IV. La sécurité du sans-fil

Le Wi-Fi est un vrai défis et une vraie révolution. Le développement de ces outils à été plus vite que l'apparition des normes, il en découle de sérieux problèmes de base. Nul jour sans un article de presse sur la faiblesse de la sécurité du Wi-Fi. La sécurité autour de Bluetooth est moins problématique du fait de sa faible portée et des mécanismes hérités des téléphones portables.
Nous allons donc nous focaliser sur la sécurité autour du Wi-Fi (norme 802.11b et 802.11g).

IV.1 Principes de base

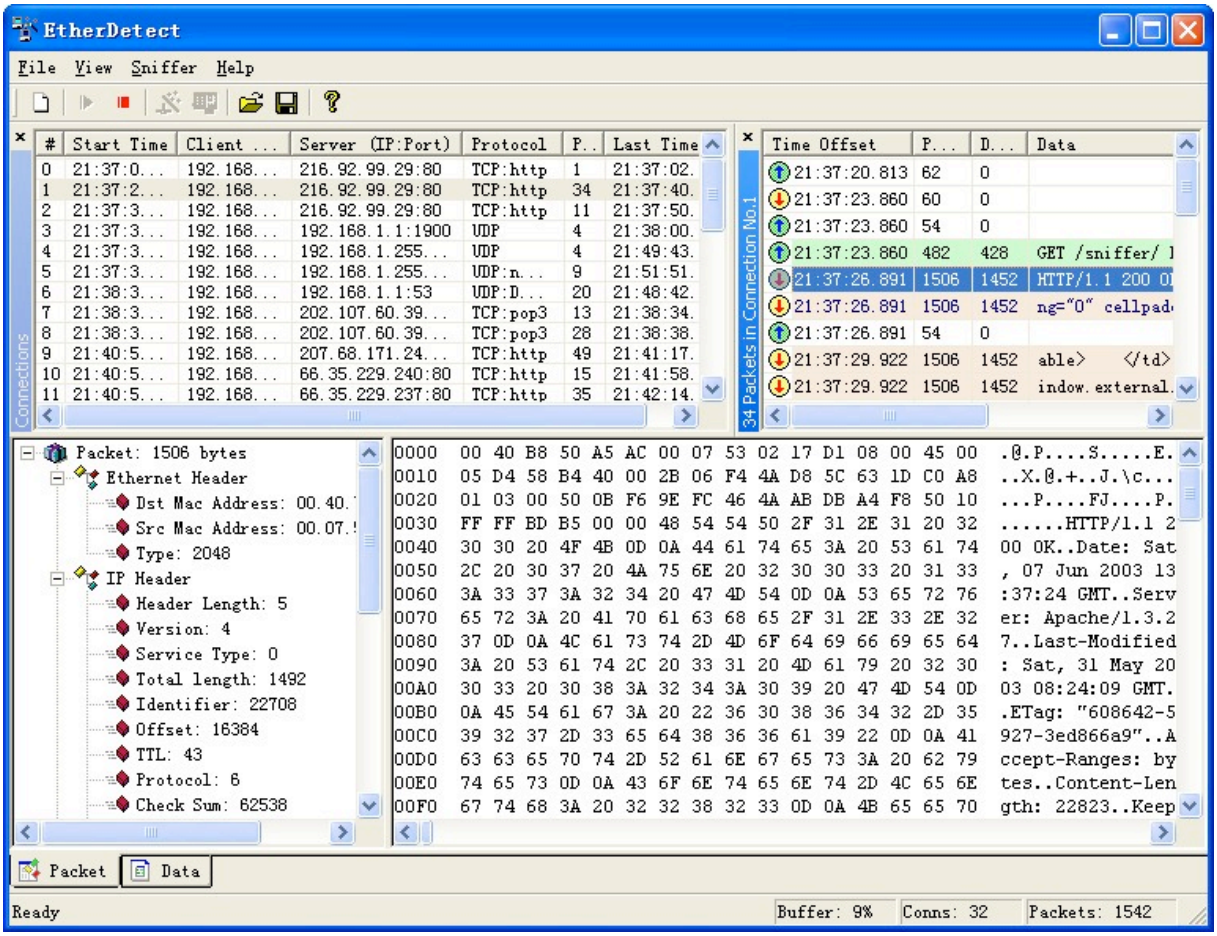
Rappelons le principe de base du 802.11 qui est celui de permettre à tous les matériels désirant se connecter à une borne (Point d'Accès) de scanner tous les canaux disponibles pour ensuite tomber sur l'AP désiré. Avec ce système, il est donc impossible de « masquer » l'existence d'un AP. il suffit de se promener avec son portable ou son PDA pour découvrir le plus simplement du monde l'existence dans un lieu d'un AP.

