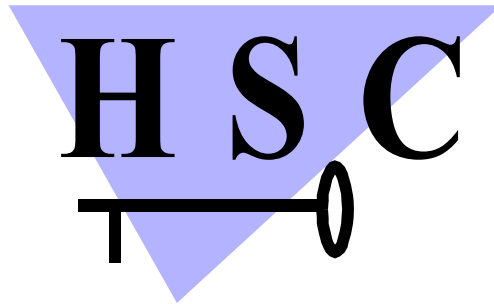


SÉCURITÉ DES RÉSEAUX SANS FIL 802.11B

par Hervé Schauer



Lundi 8 juillet 2002

HERVÉ SCHAUER CONSULTANTS

4bis, rue de la Gare - 92300 LEVALLOIS-PERRET

Tél. : +33 141 409 700 - Fax : +33 141 409 709

NAF : 741G - Siret : 351 447 537 00025

SÉCURITÉ DES RÉSEAUX SANS FIL 802.11B
HERVÉ SCHAUER
8 JUILLET 2002

Le monde sans fil fait souvent référence aux réseaux cellulaires ou par satellites. Nous analysons ici des réseaux sans fil de type réseaux locaux, indiqués en rouge dans la figure ci-dessous :

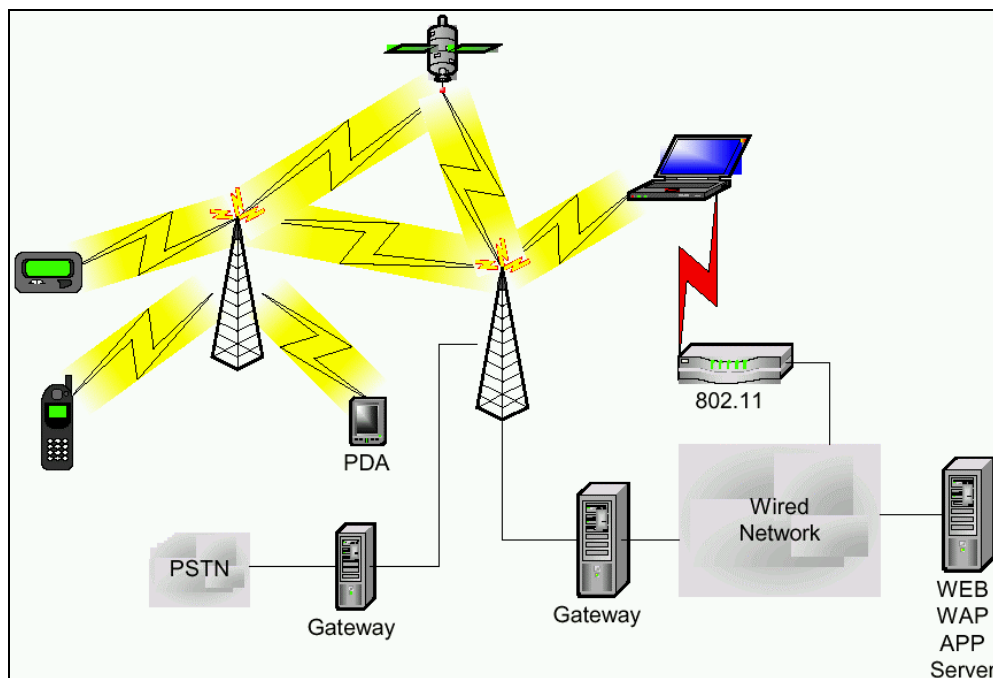


Figure 1 : [general.gif]

Le succès des réseaux locaux sans fil s'explique facilement par leur facilité de déploiement, associée à des coûts faibles : pas de frais de câblage, ce qui est souvent un atout, notamment dans les immeubles anciens.

Un réseau sans fil se déploie très rapidement, sans aucune démarche auprès d'un service précis de l'entreprise, ce qui le rend idéal pour des réseaux de tests ou des réseaux temporaires. Les réseaux sans fil permettent également de répondre aux besoins de mobilité entre les bureaux, les salles de réunions et le laboratoire, ou bien pour des chariots élévateurs dans les entrepôts et les usines. Les réseaux sans fil permettent également de répondre à la problématique de grands sites où le câblage est trop coûteux : campus, usines, etc. Ils permettent enfin des liaisons au travers des rues ou des voies ferrées.

Réseaux locaux sans fil (WLAN)

Les réseaux locaux sans fil (WLAN) existants, équivalents d'Ethernet IEEE 802.3, sont les normes IEEE 802.11b et 802.1a. La norme IEEE 802.11b s'appelle commercialement WiFi. Elle utilise la bande des 2,4 GHz et permet un débit de 11 Mb/s.

La norme IEEE 802.11a, appelée WiFi5, sur la bande des 5 GHz, permet un débit de 54 Mb/s.

Il existe également de nombreuses technologies propriétaires utilisant la bande des 2,4 GHz, concurrentes aux normes IEEE mais abandonnées car supplantées par 802.11, comme Home RF d'Intel ou OpenAir. Cependant, une autre norme, IEEE 802.15.3 reprend des caractéristiques de la technologie Home RF. Il existe également des applications spécifiques qui souhaitent éviter l'utilisation d'une norme. Si Alcatel utilise IEEE 802.11b pour le métro de Paris, Siemens Transports (ex Matra Transports) utilise une technologie propriétaire sur la bande des 2,4 GHz pour le métro de New York.

IEEE 802.11b (WiFi) est la principale technologie. Elle est disponible depuis 1997.

La bande de fréquence des 2,4 GHz est d'usage libre sans licence dans le monde entier.

La France où cette technologie n'a été autorisée qu'en 2001, est le seul pays qui fait exception depuis que le Japon a libéré les 14 canaux. La France poursuit une politique isolationniste avec une législation spécifique, qui limite le nombre de canaux autorisés et la puissance en sortie d'antenne en différenciant l'intérieur et l'extérieur des bâtiments.

Dans le reste du monde, IEEE 802.11b est utilisé en plus des réseaux privés pour des accès à l'Internet. HSC s'en est servi dans des aéroports et hôtels aux États-Unis et dans le train au Japon.

Le débit de 802.11b est de 11 Mb/s. Cependant, des cartes propriétaires 3Com disponibles depuis début 2002 autorisent 22 Mb/s.

IEEE 802.11a (WiFi5) est la technologie la plus récente, apparue fin 2001 aux États-Unis. Elle utilise une autre bande de fréquence, 5 GHz, qui est également d'usage libre dans le monde entier. À certains endroits, cette fréquence a l'avantage d'être beaucoup moins utilisée que 2,4 GHz. Le débit autorisé par 802.11a est de 54 Mb/s. Les fournisseurs sont, par exemple, Airaya, Cisco, Enterasys et Proxim. En 2002, ces équipements demeurent encore coûteux comparativement aux équipements 802.11b.

Dans le futur, les normes en cours d'élaboration IEEE 802.11g et IEEE 802.11e remplaceront IEEE 802.11b et IEEE 802.11a. Celles-ci ne sont pas encore disponibles sur le marché, même si 802.11g est annoncé pour fin 2002. Il sera possible de faire une mise à jour logicielle de 802.11b vers la version de base de 802.11g, et de faire une mise à jour matérielle dans un équipement existant en ajoutant une carte 802.11g ou 802.11e.

Le futur apportera également la qualité de service, définie dans IEEE 802.11f, et la gestion dynamique de la puissance et des fréquences normalisées dans IEEE 802.11h.

Une norme européenne concurrente de IEEE 802.11a et IEEE 802.11^e, incluant d'origine la qualité de service et la gestion dynamique des fréquences, est Hiperlan 2, défini par l'ETSI, qui utilise également sur la bande des 5 GHz. Sa disponibilité sur le marché est prévue fin 2003, mais il semble difficile de prévoir un avenir à la normalisation de l'ETSI dans ce domaine car celle-ci n'est pas soutenue par les industriels.

Réseaux personnels sans fil (WPAN)

Les réseaux personnels sans fil (WPAN) sont connus sous le nom Bluetooth, qui est devenu la norme IEEE 802.15.1. Bluetooth est sur 2,4 GHz comme WiFi. Il est intégré en standard dans Windows XP et disponible depuis début 2001 en carte PCMCIA mais son usage a été jusqu'à présent plus orienté vers l'audio.

Le futur des réseaux personnels se découpe en deux directions :

- d'une part, IEEE 802.15.3, appelé Bluetooth 2, qui évoluera vers des débits similaires aux réseaux locaux sans fil,
- d'autre part, IEEE 802.15.4, appelé Zigbee, qui évoluera vers une consommation électrique encore plus faible, avec un coût du composant inférieur à un euro. Cela permettra, par exemple, une intégration dans les jouets.

IEEE 802.15.3 (Bluetooth 2), proposera à partir de 2003 des débits de 11 Mb/s, 22 Mb/s, 33 Mb/s, 44 Mb/s et 55 Mb/s, avec des notions de sécurité de groupe, élection automatique d'un chef de groupe, authentification mutuelle, gestion de clefs et confidentialité. Il s'inspire de système propriétaire HomeRF d'Intel.

