Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité des systèmes d'information
CERTA

Paris, le 21 novembre 2008
N° CERTA-2002-REC-002

Affaire suivie par :
CERTA

RECOMMANDATION DU CERTA

Objet : Sécurité des réseaux sans fil (Wi-Fi)

Gestion du document

Référence	CERTA-2002-REC-002
Titre	Sécurité des réseaux sans fil (Wi-Fi)
Date de la première version	8 août 2002
Date de la dernière version	21 novembre 2008
Source(s)	
Pièce(s) jointe(s)	Aucune

TAB. 1 – *gestion du document*

Une gestion de version détaillée se trouve à la fin de ce document.

Table des matières

1 Résumé

Afin d'obtenir un niveau de sécurité satisfaisant sur un réseau sans fil, il est nécessaire de connaître les vulnérabilités inhérentes à ce type de réseau :

- la diffusion de l'information facilitant l'**interception passive à distance** ;
- la sensibilité au brouillage diminuant la disponibilité du réseau ;
- les configurations non sécurisées par défaut des nouveaux équipements, facilitant les attaques.

Au delà de la formation et de la sensibilisation des utilisateurs, il est indispensable de configurer son réseau de façon sécurisée. Cette étape comprend la configuration des différentes couches protocolaires mais également l'audit périodique et la surveillance continuelle de son réseau.

2 Position du Wi-Fi par rapport aux réseaux sans fil

En raison de leur facilité de déploiement et de leur coût relativement faible, les réseaux sans fil sont de plus en plus utilisés. Comme pour les réseaux filaires, on classe généralement les réseaux sans fil selon leur domaine de couverture : les réseaux personnels `WPAN` (`Wireless Personal Area Networks`), les réseaux locaux `WLAN` (`Wireless Local Area Networks`), les réseaux métropolitains `WMAN` (`Wireless Metropolitan Area Networks`) et les réseaux nationaux `WWAN` (`Wireless Wide Area Networks`).

2.1 Les réseaux sans fil de type `WPAN`

Les `WPAN` sont des réseaux sans fil de faible portée (quelques dizaines de mètres) qui, comme leur nom l'indique, sont des réseaux à usage personnel. Ils sont déjà présents sous différents noms :

- `Bluetooth` : nom commercial de la norme IEEE 802.15.1, `Bluetooth` est aujourd'hui présent dans de nombreux dispositifs. Malgré un débit de 1 Mb/s et une portée d'environ 30 mètres, `Bluetooth` offre de nombreuses possibilités grâce à la faible consommation de ses équipements. On trouve des composants `Bluetooth` dans beaucoup d'ordinateurs portables mais aussi dans de nombreux périphériques (appareils photo, téléphones portables, assistants personnels, ...). La norme IEEE 802.15.3 (`Bluetooth2`) est une évolution de la norme `Bluetooth` permettant des débits plus rapides et intégrant des mécanismes de sécurité très limités dans le protocole `Bluetooth`. Une note d'information portant sur le Bluetooth a été rédigée par le CERTA. Elle porte la référence CERTA-2007-INF-003.

- `ZigBee` : avec un débit plus faible que `Bluetooth`, la norme IEEE 802.15.4 (`ZigBee`) pourrait être très utilisée dans les années à venir. Les équipements `ZigBee` moins consommateurs et moins onéreux que les équipements `Bluetooth` devraient trouver leur place dans les périphériques informatiques mais également en domotique (éclairage, système de sécurité, ...).

- Les `liaisons infrarouges` : elles sont majoritairement utilisées pour des communications courte distance, cependant leur sensibilité aux perturbations empêche le développement de cette technologie dans les réseaux sans fil supérieurs à une distance d'une dizaine de mètres. Néanmoins, la portée d'interception peut-être très supérieure.

2.2 Les réseaux sans fil de type `WLAN` (norme IEEE 802.11)

La norme IEEE 802.11 (ISO/IEC 8802-11) est un standard qui décrit les caractéristiques des réseaux sans fil et est équivalente à la norme IEEE 802.3 (`Ethernet`) pour les réseaux filaires.