Carte Wi-fi pour PDA

Les ondes ne sont pas « directionnelles » et bien éduquées, elles vont partout où leur puissance le permet. Il est donc « facile » de capter le signal d'un AP même si vous n'êtes pas invités. Il suffit que ce matériel possède un sniffer pour capter les paquets de données.
Pour utiliser un AP, il faut s'y associer. Pour cela il faut trouver le canal utilisé et connaître le numéro d'identification de cet AP (SSID).

IV.2 Récupération des informations importantes

Le premier point est automatiquement fait par la carte sans-fil, l'AP émettant régulièrement des trames (Beacon Frames) pour s'annoncer.
Pour le second point, il faut savoir que le SSID est contenu dans les trames émises et ce en clair. Il suffit de sniffer ces trames pour obtenir le SSID de l'AP à laquelle on veut se connecter. Ceci peut même être fait avec un simple PDA ou des outils comme airtraf, WiFiScanner sous linux, APScanner sous Mac, linkferret (sniffer basique) sous windows par exemple (Voir le site de hacker http://www.wlanhacker.de/dietools.html) ou ethereal-XTRA (http://www.ethereal.com sur toutes plateformes).
Un outils commercial mais utilisable en test est assez intéressant EtherDetect (http://www.effectech.com).



Attention
Si vous récupérez des logiciels sur des sites de hacker ou des sites de faible confiance, ces logiciels peuvent être des piéges et peuvent aider à vous faire pirater donc MEFIANCE !

Le rapport basique suivant est fourni par le logiciel Wireless Scanner, mais c'est le point de départ aux attaques. Ce type de logiciel permet de

déterminer le niveau de vulnérabilité de l'AP. 0 représentant une borne « sûre » (cryptage …).

MAC Address	SSID	Signal	Channel	Vulns	Probable Vendor
00:02:2D:77:77:77	Hacme	45	6	2	Lucent ORiNOCO
00:04:5A:CC:BB:AA	linksys	54	6	4	Linksys
00:05:5D:78:9A:BC	GoISS!	105	6	0	D-Link
00:06:1D:88:88:88	Andy	42	10	3	Lucent ORiNOCO
00:07:0E:66:77:88	Leslie	54	4	2	Cisco Aironet
00:20:D8:AA:AA:AA	Internetx	50	9	2	Baystack
00:30:AB:55:55:55	secure1	72	6	2	Netgear
00:40:96:EE:EE:EE	400	36	3	2	Cisco Aironet
00:80:C6:99:99:99		60	2	0	SOHOware NetBlaster II
00:90:D1:BB:BB:BB		60	11	1	SMC
00:A0:0F:33:33:33		36	8	1	Symbol
00:A0:F8:66:66:66	Bob_in_Marketi	42	3	3	Symbol

Il est nécessaire de s'associer à l'AP ce qui peut impliquer d'être vite découvert.
Il est malgré tout possible de sniffer le réseau sans-fil sans s'associer à l'AP. Pour cela il faut utiliser le mode monitor ou RFMON (appellation CISCO). Dans ce cas, la carte remonte toutes les trames 802.11 brutes.

Remarque
Pour pouvoir utiliser un sniffer et récupérer les trames (niveau 2) vous devez basculer votre carte réseau en mode promiscuous afin de permettre a ces informations de remonter aux couches supérieures. Sans ce basculement, votre sniffer ne récupérera pas grand chose d'intéressant.

