CYBER NETWORKS

LIVRE BLANC
Sécurité des systèmes sans-fil

Version 1.2

Dernière révision : 25 Avril 2003

Auteurs :

Julien STEUNOU – Ingénieur Sécurité CYBER NETWORKS
jsteunou@cyber-networks.fr

Aurélie PEREZ – Ingénieur Sécurité CYBER NETWORKS
aperez@cyber-networks.fr

Tables de matières

©2003-Cyber Networks-tous droits réservés

©2003-Cyber Networks-tous droits réservés

Table des schémas

©2003-Cyber Networks-tous droits réservés

1. Introduction

L'année 2002 a été marquée par la montée en puissance d'une véritable révolution des réseaux informatiques : celle des systèmes sans-fil. En alliant connectivité et mobilité, ces nouvelles technologies sont en passe de modifier en profondeur les systèmes d'information et leurs infrastructures aussi sûrement et durablement que l'avènement de la téléphonie mobile a impacté le monde télécom.

En effet les réseaux sans-fil, en faisant émerger de nouvelles façons d'accéder aux ressources informatiques et d'échanger des données, ne laissent personne indifférent : utilisateurs et responsables informatique y trouvent sans cesse de nouvelles applications … tout comme les pirates ! car force est de constater que ces réseaux se mettent en place de façon parfois anarchique, souvent à l'insu même des responsables, et remettent en cause des pans entiers de la sécurité informatique des entreprises.

L'objectif de ce livre blanc est de faire le point sur ces nouvelles technologies en mettant l'accent sur les problématiques de sécurité et les méthodes de sécurisation possibles.

©2003-Cyber Networks-tous droits réservés

2. Présentation des réseaux sans-fil

Un réseau sans-fil substitue aux habituels câbles des connexions aériennes via des ondes radios, infrarouges ou éventuellement des faisceaux laser. Cette définition, assez large, nous amène à considérer plusieurs types de réseaux sans-fil :

2.1. Les réseaux sans fil de type infrastructure

Les réseaux de type infrastructure sont des réseaux structurés, basés sur des équipements d'interconnexion faisant office de ponts entre un réseau radio et un réseau câblé permettant ainsi à de nombreux clients mobiles d'accéder à des ressources informatiques.

2.1.1. Les réseaux sans-fil locaux

Les réseaux sans-fil locaux pour terminaux mobiles, et en particulier les réseaux Wi-Fi ou 802.11b, sont à la fois les plus répandus et les plus médiatisés à l'heure actuelle.

Le terme technique pour ces réseaux est WLAN (pour Wireless Local Area Network) par opposition à LAN (Local Area Network) qui désigne un réseau câblé traditionnel.

Un WLAN est constitué de bornes d'accès (appelées points d'accès ou points d'extension selon leur rôle exact dans l'architecture) équipées d'une antenne et d'une interface réseau Ethernet standard. Chaque borne forme une zone de couverture radio appelée cellule. L'ensemble des cellules constitue le WLAN.

Les terminaux mobiles (PC portable, PDA…) équipés d'adaptateur réseau sans-fil naviguent dans la zone de couverture du WLAN et restent connectés en permanence au réseau de l'entreprise sans contrainte physique. Ils accèdent ainsi aux ressources informatiques situées sur la partie câblée des points d'accès de la même façon que les stations de travail standards : le seul changement vient du lien physique utilisé pour la connexion.

©2003-Cyber Networks-tous droits réservés

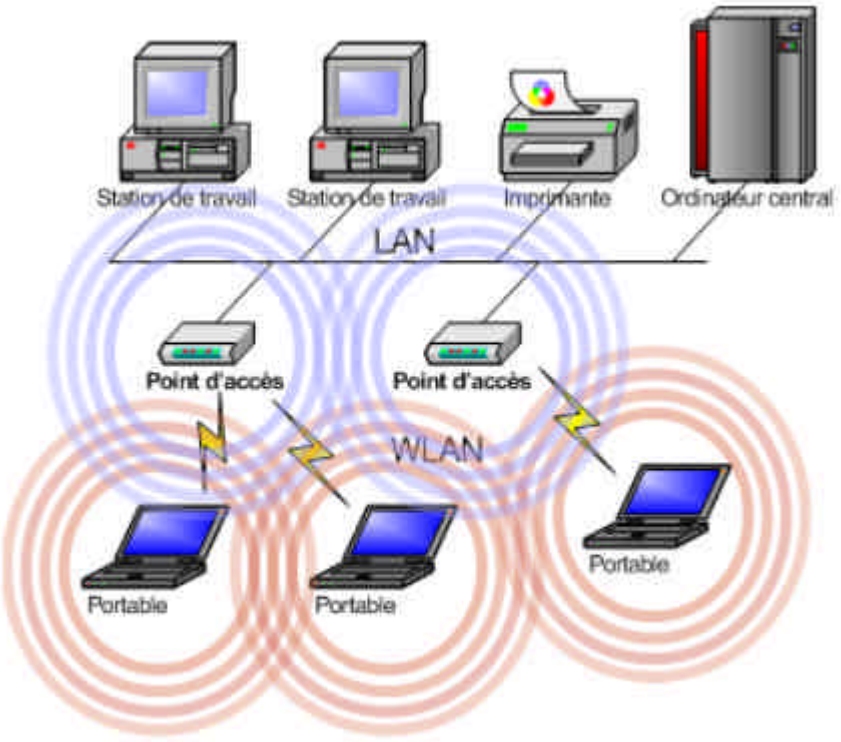


Figure 1 : Exemple de WLAN

Pour rester dans le cadre d'un WLAN, il faut que le réseau respecte deux conditions :

- La zone de couverture utile doit être de l'ordre d'un bâtiment ou d'un site.
- L'infrastructure réseau utilisée doit être contrôlée par l'entreprise.

Selon leur vocation les WLAN peuvent être :

- **Des WLANs privés ou d'entreprise** : les terminaux mobiles servent à des employés dans l'enceinte de l'entreprise pour accéder au système d'information traditionnel.

  Exemple : Dans un hôpital, les médecins vont de chambre en chambre tout en accédant aux dossiers des patients en ligne et aux applications médicales depuis des PC portables.

- **Des WLANs publics ou hot-spots :** les terminaux mobiles appartiennent dans ce cas à des clients accédant à une ressource particulière (le plus souvent un accès à Internet) proposée par le propriétaire du hot-spot.

  Exemple : Des hôtels, des aéroports ou des cyber-cafés mettent à la disposition de leurs clients un accès Internet sans-fil.

- **Des WLANs domestiques :** un particulier forme un réseau sans-fil pour relier plusieurs PC et son routeur d'accès Internet.

©2003-Cyber Networks-tous droits réservés

Ces WLANs utilisent des technologies semblables mais leur intégration est très différente.

2.1.2. Les réseaux sans-fil étendus

Les réseaux sans-fil étendus reposent exactement sur le même principe que les WLANs mais avec des zones de couverture nettement plus larges, allant de la ville au monde entier. Ils sont souvent basés sur des technologies télécoms (GSM, GPRS, UMTS…) ou des normes radios propriétaires.

On parle de WMANs (Wireless Metropolitan Area Network) ou de WWANs (Wireless Wide Area Network) selon les distances.

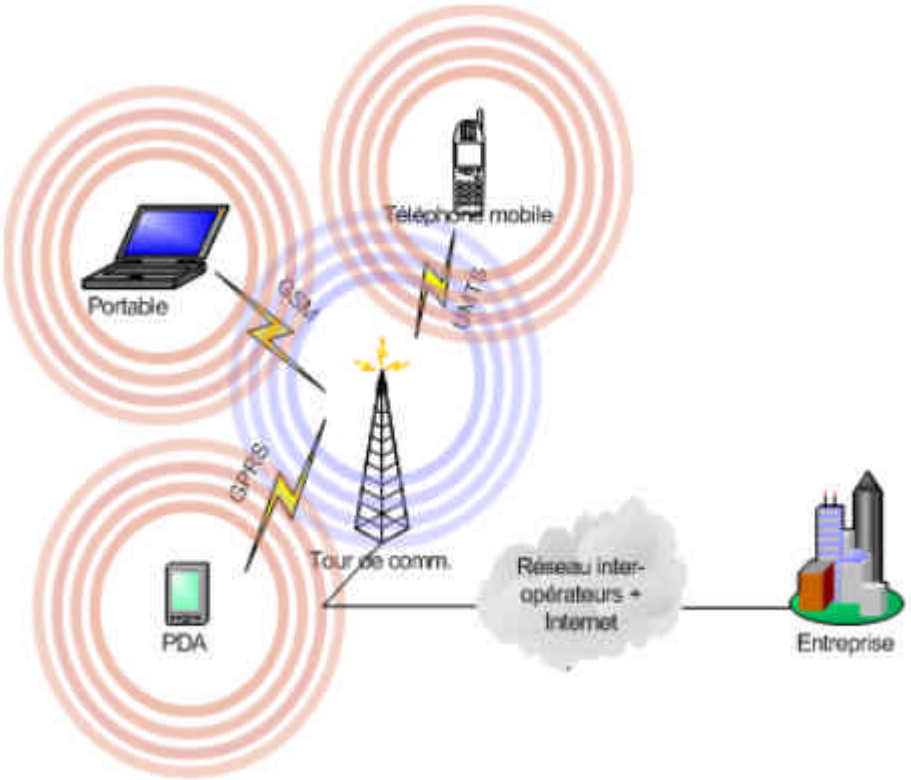


Figure 2 : Exemple de WWAN ou WMAN

Les WWANs peuvent être catégorisés de la façon suivante :

- **Les WWANs publics :** ils sont mis en œuvre par des opérateurs pour offrir des services réseaux à un grand nombre de clients mobiles. Ce sont l'équivalent des hot-spots publics des WLANs mais à plus grande échelle.

  Exemple : Les opérateurs télécoms offrent des accès Internet ou des services de messagerie accessibles sur des téléphones mobiles évolués.

- **Les WWANs privés sur infrastructure publique :** ces WWANs sont mis en place par les entreprises pour relier leurs terminaux mobiles à leurs systèmes d'information via une infrastructure publique de type télécom. Un WWAN de ce type est une véritable extension d'Internet.

©2003-Cyber Networks-tous droits réservés

Exemple : Les employés nomades accèdent à l'intranet et à la messagerie interne de l'entreprise depuis leurs PDA connectés en GPRS sur Internet.

- **Les WWANs totalement privés :** assez rares dans le secteur civil, les WWANs totalement privés connectent sur de grandes distances les terminaux mobiles d'une entreprise à un central via une infrastructure réseau radio privée.

  Exemple : Une compagnie de taxi connecte par liaison radio dédiée sa flotte de véhicules à son système informatique.

2.1.3. Les réseaux sans-fil spécifiques

Il existe des WLANs particuliers ne concernant pas directement des utilisateurs : par exemple un réseau de caméras de surveillance sans-fil, un réseau connectant des horodateurs ou des distributeurs de boisson avec un serveur… Beaucoup de ces réseaux sont complètement nouveaux ou prennent un nouvel essor grâce aux WLANs.

On peut également considérer les systèmes de téléphones sans-fil radio basés sur DECT comme des WLANs. Avec les prochaines évolutions de la voix sur IP, ce ne sera plus une simple extension du concept.

Les réseaux sans-fil de type infrastructure ne se limitent pas aux seuls réseaux de technologie Wi-Fi : tout composant mobile connecté à un point d'accès via un lien aérien est à prendre en considération.