En fait, la norme IEEE 802.11 est la norme initiale à partir de laquelle un certain nombre de normes dérivées ont été créées afin de répondre à des objectifs d'interopérabilité ou de sécurité. Les normes dérivées les plus connues aujourd'hui sont les normes IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11i, et prochainement IEEE 802.11n.

La **norme IEEE 802.11a**, est aussi appelée Wi-Fi5. Elle utilise la bande de fréquence des 5 GHz et autorise un débit théorique de 54Mbps. Aujourd'hui, la législation française interdit l'utilisation de cette bande de fréquence en extérieur. L'utilisation de cette bande de fréquence est autorisée en intérieur pour des puissances d'émission inférieures à 100mW.

La **norme IEEE 802.11b**, adoptée en septembre 1999, est plus connue sous le nom de WiFi ou Wi-Fi.
De manière plus générale, le nom WiFi ou Wi-Fi (contraction de Wireless Fidelity) ne désigne pas réellement la norme IEEE 802.11 mais une certification délivrée par la Wi-Fi Alliance (anciennement WECA - Wireless Compatibility Alliance) qui s'occupe de l'interopérabilité entre les équipements répondant aux différentes normes IEEE 802.11.
La norme IEEE 802.11b permet d'atteindre un débit théorique de 11Mbps avec une portée pouvant atteindre plusieurs centaines de mètres en environnement dégagé. La norme 802.11b, comme d'autres technologies propriétaire (HomeRF d'Intel, OpenAir) utilise la bande de fréquence des 2,4 Ghz. 14 canaux de transmission différents, dont trois seulement sont utilisables simultanément au débit maximal, sont utilisables dans cette bande de fréquence, ce qui permet à plusieurs réseaux de cohabiter au même endroit, sans interférence.

La **norme IEEE 802.11g** permet un débit théorique (sans aucune perturbation) de 54Mbps dans la bande de fréquence des 2.4Ghz. Cette norme est compatible avec la norme IEEE 802.11b : les équipements répondant à la norme IEEE 802.11g peuvent fonctionner en environnement 802.11b, avec une dégradation des performances.

La **norme IEEE 802.11i** a été ratifiée en juin 2004 et met l'accent sur la sécurité en proposant des mécanismes de contrôle d'intégrité, d'authentification et de chiffrement.

La **norme IEEE 802.11n** est une norme à venir (sous forme de *draft* actuellement, prévue courant 2009) permettant d'atteindre des débits de l'ordre de 100Mbps et supérieur. Cette norme utilisera la bande de fréquence 2.4Ghz et sera compatible avec les normes IEEE 802.11g et IEEE 802.11b.

Il est important de noter que **des constructeurs vont au-delà des normes en proposant des extensions propriétaires**. Ce document ne s'attachera pas à ces extensions.

2.3 Les réseaux sans fil de type `WMAN` (norme IEEE 802.16)

La B.L.R. (Boucle Locale Radio) fait partie des réseaux sans fil de type `WMAN`. La BLR est une technologie sans fil capable de relier les opérateurs à leurs clients grâce aux ondes radio sur des distances de plusieurs kilomètres.

Les réseaux sans fil de type `WMAN` sont en train de se développer. Ce phénomène risque de s'amplifier dans les années à venir. La norme IEEE 802.16, est plus connue sous son nom commercial WiMax. La dernière version de la norme est IEEE 802.16-2004, ratifiée en juin 2004.

Comme dans le cas de la dénomination Wi-Fi, WiMax désigne en fait un ensemble de normes regroupées sous une appellation commune.

Techniquement, le WiMax permet des débits de l'ordre de 70Mbps avec une portée de l'ordre de 50km. Actuellement, le WiMax peut exploiter les bandes de fréquence 2.4Ghz, 3.5Ghz et 5.8Ghz. Aujourd'hui, en France, la bande de fréquence 2.4Ghz est libre, la bande de fréquence 5.8Ghz est interdite en utilisation extérieure et la bande des 3.5Ghz est licenciée à un unique opérateur.