IEEE 802.15.4 (Zigbee) n'aura que des débits de 20 et 250 Kb/s. Sa normalisation a été faite en 2001. Sa disponibilité est donc prévue en 2003: il sera le réseau sans fil le plus répandu, notamment dans tous les équipements de la maison. Dans ces évolutions, la fréquence reste la bande des 2,4 GHz.

Il existe également les bus série sans fil (WSB), avec IEEE 802.15.1 (Bluetooth), qui s'apparente aux liaisons infrarouges, mais aussi IEEE 1394 (FireWire ou i.Link). Le bus IEEE 1394 peut être émulé sur 802.11 et une version sans fil a fait l'objet de nombreuses démonstrations de salons, à très au débit, notamment par les fabricants de téléviseurs, sans qu'une date de disponibilité sur le marché puisse être entrevue.

Réseaux métropolitains (WMAN)

Actuellement, les réseaux métropolitains (WMAN) sont connus pour la boucle locale radio (BLR), qui permet 2 Mb/s en utilisant des technologies propriétaires comme PMP/MMDS ou LMDS sur des bandes de fréquences soumises à licence.

Il est cependant possible d'utiliser également IEEE 802.11b et 802.11a, et le futur est sans doute pour IEEE 802.16. Sur les fréquences soumises à licence, il existe déjà des équipements depuis fin 2001, basés sur le draft en cours d'IEEE 802.16a, permettant 32 Mb/s à 134 Mb/s sur la bande de 3,5 GHz, par exemple chez Alvarion (ex-Breezecom) et Runcom.

Ce qui devrait attirer l'attention est IEEE 802.16b ou WHUMAN, qui permet des réseaux métropolitains, avec gestion de bande passante et des émetteurs entre eux, sur la bande des 5 GHz, donc sans licence. Ceci pourrait arriver en 2004 et être un concurrent de l'UMTS dans les zones à forte densité de population.

Réseaux cellulaires (WWAN)

Il existe de nombreux réseaux cellulaires (WWAN), comme Rubis de la gendarmerie, qui a été un précurseur des réseaux numériques. Ces techniques ont évolué pour donner la norme Tetra, qui permet un usage par un opérateur, ou marcher en autonome multipoints sur des fréquences variées : 380 MHz, 410 MHz et 800 MHz, avec des fonctions évoluées comme la diffusion. Cependant, la transmission de données n'est qu'à 9,6 Kb/s.

Le CDPD sur 800 MHz est utilisé par Palm.net aux États-Unis par les assistants personnels compatible PalmOS. Le débit est de 19,2 Kb/s.

Le GSM avec GPRS et les systèmes propriétaires japonais permettent 56 Kb/s.

L'avenir nous promet 384 Kb/s avec UMTS en 2004 mais la date réelle de déploiement sur le marché pourrait être retardée. Toutes ces technologies cellulaires supportent IP.

Synthèse des principales technologies en réseau local

Catégorie	WSB et WPAN	WLAN	WLAN
Nom commercial	Bluetooth www.bluetooth.com	WiFi www.wirelessethernet.org	Wifi5
Norme	IEEE 802.15.1 www.ieee802.org/15	IEEE 802.11b www.ieee802.org/11	IEEE 802.11a
Consommation électrique	très faible	forte	forte
Débit type	0.2 Mb/s	11 Mb/s	54 Mb/s
Distance type	10 m	100 m	100 m
Bande de fréquence	2,4 GHz	2,4 GHz	5 GHz
Topologie type	Point à point	Multipoints	Multipoints
Protocole principal	Audio et L2CAP	IP	IP
Support d'IP	PPP Émulation Ethernet IP over Bluetooth	natif	natif

Problématique de la sécurité

La problématique de la sécurité sur ces différents réseaux est variée.

Vis-à-vis des deux types d'attaque basiques : le déni de service et l'intrusion sur IP, les différents types de réseaux ont une réaction variable.

En réseau local sans fil avec IEEE 802.11 (WiFi), le support d'IP est natif : une interface active suffit donc généralement pour être attaqué. La connexion est permanente : un ordinateur portable avec une carte restée allumée peut sans problème être attaqué par une autre machine qui peut, si nécessaire, se faire passer pour une borne. Ainsi, une intrusion au niveau IP est un risque permanent avec une interface de réseau local allumée.

En réseau personnel IEEE 802.15 (Bluetooth), le support d'IP est natif sur Windows XP mais pas sur les autres systèmes, où il faut généralement configurer volontairement une émulation Ethernet ou une PPP sur l'émulation de la liaison série. Dans beaucoup de cas, il semble qu'une carte allumée ne suffise généralement pas pour être attaqué au niveau du système d'exploitation. Si la connexion est permanente en émulation Ethernet mais pas si une session PPP est utilisée.

Intrusion sur IP

Sur un ordinateur utilisant une liaison IP sur GPRS, il faut généralement configurer volontairement son PPP. Une carte mixte permettant l'itinérance GSM/GPRS et IEEE 802.11b supportera IP de manière native vis-à-vis des applications, mais dans le cas général, les risques sont identiques à toute connexion Internet temporaire comme avec un autre type de modem. Les opérateurs proposent des tunnels privés IP sur GPRS, permettant uniquement un accès au réseau privé de l'entreprise à la place d'un accès Internet. Ceci peut éviter d'être obligé de refabriquer un tunnel chiffré et d'avoir un garde-barrière (*firewall*) personnel sur son ordinateur.

Déni de service sur la batterie

IEEE 802.15 (Bluetooth) est délibérément conçu pour fonctionner avec une faible consommation d'énergie. Généralement, le composant Bluetooth utilise la batterie de l'équipement hôte. En conséquence, la principale attaque est le déni de service sur la batterie de l'équipement, en provoquant par exemple, des tentatives de connexion avec des calculs cryptographiques inutiles sur l'interface Bluetooth.

IEEE 802.11 (WiFi) consomme beaucoup d'énergie : aussi, sur les assistants personnels, il faudra même utiliser une batterie propre à la carte 802.11b. Sur un mobile GSM/GPRS, la consommation est supérieure à celle de l'usage du téléphone à la voix lors de l'usage de la transmission de données, mais dans les deux cas, je n'ai pas vu jusqu'à présent d'attaque sur la batterie.

Principes dans un réseau local sans fil

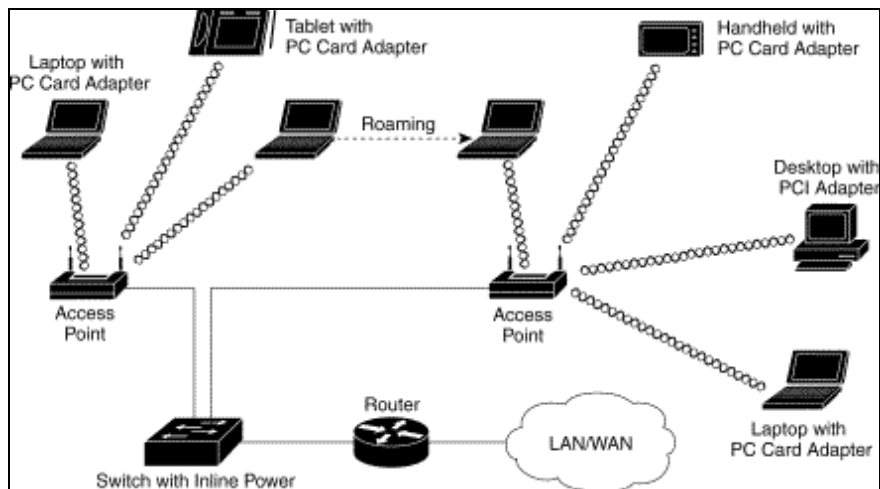


Figure 2 : [54973.gif]

Un réseau sans fil 802.11b est composé de bornes ou point d'accès (AP : *Access Points*) et de clients. La borne agit comme un pont entre un réseau filaire et un réseau sans fil, mais peut aussi être vue comme un concentrateur sans fil, et beaucoup de bornes sans fil possèdent aussi des fonctions de routage et de sécurité avec du filtrage IP. Les clients sont les cartes réseau (NIC : *Network Interface Card*), c'est-à-dire l'interface Ethernet sur l'équipement.

La fonctionnement par défaut est lorsque les interfaces Ethernet des clients dialoguent avec les bornes. Ce mode s'appelle "*infrastructure*". Il propose une topologie multipoints. Il est possible d'avoir un dialogue direct entre deux interfaces Ethernet sans fil, c'est le mode "*ad-hoc*", en topologie point à point. Il est également possible pour une machine munie d'une carte Ethernet de se transformer en borne.

Chaque réseau est identifié par un SSID : identificateur du réseau, qui est configuré dans les bornes, et éventuellement dans les clients, et envoyé dans les trames.

Plusieurs réseaux avec des SSID différents peuvent cohabiter au même endroit. La bande de fréquence des 2,4 GHz possède 14 canaux. Un même réseau utilisera plusieurs réseaux pour couvrir correctement un large espace avec plusieurs bornes. À l'inverse, plusieurs réseaux peuvent cohabiter au même endroit, même sur le même canal.

