

# ITRAINONLINE MMTK

## SECURITE SANS FIL

Préparé par : Alberto Escudero Pascual/ IT +46 <aep@it46.se>

---

|   |                    |
|---|--------------------|
| <a href="#">ITRAINONLINE MMTK.....</a>  | <a href="#">1</a>  |
| <a href="#">SECURITE SANS FIL.....</a>  | <a href="#">1</a>  |
| <a href="#">Au sujet de ce document.....</a>  | <a href="#">1</a>  |
| <a href="#">Renseignements sur le droit d'auteur.....</a>                               | <a href="#">1</a>  |
| <a href="#">Introduction.....</a>   | <a href="#">2</a>  |
| <a href="#">Définir la sécurité sans fil.....</a>                                       | <a href="#">2</a>  |
| <a href="#">Qu'est-ce que la sécurité de l'information?.....</a>                        | <a href="#">2</a>  |
| <a href="#">Confidentialité.....</a>  | <a href="#">2</a>  |
| <a href="#">Identification.....</a>   | <a href="#">3</a>  |
| <a href="#">Intégrité.....</a>  | <a href="#">3</a>  |
| <a href="#">Disponibilité.....</a>  | <a href="#">3</a>  |
| <a href="#">Non-reniement (imputabilité).....</a>                                       | <a href="#">3</a>  |
| <a href="#">Sécurité de l'information et réseau local (WLAN).....</a>                   | <a href="#">3</a>  |
| <a href="#">Mise en oeuvre des attributs de sécurité.....</a>                           | <a href="#">4</a>  |
| <a href="#">Commentaires généraux sur le cryptage au niveau du lien.....</a>            | <a href="#">5</a>  |
| <a href="#">Confidentialité sans fil (LAN).....</a>                                     | <a href="#">6</a>  |
| <a href="#">WEP ou ne pas WEP.....</a>  | <a href="#">6</a>  |
| <a href="#">WEP est mort. WPA et WPA2 sont nés.....</a>                                 | <a href="#">6</a>  |
| <a href="#">Identification sans fil (LAN).....</a>                                      | <a href="#">7</a>  |
| <a href="#">Arrêter la diffusion du SSID comme mesure de sécurité.....</a>              | <a href="#">8</a>  |
| <a href="#">Utiliser le filtrage des adresses « MAC » comme mesure de sécurité.....</a> | <a href="#">9</a>  |
| <a href="#">Portails captifs sans fil.....</a>  | <a href="#">9</a>  |
| <a href="#">Intégrité des données sans fil (LAN).....</a>                               | <a href="#">10</a> |
| <a href="#">Note de sécurité sur WPA.....</a>   | <a href="#">10</a> |
| <a href="#">Disponibilité sans fil (LAN).....</a>                                       | <a href="#">11</a> |
| <a href="#">Non-reniement sans fil (imputabilité).....</a>                              | <a href="#">11</a> |
| <a href="#">Menaces à la sécurité sans fil (LAN).....</a>                               | <a href="#">12</a> |
| <a href="#">Conclusion.....</a>   | <a href="#">13</a> |

### ***Au sujet de ce document***

Ces documents font partie du ItrainOnline MMTK. Le MMTK est un ensemble intégré de documents et de ressources de formation multimédia destiné à aider les médias communautaires, les centres multimédia communautaires, les télécentres et autres initiatives qui utilisent les technologies de l'information et des communications (TIC) à renforcer les communautés et soutenir le travail de développement.

### ***Renseignements sur le droit d'auteur***

Cette unité est présentée sous licence Creative Commons. Pour savoir comment utiliser ces documents, veuillez lire la déclaration sur le droit d'auteur accompagnant cette unité ou consulter

<http://creativecommons.org/licenses/by-sa/2.5/deed.fr>

---

## Introduction

Il est recommandé que vous lisiez l'unité sur le « **Reseaux TCP/IP: Notions avancées** » avant de lire cette unité.

Ce guide commence par vous donner une brève introduction sur les concepts clés dans le contexte de IEEE 802.11 ou WLAN, et présente une synthèse brève du modèle de référence OSI.