La norme 802.16e ajoutera de la mobilité à la norme actuelle IEEE 802.16.

2.4 Les réseaux sans fil de type `WWAN`

Bien que ces réseaux ne soient pas connus sous ce nom, ce sont aujourd'hui les réseaux sans fil les plus utilisés en France. Les technologies cellulaires tel que le GSM (Global System for Mobile Communication), le GPRS (General Packet Radio Service) et l'UMTS (Universal Mobile Telecommunication System) font ou feront partie de ce type de réseau.

3 Présentation du Wi-Fi

Comme il a été précisé plus haut dans le document, par Wi-Fi nous désignerons les normes de type IEEE 802.11.

3.1 Utilisation du Wi-Fi

De nos jours les réseaux sans fil se développent très rapidement :

- pour des réseaux temporaires (salons, conférences, ...) ;
- pour des points d'accès haut débit dans les lieux publics (aéroports, gares, métros, ...) connus sous le nom de `hotspot` ou des lieux privés accueillant du public (hôtel, restaurant, ...) ;
- dans de nombreux organismes attirés par la souplesse des réseaux sans fil.

3.2 Caractéristiques techniques du Wi-Fi

3.2.1 Fonctionnement du Wi-Fi

Un réseau sans fil est fondé sur une architecture cellulaire où chaque cellule appelée BSS (Basic Service Set) est contrôlée par un AP (Access Point) ou point d'accès, le tout formant un réseau appelé ESS (Extended Service Set). Ce mode de communication est appelé le mode `infrastructure`. Les points d'accès peuvent être reliés entre eux par des liaisons radio ou filaires et un terminal peut alors passer d'un point d'accès à un autre en restant sur le même réseau (concept du `roaming`).

Pour s'identifier auprès d'un réseau, les utilisateurs d'un réseau sans fil utilisent un identifiant de réseau (`SSID`).

Un point d'accès sur un réseau sans fil équivaut à un concentrateur (hub) sur un réseau filaire. Chaque terminal sans fil reçoit donc tout le trafic circulant sur le réseau. Si ce terminal scrute simultanément plusieurs canaux, il recevra alors le trafic de tous les réseaux qui l'entourent.

Le mode de communication `ad-hoc` est également disponible : il s'agit d'un mode point à point entre des équipements sans fil. Avec ce mode de fonctionnement, il est possible d'utiliser des protocoles de routage proactifs (échange périodique des tables de routage pour la détermination des routes) ou des protocoles de routage réactifs (les routes sont établies à la demande) afin de reconstituer un réseau maillé (`mesh networks`).

L'accès radio au réseau sans fil se fait par le protocole CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) : quand un équipement du réseau veut émettre, il écoute le support de transmission et si celui-ci est libre, alors il émet. Ce protocole s'appuie sur des accusés de réceptions entre les récepteurs et les émetteurs.

3.3 Les avantages du Wi-Fi

Comme les autres réseaux sans fil, le Wi-Fi possède plusieurs avantages :

- la facilité de déploiement ;
- le faible coût d'acquisition ;
- la mobilité.

De plus, le Wi-Fi est intéropérable avec les réseaux filaires existants et garantit une grande souplesse sur la topologie du réseau.

Attention, il est toutefois nécessaire de relativiser les trois avantages cités ci-dessus en fonction du niveau de sécurité que l'on compte appliquer sur son réseau (cf. section Sécurité du Wi-Fi).

4 Sécurité du Wi-Fi

Installer un réseau sans fil sans le sécuriser peut permettre à des personnes non autorisées d'écouter, de modifier et d'accéder à ce réseau. Il est donc indispensable de sécuriser les réseaux sans fil dès leur installation. Il est possible de sécuriser son réseau de façon plus ou moins forte selon les objectifs de sécurité et les ressources que l'on y accorde. La sécurité d'un réseau sans fil peut être réalisée à différents niveaux : configuration des équipements et choix des protocoles.