2.2. Les réseaux ad-hoc

Les réseaux ad-hoc sont connus sous le nom de WPAN (Wireless Personal Area Network) ou de réseaux personnels. L'objectif de ces réseaux est de fournir une connectivité sans infrastructure dédiée. Ils sont donc exclusivement point à point et ne comptent en général que deux participants :

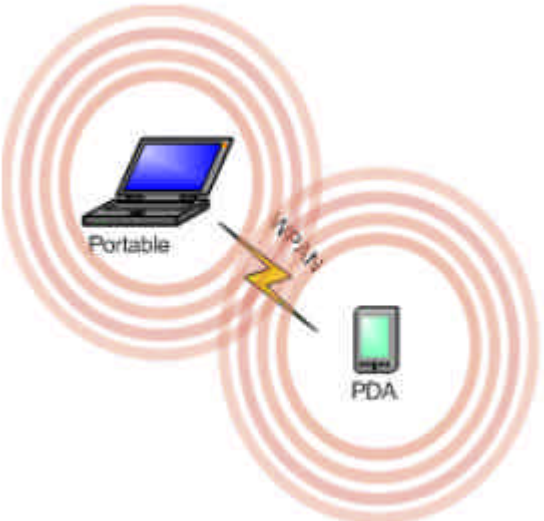


Figure 3 : Exemple de WPAN

©2003-Cyber Networks-tous droits réservés

Les terminaux mobiles friands de connectivité sans-fil comme les nouveaux téléphones portables et les PDA rassemblent la majeure partie des applications actuelles des WPANs.

Exemples : l'échange de carte de visite ou de fichiers en infrarouge entre deux PDA, la connexion d'un PDA avec un téléphone mobile en Bluetooth pour permettre un accès Internet GPRS, la connexion sans-fil d'un PDA sur une imprimante…

Les WPANs ont beaucoup d'avenir dans les réseaux dédiés entre des équipements non informatiques, en particulier dans la domotique.

Exemples : les connexions utilisées par les périphériques comme les claviers et les souris sans-fil, la connexion sans-fil Bluetooth entre un lecteur CD portable et le casque audio…

Les WPANs sont exceptionnellement variés et doivent être considérés comme des réseaux sans-fil à part entière, surtout du point de vue de la sécurité.

2.3. Les réseaux point à point

Ce type de réseau sans-fil englobe toutes les liaisons point à point longue distance utilisées pour relier des bâtiments ou des sites distants. Ces réseaux utilisent généralement des équipements spécifiques comme des antennes directionnelles ou des technologies plus pointues (liaison laser par exemple) :

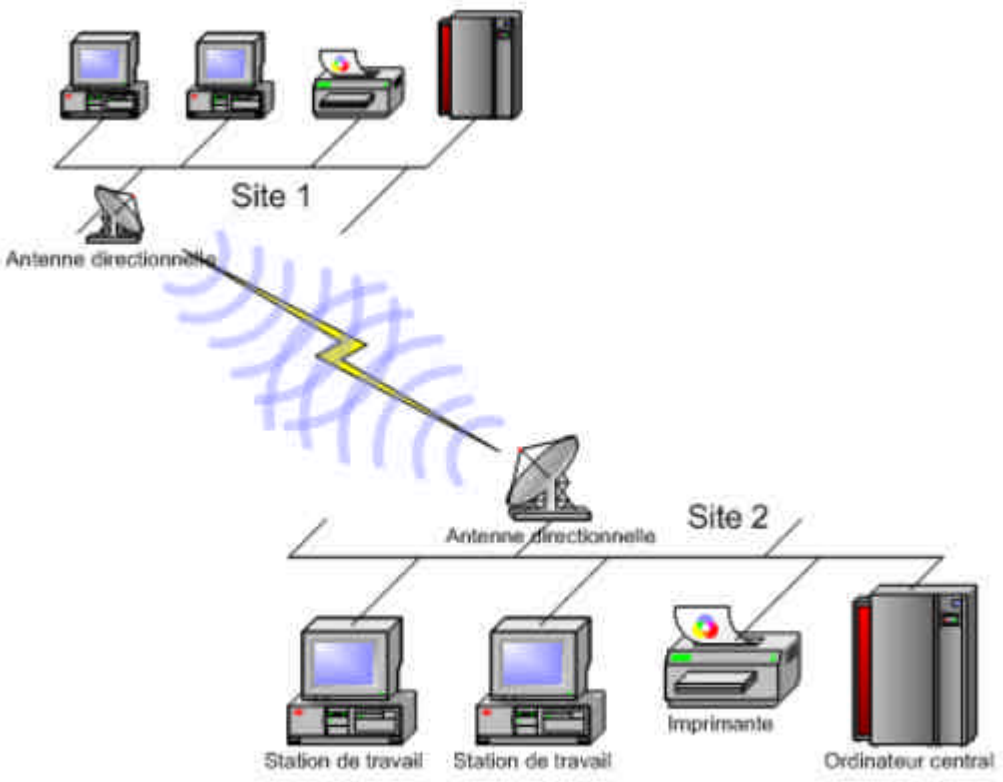


Figure 4 : Exemple de liaison point à point

©2003-Cyber Networks-tous droits réservés

Ce type de liaison peut encore se heurter à d'importants problèmes légaux : même si l'ART (organisme régissant l'utilisation des fréquences radio en France) assouplit certaines lois, la réglementation reste assez stricte sur les réseaux radio en extérieur.

2.4. Les réseaux point à multipoint

Les réseaux point à multipoints sont semblables à ceux formés par les stations radios ou la télévision hertzienne traditionnelle : un émetteur diffuse une information à un nombre important de récepteurs sur des distances étendues. Ces réseaux sans-fil particuliers restent encore très spécialisés.

La montée en puissance des normes comme l'IEEE 802.16 pour les accès sans-fil à large bande passante sur de longues distances va probablement ouvrir la voie à de nouvelles applications informatiques pour ce type de réseau.

©2003-Cyber Networks-tous droits réservés

3. Pourquoi utiliser un réseau sans-fil ?

Les motivations pour utiliser un réseau sans-fil ne manquent pas, que ce soit pour améliorer un système d'information existant ou pour mettre en place des applications entièrement nouvelles. Dans tous les cas le retour sur investissement apporté par ces technologies est exceptionnel.

Voici un bref aperçu des différents avantages des solutions sans-fil :

- **Mobilité :** les utilisateurs sont généralement très satisfaits des libertés offertes par les réseaux sans-fil et de fait sont plus enclin à utiliser les moyens informatiques mis à leur disposition. Le gain en productivité est important.

- **Evolutivité** : ces réseaux peuvent être dimensionnés au plus juste et suivre simplement l'évolution des besoins par simple ajout ou suppression de points d'accès par exemple.

- **Souplesse et facilité d'utilisation** : un système sans-fil peut être utilisé dans des installations temporaires (manifestation, salon…), couvrir des zones non accessibles aux câbles et relier facilement des bâtiments ou des sites distants. En étant peu intrusifs, ils permettent des installations dans un monument classé par exemple.

- **Coût réduit :** si leur installation est souvent plus coûteuse que celle d'un réseau câblé, les réseaux sans-fil ont des coûts de maintenance très réduits. Sur le long terme, l'investissement est bien rentabilisé.

©2003-Cyber Networks-tous droits réservés

4. Aperçu des différentes normes radio

Comme toutes les technologies naissantes, les réseaux sans-fil font l'objet d'un nombre impressionnant de normes en constante évolution et malheureusement pas toujours interopérables… Voici un aperçu rapide des principales normes radio actuellement en vigueur :

4.1. Les normes radio WLANs

Plusieurs normes concurrentes se partagent le marché des WLANs :

- **IEEE 802.11 :** avec les volets 802.11b (Wi-Fi), 802.11a (Wi-Fi5) et 802.11g, c'est la norme principale.
- **ETSI HiperLan :** c'est une norme européenne concurrente du 802.11. Hiperlan 2 est en cours de préparation.
- **IEEE 802.15 :** ce protocole dont l'appellation commerciale est Bluetooth est très orienté WPANs mais reste encore utilisé dans certains WLANs.
- **HomeRF :** ce protocole est utilisé dans certains réseaux pour particuliers.

Actuellement, la majorité des WLANs est basée sur les normes IEEE 802.11 et en particulier la 802.11b. Le 802.11g est une amélioration du 802.11b qui va apporter un meilleur débit. Cette norme est promise à un bel avenir, en particulier en France où le 802.11a se heurte à la réglementation stricte de l'ART. Les normes IEEE 802.11 ont de très bonnes chances de devenir le standard incontesté pour les WLANs.

Voici un aperçu des différents volets du 802.11 :

802.11a	54Mbps en 5 GHz (5.15 à 5.35) sur 8 canaux. Non compatible avec la 802.11b ou 802.11g et non utilisable en France.
802.11b	11Mbps en 2.4 GHz sur 14 canaux.
802.11b.corl	Corrige les problèmes liés au MIB (Management Information Base, gestion des AP) dans le 802.11b
802.11d	802.11b en plus souple au niveau fréquence pour éviter les problèmes de régulations dans les pays du monde ayant une norme différente des Etats Unis
802.11e	Norme de qualité de service (QoS) pour applications multimédia (Téléphone, Video on Demande). S'applique sur le 802.11 a, b et g.
802.11f	Norme pour permettre l'utilisation d'infrastructures multi vendeur.
802.11g	54 Mbps en 2.4Ghz (pareil que le 802.11b). Utilise l'OFDM (orthogonal frequency division multiplexing). Directement compatible avec le 802.11b.
802.11h	802.11a en plus souple au niveau fréquence pour éviter les problèmes de régulations en Europe.
802.11i	Norme de chiffrement alternative au WEP. S'applique au 802.11 a, b et g.

©2003-Cyber Networks-tous droits réservés

4.2. Les normes radio WMANs et WWANs

En Europe, la plupart des WWANs actuels sont basés sur des technologies télécoms capables de transporter à la fois des données informatiques et de la voix :

- Le GSM (faible débit et facturation à la durée)
- Le GPRS (basé sur le GSM mais permettant des débits plus élevés et une facturation au volume de donnée échangé).
- Le futur UMTS qui permettra des applications beaucoup plus évoluées via des débits nettement plus élevés que le GSM / GPRS.

Les autres réseaux étendus civils reposent sur des protocoles radio traditionnels et propriétaires.

Des projets de création de WMANs basés sur des normes WLAN mis en place à l'échelle d'une ville sont actuellement à l'étude. La couverture de villes par des hot-spots publics étendus basés sur 802.11 pourrait concurrencer sérieusement ou venir en complément des protocoles télécoms, surtout l'UMTS. Une autre application des WMANs 802.11 envisagée est d'offrir un accès Internet haut débit dans des zones non couvertes par l'ADSL.

4.3. Les normes radio WPANs

Les WPANs reposent également sur des protocoles variés. Les antiques connexions IrDA (Infrarouge) laissent progressivement la place à des technologies radios. Les acteurs les plus sérieux sont alors Bluetooth (norme IEEE 802.15) et les normes Wi-Fi (IEEE 802.11) en mode IBSS.

L'homogénéisation avec les WLANs avantage nettement les normes 802.11 dans la course au standard, surtout pour les applications liées aux réseaux informatiques. Cependant Bluetooth, prochainement disponible en version 2.0, reste encore avec l'IrDA la technologie la plus utilisée pour les WPANs généralistes.

©2003-Cyber Networks-tous droits réservés

5. Les problématiques associées aux systèmes sans-fil

En faisant tomber la barrière de l'isolement physique sur lequel reposait la majeure partie de la sécurité interne des systèmes d'information, les réseaux sans-fil ont fait émerger des problématiques sécurité entièrement nouvelles.