Ces caractéristiques apportent plusieurs considérations vis-à-vis des dénis de service. Dans un même endroit, il faut que les réseaux multipoints (mode *architecture*) et point à points (mode *ad-hoc*) utilisent des SSID différents. Si une machine a sa carte en mode *ad-hoc* avec le même SSID que le réseau officiel des bornes, elle va perturber le bon fonctionnement du réseau et provoquer un déni de service pour ses voisins. Une attaque plus violente permettant de s'attirer le trafic est une machine se transformant en borne. Elle peut s'attirer le trafic par sa puissance ou par une attaque ARP, et, au-delà du déni de service, bâtir des attaques de l'intercepteur en renvoyant le trafic capturé sur la véritable borne.

Au niveau Ethernet, la vision des réseaux sans fil est similaire à celle des réseaux filaires. Elle est identique pour les ordinateurs et pour TCP/IP. Ethernet filaire 802.3 utilise CSMA/CD et détecte les collisions, alors qu'Ethernet sans fil 802.11 utilise CSMA/CA qui prévient les collisions. L'adressage MAC est identique, sauf que dans 802.11 il y a les adresses des bornes en plus, ce qui donne quatre adresses MAC au lieu de deux dans la trame.

802.11b a ajouté une fonction nouvelle WEP (*Wired Equivalent Privacy*), qui permet en théorie d'assimiler un réseau Ethernet sans fil à un réseau Ethernet filaire, en assurant une sécurité équivalente à celle d'un câble. Malheureusement le WEP de première génération n'a pas rempli son objectif.

Problèmes avec les réseaux sans fil

Les réseaux sans fil posent de nombreux problèmes de sécurité. Beaucoup de leurs caractéristiques ouvrent des vulnérabilités : les propriétés du média, la liberté topologique, les caractéristiques de la technologie, celles des implémentations, la fonctionnalité des équipements et la manière de positionner les bornes dans l'architecture des réseaux de l'entreprise.

Le média se compose d'ondes radioélectriques : c'est donc par construction, un support sans protection vis-à-vis des signaux externes, donc sensible au brouillage et au déni de service. Les caractéristiques de propagation des ondes sont complexes, dynamiques et difficiles à prévoir, avec beaucoup de phénomènes : absorption, diffraction, réfraction, réflexion, en fonction de l'humidité, du verre, du béton, du démarrage d'un moteur, d'un four à micro-ondes, etc. Il est donc très difficile d'envisager une limite absolue au réseau, et sa frontière n'est pas observable. Les écoutes et interceptions sont donc aisées : il sera même possible d'insérer du trafic illégal et de s'introduire malicieusement dans le réseau.

Liberté topologique

La topologie d'un réseau sans fil est dynamique. Les clients peuvent choisir entre les modes *ad-hoc* et *infrastructure*. En mode *infrastructure*, ils peuvent choisir leurs bornes, et, s'ils sont mobiles, ils s'en servent pour l'itinérance. Il est également possible d'utiliser des liaisons sans fil entre bornes pour l'architecture du réseau lui-même, où la borne agit en pont entre deux réseaux sans fil (voir figure 3). Certaines cartes et bornes peuvent dialoguer avec plusieurs autres cartes ou bornes à la fois. Exemple de la topologie utilisée lors d'une conférence :

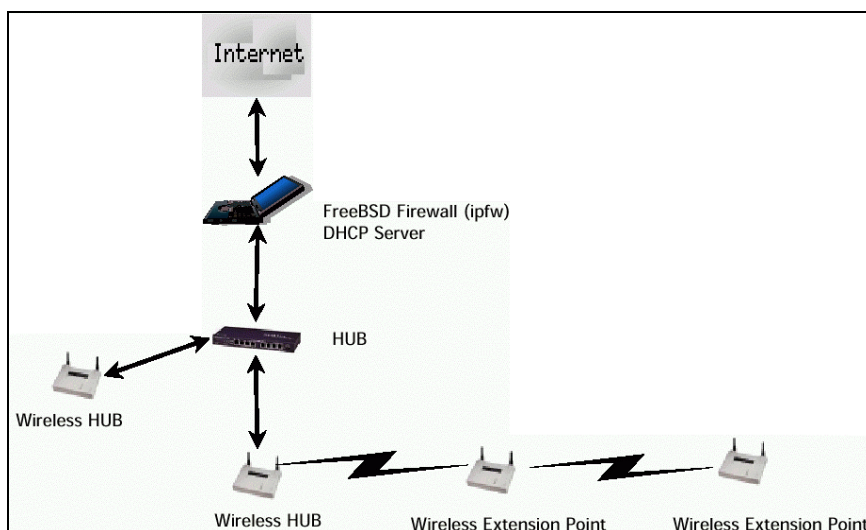


Figure 3 : [usenix.gif]

Caractéristiques de la technologie

Une borne peut être placée n'importe où, là où se trouvent le courant électrique et une connexion filaire. Cette absence de contraintes amène souvent à ne pas analyser le placement des bornes par rapport à la zone qui mérite d'être couverte. Les utilisateurs et les intégrateurs ne savent pas comment se propagent les ondes à partir des antennes, ni même comment les antennes sont orientées dans leur borne. En conséquence, il est courant de trouver des bornes mal placées et mal orientées, couvrant parfois mieux les étages des voisins que l'étage où se trouve l'entreprise.

Le protocole 802.11b envoie en permanence des paquets de contrôle (*beacon*). Cela permet de toujours détecter un réseau sans fil. Due à l'interface *air*, une borne sans fil ne peut agir comme un commutateur (*switch*) où le destinataire ne reçoit que les paquets lui étant destinés. Elle est comme un concentrateur (*hub*) qui diffuse toutes les trames à tous les clients. Chaque carte Ethernet sans fil reçoit le trafic de toutes les bornes sur le canal qu'elle utilise, et certaines cartes peuvent écouter sur les 14 canaux en même temps. Il est donc aisé d'écouter le trafic sans fil.

Le principe de déploiement simple impose un fonctionnement le plus automatique possible, avec une configuration minimale. IEEE 802.11b utilise donc le protocole STP (*Spanning Tree Protocol*, IEEE 802.1d) pour gérer automatiquement plusieurs bornes et commutateurs. Il est possible de transformer un PC sous Linux en borne (voir opensource.instant802.com ou people.ssh.com/jkm/Prism2/), et donc, potentiellement effectuer des manipulation malveillantes au niveau 2.

Le protocole WEP chiffre le trafic, pour apporter une confidentialité similaire à une Ethernet filaire. Dans sa première génération, le protocole WEP n'intègre pas de mécanisme de distribution des clefs, alors que les clefs de chiffrement sont indispensables à son utilisation.

Cette génération largement utilisée, impose actuellement une organisation pour distribuer et configurer manuellement la clef sur chaque client, ce qui rend l'usage du WEP très difficile à gérer, et implique donc un faible usage du chiffrement de la part des utilisateurs. Les écoutes réalisées dans les grandes villes révèlent de 10 à 75% des réseaux avec chiffrement, suivant si l'on se trouve dans des quartiers d'affaires de grandes entreprises ou de zones résidentielles.

Même avec WEP, les trames de gestion et celles contenant le SSID ne sont pas chiffrées par la spécification du protocole. Il sera ainsi aisé de développer beaucoup d'attaques ne serait-ce que sur les trames de gestion.

Caractéristiques des implémentations

Les identificateurs de réseau et des clefs de chiffrement sont généralement stockés dans un fichier sur le disque de la machine ou sur Windows dans la base de registres en *Lecture pour Tous* comme avec Agere, ou, plus rarement, sur la carte elle-même comme chez Cisco. Le vol de l'ordinateur ou de la carte sans fil, entraîne alors le risque du vol de la clef.

Fonctionnalités des équipements

Les équipements bon marché et faciles à mettre en œuvre, ont multiplié les déploiements 'sauvages' de réseaux 802.11b, par des utilisateurs souvent inconscients des risques. Ils ne préviennent ni ne consultent les services informatiques ou réseaux de l'entreprise. Les bornes sont mises en œuvre par défaut, sans sécurité, et ouvrent le réseaux interne, privé, sur l'extérieur sans sécurité : manque de SSID ou SSID indiquant de quel réseau il s'agit, pas de mise en œuvre du chiffrement (WEP), communauté SNMP par défaut, et administration de la borne par une interface web ouverte à tous et accessible depuis le réseau sans fil.

Positionnement dans l'architecture

Même lorsque les bornes sont sciemment déployées par le service réseau au sein du périmètre interne du réseau d'entreprise, elles sont mises trop souvent directement sur le réseau privé, sans filtrage, avec une puissance d'émission réglée au maximum, et parfois sans authentification des utilisateurs.

Attaques

Les attaques contre les réseaux sans fil sont simples : un attaquant, éventuellement positionné à l'extérieur du périmètre physique de l'entreprise comme le parking, se connecte au réseau.