4.1 Sécurité des points d'accès

Changer la configuration par défaut des points d'accès est une première étape essentielle dans la sécurisation de son réseau sans fil. Pour cela il est nécessaire de :

- changer les mots de passe par défaut (notamment administrateur) par des mots de passe plus forts ;
- modifier la configuration par défaut (adressage privé utilisé avec DHCP ou adresse de l'interface par exemple) ;
- désactiver les services disponibles non utilisés (SNMP, Telnet...) ;
- régler la puissance d'émission du point d'accès au minimum nécessaire.

Il est également important de **mettre à jour le `firmware` de son point d'accès** dès que le constructeur propose une mise à jour (résolution d'un problème de sécurité sur un des services disponibles par exemple). Cette mise à jour suppose des tests préalables poussés afin de vérifier la compatibilité avec l'existant une fois la mise à jour effectuée.

Changer le SSID par défaut est une bonne pratique, largement recommandé dans la plupart des cas. Il est judicieux de ne pas choisir un SSID attractif.

La plupart des points d'accès donne la possibilité de désactiver la diffusion du SSID. Il ne s'agit nullement d'une mesure de sécurité car une personne informée pourra obtenir le SSID très facilement : le SSID est une donnée qui est visible lors de l'association d'un client.

Ensuite, il s'agit de **configurer le point d'accès en activant les options de sécurité** répondant aux objectifs choisis en matière de sécurité. Les différents protocoles relatifs à la sécurité des réseaux sans fil sont exposés dans la suite de ce document.

L'**activation de la journalisation de l'activité du point d'accès** est nécessaire. Exporter ces journaux vers une machine de confiance, sécurisée dans cette optique, est largement recommandé.

Enfin, au-delà de la sécurité logique, il est nécessaire de **prendre en compte la sécurité physique des points d'accès**. Une protection des points d'accès doit être mise en place afin de contrer un utilisateur mal intentionné ayant un accès physique aux bornes (connection de l'attaquant par cable croisé ou cable série, modification matérielle de la totalité ou d'une partie du point d'accès ...).

4.2 Sécurité des protocoles liés aux réseaux sans fil

De nombreuses évolutions protocolaires ont rythmé la sécurité des réseaux sans fil. Les objectifs sont les suivants :

- garantir la confidentialité des données ;
- permettre l'authentification des clients ;
- garantir l'intégrité des données.

4.2.1 Chiffrement

L'absence de chiffrement dans un réseau sans fil laisse l'ensemble des données qui transitent sur ce réseau à la merci d'une personne munie d'une carte Wi-Fi et située dans le périmètre de réception des ondes émises par les autres équipements.
En raison de la propagation des ondes, il est nécessaire de protéger son réseau par un chiffrement approprié.

Le protocole initialement proposé pour le chiffrement des communications entre éléments d'un réseau sans fil est le WEP (`Wired Equivalent Privacy`). Le WEP est une option proposée dans le standard IEEE 802.11 et, en plus de chiffrement, traite de l'authentification et de l'intégrité. Le principe du chiffrement WEP est un chiffrement par flot utilisant l'algorithme RC4 et nécessitant un secret partagé encore appelé clef. Cette clef peut être de longueur 64 ou 128 bits (compte tenu de l'utilisation d'un vecteur d'initialisation de 24 bits, la longueur réelle du secret partagé est de 40 ou 104 bits). **Le chiffrement proposé par le protocole WEP s'est révélé rapidement inapte à offrir un niveau de sécurité suffisant** pour la plupart des utilisateurs. En effet, il est possible en écoutant une quantité suffisante de trafic (cela peut prendre plusieurs heures selon l'activité du réseau), de casser une clef WEP en quelques secondes. Une documentation abondante est disponible sur l'Internet sur le sujet. Plusieurs outils d'attaque publics permettent de faire cela facilement, sans matériel spécialisé, dans un temps raisonnable.

