Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Premier ministre

Secrétariat général de la défense nationale

Recommandations

La sécurisation des réseaux sans fil

1- Introduction

Les réseaux sans fil rencontrent aujourd'hui un succès important car ils permettent, via la norme IEEE[1] 802.11b, dite Wi-Fi ("Wireless Fidelity"), de déployer des moyens de transmissions sans contrainte d'immobilité liée aux câblages et aux prises (hormis l'alimentation). La promotion actuelle de ce type de solution, est uniquement axée sur les avantages qu'elle procure : facilité et rapidité d'installation, coût inférieur à un système filaire, mobilité, accès partagé à des services de haut débit – Internet. Toutefois, les coûts induits par la gestion des risques associés sont bien souvent omis.

Bien que la norme 802.11b présente certaines options de sécurité, les protections des réseaux Wi-Fi restent faibles, même vis-à-vis d'attaques simples. La nature du signal transmis (onde électromagnétique) rend difficile, voire impossible la maîtrise complète de la propagation. En conséquence, il est assez facile d'écouter les messages et même de s'introduire sur de tels réseaux, à l'insu des utilisateurs et de l'opérateur, pour y accomplir des actes malveillants sans laisser de trace. La disponibilité publique, la gratuité et la facilité de mise en oeuvre des outils de localisation, d'interception passive et d'agression confirment l'importance de cette menace.

Le présent document présente d'une part une analyse des différents types de risques auxquels les réseaux Wi-Fi sont exposés, d'autre part une série de conseils permettant à leurs administrateurs et usagers de mieux contrôler et si possible réduire les risques. Ces conseils concernent les questions de déploiement, de protection physique ou de protection logique du réseau. Ils peuvent aider à mettre en place un réseau sécurisé (action a priori), ou à sécuriser physiquement et logiquement un réseau déjà existant (action a posteriori).

2- Évaluation générale des risques

En raisonnant par analogie, implanter un réseau sans fil est similaire au fait de placer en pleine rue une prise téléphonique connectée à la ligne téléphonique d'un particulier ou d'un organisme, ou bien de positionner des prises Ethernet sur un réseau filaire en dehors de tout contrôle.

En effet, pour constituer un réseau local sans fil, il suffit d'équiper les postes informatiques, fixes ou portables, d'adaptateur 802.11b (sous forme de cartes, internes ou externes, avec une antenne) et si nécessaire, d'installer dans les locaux des points d'accès. Ces derniers sont connectés au serveur d'accès soit par une liaison à un autre point d'accès, soit par un accès filaire. Les données circulent alors sur le réseau par ondes radioélectriques.

Les risques encourus du fait de l'emploi de ce type de réseaux sont de même nature que pour les réseaux filaires, ils sont simplement plus élevés. En effet, l'écoute d'un message par un intrus ou son entrée sur un réseau 802.11.b sont facilitées du fait de la disponibilité en accès libre sur l'Internet d'outils d'agression et de la médiatisation qui est faite de leur emploi. Leur utilisation peut permettre des interceptions totalement passives ou au moins très discrètes, voire la réalisation de méfaits en usurpant l'identité d'un des utilisateurs légitimes du réseau sans fil.

Il importe de garantir à un niveau suffisant :

- la disponibilité et la qualité de service face aux agressions en saturation (cf. § 2.1) ;
- le caractère intègre des contenus face à des actes de malveillance (cf.§2.2) ;

[1] IEEE : Institute for Electronics and Electrical Engineering

- la confidentialité des échanges face à des interceptions passives (cf. § 2.3) ;
- la qualité des preuves techniques d'accès aux services et des actions, notamment pour assurer la facturation et l'engagement des responsabilités (cf. §2.4).

Ainsi, une bonne gestion des risques liés à un réseau nécessite toujours une approche globale. Pour répondre à cet objectif, la méthode EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité)[2] est librement accessible en ligne.

2.1) Disponibilité

La disponibilité d'un réseau peut être remise en cause soit par le brouillage radioélectrique, soit par une attaque en déni de service consistant à rendre inopérant le réseau par un envoi massif d'informations.