En dépit de la variété des réseaux sans-fil, on retrouve dans tous les cas les mêmes problématiques mettant en péril le CID (Confidentialité, Intégrité, Disponibilité) des informations :

Utilisation d'un système sans-fil
=
Perte du confinement physique de l'information
→ Risque d'espionnage
+
Perte de l'isolement physique des systèmes d'information
→ Risque d'intrusion
+
Perte de la fiabilité des liens câblés
→ Risque de dénis de service

5.1. La perte du confinement physique de l'information

Les systèmes sans-fil fonctionnent généralement en mode diffusion : les ondes radios se propagent sur toute la zone de couverture de l'émetteur. Tout récepteur adapté situé à portée est en mesure de capter ces ondes, donc le trafic réseau, et de l'analyser.

La portée utile des émetteurs est très variable en fonction de la technologie utilisée, du matériel et de l'environnement : quelques mètres pour Bluetooth, une petite centaine de mètres pour un point d'accès 802.11b.

Cependant il faut absolument faire la distinction entre la portée utile et la porté d'attaque : un simple amplificateur étend grandement la portée d'un récepteur. Ces amplificateurs sont courants, peu coûteux et une simple boite de biscuits peut servir de base à un amplificateur artisanal pour carte 802.11 !

Pour un attaquant la zone de couverture radio réellement utile d'un WLAN s'étend largement au delà de la zone de contrôle physique d'une entreprise : pour peu que des points d'accès sans-fil non sécurisés existent dans son réseau, son système d'information peut être facilement espionné à distance par un simple PC portable équipé d'une carte sans-fil passive.

©2003-Cyber Networks-tous droits réservés

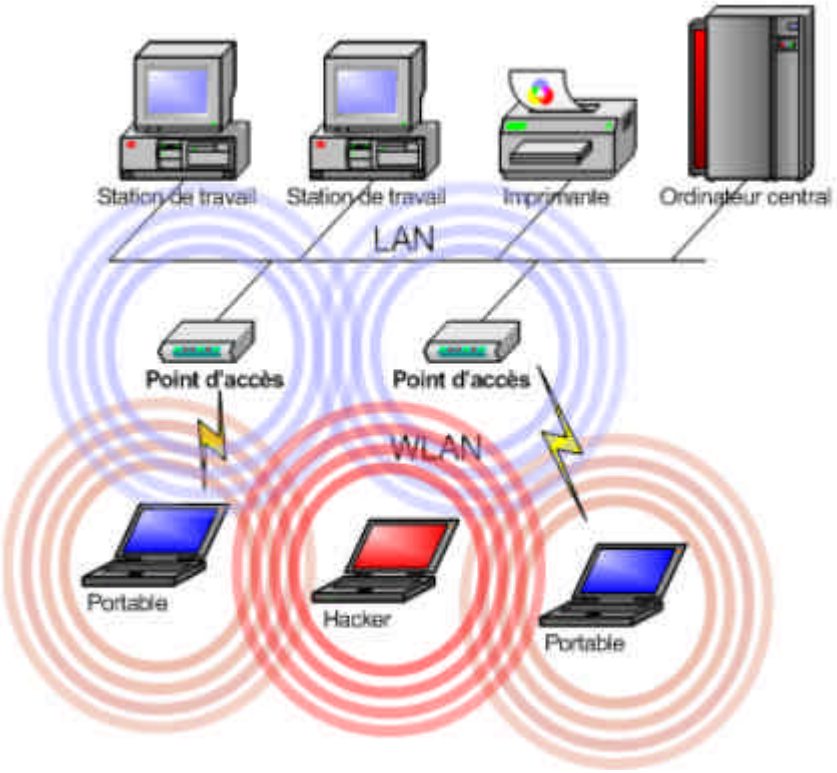


Figure 5 : Espionnage d'un WLAN

La mobilité des terminaux et les WPANs entraînent fréquemment la création de réseaux non sécurisés en dehors de l'entreprise. Un commercial synchronisant son PDA avec son portable en Bluetooth dans le train diffuse dans tout le wagon des informations parfois très critiques…

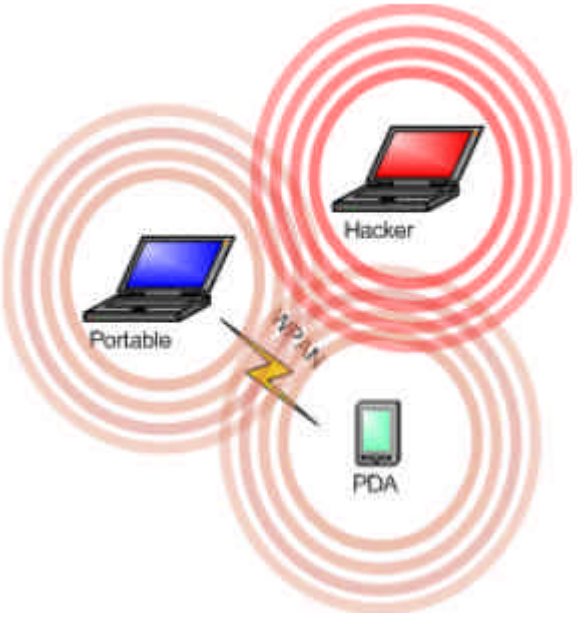


Figure 6 : Espionnage d'un WPAN

Les WPANs spécifiques sont également dangereux pour la confidentialité du système d'information : par exemple toutes les données saisies sur un clavier

©2003-Cyber Networks-tous droits réservés

sans-fil standard, dont les mots de passe, sont diffusées en clair dans tout le bâtiment !

En configuration par défaut presque aucun système sans-fil, excepté le GSM, n'offre un chiffrement satisfaisant du trafic sur le segment radio. Pour les réseaux Wi-Fi, le trafic passe tout simplement en clair avec une configuration par défaut ! Pire, les solutions de chiffrements proposées en standard dans le 802.11 comme le WEP sont notoirement inefficaces.

L'utilisation d'un système sans-fil non chiffré expose fortement la confidentialité des données. L'espionnage à distance de ce type de réseau est facile et sans risque pour l'attaquant.

5.2. La perte de l'isolement physique des systèmes d'information

Les systèmes sans-fil remettent en question les politiques de sécurité classiques. En effet la plupart des entreprises sont actuellement des villes fortifiées : des murailles bien conçues (firewalls, proxy…) et bien gardées (système de détection d'intrusion) isolent de l'extérieur les ressources internes critiques. Les défenses périphériques sont fortes mais, une fois dans la ville, les systèmes de sécurité sont faibles ou inexistants : le réseau interne est une zone considérée à tort comme sécurisée de nature (zone de confiance).

Tout équipement disposant d'une interface sans-fil active, que ce soit un point d'accès Wi-Fi ou un terminal utilisateur équipé d'un adaptateur réseau Bluetooth actif par exemple, est attaquable directement depuis l'extérieur. Ces équipements constituent alors autant de portes potentielles vers les ressources informatiques auxquelles ils sont connectés par le réseau câblé.

Les défenses périphériques de l'entreprise ne sont plus à même de sécuriser seules les ressources internes contre les intrusions : elles peuvent se retrouver complètement court-circuitées depuis l'extérieur. Dans le cas des équipements mobiles, ces défenses ne rentrent même plus en ligne de compte.

Une attaque contre un équipement via son interface sans-fil peut être menée sans équipement spécifique depuis n'importe quel point de la zone de couverture radio utile, donc depuis des zones non contrôlées physiquement par l'entreprise.

Le facteur aggravant est que la majorité des systèmes sans-fil sont conçus dans un esprit d'ouverture et de connectivité : tout est pensé pour faciliter l'accès au réseau au détriment de la sécurité.

5.2.1. L'ouverture sur l'extérieur des réseaux internes

En standard, les points d'accès d'un WLAN ne demandent pas d'authentification : les paramétrages par défaut sont pensés pour faciliter au maximum la vie des utilisateurs. En d'autres termes si un point d'accès est sorti de sa boite et branché sur le réseau, il va commencer à se signaler au niveau radio et à diffuser toutes les informations nécessaires pour que les

©2003-Cyber Networks-tous droits réservés

cartes sans-fil à portée se connectent. Toute demande de connexion sera acceptée sans autre forme de procès et le point d'accès ira jusqu'à chercher sur le serveur DHCP de l'entreprise des adresses IP libres pour les nouveaux venus !

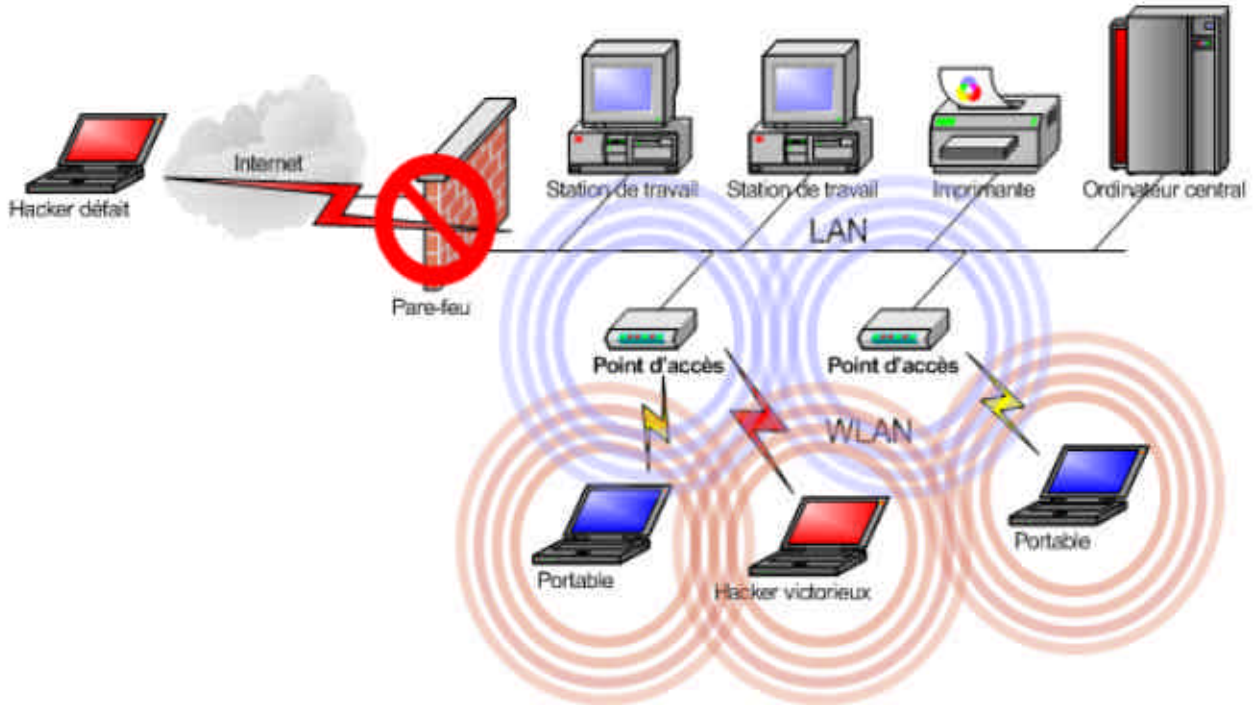


Figure 7 : Intrusion sur un LAN via un WLAN

Le pire est que les points d'accès constituant un WLAN sont généralement connectés sans précaution directement sur le LAN de l'entreprise et donnent donc accès au cœur des ressources informatiques internes peu sécurisées…

Un WLAN non sécurisé rend réellement triviale une intrusion à distance sur le réseau interne de l'entreprise et revient schématiquement à installer dans la rue une prise réseau brassée sur le LAN !