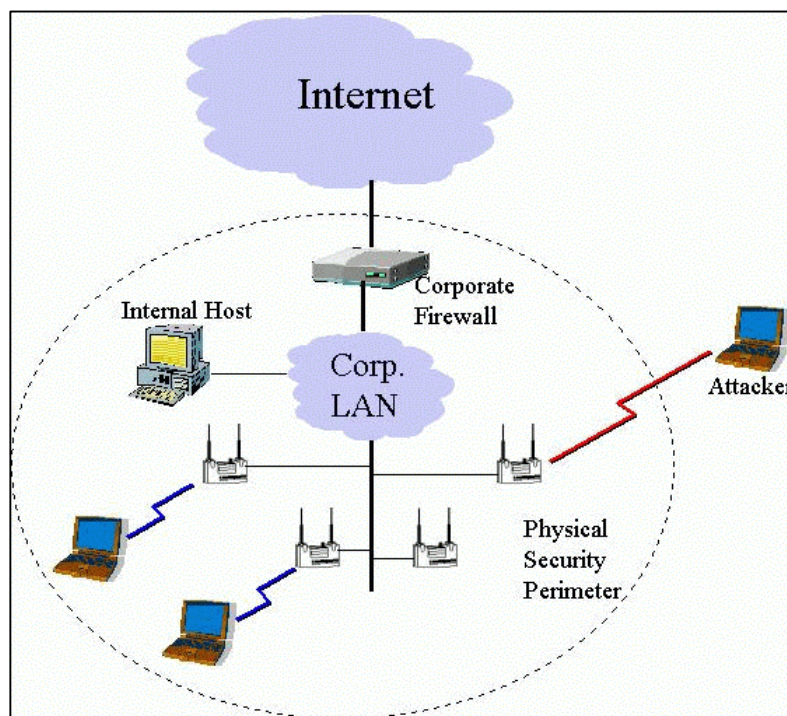


Figure 4 : [parking.gif]

Il est ainsi possible de s'introduire dans le réseau, de pirater les serveurs et même d'y ajouter un faux serveur.

Le "*War Driving*" ou quadrillage d'une ville avec un ordinateur portable, une carte 802.11b munie d'une antenne externe et un récepteur GPS pour la localisation est devenu un sport à la mode. Nous verrons dans l'audit que de nombreux logiciels sont disponibles pour détecter les réseaux sans fil.

Les solutions se décomposent en quatre grands principes :

- 1) S'organiser pour gérer correctement ses réseaux sans fil
- 2) Auditer et surveiller les réseaux sans fil
- 3) Authentifier les utilisateurs de réseaux sans fil
- 4) Architecturer correctement ses réseaux sans fil.

1) S'organiser pour gérer correctement ses réseaux sans fil

Dans une grande organisation, la sécurité à tout intérêt à être découpée entre le service du RSSI et le service sécurité production ou SOC (*Security Operation Center*). Le service du RSSI sera rattaché à une direction générale pour définir une politique de sécurité adaptée aux besoins, aux métiers et aux objectifs de l'entreprise.

Le service sécurité production ou SOC sera quant à lui, au sein de la direction informatique, comme le service informatique qui gère les serveurs centraux, ou le service bureautique qui gère les PC et les serveurs bureautiques.

Un service de production sécurité ou SOC gère, d'une part les composants du système d'information dont l'objectif principal est la sécurité, et d'autre part, apporte la vision globale de la sécurité sur l'ensemble du système d'information. Ces fonctions centralisées sont notamment l'analyse et la corrélation de la journalisation et la détection d'intrusion.

Les composants dont l'objectif principal est la sécurité sont avant tout l'ensemble des moyens d'interconnexion avec l'extérieur, ce qui se trouve sur le périmètre de l'entreprise : accès Internet, VPN pour accès distants, extranets, plate-forme de commerce électronique. Ces équipements seront gérés de manière opérationnelle par un service dédié orienté sécurité. Cela sera aussi le cas de l'authentification des utilisateurs, par exemple dans le cadre des accès distants ou des accès Internet.

Dans les PME-PMI, la fonction informatique est déjà très limitée : la sécurité informatique sera sous la responsabilité d'un directeur sans connaissance du sujet comme le PDG ou le directeur financier. Les fournisseurs de services et les intégrateurs ont alors une lourde responsabilité de conseil pour éviter que les PME-PMI soient les principales victimes des risques apportés par les réseaux sans fil. Celles-ci n'auront pas de moyens d'exploitation appropriés des composants de sécurité.

Dans des organismes distribués comme certaines organisations publiques, l'aspect RSSI n'existera que de manière centralisée, et chaque entité comme les laboratoires du CNRS, auront à leur charge l'exploitation des équipements de sécurité : souvent la même personne aura donc des responsabilités très variées et elle devra être sensibilisée aux risques des réseaux sans fil.

De par la nature d'un réseau sans fil, une borne d'accès sans fil est toujours sur le périmètre du réseau. En conséquence, celle-ci doit être gérée par le SOC, comme tous les périphériques situés sur le périmètre du réseau. L'authentification des utilisateurs nomades en accès distant sera ainsi réutilisable pour les accès sans fil. La gestion des réseaux sans fil réussit quand elle est réalisée par une équipe formée et compétente en sécurité.

Des exceptions sont possibles : par exemple dans le cas de bornes utilisées uniquement pour construire des liens point à point entre des réseaux distants, et configurées pour n'accepter aucune connexion cliente.

Mais la gestion des bornes sans fil par une équipe formée et dédiée à la sécurité est un facteur de l'intégration des réseaux sans fil en toute sécurité dans un grand réseau.

Rôle du RSSI

Le RSSI doit ajouter les réseaux sans fil dans la sensibilisation des utilisateurs à la sécurité, pour leur expliquer le danger des réseaux sans fil, jusqu'à ce qu'ils reportent au service sécurité comme incident, toute connexion sans fil réalisée sans authentification. Il doit ajouter les audits de recherche de réseaux aux audits sur son périmètre, même si le service réseau est persuadé que les réseaux sans fil ne sont pas utilisés chez lui. De manière générale, il doit intégrer les problématiques des réseaux sans fil dans sa politique de sécurité et ses procédures. À noter que l'ISO17799 ignore l'existence des réseaux sans fil.

Utiliser la sécurité des bornes

Les bornes possèdent de nombreuses fonctions permettant d'éviter une intrusion trop facile, cependant, ces fonctions ne sont pas activées par défaut. Pour l'administration de la borne elle-même, il faut choisir des mots de passe de qualité, en désactivant tous les services d'administration (Interface Web, SNMP, TFTP) sur l'interface sans fil, et en gérant et supervisant des bornes uniquement par l'interface filaire. Il faut choisir un SSID approprié, sans lien avec le réseau ou l'entreprise, et supprimer la diffusion du SSID par défaut. Ainsi le SSID du client doit correspondre à celui de la borne pour s'associer. Ce n'est pas une sécurité absolue et au travers d'autres clients, un intrus pourra toujours retrouver le SSID et s'associer, mais, combiné avec le WEP, cela constitue une barrière forte vis-à-vis de certains logiciels d'écoute disponibles sur Internet et qui ne fonctionneront plus. Il faut configurer la clef WEP même si dans un premier temps, celle-ci est statique, et la configurer sur les clients en utilisant le WEP 128 bits et non le WEP 40 bits.

La borne permet aussi un filtrage par adresse MAC (adresse Ethernet) : ainsi, seules les cartes enregistrées sont autorisées à utiliser le réseau. La gestion quotidienne de cette fonctionnalité sera lourde si les clients changent souvent, notamment lorsque l'on ne dispose pas de logiciel de gestion centralisée de toutes ses bornes, mais c'est une très bonne barrière. L'adresse MAC figure cependant en clair dans toutes les trames : même si WEP est employé, un intrus peut repérer les adresses MAC valides en écoutant le trafic, puis générer de trames falsifiées avec une adresse MAC valide.

Enfin il faut mettre à jour le logiciel de la borne (*firmware*) régulièrement car chaque nouvelle version chez la plupart des constructeurs, apporte des fonctionnalités de sécurité supplémentaires et corrige les erreurs de la version précédente. Certaines bornes ont connu des failles graves, comme la diffusion de la communauté SNMP sur réception d'une trame formée de manière appropriée sur les Compaq WL310. Avec l'accès SNMP, l'intrus peut obtenir ensuite la clef WEP en clair, s'il a accès à l'interface filaire.

Mécanisme de sécurité de 802.11b : WEP

Le WEP (*Wired Equivalent Privacy*) de première génération équipe la grande majorité des équipements actuels. La clef secrète partagée est statique et tous les clients doivent posséder la même clef. Les clefs sont configurées et déployées manuellement et rarement changées.

Ce WEP de première génération a fait l'objet de beaucoup d'attaques relayées par les médias. Début 2001, l'attaque par dictionnaire contre la clef de chiffrement a mis en relief le fait qu'une clef est un mot de passe partagé potentiellement faible (www.lava.net/~newsham/wlan).

En février 2001, l'université de Berkeley a publié une attaque contre le WEP statique : (www.isaac.cs.berkeley.edu/isaac/wep-faq.html).

En avril 2001, l'université du Maryland s'est attaqué à l'authentification en relevant une faille dans le schéma d'authentification 802.1X d'un des principaux constructeurs : (www.missl.cs.umd.edu/Projects/wireless/infrastructure.shtml).