En plus de la faiblesse de la mise en oeuvre du chiffrement, le chiffrement WEP introduit des **problèmes de gestion de clefs** qui rapidement dégradent la sécurité du réseau, en plus d'être extrêmement difficile à mettre en place selon une politique rigoureuse. Afin d'augmenter la sécurité fournie par le chiffrement WEP, il est nécessaire de changer les clefs sur une base de temps à définir (dépend de la taille du réseau, du nombre d'utilisateurs, du trafic engendré...). Il faut également changer les clefs lors du départ d'un employé, du vol d'un portable...

Enfin, il faut également garder à l'esprit que tous les utilisateurs d'un réseau Wi-Fi protégé avec le chiffrement WEP partagent la même clef WEP. Ainsi, **tout utilisateur peut écouter les autres utilisateurs** comme si aucun chiffrement n'était en place.

L'évolution du chiffrement dans les réseaux sans fil est apparu avec le standard WPA (`Wi-Fi Protected Access`). Cette norme était initialement une norme intermédiaire en attendant la finition et la ratification de la norme IEEE 802.11i, devant apporter un niveau de sécurité satisfaisant pour l'ensemble des exigences en matière de chiffrement, authentification et intégrité.

Le WPA introduit le protocole TKIP (`Temporal Key Integrity Protocol`), qui sera repris par la norme IEEE 802.11i. Ce protocole permet de remédier aux faiblesses du chiffrement WEP en introduisant un chiffrement par paquet ainsi qu'un changement automatique des clefs de chiffrement. L'algorithme de chiffrement sous-jacent est toujours le RC4 utilisé avec des clefs de 128 bits, mais contrairement au WEP, il est utilisé plus correctement. Des méthodes d'attaques ont cependant été publiées en novembre 2008 ; elles permettent sous certaines conditions de déchiffrer quelques trames arbitraires émises par le point d'accès vers une station et d'injecter de nouvelles trames (empoisonnement de table ARP par exemple). Les bulletins d'actualité CERTA-2008-ACT-045 et CERTA-2008-ACT-047 abordent ces problèmes.

Le standard WPA définit deux modes disctincts :

- `WPA-PSK Mode` : repose sur l'utilisation d'un secret partagé pour l'authentification ;
- `WPA Enterprise Mode` : repose sur l'utilisation d'un serveur RADIUS pour l'authentification.

Le mode WPA-PSK est vulnérable à des attaques par dictionnaire. Il est donc très important de **choisir un secret (`passphrase`) fort** afin de limiter ces risques.
Cependant, en ce qui concerne le chiffrement dans les réseaux sans fil, le WPA apporte un niveau de sécurité supérieur à celui fourni par le WEP. Il permet aujourd'hui de se prémunir contre la plupart des attaques cryptographiques connues contre le protocole de chiffrement WEP.

La dernière évolution en date de juin 2004, est la ratification de la norme IEEE 802.11i, aussi appelé WPA2 dans la documentation grand public. Ce standard reprend la grande majorité des principes et protocoles apportés par WPA, avec une différence notoire dans le cas du chiffrement : l'intégration de l'algorithme AES (`Advanced Encryption Standard` - FIPS-197). Les protocoles de chiffrement WEP et TKIP sont toujours présents. Deux autres méthodes de chiffrement sont aussi incluses dans IEEE 802.11i en plus des chiffrements WEP et TKIP :

- WRAP (`Wireless Robust Authenticated Protocol`) : s'appuyant sur le mode opératoire OCB (`Offset Codebook`) de AES ;
- CCMP (`Counter Mode with CBC MAC Protocol`) : s'appuyant sur le mode opératoire CCM (`Counter with CBC-MAC`) de AES ;

Le chiffrement CCMP est le chiffrement recommandé dans le cadre de la norme IEEE 802.11i. Ce chiffrement, s'appuyant sur AES, utilise des clefs de 128 bits avec un vecteur d'initialisation de 48 bits.

