



SÉCURITÉ DES TI

PUBLICATION TECHNIQUE

Évaluation de la vulnérabilité des réseaux locaux sans fil (WLAN) 802.11 (ITSPSR-21A)

ITSPSR-21A

Mai 2009



Évaluation de la vulnérabilité des réseaux locaux sans fil (WLAN) 802.11 (ITSPSR-21A)

Page laissée intentionnellement en blanc.



Évaluation de la vulnérabilité des réseaux locaux sans fil (WLAN) 802.11 (ITSPSR-21A)

Avant-propos

Le document intitulé *Évaluation de la vulnérabilité des réseaux locaux (WLAN) sans fil 802.11 (ITSPSR-21A)* est NON CLASSIFIÉ et est publié avec l'autorisation du chef du Centre de la sécurité des télécommunications Canada (CSTC).

Les suggestions de modification devraient être transmises au représentant des Services à la clientèle au CSTC par l'entremise des responsables de la sécurité des communications du ministère.

Les demandes de copies additionnelles ou de modification de la distribution devraient être transmises au représentant des Services à la clientèle du CSTC.

Pour de plus amples renseignements, prière de communiquer avec les Services à la clientèle de la Sécurité des TI au CSTC par courriel à l'adresse client.svcs@cse-cst.gc.ca ou par téléphone au (613) 991-7600.

Date d'entrée en vigueur

Le présent document entre en vigueur le 1 Mai 2009.

Gwen Beauchemin
Directrice, Gestion de la mission de la Sécurité des TI

© Gouvernement du Canada, Centre de la sécurité des télécommunications Canada 2009

Il est interdit de reproduire cette publication, en totalité ou en partie, sans l'autorisation écrite du CSTC.



Évaluation de la vulnérabilité des réseaux locaux sans fil (WLAN) 802.11 (ITSPSR-21A)

Page laissée intentionnellement en blanc.



Évaluation de la vulnérabilité des réseaux locaux sans fil (WLAN) 802.11 (ITSPSR-21A)

Résumé

Les dispositifs WLAN reposant sur la norme IEEE 802.11 comportent de nombreuses vulnérabilités liées au fait que leurs signaux sont diffusés plutôt qu'acheminés par connexions filaires. Dans les WLAN, le trafic réseau est diffusé dans des endroits publics non contrôlés, ce qui peut donner lieu à la compromission de renseignements sensibles. Par ailleurs, les signaux provenant de sources externes non autorisées peuvent facilement pénétrer le réseau et permettre à des attaquants de se connecter à titre d'utilisateurs légitimes. Cela crée des risques non seulement pour le WLAN, mais aussi pour tout autre réseau auquel il est connecté. Sont également à risque les réseaux filaires traditionnels parce que n'importe quel utilisateur peut facilement installer des dispositifs WLAN peu coûteux à l'insu des autorités responsables. Le risque d'attaques externes est très élevé : des activités telle la conduite guerrière et la disponibilité d'outils logiciels gratuits et conviviaux pour découvrir et exploiter les vulnérabilités des WLAN peuvent permettre à un attaquant de pénétrer dans un réseau.

La norme 802.11 intégrait à l'origine un schéma de sécurité appelé Wired Equivalent Privacy (WEP), qui offrait une certaine protection contre l'interception accidentelle du trafic réseau ou l'insertion de trafic non autorisé. Or, WEP souffrait de sérieuses lacunes du point de vue de la conception qui l'ont rendu vulnérable aux outils d'exploitation des pirates informatiques. Des révisions récentes de la 802.11 incluait des mécanismes de sécurité améliorés dont le Wi-Fi Protected Access (WPA) et la norme 802.11i (également appelée WPA2). WPA2 remédie aux faiblesses des schémas précédents et se caractérise par un chiffrement robuste reposant sur l'algorithme AES (certaines marques et certains modèles de points d'accès WLAN sont certifiés FIPS140-2). Elle comporte aussi des fonctions d'authentification d'entreprise 802.1X permettant d'intégrer l'authentification de l'accès WLAN aux mécanismes d'authentification des utilisateurs de l'entreprise (cartes à puce, jetons, ICP, paramètres biométriques, etc.). Les attaques pratiques contre WPA2 sont peu nombreuses et sont réalisées principalement au cours des déploiements des clés prépartagées (PSK pour Pre-Shared Key).

À remarquer que ces fonctions de sécurité sont généralement désactivés par défaut et qu'elles doivent être activées pour qu'elles puissent fonctionner : en effet, les WLAN déployés sans qu'on y ait activé les fonctions de sécurité laissent le réseau complètement exposé à la découverte et aux attaques.

Le CSTC recommande que la sécurité WPA2 soit obligatoire avec l'authentification 802.1X dans toute la mesure du possible pour tous les déploiements WLAN au sein du gouvernement du Canada. Le matériel plus ancien qui ne prend pas en charge la norme WPA2 doit être remplacé ou mis à niveau. Dans les cas où des renseignements particulièrement sensibles peuvent être transférés à travers un WLAN, il faut prendre des mesures de sécurité additionnelles, tels le chiffrement de bout-en-bout ou les réseaux privés virtuels (RPV). D'autres mesures de protection essentielles comprennent la surveillance du réseau pour la détection de trafic inhabituel et la présence de dispositifs sans fil non autorisés.



Évaluation de la vulnérabilité des réseaux locaux sans fil (WLAN) 802.11 (ITSPSR-21A)

Le CSTC est en train de développer une solution de sécurité exhaustive pour atténuer les risques présentés par la technologie WLAN 802.11. Cette solution englobera une variété de mesures dont l'utilisation de pare-feu, le chiffrement des réseaux privés virtuels et l'authentification robuste, que les ministères devraient déployer pour isoler les WLAN des réseaux sensibles du gouvernement.



Évaluation de la vulnérabilité des réseaux locaux sans fil (WLAN) 802.11 (ITSPSR-21A)

Page laissée intentionnellement en blanc.



Évaluation de la vulnérabilité des réseaux locaux sans fil (WLAN) 802.11 (ITSPSR-21A)

Table des matières

Avant-propos	iii
Date d'entrée en vigueur	iii
Résumé	v
Historique des révisions.....	vii
Table des matières	ix
Liste des abréviations et des acronymes	xiii
1 Introduction	1
1.1 Contexte	1
1.2 Objet.....	1
1.3 Portée.....	1
1.4 Structure du document	1
2 Aperçu du système WLAN 802.11.....	3
2.1 Technologie.....	3
2.1.1 Contexte	3
2.1.2 Technologie infrarouge (IR)	3
2.1.3 Technologie des radiofréquences (RF).....	4
2.2 Architecture	5
2.2.1 Généralités	5
2.2.2 Mode ad hoc	5
2.2.3 Mode infrastructure	6
2.2.4 Mode système de distribution	6
2.2.5 Mode système de distribution sans fil	7
2.2.6 Réseaux maillés sans fil	8
2.3 Normes pour les WLAN.....	9
2.4 Normes IEEE 802.11.....	11
2.4.1 Contexte	11
2.4.2 Groupes de travail/amendements pour la norme IEEE 802.11	12
2.5 Norme d'interopérabilité Wi-Fi™	14
2.5.1 La Wireless Ethernet Compatibility Alliance (WECA) et la Wi-Fi Alliance	14
3 Mécanismes de sécurité	17
3.1 Généralités	17
3.2 Contrôle de l'accès	17
3.2.1 Généralités	17
3.2.2 Identificateur d'ensemble de services (SSID)	17
Liste de contrôle d'accès (ACL) des adresses.....	18



Évaluation de la vulnérabilité des réseaux locaux sans fil (WLAN) 802.11 (ITSPSR-21A)

3.2.3	MAC.....	18
3.3	Services d'authentification.....	18
3.3.1	Généralités	18
3.3.2	Authentification par système ouvert.....	19
3.3.3	Authentification par clé partagée	19
3.3.4	Authentification 802.1X.....	20
3.4	Confidentialité des données et WEP/WPA/802.11i/WPA2	21
3.4.1	Généralités	21
3.4.2	Protocole WEP (<i>Wired Equivalent Privacy</i>)	22
3.4.3	Le protocole WPA (<i>Wi-Fi Protected Access</i>)	23
3.4.4	Le protocole WPA2 (IEEE 802.11i/ <i>Wi-Fi Protected Access version 2</i>).....	24
4	Vulnérabilités.....	27
4.1	Vulnérabilités des mécanismes de contrôle d'accès	27
4.1.1	Généralités	27
4.1.2	SSID	27
	Liste de contrôle d'accès (ACL) pour les adresses.....	27
4.1.3	MAC.....	27
4.2	Vulnérabilités du mécanisme d'authentification.....	27
4.2.1	Généralités	27
4.2.2	Lacune de l'authentification par clé partagée.....	27
4.2.3	Vulnérabilités liées au 802.1X/EAP.....	28
4.3	Vulnérabilités de WEP.....	28
4.3.1	Généralités	28
4.3.2	Réutilisation du flot de clés	28
4.3.3	Intégrité des messages.....	28
4.3.4	Gestion des clés	28
4.4	Vulnérabilités liées au WPA/WPA2	29
4.4.1	Généralités	29
4.4.2	Gestion des clés	29
4.4.3	Vulnérabilité de l'échange de 4 messages et de phrase de passe faible	29
4.4.4	Contremesure de mystification WPA MIC.....	30
4.5	Valeurs par défaut de la configuration.....	30
4.6	Protocole SNMP (<i>Simple Network Management Protocol</i>).....	31
5	Exploits	33
5.1	Attaques par découverte de réseau et accès	33
5.1.1	Généralités	33
5.1.2	Découverte de réseau	33
5.1.3	Accès réseau par routeur sans fil	33
5.2	Attaques par saturation (déni de service).....	34
5.2.1	Généralités	34



Évaluation de la vulnérabilité des réseaux locaux sans fil (WLAN) 802.11 (ITSPSR-21A)

5.2.2	Capture d'un point d'accès	34
5.2.3	Clonage de PA.....	34
5.2.4	Brouillage des radiofréquences	34
5.3	Attaques contre le protocole WEP.....	35
5.3.1	Généralités	35
5.3.2	Attaques passives.....	35
5.3.3	Attaques actives	35
5.3.4	Attaque contre la table de déchiffrement	36
5.4	Attaques contre WPA et WPA2	36
5.4.1	Généralités	36
5.4.2	Attaques de dictionnaire de clés prépartagées	36
5.5	Attaques par surveillance et interception.....	37
5.5.1	Généralités	37
5.5.2	Reniflage de trafic.....	37
5.5.3	Surveillance des signaux diffusés.....	37
5.5.4	Attaque <i>man-in-the-middle</i>	37
6	Solutions.....	39
6.1	Aperçu.....	39
6.2	Déterminer la zone de couverture du réseau	39
6.3	Ne pas diffuser le SSID	40
6.4	Ne pas utiliser le SSID par défaut	40
6.5	Utiliser WPA2	40
6.6	Utiliser l'authentification 802.1X sur serveur.....	41
6.7	Changer les clés fréquemment.....	41
6.8	Mettre en place un RPV et un pare-feu pour isoler le WLAN	41
6.9	Utiliser un pare-feu personnel sur chaque client sans fil	41
6.10	Considérer l'utilisation de systèmes de détection/prévention d'intrusions sans fil	42
7	Travaux futurs	43
8	Conclusions et recommandations.....	45
9	Références.....	47



Évaluation de la vulnérabilité des réseaux locaux sans fil (WLAN) 802.11 (ITSPSR-21A)

Page laissée intentionnellement en blanc.



Liste des abréviations et des acronymes

AES	Advanced Encryption Standard
ACL	Liste de contrôle d'accès
ARP	Protocole de résolution d'adresses
ATM	Mode de transfert asynchrone
BSS	Ensemble de services de base
CBC	Enchaînement de bloc de chiffrement
CCMP	Counter-mode with CBC-MAC Protocol
CRC	Somme de contrôle de redondance cyclique
CSTC	Centre de la sécurité des télécommunications Canada
DHCP	Protocole de configuration dynamique de l'hôte
DES	Data Encryption Standard
3DES	Triple DES
DoS	Déni de service
DSSS	Étalement du spectre en séquence directe
EAP	Extensible Authentication Protocol
ESS	Ensemble de services étendus
ETSI	European Telecommunications Standards Institute
FCC	Federal Communications Commission
FHSS	Étalement du spectre par sauts de fréquence
FIPS	Federal Information Processing Standards (USA)
GC	Gouvernement du Canada
GHz	GigaHertz
GPS	Système mondial de localisation
HiperLAN	High Performance Radio Local Area Network (ETSI)
IBSS	Ensemble de services de base indépendant
ICP	Infrastructure à clé publique
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IP	Protocole Internet
IR	Infrarouge
IrDA	Infrared Data Association
ISM	Industriel, scientifique et médical
ISO	Organisation mondiale de normalisation
IV	Vecteur d'initialisation
LAN	Réseau local
MAC	Contrôle d'accès au support (IP)



Évaluation de la vulnérabilité des réseaux locaux sans fil (WLAN) 802.11 (ITSPSR-21A)

MAC	Code d'authentification de message (Crypto)
MAN	Réseau métropolitain
Mbps	Mégabits par seconde
MIC	Code d'intégrité de message
MIMO	Entrée multiple, sortie multiple
MROF	Multiplexage par répartition orthogonale de la fréquence
NAI	Identificateur d'accès de réseau
OCB	Offset Code Book
OSI	Interconnexion de systèmes ouverts
PA	Point d'accès
PHY	Physique (couche)
PMK	Pairwise Master Key
PPP	Protocole point-à-point
PRNG	Générateur de nombre pseudo aléatoires
PSK	Clé prépartagée
PTK	Pairwise Transient Key
RC4	Rivest Cipher 4/Ron's Code 4 (algorithme de chiffrement)
RF	Radiofréquence
RPV	Réseau privé virtuel
RSN	Robust Security Network
SNMP	Protocole de gestion de réseau simple
SSH	Secure Shell
SSID	Identificateur d'ensemble de services
STI	Sécurité des technologies de l'information
TI	Technologie de l'information
TKIP	Temporal Key Integrity Protocol
TMTO	Time-Memory Trade-Off
UMTS	Système universel de télécommunications mobiles
WAN	Réseau étendu
WECA	Wireless Ethernet Compatibility Alliance (voir aussi WFA)
WEP	Confidentialité équivalente aux transmissions par fil
WFA	Wi-Fi Alliance (nouveau nom pour WECA)
WIDS	Système de détections d'intrusions sans fil
Wi-Fi™	Wireless Fidelity (marque de commerce de Wi-Fi Alliance)
WIPS	Système de prévention d'intrusion sans fil
WLAN	Réseau local sans fil
WPA	Accès protégé Wi-Fi
WPA2	Accès protégé Wi-Fi , version 2
WPAN	Réseau personnel sans fil



Évaluation de la vulnérabilité des réseaux locaux sans fil (WLAN) 802.11 (ITSPSR-21A)

WRAP Wireless Robust Authenticated Protocol
XOR OU exclusif (opération booléenne)



Évaluation de la vulnérabilité des réseaux locaux sans fil (WLAN) 802.11 (ITSPSR-21A)

Page laissée intentionnellement en blanc.