5.2.2. L'ouverture sur l'extérieur d'équipements utilisateurs

Un attaquant peut tenter de se connecter directement sur tout équipement disposant d'une interface sans-fil active en mode ad-hoc en établissant un WPAN pirate entre sa victime et sa propre machine. S'il y parvient, il lui est possible d'attaquer l'équipement lui-même et toutes les ressources qui lui sont connectées !

©2003-Cyber Networks-tous droits réservés

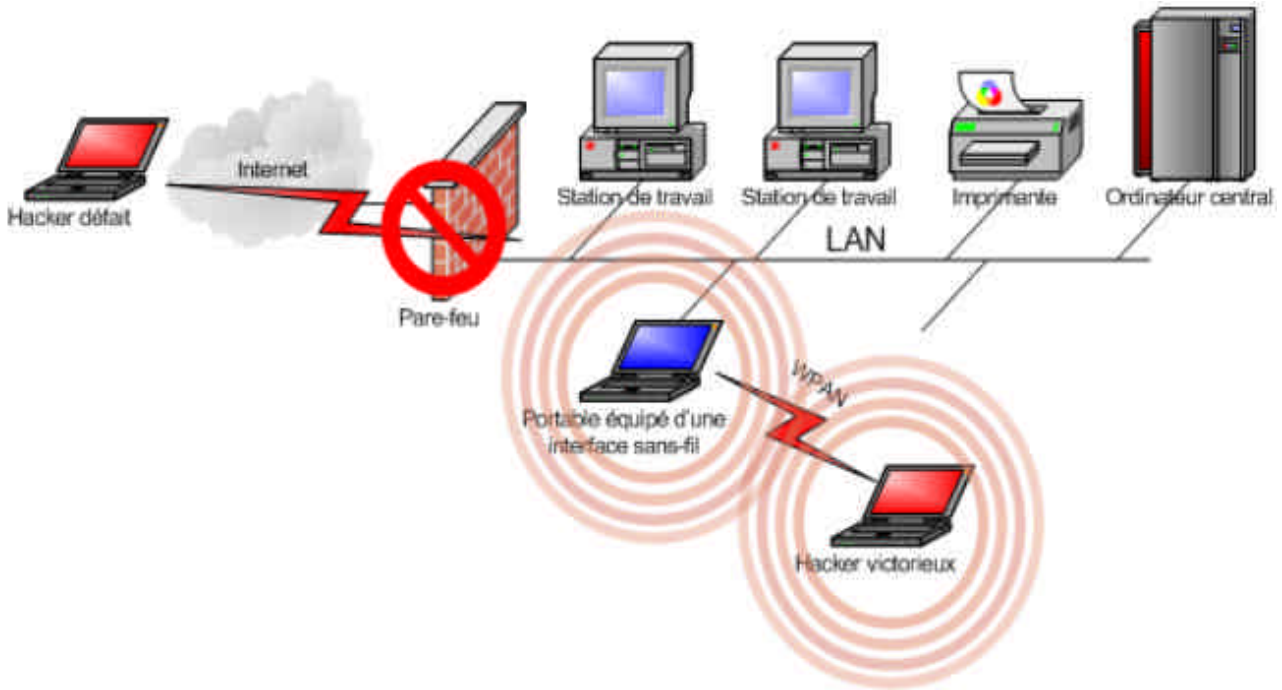


Figure 8 : Intrusion sur un LAN via un WPAN

Les équipements ciblés sont en grande partie des postes ou des terminaux utilisateurs, mobiles ou non. Ces derniers ne sont pas préparés à ce type de menace : jusqu'à présent une attaque informatique directe contre ces équipements présupposait une intrusion physique, un vol…

Il est devenu excessivement dangereux de se reposer exclusivement sur des défenses périphériques, même si elles sont fortes, pour prévenir les intrusions informatiques. L'ouverture sur l'extérieur des ressources internes à travers des systèmes sans-fil doit s'accompagner de la mise en place de mesures de sécurité adaptées comme par exemple :

- **L'intégration des systèmes sans-fil dans des architectures sécurisées (cloisonner les WLAN du LAN par exemple).**
- **La mise en place de solutions d'authentification des utilisateurs et des équipements matériels.**
- **La sécurisation des terminaux mobiles ou fixes exposés.**
- **Le renforcement de la sécurité interne générale du système d'information.**

5.2.3. La maîtrise délicate de l'espace radio

Si un WLAN mal intégré remet en cause la sécurité de l'entreprise, que dire des dispositifs sans-fil connectés au LAN à l'insu des responsables informatiques ?

En interne, cela peut être un point d'accès connecté au réseau par un utilisateur inconscient ou plus couramment encore par un informaticien faisant quelques tests. Ces points d'accès, généralement qualifiés de renégats, sont bien plus courants dans les entreprises que l'on pourrait l'imaginer et ne

©2003-Cyber Networks-tous droits réservés

sont bien sûr jamais sécurisés. On retrouve l'épineuse problématique des modems non contrôlés…

Nous estimons qu'actuellement environ 20% des entreprises françaises hébergent au minimum un point d'accès Wi-Fi renégat.

La plupart des équipements connectés au réseau par câble et disposant d'une interface sans-fil sont également éligibles au rang de point d'accès renégat : un PC sur le LAN avec une carte 802.11b active en mode had-hoc est une véritable passerelle vers les ressources informatiques de l'entreprise.

Le problème est que ces interfaces sans-fil, d'ailleurs rarement utilisées et intégrées dans la politique de sécurité, prolifèrent littéralement sur les PC portables (interfaces IrDA, cartes PCMCIA 802.11b…), les PDA (interfaces IrDA et Bluetooth) et même les stations de travail (Intel a annoncé récemment l'intégration d'interfaces 802.11b directement sur ses cartes mères via la technologie Centrino).

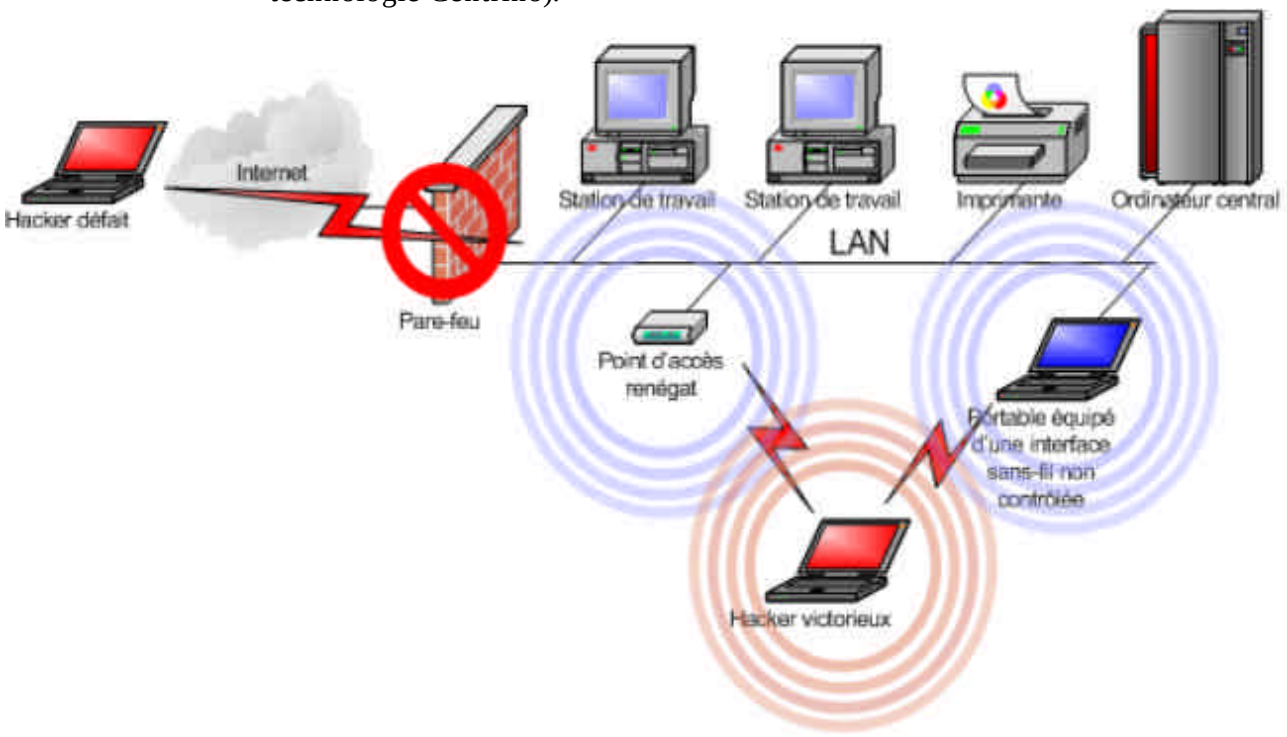


Figure 9 : Intrusion sur un LAN via un système sans-fil renégat

Il faut donc bien être conscient que les problématiques sécurité des réseaux sans-fil sont à prendre en compte dans toutes les entreprises, même dans celles n'ayant pas comme projet d'utiliser un WLAN.

Enfin la baisse des prix et la miniaturisation des équipements sans-fil font que les pirates n'hésitent plus à utiliser des points d'accès comme vecteur d'attaque. Plusieurs attaques sont envisageables, par exemples :

- L'installation d'un point d'accès Wi-Fi renégat directement sur le réseau câblé de leurs victimes.

©2003-Cyber Networks-tous droits réservés

- L'insertion à distance dans un WLAN d'un point d'accès pirate via les mécanismes de chaînage d'équipement ou de mise en haute disponibilité.
- La création d'un WLAN pirate parallèle sur lequel les utilisateurs vont se connecter automatiquement en pensant être sur le réseau de l'entreprise.

L'audit régulier de l'espace radio de l'entreprise est important pour détecter les équipements non autorisés et faire le point sur la sécurité des systèmes sans-fil.

5.3. La perte de la fiabilité des liens câblés

La qualité de service sur un réseau sans-fil est un point sensible. Si elle a été relativement bien maîtrisée dans le cadre de la téléphonie mobile, elle reste un sujet à problème pour les WLANs ou les liaisons point à point.

En effet la qualité finale d'une connexion réseau radio est influencée par de nombreux paramètres extérieurs très divers : la distance entre l'émetteur et le récepteur, la pollution de la bande de fréquence utilisée, le nombre d'utilisateurs se partageant la bande passante du point d'accès… Maintenir une qualité de service optimale dans des conditions de production normales nécessite une infrastructure réellement bien pensée et adaptée aux besoins.

Cependant cela devient nettement plus complexe quand il faut prendre en compte la disponibilité de l'infrastructure et les risques d'atteinte volontaire à la qualité du service.

Les communications radio ont un long historique, particulièrement militaire, en matière d'attaque par déni de service. Les guerres récentes ont démontré que les armées modernes sont capables de mettre rapidement et à distance une véritable chape de plomb sur toutes les communications radio de l'ennemi. Les principes issus des techniques militaires de déni de service (DoS) radio sont tout à fait utilisables dans le milieu civil.

Il est impossible de faire le tri dans les ondes avant que celles-ci n'atteignent les équipements radio : dès lors créer une interruption ou une perturbation du service est relativement aisé, qu'elle soit temporaire (simple brouillage par pollution de bande de fréquence) ou de longue durée (destruction à distance des équipements radio via des bombes électromagnétiques artisanales).