Ces mécanismes cryptographiques sont assez récents et peu de produits disponibles sont certifiés WPA2. **Le recul est donc faible quant aux vulnérabilités potentielles de cette norme**. Même si ce recul existe pour l'algorithme AES, le niveau de sécurité dépend fortement de l'utilisation et de la mise en oeuvre de AES.

De plus, WPA2 pose aujourd'hui des **problèmes de compatibilité** pour les clients d'un réseau sans-fil. En plus du matériel non encore répandu, tous les systèmes d'exploitation n'intègrent pas la norme WPA2 ou IEEE 802.11i.

A ce jour, compte tenu de la disponibilité du matériel, des problèmes de compatibilité et en l'absence de recul suffisant, **la solution la plus sûre d'un point de vue cryptographique reste l'utilisation simultanée d'IPSEC**. Contrairement au standard IEEE 802.11i, IPSEC bénéficie d'un recul certain quant à la qualité de la sécurité offerte. Le coût de mise en oeuvre est sans doute plus élevé. Néanmoins l'absence de recul concernant la norme IEEE 802.11i oblige à être prudent lorsque l'on désire un chiffrement d'un niveau éprouvé.

En résumé :
La norme WPA offre un niveau de sécurité correct, le WPA-PSK nécessitant la définition d'un secret robuste afin de se prémunir contre les attaques par dictionnaire (énumération de tous les mots de passe en essayant les plus simples et évidents en premier). La norme WPA2 spécifie l'utilisation de l'algorithme AES, aujourd'hui standard international réputé d'un point de vue cryptographique. Il faut le préférer à TKIP quand cela est possible. La mise en place d'IPSEC, chiffrement au niveau IP, reste néanmoins le complément de la solution la plus sûre en l'absence d'une grande disponibilité de matériel certifié WPA2, de problèmes de compatibilité et d'un recul suffisant concernant la norme IEEE 802.11i. Le chiffrement est un des maillons d'un réseau sans fil sûr. **Un chiffrement robuste ne garantit en aucun cas à lui seul un bon niveau de sécurité de son réseau sans fil**.

4.2.2 Authentification

La norme 802.11 initiale spécifie deux modes d'authentification : ouvert ou partagé (`open` ou `shared`). L'authentification ouverte signifie l'absence d'authentification et l'authentification partagée signifie l'utilisation d'un secret partagé, en l'occurrence une clef WEP dans un mécanisme challenge/réponse. Il est vite apparu que **ce mode d'authentification était très largement insuffisant**, induisant même une dégradation du chiffrement par l'intermédiare du challenge/réponse donnant de la matière à des attaques cryptographiques.

La plupart des équipements donnent la possibilité de filtrer les adresses MAC ayant le droit de s'associer avec le point d'accès. Cette liste doit être reproduite sur chaque point d'accès du réseau sans fil si l'on désire garder toute la mobilité du réseau.

Ce seul mécanisme d'authentification s'avère souvent inefficace. En effet, il est toujours **possible pour un utilisateur mal intentionné de changer son adresse MAC** afin d'usurper l'identité d'un client valide. L'adresse MAC est censée servir d'identifiant unique au niveau de la couche 2, cependant tous les systèmes d'exploitation actuels permettent à un utilisateur mal intentionné de modifier cette donnée très facilement.

A ces problèmes d'authentification, **une solution plus robuste est apportée par la norme IEEE 802.1X**. Le standard IEEE 802.1X est utilisable en environnement sans fil comme en environnement filaire. IEEE 802.1X définit une encapsulation de EAP (`Extensible Authentication Protocol`) au dessus du protocole IEEE 802.11. L'équipement d'accès au réseau sans fil (point d'accès) relaie les trames entre le client et le serveur d'authentification (serveur RADIUS), sans connaître le protocole EAP utilisé. Dans le cas où le protocole d'authentification prend en charge la gestion des clefs, celles-ci sont transmises à l'équipement d'accès puis au client dans le cadre du chiffrement.