Évaluation de la vulnérabilité des réseaux locaux sans fil (WLAN) 802.11 (ITSPSR-21A)

1 Introduction

1.1 Contexte

Avec l'adoption rapide de la technologie 802.11, les produits WLAN sont devenus monnaie courante et on les retrouve de plus en plus dans le monde des affaires et de l'éducation, de même qu'à la maison. La mobilité et la productivité accrues offertes par la technologie sans fil ainsi que les économies à long terme et sa facilité d'utilisation ont amené les organisations à adopter cette technologie novatrice. Toutefois, les ministères et les sociétés privées mettent en place des réseaux sans fil sans comprendre pleinement les risques pour la sécurité que représente leur utilisation.

1.2 Objet

Le présent rapport présente les vulnérabilités associées à l'utilisation d'un WLAN 802.11 dans l'environnement du gouvernement fédéral, de même que les solutions permettant d'y pallier. Il s'appuie sur une analyse des renseignements obtenus au laboratoire d'essai du CSTC et de l'information actuellement disponible auprès de sources ouvertes comme les fabricants et les organisations et associations technologiques. L'objectif premier de ce rapport est de permettre aux clients du gouvernement de mieux comprendre les risques en cause, avant qu'ils n'élaborent des plans de mise en place de réseaux sans fil.

1.3 Portée

Ce rapport porte essentiellement sur les principales variantes commerciales de la norme WLAN : soit 802.11b, 802.11g et 802.11n qui est sur le point d'être approuvée. Leur popularité, leur degré de perfectionnement et la grande disponibilité des produits font de ces versions de la norme les meilleurs modèles pour une évaluation des vulnérabilités de la technologie WLAN 802.11. Toutefois, il y a lieu de souligner que la majeure partie de l'information présentée dans le présent document n'est pas exclusive aux normes 802.11b, g et n, mais peut également s'appliquer à la norme 802.11a et à d'autres normes WLAN 802.11 à divers degrés.

1.4 Structure du document

Ce rapport présente un bref aperçu des architectures WLAN et de la norme IEEE 802.11 qui domine actuellement le marché des WLAN. Suit une explication des mécanismes de sécurité, de leurs vulnérabilités et de certains exploits bien connus de la norme 802.11. Le document présente également des mesures provisoires visant à atténuer les risques.



Évaluation de la vulnérabilité des réseaux locaux sans fil (WLAN) 802.11 (ITSPSR-21A)

Page laissée intentionnellement en blanc.



2 Aperçu du système WLAN 802.11

2.1 Technologie

2.1.1 Contexte

Contrairement aux réseaux locaux (LAN pour *Local Area Network*) conventionnels, qui reposent sur des connexions physiques réalisées au moyen de fils de cuivre ou de fibres optiques pour transmettre l'information, les réseaux locaux sans fil (WLAN pour *Wireless Local Area Network*) font appel aux ondes électromagnétiques infrarouges (IR) ou à radiofréquences (RF) pour transmettre et recevoir des données. La technologie du sans-fil offre toutes les fonctionnalités des LAN filaires mais elle élimine les contraintes matérielles que le câblage impose sur les utilisateurs réseau. Elle simplifie et accélère l'installation des réseaux et accroît leur souplesse et leur évolutivité, tout en favorisant une plus grande mobilité des utilisateurs. Si l'on ajoute à ces avantages la large bande passante en perpétuelle croissance qu'offre la technologie du sans-fil, on comprend aisément que les WLAN constituent une solution des plus intéressantes pour les particuliers ou les organisations qui désirent mettre en oeuvre ou étendre un réseau local sans devoir installer ou déplacer des câbles.

Dans un environnement WLAN, chaque ordinateur nécessitant une connectivité sans fil doit être équipé d'un adaptateur WLAN. Ces adaptateurs prennent généralement la forme d'une carte enfichable qui s'installe dans un emplacement de carte d'un ordinateur de bureau, ou même d'une carte PC ou d'une clé USB qui s'enfiche dans le connecteur approprié d'un ordinateur bloc-notes ou portatif. Il s'agit en fait de cartes d'interface réseau dotées d'un émetteur-récepteur radio intégré et d'une antenne miniature permettant l'établissement de la liaison RF (ou, dans le cas d'un WLAN articulé sur la technologie IR, une paire émetteur-récepteur infrarouge). Pratiquement tous les modèles d'ordinateurs portatifs récents comportent un ou plusieurs éléments WLAN intégrés (IR, 802.11, Bluetooth). Certes, cette pratique augmente la commodité des dispositifs et élimine le nombre de cartes et d'adaptateurs additionnels que doit transporter l'utilisateur, mais elle complique également les choses car, dans la plupart des cas, il est difficile de mettre à niveau ce matériel WLAN intégré pour tirer profit des nouvelles fonctions de sécurité ou fonctions utilisateur.

2.1.2 Technologie infrarouge (IR)

Le rayonnement infrarouge est utilisé dans diverses applications des technologies de l'information (TI), y compris les WLAN et les interfaces sans fil reliant les ordinateurs et les périphériques. À l'origine, l'infrarouge était une technologie non standardisée, où chaque fournisseur et chaque fabricant de matériel avait mis en oeuvre un protocole propriétaire. Or, un groupe, l'*Infrared Data Association* (IrDA), s'est rapidement formé pour produire un ensemble de normes régissant la connectivité des ordinateurs par infrarouge. La norme *IrDA Data* porte sur l'utilisation de l'infrarouge pour le transfert de données sans fil à haute vitesse, à faible portée et en visibilité directe point-à-point. La norme *IrDA Control* porte sur les communications entre les PC et les périphériques sans fil comme les claviers ou les souris. On utilise également



Évaluation de la vulnérabilité des réseaux locaux sans fil (WLAN) 802.11 (ITSPSR-21A)

la technologie laser pour établir des liaisons de données optiques pouvant transmettre de l'information en visibilité directe, à des distances atteignant plusieurs kilomètres.

La norme initiale IEEE 802.11 définit également l'utilisation de l'infrarouge comme technologie de transmission; toutefois, à ce qu'on sache aucun produit IR 802.11 n'a été développé et cette portion de la norme n'a pas été mise à jour depuis sa publication initiale en 1997. Ce fait n'est mentionné ici qu'à titre historique.

2.1.3 Technologie des radiofréquences (RF)

2.1.3.1 Généralités

La technologie des radiofréquences est devenue la technologie de fait pour la majorité des WLAN d'aujourd'hui. Les signaux radio peuvent se propager dans toutes les directions, à des distances allant de quelques mètres à plusieurs kilomètres. Ces caractéristiques peuvent être très pratiques dans une situation où une couverture élargie ou à longue portée est requise, mais peut poser un problème si la propagation des signaux doit être limitée. Comme la destination de la plupart des signaux radio ne peut pas être contrôlée, ce moyen de communication est le plus vulnérable à l'interception et à l'exploitation clandestines. Toute communication radio non protégée peut être captée, grâce à de l'équipement radio facilement disponible et utilisable par quiconque est situé à portée de l'émetteur. Or, il est important de noter que les amplificateurs et les antennes spécialisées peuvent également être utilisés uniquement au site du récepteur pour augmenter la portée efficace des signaux radio. Par conséquent, le simple contrôle de la puissance de l'émetteur ne suffit pas à limiter la propagation des signaux. Par exemple, on devrait éviter d'utiliser des claviers d'ordinateur sans fil RF pour traiter de l'information sensible, car ils diffusent en direct l'information qui y est tapée. Même si leur puissance de transmission est comparativement faible, cette information peut quand même être interceptée. En plus de l'interception des signaux, les communications RF peuvent être perturbées par des interférences électromagnétiques, parasites ou délibérées, qui peuvent rendre les communications impossibles.

2.1.3.2 Étalement du spectre

Le développement des communications à étalement de spectre est prétendu avoir atténué quelque peu les vulnérabilités de la transmission RF standard. À la différence des systèmes à bande étroite qui transmettent un signal puissant sur une seule fréquence, les systèmes à spectre étalé transmettent un signal de faible puissance, mais étalé sur une large plage de fréquences. Le signal est étalé selon une structure ou des paramètres établis au préalable que doit également connaître le récepteur pour pouvoir récupérer le signal. Cette technique de transmission s'avère plus résistante au bruit et à l'interférence et moins vulnérable au brouillage et à l'interception épisodique. Dans le cas des WLAN, le matériel doit connaître les paramètres d'étalement des signaux afin de pouvoir recevoir un signal à étalement de spectre; ces paramètres sont-ils donc préprogrammés dans les jeux de puces utilisés pour construire ces produits. Quoique ces jeux de puces aient été destinés à être développés dans le matériel de points d'accès (PA) WLAN et de



Évaluation de la vulnérabilité des réseaux locaux sans fil (WLAN) 802.11 (ITSPSR-21A)

postes de travail autonomes, il est inévitable que des outils et méthodes aient été développés pour exploiter ces récepteurs aux fins d'interception des communications WLAN à étalement de spectre. Bon nombre de ces outils sont disponibles gratuitement sur le Web et, par conséquent, aucune des technologies à étalement du spectre ne devrait être considérée comme étant suffisante pour sécuriser un WLAN.

De nombreuses méthodes d'étalement du signal ont été mises au point, mais celles qui sont le plus fréquemment utilisées pour les WLAN sont les suivantes :

1. l'étalement de spectre avec sauts de fréquence (FHSS – *Frequency Hopping Spread Spectrum*);
2. l'étalement du spectre en séquence directe (DSSS – *Direct Sequence Spread Spectrum*);
3. le multiplexage par répartition orthogonale de la fréquence (MROF).

Les technologies FHSS et DSSS sont les technologies à étalement du spectre originales employées dans les WLAN 802.11. Le concept d'étendre l'utilisation du spectre par des sauts de fréquence est assez explicite; le DSSS repose sur le principe mathématique de la convolution et procure un débit de données plus élevé et une plus grande immunité aux interférences que le FHSS. Le MROF est un schéma de modulation à large bande multiporteuse introduit dans la révision 802.11g et fournit un débit de données encore plus grand et est beaucoup plus résistant aux interférences que les schémas précédents. La norme 802.11n introduit la technologie MROF+MIMO, qui continue d'utiliser la même bande de fréquences de 2,4 GHz et le schéma de modulation de base du MROF, mais auxquels elle ajoute des techniques faisant appel à des émetteurs et des récepteurs multiples tout en tenant compte de la caractérisation spatiale et temporelle de l'environnement RF. Cela a pour effet d'augmenter la largeur de bande disponible à l'aide d'une pratique appelée « aggrégation de canaux » (*channel bonding*), qui consiste à combiner plusieurs canaux adjacents en un seul grand canal, pour accroître davantage la portée et le débit.

2.2 Architecture

2.2.1 Généralités

La norme 802.11 permet actuellement cinq formes d'architecture pour les réseaux sans fil : le mode « ad hoc », le mode « infrastructure », le mode « système de distribution », le mode « système de distribution sans fil » et le mode « maille sans fil ».

2.2.2 Mode ad hoc

En mode « ad hoc », illustré à la figure 1, les dispositifs sans fil créent un LAN en communiquant librement et directement entre eux, sans station de base centralisée. Cette architecture est également appelée « réseau point-à-point », ou encore « ensemble de services de base indépendant » (IBSS pour *Independent Basic Service Set*). Cette structure de réseau est facile à mettre en œuvre, car elle n'exige pas d'infrastructure et requiert peu d'administration.



Évaluation de la vulnérabilité des réseaux locaux sans fil (WLAN) 802.11 (ITSPSR-21A)

Cependant, son étendue se limite à la portée de diffusion des dispositifs de transmission.

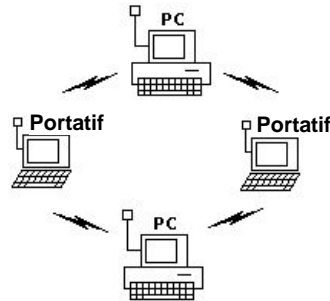


Figure 1 - WLAN en mode ad hoc

2.2.3 Mode infrastructure

La deuxième architecture, plus couramment utilisée, est celle qui consiste à construire le réseau autour d'une station de base centrale, ou point d'accès (PA). L'information transmise par le dispositif émetteur est reçue par le PA et acheminée vers la destination appropriée. Comme l'illustre la figure 2, le point d'accès est physiquement relié au réseau fédérateur filaire du LAN pour établir la communication entre les dispositifs sans fil et les dispositifs filaires. Par ailleurs, le point d'accès agit aussi comme relais radio pour réacheminer l'information entre les dispositifs sans fil qui sont trop éloignés les uns des autres pour pouvoir communiquer directement entre eux. Le mode infrastructure est également appelé « ensemble de services de base » (BSS pour *Basic Service Set*).

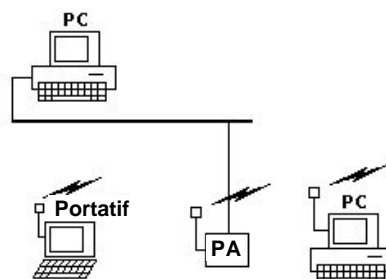


Figure 2 - WLAN en mode infrastructure

2.2.4 Mode système de distribution

Dans le mode « système de distribution », également appelé « ensemble de services étendus » (ESS pour *Extended Service Set*), plusieurs PA sont reliés à un réseau filaire au moyen d'un



Évaluation de la vulnérabilité des réseaux locaux sans fil (WLAN) 802.11 (ITSPSR-21A)

commutateur ou d'une passerelle, ce qui permet à un client WLAN de se prévaloir des fonctionnalités d'itinérance entre les PA et de bénéficier d'une mobilité et d'une portée accrues. Ce mode permet également l'itinérance des utilisateurs mobiles. À noter que la capacité d'itinérance nécessite un soutien PA spécial qui n'est pas disponible dans toutes les marques ou tous les modèles de PA. Par ailleurs, la communication entre les PA qui est nécessaire pour prendre en charge l'itinérance sans fil n'est pas couverte par la norme 802.11 étant donné qu'il s'agit d'un protocole de couche supérieure et que la plupart des fabricants ne mettent pas en oeuvre cette fonction ou utilisent un protocole propriétaire. Par conséquent, l'itinérance entre des PA de marques différentes, même s'ils sont connectés au même réseau, n'est généralement pas possible.

, Quand un utilisateur se déplace et s'éloigne de la couverture d'un PA dans un système WLAN 802.11 fonctionnant en mode distribution, son dispositif mobile s'associe au PA suivant dans l'ensemble étendu. Il demeure ainsi « connecté » au réseau et peut établir ou recevoir de nouvelles connexions sur le nouveau PA. Toutefois, sans soutien d'itinérance PA spécialisé, la session réseau qui était ouverte sur le PA précédent ne suivra généralement pas l'utilisateur sur le nouveau PA (à moins que l'application dont se sert l'utilisateur comporte sa propre fonction d'itinérance). Cette structure de réseau local est plus complexe et, dans le cas d'un réseau sans fil basé sur la technologie des radiofréquences, elle requiert une gestion attentive des canaux et des fréquences pour éviter les interférences entre les PA.