Enfin en juillet 2001, Fluhrer, Mantin et Shamir ont publié une attaque pragmatique contre le vecteur d'initialisation de RC4 tel que spécifié dans WEP : "*Weaknesses in the Key Scheduling Algorithm of RC4*". Celle-ci a rapidement été implémentée et est disponible sur Internet, et son aspect cryptographie comme ses auteurs; lui ont donné une fort retentissement, alors que sa mise en œuvre n'est pas si facile. Il n'en demeure pas moins que cela a montré que les normes devaient être, d'une part très précises dans leur description, jusqu'à imposer des principes d'implémentation, et que d'autre part, ces normes devaient être relues par des spécialistes en sécurité. Lorsque les normes IEEE 802.11 ont été écrites, personne ne s'y intéressait et personne n'avait accepté de les relire. Une fois que le 802.11 a connu le succès que nous connaissons, beaucoup d'universitaires se sont alors penchés sur le sujet pour y trouver la célébrité en y détectant des faiblesses. Il faudrait aussi s'attaquer à ce processus pour l'inverser...

Beaucoup de logiciels de mise en œuvre des attaques sur le WEP de première génération sont désormais disponibles : WEPCrack (wepcrack.sourceforge.net), Airsnort (airsnort.sourceforge.net), PrismSnort, etc. La configuration la plus courante est : un ordinateur portable sous Linux, une carte Ethernet sans fil équipée du chipset 'Prism II'. Avec 100 Mo à 1 Go de données capturées, il faut selon la publicité, quelques secondes de calcul pour déchiffrer la clef. Mais la publicité 'oublie' de préciser que, pour avoir une telle masse de données, il faut générer du trafic soi-même avec la borne et donc être particulièrement intrusif.

Le WEP première génération ne répond plus à son objectif mais il faut le mettre en œuvre.

Le niveau de sécurité de son réseau sans fil change complètement avec le WEP : les attaques sont ralenties, plus complexes, et imposent à l'attaquant de prendre plus de risques en laissant plus de traces lors de son attaque. Le WEP est vraiment la brique de base qui, combinée avec d'autres, permettra de déployer la sécurité sur les réseaux sans fil.

À court terme, le WEP n'est généralement pas suffisant : il sera complété par d'autres mécanismes de sécurité comme un tunnel chiffré dans les couches supérieures.

Surveillance

Compte tenu des risques qu'apportent les réseaux sans fil, leur surveillance est indispensable. Cette surveillance pourra s'appliquer au travers de l'architecture du réseau et par des moyens externes. Toutes les grandes organisations dont le responsable sécurité indique "nous n'utilisons pas de réseaux sans fil", se sont toutes avérées avoir au moins un réseau sans fil quelque part, sans le savoir.

Pour la découverte des réseaux sauvages, les moyens au travers de l'infrastructure du réseau seront la découverte des bornes comme le permettent les logiciels de gestion de réseau. Cette technique de découverte peut-être limitée et ne suffira pas.

Pour les réseaux déployés par le service adéquat dans l'organisation, il est possible de mettre en place une bonne surveillance au niveau de l'infrastructure, en utilisant un commutateur en apprentissage d'adresse MAC. Une fois les bornes branchées sur le commutateur, chaque connexion de client déclenche une alarme car c'est l'adresse MAC du client qui parvient au commutateur. Au départ, le commutateur apprend les adresses. Il est ensuite facile de détecter tout intrus inconnu qui tenterait de se connecter. Cette technique ne résiste pas à l'usurpation d'une adresse MAC valide mais elle est plus simple à gérer que le filtrage des adresses MAC sur les bornes.

Les bornes possèdent également des bonnes possibilités de journalisation, soit avec leur système et leur interface propre, soit par des alarmes SNMP ou par le protocole Syslog.

Enfin, il sera possible de surveiller le trafic au niveau réseau IP classique avec des logiciels de détection d'intrusion comme la sonde Snort (www.snort.org) ou le système distribué Prelude (www.prelude-ids.org), ou, au niveau d'Ethernet sans fil, en laissant une sonde sans fil à demeure, avec des logiciels comme :

- PrismDump (www.guerrilla.net/gnet_linux_software.html),
- AirTraf (sourceforge.net/projects/airtraf),
- AirIDS (www.internetcomealive.com/clients/airids).

Recherche des réseaux 'sauvages'

Les réseaux sauvages peuvent être le fait d'employés inconscients pour des réseaux temporaires ou de tests, d'employés indéclicats pour leur usage, ou d'intrus pour renvoyer le trafic du réseau privé plus loin, hors des limites physiques du site.

Souvent, il y aura des clients 'sauvages', qui ont une interface de réseau sans fil configurée par défaut, et une interface filaire sur le réseau privé.

Une tâche indispensable est donc de vérifier s'il n'y a pas de tels réseaux 'sauvages' connectés au réseau privé de l'entreprise. La technique employée sera similaire à celle des intrus, en recherchant les interfaces *air*. Il n'existe pas encore d'outils distribués permettant par le réseau filaire, de gérer des recherches de bornes sur un ensemble de sites. Cela constitue les audits de réseaux locaux sans fil.

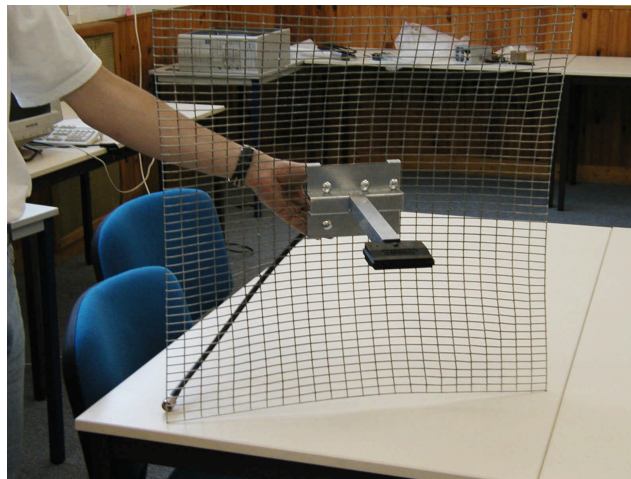
Audit de réseaux locaux sans fil

L'objectif d'un tel audit est de détecter les réseaux sans fil IEEE 802.11b sauvages et les stations mal ou auto-configurées, et d'évaluer la sécurité des réseaux sans fil.

L'auditeur parcourt le périmètre de l'audit à la recherche de réseaux avec un équipement portable, généralement un ordinateur ou un assistant personnel, avec une carte sans fil (photo 2). Il existe aussi des sondes dédiées qui sont plus coûteuses. Il est possible d'utiliser des antennes pour amplifier la réception. Une antenne omnidirectionnelle (photo 3) évite de parcourir trop de chemin ou permet un audit en cas d'humidité.

Une fois une borne détectée, il sera possible de voir le SSID, éventuellement de s'associer à celle-ci, puis de poursuivre en fonction de la nature de la prestation. Si le réseau appartient au client, une attaque sur la clef WEP, le mot de passe de la borne, et un test d'intrusion comme ceux réalisés par Internet est envisageable. Ce type de prestation demeure délicate car il faut toujours bien vérifier à qui les réseaux appartiennent préalablement à toute action.

Une antenne directionnelle (photo 1) permettra de cibler une borne à distance respectable, et ainsi, de démontrer l'accès au réseau sans fil hors du périmètre physique contrôlé par l'entreprise, par exemple un étage élevé d'une tour.



[p6250027.jpg]

Photo 1 : antenne directionnelle



[cartes-pale.png]

Photo 2 : cartes avec connexion d'antenne externe



[antenne.png]

Photo 3 : antenne omnidirectionnelle

Outils d'audit

De nombreux outils d'audit sont disponibles en logiciel libre. Le plus connu est NetStumbler (www.netstumbler.org) car il fonctionne sous Windows et propose une interface accessible à tout un chacun. Les autres logiciels disponibles sont sous Linux :

- AirTraf Linux (sourceforge.net/projects/airtraf/),
- GtkScan/PerlSkat (sourceforge.net/projects/wavelan-tools/),
- Kismet (www.kismetwireless.net/),
- PrismStumbler (prismstumbler.sourceforge.net/),
- Wardrive (www.thehackerschoice.com/).

Au départ, HSC a préféré Kismet, mais rapidement, il est devenu plus pratique d'avoir son propre outil pour pouvoir y implémenter plus facilement ses idées et besoins. Aussi, Jérôme Poggi a développé WifiScanner (photo 4), disponible sur www.hsc.fr/ressources/outils/wifiscanner/.