Cette unité décrit la sécurité dans le contexte de la sécurité de l'information. Cinq attributs élémentaires de la sécurité (confidentialité, identification, intégrité, non-reniement, et disponibilité) y sont décrits et évalués dans le contexte de IEEE 802.11 (WLAN). L'unité se termine en présentant les menaces importantes à la sécurité qui doivent être prises en considération lors d'un désign sans fil.

## Définir la sécurité sans fil

La définition de la sécurité est, dans une large mesure, une question de contexte. Le mot sécurité touche à de nombreux aspects, à l'extérieur comme à l'intérieur de la question informatique. Nous pouvons parler de sécurité en décrivant les mesures de sécurité sur une route ou une nouvelle plateforme informatique qui serait sécuritaire vis-à-vis des virus. Plusieurs disciplines ont été développées pour chaque aspect de la sécurité.

Considérant cela, nous avons essayé de contenir l'expression « sécurité sans fil » dans une catégorie qui nous aidera à aborder la sécurité au sein des réseaux sans fil. Cette unité décrit la sécurité sans fil dans le contexte de la sécurité de l'information. Lorsque nous traitons de sécurité sans fil, nous traitons de la **sécurité de l'information dans le réseau sans fil (WLAN<sup>1</sup>)**.

## Qu'est-ce que la sécurité de l'information?

Pour comprendre la signification de la sécurité de l'information, il est nécessaire de comprendre comment le terme a évolué dans le temps.

Jusqu'aux années 70, cet aspect de la sécurité était connu sous le vocable « *Communication Security* » ou « *COMSEC* ». La COMSEC était définie par la NSTISSI (Etats-Unis) pour « National Security Telecommunications and Information Systems Security Instruction »

*« Les mesures prises et les contrôles fait pour refuser aux personnes non-autorisées, l'accès à des informations dérivant de télécommunications et pour assurer l'authenticité de ces télécommunications. »*

Quatre zones furent intégrées dans les activités de sécurité de COMSEC: Sécurité du cryptage, de la transmission, de l'émission et sécurité physique. La sécurité selon COMSEC incluait deux attributs reliés à cette unité : la confidentialité et l'identification.

## Confidentialité

*L'assurance que l'information n'est pas accessible à des personnes, des processus ou des équipements non-autorisés (Protection contre l'accès non autorisé).*

---

<sup>1</sup> Nous référons ici au groupe de travail sur IEEE 802.11

## Identification

*Les mesures de sécurité conçues pour établir la validité d'une transmission, d'un message, d'un **originator**, ou le moyen de vérifier l'autorisation d'une personne pour recevoir une catégorie spécifique d'information (vérification de l'**originator**).*

Dans les années 80, avec la croissance des ordinateurs (personnels), une nouvelle ère de sécurité commence. La NSTISSI définit la sécurité des ordinateurs « COMPUSEC » comme suit :

*“Les mesures et les contrôles qui assurent la confidentialité, l'intégrité, et la disponibilité de l'information système incluant l'équipement, les logiciels et l'information communiquée, stockée et en processus. »*

COMPUSEC a introduit deux nouveaux attributs de sécurité reliés à cette unité : l'intégrité et la disponibilité.

## Intégrité

*La qualité d'un système d'information (SI) reflète l'exactitude et la fiabilité du système local d'opération., l'intégrité logique de l'équipement et du logiciel mettant en œuvre les mécanismes de protection, et la consistance des structures de données, en occurrence des données conservées.*

## Disponibilité

*Un accès précis et fiable aux données et aux services d'informations pour les usagers autorisés.*

Finalement, durant les années 90, les deux précédents concepts ont été fusionnés en un seul pour former INFOSEC pour « *Information Systems Security* ». Le nouveau concept inclut les 4 attributs des deux premiers : confidentialité, identité, intégrité et disponibilité et un 5<sup>e</sup>, le non-reniement.