En plus des attaques orientées radio, de nombreuses attaques DoS réseaux ou logiques sont dès à présent opérationnelles et faciles à mettre en œuvre sans équipement spécifique pour perturber le fonctionnement des réseaux sans-fil.

©2003-Cyber Networks-tous droits réservés

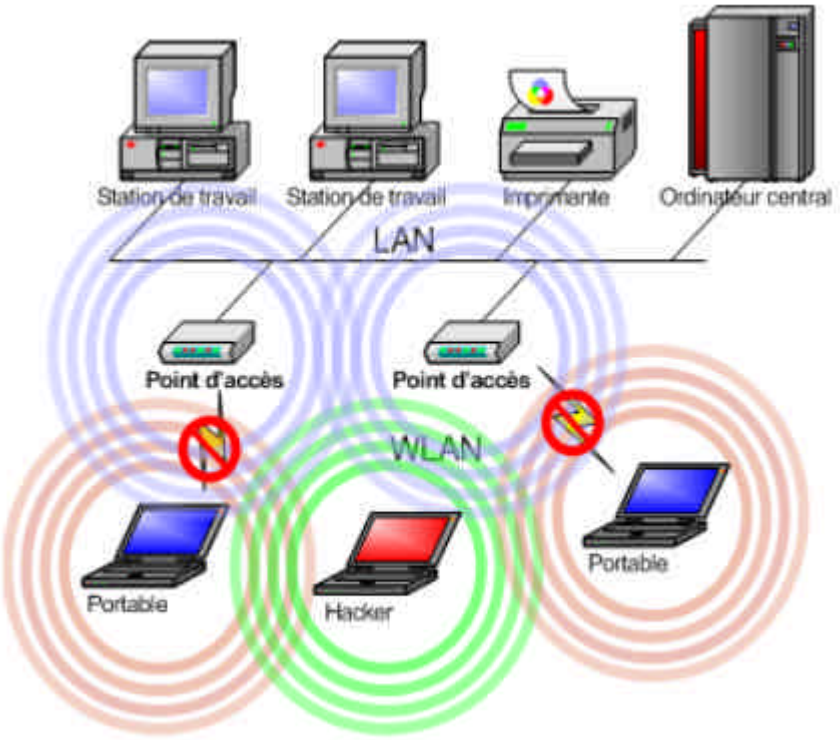


Figure 10 : Dénis de service sur un WLAN

Les architectures sans-fil doivent être bien étudiées pour optimiser la qualité de service et réduire les conséquences d'attaques par déni de service. Dans les situations où la disponibilité du service est primordiale, l'utilisation des principales technologies sans-fil civiles actuelles reste un pari risqué.

©2003-Cyber Networks-tous droits réservés

6. La menace

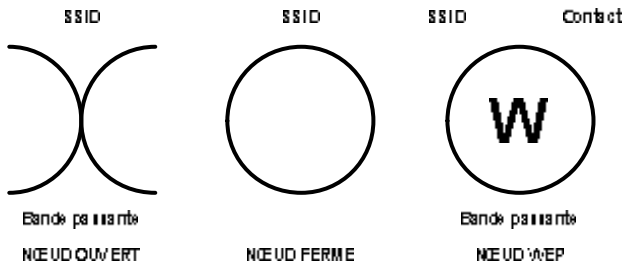
Mal intégrés, les systèmes sans-fil ouvrent une voie royale aux pirates informatiques. Ces derniers ne s'y sont d'ailleurs pas trompés : leurs communautés sont en pleine ébullition. A présent nous estimons que les attaques réussies portées via les systèmes sans-fil ont largement dépassé en nombre les attaques via les accès Internet, et pour cause :

- **La prise de risque est faible** : Prendre d'assaut un réseau sans-fil fait prendre très peu de risque à l'attaquant, voir aucun dans le cas du simple espionnage : les actions sont menées à distance et ne laissent pas de traces exploitables pour remonter jusqu'au coupable.

- **Le gain potentiel est énorme** : Quel que soit l'objectif du pirate, espionnage, intrusion ou simple déni de service, son "retour sur investissement" peut être très important, d'autant plus que contrairement aux attaques Internet, les grandes entreprises ou organisations gouvernementales sont encore très vulnérables.

- **Les compétences nécessaires sont minimes** : Un simple portable, voir un PDA, équipé d'une carte 802.11b et un logiciel trouvé sur Internet peut pirater automatiquement 80% des points d'accès et donner accès aux LANs…

Ce n'est donc pas un hasard si le war-driving (détection et piratage automatisé de réseaux sans-fil vulnérables à bord d'une voiture) devient une véritable mode dans les centres urbains. Aux Etat-Unis, certains sont même passés au war-flying (même principe à bord d'un hélicoptère) ou mettent en place un système de tag fait à la craie (war-chalking) indiquant la proximité et les caractéristiques d'un point d'accès :



La problématique sécurité des systèmes sans-fil est bien réelle et ne relève pas de la paranoïa aiguë : les failles existent, sont faciles à exploiter et des milliers de pirates n'ont de cesse de s'y engouffrer, par jeu ou pour des raisons plus malsaines : espionnage, intrusion, déni de service…

©2003-Cyber Networks-tous droits réservés

7. Les méthodes de sécurisation

S'il est clair que les problématiques de sécurité posées par les réseaux sans-fil sont réelles et complexes, elles ne restent heureusement pas sans réponse. En effet, des systèmes éprouvés, venus en grande partie du monde de la sécurité LAN et Internet, permettent de sécuriser simplement et efficacement les systèmes sans-fil ou de se prémunir d'une utilisation néfaste.

La première et principale solution est de bien prendre en compte les technologies sans-fil dans la réflexion sur la sécurité globale de l'entreprise.

Les réseaux sans-fil pouvant avoir des formes et des applications très variées, il est impossible de parler de solution de sécurité clé en main. Il est évident que l'on ne sécurise pas un WLAN comme un WPAN ou un réseau privé comme un hot-spot public. Chaque projet et chaque cas est réellement unique et doit être étudié puis intégré avec soin.

Cependant il est possible de dégager des concepts généraux qui sont autant de guides dans la définition d'une solution de sécurité :

7.1. Intégrer les réseaux sans-fil dans une architecture sécurisée

Les réseaux sans-fil doivent être déployés dans des architectures sécurisées pour limiter les risques d'une intrusion ou ses conséquences. Les principes généraux à respecter sont :

7.1.1. Le cloisonnement des réseaux

Il est très important de cloisonner les WLANs des LANs afin d'éviter que les points d'accès donnent directement sur le réseau interne de l'entreprise en cas d'intrusion.

La partie câblée d'interconnexion des points d'accès doit être dédiée à cette seule utilisation (câblage physiquement séparé) et doit être implémentée comme une zone démilitarisée (DMZ) à part entière : un firewall doit impérativement filtrer le trafic entre le WLAN et le LAN.

Principe de base : Un WLAN = Une DMZ

Ce type d'architecture permet non seulement de sécuriser les ressources internes du réseau vis-à-vis du WLAN mais également de contrôler la quantité d'information diffusée sur la partie sans-fil.

©2003-Cyber Networks-tous droits réservés

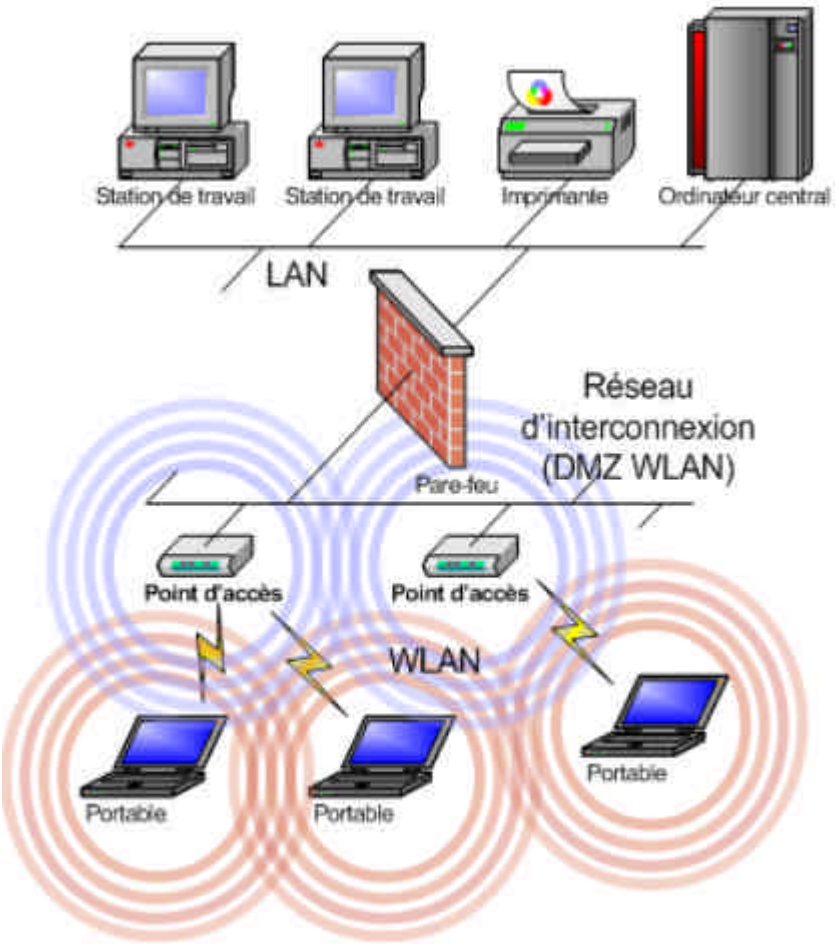


Figure 11 : Cloisonnement du WLAN et du LAN

Lorsque plusieurs populations différentes d'utilisateurs doivent être gérées sur la même infrastructure WLAN, il est également intéressant de mettre en place des VLANs sur la partie d'interconnexion câblée.

7.1.2. La sécurisation des équipements d'interconnexion

Il est important de bien sécuriser les équipements d'interconnexion (points d'accès, points d'extension…). En effet ils sont vulnérables à plus d'un titre :

- Ils ont des fonctionnalités de chaînage et de mise en haute disponibilité exploitables par un attaquant pour insérer un point d'accès pirate sur le réseau.
- Ils ont des interfaces d'administration potentiellement vulnérables depuis la partie radio et câblée.
- Ils sont physiquement très exposés (port d'administration console…).
- Ils ont des configurations par défaut très peu sécurisées (pas de chiffrement ni d'authentification pour l'administration).

©2003-Cyber Networks-tous droits réservés

7.1.3. La sécurisation des ressources informatiques internes

Il est devenu essentiel de mettre en place des systèmes de sécurité en profondeur sur le LAN pour compléter les défenses périphériques et sécuriser le cœur des systèmes d'information.

La sécurisation interne peut s'appuyer sur plusieurs points. Par exemple :

- La sécurisation réseau : séparation des serveurs et des stations de travail au niveau réseau (utilisation de réseaux IP différents, de VLANs…), contrôle d'accès au réseau câblé, installation de firewalls logiciels dédiés sur les serveurs…
- La sécurisation système et applicative des serveurs : mise à jour régulière via les hotfix de sécurité, blindage des moyens d'administration…
- La mise en place de sondes de détection d'intrusion surveillant le trafic réseau sur le LAN interne et les serveurs.