WifiScanner fonctionne avec les cartes basées sur le composant Prism II comme la majorité des logiciels de détection et d'écoute des réseaux sans fil. WifiScanner détecte les clients et les bornes 802.11b, écoute alternativement sur les 14 canaux en temps réel, et peut rechercher les bornes et leurs clients pour en générer la visualisation de l'architecture réseau avec GraphViz (www.graphviz.org). WifiScanner sauvegarde le trafic réseau capturé en format standard libpcap, permettant une analyse par d'autres logiciels.

```

WifiScanner v0.6.1 (14) (c) 2002 Hervé Schauer Consultants (Jérôme.Poggi@HSC.FR)
-----
BEP: 001022D10F1B0153 ** (31.34)
STA: 0010510418211314B ** (0.32)
-----
Summary
  AP: 1
  STA: 0
  BECON: 169
  SSID: 0
  Channel: 0
  Invalid: 4
  Packets: 176
-----
07/20/2002 22142157.031, " 10_Mep_AP_034_12,FFFFFFFFFFFFFFFF,0010212D10F1B0153,0010212D10F1B0153,2Mb/s,AP Base (dedicated),Radio o
nly, BECON
07/20/2002 22142157.949, " 10_Mep_AP_034_4,FFFFFFFFFFFFFFFF,0010212D10F1B0153,0010212D10F1B0153,2Mb/s,AP Base (dedicated),Radio on
ly, BECON
07/20/2002 22142158.1000, " 10_Mep_AP_032_12,FFFFFFFFFFFFFFFF,0010212D10F1B0153,0010212D10F1B0153,2Mb/s,AP Base (dedicated),Radio o
nly, BECON
07/20/2002 22142159.920, " 10_Mep_AP_033_4,FFFFFFFFFFFFFFFF,0010212D10F1B0153,0010212D10F1B0153,2Mb/s,AP Base (dedicated),Radio on
ly, BECON
07/20/2002 22143101.962, " 10_Mep_AP_030_12,FFFFFFFFFFFFFFFF,0010212D10F1B0153,0010212D10F1B0153,2Mb/s,AP Base (dedicated),Radio o
nly, BECON
07/20/2002 22143102.880, " 10_Mep_AP_030_3,FFFFFFFFFFFFFFFF,0010212D10F1B0153,0010212D10F1B0153,2Mb/s,AP Base (dedicated),Radio on
ly, BECON
07/20/2002 22143104.940, " 10_Mep_AP_032_12,FFFFFFFFFFFFFFFF,0010212D10F1B0153,0010212D10F1B0153,2Mb/s,AP Base (dedicated),Radio o
nly, BECON
07/20/2002 22143107.910, " 10_Mep_AP_032_12,FFFFFFFFFFFFFFFF,0010212D10F1B0153,0010212D10F1B0153,2Mb/s,AP Base (dedicated),Radio o
nly, BECON
07/20/2002 22143110.871, " 10_Mep_AP_028_11,FFFFFFFFFFFFFFFF,0010212D10F1B0153,0010212D10F1B0153,2Mb/s,AP Base (dedicated),Radio o
nly, BECON
07/20/2002 22143113.898, " 10_Mep_AP_028_11,FFFFFFFFFFFFFFFF,0010212D10F1B0153,0010212D10F1B0153,2Mb/s,AP Base (dedicated),Radio o
nly, BECON
07/20/2002 22143115.881, " 10_Mep_AP_027_11,FFFFFFFFFFFFFFFF,0010212D10F1B0153,0010212D10F1B0153,2Mb/s,AP Base (dedicated),Radio o
nly, BECON
07/20/2002 22143116.791, " 10_Mep_AP_028_4,FFFFFFFFFFFFFFFF,0010212D10F1B0153,0010212D10F1B0153,2Mb/s,AP Base (dedicated),Radio on
ly, BECON
07/20/2002 22143117.841, " 10_Mep_AP_030_12,FFFFFFFFFFFFFFFF,0010212D10F1B0153,0010212D10F1B0153,2Mb/s,AP Base (dedicated),Radio o
nly, BECON
07/20/2002 22143120.821, " 10_Mep_AP_030_12,FFFFFFFFFFFFFFFF,0010212D10F1B0153,0010212D10F1B0153,2Mb/s,AP Base (dedicated),Radio o
nly, BECON
07/20/2002 22143123.872, " 10_Mep_AP_030_12,FFFFFFFFFFFFFFFF,0010212D10F1B0153,0010212D10F1B0153,2Mb/s,AP Base (dedicated),Radio o
nly, BECON
07/20/2002 22143124.782, " 10_Mep_AP_031_11,FFFFFFFFFFFFFFFF,0010212D10F1B0153,0010212D10F1B0153,2Mb/s,AP Base (dedicated),Radio o
nly, BECON

```

[wifiscanner.jpg]

Photo 4 : exemple d'écran WifiScanner

3) Authentifier les utilisateurs de WLAN

Pour sécuriser les réseaux sans fil, il faut les surveiller par l'architecture et par des audits externes. Cependant, l'élément le plus important est d'authentifier les utilisateurs du réseau. Ceci peut se faire avec un portail HTTP ou avec la norme IEEE 802.1X, dont la disponibilité et l'usage se développent.

Portail HTTP

La méthode utilisable dans tous les cas et qui demeure la plus simple, est d'utiliser un portail web qui authentifie l'utilisateur. L'utilisateur est filtré au niveau TCP/IP sur un firewall derrière la borne ou sur la borne elle-même : il ne peut rien faire tant qu'il n'a pas essayé de consulter un serveur web. À ce moment là, sa première tentative de connexion en HTTP est usurpée par le portail qui se fait passer pour le site qu'il cherchait à joindre. Le portail demande alors à l'utilisateur une authentification, qui est généralement par login/mot de passe, avec un serveur d'authentification Radius derrière : mais d'autres possibilités y compris des certificats clients, sont également utilisables. Cette technique est utilisée par les fournisseurs de service d'accès à l'Internet pas réseau sans fil. Elle n'est pas spécifique aux réseaux sans fil et est disponible depuis de nombreuses années dans beaucoup d'équipements comme les routeurs Cisco. Son avantage indéniable est qu'il n'y a pas de logiciel spécifique à déployer sur le poste client, ni aucune gestion de clefs, mais les communications seront en clair, sans usage du WEP. Un logiciel libre permettant de mettre en œuvre un tel portail dans le cas des réseaux sans fil est NoCatAuth (www.nocat.net).

IEEE 802.1X

IEEE 802.1X (*Port Based Network Access Control*) est une norme développée à l'origine pour les VLAN (standards.ieee.org/getieee802/802.1.html), qui est commune à toutes les normes de niveau 2 comme 802.3 (Ethernet) ou 802.5 (Token Ring).

IEEE 802.1X définit un cadre (voir figure 5) permettant l'élaboration de mécanismes d'authentification et d'autorisation pour l'accès au réseau, et également de distribution des clefs de session, ce qui sera très utile pour le 802.11.

IEEE 802.1X utilise le protocole d'authentification EAP (*Extensible Authentication Protocol*) pour authentifier le client. EAP a été normalisé par l'IETF dans le RFC2284, mais dans le cas d'IEEE 802.1X, il sera aussi utilisé sans protocole de transport directement au-dessus du réseau local Ethernet : EAPOL (*EAP over LANs*).

Le protocole EAP est en fait lui-même un protocole générique qui permet encapsuler toute forme de méthode d'authentification : mots de passe, biométrie, cartes à puce, calculatrice, clef publique, et d'y associer les échanges spécifiques à chaque méthode d'authentification.

Le cadre IEEE 802.1X (voir figure 5) intègre quatre couches :

- Une couche infrastructure, avec les serveurs d'authentification (Radius, AAA, Kerberos) et les annuaires.
- Une couche méthodes d'authentification, où l'on pourra distinguer les méthodes basées sur des mots de passe, celles basées sur des certificats, celles utilisant des cartes ou calculatrices et les GSS-API qui sont génériques.
- Une couche protocole d'authentification où c'est toujours EAP qui est utilisé.
- Une couche média, où l'on peut avoir Ethernet 802.3 et 802.11, mais aussi, Token Ring, IEEE 802.16, PPP, etc.

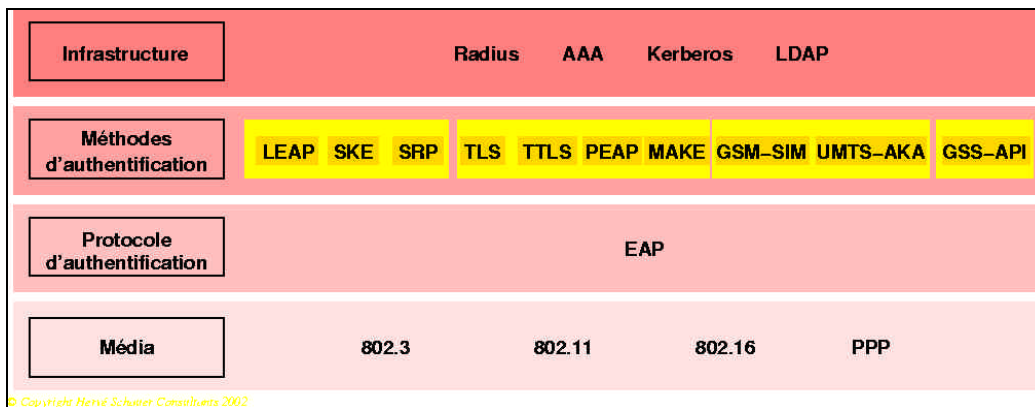


Figure 5 : cadre 802.1X [802.1X-framework.png]

L'utilisation de la norme 802.1X avec les réseaux sans fil 802.11, permettra : l'authentification de l'utilisateur depuis le poste client, le contrôle d'accès à la borne et la distribution des clefs WEP. Il faut cependant être prudent et toujours bien regarder ce qui est implémenté dans le matériel proposé, car 802.1X avec 802.11 permet beaucoup de possibilités. Chaque fabricant n'en a implémenté qu'une partie : il faut que la même chose soit implémenté sur ses postes clients, dans ses bornes et sur son serveur d'authentification pour que cela soit interopérable et fonctionne.