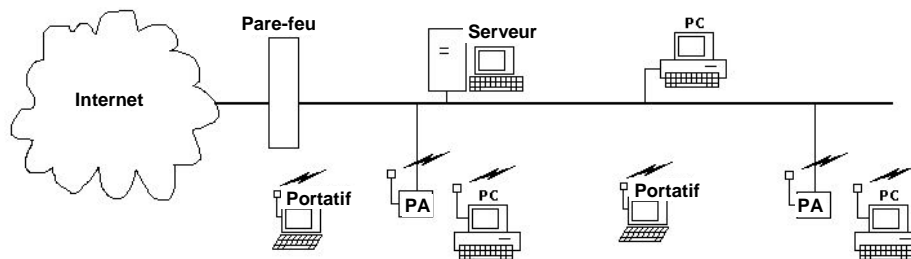


Figure 3 - WLAN en mode système de distribution

2.2.5 Mode système de distribution sans fil

Dans le mode « système de distribution sans fil » (WDS pour *Wireless Distribution System*), une liaison sans fil est utilisée pour interconnecter plusieurs PA, permettant ainsi d'étendre le réseau sans faire appel à l'infrastructure filaire. Les gains de réduction en infrastructure filaire offerts par la technologie WDS sont obtenus aux dépens du débit. Parce que chaque PA doit rediffuser tout trafic WDS reçu de manière semblable à un répéteur, le débit sans fil est coupé environ de moitié pour chaque saut qu'un message doit effectuer, de sorte que les clients sans fil qui se trouvent à l'extrémité d'une longue série de PS connectés selon le mode WDS pourraient connaître de très faibles débits. De plus, comme la fonctionnalité d'itinérance mentionnée plus



Évaluation de la vulnérabilité des réseaux locaux sans fil (WLAN) 802.11 (ITSPSR-21A)

haut, le mode WDS nécessite une interaction des couches 3 et 4 pour gérer le routage et cet aspect n'est pas standardisé en vertu de la norme 802.11, qui porte principalement sur les couches 1 et 2; par conséquent, il est possible que le mode WDS ne soit pas compatible entre des PA de marques différentes. Enfin, dans le mode WDS, tous les PA dans la chaîne doivent partager le même canal radio et les mêmes clés de sécurité; par conséquent, les clés de chiffrement dynamiquement attribuées (p. ex., WPA/WPA2 d'entreprise) ne sont généralement pas prises en charge dans une connexion WDS.

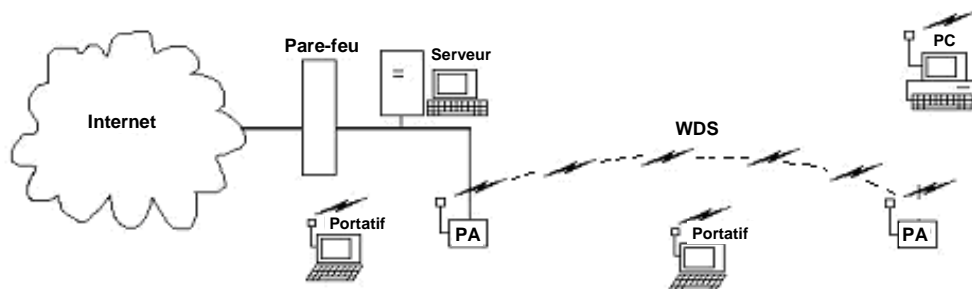


Figure 4 - WLAN en mode système de distribution sans fil

2.2.6 Réseaux maillés sans fil

Les réseaux maillés sans fil combinent les caractéristiques des réseaux sans fil ad hoc et infrastructure dans un mode système de distribution sans fil. Il en résulte un réseau infrastructure sans fil robuste qui peut être déployé avec des coûts de connexion filaire minimes et qui n'est plus limité à un réseau local mais qui peut s'étendre à un réseau métropolitain (MAN pour *Metropolitan Area Network*) ou un réseau étendu (WAN pour *Wide Area Network*).

Les produits de réseau maillé sans fil précédemment diffusés sous des normes propriétaires ont commencé à converger sous la bannière de la Wi-Mesh Alliance et de la norme 802.11s proposée. Cette norme permet à la fois les réseaux ad hoc maillés sans fil et les réseaux infrastructure maillés sans fil, et définit les protocoles de routage nécessaires au bon fonctionnement du système. La sécurité pour la norme proposée comprend la définition de la 802.11i à laquelle on a ajouté des améliorations pour remédier aux problèmes de remise à la clé et d'authentification qu'on retrouve dans cette architecture.

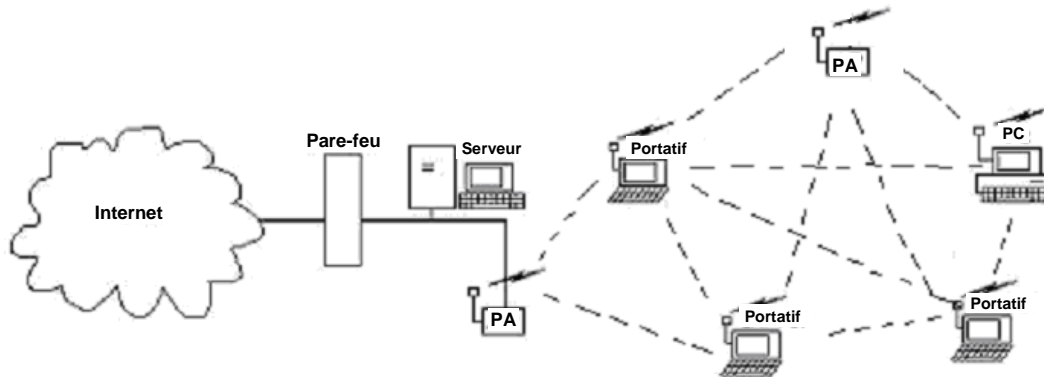


Figure 5 - WLAN en mode maillé sans fil

2.3 Normes pour les WLAN

L'évolution de la technologie des réseaux sans fil a été jalonnée par la mise en place de systèmes propriétaires, développés par divers fabricants. En l'absence de normes officielles, de nombreux fabricants ont élaboré leurs propres normes. Or, la plupart de ces systèmes propriétaires ont été remplacés par des systèmes reposant sur les diverses normes IEEE. Le Tableau 1 répertorie certaines des principales normes en vigueur dans l'industrie, ainsi que leurs spécifications et les applications visées. Il n'y a généralement pas d'interopérabilité possible entre les produits conformes à ces diverses normes propriétaires. De plus, il peut y avoir interférence entre les produits développés par différents fabricants, laquelle se traduit par une réduction du débit de données. Comme plusieurs de ces normes exploitent la même bande de fréquence sans licence, la technologie d'étalement du spectre ne peut éliminer complètement les risques de collision de paquets.

En plus des normes décrites dans le tableau ci-après, de nombreuses autres normes de réseautage sans fil sont utilisées. Ces normes ne sont pas liées à la norme 802.11 et visent à satisfaire des besoins différents. On retrouve entre autres l'USB sans fil (IEEE 802.15.3), le ZigBee Industrial Control (802.15.4) ou les normes pour les réseaux métropolitains sans fil WiMAX (802.16e).



Évaluation de la vulnérabilité des réseaux locaux sans fil (WLAN) 802.11 (ITSPSR-21A)

Tableau 1 – Principales normes WLAN

	IEEE 802.11	802.11b	802.11a	802.11g	802.11n (ébauche 2.0)	HiperLAN (ETSI)	HiperLAN/2 (ETSI)	HomeRF	IEEE 802.15.1 Bluetooth
Fréquence	2,4 GHz	2,4 GHz	5 GHz	2,4 GHz	2,4 GHz	2,4 GHz	5 GHz	2,4 GHz	2,4 GHz
Technologie	FHSS ou DSSS	DSSS	MROF	MROF	MROF+MIMO	Porteuse unique	Porteuse unique	FHSS	FHSS
Débit de transfert maximal	2 Mbps	11 Mbps	54 Mbps	54 Mbps	248 Mbps	23 Mbps	Jusqu'à 54 Mbps	1,6 Mbps	1 Mbps
Portée extérieure type	100 mètres	150 mètres	120 mètres	150 mètres	250 mètres	100 mètres	100 mètres	50 mètres	10 mètres
Sécurité	Wired Equivalent Protection (WEP)	Wired Equivalent Protection (WEP) + WiFi Protected Access (WPA) facultatif	Wired Equivalent Protection (WEP) + WiFi Protected Access (WPA) facultatif	Wired Equivalent Protection (WEP) /WiFi Protected Access (WPA) / 802.11i (WPA2)	Wired Equivalent Protection (WEP) /WiFi Protected Access (WPA) / 802.11i (WPA2)	NAI/adresse IEEE/X.509	NAI/adresse IEEE/X.509	Facultatif	Interrogation- réponse à l'aide d'une clé secrète (Bluetooth 1.0-2.0), courbe elliptique Diffie-Hellman (Bluetooth 2.1)
Chiffrement	RC4 40 bits	RCA jusqu'à 104 bits (WEP), RCA 128 bits avec ordonnancement des clés TKIP (WPA)	RCA jusqu'à 104 bits (WEP), RCA 128 bits avec ordonnancement des clés TKIP (WPA)	RCA jusqu'à 104 bits (WEP), RCA 128 bits avec ordonnancement des clés TKIP (WPA), AES 128 bits (WPA2)	RCA jusqu'à 104 bits (WEP), RCA 128 bits avec ordonnancement des clés TKIP (WPA), AES 128 bits (WPA2)	DES, 3DES	DES, 3DES	128 bits	E0 Cipher 128 bits, SAFER+, ECDH 128 bits (versions 2.1 et ultérieures)
Soutien réseau fixe	Ethernet	Ethernet	Ethernet	Ethernet	Ethernet	Ethernet	Ethernet, IP, ATM, UMTS, FireWire, PPP 5	Ethernet	PPP, Ethernet
Applications		Transmission des données sans fil	Transmission des données sans fil	Transmission des données sans fil	Transmission des données sans fil, multimédia	Transmission des données sans fil	Transmission des données sans fil	Transmission des données et de la voix sans fil	Abolition des fils, transmission des données et de la voix sans fil



2.4 Normes IEEE 802.11

2.4.1 Contexte

En 1985, la U.S. Federal Communications Commission (FCC) a décidé de libérer les bandes réservées aux usages industriels, scientifiques et médicaux (ISM) comprises entre 902 et 928 MHz, 2,4 et 2,483 GHz, et 5,725 et 5,875 GHz, pour utilisation publique sans licence. Non seulement cette décision répondait-elle à une demande du secteur des communications commerciales, mais elle a été la bougie d'allumage du développement de la technologie WLAN. L'Institute of Electrical and Electronics Engineers (IEEE) a établi en 1997 la norme 802.11 WLAN [1], afin de normaliser les produits qui utilisent la bande ISM. Cette norme a depuis été adoptée par l'Organisation internationale de normalisation/Commission électrotechnique internationale (ISO/CEI).

Les spécifications de base de la norme IEEE 802.11 portent sur la couche physique (PHY) et la couche liaison de données du modèle de référence Interconnexion des systèmes ouverts (OSI pour *Open Systems Interconnection*). La norme initiale proposait trois mises en oeuvre (mutuellement incompatibles) pour la couche physique : modulation par impulsion IR, signalisation RF avec modulation FHSS, et signalisation RF avec modulation DSSS. La différence la plus manifeste entre les WLAN et les réseaux LAN filaires classiques est l'absence d'un support physique pour la transmission des données : en effet, aucune connexion physique n'est requise pour un réseau 802.11.

La norme IEEE 802.11 initiale a été améliorée à plusieurs reprises (ces améliorations étant désignées comme étant des amendements). Les produits conformes aux amendements 802.11a, b et g sont couramment utilisés à l'heure actuelle, tandis qu'un nombre croissant de produits reposant sur l'ébauche 2.0 de l'amendement 802.11n sont mis en marché. Les principales spécifications pour chacune de ces normes sont données au Tableau 1.

Sur le plan historique, les premiers produits WLAN 802.11 commerciaux qui ont connu du succès étaient conformes à la norme 802.11b. Les amendements 802.11a et b ont en fait été adoptés simultanément, mais parce que 802.11b était moins complexe que 802.11a, les produits conformes à la norme 802.11b ont rapidement vu le jour tandis que les produits fabriqués en vertu de la norme 802.11a n'ont atteint le marché qu'en 2002. Depuis, l'amendement 802.11g qui utilise la même bande de 2,4 GHz que la norme 802.11b, mais qui fournit des connexions plus rapides et plus robustes, de même qu'une plus grande portée, est en voie de dominer le marché. Même si les produits 802.11b représentent toujours le plus grand nombre d'unités vendues dans le marché WLAN mondial, les ventes des produits 802.11g sont sur le point de les surpasser.



Évaluation de la vulnérabilité des réseaux locaux sans fil (WLAN) 802.11 (ITSPSR-21A)

2.4.2 Groupes de travail/amendements pour la norme IEEE 802.11

2.4.2.1 Généralités

Les WLAN conformes à la norme 802.11 originale et articulés sur la transmission infrarouge n'ont jamais été mis en oeuvre commercialement et les versions IR souffraient d'une faible vitesse de transmission (2 Mbps). L'IEEE a ultérieurement créé plusieurs groupes de travail afin de chercher à améliorer la norme 802.11 originale.

2.4.2.2 Amendement 802.11a

Le groupe de travail A a étudié la bande de fréquence de 5,0 GHz, utilisable sans licence, avec le mode multiplexage par répartition orthogonale de la fréquence (MROF), dans le but d'atteindre un débit de l'ordre de 54 Mbps. L'amendement 802.11a [2] a été formulé en 1999, et les fournisseurs ont commencé à offrir en 2002 des produits conformes à cette variante. Étant donné qu'elle utilise une bande d'exploitation et une modulation différentes, la norme 802.11a n'est pas rétrocompatible, ni interopérable avec la norme 802.11b. Plusieurs fournisseurs vendent donc des appareils à point d'accès à double bande multinorme (802.11a et 802.11b/g). La norme 802.11a est actuellement autorisée sous licence en Amérique du Nord et dans la plupart des pays européens quoique son utilisation commerciale ait été traditionnellement plutôt limitée.

Récemment, la norme 802.11a a connu une résurgence de popularité en raison du développement des réseaux infrastructure maillés d'entreprise. Dans de tels réseaux, la norme 802.11a est utilisée pour les communications entre les PA, tandis que les normes 802.11b/g servent aux communications entre les PA et les clients sans fil.

2.4.2.3 Amendement 802.11b

Le groupe de travail B a étudié la technologie DSSS afin d'accroître le débit de données dans la bande initiale de 2,4 GHz. L'amendement 802.11b [3], publié en septembre 1999, permet d'atteindre un débit brut de données de 11 Mbps, ce qui l'a placé au même niveau que les systèmes LAN filaires de 10 Mbps (10Base) très populaires à l'époque. La majorité des systèmes WLAN qu'on retrouve à l'heure actuelle sont conformes à la norme 802.11b, et sont acceptés partout en Amérique du Nord, en Europe et en Asie.

2.4.2.4 Amendement 802.11g

Le groupe de travail G a approuvé l'élaboration d'un nouvel amendement à la norme 802.11 en novembre 2001, qui a été ratifié dans sa version définitive en 2003. La norme 802.11g utilise la bande de 2,4 GHz, avec compatibilité obligatoire avec la norme 802.11b, et fait appel au schéma de modulation multiporteuse MROF afin d'atteindre un débit de données maximal de 54 Mbps.