## Non-reniement (imputabilité)

*L'assurance qui est donnée à l'expéditeur, preuve de livraison à l'appui de même que celle donnée au récepteur avec la preuve de l'identité de l'expéditeur; de façon à ce qu'aucun des deux ne puissent nier que les données aient été transmises.*

## **Sécurité de l'information et réseau local (WLAN)**

Le NSTISSI définit l' INFOSEC de la façon suivante :

*La protection de systèmes d'information contre la modification de l'information, qu'elle soit stockée, en transition ou en application, contre le refus de service aux usagers autorisés ou la livraison de service aux usagers non autorisés et incluant les mesures nécessaires pour détecter, documenter ou empêcher ces menaces.*



La sécurité sans fil est présentée du point de vue de l'INFOSEC; « Information Systems Security ».

Il est très commun dans la littérature reliée à la sécurité des WLAN que soit décrit des fonctions de sécurité sans que soit fourni un cadre sécurité approprié. En listant les fonctions de sécurité, le lecteur se remémore d'acronymes mais oublie le but exact de chacune de ces fonctions. Pour éviter cela, nous ne listerons PAS tous les attributs de sécurité dans WLAN mais plutôt, nous allons présenter les 5 attributs de sécurité de INFOSEC puis discuterons de comment WLAN met en œuvre chacun d'eux.

Cette approche aidera le lecteur à avoir une approche méthodologique en mettant sur pied des réseaux sans fil sécurisés.

Les cinq attributs présentés ici sont : confidentialité, identité, intégrité, non-reniement et disponibilité<sup>2</sup>.

## Mise en oeuvre des attributs de sécurité

Le Modèle de référence OSI « *Open Systems Interconnection* », créé par ISO « *International Standards Organization* », est une description abstraite pour design de protocole de réseau (de communication) d'ordinateurs. Le modèle divise les différentes fonctions de la communication en sept différentes couches qui peuvent fonctionner les une indépendamment des autres.

Tel que décrit dans l'unité « Réseautage avancé », le design de protocole OSI propose le principe d'une pile. Avoir un modèle en pile de couches implique que chaque couche n'utilise que les fonctions de la couche inférieure et fournit en conséquence des fonctions aux couches supérieures.

Cette approche en couche a des implications directes sur comment nous mettons en œuvre les attributs de sécurité.



Les normes sans fil réfèrent normalement aux couche 1 et 2 du protocole en pile OSI, laissant le paquet IP non-modifié. Les « paquets IP » sont transportés sur les protocoles données-lien et physique **spécifiques au sans fil**.

Par exemple, si nous considérons la « confidentialité du trafic de données » entre les 2 points d'accès, nous pouvons atteindre des résultats similaires (secret des paiements) par trois façons différentes:

- La couche de logiciel d'application(par la voie du TLS/SSL)
- Couche IP (par IPSEC) et,
- Couche lien (au moyen du cryptage sans fil)

Souvenez-vous que lorsque nous parlons de sécurité sans fil, nous parlons seulement des mécanismes de sécurité qui sont présents dans les couches 1 et 2, c'est-à-dire celles du cryptage sans fil (niveau lien). Les autres mécanismes qui sont présents dans la couche 3 et au-dessus font partie de la sécurité de réseau ou des logiciels d'application.

<sup>2</sup> Pour une approche plus formelle de la sécurité, lisez: The Common Criteria for Information Technology Security Evaluation, plus connu sous l'abréviation "Common Criteria" ou seulement "CC." Le CC fournit à la fois les exigences d'assurance et les fonctionnalités pour le produits de sécurité et les systèmes.

## Commentaires généraux sur le cryptage au niveau du lien

Le cryptage au niveau du lien est le processus pour sécuriser les données au niveau du lien quand les données sont transmises entre deux nodes attachées au même lien physique (il est possible qu'ils soient aussi attachés à deux différents liens physiques au moyen d'un répéteur). Avec le cryptage au niveau du lien, tous les autres protocoles ou logiciels fonctionnant par le lien physique sont protégés de l'écoute clandestine.

Le cryptage requiert une certaine clef, un secret et un algorithme partagé entre les parties communicantes. Quand l'envoyeur et le récepteur ne sont pas présents sur le même média, les données doivent être décryptées puis recryptées à chaque node le long de la route jusqu'au récepteur.

Le cryptage au niveau du lien est normalement utilisé quand il n'y a pas de cryptage aux niveaux plus élevés de protocole.