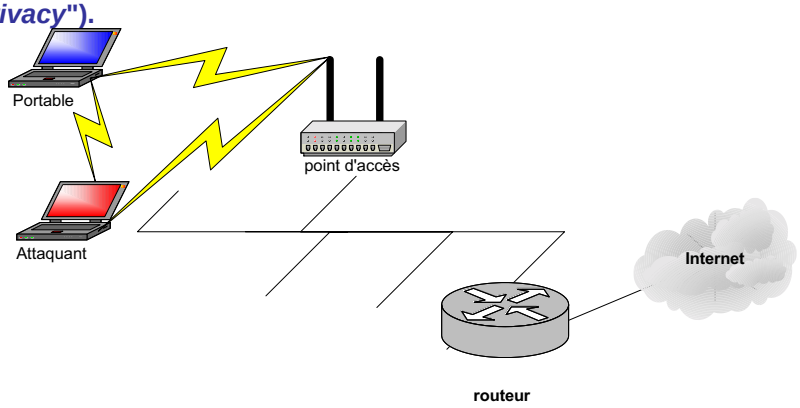
Le brouillage radioélectrique du réseau est relativement aisé par exemple avec du bruit blanc[3] diffusé dans la gamme de fréquence des 2,4 GHz et qui suffira à empêcher l'utilisation du réseau. Réalisable avec des composants du commerce, le brouillage peut être général ou sélectif. Un brouillage général interdira l'usage de la totalité du réseau. Un brouillage sélectif pourra empêcher la prise en compte des communications d'un élément du réseau. La perte de disponibilité pourrait devenir définitive (destruction des interfaces de réseau sans fil) dans le cas où la puissance du brouilleur s'avèrerait très supérieure au niveau admissible par les matériels visés.

Le déni de service logique consiste à saturer le point d'accès en multipliant artificiellement le nombre de demandes d'association. Le point d'accès considère alors que de nombreuses machines veulent se connecter. Or, il n'accepte en général que 256 associations (machines). Ne pouvant faire la distinction a priori entre une demande légitime et une demande illicite, il va donc refuser toutes les demandes d'association et donc provoquer un déni de service. Par ailleurs, sur un poste autonome (PDA, portable), la surconsommation due à l'obligation de répondre aux sollicitations de l'attaquant provoque un affaiblissement rapide des batteries et donc une perte importante d'autonomie.

2.2) Intégrité

2.2.1 Intrusion

L'intrusion revêt un caractère actif, consistant à pénétrer un réseau directement, sans nécessairement usurper une identité, afin de pouvoir bénéficier de l'infrastructure du réseau (accès Internet, intranet..), voire pour effectuer divers types d'actes malveillants. Une intrusion est souvent facilitée par l'absence totale d'authentification (cf. §6.1). Sur un réseau radio 802.11b chiffré, elle peut passer par une attaque de la clé de chiffrement, par défaut la clé WEP ("*Wire Equivalent Privacy*").



[2] http://www.ssi.gouv.fr/fr/confiance/documents/EBIOS_memento.pdf

[3] Bruit uniforme et constant dans la gamme de fréquence considérée

Pour ce faire, après avoir capté et enregistré une partie de la communication, l'attaquant doit reconstituer la clé de chiffrement WEP. Cette reconstitution passe par une étude des flux de données chiffrées circulant sur le réseau. Une fois la clé de chiffrement reconstituée, il est possible de s'introduire dans le réseau de manière transparente car on ne peut différencier un poste normalement autorisé d'un poste usurpant la même identité, contrairement au cas d'un réseau filaire bien configuré.

Il convient de noter que les machines d'un réseau interne sont bien souvent peu protégées. Elles constituent des cibles de choix pour mener des attaques par rebond ou des agressions sur d'autres entités. Dans ce cas, le gestionnaire ou l'exploitant du réseau radio deviendrait structurellement incapable de remonter à la source de l'agression.