2.4.2.5 Amendement 802.11n

Le groupe de travail N travaille présentement à l'élaboration d'un amendement à la norme 802.11 qui offre de plus grands débits de transmission. Comme dans le cas des amendements



Évaluation de la vulnérabilité des réseaux locaux sans fil (WLAN) 802.11 (ITSPSR-21A)

802.11b et g, la norme 802.11n utilisera la bande 2,4 GHz avec compatibilité obligatoire avec les normes 802.11b/g et fera appel aux techniques MROF + MIMO pour atteindre un débit de données projeté de 248 Mbps. Comme il a été décrit plus haut dans le présent document, la technique MROF + MIMO utilise la même modulation de base que 802.11g. Elle fait toutefois appel à plusieurs émetteurs et récepteurs et à des techniques évoluées pour compenser les variations spatiales et temporelles du canal RF, de même qu'à la pratique d'agrégation des canaux afin d'accroître considérablement la portée et le débit de transmission des données brutes. L'amendement 802.11n est encore à l'état d'ébauche et sa ratification définitive est prévue pour 2008. Toutefois, des produits « pré-N » ou « d'ébauche N » ont déjà commencé à faire leur apparition sur le marché. Les consommateurs devraient toutefois faire preuve de prudence lorsqu'ils achètent de tels produits, car ils n'ont pas été soumis aux mêmes tests d'interopérabilité que les produits pleinement conformes à la norme. Rien ne garantit non plus que ces produits seront compatibles avec la version définitive de la norme et il est également possible qu'ils ne puissent pas être élevés à la version définitive de la norme.

2.4.2.6 Amendement 802.11i

Contrairement aux amendements décrits précédemment, 802.11i ne se concentre pas sur les technologies, fréquences et débits RF. Plutôt, le groupe de travail I a été chargé de se pencher sur les vulnérabilités qu'on retrouve présentement dans la sécurité WEP. Bien que les travaux sur l'amendement 802.11i aient commencé en 2000, celui-ci n'a été ratifié qu'en 2004. Consciente du besoin d'améliorer la sécurité WLAN 802.11 sans tarder, la Wi-Fi Alliance a développé en 2001 une norme intérimaire de sécurité reposant sur l'ébauche de l'amendement 802.11i. Cette variante intérimaire appelée *Wi-Fi Protected Access* (WPA) s'est avérée en grande partie compatible avec la norme 802.11i définitive, laquelle a été nommée par la suite *Wi-Fi Protected Access version 2* (WPA2). C'est sous ce nom que la norme 802.11i est le plus largement connue.

WPA2 améliore le cadre de sécurité WEP de base de plusieurs façons. Premièrement, en ajoutant une authentification améliorée : (tous les schémas d'authentification permis sous le protocole EAP [*Extensible Authentication Protocol*], définis par le document RFC 3748, sont pris en charge par la norme 802.11i; toutefois, la majorité des produits commerciaux ne prennent en charge qu'un nombre limité de modes : l'authentification d'entreprise utilisant un serveur RADIUS et le mécanisme de clé prépartagée héritée de WEP). Deuxièmement, en améliorant de façon significative la robustesse des algorithmes cryptographiques : WPA2 utilise comme algorithme de chiffrement l'AES-CCMP 128 bits, lequel offre une marge de sécurité considérablement plus grande que les algorithmes RC4, CRC-32 et Michael utilisés précédemment dans WEP et WPA.

Quoique la norme WPA2/802.11i ait remédié à la majorité des lacunes du WEP, elle a fait l'objet d'une critique surprenante concernant son utilisation du chiffrement AES. En effet, l'AES est très robuste mais il augmente considérablement les exigences en matière de traitement, ce qui le rend inaccessible par de nombreux dispositifs faisant appel à des microprocesseurs plus lents. Il en résulte qu'il existe encore à l'heure actuelle sur le marché de nombreux dispositifs qui n'ont



Évaluation de la vulnérabilité des réseaux locaux sans fil (WLAN) 802.11 (ITSPSR-21A)

mis en oeuvre que la norme WPA intérimaire, avec ses exigences réduites en matière de traitement et sa sécurité plutôt faible.


2.4.2.7 Autres amendements 802.11

De nombreux autres amendements de la norme 802.11 portant sur divers aspects des WLAN sont en cours d'élaboration ou de planification. Par exemple : 802.11e traite des questions liées à la qualité du service sans fil; 802.11p et 802.11r portent sur la mobilité et l'itinérance; 802.11s concerne les réseaux maillés ad hoc; 802.11w est un amendement lié à la sécurité qui a été proposé pour résoudre le problème liée aux trames d'information de gestion réseau transmises sans protection, ni chiffrement; 802.11y propose d'étendre l'utilisation de 802.11 dans la bande de fréquence 3,7 GHz. Une liste complète des amendements 802.11 et des groupes de travail est disponible sur le site Web de l'IEEE.

2.5 Norme d'interopérabilité Wi-Fi™

2.5.1 La Wireless Ethernet Compatibility Alliance (WECA) et la Wi-Fi Alliance

Les fabricants intègrent souvent dans leurs produits des caractéristiques propriétaires qui rendent ces derniers incompatibles avec ceux d'autres compagnies. Pour remédier à cette situation, de nombreux fabricants ont formé la Wireless Ethernet Compatibility Alliance ou WECA en 1999. La WECA a défini une suite de tests [5] pour assurer l'interopérabilité des produits 802.11b et la mise en oeuvre correcte du WEP. Cela s'est étendu rapidement par la suite pour inclure des suites d'interopérabilité pour 802.11g et WPA. En 2002, la WECA a changé son nom pour Wi-Fi Alliance, et au moment de la rédaction du présent document, comptait plus de 320 membres parmi les acteurs de l'industrie et leurs affiliés.

Les produits qui réussissent ces tests sont considérés conformes à la norme **Wi-Fi** (Wireless Fidelity) et sont autorisés à afficher le logo . L'appui populaire accordé à la norme Wi-Fi™ a permis à la famille de produits 802.11b/g de dominer le marché des WLAN.

Quoique souvent utilisés de manière interchangeable dans les médias, les termes 802.11 et Wi-Fi™ ne sont pas synonymes. La norme IEEE 802.11 contient des amendements portant sur tous les aspects des WLAN, et les amendements 802.11a/b/g/n en particulier sont des spécifications des couches physique et contrôle d'accès au support (MAC pour *Medium Access Control*), tandis que Wi-Fi™ n'est qu'une certification d'interopérabilité pour les produits 802.11a/b/g. À l'origine, le terme Wi-Fi ne devait faire référence qu'aux produits interopérables dans la bande des 2,4 GHz, et une désignation Wi-Fi5™ a été créée pour la certification des produits WLAN 802.11a dans la bande des 5 GHz. Or, en raison de la prédominance des produits à double bande prenant en charge les bandes 2,4 GHz et 5 GHz, la certification a été unifiée en une seule certification Wi-Fi. Au moment de la rédaction du présent document, les aspects obligatoires suivants étaient couverts :

1. normes radio pour 802.11a, b et g, y compris la prise en charge de bandes multiples;



Évaluation de la vulnérabilité des réseaux locaux sans fil (WLAN) 802.11 (ITSPSR-21A)

2. mise en oeuvre de la sécurité : WEP, WPA, WPA2;
3. mise en oeuvre de l'authentification : EAP.

La Wi-Fi Alliance offre également des programmes de certification facultatifs pour :

1. l'interopérabilité des produits pour la norme 802.11n, ébauche 2.0;
2. la validation des fonctions de sécurité à « installation facile »;
3. les fonctions multimédia sur Wi-Fi;
4. le Wi-Fi à faible puissance pour les applications multimédias;
5. le Wi-Fi + dispositifs cellulaires combinés (cette certification est obligatoire pour les fabricants de dispositifs combinés recherchant la certification CTIA).

Il est important de noter que les produits certifiés Wi-Fi ne le sont que dans les limites imposées à leur exploitation par les normes 802.11 particulières. Ils peuvent quand même contenir des modes d'exploitation non standard propriétaires qui ne sont pas couverts par les exigences d'interopérabilité Wi-Fi. Par exemple, le débit « amélioré » de 104 Mbps de nombreux dispositifs 802.11 commerciaux n'est pas conforme aux normes 802.11 officielles et un tel mode n'est généralement PAS compatible ou interopérable avec les produits d'autres fabricants; en fait, il pourrait même interférer avec le bon fonctionnement de dispositifs strictement conformes aux normes qui se situent dans les limites de la portée de transmission commune. On conseille aux utilisateurs de vérifier la conformité aux règlements d'Industrie Canada avant d'utiliser ces modes non standard, car certains d'entre eux sont reconnus pour causer des interférences dans l'exploitation des réseaux 802.11 situés à proximité.



Page laissée intentionnellement en blanc.



3 Mécanismes de sécurité

3.1 Généralités

Comme dans tout réseau, la sécurité est un point important à considérer. L'accès non autorisé peut donner lieu à la divulgation d'information, à la modification de données, au déni de service et à l'utilisation illicite des ressources. Dès qu'un utilisateur non autorisé a obtenu l'accès au réseau, la surveillance étroite des données désormais non protégées peut mener à l'interception des noms des utilisateurs et de leurs mots de passe. Il peut ensuite se servir d'eux pour faire d'autres attaques. Les réseaux WLAN souffrent de tous les problèmes de sécurité que l'on rencontre normalement dans les réseaux locaux filaires classiques. En outre, ils souffrent de vulnérabilités attribuables directement à l'utilisation de la connectivité sans fil. En effet, de par la nature même du sans-fil, il est pratiquement impossible de confiner les signaux radio à une région contrôlée. Ces signaux rayonnés peuvent être interceptés et exploités de manière clandestine. Dans un environnement LAN filaire classique, la sécurité physique du lieu de travail assure une certaine protection au réseau, car les utilisateurs doivent s'y connecter physiquement pour accéder à ses ressources. Dans un environnement WLAN, cette protection n'est plus suffisante, car il est possible d'accéder au réseau à distance sans devoir établir de connexion physique : quiconque utilise un matériel sans fil compatible peut, potentiellement, accéder au LAN.

Afin d'atténuer ces préoccupations en matière de sécurité, on fait appel au chiffrement pour tenter de rendre inutilisables les signaux interceptés par toute personne non autorisée. Toutefois, comme c'est le cas dans la plupart des produits commerciaux, la facilité d'emploi pour le consommateur prime avant tout. À ce jour, les options de chiffrement et de sécurité qu'on retrouve dans la majorité des produits WLAN 802.11 sont désactivées par défaut et, lorsqu'elles sont activées, utilisent généralement le schéma le plus faible et le plus simple possible.

3.2 Contrôle de l'accès

3.2.1 Généralités

Le contrôle de l'accès est une exigence fondamentale dans tout réseau sensible. Toutefois, les mécanismes de contrôle d'accès précisés dans la norme IEEE 802.11 sont faibles. Les deux mécanismes suivants, malgré qu'ils sont souvent décrits comme étant des fonctions de sécurité, visent davantage à prévenir les interférences, qu'à constituer une mesure de contrôle d'accès.

3.2.2 Identificateur d'ensemble de services (SSID)

Les PA transmettent des messages de balise pour annoncer leur présence et les paramètres de fonctionnement aux clients. Le SSID fait partie de ce message de balise qui déclare l'identité du PA au réseau. Un client qui cherche à se connecter à un réseau spécifique balaie les signaux pour trouver ce SSID et, quand il découvre le réseau, le processus d'authentification débute. La désactivation de la diffusion de ce SSID empêcherait les clients d'identifier automatiquement le



Évaluation de la vulnérabilité des réseaux locaux sans fil (WLAN) 802.11 (ITSPSR-21A)

PA et de s'y associer et nécessiterait une connaissance préalable du SSID. Malheureusement, ce mécanisme constitue une faille de sécurité étant donné que le SSID, qui n'est plus diffusé dans le message balise, continue d'être envoyé à même le trafic de gestion réseau et peut être reniflé par un attaquant.

3.2.3 Liste de contrôle d'accès (ACL) des adresses MAC

Certains fournisseurs mettent en oeuvre un filtre ou une ACL des adresses MAC (c.-à-d. les adresses Ethernet) afin d'empêcher l'accès non autorisé à un PA. Les adresses MAC des clients autorisés sont entrées et enregistrées dans une liste conservée dans le PA, et seuls les clients qui correspondent aux critères de cette liste sont autorisés à accéder au PA (certaines adresses MAC peuvent également être bloquées de cette manière). Cette mesure de sécurité est inefficace parce que tout le trafic envoyé dans le réseau comporte l'adresse MAC dans un en-tête non chiffré. Par conséquent, il suffit à un attaquant de capturer un seul paquet et d'examiner son en-tête pour déterminer une adresse MAC légitime et la programmer dans son dispositif. Par ailleurs, la mise à jour manuelle de la liste de toutes les adresses MAC autorisées prend du temps et peut donner lieu à des erreurs de saisie, ce qui la rend pratique seulement pour les réseaux de petite taille et plutôt statiques.

3.3 Services d'authentification

3.3.1 Généralités

À la différence des réseaux LAN filaires, les WLAN émettent des signaux sur un support qui ne connaît pas de limite physique. La norme IEEE 802.11 assure un contrôle d'accès par l'intermédiaire du service d'authentification. Tous les dispositifs sans fil utilisent un mécanisme d'authentification afin d'établir leur identité, avant de s'associer au réseau. L'association d'un dispositif sans fil est établie uniquement si l'authentification est acceptée. L'authentification peut être exécutée entre deux dispositifs ou entre un dispositif et un PA. La norme IEEE 802.11 définit deux types d'authentification : le système ouvert et la clé partagée. La norme WPA de la Wi-Fi Alliance et les normes 802.11i/WPA2 ajoutent des modes d'authentification et l'authentification IEEE 802.1X faisant appel au protocole EAP (pour *Extensible Authentication Protocol*) est également prise en charge comme extension facultative pour tous les modes d'authentification natifs.

Il est important de noter que les méthodes d'authentification native authentifient les **dispositifs** et non pas les **utilisateurs** de ces dispositifs. Par ailleurs, dans une configuration infrastructure, l'authentification n'est pas mutuelle. Seul le dispositif client sans fil doit prouver son identité; le PA est implicitement reconnu comme étant un dispositif fiable et le client n'a aucun moyen de vérifier si le PA est légitime. On peut avoir recours à l'authentification 802.1X additionnelle pour corriger ce problème, mais cela nécessite l'utilisation d'un serveur RADIUS ou d'un serveur d'authentification spécialisé et l'infrastructure connexe pour prendre en charge la couche d'authentification supplémentaire.



Évaluation de la vulnérabilité des réseaux locaux sans fil (WLAN) 802.11 (ITSPSR-21A)

3.3.2 Authentification par système ouvert

Le système ouvert offre uniquement l'identification et est essentiellement une authentification « nulle ». Un client qui demande l'accès à un PA envoie simplement son adresse MAC à ce dernier qui répond au moyen d'un message de vérification d'authentification : tout client qui demande une authentification à l'aide de cet algorithme sera authentifié. Ce mode d'authentification est mis en place là où la facilité d'utilisation est prioritaire, ou encore là où la sécurité n'est pas un problème pour un administrateur réseau. On doit souligner que l'authentification par système ouvert est la configuration par défaut dans de nombreux dispositifs WLAN 802.11.

La norme 802.11 permet l'utilisation du chiffrement WEP même avec l'authentification par système ouvert. En pareil cas, les deux dispositifs doivent partager une clé WEP, mais, contrairement à l'authentification par clé partagée décrite dans la section suivante, la clé n'est pas utilisée pour l'authentification, seulement pour le chiffrement. Dans ce mode, un client est authentifié au moyen de l'authentification par système ouvert et les deux extrémités commencent immédiatement une communication chiffrée au moyen du WEP. Ce mode est considéré un peu plus sécurisé que l'authentification par clé partagée car l'information liée à la clé n'est pas échangée en direct.

3.3.3 Authentification par clé partagée

L'authentification par clé partagée est une fonction de la norme 802.11 d'origine et ne peut être utilisée que si les fonctions de sécurité sans fil initiales du dispositif sont activées. Elle ne s'applique pas lorsque WPA ou WPA2/802.11i est utilisé, où un schéma de clé prépartagée semblable mais un peu plus robuste est disponible.