Sur les postes clients, les implémentations d'IEEE 802.1X sont toujours disponibles auprès des fournisseurs de bornes pour toutes les plates-formes (Windows, Mac, Unix, etc) mais il faudra installer un logiciel sur tous les postes clients devant se connecter au réseau sans fil. Petit à petit, 802.1X sera intégré en standard dans le système d'exploitation, avec de plus en plus de possibilités. Actuellement 802.1X est fourni en standard dans Windows XP et il est disponible en logiciel libre pour Linux avec Xsupplicant (www.missl.cs.umd.edu/lx).

Principe d'IEEE 802.1X

802.1X découpe les ports physiques d'un commutateur ou les ports virtuels d'une borne sans fil en deux ports logiques (voir figure 6) appelés PAE (*Port Access Entity*) : le PAE d'authentification (*Authenticator PAE*) qui est toujours ouvert, et le PAE de service ou port contrôlé, qui ne sera ouvert qu'après une authentification réussie.

Le PAE du client (*Supplicant PAE*) demande l'accès au PAE de service. Le client est bloqué par la borne mais son PAE d'authentification laisse passer les trames d'authentification EAP et les renvoie vers un serveur d'authentification. Pour ce faire, la borne traduit EAP sur Ethernet sans fil en EAP dans RADIUS sur IP.

Après l'authentification, la borne débloque le PAE du client sur le PAE de service et toutes les trames sont autorisées à passer.

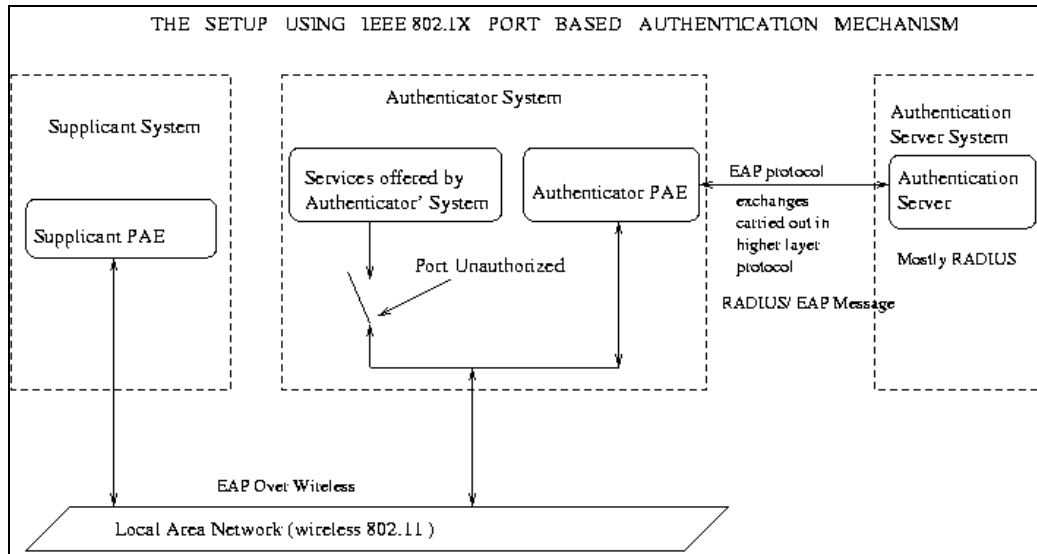


Figure 6 : Principe de 802.1X [802.1X.gif]

Protocole 802.1X dans le protocole 802.11b

```

| client | | _i_ _i_ | | serveur |
|         | | borne | --- | authentication |
EAP start --->
<--- EAP request identity
EAP identity resp ---> - - - --->
<--- - - - <--- EAP auth request
EAP auth response ---> - - - --->
<--- EAP success / key material
<--- EAP success / WEP key
encrypted data --->
<--- encrypted data

```

Suivant les méthodes d'authentification utilisées dans EAP, les trames 802.1X contiennent le nom et mot de passe de l'utilisateur en clair ou chiffré et la clef WEP dynamique.

Les méthodes d'authentification utilisables dans le cadre de 802.1X peuvent être classées entre : celles basées sur des mots de passe, celles basées plutôt sur l'utilisation de certificats et celles utilisant un élément extérieur comme une carte à puce.

Les méthodes basées sur des mots de passe incluent :

- EAP-MD5 qui envoie un condensat du nom et mot de passe, et ne permet pas d'authentification mutuelle.
- LEAP (*Lightweight Extensible Authentication Protocol*) qui a été la méthode la plus utilisée jusqu'à présent, récemment renommé Cisco-EAP par Cisco.
- EAP-SKE (*Shared Key Exchange*) qui propose une authentification mutuelle et permet l'itinérance entre des réseaux de différents fournisseurs d'accès Internet.
- EAP-SRP (*Secure Remote Password*, défini dans www.ietf.org/internet-drafts/draft-ietf-pppext-eap-srp-04.txt) qui est l'adaptation à EAP du protocole SRP [RFC2945].

Les méthodes basées sur des certificats incluent :

- EAP-TLS (*Transport Layer Security*, défini dans www.ietf.org/rfc/rfc2716.txt), qui permet aussi d'utiliser un mot de passe et qui est la méthode la plus répandue.
- EAP-TTLS (*Tunneled-TLS*, défini dans www.ietf.org/internet-drafts/draft-ietf-pppext-eap-ttls-01.txt), qui est une extension d'EAP-TLS utilisant la connexion TLS pour échanger des informations complémentaires permettant de protéger l'identité de l'utilisateur.
- PEAP (*Protected Extensible Authentication Protocol*, défini dans www.ietf.org/internet-drafts/draft-josefsson-pppext-eap-tls-eap-02.txt) qui sera sans doute beaucoup utilisé à l'avenir.
- EAP-MAKE (*Mutual Authentication Protocol*), qui utilise un mécanisme basé sur Diffie-Hellman pour l'authentification avec une clef symétrique commune dérivée. Son défaut est d'imposer une PKI.

Les méthodes utilisant des cartes ou caulettes incluent :

- EAP-SIM (*Subscriber Identity Module*, défini dans www.ietf.org/internet-drafts/draft-haverinen-mobileip-gsmsim-03.txt) qui utilise la carte à puce SIM du GSM. EAP-SIM permet l'authentification de l'utilisateur et la distribution d'une clef de session. Il a été implémenté par Nokia et permet de construire des réseaux permettant une itinérance entre des WLAN et le réseau GPRS. Cette itinérance entre ces deux technologies complémentaires est importante pour la facilité d'usage pour l'utilisateur.
- EAP-AKA (*Authentication and Key Agreement*, défini dans www.ietf.org/internet-drafts/draft-arkko-pppext-eap-aka-04.txt) utilise le système d'authentification AKA de l'UMTS, c'est-à-dire la carte USIM de l'UMTS, qui est compatible avec la SIM du GSM.

Il existe aussi une méthode générique avec GSS-API (défini dans www.ietf.org/internet-drafts/draft-aboba-pppext-eapgss-12.txt), qui permet à nouveau, un support de multiples méthodes d'authentification : clef publique, carte à puce, Kerberos, mot de passe à usage unique, etc.

Cette diversité montre bien les difficultés d'interopérabilité.

LEAP (*Lightweight Extensible Authentication Protocol*) n'est implémenté que dans les bornes Cisco. Il doit sa popularité au fait que cela a été la première implémentation de 802.1X dans le cadre des réseaux sans fil 802.11b, et pendant plus d'un an, la seule viable pour une entreprise. LEAP supporte lui-même de multiples mécanismes d'authentification : il fonctionne avec la plupart des serveurs Radius, génère et distribue des clefs WEP dynamiques, et Cisco propose les logiciels pour les postes clients Windows, MacOS 9 et Linux.

EAP-TLS est normalisé dans un RFC expérimental [RFC2716] et largement disponibles chez les fournisseurs de bornes : 3Com, Agere, Proxim, etc, et leur nombreux OEM. Cisco inclut aussi EAP-TLS dans ces bornes. Il est disponible dans de nombreux serveurs d'authentification Radius dont FreeRadius (www.freeradius.org) qui est gratuit. EAP-TLS permet une authentification mutuelle entre le client et le serveur d'authentification par le protocole d'établissement d'une communication TLS, et peut utiliser un certificat client si une PKI existe. EAP-TLS génère et distribue des clefs WEP dynamiques par utilisateur, par session et par nombre de paquets transmis, ce qui rend caduques les attaques sur les clefs WEP. EAP-TLS est disponible en standard dans Windows XP, dans tous les logiciels clients 802.1X du marché et sous Linux avec Xsupplicant.

EAP-TTLS qui était EAP-TLS est la solution la plus sûre. Elle est disponible sur les bornes Agere (ex-Lucent) et chez de plus en plus de fournisseurs. Pour les postes clients, le logiciel est disponible notamment chez : Funk Software, LeapPoint Technologies et Meetinghouse Data Communications.