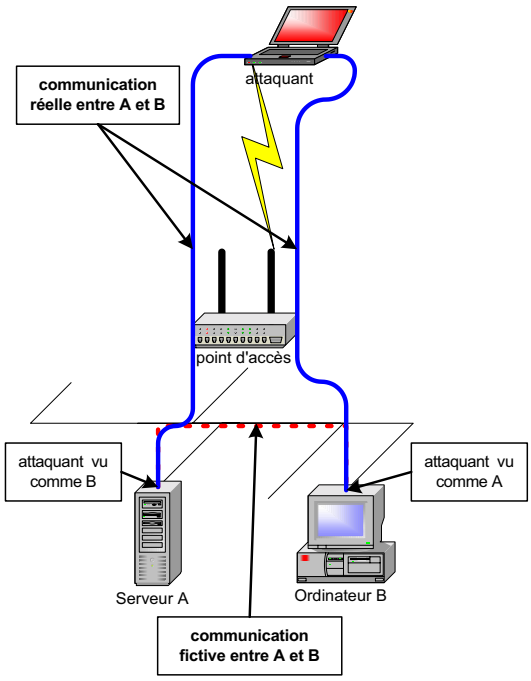
2.2.2 Usurpations d'identité

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

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

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

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



Ce type d'attaques est actuellement possible car la norme 802.11b propose un "système d'authentification" basé sur le contrôle des adresses machines (MAC) transmises en clair. Ce système ne peut être considéré comme un réel système d'authentification.

2.3) Confidentialité

Un agent malveillant disposant du matériel adéquat (un ordinateur portable ou simplement un PDA (assistant personnel) muni d'une carte 802.11b), peut écouter le réseau et par conséquent capter et interpréter les paquets d'informations circulant sur celui-ci. Ce phénomène est d'autant plus dangereux qu'il est invisible et non détectable, car complètement passif.

Or, la majorité des cartes réseau sans fil peut être configurée à cet effet et des manuels de fabrication d'antennes sont disponibles sur Internet. Pour quelques dizaines d'euros, il devient possible de concevoir des antennes permettant d'accroître la distance de captation de plusieurs centaines de mètres sans pour autant perdre des informations.

Par ailleurs, l'activation du protocole de chiffrement natif WEP ne suffit pas à garantir la confidentialité des informations (cf. § 2.2.a).

2.4) Qualités des preuves techniques

La qualité des preuves techniques d'accès et de tentatives d'accès aux services et des actions doit être assurée face aux risques suivants :

- accès frauduleux aux services sans facturation possible (par exemple accès Internet gratuit) ;
- accès utilisé par malveillance avec fausse indication d'origine.

Un agresseur suffisamment aguerri tentera quant à lui d'effacer les traces minimes qui pourraient rester de son agression, par exemple en arrêtant la journalisation des incidents dans les points d'accès, empêchant leur remontée vers le centre de gestion, voire en attaquant le centre de gestion.

3- Planification et déploiement

La mise en place d'un réseau sans fil est un projet à part entière qu'il convient de bien étudier afin d'éviter tous les écueils d'un "effet de mode". Pour un déploiement efficace, il est nécessaire de **bien planifier** les objectifs fonctionnels (gestion des services offerts et de leur qualité) et **les objectifs de sécurité (gestion des différents risques).** Il doit également respecter strictement l'enveloppe financière, les contraintes réglementaires et les contraintes juridiques. L'aspect juridique ne sera pas traité dans ce document.

Il faut planifier les objectifs et les mesures de sécurité nécessaires **avec l'aide d'un spécialiste toujours distinct et indépendant du fournisseur**, puis faire analyser ("auditer") à intervalles réguliers l'efficacité des mesures prises par rapport aux objectifs visés. **Cet auditeur effectuera ces tests de pénétration en utilisant notamment les outils d'agression disponibles dans le domaine public**.

La planification doit passer par l'étude des divers aspects relatifs à la mise en place d'un réseau sans fil.