### ***Le cryptage au niveau du lien dans IEEE 802.11***

Algorithme le plus connu pour le cryptage au niveau du lien pour IEEE 802.11 est appelé WEP pour « *Wired Equivalent Privacy* ». Le WEP a cependant été démontré comme non sécuritaire et les autres alternatives telles que WPA « *Wi-Fi Protected Access* » ont été normalisées. La nouvelle norme IEEE 802.11i inclura une amélioration de WPA appelée WPA2.

Le cryptage au niveau du lien ne fournit pas une sécurité d'un bout à l'autre à l'extérieur du lien physique et devrait toujours être considéré comme une sécurité supplémentaire dans votre planification de réseau.

Le cryptage au niveau du lien requiert plus de ressources d'équipement dans les points d'accès et le design de la sécurité pour la distribution et la gestion.

## **Confidentialité sans fil (LAN)**

### **WEP ou ne pas WEP**

Nous définissons la confidentialité sans fil par l'assurance que l'information transmise entre les points d'accès et les clients n'est pas libre d'accès à des personnes non autorisées. La confidentialité sans fil doit assurer que la communication entre un groupe de points d'accès dans un système de distribution sans fil ou entre un point d'accès et un client demeure protégée.

La confidentialité sans fil fut traditionnellement associée au terme WEP. WEP faisait partie de la norme originale IEEE 802.11 de 1999.

Le but de WEP était de fournir aux réseaux sans fil un « niveau comparable de confidentialité » à celui des réseaux traditionnels avec fil. Le besoin pour un protocole comme le WEP était évident : les réseaux sans fil utilisent les ondes radio et sont donc ouverts à l'écoute clandestine.

Doté d'un mauvais design, peu transparent et qui a mené à différentes attaques durant sa mise en œuvre, la vie de WEP fut très courte. Quelques mois après que WEP fut lancé, le protocole était brisé et obsolète. Bien que la longueur de la clé fût initialement limitée en longueur à cause de restriction pour l'exportation, le protocole, indépendamment de la longueur de la clé, fut reconnu comme faible.

Ce ne fut pas son design qui rendit WEP obsolète, ce fut aussi et surtout le manque de système de gestion de la clé dans le protocole lui-même. WEP n'incluait justement aucune clef de gestion. La façon utilisée pour distribuer les

clefs étaient aussi simple que configurer (taper manuellement) une clef dans tous les équipements sans fil (un secret connus par plusieurs n'est plus un secret!)

WEP fut suivi par quelques améliorations propriétaire qui furent aussi inadéquates comme par exemple :WEP+ de Lucent et WEP2 de Cisco.



**WEP** et ses descendants (WEP+, WEP2) sont aujourd'hui obsolètes. WEP est basé sur le « *RC4 stream cypher* » dont la mise en œuvre sur IEEE 802.11 est reconnue non-sécuritaire.

Il existe de multiple attaques disponibles et logiciels démontrés efficaces pour craquer WEP (Airsnot, wepcrack, kismac, aircrack, etc). Quelques-unes des attaques furent basées sur la limitation numérique des vecteurs d'initialisation du « *RC4 stream cypher* » ou la présence du « weak IV » dans le datagram.

On peut en apprendre davantage sur l'histoire de la sécurité WEP dans le document sur les ressources additionnelles de cette unité.

## WEP est mort, WPA et WPA2 sont nés...

Après la mort de WEP, le WPA « Wi-Fi Protected Access » fut proposé en 2003 et plus tard certifié partie intégrante de la norme IEEE 802.11i sous le nom de WPA2 (2004).

WPA et WPA2 est conçu pour fonctionner avec ou sans un serveur de clefs de gestion. Si le serveur de clefs de gestion n'est pas utilisé, toutes les stations partage un clef pré-échangée « pre-shared key - PSK ». Le mode PSK est connu comme WPA ou WPA2 personnel.

Quand un serveur de clefs de gestion est utilisé, WPA2 est connu comme WPA2-Enterprise. Dans WPA-Enterprise, un serveur IEEE 802.1X est utilisé pour la distribution des clefs.

Une amélioration majeure de WPA2 par rapport à WEP est la possibilité d'échanger les clefs dynamiquement par le protocole TKIP « Temporal Key Integrity Protocol ».