7.2. Chiffrer systématiquement le trafic sur les segments sans-fil

La perte du confinement physique de l'information fait qu'il est impossible d'empêcher un espion de récupérer le trafic réseau transitant sur un lien sans-fil. Afin de sauvegarder la confidentialité et l'intégrité des données circulant sur ce type de lien, il est indispensable de chiffrer le trafic de telle sorte qu'il ne soit intelligible que par les destinataires légitimes.

Les techniques de saut de fréquence radio comme FHSS (Frequency Hopping Spread Spectrum) implémentées sur les WLANs sont parfois présentées comme un atout sécurité contre l'espionnage. Ce n'est absolument pas le cas dans les réseaux civils car contrairement aux implémentations FHSS sécurisées utilisées par les militaires, la séquence de saut sur un WLAN est volontairement calculable par tous les récepteurs !

Il est donc indispensable de mettre en place un système de chiffrement au niveau réseau pour sécuriser le trafic sur la partie radio :

7.2.1. Chiffrement pour les WLANs

7.2.1.1. Les solutions spécifiques 802.11

Par défaut le trafic sur un WLAN n'est pas chiffré : devant cet état de fait particulièrement critique, les initiateurs du 802.11 ont conçu le protocole WEP (Wired Equivalent Privacy) qui est censé offrir un niveau de sécurité équivalent à celui obtenu par une connexion câblée.

Le WEP utilise l'algorithme de chiffrement RC4 avec une clé unique et statique connue de tous les points d'accès et des clients. Cette clé, véritable secret partagé dans tout le WLAN, sécurise le trafic uniquement sur la partie radio, entre les terminaux mobiles et les points d'accès.

©2003-Cyber Networks-tous droits réservés

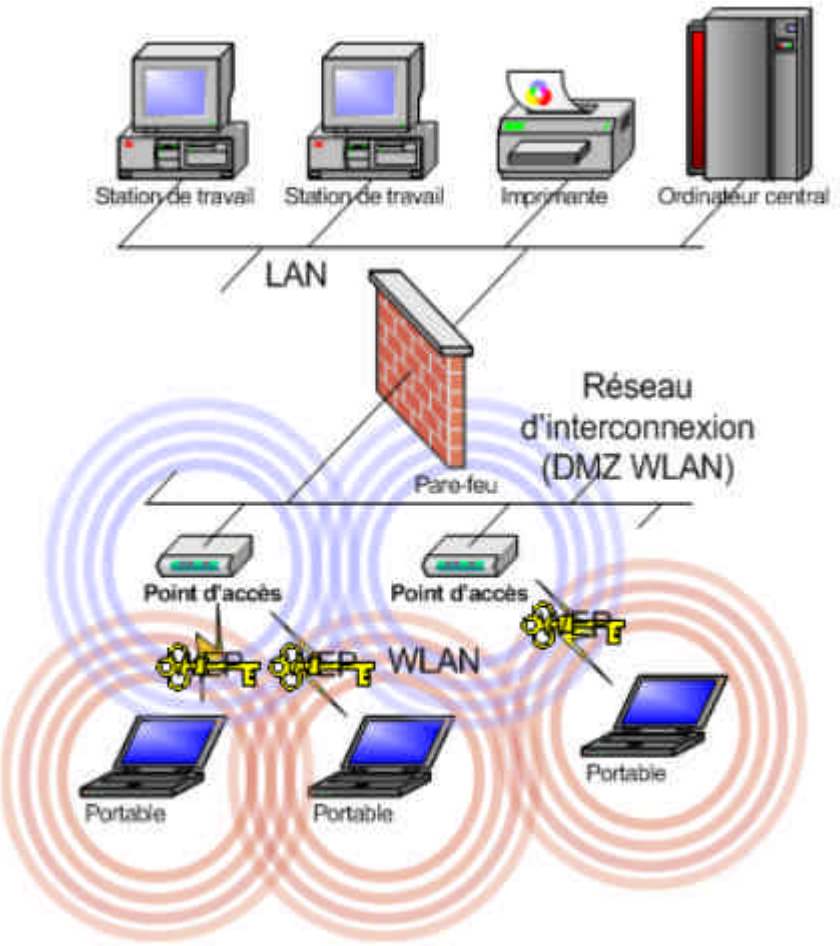


Figure 12 : Chiffrement pour WLAN via WEP

Le WEP souffre de plusieurs graves failles de sécurité qui le rendent totalement inefficace :

- L'implémentation de RC4 utilisée par le WEP est extrêmement peu sécurisée. Les clés de chiffrement sont statiques, très exposées par le protocole cryptographique (voir les failles exploitant les vecteurs d'initialisation IV) et ne permettent au final qu'une confidentialité très limitée pour les données et ce quelque que soit leurs longueurs (128bits maximum). Un attaquant analysant le trafic réseau sécurisé par le WEP peut casser sans peine le chiffrement en quelques heures d'écoute. Ces attaques sont d'ailleurs automatisées dans plusieurs logiciels de hack dont, par exemple, Airsnort.

- Le WEP n'implémente aucun contrôle d'intégrité des paquets : il est possible de changer des bits dans un paquet chiffré sans que ce soit détecté par le protocole. La possibilité de forger facilement des paquets est à la base de nombreuses attaques sophistiquées.

- Le WEP ne dispose pas de mécanisme anti-rejeu. Il est possible pour un attaquant de rejouer plusieurs fois une séquence enregistrée.

©2003-Cyber Networks-tous droits réservés

La faiblesse du WEP est reconnue et son exploitation est complètement automatisée dans de nombreux outils de piratage. Les constructeurs de matériel ont librement amélioré le protocole par des évolutions souvent propriétaires en gardant comme base RC4, seul algorithme de chiffrement compatible avec la puissance de calcul des équipements actuels.

Ces améliorations sont très souvent inspirées des travaux du groupe de travail IEEE 802.11i (volet sécurité pour le 802.11) et du prochain WPA (Wi-Fi Protected Access). Les améliorations classiques sont :

- La mise en place de systèmes de management des clés de chiffrement type TKIP (Temporal Key Integrity Protocol) pour doter le WEP de clés dynamiques et uniques pour chaque utilisateur. Ces systèmes nécessitent un processus d'authentification comme 802.1x/EAP (voir la partie 7.3.2 sur l'authentification) pour dériver le matériel cryptographique servant à générer la clé de base et un protocole de renouvellement des clés.

- L'ajout de contrôles d'intégrité type MIC (Message Integrity Check) et de systèmes de vérification des séquences pour éviter qu'un attaquant puisse forger ou rejouer facilement des paquets.

Ces améliorations adressent la majeure partie des vulnérabilités du WEP. Bien implémentées, la plupart de ces solutions "WEP amélioré" offrent un niveau de sécurité satisfaisant pour des environnements où la confidentialité absolue n'est pas vitale. Elles sont cependant très dépendantes des matériels utilisés donc peu interopérables, intimement liées à la mise en place du système d'authentification et dans l'ensemble assez peu pérennes.

L'arrivée fin 2003 du WPA, véritable successeur du WEP en attendant 802.11i, va formaliser et homogénéiser l'ensemble de ces améliorations et doter les réseaux 802.11 d'une solution de sécurité standard et efficace (voir la partie 7.2.3.1 sur les futures solutions de chiffrement).

7.2.1.2. Les tunnels VPN basés sur IPSec

Actuellement, la seule solution parfaitement éprouvée et stabilisée pour assurer la confidentialité totale des données sur un WLAN est l'utilisation de tunnels VPN basés sur IPSec.

Cette solution requiert que le WLAN soit séparé des ressources de l'entreprise avec une passerelle firewall/VPN (voir la partie sur le cloisonnement en 7.1.1). Le WLAN et le réseau d'interconnexion des points d'accès sont alors considérés comme une zone pratiquement publique. Un simple accès sur le WLAN ne donne accès à aucune ressource intéressante.

L'accès aux ressources nécessite pour le terminal mobile de s'authentifier puis de monter un tunnel avec la passerelle firewall/VPN. Le tunnel VPN sécurise alors le trafic sur toute la partie à risque par un chiffrement fort.

©2003-Cyber Networks-tous droits réservés

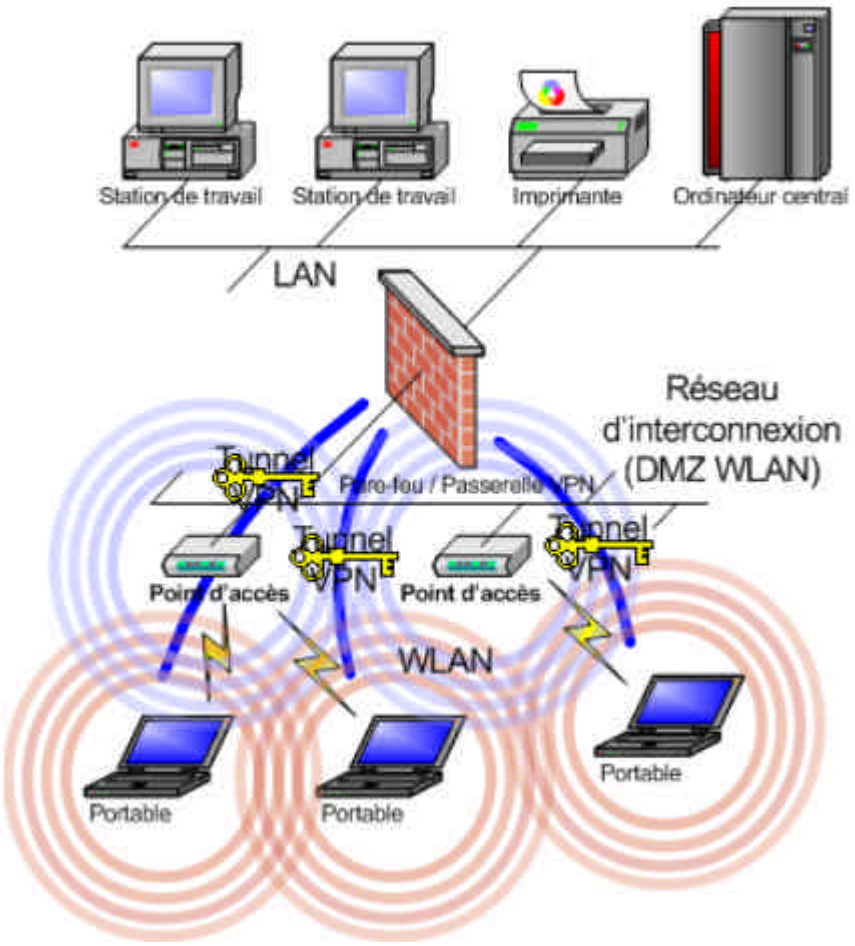


Figure 13 : Chiffrement pour WLAN via IPSec

Cette solution nécessite de disposer d'un client VPN sur les terminaux mobiles. Cela peut être un client lourd ou, pour les hot-spot public, une solution "clientless" utilisant les fonctionnalités VPN disponibles sur les systèmes d'exploitation récents ou intégrées dans les clients des adaptateurs sans-fil.

L'utilisation de tunnels VPN décharge le matériel, et en particulier les points d'accès, des opérations de chiffrement / déchiffrement. L'impact en terme de gain de performance n'est pas négligeable.

Un autre intérêt majeur de la solution VPN est qu'elle facilite le roaming des terminaux mobiles : en effet les informations cryptographiques n'ont plus à être partagées entre les différents points d'accès constituant le WLAN.

Le seul défaut possible de cette solution est qu'elle rend impossible toute communication directe entre les terminaux mobiles. Cependant dans la plupart des architectures il s'avère que ce défaut devient un atout sécurité.