3.1) Étude du coût

La mise en place d'un réseau sans fil est, en principe, d'un coût inférieur à celle d'un réseau filaire. Toutefois, dans le cas du déploiement d'un système basé sur la norme 802.11.b, le surcoût lié à une sécurisation efficace peut rapidement rendre le coût d'installation bien supérieur à ce qui était prévu initialement (cf. § 6).

Le rapport entre débit réel et coût d'une solution filaire ou sans fil doit aussi être étudié avec soin.

Les frais liés à la maintenance doivent également être pris en compte. Ils couvrent notamment la vérification périodique des matériels (puissance d'émission, plage de fréquences annoncées) et l'intégrité du réseau (bornes illicites…).

3.2) Les contraintes réglementaires

Depuis la **décision de l'autorité de régulation des télécommunications (ART), en date du 7 novembre 2002**, l'usage des bandes de fréquences 2,4 GHz a été assoupli pour trente-huit départements[4]. Dès lors, la bande 2400-2454 MHz est utilisable à l'intérieur des bâtiments comme à l'extérieur avec une puissance inférieure à 100 milliwatts (mW). La bande 2454-2483,5 MHz est utilisable, quant à elle, à l'intérieur des bâtiments avec une puissance inférieure à 100 mW et à l'extérieur des bâtiments avec une puissance inférieure à 10 mW. Sur les propriétés privées, cette puissance peut atteindre 100 mW à l'extérieur avec une autorisation explicite du ministère de la Défense.

Pour les autres départements du territoire national, la bande 2400-2446,5 MHz n'est utilisable qu'à l'intérieur des bâtiments et seulement avec une puissance inférieure à 10 mW, alors que la bande 2446,5-2843,5 est utilisable à 100 mW en intérieur et en extérieur sur des propriétés privées, sous réserve d'autorisation du ministère de la Défense.

Cette décision s'est inscrite dans un processus de fourniture au public de services Internet haut débit, en particulier dans les lieux de passage, les « hotspots » et dans les zones du territoire aujourd'hui mal desservies par les réseaux haut débit existants.

3.3) Évaluation des besoins

Il est impératif de définir, que le réseau soit privé ou public, l'environnement du réseau, le nombre de stations à connecter, les services désirés et le type d'information circulant sur le réseau.

- **Pour un réseau privé**
  - **l'environnement doit être défini** : pour un tel réseau, dont la couverture est limitée géographiquement (organisme, bâtiment, entreprise, cabinet médical, mairie, etc.), l'espace à couvrir et l'espace couvert non désiré doivent être indentifiés et contrôlés. Il convient aussi de s'assurer de la non-préexistence ou proximité d'autres réseaux ou équipements risquant d'entraîner des perturbations ;
  - **le positionnement des points d'accès est un élément essentiel** aussi bien pour la sécurité du réseau que pour son bon fonctionnement ; une étude préalable par un spécialiste est fortement recommandée ;
    - **ils doivent être placés en fonction du type d'antenne utilisée. En effet, la zone de couverture diffère suivant le modèle (fouet, parabole…).** L'objectif visé est d'éviter une trop grande diffusion hors du périmètre visé de l'entité,
    - **leur nombre doit être précisément déterminé** car il doit être suffisant pour permettre une couverture de l'ensemble de la zone mais sans être excessif pour éviter tout risque de perturbations du réseau,

[4] http://www.art-telecom.fr/communiques/communiques/2002/07-11-2002.htm

- **la qualité du signal doit être étudiée** (portée et perturbations électromagnétiques) pour chaque point d'accès (puissance d'émission et réglementation) ;

- **les services désirés doivent être définis** : quelles sont les informations diffusées sur le réseau (dialogue par messagerie, diffusion d'informations, remontée de données)? Quel est leur niveau de sensibilité ? Le réseau interne est-il connecté à d'autres réseaux ? Est-il connecté à Internet ?