### WPA2 Accès protégé Wi-Fi

WPA2 est une version certifiée de WPA et partie prenante de la norme IEEE 802.11i. Deux changements importants sont inclus dans WPA2 par rapport à WPA:

1. Le remplacement de l'algorithme Michael par un message code d'identification connu comme le « *Counter-Mode/CBC-Mac Protocol - CCMP* » qui est considéré cryptographiquement non sécuritaire.
2. Le remplacement de la « *stream cypher RC4* » par la norme aussi connue sous le nom de Rijndae, « *Advanced Encryption Standard - AES* »

Recommandations de confidentialité des données

Si la confidentialité sans fil est requise par le cryptage au niveau lien : le mode WPA2-Enterprise est la meilleure option.

Si vous choisissez un solution plus simple comme WPA-2-Personnel, des soins spéciaux devront être pris en choisissant les mots de passes (clefs pré-échangées).

WEP et ses variantes WEP+, WEP2 sont à oublier.

## Identification sans fil (LAN)

Dans le contexte d'un réseau local « LAN » sans fil, l'identification est la mesure désignée pour établir la validité de la transmission entre les points d'accès et-ou les stations sans fil. En mots simples, l'identification sans fil signifie « le droit d'envoyer des données à et via un point d'accès ».

Pour comprendre le processus d'identification dans le réseau sans fil, il est nécessaire de comprendre ce qui arrive au début de la session de communication entre un point d'accès et une station sans fil. La communication débute par un processus appelé « association ». Deux mécanismes principaux d'association furent introduits quand IEEE 802.11b a été conçu :

- Identification d'ouverture
- Identification à clef partagée

**L'identification d'ouverture** n'implique pas de sécurité et tout le monde peut parler au point d'accès. Dans l'identification à clef partagée, un mot de passe (secret) est partagé entre le point d'accès et la station client. Un mécanisme de réponse « à défi » permet au point d'accès de vérifier si le client connaît le secret et éventuellement lui garantir l'accès.



### WEP et identification dans la couche 2

L'identification à clef partagée mise en œuvre par WEP est aussi obsolète. Plusieurs attaques « **plain-cypher text** » peuvent aisément être faites contre l'identification basée sur WEP. Puisque la clef de cryptage et la clef d'identification sont la même, lorsqu'un est connu, l'autre l'est aussi.

Recommandations d'identification sans fil

L'identification sans fil au moyen de la couche 2 requiert l'utilisation du mode WPA-2-Entreprise. L'identification dans les réseaux sans fil, telle que celle mise en œuvre par les fournisseurs de services Internet, s'exécute normalement dans les couches plus hautes (couche IP) au moyen de portes d'entrée captives (identification dans un site Web).

Il est important de comprendre qu'en bougeant le processus d'identification jusqu'à un portail, nous ne nous laissons tout simplement aucun moyen d'arrêter le flot de trafic qui traverse le point d'accès.

## Arrêter la diffusion du SSID comme mesure de sécurité

Lucent Technologies ont développé en 2000, une variation du schéma d'identification ouvert appelé « *Closed Networks* » - réseaux fermés. Close Networks est différent de la norme de réseaux IEEE 802.11b parce que les points d'accès ne diffusent PAS périodiquement le SSID.

Ne pas diffuser le SSID implique que les clients sans fil doivent connaître à l'avance quel SSID utiliser pour l'associer à un (ou à la distribution d'un) point d'accès. La nouvelle fonction a été mis en place par plusieurs vendeurs en tant qu'amélioration de « sécurité ». En réalité, bien que la non-distribution du SSID empêchera effectivement les clients normaux de découvrir le SSID à partir d'une balise, cela n'empêchera pas à un autre logiciel de trouver le nom du SSID en écoutant clandestinement les cadres d'association d'une autre station. Trouver le SSID d'un réseau fermé « Close networks » est aussi simple que d'attendre que quelqu'un se connecte au réseau sans fil pour extraire la ligne du SSID du cadre d'association.