Dans ce mode, la clé partagée secrète est distribuée manuellement et configurée sur toutes les stations participantes. Le processus d'authentification par clé partagée fonctionne selon un schéma interrogation-réponse, où le chiffrement/déchiffrement est exécuté à l'aide du générateur de nombres pseudo aléatoires (PRNG) RC4 du protocole WEP pour valider l'interrogation-réponse. Après réception d'un signal d'acceptation, la liaison est jugée authentifiée. Il est à noter que la norme 802.11 permet également l'authentification par clé partagée sans chiffrement de liaison, mais que pratiquement tous les dispositifs WLAN 802.11 activeront par défaut le chiffrement de liaison si l'authentification par clé partagée est utilisée.

L'authentification par clé partagée visait à fournir un plus grand degré de sécurité que l'authentification par système ouvert. Toutefois, des faiblesses dans le chiffrement WEP utilisé dans le schéma interrogation-réponse peuvent permettre la récupération facile de la clé si cet échange est intercepté par un attaquant. De même, il faut noter également que cette authentification ne fait que confirmer l'identité du matériel et non pas celle de l'utilisateur. Par conséquent, toute personne obtenant l'accès non autorisé à des dispositifs sans fil inscrits dans un réseau peut potentiellement obtenir l'accès au réseau lui-même. Pour cette raison, la méthode précédemment décrite de l'authentification par système ouvert avec le chiffrement WE constitue le mode d'exploitation de prédilection si aucune mesure d'authentification ou de chiffrement



Évaluation de la vulnérabilité des réseaux locaux sans fil (WLAN) 802.11 (ITSPSR-21A)

plus robuste (p.ex., WPA/WPA2) n'est disponible. Or, une authentification adéquate de l'utilisateur est également essentielle, indépendamment du mode sélectionné.

La norme 802.11 ne précise aucun processus ou mécanisme de gestion des clés. Par conséquent, la sécurité des clés partagées relève de l'utilisateur. Comme dans tout système articulé sur une phrase de passe, il faut choisir des phrases passe robustes afin de réduire au minimum la possibilité qu'elles soient devinées et il faudrait les changer régulièrement.

3.3.4 Authentification 802.1X

Les amendements WPA et WPA2/IEEE 802.11i spécifient tous deux l'utilisation obligatoire d'une autre norme, IEEE 802.1X, pour l'authentification réseau. 802.1X est une norme Ethernet (de la famille IEEE 802.1; non propre aux LAN sans fil) qui fournit un cadre pour l'authentification, en sus de diverses méthodes (comme les mots de passe, les cartes à puces, les certificats, etc.) utilisées pour vérifier l'identité. La norme 802.1X fonctionne au niveau de la couche MAC pour restreindre l'accès réseau aux entités autorisées. La connectivité réseau est fournie par le concept de ports, chacun représentant une association entre une station client et un point d'accès. De plus, la norme précise trois entités qui participent à la transaction d'authentification : le demandeur (*supplicant*), l'authentificateur (*authenticator*) et le serveur d'authentification (*authentication server*). Le demandeur (client sans fil) est une entité qui désire utiliser un service offert par l'intermédiaire d'un port sur l'authentificateur (point d'accès sans fil). Un réseau type peut comprendre plusieurs ports disponibles par l'intermédiaire desquels un demandeur peut être authentifié afin d'accéder à un service. Le serveur d'authentification est l'entité qui vérifie l'identité du demandeur soumise à l'authentificateur et indique à celui-ci d'accorder l'accès si la vérification est valide.

La norme IEEE 802.1X utilise le protocole EAP (*Extensible Authentication Protocol*) pour permettre l'utilisation d'une gamme variée de mécanismes d'authentification. Comme l'authentification par clé partagée, le protocole EAP repose sur un schéma interrogation-réponse utilisant quatre types distincts de message: *EAP Request* (demande EAP), *EAP Response* (réponse EAP), *EAP Success* (réussite EAP) et *EAP Failure* (échec EAP). Le protocole EAP est considéré comme étant extensible parce que ces messages peuvent servir à encapsuler pratiquement n'importe quel type de mécanisme d'authentification quoique, dans la pratique, seulement un ensemble limité de protocoles soit pris en charge par le matériel WLAN commercial. Dans l'authentification reposant sur le protocole EAP, le message *EAP Request* est envoyé au demandeur, indiquant une interrogation à la quelle le demandeur répond au moyen du message *EAP Response*. Dépendant de la méthode d'authentification utilisée, cet échange interrogation-réponse peut être répété plusieurs fois et dans les deux sens (afin de permettre l'authentification mutuelle) pour échanger des données d'authentification jusqu'à ce que le message *EAP Success* ou *EAP Failure* soit envoyé pour autoriser ou refuser la demande de connexion, respectivement.

L'utilisation de l'authentification 802.1X a le potentiel d'accroître grandement la sécurité d'une installation LAN, spécialement qu'il est possible d'orienter la méthode d'authentification vers l'utilisateur individuel plutôt que vers le dispositif, ce qu'on recommande d'utiliser dans la



Évaluation de la vulnérabilité des réseaux locaux sans fil (WLAN) 802.11 (ITSPSR-21A)

mesure du possible. À noter toutefois que, dans la plupart des cas, un réseau utilisant l'authentification 802.1X nécessite l'installation d'une infrastructure spécialisée sous la forme d'un serveur d'authentification (serveur RADIUS). De plus, même lorsqu'on utilise une authentification sur serveur, il est important de sélectionner une méthode qui réponde aux exigences de sécurité nécessaires, car les méthodes EAP n'ont pas toutes été créées égales. Des méthodes s'intégrant à l'infrastructure à clé publique (ICP), l'authentification à deux facteurs à l'aide d'un jeton, etc., sont disponibles mais la plupart des dispositifs prennent en charge au moins la méthode EAP-TLS qui repose sur le protocole TLS (*Transport Layer Security*).

Comme il a été décrit plus haut, les protocoles WPA et WPA2/802.11i mettent tous deux en oeuvre un schéma d'authentification par clé prépartagée qui ne nécessite pas de serveur d'authentification externe et qui est destiné aux réseaux de petite taille (à domicile, etc.). Comme l'authentification par clé partagée initiale, ce schéma compte sur l'interrogation-réponse tirée d'une clé partagée pour authentifier un dispositif. Le mécanisme fait appel à l'établissement de liaisons à 4 sens reposant sur les échanges 802.1X et est beaucoup plus robuste que l'interrogation-réponse du RC4; il est quand même vulnérable aux attaques si on utilise une phrase de passe faible. De plus, l'utilisation du mode d'authentification PSK souffre des mêmes lacunes que le mécanisme initial, à savoir celles liées à la gestion des clés et à l'authentification utilisateur contre l'authentification du dispositif.

3.4 Confidentialité des données et WEP/WPA/802.11i/WPA2

3.4.1 Généralités

La norme IEEE 802.11 d'origine spécifie un mécanisme facultatif de confidentialité des données, faisant appel au protocole WEP. Ce mécanisme vise à protéger les réseaux WLAN contre l'écoute clandestine épisodique non autorisée, et à assurer l'intégrité des données. Depuis sa publication, le protocole WEP a exhibé plusieurs faiblesses qui ont donné lieu au développement de mesures de sécurité et de confidentialité des données plus rigoureuses. Comme il a été documenté plus tôt, le groupe de travail I de l'IEEE 802.11 a été formé pour se pencher sur le sujet. Le processus étant très long, la Wi-Fi Alliance a publié une norme intérimaire appelée *Wi-Fi Protected Access* (WPA) qui reposait sur une première ébauche de ce qui allait éventuellement devenir la norme 802.11i. Étant donné que les deux normes de sécurité améliorées se sont avérées largement compatibles, la Wi-Fi Alliance a également adopté la 802.11i, désormais connue sous le nom de *Wi-Fi Protected Access version 2* (WPA2). Quoique les normes WEP/WPA/WPA2 soient strictement facultatives dans la norme 802.11, elles sont obligatoires pour la certification de conformité Wi-Fi™.



3.4.2 Protocole WEP (*Wired Equivalent Privacy*)

3.4.2.1 Propriétés du protocole WEP

Le protocole WEP emploie l'algorithme PRNG RC4, mis au point par RSA Data Security, Inc. Le RC4 est un algorithme de chiffrement en continu, conçu en 1987 par Ronald Rivest. Il utilise une clé symétrique de taille variable, indépendante du texte en clair, pour produire le texte chiffré (cryptogramme). Le protocole WEP a été conçu pour être :

- a. raisonnablement robuste (difficile à percer par une attaque par force brute);
- b. autosynchronisable (le protocole WEP s'autosynchronise pour chaque message);
- c. efficace sur le plan informatique (peut être mis en oeuvre dans le matériel ou les logiciels);
- d. exportable dans tous les pays;
- e. facultatif (sa mise en oeuvre est toutefois requise pour obtenir la désignation de produit Wi-Fi™ selon la norme 802.11).

3.4.2.2 Principes de fonctionnement du protocole WEP

Le chiffrement en continu RC4 fonctionne comme suit : il s'agit de développer une clé secrète et un vecteur d'initialisation (IV pour *Initialization Vector*) de 24 bits, concaténé à une clé prépartagée (généralement la même clé ayant servi au stade d'authentification), en un flot de clés de longueur arbitraire composé de bits pseudo aléatoires. Le chiffrement s'obtient par l'exécution d'une opération OU exclusive (XOR) entre le flot de clés et le texte en clair, pour produire le cryptogramme. Le déchiffrement se fait par génération du flot de clés identique, basé sur le vecteur d'initialisation et la clé secrète, et par application du OU exclusif sur le cryptogramme, pour récupérer le texte en clair. On trouvera plus de détails sur le fonctionnement du protocole WEP dans la norme IEEE 802.11 [1].

De nombreux fournisseurs offrent des produits conformes à la norme 802.11b, qui prennent en charge le protocole WEP 40 bits et 104 bits. Certains fournisseurs désignent le protocole WEP 40 bits par l'appellation WEP 64 bits, et WEP 104 bits par l'appellation WEP 128 bits. Cette différence provient du fait que le vecteur d'initialisation de 24 bits est transmis en clair, ce qui en fait réduit l'efficacité du protocole WEP 64 bits à un chiffrement de 40 bits. De plus, le protocole WEP 128 bits est en fait un chiffrement par clé secrète de 104 bits, plus 24 bits pour le vecteur d'initialisation. Plusieurs fournisseurs de produits 802.11a ont ajouté des longueurs WEP non standard. Par exemple, une marque populaire de produits 802.11 utilise un WEP de 152 bits ou un « vrai 128 bits » qui consiste en un vecteur d'initialisation de 24 bits et une clé de 128 bits, tandis qu'une autre marque offre un WEP de 256 bits (il s'agit en fait de 232 bits seulement à cause du vecteur d'initialisation). Les lecteurs doivent toutefois prendre note que de tels modes nécessitent du matériel et des logiciels correspondants aux deux extrémités (PA et client sans fil) pour fonctionner. Compte tenu de la faiblesse de l'algorithme WEP, ces clés plus longues ne sont pas considérées plus sécurisées que la version de base. Seul le protocole WEP 40 bits est spécifié dans la norme 802.11b et les exigences de désignation Wi-Fi™. Les autres longueurs de



Évaluation de la vulnérabilité des réseaux locaux sans fil (WLAN) 802.11 (ITSPSR-21A)

protocole WEP sont des initiatives de l'industrie qui, du point de vue de la sécurité, peuvent être plus ou moins bien réalisées.

Les faiblesses théoriques de WEP ont été signalées par Walker [8, 7] dès 2000, et les premières attaques pratiques contre WEP, apparues en 2001 [9], ont démontré qu'il n'était pas un mécanisme de protection robuste. Le protocole WEP présente des lacunes importantes en matière de sécurité qui peuvent être exploitées et donner lieu à la divulgation d'information, à l'accès non autorisé au réseau et à des attaques par saturation (déni de service). Compte tenu de ces vulnérabilités, WEP n'est pas efficace comme mesure de sécurité principale et son utilisation n'est pas recommandée pour la protection des données du gouvernement du Canada. Il est impératif que le matériel ancien qui ne prend pas en charge une sécurité plus forte que le WEP soit remplacé ou mis à niveau.

3.4.3 Le protocole WPA (*Wi-Fi Protected Access*)

La Wi-Fi Alliance a créé le système Wi-Fi Protected Access (WPA) pour tenter de corriger les vulnérabilités de WEP sur le plan de la sécurité. Le protocole WPA constituait une solution intérimaire de remplacement de WEP en attendant que la norme 802.11i officielle ait été développée. En fait, WPA repose sur une première ébauche de la norme 802.11i, dont les éléments clés d'information de trame ont été intentionnellement changés pour éviter toute possibilité de conflits entre WPA et la version 802.11i publiée.

Le protocole WPA avait sensiblement le même but que WEP; une sécurité améliorée constituait l'objectif principal, mais le nouveau schéma devait être pris en charge par le parc matériel existant. Pour ce faire, on a retenu RC4 pour chiffrer les flux de données à cause de ses exigences faibles en matière de traitement, mais on l'a enveloppé (*wrapped*) pour couvrir les insécurités de WEP.

Plusieurs améliorations majeures ont été apportées au WPA pour accroître sa sécurité : une clé secrète de 128 bits et un vecteur d'initialisation plus grand (48 bits) sont utilisés, des clés individuelles séparées sont utilisées dans chaque direction de même que pour la validation de l'intégrité, et un nouveau processus d'ordonnancement des clés appelé Temporal Key Integrity Protocol (TKIP) a été ajouté. Le protocole TKIP change continuellement et dynamiquement les clés pendant que le système fonctionne. Combiné au vecteur d'initialisation plus long, il vient remédier aux vulnérabilités liées à la récupération des clés dans WEP.

En ce qui a trait au TKIP, la sécurité des clés a été améliorée de deux façons. D'abord, lorsque le mode à clé prépartagée est utilisé, on a éliminé la pratique d'utiliser la clé partagée et le vecteur d'initialisation public directement comme clé de chiffrement maîtresse (même clé utilisée pour toutes les opérations en amont comme en aval), comme c'était le cas dans WEP. Dans le WPA, une biclé maîtresse (la PMK, qui, dans ce mode, est identique à la clé partagée) est combinée à d'autres données échangées durant l'authentification dans une procédure appelée *4-Way Handshake*, un échange de 4 messages pour déduire une biclé propre à la session, la *Pairwise Transient Key* ou PTK qui, à son tour régit la génération de la clé dynamique TKIP (de même que la génération de clés pour d'autres services WPA connexes). À noter toutefois que ce mode



Évaluation de la vulnérabilité des réseaux locaux sans fil (WLAN) 802.11 (ITSPSR-21A)

d'exploitation ne résout aucun des problèmes de distribution et de gestion de la PSK. Deuxièmement, lorsqu'un serveur d'authentification 802.1X est utilisé, celui-ci générera une PMK aléatoire au lieu d'utiliser une clé fixe, améliorant par le fait même la sécurité.