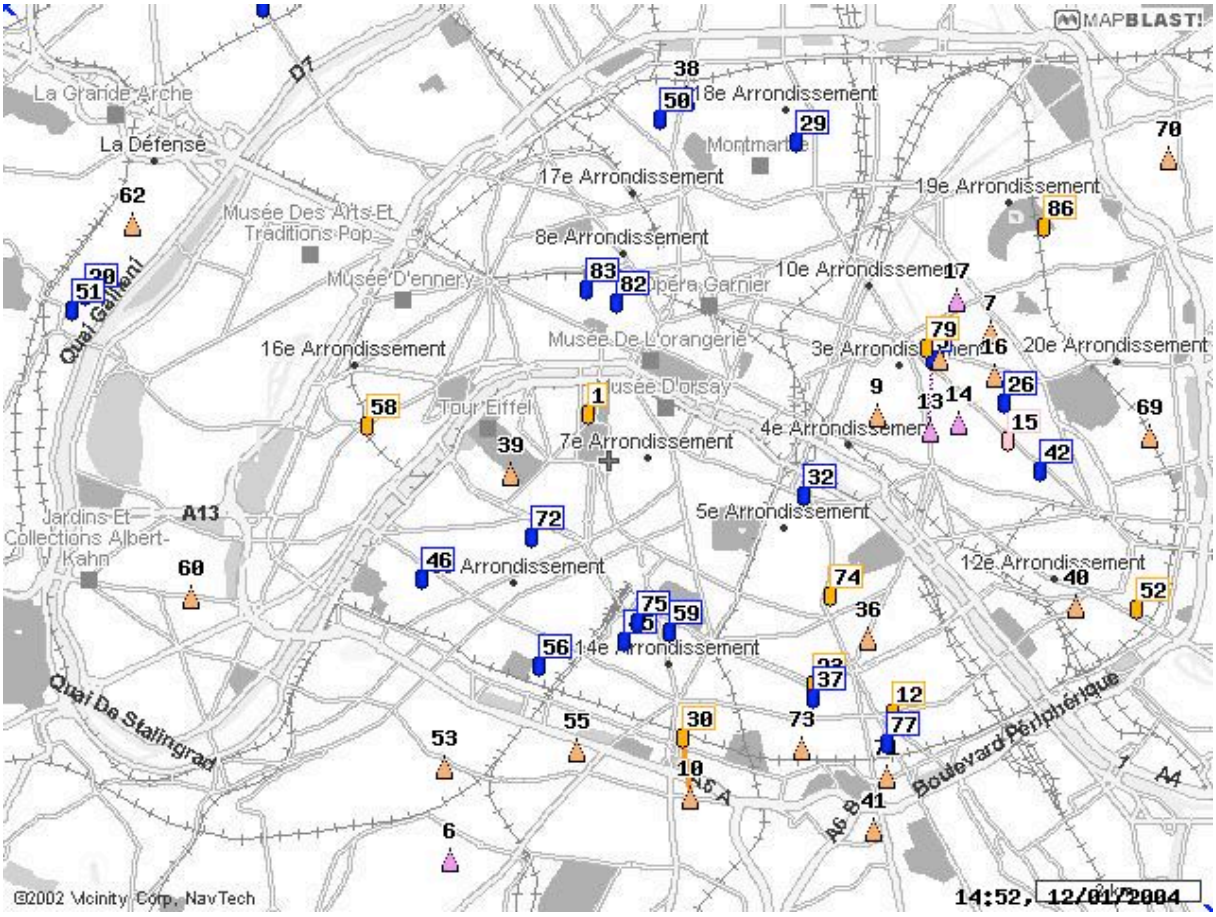
- Le WarDriving ou Trébucher sans Fil

Il existe actuellement un certain nombre d'outils logiciels et humains pour trouver les points d'accès. Un site très intéressant permet de montrer et de cartographier les points d'accès. Même si c'est aux USA, il est possible de faire de même en France et c'est édifiant (http://worldwidewardrive.org/ ou http://www.wardriving.com/). Selon leurs statistiques 88000 AP ont été trouvées et 67% n'ont pas activé le cryptage WEP, 27% possède le SSID par défaut et 24% cumule (SSID par défaut sans activer le WEP).
Cette cartographie est généralement réalisée avec des outils tels NetStumbler (pour l'écoute GPS) et StumbVerter (pour la cartographie) sous windows, kismet sous linux (http://www.kismetwireless.net/) ou macstumbler sous macintosh (http://homepage.mac.com/macstumbler/).