Etant complètement indépendante des technologies et des matériels utilisés sur le WLAN, la solution VPN est très sécurisée mais également beaucoup plus pérenne que les solutions spécifiques aux réseaux 802.11. De plus elle

©2003-Cyber Networks-tous droits réservés

peut réutiliser des technologies et des équipements déjà en place dans la majorité des architectures.

7.2.1.3. Les futures solutions de chiffrement 802.11

Le futur standard de sécurité pour les réseaux 802.11 est le volet 802.11i de la norme. Ce standard ne sera probablement pas opérationnel avant l'été 2004.

Pour le chiffrement, 802.11i propose deux solutions :

- TKIP qui est une amélioration du WEP utilisant une meilleure implémentation de RC4, une gestion dynamique des clés ainsi que des contrôles d'intégrité et de séquence des paquets. Cette solution formalise la plupart des améliorations constructeurs actuellement utilisées et ne demande qu'un simple upgrade firmware sur les matériels récents.

- AES/CMP qui est une solution nettement plus sécurisée utilisant le récent standard de chiffrement par bloc AES (Advanced Encryption Standard). Ce sera la réelle solution sécurisée native 802.11 mais cela demandera une évolution des matériels pour disposer de la puissance de calcul nécessaire à AES.

Courant 2003 la branche TKIP de la future norme 802.11i sera disponible sous le nom de WPA (Wi-Fi Protected Access). Ce standard poussé par la Wi-Fi Alliance vise à remplacer au plus vite le WEP tout en gardant une compatibilité avec le 802.11i et les matériels actuellement en production. Le WPA va normaliser et remplacer rapidement les différentes améliorations propriétaires des constructeurs.

A plus long terme les points d'accès feront probablement office de passerelles VPN et des tunnels basés sur IPSec sécuriseront les communications radio entre les points d'accès et les terminaux mobiles.

7.2.2. Chiffrement pour les WWANs

Dans le cadre des WWANs, et en particulier ceux sur infrastructure télécom publique, l'utilisation de tunnels VPN est clairement la meilleure solution pour maîtriser et assurer la confidentialité des communications de bout en bout.

Il est important de garder à l'esprit que le chiffrement sur une communication type GSM ou GPRS est assurée par le protocole télécom uniquement sur la partie radio, entre le terminal mobile et l'antenne. En revanche, entre l'antenne et la destination finale (le réseau de l'entreprise), le trafic traverse parfois des zones publiques peu ou pas sécurisées (réseaux inter-opérateurs ou même Internet) !

L'établissement de tunnels VPN entre les terminaux mobiles et une passerelle placée sur le réseau de l'entreprise permet de sécuriser efficacement ce type de

©2003-Cyber Networks-tous droits réservés

connexions en faisant totalement abstraction de la sécurité de l'infrastructure réseau sur laquelle transite les données :

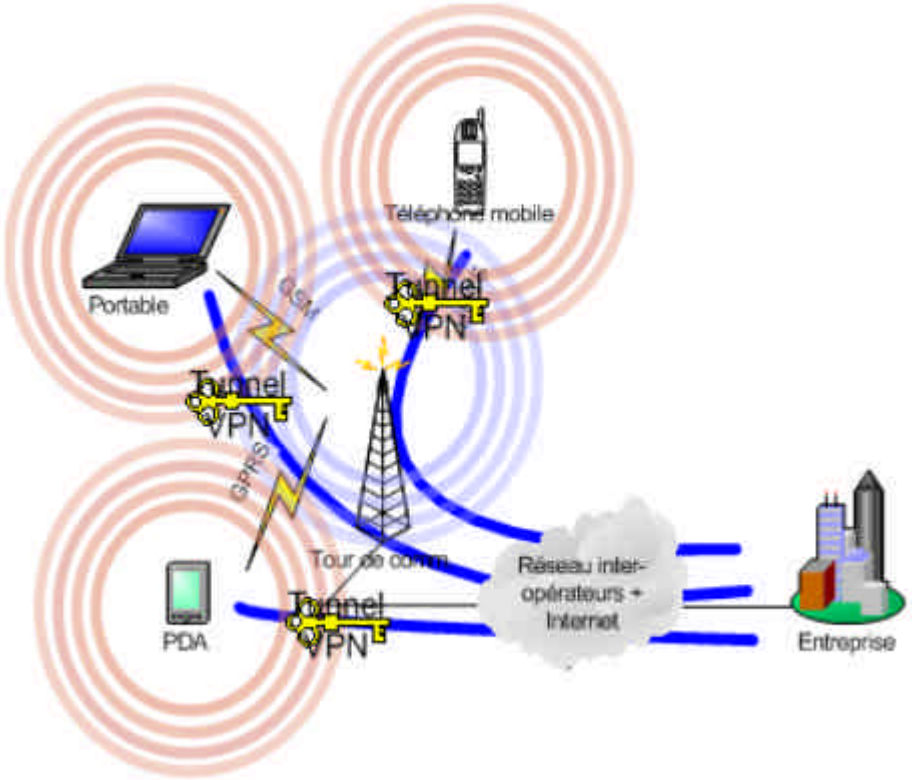


Figure 14 : Chiffrement pour un WWAN via IPSec

7.2.3. Chiffrement pour les WPANs

La gestion de la confidentialité des données échangées sur un réseau ad-hoc n'a pas encore de solution satisfaisante : en effet les possibilités de chiffrement offertes par les normes WPANs sont généralement très limitées et peu paramétrables.

Le problème principal est que le caractère basique des équipements utilisés dans ce type de réseau rend souvent impossible la modification ou l'ajout d'une couche sécurité supplémentaire (type tunnel SSL) pour assurer le chiffrement.

Coté normes WPAN, Bluetooth propose un système de chiffrement relativement efficace mais optionnel et donc peu utilisé par les équipements. 802.11 et la majorité des WPANs propriétaires ne proposent quant à eux aucun système de chiffrement correct.

En attendant les prochaines solutions de chiffrement pour WPAN qui seront éventuellement implémentées dans Bluetooth2 et le 802.11i, la meilleure protection est encore de faire en sorte qu'aucune donnée sensible ne circule sur un WPAN. La sécurité passe donc plus par la sensibilisation des utilisateurs que par un moyen technique.

©2003-Cyber Networks-tous droits réservés

7.3. Mettre en place des systèmes de contrôle d'accès réseau

Que ce soit sur un WLAN d'entreprise pour s'assurer que seuls les employés autorisés accèdent au réseau ou sur un hot-spot public pour pouvoir facturer les clients, il est nécessaire de mettre en place des solutions d'authentification des utilisateurs.

Il est également très important de mettre en place des solutions permettant aux terminaux mobiles d'authentifier les réseaux sur lesquels ils se connectent, principalement pour contrer les attaques type "man in the middle".

Ce document traite essentiellement des systèmes de contrôle d'accès sur les réseaux sans-fil en mode infrastructure. En effet pour les WPANs les systèmes d'authentification restent très limités.

7.3.1. L'authentification basique sur les réseaux 802.11

Par défaut aucune authentification n'est demandée pour l'accès à un WLAN. Cependant, trois options sont disponibles sur pratiquement tous les points d'accès 802.11 :

- L'utilisation d'un SSID (identifiant de réseau sans-fil) complexe qui devra être connu du client pour se connecter sur le point d'accès. Il est important de désactiver la diffusion du SSID dans les balises (beacons) émises par les points d'accès. Le SSID n'est pas une mesure de sécurité en soi mais plutôt un mécanisme de gestion du chevauchement de WLAN.

- L'utilisation d'une clé WEP statique unique entrée "en dur" sur chaque client et chaque point d'accès. Cette clé agit alors comme un secret partagé. C'est une solution lourde à gérer et très peu sécurisée.

- Le filtrage par adresse MAC. La plupart des points d'accès sont capables de gérer une liste des adresses MAC des cartes réseaux autorisées à accéder au WLAN. La gestion de ces listes, si elle n'est pas effectuée en central sur un serveur RADIUS, est très fastidieuse et le spoofing (usurpation) d'adresse MAC permet de contourner facilement cette sécurité.

Les solutions 802.11 basiques ne sont clairement pas suffisantes pour sécuriser l'accès à un WLAN.

©2003-Cyber Networks-tous droits réservés

7.3.2. Les solutions 802.1x/EAP (Extensible Authentication Protocol) pour WLAN

Les constructeurs ont rapidement été obligés de proposer sur leurs matériels des systèmes d'authentification palliant aux faiblesses des standards WLANs. La plupart se sont inspirés des projets de l'IEEE pour le 802.11i et ont donc proposé des implémentations souvent propriétaires de 802.1x / EAP adaptées aux WLANs.

802.1x est un système de contrôle d'accès réseau par port disponible sur tous les réseaux 802 (donc LAN ou WLAN). Basiquement les ports d'un équipement d'interconnexion (switch ou point d'accès) utilisant 802.1x ont deux états possibles :

- **Fermé** : c'est l'état par défaut. Un port fermé ne permet la communication qu'entre le client et un système d'authentification (serveur RADIUS généralement). Une fois que le client s'est authentifié avec succès, le port s'ouvre.

- **Ouvert** : cet état demande que le client connecté se soit authentifié avec succès. Un port ouvert laisse tout passer et se referme dès que le client se déconnecte.

802.1x sert de support pour EAP. EAP n'est pas un système d'authentification en soi mais un protocole de transport de l'authentification. EAP s'appuie donc obligatoirement sur une ULA (Upper Layer Authentication) pour l'authentification proprement dite. Les ULA sont basées soit sur une vérification d'un login / password, soit sur un système de certificats.

Le couple 802.1x / EAP est le socle du système d'authentification (ULA). De l'ULA utilisée découlent les principales implémentations de EAP. Selon les cas l'authentification est simple (le réseau authentifie le client) ou double (le réseau authentifie le client et le client authentifie le réseau) :

- **LEAP (Lightweight EAP)** : EAP développé par Cisco de type challenge-response basé sur un serveur RADIUS et un login / password.

- **EAP-TLS (EAP with Transport Layer Security)** : EAP basés sur des certificats gérés manuellement coté clients et coté serveurs.

- **PEAP (Protected EAP)** : EAP utilisant un certificat coté serveur et une authentification par login / password de l'utilisateur.

- **EAP-TTLS (EAP with Tunneled Transport Layer Security)** : EAP très similaire au PEAP.

L'implémentation de cette solution requiert systématiquement un serveur d'authentification type RADIUS s'appuyant sur une source d'authentification intégrée ou externe (service d'authentification forte, annuaire LDAP…).

©2003-Cyber Networks-tous droits réservés

Certaines implémentations nécessitent également une infrastructure simplifiée de gestion des certificats (PKI).

Le processus d'authentification 802.1x/EAP est indispensable au système type TKIP pour la génération des clés de chiffrement dynamiques. En effet TKIP utilise les informations issues du processus d'authentification pour dériver les informations cryptographiques servant à créer les clés de chiffrement sur le client et le point d'accès.

Le niveau de sécurité offert par une implémentation de ce type de solution varie selon les options choisies par le constructeur du matériel et selon l'ULA utilisée. Une bonne implémentation permet un contrôle d'accès au WLAN bien sécurisé et natif 802.11.

En attendant la normalisation de l'implémentation de 802.1x/EAP par le standard WPA (Wi-Fi Protected Access) puis 802.11i, le plus grand défaut de cette solution reste sa dépendance aux choix des constructeurs de matériel, donc une interopérabilité réduite et une pérennité parfois incertaine.