### Arrêter la diffusion du SSID

Arrêter la diffusion du SSID n'empêchera PAS une personne « intéressée » de trouver le SSID de votre réseau. Configurer votre réseau sans fil en mode « fermé » ajoutera seulement un niveau de problème supplémentaire pour l'intrus moyen. Arrêter la diffusion du SSID devrait être considéré comme une précaution supplémentaire, PAS comme une mesure de protection sécuritaire.

## Utiliser le filtrage des adresses « MAC » comme mesure de sécurité

C'est devenu très commun chez les fournisseurs de services Internet sans fil « WISP » d'utiliser les adresses MAC (pour Media Access Control) de l'interface sans fil comme mécanismes pour limiter/fournir l'accès à un réseau sans fil. L'idée derrière cela est que les adresses MAC sont codées « en dur » et ne peuvent pas être modifiées par l'utilisateur moyen. La réalité est très différente et les adresses MAC dans la plupart des interfaces de réseaux (sans fil) peuvent facilement être modifiées.



### Utiliser les adresses MAC pour l'identification

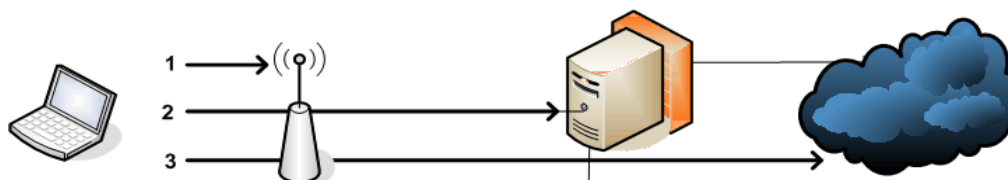
Un mécanisme d'identification basé exclusivement sur les adresses MAC n'est pas sécuritaire.

## Portails captifs sans fil

La discussion sur les portails captifs sans fil mérite une unité complète, mais nous nous contenterons d'une brève introduction dans cette unité à cause de leur pertinence dans la sécurité sans fil.

Bien qu'il existe différentes mises en œuvre de portails captifs sans fil, la majorité d'entre eux sont basés sur le même concept. Dans un réseau où l'identification fonctionne autour de portails captifs, le client peut s'associer à un point d'accès (pas d'identification sans fil) et obtenir un IP par DHCP (pas d'identification pour obtenir l'adresse IP). Dès que le client a reçu l'adresse IP, toutes les requêtes http sont capturées et le client est dirigé de force vers un page d'identification.

Les portails captifs sont responsables de vérifier la validité du mot de passe de l'utilisateur et de modifier le statut du pare-feu. Les règles des pare-feu sont normalement basées sur les valeurs de l'Adresse MAC du client de même que l'adresse IP provenant du serveur DHCP.



Sur l'image, nous pouvons voir les trois étapes d'identification du portail Captif. La première étape (1) requiert que le client s'associe au réseau sans fil. L'identification sans fil en termes de WEP-WPA n'est pas requise et le SSID est normalement annoncé. Dans la deuxième étape (2), le client va obtenir une adresse IP par DHCP. Le trafic IP est connecté au point d'accès sans identification. À l'étape finale (3), les connexions HTTP du client sont redirigés au serveur du portail captif. Le client se connecte via le portail (en utilisant normalement HTTPS + serveur + mot de passe). Finalement, le serveur captif modifie/crée des règles pour le pare-feu qui permettent au client de rejoindre l'Internet.

Il y a plusieurs problèmes de sécurité avec ce type de mise en place. Pour de plus amples informations, voyez l'unité sur les exercices.

## **Intégrité des données sans fil (LAN)**

Nous définissons l'intégrité des données sans fil comme la capacité d'un protocole sans fil de déterminer si la charge utile a été altérée par des usagers non autorisés.

En 1999, WEP a aussi essayé de fournir l'intégrité de la charge utile mais malheureusement le mécanisme d'intégrité ou la vérification de la redondance cyclique « cyclic redundancy check - CRC » était aussi non-sécuritaire. Le mauvais design de WEP permet des altérations de la charge et les mises à jour du message CRC sans même connaître la clé WEP. Le trafic peut être ainsi modifié SANS que cela ne soit perçu.