En plus des changements apportés à l'authentification et au chiffrement, WPA améliore également la sécurité entourant l'intégrité des messages. Le contrôle de redondance cyclique faible de 32 bits (CRC32) utilisé dans le WEP a été remplacé par un code d'intégrité de message MIC pour *Message Integrity Code* reposant sur une clé, et par un compteur de trames pour prévenir les attaques par réinsertion (*replay*). Quoiqu'il soit meilleur à détecter les erreurs que le CRC32, l'algorithme MIC (appelé Michael) utilisé dans le WPA est toujours considéré comme étant faible du point de vue cryptographique puisqu'il s'agit d'un algorithme renversible, comme le CRC32, conçu pour pouvoir s'exécuter sur de vieilles plateformes ayant une puissance de traitement limitée. Le protocole WPA met en oeuvre également une contremesure de mystification MIC qui est supposée désactiver la connexion sans fil pendant une minute lorsqu'elle détecte plus de deux trames qui échouent le contrôle d'intégrité MIC dans un intervalle d'une minute. Malheureusement, parce que le système est sans fil et qu'il est sujet aux interférences RF, les trames bruitées occasionnelles peuvent toujours réussir tous les contrôles d'intégrité les plus simples, déclencher le contrôle MIC et entraîner l'arrêt du réseau; les attaquants peuvent également profiter de ce mécanisme pour créer des dénis de service. Pour cette raison, il est possible que certains dispositifs commerciaux ne mettent pas en oeuvre cette contremesure ou permettent qu'elle soit désactivée, ce qui a pour effet d'augmenter quelque peu les risques d'attaques par mystification (*spoofing*) mais d'accroître également la robustesse générale du réseau.

3.4.4 Le protocole WPA2 (IEEE 802.11i/Wi-Fi Protected Access version 2)

La norme d'amélioration de la sécurité 802.11i n'a été ratifiée officiellement par l'IEEE qu'en 2004. En raison de sa rétrocompatibilité avec la norme WPA intérimaire, la norme 802.11i est connue sous le nom de WPA2. Dès 2006, tous les produits commerciaux doivent prendre en charge les mesures de sécurité préconisées par WPA2 pour pouvoir être certifiés Wi-Fi.

WPA2 continue de prendre en charge le mode d'exploitation par clé prépartagée (PSK), lequel peut compliquer la gestion et la distribution des clés même lorsque le nombre d'utilisateurs sans fil est modéré. Comme avec WPA, WPA2 prend en charge le protocole EAP de 802.1X; toutefois la Wi-Fi Alliance exige maintenant la validation d'une gamme plus variée de méthodes EAP 802.1X sous WPA2 dans le cadre de son programme de certification.

D'une importance primordiale dans WPA2 est l'introduction d'un algorithme de chiffrement reposant sur AES appelé *Counter-mode with CBC-MAC Protocol* ou CCMP, qui consiste en un mode d'enchaînement de blocs de chiffrement AES de 128 bits avec un contrôle intégré de l'intégrité des messages (MAC 64 bits), de même qu'un compteur pour la protection contre les attaques de réinsertion des paquets.

À noter que la définition WPA2 continue d'accepter les anciens mécanismes RC4/TKIP/Michael aux fins de rétrocompatibilité, mais que le chiffrement CCMP, dès qu'il est activé, vient



Évaluation de la vulnérabilité des réseaux locaux sans fil (WLAN) 802.11 (ITSPSR-21A)

remplacer complètement ces mécanismes par d'autres plus robustes et corrige des lacunes qu'on retrouve dans de nombreux mécanismes WPA. Le protocole CCMP est maintenant utilisé pour renforcer les phases d'authentification et d'échange de clés, et le mécanisme Michael faible est remplacé par le CBC-MAC intégral dans CCMP. Ces mesures, et d'autres mesures introduites dans WPA2 forment la nouvelle architecture de réseau de sécurité robuste (RSN pour *Robust Security Network*) 802.11i, qui vient remédier aux défauts des normes de réseau sans fil précédentes. Les utilisateurs du gouvernement du Canada devraient noter que l'AES-CCMP est un mécanisme approuvé par le gouvernement pour sécuriser les données allant jusqu'au niveau PROTÉGÉ B inclusivement et que, si l'utilisation des WLAN est appuyée par une évaluation appropriée des menaces et des risques, l'utilisation de WPA2 est obligatoire pour les WLAN du GC (aux États-Unis, le NIST exige également l'utilisation du CCMP pour sécuriser les WLAN IEEE 802-11 des agences fédérales) [21].

Enfin, WPA2 permet d'utiliser en option un autre mécanisme AES appelé WRAP (*Wireless Robust Authenticated Protocol*). Ce mécanisme avait été sélectionné à l'origine par le comité 802.11i. Il utilise l'AES dans le mode OCB (*Offset Code Book*), considéré légèrement plus robuste que le mode CCMP. Il a toutefois été abandonné en faveur du mode CCMP à cause de problèmes liés à la propriété intellectuelle et la possibilité d'imposition de droits de permis.



Évaluation de la vulnérabilité des réseaux locaux sans fil (WLAN) 802.11 (ITSPSR-21A)

Page laissée intentionnellement en blanc.



4 Vulnérabilités

4.1 Vulnérabilités des mécanismes de contrôle d'accès

4.1.1 Généralités

La norme 802.11b ne gère pas adéquatement le contrôle d'accès. Les deux fonctionnalités suivantes offrent seulement une forme restreinte de contrôle d'accès.

4.1.2 SSID

La fonctionnalité SSID sert à identifier le réseau, mais pas à titre de mesure de sécurité. Malheureusement, on croit souvent à tort que l'utilisation du SSID équivaut à une protection par mot de passe. Le SSID contenu dans la trame de balise est toujours transmis en clair, peu importe si l'option WEP est activée ou non. Tout client sans fil, malveillant ou non, peut être à l'écoute de cette balise pour obtenir le SSID et contourner ce contrôle d'accès de bas niveau.

4.1.3 Liste de contrôle d'accès (ACL) pour les adresses MAC

Certains fournisseurs de produits 802.11 offrent une fonction dite *MAC Address ACL*, c'est-à-dire une liste de contrôle d'accès pour les adresses MAC, qui offre un contrôle d'accès minimal en limitant l'accès uniquement aux cartes sans fil autorisées. Malheureusement, les paquets qui contiennent les adresses MAC sont transmis en clair et les entrées dans la liste ACL peuvent facilement être obtenues par surveillance du trafic. Un utilisateur non autorisé peut usurper ces adresses MAC et tenter d'accéder au PA. La plupart du temps, le PA comporte la configuration en usine pour l'ID utilisateur et le mot de passe de l'administrateur. Quand un utilisateur non autorisé a accédé au PA, il peut en modifier la configuration.

4.2 Vulnérabilités du mécanisme d'authentification

4.2.1 Généralités

Le mécanisme d'authentification défini dans la norme 802.11 sert à donner aux liaisons sans fil les mêmes normes de sécurité physiques que celles des liaisons filaires. Cependant, la conception et la mise en oeuvre de ce service présentent des vulnérabilités.

4.2.2 Lacune de l'authentification par clé partagée

Le mécanisme d'authentification par clé partagée est utilisé avant qu'une association soit autorisée. Pendant la séquence interrogation-réponse, l'interrogation en clair et la réponse chiffrée sont transmises. Cela présente une vulnérabilité potentielle pour la sécurité, car une personne malveillante pourrait découvrir la paire clé-IV utilisée pour la séquence d'authentification. La norme 802.11 recommande d'éviter d'utiliser la même paire clé-IV pour la trame suivante transmise, mais rien ne garantit que cette recommandation soit suivie dans les faits. Pour cette raison, comme il a été noté plus haut dans le présent document, l'utilisation



Évaluation de la vulnérabilité des réseaux locaux sans fil (WLAN) 802.11 (ITSPSR-21A)

simultanée de l'authentification par système ouvert et de WEP est considérée généralement **plus** sécurisée puisque l'information liée à la clé n'est pas transmise.

4.2.3 Vulnérabilités liées au 802.1X/EAP

Introduit pour la première fois dans le WPA, le cadre 802.1X a le potentiel d'améliorer grandement les capacités d'authentification des réseaux sans fil 802.11. L'ironie de la chose, c'est que le protocole d'authentification spécifié dans la norme 802.1X est vulnérable aux attaques principalement à cause de son incapacité à authentifier ses propres messages. À cause de cette lacune, il est possible de forger les messages EAP dans un scénario d'attaque de l'homme au milieu (*man-in-the-middle*) permettant à un attaquant de contourner le mécanisme d'authentification ou de détourner une session 802.11. [20]

4.3 Vulnérabilités de WEP

4.3.1 Généralités

De nombreux rapports et articles [6, 7, 8, 9, 10, 11] ont été publiés au sujet des vulnérabilités que représente pour la sécurité la mise en oeuvre du protocole WEP. Ces rapports portent sur la sécurité minimale offerte par ce protocole, notamment sur les lacunes suivantes :

- a. probabilité élevée de réutilisation des clés, en raison de la courte longueur du vecteur d'initialisation (IV) – dans un réseau achalandé, la réutilisation de l'IV se produit suffisamment souvent pour permettre à un pirate d'obtenir la clé en quelques minutes ou en quelques heures);
- b. faiblesse du message d'authentification due à la courte longueur de clé utilisée
- c. absence d'une spécification de gestion des clés.

4.3.2 Réutilisation du flot de clés

En raison de l'utilisation d'un vecteur d'initialisation relativement court (24 bits), il est fort probable que, après une courte période de temps sur un réseau sans fil actif, l'IV sera réutilisé. Cela pourrait faciliter une attaque contre le système visant à récupérer du texte en clair [7]. Cette vulnérabilité existe, peu importe que le protocole WEP utilisé soit à 64 bits ou 128 bits.

4.3.3 Intégrité des messages

La somme de contrôle CRC-32 est utilisée pour assurer l'intégrité des paquets pendant leur transmission. Il est possible d'apporter des modifications contrôlées au texte chiffré, sans pour autant modifier la somme de contrôle annexée au message, et ainsi injecter des messages sans qu'ils ne soient détectés [9].

4.3.4 Gestion des clés

La clé partagée distribuée est l'aspect le plus faible du système. En utilisant des clés partagées statiques, distribuées entre les clients sous forme de « mots de passe », le nombre d'utilisateurs



Évaluation de la vulnérabilité des réseaux locaux sans fil (WLAN) 802.11 (ITSPSR-21A)

connaissant ces clés augmentera à mesure que le réseau croîtra. Cela crée les problèmes suivants :

- a. une clé partagée entre de nombreuses personnes ne demeure pas secrète très longtemps;
- b. la distribution manuelle de la clé partagée peut être fastidieuse et prendre passablement de temps, notamment dans les grandes organisations où les utilisateurs sont nombreux. Très souvent, le résultat est que la clé n'est pas modifiée aussi souvent qu'elle le devrait;
- c. la fréquence de réutilisation de l'IV augmente avec l'accroissement du réseau, ce qui le rend plus vulnérable aux attaques.

4.4 Vulnérabilités liées au WPA/WPA2

4.4.1 Généralités

Les protocoles WPA et WPA2 ont introduit des mesures conçues pour corriger les principales vulnérabilités du WEP. Or, de nouvelles vulnérabilités sont apparues et certaines vulnérabilités sont demeurées, particulièrement dans WPA à cause de l'exigence liée à la rétrocompatibilité et aux exigences faibles en matière de calcul.

4.4.2 Gestion des clés

Quoique la prise en charge de l'authentification 802.1X ait été rendue obligatoire dans WPA et WPA2, elle requiert l'emploi d'un serveur d'authentification externe de sorte que l'utilisateur a également l'option d'utiliser un simple mécanisme de clé prépartagée comme WEP. Malheureusement, comme avec le WEP, le mécanisme d'authentification à clé prépartagée de WPA et WPA2 est vulnérable aux problèmes de gestion de clé : il est pratiquement impossible de garder secrète une seule clé partagée au sein d'un large groupe d'utilisateurs; pareillement, la remise à la clé et la distribution de nouvelles clés sont difficiles à réaliser pour un large groupe.

4.4.3 Vulnérabilité de l'échange de 4 messages et de phrase de passe faible

Le mécanisme de clé prépartagée permet l'utilisation de fonctions de sécurité dans WPA et WPA2 là où l'infrastructure 802.1X additionnelle n'est pas disponible. Comme dans le cas de la clé partagée dans WEP, tous les utilisateurs partagent une clé « secrète » commune. Quoique la clé prépartagée soit utilisée dans une biclé maîtresse (PMK) dans WPA et WPA2, la clé partagée dans WPA, contrairement à WEP, n'est pas utilisée directement comme clé de chiffrement, mais elle est plutôt combinée à d'autres informations propres à la session durant la procédure d'échange de 4 messages (*4-Way Handshake*) pour générer une biclé transitoire, la PTK, qui à son tour sert à générer des clés dynamiques de chiffrement et d'intégrité des messages.



Évaluation de la vulnérabilité des réseaux locaux sans fil (WLAN) 802.11 (ITSPSR-21A)

Quoique les problèmes liés à la faible longueur de la clé et à la réutilisation de l'IV soient résolus par ce mécanisme, une clé prépartagée dans WPA et WPA2 est maintenant vulnérable aux attaques par dictionnaire. En captant l'échange d'authentification à 4 messages et en utilisant cette information avec un fichier dictionnaire, il est possible de deviner facilement les clés de session si la clé prépartagée est l'un des mots figurant dans le dictionnaire. Si la clé partagée est courte ou très simple, il est possible de la trouver au moyen d'une recherche exhaustive (*brute force search*). Une attaque par dictionnaire qui réussit peut mener à deux scénarios : 1) les clés de session récupérées peuvent être utilisées pour écouter ou interrompre une session en cours; 2) la PSK récupérée peut être utilisée pour lancer une nouvelle session et accéder aux ressources du réseau sans autorisation. Si ce mécanisme doit être utilisé, il est impératif qu'une phrase de passe longue ne représentant aucun mot de dictionnaire soit utilisée pour sécuriser le point d'accès.

4.4.4 Contremesure de mystification WPA MIC

Comme il a été décrit plus haut dans le présent document, l'algorithme Michael MIC dans WPA a été sélectionné pour assurer l'équilibre entre l'intégrité des données, la sécurité et les exigences réduites en matière de traitement afin qu'il puisse être pris en charge par le matériel LAN sans fil existant. Quoiqu'il représente une amélioration sur l'algorithme CRC32 original utilisé dans WEP, l'algorithme Michael est renversable et sa clé peut être découverte, ce qui le rend vulnérable aux attaques de mystification. Pour remédier à cette vulnérabilité, les concepteurs de la norme WPA ont mis en oeuvre une contremesure de mystification qui interrompt la connexion sans fil pendant une minute si plus de deux mauvais MIC sont reçus à l'intérieur d'une période d'une minute. Malheureusement, cette contremesure constitue elle-même une vulnérabilité parce qu'elle peut servir de porte d'accès aux attaques par déni de service (en injectant délibérément de mauvais MIC dans les paquets) et, dans les environnements RF bruyants où les erreurs de paquets sont communes, cette contremesure peut accidentellement déclencher l'interruption de la liaison et nuire de manière négative à la robustesse du réseau sans fil.

4.5 Valeurs par défaut de la configuration

Afin de simplifier le processus de configuration initiale, de nombreux fournisseurs offrent une configuration par défaut établie en usine, qui assure très peu de sécurité. Par exemple, certains paramètres par défaut, définis en usine par le fournisseur, permettent la configuration du PA à partir du segment sans fil. De plus, ils ne mettent en oeuvre aucune sécurité et utilisent les paramètres système par défaut documentés, comme les adresses IP, le mot de passe de l'administrateur et le SSID.

De nombreux PA ont un bouton de remise à zéro facilement accessible qui rétablit la configuration du dispositif à ses paramètres d'usine par défaut, ce qui nécessiterait un degré de sécurité physique ou de contrôle d'accès pour empêcher cette fonction.