➢ **Pour un réseau public**

- **l'environnement doit être défini** : pour un tel réseau la couverture est généralement ouverte et étendue. Ce type de réseau est aussi bien souvent connecté au final à un réseau filaire. Mis en place dans des lieux publics, il permet la fourniture de services Internet à grand débit, en particulier dans les lieux de passage ou salles d'attentes, les « hotspots ». Les utilisateurs de terminaux portables (ordinateurs portables ou assistants numériques personnels (PDA)) peuvent alors jouir d'accès Internet confortables dans des endroits tels que les aéroports, les gares, les hôtels, les centres de congrès et les cafés Internet. Ce type de déploiement pourrait également contribuer à fournir un accès au "haut" débit dans des zones du territoire aujourd'hui mal desservies par les réseaux existants ;

- **l'étude de l'implantation et de la couverture des points d'accès doit être faite par un spécialiste**. La position des points d'accès est cruciale pour le bon fonctionnement du réseau ;

- **les services désirés doivent être définis** : principalement dédiés à l'accès Internet, ces réseaux doivent être sécurisés par un renforcement de l'authentification des utilisateurs interdisant le rejeu pour limiter le vol des autorisations d'accès (pas de mots de passe mais des jetons logiciels ou matériels : OTP, clés USB, cartes à puce, carte PCMCIA).

4- Protection physique des équipements et des sites

Les premières règles à mettre en place pour sécuriser un système d'information, qu'il soit filaire ou sans fil, sont celles qui ont trait à la sécurité physique des équipements et des sites. Bien évidement, le premier risque à prendre en compte est le **risque naturel**, qui passe par une **étude préalable de l'environnement du site** : risques d'inondations, d'impact de foudre, variations de température, risques d'incendie… Cette étude permettra de définir si les lieux d'installation retenus sont adéquats et si des protections complémentaires sont nécessaires : énergie secourue, éclateurs contre la foudre, ventilation, climatisation, détection/extinction incendie, renvois d'alarmes sur défaillance....

L'**étude physique du site** (accessibilité, possibilité d'inspection visuelle, nature des bâtiments) établira la vulnérabilité intrinsèque du site et la nature des moyens de protection à mettre en œuvre.

La protection physique passe par un **contrôle anti-intrusion** des accès. En fonction du niveau de protection choisi, sa nature (humain, électronique, mixte...) et son type (contrôle visuel, portiques, badges, cartes électroniques...) seront définis. Enfin, au regard de l'environnement et du type d'activité, des systèmes anti-intrusions actifs ou passifs (grillage, barreaux, radars, infrarouge...) peuvent être mis en œuvre selon différents niveaux (enceinte, bâtiments, locaux sensible).

La protection physique du système permettra de détecter et d'éviter de nombreux types d'agression (installation frauduleuse de matériels, manipulation illicite sur les matériels…) qui pourraient remettre en cause les protections logiques retenues par ailleurs.

Dans le cas des réseaux privés et conformément à la législation en vigueur, la couverture du réseau devra, autant que possible, être circonscrite dans le périmètre de l'entité. Ceci est d'autant plus nécessaire pour un réseau sans fil 802.11.b, qui peut être écouté, par exemple depuis le parking voisin par une personne installée avec son portable. La protection et la surveillance physique du site à protéger et de ses abords pourront alors limiter ce type de menaces. Des outils d'audit (téléchargeables sur Internet) pourront être utilisés pour vérifier la couverture réelle du réseau à condition de les compléter par des antennes à fort gain. Si le déplacement ou la limitation en puissance des équipements émettant au delà du périmètre n'est pas possible, les zones identifiées devront faire l'objet d'une surveillance particulière.

5- Protections logiques et organisationnelles

La confidentialité des données ne peut être obtenue qu'en utilisant un tunnel chiffrant basé par exemple sur une réalisation de confiance du protocole IPSEC en mode tunnel. La mise en place de ce tunnel doit être faite avec des couples clé publique/clé privée ou des certificats et nécessite le déploiement d'une infrastructure de gestion de clé.