Il fleurit en ce moment des associations dont le but est intéressant mais très dangereux. Elles mettent en place des réseaux associatifs d'utilisateurs qui ouvrent leur AP pour permettre une utilisation « libre » des réseaux sans-fil.
Attention à ne pas faire n'importe quoi et mettre une politique de sécurité en place sinon cela risque de poser de gros problèmes en cas de piratage via une des structures à disposition.
La ville de Nantes fait partie des pionnières (http://www.nantes-wireless.org/) et met en place ces sécurités comme me l'a signalé l'un des initiateurs du projet.
« Notre but n'est pas de créer un réseau communautaire sans sécurité, mais de construire (un) des réseaux communautaires de la taille d'un quartier, d'une rue et tout ça avec un minimum de sécurité (openVPN sécurité, FreeRadius ..). »

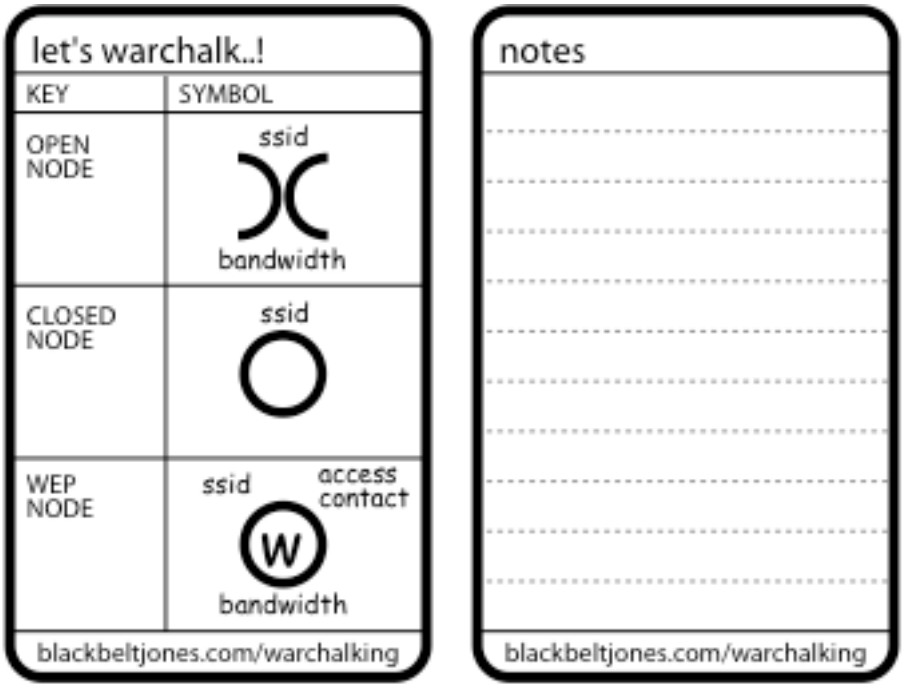
Ces points d'accès libres sont appelés Hotspots (en rapport avec le surf sur les grandes vagues).
Il existe là aussi des sites qui référencent ces zones « libres » (http://www.journaldunet.com/dossiers/wifi/annuairewifi.shtml).

Vous trouverez un exemple de carte intéractive de Paris, fournissant les informations nécessaires pour se connecter aux bornes détectées en cliquant simplement sur les numéros indiquées sur la carte (http://www.paris-sansfil.fr/index.php/?CartePSF2004).



- WarChalking ou CraieFiti

Il existe aussi d'autres méthodes pour détecter les AP et leurs états : regarder les trottoirs. En effet une nouvelle mode est lancée, qui existait déjà au niveau artistique mais qui est mise au service (ou le contraire) du WiFi : le warchalkink en Français le craiefiti. Des dessins à la craie sont mis au endroit ou des AP ont été découvertes avec en prime l'état voir des renseignements plus complets sur cet AP. Les codes sont proposés dans l'image ci-dessous.