Récemment, on a introduit sur le marché des PA qui permettent d'activer des paramètres de sécurité, mais pour les besoins d'une configuration simple et facile, plusieurs d'entre eux



Évaluation de la vulnérabilité des réseaux locaux sans fil (WLAN) 802.11 (ITSPSR-21A)

n'utiliseront que WEP avec seulement une clé de 40 bits, même si le dispositif peut accepter des mécanismes plus robustes.

4.6 Protocole SNMP (*Simple Network Management Protocol*)

De nombreux PA conformes à la norme 802.11 prennent en charge la gestion des dispositifs sans fil par l'intermédiaire du protocole SNMP (*Simple Network Management Protocol*). Souvent, cette fonction permet à une personne de voir l'information du système et de configuration et, dans certains cas, il lui est même possible de mettre à jour cette information. L'accès à cette information est normalement restreint par l'utilisation d'une chaîne de communauté, qui **n'est pas** un mot de passe, mais simplement un identificateur donné au réseau SNMP. Il s'agit habituellement d'une valeur bien connue, qui peut être obtenue au moyen d'une simple recherche Internet ou qui peut être devinée facilement (p. ex. : GouvernementduCanada, MDN ou MAECI).



Évaluation de la vulnérabilité des réseaux locaux sans fil (WLAN) 802.11 (ITSPSR-21A)

Page laissée intentionnellement en blanc.



5 Exploits

5.1 Attaques par découverte de réseau et accès

5.1.1 Généralités

La « conduite guerrière » ou « piratage Wi-Fi » (*war driving*) est similaire dans son essence à la « composition automatique de numéros » (*war dialing*). Cette dernière, une technique que les pirates informatiques emploient depuis plusieurs années, fait appel à des logiciels qui composent automatiquement et systématiquement des numéros de téléphone afin de découvrir des modems vulnérables qui permettraient de se connecter à un réseau. La conduite guerrière exploite le même type de vulnérabilité que la composition automatique de numéros : l'attaquant se déplace en véhicule avec un client sans fil portatif, à la recherche de points d'entrée non protégés dans un réseau sans fil. La conduite guerrière est devenue un sport au sein de la communauté des pirates qui mettent régulièrement à jour sur Internet (p. ex., www.wigle.net) des cartes de points d'accès sans fil pour les communautés partout dans le monde. Dans la plupart des cas, la conduite guerrière représente le défi de découvrir un nouveau point d'accès avant tout autre pirate, et l'accès illicite au réseau n'est pas réalisé. Il existe toutefois à l'heure actuelle de nombreux outils commerciaux et gratuits de piratage qui exploitent les vulnérabilités des réseaux sans fil 802.11, décrites dans le présent document, et qui peuvent être utilisés par des individus malveillants pour pénétrer dans un réseau.

5.1.2 Découverte de réseau

Les outils de découverte ou de vérification de réseau sont des types de logiciel mis au point afin d'aider les administrateurs réseau à gérer et à dépanner les problèmes liés aux réseaux. Comme la plupart des outils de vérification de réseau sont assez sophistiqués et coûteux, ils ne sont pas recherchés pour la conduite guerrière. Toutefois, on trouve dans le domaine public divers logiciels gratuits de découverte de réseau, très simples à utiliser [13] et permettant de balayer les ondes à la recherche de réseaux. Ils peuvent enregistrer des renseignements détaillés, y compris l'identificateur SSID, l'adresse MAC du point d'accès, l'information sur le fournisseur, le rapport signal/bruit et si des fonctions de sécurité sont activées ou non. Un pirate équipé d'un tel logiciel, d'un portatif configuré pour la norme 802.11 et d'un récepteur GPS (système de positionnement global) peut déterminer exactement la latitude et la longitude des points d'accès, outre l'information susmentionnée.

5.1.3 Accès réseau par routeur sans fil

La plupart des PA vendus de nos jours sont pourvus d'un routeur intégré sur lequel les services DHCP (*Dynamic Host Configuration Protocol* – protocole de configuration dynamique de l'hôte) sont souvent activés. Ces routeurs sans fil sont particulièrement vulnérables aux attaques par détournement de bande passante. Quand un routeur sans fil est découvert, un attaquant n'a qu'à demander une adresse IP au serveur DHCP, ou encore réamorcer le portatif et une adresse



Évaluation de la vulnérabilité des réseaux locaux sans fil (WLAN) 802.11 (ITSPSR-21A)

IP lui sera automatiquement assignée. Si les fonctions de sécurité ne sont pas activées, l'attaquant aura un accès complet au réseau ciblé.

5.2 Attaques par saturation (dénier de service)

5.2.1 Généralités

Une attaque par saturation (dénier de service ou *denial of service*) est l'une des attaques les plus faciles et les plus répandues réalisées contre les réseaux informatiques. Ce type d'attaque consiste habituellement à accaparer ou surcharger les ressources d'un réseau, de façon à en empêcher l'exploitation normale.

5.2.2 Capture d'un point d'accès

De nombreux PA utilisent le protocole SNMP ou une interface basée sur le Web pour les tâches de configuration et de gestion. Si le mot de passe de la communauté ou de l'administrateur est mal configuré ou si on utilise la valeur par défaut, un intrus peut obtenir du PA même de l'information sensible sur la configuration. L'intrus peut également être capable de récrire l'information dans le PA et, à toute fin pratique, prendre possession de celui-ci, déniaient ainsi l'accès des clients légitimes au réseau.

5.2.3 Clonage de PA

Le clonage des PA est parfois appelé « hameçonnage au point d'accès » (*evil twin attack*). Un attaquant installe un PA malveillant, ou un ordinateur portable équipé d'une carte sans fil et des logiciels appropriés, et diffuse le même SSID, mais à une puissance du signal RF plus forte que celle du PA ciblé, de sorte que les clients sans fil s'associent au PA illicite. Par défaut, la plupart des cartes clients passeront au PA le plus puissant pour assurer la connexion. Règle générale, les clients s'authentifieront auprès du nouveau PA, fournissant par le fait même à l'attaquant un ensemble de justificatifs d'identité valides qu'il pourra utiliser pour se connecter au vrai PA. L'attaquant qui contrôle le PA illicite a donc la possibilité d'exploiter toute faiblesse de sécurité pouvant exister sur les dispositifs clients associés de façon erronée à la station de base illicite. Le clonage des PA est une technique plus difficile que le simple déni d'accès des clients à une station de base, car il requiert la mise en place physique d'un PA modifié, ou d'un ordinateur portable et d'une carte sans fil émettant à une puissance plus grande que celle du PA visé ou situé physiquement plus près de ce dernier.

5.2.4 Brouillage des radiofréquences

Une attaque par brouillage des radiofréquences n'est pas la même chose qu'une attaque par surcharge des ressources réseau. Au lieu de créer des données illégales en nombre afin d'écraser sous la quantité les dispositifs réseau, le brouillage des RF vise à accaparer le support de transmission, dans ce cas-ci, les ondes radios. En effet, l'attaquant équipé d'outils très simples peut facilement inonder de bruit les ondes utilisées par le réseau (dans le cas des réseaux de type 802.11b/g/n, il s'agit de la bande de fréquence de 2,4 GHz). Le brouillage RF est très efficace,



Évaluation de la vulnérabilité des réseaux locaux sans fil (WLAN) 802.11 (ITSPSR-21A)

car il opère contre toutes les mesures de sécurité du WLAN. Quand du bruit est injecté à la fréquence de fonctionnement d'un réseau WLAN, le rapport signal/bruit chute en deçà d'un niveau acceptable et le réseau cesse tout simplement de fonctionner.

5.3 Attaques contre le protocole WEP

5.3.1 Généralités

L'algorithme WEP facultatif, défini dans la norme IEEE 802.11, était censé assurer une confidentialité des données équivalente à celle d'un réseau filaire non protégé de base. De nombreux rapports et articles [10, 11, 14, 15] ont été publiés au sujet des attaques qui exploitent les diverses faiblesses et lacunes conceptuelles du protocole WEP. Ces attaques sont faciles à exécuter à l'aide d'appareils couramment disponibles. Les attaques s'appliquent autant aux versions 40 bits et 104 bits du protocole WEP, de même qu'à d'autres variantes de longueur de clé non standard.

5.3.2 Attaques passives

Dans une attaque passive, l'attaquant exploite la faiblesse de réutilisation du vecteur d'initialisation (IV) du flot de clés, due à la piètre mise en oeuvre de l'algorithme RC4 par le protocole WEP. Un dispositif d'écoute intercepte tout le trafic sans fil, recueille les paquets quand il y a collision des données IV et effectue une analyse statistique de ces paquets pour en déduire la clé de chiffrement. La clé de chiffrement peut ensuite être utilisée pour accéder au réseau WLAN. On peut trouver gratuitement sur Internet des outils qui effectuent ce type d'attaque [15, 16].

5.3.3 Attaques actives

Deux types différents d'attaques actives peuvent être réalisés contre une installation WLAN 802.11. Le premier type consiste à créer ou à modifier des paquets et à les injecter dans le réseau, à des fins malveillantes, et nécessite l'accès au côté filaire du réseau. L'injection de paquets de texte en clair, puis l'interception de la version chiffrée de ces paquets connus, quand ils sont radiodiffusés à travers le réseau, permettent à un attaquant d'extraire le flot de clés utilisé. Ce type d'attaque permet également d'injecter des commandes ou des virus malveillants dans le réseau.

L'autre type d'attaque peut s'effectuer entièrement sur le côté sans fil du réseau. Cette catégorie d'attaques, qui comprend les attaques par mystification, les attaques de l'homme au milieu et les attaques par injection de paquets peuvent toutes être réalisées à partir du côté sans fil du réseau. Par exemple, une version active d'une attaque contre la vulnérabilité liée à la réutilisation de l'IV de WEP est possible et mettrait en jeu une mystification et l'injection de paquets dans le réseau sans fil, ce qui donnerait lieu au retour de paquets comportant différents IV. À cause de cette propriété, cette version active peut réduire considérablement le temps nécessaire pour recueillir des paquets dans la version passive de l'attaque décrite plus haut et peut permettre à un attaquant de casser WEP en secondes ou minutes au lieu d'heures ou de jours. De même, il est



Évaluation de la vulnérabilité des réseaux locaux sans fil (WLAN) 802.11 (ITSPSR-21A)

possible de porter une attaque active contre le contrôle d'intégrité CRC [22] faible en interceptant un paquet chiffré, en modifiant des portions choisies qui ne sont pas adéquatement protégées par le CRC et en les remplaçant par une valeur devinée et en rediffusant le paquet modifié. En devinant les valeurs, en remplaçant progressivement les diverses portions d'un paquet et en surveillant le comportement du réseau durant la retransmission, l'attaquant peut déchiffrer des paquets chiffrés par WEP sans connaître la clé.

Quoique les attaques actives puissent être extrêmement efficaces, elles sont généralement plus difficiles à mettre en oeuvre que les attaques passives car elles requièrent une compréhension plus poussée des protocoles en jeu de même qu'un certain degré de connaissances dans le domaine des radiofréquences. Par ailleurs, l'attaquant risque davantage d'être détecté lors d'une attaque active étant donné qu'il doit diffuser ou injecter des paquets dans le réseau.

5.3.4 Attaque contre la table de déchiffrement

En utilisant les diverses techniques décrites dans les articles précédents, un attaquant peut déterminer plusieurs flots de clés et construire une table de déchiffrement qu'il pourrait utiliser pour déchiffrer chaque paquet qui utilise le même IV. Comme les vecteurs d'initialisation sont transmis en clair, il serait très facile alors d'en apparier un à un flot de clés dans la table et de décoder par conséquent le message. De plus, on peut utiliser la table de déchiffrement pour créer de nouveaux paquets comportant des flots de clés connus et donc créer de faux paquets et les injecter dans le réseau.

Pour construire cette table, le pirate n'a qu'à enregistrer 1 500 octets de flot de clés, pour chacun des 2^{24} vecteurs d'initialisation possibles, ce qui représente à peu près 24 gigaoctets d'espace [9]. Le niveau de difficulté pour déterminer les flots de clés dépend de la taille de l'IV (24 bits), et non de la clé partagée (40 bits). Les réseaux WLAN qui utilisent une clé de 104 bits (128 bits) sont plus difficiles à attaquer de cette façon, mais demeurent néanmoins vulnérables.

5.4 Attaques contre WPA et WPA2

5.4.1 Généralités

Les améliorations qu'apportent les protocoles WPA et WPA2 à la norme 802.11 viennent grandement élever le niveau de sécurité et de robustesse des réseaux sans fil où ils sont mis en oeuvre. Quoiqu'il existe toujours des faiblesses et des vulnérabilités, peu d'exploits pratiques ont été recensés.

5.4.2 Attaques de dictionnaire de clés prépartagées

Les protocoles WPA et WPA2 tentent de renforcer la sécurité en utilisant des clés multiples pour toutes les opérations et ce, dans les cas où une clé prépartagée est utilisée; toutes ces clés additionnelles sont dérivées de la même clé partagée, laquelle peut être récupérée au moyen d'une attaque par dictionnaire ou même d'une recherche exhaustive sur le deuxième message du processus d'échange à 4 messages de 802.11i. Plusieurs outils gratuits sont disponibles pour



Évaluation de la vulnérabilité des réseaux locaux sans fil (WLAN) 802.11 (ITSPSR-21A)

ceux qui cherchent à exploiter cette faiblesse. L'exploitation de la vulnérabilité de la PSK est atténuée par l'emploi de l'authentification 802.1X sur serveur. Toutefois, si le mécanisme de la PSK doit être utilisé, il faut recourir à une phrase de passe longue ne figurant dans aucun dictionnaire.

5.5 Attaques par surveillance et interception

5.5.1 Généralités

Les attaques par surveillance et interception consistent à recueillir de l'information de manière passive. La vulnérabilité de ce type d'attaque n'est pas apparente, mais elle est tout aussi dangereuse et ne devrait pas être négligée.

5.5.2 Reniflage de trafic

Une fois qu'un attaquant a, à l'aide des techniques de découverte de réseau, identifié un réseau sans fil qui devient alors sa cible, il peut y mettre en place un renifleur pour surveiller le trafic sur ce réseau. Des versions modifiées des pilotes de dispositif permettent à la carte client sans fil du pirate de fonctionner en mode espion (*promiscuous mode*), ce qui rend cette attaque passive furtive et intraçable. La seule contrainte à laquelle doit se soumettre l'attaquant est qu'il doit se trouver à portée de transmission du réseau sans fil, mais cette portée peut facilement être élargie à quelques centaines de mètres, grâce à l'utilisation d'une antenne.

Comme le format des paquets 802.11 est une norme connue, il est facile d'analyser les paquets capturés pour obtenir de l'information essentielle. Ce type d'information peut ensuite servir à faciliter des attaques contre le protocole WEP, si cette fonction de sécurité a été activée. Certains produits commerciaux [17, 18] peuvent faire cette analyse en temps réel, à mesure que les paquets sont capturés.

5.5.3 Surveillance des signaux diffusés

À la différence d'un commutateur, un concentrateur envoie tout le trafic à tous les dispositifs connectés, plutôt qu'au seul destinataire voulu. Un PA connecté à un concentrateur plutôt qu'à un commutateur pourrait donc recevoir et rediffuser des paquets de données qui ne sont pas destinés à des clients sans fil. Cela permettrait à un attaquant de surveiller le trafic sensible du côté filaire du réseau.