Dans le cadre de l'authentification en environnement sans fil basée sur le protocole 802.1X, différentes variantes de EAP sont disponibles aujourd'hui :

- Protocole EAP-MD5 (EAP - Message Digest 5) ;
- protocole LEAP (Lightweight EAP) developpé par Cisco ;
- protocole EAP-TLS (EAP - Transport Layer Security) crée par Microsoft et accepté sous la norme RFC 2716 ;
- protocole EAP-TTLS (EAP - Tunneled Transport Layer Security) developpé par Funk Software et Certicom ;
- protocole PEAP (Protected EAP) developpé par Microsoft, Cisco et RSA Security ...

Certaines de ces variantes se sont révélées trop faible pour prendre en charge une authentification de qualité satisfaisante. Ainsi **EAP-MD5 et LEAP sont peu à peu abandonnés** car ils sont sujet à des attaques par dictionnaire et des attaques de type `homme du milieu` (`man-in-the-middle`).

La norme IEEE 802.1X est incluse dans les standards WPA et WPA2 (IEEE 802.11i).

Il est évident que **les recommandations de sécurité portent également sur le serveur d'authentification (serveur RADIUS)** qui devra être à jour en ce qui concerne les vulnérabilités. En plus de la sécurité logicielle, une attention particulière devra être prise quant à l'insertion du serveur RADIUS dans son architecture réseau.

Conclusion :
L'utilisation du protocole IEEE 802.1X est recommandée si l'on désire un mécanisme d'authentification robuste et il est déconseiller d'utiliser une authentification qui s'appuie sur une clef partagée ou sur un filtrage des adresses MAC. En ce qui concerne **l'authentification EAP-TLS semble aujourd'hui s'imposer comme un protocole robuste** s'il est mis en place selon une politique de sécurité bien définie et mise en place avec rigueur. **La sécurité du serveur d'authentification doit être également prise en compte**.

4.2.3 Intégrité

Le standard IEEE 802.11 définit un mécanisme sommaire d'intégrité des trames basé sur le CRC (`Control Redondancy Check`). Cette valeur est appelée ICV (`Integrity Check Value`) et est de longueur 4 octets. Les propriétés du CRC sont telles que **le niveau de sécurité atteint est très faible**. Il est ainsi possible pour un utilisateur mal intentionné de modifier une trame tout en mettant à jour le CRC afin de créer une trame modifiée valide.

Le standard WPA introduit un mécanisme d'intégrité beaucoup plus robuste appelé MIC (`Message Integrity Check` - aussi appelé Michael dans le cadre du WPA et WPA2). Ce champ a pour longueur 8 octets et permet de se prémunir contre le rejeu (qui consiste à réémettre une trame interceptée de telle sorte qu'elle soit valide au sens cryptographique).

Le standard WPA2 ou IEEE 802.11i utilise également ce mécanisme d'intégrité.

L'utilisation de MIC est recommandée afin d'obtenir un niveau de sécurité plus élevé que l'utilisation d'une simple valeur de type CRC, présentant des propriétés cryptographiques trop faible pour assurer l'intégrité des trames dans un réseau sans fil.

4.3 Sécurité de la technologie

De par sa technologie le Wi-Fi est un protocole qui **diffuse les données vers toutes les stations qui sont aux alentours**. Un utilisateur mal intentionné peut se placer dans le périmètre des équipements du réseau afin de récupérer les informations qui lui permettront d'avoir accès au réseau.

La sensibilité au brouillage est une autre vulnérabilité induite par la technologie des réseaux sans fil. Elle peut entraîner un déni de service des équipements du réseau, voire la **destruction de ces équipements** dans le cas de bruit créé artificiellement.