Il y a trois états définis ouvert, fermé et Wep actif.

Quelques photos (http://craiefiti.free.fr):

Remarque

Autre problème peu évoqué, si vous utilisez une borne dont vous n'avez pas la gestion qui dit que celui qui la gère n'épie pas vos communications (mél, banque, navigation …). Il suffit de posséder un sniffer ou simplement de loguer ce qui passe par la borne et le tour est joué. Regardez un peu les forums de discussions sur le sans fil « j'utilise la connexion sans fil de mon voisin, c'est super ». Il ne faut pas voir le mal partout mais certaines bornes peuvent être ouvertes volontairement, pensez-y.

IV.2 Le cryptage WEP

Afin « d'augmenter » la sécurité, l'idée du cryptage des communications paraît une bonne solution. WEP (Wired Equivalent Privacy) propose cette solution. Ce système permet d'intégrer une clé de cryptage basé sur l'algorithme RC4 jusqu'à 128 bits, sur l'AP et sur les clients. Cette clé a le défaut d'être statique et donc en cas de changement, la modification doit se faire sur tous les matériels utilisant le réseau sans-fil.
Le principal problème du WEP est qu'il est basé sur un algorithme de chiffrage le RSA (inventé en 1977 par Rivest-Shamir-Adleman).
Cet algorithme est public depuis 1994 et des mathématiciens (Fluhrer, Mantin et Shamir) ont montré qu'il y avait des failles dans cet algorithme.
En effet, sur une clé de 64 bits (ou 128 bits), 24 servent pour l'initialisation et les 40 (ou 104) autres servent pour le chiffrement. De plus la partie qui sert au chiffrement est statique et peut être « facilement » découverte si le vecteur d'initialisation n'est pas correctement généré (mode pseudo aléatoire, compteurs …) ou simplement en récupérant les en-têtes des paquets IP.
Il a été démontré qu'en moins de 20 minutes d'écoute du réseau tous ces éléments sont crackés.
Malgré le chiffrage, il existe donc des trous de sécurité. Certaines trames passent en clair lors d'échanges, il est donc possible à partir de ces trames et d'un outils tel airsnort (http://airsnort.shmoo.com/) et wepcrack (http://wepcrack.sourceforge.net/), de déduire la clé Wep.
Bien que ces trous de sécurité soient connus, les constructeurs proposent encore des matériels potentiellement piratables via ce biais.
Récemment (02 Décembre 2003) sur les modèles airconect 1100, 1200 et 1400 de Cisco un correctif sécurité a du être proposé:

Cisco Security Advisory: SNMP Trap Reveals WEP Key in Cisco Aironet Access Point Document ID: 46468 Revision 1.0 For Public Release 2003 December 02 17:00 UTC (GMT)

http://www.cisco.com/warp/public/707/cisco-sa-20031202-SNMP-trap.shtml. Mais ce n'est hélas pas le seul.

Pour plus d'informations : http://www.security-labs.org/.
Il existe des solutions basées sur la norme 802.1x qui permet une génération de clés dynamiques plus sûres mais plus complexes à mettre en œuvre car nécessitant un serveur d'authentification (Voir IV.3).

