aussi incluses dans IEEE 802.11i en plus des chiffrements WEP et TKIP :

- WRAP (Wireless Robust Authenticated Protocol) :
s'appuyant sur le mode opératoire OCB (Offset Codebook) de AES ;
- CCMP (Counter Mode with CBC MAC Protocol) :
s'appuyant sur le mode opératoire CCM (Counter with CBC-MAC) 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 oeuvre de AES.



Pour en profiter du WPA2 les entreprises devront bien souvent passer par le remplacement de leur équipements sans-fil : les calculs exigés par AES nécessitent la présence d'une puce cryptographique dédiée et d'une alimentation électrique plus consistante (certains produits récents, qui supportent déjà AES, pourront migrer vers WPA2 avec une simple mise à jour logicielle).

Fort heureusement pour les possesseurs d'équipements anciens, WPA2 est compatible avec son prédécesseur : les entreprises ayant déployés des réseaux WPA pourront y intégrer des équipements à la nouvelle norme à leur rythme. Elles apprécieront.

Pour l'heure, six fabricants seulement proposent des matériels agréés WPA2. Il s'agit de Cisco, Intel (dont les chipset Centrino), Broadcom, Realtek, Atheros et Instant802 Networks.

De plus, WPA2, tous les systèmes d'exploitation n'intègrent pas la norme WPA2 ou IEEE 802.11i.



8. Réseaux Privés virtuels (VPN)

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 (VPN).

a. Le concept de réseau privé virtuel

Une solution consiste à utiliser le réseau WiFi 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 Virtual Private Network) 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 oeuvre des équipements terminaux.



b. Fonctionnement d'un VPN

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.

c. Le certificat numérique

La sécurité du VPN repose sur l'utilisation de certificats numériques, et la plupart des solutions actuelles du marché prévoient de stocker le certificat de l'utilisateur sur le disque dur de sa machine, d'autre abrite ces certificats dans un support amovible,. Le certificat n'est donc plus associé à une machine mais à un utilisateur.

Lors de l'établissement de la connexion, l'utilisateur doit s'authentifier en introduisant sa clé dans le connecteur USB ou sa carte dans un lecteur, puis en saisissant son code secret.



d. Les protocoles de tunnelisation

Les principaux protocoles de tunneling sont les suivants :

- PPTP (Point-to-Point Tunneling Protocol) est un protocole de niveau 2 développé par Microsoft, 3Com, Ascend, US Robotics et ECI Telematics.
- L2F (Layer Two Forwarding) est un protocole de niveau 2 développé par Cisco, Northern Telecom et Shiva. Il est désormais quasi-obsolète
- L2TP (Layer Two Tunneling Protocol) est l'aboutissement des travaux de l'IETF (RFC 2661) pour faire converger les fonctionnalités de PPTP et L2F. Il s'agit ainsi d'un protocole de niveau 2 s'appuyant sur PPP.
- IPSec est un protocole de niveau 3, issu des travaux de l'IETF, permettant de transporter des données chiffrées pour les réseaux IP.