***05-Sécurité des réseaux sans fils***

***Définition***

* Le Wifi est une technologie permettant de créer des réseaux informatiques sans fil (Wireless). Il s'agit d'une norme de l'IEEE baptisée 802.11.   
    
  Sa portée varie d'un appareil à l'autre entre quelques dizaines de mètres à plusieurs centaines de mètres, ce qui en fait une technologie de premier choix pour le réseau domestique avec connexion internet.

***Fonctionnement***

Un réseau Wifi peut fonctionner de deux manières différentes :

* Le mode **Ad-Hoc** chaque membre du réseau retransmet les informations qu'il reçoit aux autres membres du réseau. Le problème dans ce type de réseau, c'est que d'une part, la bande passante du réseau est basée sur la vitesse de l'hôte le plus lent et que d'autre part, ce mode peut être utilisé dans une maison pour un réseau simple, il a l'avantage de ne pas coûter cher.
* Le mode **Infrastructure** : avec ce mode, tout est géré par un point d'accès, les données qu'un hôte émet lui sont transmises et lui seul les renvoie aux autres membres du réseau. Ainsi, la bande passante est économisée. De plus, plusieurs points d'accès peuvent être reliés ensemble (par câble ou par wifi relais) pour augmenter la portée du réseau Wifi. Ce mode est le plus utilisé car il est bien plus fiable.

***Infrastructure réseau***

L'établissement d'une structure wifi nécessite au minimum :

* Un routeur wifi ou un point d'accès (nécessaires uniquement pour le mode infrastructure).
* Une ou plusieurs cartes wifi (se branchent généralement sur un port USB, PCI, PCMCIA ou adaptateurs Ethernet / Wifi ).

Ce matériel correspond à une norme. Actuellement, la plus *courante* est la **802.11g** (54 Mbps de débit) mais les cartes ou routeurs **802.11b** (11Mbps) sont compatibles avec du matériel plus récent.

Il existe aussi la norme **802.11g+**, qui fonctionne à une vitesse de 108 Mbps.

***Les risques en matière de sécurité***

**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.

**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.

le réseau sans fil peut représenter une aubaine pour le pirate dans le but de mener des attaques sur Internet (il n'y a aucun moyen d'identifier le pirate sur le réseau, l'entreprise risque d'être tenue responsable de l'attaque).

**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.

**Les dénis de service**

La méthode d'accès au réseau de la norme 802.11 consiste 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.

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.

**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.

**Le danger des postes nomades**

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...).

***La sécurisation d’un réseau WiFi***

**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.

**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.

**Le filtrage des adresses MAC**

Chaque adaptateur réseau possède une adresse physique qui lui est propre.

Les points d'accès permettent généralement de gérer une liste de droits d'accès 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.

***WEP - Wired Equivalent Privacy***

**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.

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.

**La clé WEP**

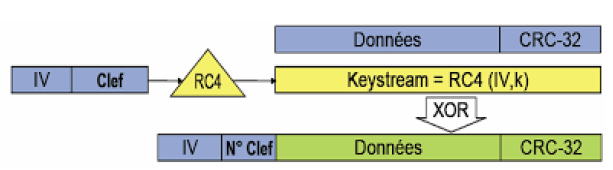
La clé de session partagé par toutes les stations est statique, c'est-à-dire que pour déployer un grand nombre de stations WiFi il est nécessaire de les configurer en utilisant la même clé de session.

Ainsi la connaissance de la clé est suffisante pour déchiffrer les communications. De plus, 24 bits de la clé servent uniquement pour l'initialisation (le nombre IV), 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.

**Le principe du WEP**

Le 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.



***Le 802.1X***

* La norme IEEE 802.1X 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).
* EAP permet de transporter divers protocoles d'authentification tel que: TLS, PEAP,TTLS.

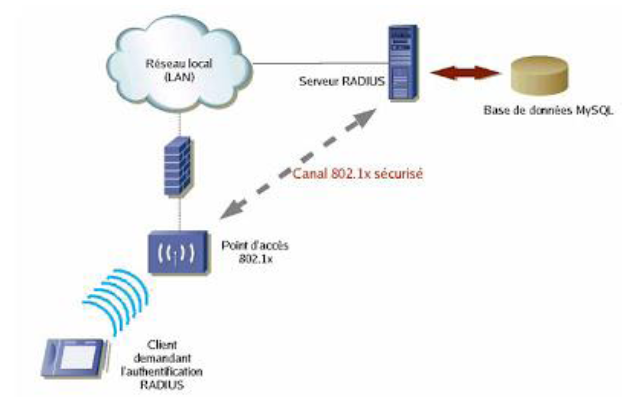
L'utilisation de l'authentification 802.1X avec le chiffrement WEP permet de pallier certains des ses problèmes tel qu'il est défini dans 802.11:

* 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.

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.

* Le principe de l'authentification 802.1X consiste à relier les trames EAP entre le poste client et le 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.



***WPA (wifi protected access)***

* Le WPA est une version « allégée » du protocole 802.11i, reposant sur des protocoles d'authentification et un algorithme de cryptage robuste : **TKIP** (*Temporary Key Integrity Protocol*).
* Le protocole TKIP permet la génération aléatoire de clés et offre la possibilité de modifier la clé de chiffrement plusieurs fois par secondes, pour plus de sécurité.
* WPA 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 ne soit recyclé.
* WPA est supérieur dans sa méthode de connexion lorsque des utilisateurs sont connectés, ils sont authentifiés par des clefs pré-partagées (authentification RADIUS).
* Sur la transmission de chaque paquet, WPA ajoute un code de vérification d'intégrité de 4 bit (ICV) afin de les vérifier. On peut donc en conclure que l'utilisation de WPA est renforcée par rapport à la vérification WEP.

***WPA2***

* La dernière évolution, est la ratification de la norme IEEE 802.11i (aussi appelé WPA2). 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 (Advanced Encryption Standard). Les protocoles de chiffrement WEP et TKIP sont toujours présents.

***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).
* Une solution consiste à utiliser le réseau WiFi comme support de transmission en utilisant un protocole d'encapsulation (tunneling) c'est-à-dire encapsulant les données à transmettre de façon chiffrée. On parle alors de réseau privé virtuel pour désigner le réseau ainsi artificiellement créé.
* Un VPN repose sur un protocole de tunnelisation, 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.
* 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.
* La sécurité du VPN repose sur l’utilisation de certificats numériques qui sont stockés sur le disque dur ou un support amovible de l’utilisateur.
* **Les protocoles de tunnelisation**
* PPTP (Point-to-Point Tunneling Protocol) de Microsoft.
* L2F (Layer Two Forwarding) de Cisco.
* L2TP (Layer Two Tunneling Protocol) est l'aboutissement des travaux de l'IETF.