Dans tous les cas, il est indispensable d'**activer le chiffrement WEP** (cf. §6). Afin de limiter les risques d'attaques, la **clé WEP :**

- **doit être changée fréquemment** ("TKIP"), dans le pire des cas, tous les 1 million de paquets ;
- **ne doit pas être communiquée en clair** sur le réseau radio; pour cela, il faut utiliser le canal chiffré créé par la norme 802.1X. Il peut être activé sur le point d'accès et/ou les cartes lorsque celles-ci sont compatibles ; sinon de façon logicielle sur le pare-feu ("firewall") et/ou sur le poste client.

Dans l'hypothèse où le réseau filaire ne serait pas considéré comme sûr, la communication entre les différentes machines de ce réseau doit utiliser un chiffrement adapté.

Afin de limiter les tentatives d'accès frauduleux dont la responsabilité juridique incomberait au gestionnaire du réseau sans fil, il est **indispensable de mettre en place un système d'authentification forte**. La norme 802.1X, une fois ses modes configurés correctement, permet l'authentification réciproque des clients et de l'infrastructure (cf. §6). La mise en place d'une infrastructure de gestion de clé est un préalable utile à l'usage d'un système d'authentification. La totalité de l'infrastructure filaire doit si possible être configurée **pour utiliser IEEE 802.1X** (point(s) d'accès, pare-feu, commutateur). La mise en place de 802.1X nécessite l'installation d'un ou plusieurs **serveurs d'authentification RADIUS** ("Remote Authentification Dial-In User Service") dont **la configuration doit être correctement réalisée**.

Le point d'accès doit **diffuser le minimum d'informations** nécessaires à la connexion des clients. En particulier, **l'identifiant du réseau ("SSID") et les paquets de balise ("beacon")** ne seront pas diffusés ou leur fréquence de **diffusion sera réduite au minimum**.

Le choix des matériels (points d'accès, carte réseau) doit dans la mesure du possible s'orienter vers des produits dont le micro-logiciel ("firmware") peut être mis à jour et qui intègrent l'authentification IEEE 802.1X ainsi que le WEP 128 bits.

Un pare-feu ("firewall") doit être installé entre le réseau sans fil et le réseau filaire. Il peut être également prudent de distinguer ces deux réseaux tant en termes de confidentialité que de contrôle d'accès. Le pare feu peut intégrer l'authentification IEEE 802.1.X si le point d'accès ne la gère pas. Le pare-feu doit également contrôler la couche applicative pour bloquer les attaques via des ports normalement autorisés (par exemple le port 80, virus, tunnels).

Des antivirus si possible différents, installés sur le pare-feu et sur les postes nomades permettent de limiter la propagation des chevaux de Troie et des virus.

Enfin, sur le réseau filaire, il est préférable **d'utiliser des commutateurs** ("switch") plutôt que des concentrateurs ("hub") qui diffusent le trafic sur la totalité du réseau sans contrôle possible.

6- Outils de protection : authentification et chiffrement

6.1) Authentification

La première barrière à mettre en place est l'authentification des machines.

La norme 802.11b ne permet pas l'authentification. Seul le contrôle des adresses MAC est possible. Sauf cas particuliers (petit réseau), ce contrôle se configure difficilement. La plupart des points d'accès n'installent pas par défaut ce type de contrôle, ce qui rend le réseau démuni de toute vérification de droit d'accès. Même si l'opérateur valide l'option d'authentification, il n'en demeure pas moins que les adresses MAC sont diffusées en clair sur la voie radio ce qui constitue une faille de sécurité.

Pour pallier cette lacune, la norme 802.1x propose un protocole d'authentification modulaire **EAP (Extensible Authentification Protocol).** Ce protocole permet la vérification des autorisations des postes qui se connectent. Ce protocole, pour être efficace, doit être utilisé conjointement avec le protocole **TLS (Transport Layer Security)** pour le transfert des communications d'authentification chiffrées. D'autres protocoles de transfert existent, en particulier EAP-TTLS et EAP-PEAP. Tous ces protocoles doivent être associés à une **infrastructure de gestion de clés**.