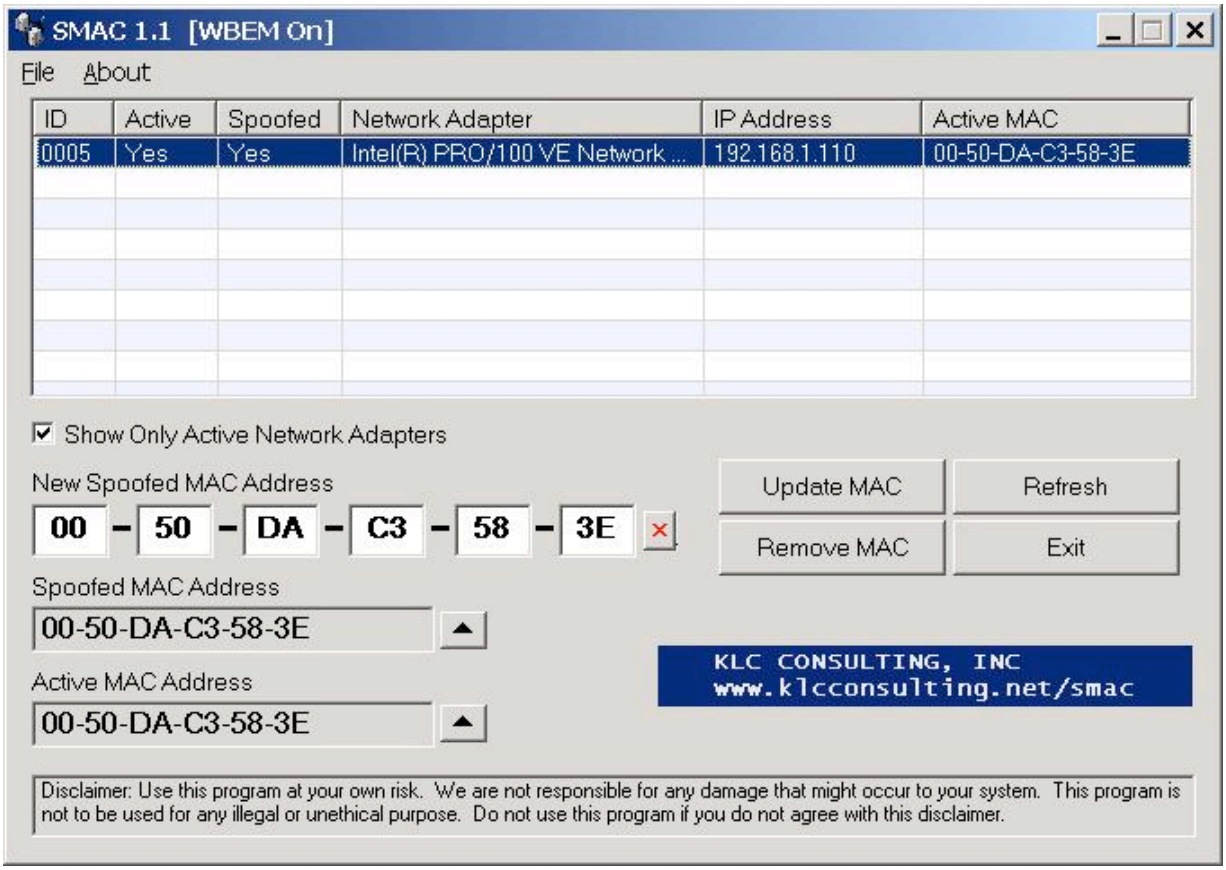
Pire, lors de la phase d'authentification entre le client et l'AP, ce dernier envoie un texte en clair au client qui crypte cette chaîne avec sa clé et renvoie ce cryptage. Si le cryptage est conforme, l'AP accepte la communication et l'association du client. Connaissant le texte en clair et son cryptage, il est alors possible d'en déduire la clé.
Il est aussi possible de récupérer la communication après l'AP au niveau de la partie filaire. A ce niveau, les communications ne sont plus cryptées.
Il est tout de même à noter que ces méthodes ne sont pas à la portée de n'importe qui mais il faut aussi noter que beaucoup d'utilisateurs de solution sans-fil ne mettent pas en place le cryptage rendant le travail du pirate plus simple (Voir statistiques dans la partie IV.2).

Pour apporter un peu plus de sécurité à votre réseau sans-fil :

- Mettre le réseau sans-fil dans une DMZ (DeMilitary Zone)
- Affecter une adresse IP fixe à l'AP mais aussi aux autres matériels
- Mettre l'AP à un endroit impossible à atteindre physiquement
- Modifiez le SSID par défaut
- Désactivez la diffusion du SSID (SSID Broadcasts)
- Modifiez le mot de passe par défaut du compte administrateur
- Activez le filtrage des adresses MAC (MAC Address Filtering)
- Modifiez régulièrement le SSID
- Activez le cryptage WEP 128 bits
- Modifiez les clés de cryptage WEP régulièrement.

Bien évidemment tout ceci n'est pas des plus simples car certaines informations doivent, dans le même temps, être modifiées sur les clients (SSID, Clé WEP) ce qui rend ces recommandations difficiles à suivre, mais la sécurité est à ce prix.