4.4 Sécurité après la mise en place du réseau sans fil

Afin de conserver un niveau de sécurité satisfaisant de son réseau sans fil, il est nécessaire d'appliquer les mêmes procédures que pour les réseaux filaires, à savoir :

- informer les utilisateurs : la sécurité d'un réseau passe avant tout par la prévention, la sensibilisation et la formation des utilisateurs ;
- gérer et surveiller son réseau : la gestion et la surveillance d'un réseau sans fil peut, elles aussi, s'effectuer à deux niveaux. La surveillance au niveau IP avec un système de détection d'intrusions classique (`prelude`, `snort`, ...) et la surveillance au niveau physique (sans fil) avec des outils dédiés (`Kismet`, ...).
- auditer son réseau : l'audit d'un réseau sans fil s'effectue en deux parties. Un audit physique pour s'assurer que le réseau sans fil ne diffuse pas d'informations dans des zones non désirées et qu'il n'existe pas de réseau sans fil non désiré dans le périmètre à sécuriser. Un audit informatique, comme pour les autres réseaux, pour mesurer l'écart entre le niveau de sécurité obtenu et celui désiré.

La sécurité d'un réseau sans fil comprend aussi sa gestion. Gérer un réseau sans fil nécessite de s'appuyer sur une équipe ayant une bonne connaissance des réseaux et de la sécurité des systèmes d'information.

5 Conclusion sur le Wi-Fi

Malgré des problèmes de sécurité intrinsèques, les réseaux sans fil continuent et continueront probablement à se développer. Il est donc important de bien connaître les problèmes liés à la mise en place de ce type de réseaux afin d'en limiter les effets néfastes. Il est également important de déterminer le niveau de sécurité souhaité afin de mettre en place une solution en adéquation avec ce choix.
Malgré le peu de recul sur la norme IEEE 802.11i, celle-ci est vouée à s'imposer comme la norme unificatrice en matière de sécurité.
A ce jour, avec le peu de recul sur la norme IEEE 802.11i, l'utilisation d'IPSEC reste la manière la plus sûre de sécuriser son réseau sans fil, ce qui n'interdit pas de mettre en place le chiffrement disponible sur le lien radio.

6 Documentation

- Présentation synthétique : La sécurité des réseaux sans fil :
  http://www.ssi.gouv.fr/archive/fr/actualites/synthwifi.pdf
- Recommandations : La sécurisation des réseaux sans fil :
  http://www.ssi.gouv.fr/archive/fr/actualites/Rec_WIFI.pdf
- Le cadre réglementaire des réseaux RLAN / Wi-Fi depuis le 25 juillet 2003 sur le site de l'ART :
  http://www.art-telecom.fr/dossiers/rlan/schema-rlan.htm
- Synthèse de la consultation publique sur la technologie RLAN sur le site de l'ART :
  http://www.art-telecom.fr/publications/rlan/rlanreponse.htm
- Site Internet de la Wi-Fi Alliance :
  http://www.wi-fi.org
- Document sur la faiblesse structurelle du WEP :
  http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html
- Sécurité informatique numéro 40 du CNRS de juin 2002 :
  http://www.cnrs.fr/Infosecu/num40-sansFond.pdf
- Site Internet de l'outil Kismet :
  http://www.kismetwireless.net
- Site Internet de l'outil Snort :
  http://www.snort.org
- Site Internet de l'outil Snort-Wireless :
  http://snort-wireless.org
- Note d'information du CERTA CERTA-2007-INF-003, « Sécurité des réseaux sans fil Bluetooth » :
  http://www.certa.ssi.gouv.fr/site/CERTA-2007-INF-003/
- Bulletin d'actualité CERTA-2008-ACT-045, « Vulnérabilités dans certaines mises en oeuvre de WPA » :
  http://www.certa.ssi.gouv.fr/site/CERTA-2008-ACT-045.pdf
- Bulletin d'actualité CERTA-2008-ACT-047, « Retour sur la vulnérabilité de TKIP » :
  http://www.certa.ssi.gouv.fr/site/CERTA-2008-ACT-047.pdf

Gestion détaillée du document

8 août 2002 version initiale.

26 octobre 2004 mise à jour en profondeur compte tenu des nouvelles normes et évolutions en matière de sécurité des réseaux sans fil.

21 novembre 2008 ajout de références aux nouveaux risques TKIP publiés en novembre 2008.