WPA et WPA2 ont résolu le problème d'intégrité des données de WEP en introduisant un message codé d'identification plus sécuritaire de même que l'introduction d'un compteur de frame qui prévient les « attaques à reprises ». Dans une attaque à reprise, l'attaquant enregistre la conversation entre le client sans fil et le point d'accès pour obtenir un accès non-autorisé. Il peut par la suite refaire défiler la conversation préenregistrée et entrer sans avoir à connaître la clé.



### **Intégrité des données: WEP vs WPA2**

Intégrité des données au moyen de WEP est obsolète.

Recommandations sur l'intégrité des données

WPA ou WPA2 devraient être mis en œuvre pour assurer l'intégrité des données sans fil au moyen du cryptage dans le niveau lien.

## **Note de sécurité sur WPA**

WPA a été conçu comme une étape intermédiaire vers WPA2 (norme IEEE 802.11i). WPA inclut un sous groupe de fonctions de IEEE 802.11i et s'arrête à être compatible avec les adaptateurs de WEP IEEE 802.11b.

WPA vise les faiblesses découvertes dans WEP. WPA augmente la longueur de la clé, le nombre de clés utilisées et ajouta un nouveau message codé d'identification. L'algorithme Michael fut choisi car il était le plus fort pouvant fonctionner avec la plupart des vieilles cartes réseau. L'algorithme Michael est toujours sujet à des attaques et c'est pourquoi les réseaux basés sur WPA possèdent un mécanisme de fermeture de 30 secondes à chaque fois qu'une attaque est détectée.

|                 |                | <b>WPA</b>                   | <b>WPA2</b>     |
|-----------------|----------------|------------------------------|-----------------|
| Mode Entreprise | Identification | IEEE 802.1X/EAP <sup>3</sup> | IEEE 802.1X/EAP |
|                 | Cryptage       | TKIP <sup>4</sup> /MIC       | AES-CCMP        |
| Mode Personnel  | Identification | PSK                          | PSK             |
|                 | Cryptage       | TKIP/MIC                     | AES-CCMP        |

3 EAP stands for Extensible Authentication Protocol, it is a security protocol invoked by an IEEE 802.1X enabled Network Access Server (NAS) device such as an IEEE 802.11 a/b/g Wireless Access Point.

4 TKIP stand for the Temporal Key Integrity Protocol.

## **Disponibilité sans fil (LAN)**

Nous définissons la disponibilité sans fil (LAN) par la capacité de la technologie d'assurer un accès aux données et aux services d'information pour les usagers autorisés.

La première chose que vous devez considérer est que ce n'est pas simple d'arrêter quelqu'un qui veut interférer avec votre signal radio sans fil. WLAN fonctionne avec des canaux radios prédéfinis que n'importe qui peut utiliser pour envoyer des signaux radio. Empêcher des usagers non-autorisés d'interférer avec votre réseau est presque impossible. La seule chose que vous pouvez faire est de surveiller vos liens avec attention pour identifier les sources potentielles d'interférence (voyez l'unité sur la gestion et la surveillance).



### **Refus de Service**

Les réseaux WLAN sont vulnérables au refus de service par interférences radio. Imaginer le scénario où un autre opérateur de réseau déciderait d'utiliser pour son réseau le même canal radio que votre réseau. Imaginez de plus que le même SSID est publicisé.

Pour éviter ce genre d'attaques intentionnelles ou non, pensez à faire des balayages périodiques des fréquences radio.

De façon à ne pas interférer avec d'autres réseaux, n'attribuez pas trop de puissance à vos liens.

Il existe de multiples raisons qui expliquent pourquoi un lien sans fil peut mal fonctionner ou même être non disponible. La présence de nodes cachés peut affecter sérieusement la performance de la famille de protocoles IEEE 802.11. Les virus, le logiciel point à point, le pourriel, etc. peuvent aussi surcharger votre réseau et ainsi limiter la bande passante disponible pour les connexions autorisées et les services légitimes

Tel que discuté dans la section sur l'identification de cette unité, il est difficile d'empêcher certains usagers de communiquer avec votre point d'accès ou votre portail captif. La disponibilité sans fil requiert l'établissement de bonnes pratiques de surveillance de réseau.