Pour une configuration optimale, une infrastructure de type RADIUS, qui gèrera la base de données des droits des utilisateurs et la procédure d'authentification, **doit être installée.**

6.2) Chiffrement

En aucun cas le chiffrement WEP proposé par la norme IEEE 802.11 ne peut suffire à lui seul à garantir la confidentialité des informations.

La plupart des équipements ne proposent que des clés d'une longueur de 40 bits insuffisante face aux attaques par "force brute". De plus, le chiffrement utilise l'algorithme RC4 dont la programmation est réalisée de manière incorrecte. En conséquence, le protocole résultant est, au plan cryptographique, faible quelle que soit la taille de la clé employée. En particulier, des outils disponibles sur Internet permettent d'obtenir le pseudo-aléa généré et de pénétrer dans le réseau rapidement.

Se pose également le problème de la gestion des clés qui n'est pas traité par le WEP : généralement tous les utilisateurs partagent la même clé, qui est stockée en clair sur un équipement mobile (fichier ou adaptateur suivant les constructeurs), donc exposée. De plus, si un utilisateur la perd, il faut la remplacer sur tous les équipements, ce qui apparaît vite très contraignant. De ce fait, **il est recommandé d'utiliser le protocole EAP pour la transmission des clés de chiffrement.**

L'évolution de la norme 802.11i devrait intégrer d'autres moyens de chiffrement (AES) et d'authentification (IEEE 802.1X). Elle fait partie des normes futures, **prévues pour 2003** et destinées à accroître la qualité des réseaux sans fil. Ainsi, la norme 802.11i est destinée à améliorer la sécurité, **la 802.11e la qualité de service**, **la 802.11f à intégrer la sélection de fréquence dynamique (DFS) et le contrôle de puissance d'émission (TPC).**

En parallèle, d'autres normes existent telles que la norme IEEE 802.11a ou la norme Hiperlan2, qui ont toutes deux la particularité d'utiliser la bande de fréquences des 5 GHz avec un débit théorique de 54 Mbit/s.

Premier ministre

Secrétariat général de la défense nationale

7- Récapitulatif des recommandations

Recommandations générales

- Planification des objectifs fonctionnels et de sécurité
- Choix des objectifs de sécurité (méthode EBIOS) en termes de :
  - disponibilité et qualité du service
  - intégrité des contenus
  - confidentialité des échanges
  - qualité des preuves techniques d'accès aux services et des actions
- Etude du coût de la mise en place d'un réseau sans fil
- Respect de la réglementation (ART, protection des données personnelles…)

Recommandations particulières en fonction des objectifs de sécurité

Protection physique des équipements et des sites

- Etude préalable de l'environnement du site (liée aux risques naturels)
- Etude physique du site (accessibilité, possibilité d'inspection visuelle…)
- Mise en place d'un contrôle anti-intrusion des accès
- Vérification de la zone de couverture du réseau via l'utilisation d'outils d'audit

Protection logique et organisationnelle

- Configuration des points d'accès pour qu'ils diffusent le minimum d'informations nécessaires à la connexion du client
- Mise en place d'un tunnel chiffrant basé par exemple sur une réalisation de confiance du protocole IPSEC en mode tunnel
- Choix de matériels évolutifs et intégrant l'authentification IEEE 802.1X ainsi que le WEP 128 bits
- Activation du chiffrement WEP
  - Changement fréquent de la clé WEP
  - Utilisation d'un tunnel chiffrant pour la communication de la clé WEP
- Mise en place d'un système d'authentification forte
  - Contrôle des adresses MAC
  - Utilisation de la norme 802.1X et de son protocole d'authentification modulaire EAP
  - Utilisation du protocole TLS pour le transfert des communications d'authentification chiffrées
  - Association de ces protocoles à une infrastructure de gestion de clés
  - Installation d'une infrastructure de type RADIUS
- Installation d'un pare-feu entre le réseau sans fil et le réseau filaire
- Installation d'antivirus entre le pare-feu et les postes nomades
- Utilisation de commutateurs (switch) plutôt que de concentrateurs (hub)