7.3.3. L'authentification intégrée aux systèmes VPN pour WLAN ou WWAN

L'alternative à l'utilisation de TKIP (chiffrement) + 802.1x/EAP (authentification) est la mise en place d'une solution VPN. Les tunnels VPN assurent le chiffrement du trafic par IPSec mais nécessitent obligatoirement l'utilisation d'un mécanisme d'authentification des utilisateurs lors du processus d'établissement du tunnel.

Dans ce cas, lauthentification n'est pas effectuée par les points d'accès du WLAN mais par le firewall/passerelle VPN cloisonnant le réseau (voir schéma numéro 13) sur la base d'une source d'authentification interne ou externe : serveur RADIUS, annuaire LDAP, serveur d'authentification forte…

Cette solution permet de s'affranchir partiellement de la sécurité et de la structure du réseau sans-fil : ce dernier n'assure plus que la liaison physique et est considéré comme un zone publique, au même titre que tout ce qui devant un firewall en frontal d'Internet.

Sur tous les réseaux sans-fil où 802.1x/EAP n'est pas implémentable, donc en pratique sur tous les réseaux autres que les WLANs 802.11, l'authentification intégrée dans l'établissement du tunnel VPN est la seule alternative possible.

7.3.4. Les futures solutions d'authentification

A court terme la norme WPA va standardiser le système 802.1x/EAP pour les WLANs et homogénéiser son implémentation par les constructeurs de matériels. Ce système sera toujours utilisé dans la future norme 802.11i.

Par contre le WPA et le 802.11i ne normaliseront pas la partie supérieure du système, à savoir l'ULA utilisée par EAP. A ce niveau tout reste ouvert mais la solution idéale est l'utilisation d'une PKI adaptée aux contraintes spécifiques

©2003-Cyber Networks-tous droits réservés

des réseaux sans-fil. Cette implémentation d'EAP, qui serait la seule à adresser les dernières grosses vulnérabilités potentielles du système d'authentification 802.1x/EAP, n'existe pas à l'heure actuelle.

Pour ce qui est des systèmes d'authentification utilisés par la solution VPN, ils sont connus et stabilisés depuis longtemps.

7.4. Auditer l'espace radio de l'entreprise

Au vu des risques posés par les systèmes sans-fil, il devient de plus en plus critique pour toute entreprise de maîtriser et de surveiller son espace radio. Pour se faire, plusieurs types d'audit peuvent être menés de façon régulière avec des objectifs variés :

7.4.1. Détecter et inventorier les équipements sans-fil

L'audit de détection est important pour toute entreprise disposant ou non d'un système sans-fil. Il a pour but d'inventorier les équipements radio non autorisés actifs sur différentes plages du spectre radio. L'objectif est alors de maîtriser la prolifération des points d'accès renégats et de dresser un état des lieux des systèmes sans-fil utilisés.

7.4.2. Valider la sécurité d'un système existant

Il est important de valider régulièrement l'architecture et les configurations mises en place afin de connaître les vulnérabilités éventuelles du système et pouvoir y pallier avant qu'un pirate ne les exploite. Si les outils sont souvent spécifiques aux réseaux sans-fil, les méthodes sont classiques : tests de pénétration, étude des configuration, …

7.4.3. Valider la qualité de service

Il est souvent nécessaire de faire une étude approfondie de la qualité de service offerte par un WLAN. En effet la qualité de la connexion réseau est affectée par des paramètres nombreux et très variés : une cartographie précise de la couverture radio permet de déterminer quels sont les points à améliorer, les équipements à doubler ou mettre en haute disponibilité, …

7.4.4. Surveiller en permanence l'espace radio

En complément d'audits approfondis mais ponctuels, il est également intéressant d'implémenter des solutions de détection permanentes, proches dans l'esprit des systèmes de sondes de détection d'intrusion (IDS) utilisées sur les réseaux conventionnels.

Ces systèmes sont constitués de sondes (points d'accès dédiés ou récepteurs radio spécialisés) reliées à un serveur d'analyse. Ils ont deux fonctions : détecter les équipements radio non autorisés et les attaques contre le WLAN de l'entreprise.

©2003-Cyber Networks-tous droits réservés

Il est également possible de compléter ces défenses radio permanentes par des systèmes de leurre (honeypot). Basiquement cela peut être des points d'accès volontairement peu sécurisés couplés à un système de détection d'intrusion, le tout ne donnant accès qu'à des ressources factices.

7.5. Protéger les terminaux équipés d'interfaces sans-fil

Les terminaux mobiles équipés d'une interface sans-fil active sont potentiellement vulnérables à une attaque directe de la part d'un pirate montant un WPAN à l'insu de sa victime. Par conséquent, il est important de fortement sécuriser tous ces terminaux pour protéger les données qu'ils contiennent et les ressources qui se trouvent éventuellement derrière (le LAN de l'entreprise en général).

Pour les terminaux comme les téléphones mobiles ou les PDA basiques, les systèmes sont très propriétaires donc peu sécurisables. En revanche, pour les PC portables, les PDA de type PocketPC et les stations de travail, plusieurs mesures doivent être prises :

7.5.1. La mise en place d'un firewall personnel administré

Le firewall personnel administré en central est indispensable sur tout équipement disposant d'une pile réseau TCP/IP évoluée. En effet imposer une politique de sécurité gérée au niveau de l'entreprise limitant l'accès aux ports réseaux ouverts par le système ou les applications est une mesure de sécurité essentielle.

A présent les systèmes de firewall personnels intègrent souvent un système de détection d'intrusion qui peut également s'avérer très utile pour prévenir l'utilisateur qu'une attaque est en cours. Le client VPN peut également être intégré à cette solution.

7.5.2. Le renforcement de la sécurité système

La sécurité du système d'exploitation et des applications sur les postes utilisateurs est généralement délaissée au profit des défenses périphériques. Les technologies sans-fil remettant en cause cette stratégie, il devient important de sécuriser et de maîtriser la partie système et applicative sur tous les équipements concernés.

7.5.3. Le renforcement du dispositif anti-virus

L'antivirus sur le poste de travail est également une brique indispensable, en particulier pour lutter contre les chevaux de Troie (trojan). En effet un terminal mobile faisant l'aller retour entre l'extérieur et le LAN d'une entreprise constitue en soit un excellent cheval de Troie. L'utilisation de ce type d'équipement comme vecteur d'attaque contre le LAN doit être empêchée.

©2003-Cyber Networks-tous droits réservés

L'antivirus doit également être capable de lutter contre des virus ou vers spécifiques, par exemple ceux conçus spécialement pour activer le mode ad-hoc des interfaces réseaux et donc ouvrir la voie à une intrusion.

7.5.4. La sécurisation du logiciel client sans-fil

Le logiciel client sans-fil installé sur un terminal utilisateur doit être configuré pour éviter l'établissement automatique de WPAN et ne pas s'associer automatiquement à des WLANs étrangers.

7.6. Sensibiliser et former

Les solutions techniques mises en place pour sécuriser un systèmes sans-fil sont inutiles si elles ne sont pas accompagnées d'une forte sensibilisation et d'une formation sécurité de tous les acteurs : utilisateurs, administrateurs, responsables…

En effet, l'homme reste potentiellement le maillon le plus faible de la chaîne de sécurité. Dans un contexte de mobilité et d'utilisation des moyens informatiques en déplacement ou à domicile, ce problème est d'autant plus critique.

Par exemple, un directeur non informé utilisant un réseau Wi-Fi domestique non sécurisé quand il travaille chez lui avec son PC portable professionnel met en danger des données confidentielles !

©2003-Cyber Networks-tous droits réservés

8. Conclusion

L'émergence des technologies sans-fil dans le monde des réseaux informatiques s'accompagne clairement de nouvelles problématiques sécurité. Ces dernières sont particulièrement graves et placent de nombreuses entreprises dans des situations d'insécurité critiques que des pirates n'hésitent pas à exploiter.

Il est important que les responsables informatiques intègrent au plus tôt ces technologies et les risques associés dans leur politique de sécurité globale puis prennent les mesures nécessaires pour protéger leur système d'informations. Cela doit être fait d'autant plus rapidement qu'il est devenu techniquement impossible de tenir complètement une entreprise à l'écart des systèmes sans-fil.

Les solutions de sécurité relatives à ces nouveaux réseaux existent et sont simples à mettre en œuvre : elles sont en grande partie basées sur des principes et des systèmes de sécurité éprouvés issus de la sécurité Internet, un renforcement de la sécurité informatique interne de l'entreprise et la mise en place de moyens de contrôle de l'espace radio.

De part son expertise acquise depuis plus de 7 ans dans le domaine de la sécurité des systèmes d'information, CYBER NETWORKS apporte à ses clients les solutions performantes qu'ils attendent, tant sur le plan du conseil et de l'audit que des projets d'intégration liés aux systèmes sans-fil et à la mobilité en général.

©2003-Cyber Networks-tous droits réservés

9. Glossaire

AES (Advance Encryption Standard) : standard de chiffrement récent et successeur du DES / 3DES. AES sera implémenté dans 802.11i pour chiffrer les communications sur les WLANs.

Bluetooth : norme radio IEEE 802.15 surtout utilisée pour les WPANs.

EAP (Extensible Authentication Protocol) : protocole servant de base au système d'authentification réseau pour l'accès à un WLAN. Il est utilisé conjointement au 802.1x et est indispensable à TKIP.

IEEE 802.1x : système de contrôle d'accès réseau par port utilisé avec EAP.

IEEE 802.11 : ensemble de normes très utilisées dans les WLANs. Les volets les plus connus sont le 802.11b et le 802.11a.

IEEE 802.11a : voir réseau Wi-Fi5.

IEEE 802.11b : voir réseau Wi-Fi.

IEEE 802.11i : volet sécurité de la norme 802.11.

IEEE 802.11g : norme compatible avec la 802.11b qui améliore les débits tout en restant dans la bande de fréquence des 2.4 GHz (donc autorisé en France)

IEEE 802.15 : nom de la norme Bluetooth.

IrDA : norme infrarouge.

Hot-spot : WLAN public destiné à offrir un service à des clients.

LAN (Local Area Network) : réseau local câblé traditionnel.

Réseau ad-hoc : autre terme désignant un WPAN.

TKIP (Temporal Key Integrity Protocol) : système améliorant la gestion et l'utilisation des clés de chiffrement RC4. TKIP est intégré dans certains systèmes propriétaires constructeur, WPA et 802.11i et nécessite un système d'authentification 802.1x/EAP.

WEP (Wired Equivalent Privacy) : système de sécurité natif 802.11 très faible.

Wi-Fi : norme radio WLAN basé sur la norme IEEE 802.11b (2,4 GHz - 11Mbps).

Wi-Fi5 : norme radio WLAN basé sur la norme IEEE 802.11a (5 GHz - 54Mbps).

©2003-Cyber Networks-tous droits réservés

WLAN (Wireless Local Area Network) : réseau sans-fil local à l'échelle d'un bâtiment ou d'un site : réseau d'entreprise, hot-spot public...

WMAN (Wireless Metropolitan Area Network) : réseau sans-fil à l'échelle d'une ville.

WPA (Wi-Fi Protected Access) : version allégée de 802.11i destinée à remplacer rapidement le WEP.

WPAN (Wireless Personnal Area Network) : réseau personnel temporaire et point à point entre deux ou plus équipements.

WWAN (Wireless Wide Area Network) : réseau sans-fil étendu sur de longues distances.

WWAN sur infrastructure publique : réseau sans-fil étendu basé sur une infrastructure non maîtrisée par l'entreprise, généralement une infrastructure télécom comme le réseau GSM ou GPRS.

©2003-Cyber Networks-tous droits réservés