Remarque
Le filtrage des adresses MAC n'est pas une sécurité, car il existe un certain nombre d'outils permettant de faire du « spoofing » d'adresse MAC tels etherspoof (Macintosh) ou smac (windows) pour ne citer qu'eux.

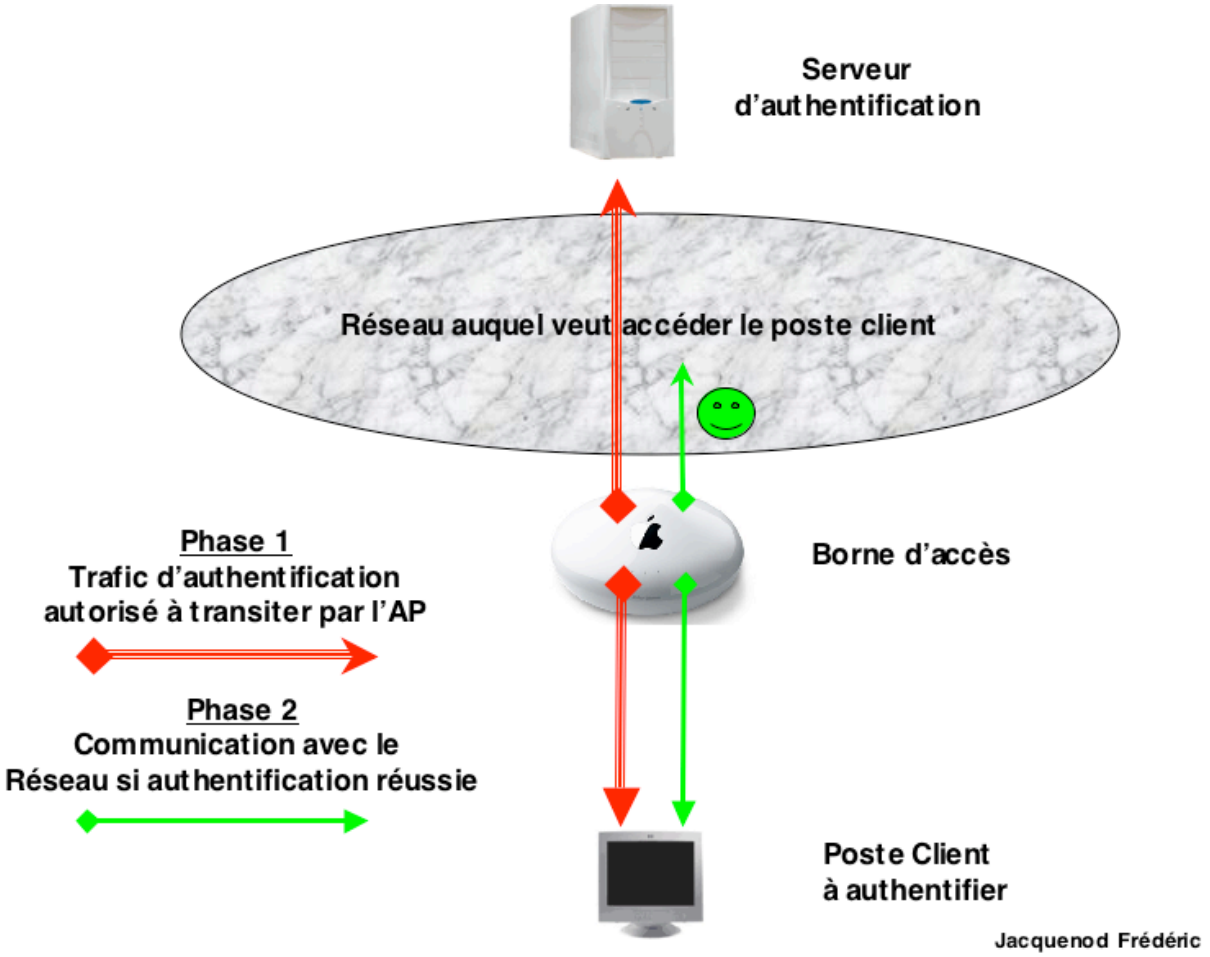


IV.3 La norme 802.1x pour une meilleure sécurité

Il existe malgré tout des possibilités de sécuriser votre réseau sans-fil. Ces possibilités sont plus complexes à mettre en œuvre et sont donc plus orientées entreprises que particuliers. La norme 802.1x, dont le draft 8 date du 3 Décembre 2003, propose une sécurisation plus forte.
La norme 802.11 s'appuie sur la norme 802.1x pour la partie authentification. Trois entités entrent en jeu :