## **Non-reniement sans fil (imputabilité)**

La famille des normes IEEE 802.11 ne traite pas avec l'imputabilité du trafic de données. Comme tel, le protocole sans fil n'a pas de mécanisme pour remettre une preuve de livraison à l'expéditeur de données, et une preuve de l'identité de l'expéditeur pour le récepteur. L'imputabilité en besoin d'être mis en œuvre dans les hautes couches du protocole.

## Menaces à la sécurité sans fil (LAN)

Le tableau présente les 10 menaces à la sécurité les plus pertinentes dans les réseaux sans fil et fournit un ensemble de recommandations pour chacune d'elles.

|    |                                |   |   |
|----|--------------------------------|---|---|
| 1  | Confidentialité                | Risque d'écoute, des usagers non autorisés peuvent accéder au trafic des données dans votre dorsale sans fil            | Utilisez le cryptage au niveau lien dans vos liens sans fil (WPA2).<br>Recommandez à vos usagers d'utilisez le cryptage dans les protocoles de haut niveau (HTTPS, SMTP sécurisé) |
| 2  | Confidentialité                | Risque de détournement du trafic. Des usagers non-autorisés peuvent attaquer par le centre « man-in-the-middle attack » | Recommandation 1 +<br>Surveillez les SNR, SSID, point d'accès, et adresse MAC de votre connexion  |
| 3  | Identification                 | Risque d'accès non autorisé à votre réseau sans fil   | Utilisez IEEE 802.1X (WPA2)<br>Ne vous fiez pas seulement au schéma d'identification MAC<br>Ne distribuez pas votre SSID  |
| 4  | Identification                 | Risque d'accès non autorisé à votre réseau sans fil et à l'Internet   | Utilisez IEEE 802.1X<br>Un portail captif   |
| 5  | Intégrité                      | Risque de modification du trafic sur le transit sans fil  | Recommandez à vos usagers d'utilisez le cryptage dans les protocoles de haut niveau (HTTPS, SMTP sécurisé)<br>Utilisez le cryptage du niveau lien dans vos liens sans fil (WPA2). |
| 6  | Disponibilité                  | Risque d'interférence sans fil<br>Refus de service radio « Jamming »  | Surveillez le spectre radio périodiquement<br>Ne surchargez pas vos liens   |
| 7  | Disponibilité                  | Risque de bande passante non disponible à cause de la retransmission radio  | Vérifiez s'il existe des nodes cachés ou d'autres sources d'interférence<br>Surveillez le point d'accès-radio pour des retransmissions au niveau lien                             |
| 8  | Disponibilité                  | Risque de bande passante non disponible à cause d'un logiciel malicieux   | Surveillez le trafic IP, spécialement les trafics ICMP et UDP<br>Si nécessaire avec des systèmes de détection des intrusions  |
| 9  | Identification<br>Imputabilité | Risque d'accès non autorisé à votre intranet  | le réseau sans fil à l'extérieur du pare-feu<br><br>Créez un réseau privé virtuel et permettez les connexions seulement sur un concentrateur VPN                                  |
| 10 | (Accès Réseau)<br>Imputabilité | Risque d'utilisation non autorisée de vos ressources sans fil   | Installez IEEE 802.1X<br>Utilisez les portails captifs basés sur les signatures digitales   |

## **Conclusion**

Cette unité présente la sécurité sans fil du point de vue de l'INFOSEC.

Cinq attributs de sécurité - confidentialité, identité, intégrité et disponibilité et non reniement. – ont été présentés dans le contexte d'un réseau local sans fil.

Puisque les normes sans fil tels que IEEE 802.11 réfère seulement aux couches 1 et 2 de la pile de protocole OSI d'autres attributs de sécurité aux niveaux des protocoles de haut niveau peuvent être mis en oeuvre.

Un bon développeur de réseau sans fil doit réfléchir à l'endroit où mettre en œuvre chaque attribut de sécurité. Par exemple, le cryptage pour la confidentialité peut être mis en œuvre dans la couche lien ou dans celle du IP, SSID peut être distribué ou pas, l'identification peut être faite en utilisant , un portail captif ou encore le filtrage simple ou statique des adresses MAC, etc.

Toute mise en oeuvre dépendra toujours du logiciel et du scénario.