PEAP est une application d'EAP dans TLS dans EAP. Cela permet une authentification mutuelle côté serveur par TLS, et côté client au minimum par EAP. PEAP génère des clefs de session en itinérance. PEAP est la technologie promue par Microsoft : son implémentation est annoncée dans les bornes Agere, Cisco et Enterasys, ainsi que son support dans Windows XP et Windows.net. En 2001, Microsoft annonçait le support pour le 2^e trimestre 2002: ce n'est pas encore disponible. PEAP impose un serveur Radius supportant TLS.

IEEE 802.11i et TKIP

Suite aux attaques sur la sécurité de 802.11b, l'IEEE a créé un groupe de travail dédié pour adresser la sécurité : IEEE 802.11i, dont les spécifications sont obligatoires dans IEEE 802.11g et IEEE 802.11e.

La WECA a annoncé l'inclusion d'IEEE 802.11i dans sa certification WiFi dès 2003.

Le groupe de travail IEEE 802.11i a défini deux niveaux :

- une solution de transition compatible avec le matériel existant, qui propose un nouveau protocole de gestion des clefs, TKIP (*Temporal Key Integrity Protocol*), qui génère et distribue des clefs WEP dynamiques, et qui sera inclus dans la certification WiFi de la WECA,
- une solution finale incompatible avec le matériel existant où 802.1X est obligatoire, avec l'algorithme de chiffrement RC4 remplacé par AES.

TKIP utilise un vecteur d'initialisation de 48 bits au lieu de 24 bits dans 802.11b actuel, avec une réinitialisation à l'établissement de la clef de session et une normalisation stricte du séquençage. TKIP dérive une clef par trame avec la clef de session, plus le vecteur d'initialisation, plus l'adresse MAC. À chaque trame, TKIP remplace le CRC32 sur les données du 802.11b actuel, par une somme de contrôle cryptographique (MIC : *Message Integrity Code*) sur toute la trame, y compris les en-têtes : ceci rend caduques les attaques actuelles avec des trames 802.11b falsifiées.

Distribution des clefs WEP de session

```

| client | | borne | --- | serveur |
| authentication |
association request--->
    <--- association response
EAP authentication --->
    <--- - - - <--- EAP responses
    <--- session key
    <--- EAP success / WEP key
    encrypted data --->
    <--- encrypted data
EAP key request --->
    <--- EAP WEP key response
association request--->
    <--- association response
    encrypted data --->
    <--- encrypted data

```

Les clefs WEP sont dynamiques par session.

Il existe d'autres possibilités propriétaires pour réaliser une authentification et un contrôle d'accès sur une borne, mais celles-ci sont obsolètes. Si l'on n'a pas la possibilité de déployer 802.1X, au moins en choisissant PEAP ou EAP-TLS, alors il faut impérativement implémenter une solution d'authentification et de contrôle d'accès au niveau 3 ou 4. Une sécurité dans les couches supérieures sera indépendante de la technologie du réseau sans fil, mais, à défaut d'usage du WEP, il faut qu'elle chiffre la session, comme SSH, SSL ou un tunnel IPsec qui permet souvent une authentification "client", spécifique à chaque éditeur mais qui est identique à celle d'un accès distant.

Enfin, il convient d'architecturer correctement ses WLAN : bien considérer les réseaux sans fil comme extérieurs à son périmètre sous contrôle, comme les flux Internet. Il faut segmenter les réseaux sans fil sur des DMZ, derrière des passerelles de sécurité, avec un filtrage et une journalisation avant d'accéder au réseau privé. Cette sécurité est indispensable et complémentaire à l'authentification et au contrôle d'accès sur l'interface *air* réalisée par la borne.

Il faut également considérer les bornes 802.11 comme des équipements sensibles et travailler la sécurité physique des ondes dans l'espace, en choisissant consciencieusement l'emplacement des bornes ou des antennes (voir www.hsc.fr/ressources/presentations/wlan02b/mgp00028.html). Il faut également penser à régler la puissance des bornes au plus juste : la majorité des utilisateurs laissent les bornes réglées par défaut, donc généralement au maximum de leur puissance.

En conclusion, il convient de bien réaliser que les réseaux locaux sans fil sont déjà déployés partout et pour toujours.

En conséquence, il faut s'organiser pour les gérer et minimiser les risques : authentifier les utilisateurs, contrôler l'usage et surveiller en permanence les réseaux sans fil.

Annexes

➤ Sélection de ressources :

802.11 (WiFi)

- Les normes IEEE 802.11
standards.ieee.org/getieee802/802.11.html
- Detecting and eavesdropping on WLANs: feasibility and countermeasures
www.hsc.fr/ressources/presentations/wlan02b/
- Exemple d'utilisation en liaison point à point sur 2.000 m
www.wifi-france.net/htm/autrans2002
- Comparatif de la consommation des cartes Ethernet sans fil
www.synack.net/wireless/consumption.html
- Caméra vidéo équipée en 802.11b
www.dlink.com/products/DigitalHome/DigitalVideo/dcs1000w/
- Wireless LAN Security in Depth
www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safwl_wp.htm
- Securing The Maginot Line of Wireless LANs
www.bluesocket.com/maginotLine.html
- La réponse de Cisco aux vulnérabilités de 802.1X
www.cisco.com/warp/public/cc/pd/witc/ao350ap/prodlit/1680_pp.htm

802.15 (Bluetooth)

- La spécification de Bluetooth 1.1 (la norme 802.15 est en draft)
www.bluetooth.com/dev/specifications.asp
- Draft IETF "IP over Bluetooth"
www.normos.org/ietf/draft/draft-akers-atwal-btooth-01.txt
- Le groupe de travail 802.15.3
www.ieee802.org/15/pub/TG3.html
- Introduction à la sécurité de 802.15.3
www.securemulticast.org/GSEC/gsec3_ietf53_Singer.pdf

Mixte

- Introduction aux réseaux sans fil
www.guill.net/reseaux/Sansfil.html
- Un prototype de borne mixte 802.11b et GPRS sous Linux
www.linuxdevices.com/articles/AT6271269832.html
- Une borne faisant à la fois 802.11b et 802.11a : Cisco Aironet 1200
www.cisco.com/warp/public/cc/pd/witc/ao1200ap/prodlit/casap_ds.htm

Administration et régulation en France

- Synthèse de la consultation publique sur la technologie RLAN
www.art-telecom.fr/publications/index-rlanreponse.htm

Réseaux locaux sans fil

www.atca.pm.gouv.fr/dossiers/documents/reseaux_locaux_sans_fil.shtml

➤ Acronymes

AP	Access Point, borne d'un réseau sans fil
BLR	Boucle Locale Radio
BNEP	Bluetooth Network Encapsulation Protocol
CSMA/CD	Carrier Sense Multiple Access / Collision Detection
CSMA/CA	Carrier Sense Multiple Access / Collision Avoidance
EAP	Extensible Authentication Protocol [RFC2284]
GPRS	General Packet Radio Service
GSS-API	Generic Security Service API [RFC1508]
IP	Internet Protocol
L2CAP	Logical Link Control and Adaptation Protocol (Bluetooth)
LAN	Local Area Network
LEAP	Lightweight Extensible Authentication Protocol
LMDS	Local Multipoint Distribution Service ou System
MAN	Metropolitan Area Network
MMDS	Microwave Multichannel Distribution System Multipoint Microwave Distribution System Multichannel Multipoint Distribution Service
NAP	Network Access Point
NIC	Network Interface Card
NOC	Network Operations Center
PAE	Port Access Entity
PAN	Personal Area Network
PEAP	Protected Extensible Authentication Protocol
PMP	Point Multi-Points
PPP	Point-to-Point Protocol [RFC1548]
SB	Serial Bus
SIM	Subscriber Identity Module
SNMP	Simple Network Management Protocol
SOC	Security Operations Center
SSID	Service Set Identifier, ou System Identifier, le nom du réseau
STP	Spanning Tree Protocol
TFTP	Trivial File Transfer Protocol
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security protocol
VLAN	Virtual Local Area Network
WAN	Wide-Area Network
WAP	Wireless Access Point
WECA	Wireless Ethernet Compatibility Alliance (voir www.wirelessethernet.org)
WEP	Wired Equivalent Privacy (souvent pris pour Wireless Encryption Protocol)
WHUMAN	Wireless High-speed Unlicensed Metropolitan Area Network
WLAN	Wireless Local Area Network
WMAN	Wireless Metropolitan Area Network
WPAN	Wireless Personal Area Network
WSB	Wireless Serial Bus
WWAN	Wireless Wide-Area Network

➤ Remerciements

Je remercie William Arbaugh et Arunesh Mishra, Université de Maryland, et Phil Cox, System Experts, pour leurs schémas. Jérôme Poggi, Ghislaine Labouret et l'ensemble des consultants HSC pour leurs expérimentations. Yann Berthier, Ghislaine Labouret, Denis Ducamp et Jérôme Poggi pour leur relecture. Jérôme Poggi et Thomas Seyrat pour leurs photos.