- Le poste à authentifier (client)
- Le Point d'Accès (borne, routeurs, pont …)
- Le serveur d'authentification

Le client doit être authentifié avant de pouvoir utiliser réellement le réseau. Pendant la phase d'authentification, seuls les échanges portant sur cette authentification sont relayés par l'AP en direction du serveur d'authentification (Voir schéma ci-dessous).



La norme 802.1x se base sur le protocole d'authentification EAP (Extensible Authentication Protocol). EAP est un standard de l'IETF (Internet Engineering Task Force). La spécification se trouve dans le RFC (Request For Comment) 2284. EAP a été défini pour la communication via modem en utilisant le protocole PPP (Point to Point Protocol). Le RFC 2284 a d'ailleurs pour titre : « PPP Extensible Authentication Protocol (EAP) ».

Il y a deux phases définies par le protocole EAP:

- La demande d'authentification entre l'AP et le client (login, mot de passe, certificat, biometrie …) appelée aussi EAPOL (EAP Over Lan)
- La transmission de ces informations entre l'AP et le serveur d'authentification (souvent un serveur RADIUS (Remote Authentication Dial In User Service)) appelée aussi EAPOR (EAP Over Radius)

Bien sûr préalablement à la partie authentification, le client doit s'associer à l'AP.

Le protocole EAP est complété par d'autres outils pour l'authentification, il en résulte un choix à faire lors du montage de son réseau et de la partie authentification. On retrouve ainsi

- EAP-TLS : EAP + Transport Layer Protocol basé sur les clés publiques PKI (Public-key infrastructure) appelées aussi certificats. Les clés WEP sont générées de manière automatique.
- EAP-TTLS (Tunneled et EAP-PEAP (Protect EAP)) assez proche de EAP-TLS à la différence près qu'un tunnel (VPN Virtual Private Network) est utilisé en plus du système de PKI. Ce système augmente la sécurité via un nouveau chiffrement de la communication. Les clés WEP sont générées de manière automatique.
- EAP-MD5 (EAP-Message Digest 5) C'est le plus simple à mettre en œuvre car seul le couple login-mot de passe est demandé. Par contre rien n'est chiffré. De plus les clés WEP ne sont pas dynamiques.
- EAP-LEAP (EAP-LightWeight EAP) Cette association est propriétaire CISCO mais il est possible d'utiliser en plus une des méthodes précédentes. Les clés WEP sont générées de manière automatique.

IV.4 L'avenir de la sécurité

Le groupement WECA vient de certifier le protocole WPA (Wi-Fi protected access) pour remplacer le protocole WEP (Wired equivalent privacy) défaillant. Ce protocole modifie l'algorithme RSA par l'algorithme TKIP (Temporal Key Integrity Protocol) qui permet la génération aléatoire et la possibilité de changer la clé plusieurs fois par secondes.
La version 2.0 est prévue pour la fin 2003, il s'inspire des travaux du 802.11i de l'IEEE.
Il suffit alors de modifier le firmware des matériels pour qu'il prenne en compte ce nouvel algorithme en remplacement du RSA (RC4).
Malgré tout, la plus grande complexité de l'algorithme nécessite des matériels plus puissants et ceux-ci ne seront disponibles que vers le troisième trimestre 2004.

Remarque
Avant que tout soit normalisé et soit disponible certains ont déjà trouvé une faille dans le WPA, dans le cas ou la clé d'origine est générée avec un mot récupérable dans le dictionnaire de moins de 20 caractères. Ce

problème est simple à résoudre en obligeant la saisie d’une clé plus grande (ce que fait déjà Apple en proposant des clés héxadécimales).