5.5.4 Attaque *man-in-the-middle*

La plupart des PA conformes à la norme 802.11 fonctionnent comme des passerelles transparentes au niveau de la couche MAC, ce qui permet aux paquets ARP (protocole de résolution des adresses) de circuler entre les réseaux filaires et sans fil. Ce mécanisme permet l'exécution d'attaques « homme au milieu » contre deux machines sur les réseaux filaires, connectées au même commutateur ou concentrateur que le PA. En utilisant de faux paquets ARP, un attaquant peut réacheminer le trafic vers son propre client sans fil, avant que le trafic



Évaluation de la vulnérabilité des réseaux locaux sans fil (WLAN) 802.11 (ITSPSR-21A)

n'atteigne les deux hôtes ciblés.



6 Solutions

6.1 Aperçu

La présente section comprend certaines lignes directrices provisoires qui sont essentielles pour atteindre un certain degré de confiance dans l'exploitation sécurisée d'un WLAN. Les solutions pour un environnement WLAN plus sécurisé seront publiées au fur et à mesure qu'elles deviendront disponibles. Dans l'intervalle, il faudrait mettre en oeuvre immédiatement les mesures ci-après pour améliorer la posture de sécurité du WLAN :

- a. Déterminer la zone de couverture du réseau et la garder petite;
- b. Ne pas diffuser le SSID;
- c. Ne pas utiliser le SSID par défaut;
- d. Utiliser WPA2;
- e. Utiliser l'authentification 802.1X sur serveur ;
- f. Changer les clés fréquemment;
- g. Mettre en place un RPV et un pare-feu pour isoler davantage le WLAN;
- h. Utiliser un pare-feu personnel sur chaque client sans fil;
- i. Considérer l'utilisation de systèmes de prévention/détection d'intrusions sans fil

6.2 Déterminer la zone de couverture du réseau

Faites appel à un renifleur sans fil ou à un ordinateur portable capable d'utiliser le réseau 802.11b afin de déterminer la distance maximale à laquelle le WLAN est accessible à partir de chaque point d'accès. Cela vous donnera une bonne idée de la distance à laquelle un attaquant non sophistiqué doit se trouver pour accéder à votre réseau ou réaliser une écoute clandestine. Rappelez-vous qu'il est possible d'utiliser des antennes à gains élevés et/ou des amplificateurs pour intercepter les communications radio à partir d'une distance encore plus grande. Si les données circulant dans votre WLAN sont extrêmement précieuses ou sensibles et qu'elles pourraient être la cible d'individus ayant accès à du matériel plus sophistiqué, il faudra que vous en teniez compte au moment de déterminer la zone de couverture de votre réseau.

Si la couverture de votre WLAN s'étend à une aire publique adjacente, à un parc de stationnement ou simplement à une distance dangereusement trop grande, vous devrez appliquer des mesures de sécurité additionnelles. Certaines marques de dispositifs WLAN vous permettent de changer le niveau de la puissance de transmission : régler ce paramètre au plus bas niveau possible vous aidera à réduire la zone de couverture de votre réseau et, par conséquent le risque qu'on y accède sans autorisation ou qu'on y effectue une écoute clandestine. Adapter des réflecteurs aux antennes équidirectives standard ou remplacer ces dernières par des antennes directives vous permettra de faire converger l'énergie RF vers les zones de couverture voulues et loin des zones indésirables et constituera un moyen très efficace et relativement peu coûteux de contrôler la couverture du WLAN. Il peut être complètement impossible d'empêcher les ondes



Évaluation de la vulnérabilité des réseaux locaux sans fil (WLAN) 802.11 (ITSPSR-21A)

radios de quitter votre immeuble sans faire appel à une cage de Faraday¹. Une telle mesure doit toutefois être considérée pour les endroits où sont traités des renseignements hautement sensibles et où l'accès sans fil est également une exigence. Des mesures physiques de ce genre sont extrêmement coûteuses et ne sont probablement pas rentables pour la plupart des cas, ce qui rend l'utilisation d'un chiffrement robuste pour protéger l'information une solution de rechange acceptable.

6.3 Ne pas diffuser le SSID

Les PA des fournisseurs sont réglés par défaut pour diffuser le nom ou le SSID du réseau afin de permettre aux utilisateurs de voir le réseau et de s'y joindre rapidement et facilement. Les intrus adeptes de la conduite guerrière parcourent les rues en voiture avec leurs renifleurs sans fil afin de trouver tous les réseaux qui radiodiffusent leur présence et de noter leurs coordonnées. Si les fonctions de sécurité sans fil ne sont pas activées sur votre WLAN, quiconque voit votre réseau peut s'y joindre. La plupart des fournisseurs vous permettront de désactiver la radiodiffusion du SSID. Bien que cela ne constitue pas une solution de sécurité complète, cela peut prévenir certaines tentatives d'attaque ou d'écoute clandestine.

6.4 Ne pas utiliser le SSID par défaut

Les SSID par défaut de la plupart des points d'accès sont généralement connus. En les utilisant, vous rendez inopérant l'aspect de secret partagé du SSID et vous affaiblissez davantage votre système. Encore là, cette précaution ne constitue pas une protection à toute épreuve, mais elle peut contrer certaines tentatives d'attaque ou d'écoute clandestine.

6.5 Utiliser WPA2

Le mécanisme de sécurité sans fil initial, le protocole WEP, présente des faiblesses et s'est révélé inefficace comme mesure de sécurité. Compte tenu du grand nombre de programmes de craquage de WEP disponibles gratuitement, ne préviendra que certaines tentatives d'écoute clandestine. La dernière norme de sécurité WPA2/802.11i est robuste (particulièrement lorsque l'authentification 802.1X est également utilisée, [voir la section suivante]), corrige pratiquement toutes les faiblesses de WEP et fait appel à un chiffrement AES très robuste. Le CSTC recommande l'utilisation de WPA2 dans tous les réseaux sans fil 802.11, particulièrement là où la sécurité et la confidentialité sont importantes.

Par conséquent, seul le matériel prenant en charge la sécurité sans fil WPA2 devrait être considéré pour les nouvelles acquisitions et le matériel existant qui ne prend pas en charge cette norme devrait être mis à niveau ou remplacé dans la mesure du possible.

¹ Enceinte métallique ajourée connectée à la masse, conçue pour former un filtre électrostatique. Peut être obtenue par l'intermédiaire d'un mur ou d'un plancher conducteur, de carreaux de plafond conducteurs ou de peintures conductrices. On peut utiliser ce dispositif pour filtrer les signaux émis par les systèmes d'information et comme protection contre la foudre et d'autres radiations à haute énergie.



Évaluation de la vulnérabilité des réseaux locaux sans fil (WLAN) 802.11 (ITSPSR-21A)

Lorsque la sécurité et la confidentialité priment avant tout, il est possible que WPA2 ne suffise pas et qu'il faille considérer d'autres options. Par exemple, l'ajout de produits robustes de chiffrement des données comme les réseaux privés virtuels pourraient grandement atténuer ce risque d'atteinte à la sécurité.

6.6 Utiliser l'authentification 802.1X sur serveur

Jusqu'à maintenant, WPA2 s'est révélé un mécanisme de sécurité robuste présentant relativement peu de vulnérabilités. Il est toutefois possible de le renforcer à l'aide de l'authentification 802.1X sur serveur. L'utilisation d'un serveur externe permet de mettre en oeuvre l'authentification et le contrôle d'accès utilisateur, et de les intégrer aux autres mécanismes de sécurité qui pourraient déjà exister, notamment les cartes à puces, les jetons de sécurité, l'ICP, la biométrie, etc.

6.7 Changer les clés fréquemment

Chaque fois qu'on fait appel au chiffrement, il faut changer les clés fréquemment afin de réduire au minimum la quantité de données qui peuvent être traitées par une seule clé. Cela rend la tâche plus difficile à l'attaquant qui doit recueillir suffisamment de données pour compromettre la clé. Cela réduit également la période pendant laquelle la clé compromise peut être utile à l'attaquant. Cette pratique s'applique aussi au chiffrement utilisé dans les produits WLAN – si l'authentification 802.1X sur serveur n'est pas disponible et que le mode à clé prépartagée doit être utilisé, il est impératif que la phrase de passe soit changée à intervalles réguliers pour assurer la sécurité du réseau.

6.8 Mettre en place un RPV et un pare-feu pour isoler le WLAN

Dans la plupart des cas, la couverture d'un WLAN déborde de l'aire sécurisée du site d'exploitation. Il faut donc considérer le WLAN comme un réseau hostile, tout comme Internet. Un pare-feu devrait alors être mis en place pour isoler le réseau local filaire interne du point d'accès du WLAN et de tous les clients sans fil. Un RPV, un tunnel Secure Shell (SSH) et le chiffrement bout-à-bout peuvent constituer des solutions supplémentaires pour protéger le trafic à qui circule à l'intérieur des réseaux locaux filaire et sans fil et entre ceux-ci.

6.9 Utiliser un pare-feu personnel sur chaque client sans fil

Les clients sans fil sont très vulnérables. Il leur faut une protection sous forme de pare-feu personnel pour filtrer à la fois le trafic entrant et le trafic sortant. On peut également utiliser ces produits pour leurs capacités d'authentification améliorées.



6.10 Considérer l'utilisation de systèmes de détection/prévention d'intrusions sans fil

On peut se procurer maintenant des systèmes de détection d'intrusions sans fil (WIDS pour *Wireless Intrusion Detection System*) et des systèmes de prévention d'intrusions sans fil (WIPS pour *Wireless Intrusion Prevention System*) pour compléter les systèmes de détection d'intrusions conçus pour les infrastructures filaires. Ces systèmes utilisent des capteurs qui se présentent sous la forme de récepteurs sans fil spécialisés pour surveiller une zone de couverture en vue de détecter les tentatives d'accès au réseau protégé par des clients non autorisés. De plus, ils détectent la présence des points d'accès illicites ou mal configurés, l'utilisation de connexions réseau ad-hoc, les tentatives de mystification d'adresses MAC et les tentatives de lancement d'attaques par saturation (dénier de service). Lorsque plusieurs capteurs sont placés à l'intérieur de la zone de couverture, le WIDS peut même déterminer l'emplacement physique de l'intrus par triangulation et, par exemple, tracer cet emplacement sur le plan de l'immeuble. Les produits de prévention d'intrusions sans fil peuvent également assurer une défense active contre l'accès non autorisé : certains de ces systèmes peuvent transmettre des paquets spécialement confectionnés pour empêcher un client non autorisé d'accéder à un réseau, désactiver un point d'accès illicite ou mal configuré, ou même empêcher certaines formes de déni de service sans fil. À noter toutefois que ces paquets confectionnés ne sont généralement pas conformes à la norme 802.11 et qu'il faudrait les tester avant de les activer afin de s'assurer qu'ils ne bloqueront pas le trafic et les dispositifs licites et qu'ils ne créeront aucune interférence avec ceux-ci.



7 Travaux futurs

Le CSTC continue de rechercher des solutions qui atténueront les vulnérabilités associées aux WLAN et mettra à jour le présent document dès que de l'information pertinente deviendra disponible. Le CSTC est en train d'élaborer une recommandation pour l'architecture WLAN sécurisée du GC afin d'atténuer davantage les risques auxquels elle est exposée.

D'ici là, les ministères du GC peuvent communiquer avec les Services à la clientèle du CSTC pour obtenir des recommandations et des conseils au sujet de la sécurité des WLAN : client.svcs@cse-cst.gc.ca ou (613) 991-7654.



Évaluation de la vulnérabilité des réseaux locaux sans fil (WLAN) 802.11 (ITSPSR-21A)

Page laissée intentionnellement en blanc.



8 Conclusions et recommandations

À la différence des réseaux locaux filaires, les réseaux locaux sans fil utilisent un support qui ne connaît aucune limite physique. Dans un WLAN, les données sont diffusées dans les airs par l'intermédiaire d'ondes radio qui peuvent être captées par tout client WLAN dans la zone desservie par l'émetteur. Comme les ondes radio traversent les plafonds, les planchers et les murs, les données transmises peuvent donc atteindre des destinataires non voulus sur différents étages, voire à l'extérieur du bâtiment où se trouve l'émetteur. Les problèmes de sécurité importants qui en résultent sont les effets secondaires de la mobilité et de la commodité offertes par un réseau WLAN.

Les dernières révisions de la norme IEEE 802.11 comportent un mécanisme de sécurité amélioré, soit 802.11i ou WPA2 pour l'authentification et la confidentialité des données. Ce mécanisme offre un chiffrement AES robuste et prend en charge pratiquement tout schéma d'authentification par l'intermédiaire de 802.1X. Lorsqu'une méthode d'authentification robuste est sélectionnée, 802.11i/WPA2 vient remédier aux faiblesses des mécanismes de sécurité précédents, y compris les protocoles WEP et WPA. D'après ces constatations, le CSTC recommande que le mécanisme de sécurité WPA2 **soit obligatoirement** activé dans tous les WLAN 802.11 du GC. Le matériel plus ancien doit être mis à niveau ou remplacé par des dispositifs qui prennent en charge WPA2. Dans les cas où on ne peut pas immédiatement mettre à niveau ou remplacer le matériel ancien, il faudrait activer le mécanisme de sécurité le plus robuste qui soit (dans la mesure du possible WPA, sinon WEP), conformément aux lignes directrices documentées dans la présente, et mettre en oeuvre des mesures de sécurité additionnelles tels les RPV afin d'atténuer les risques associés aux mécanismes de sécurité faibles du matériel sans fil.

Il faudrait noter toutefois que les mesures renforcées de WPA2 visent strictement à protéger un WLAN contre les tentatives d'écoute clandestine et à assurer l'intégrité des données. Étant donné que de nombreux aspects de WPA2 sont facultatifs ou qu'ils nécessitent des composants externes additionnels pour une sécurité maximale, il est possible de désactiver ces fonctions. En fait, dans la plupart des déploiements prêts à l'emploi du matériel WLAN, les réglages de sécurité par défaut très faibles constituent la norme. Tout ce dont un utilisateur non autorisé a besoin pour être en mesure d'observer le trafic du réseau sans fil d'une entreprise ou même de se joindre à ce réseau, est le SSID de ce dernier, qu'il peut facilement obtenir au moyen d'outils matériels et logiciels aisément disponibles. Par ailleurs, parce qu'il est difficile de concevoir une solution unique pour résoudre tous les problèmes complexes de sécurité auxquels le WLAN fait face, le protocole WPA2 ne devrait pas être considéré comme étant adéquat pour assurer la protection des renseignements personnels dans les situations où de l'information particulièrement sensible peut être transmise à travers des réseaux sans fil. Dans de telles situations, il faut considérer des mesures de sécurité supplémentaires.



Page laissée intentionnellement en blanc.



9 Références

- [1] « International Standard ISO/IEC 8802-11:1999(E); ANSI/IEEE Std 802.11, 1999 Edition; IEEE Standard for Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. » Organisation internationale de normalisation, Commission électrotechnique internationale et Institute of Electrical and Electronics Engineers, 1999.
- [2] « IEEE Std 802.11a-1999 (Supplement to ANSI/IEEE Std 802.11-1999), Supplement to International Standard ISO/IEC 8802-11:1999(E); ANSI/IEEE Std 802.11, 1999 Edition; IEEE Standard for Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Higher-Speed Physical Layer Extension in the 5 GHz Band », Organisation internationale de normalisation, Commission électrotechnique internationale et Institute of Electrical and Electronics Engineers, 1999.
- [3] « IEEE Std 802.11b-1999 (Supplement to ANSI/IEEE Std 802.11-1999), Supplement to International Standard ISO/IEC 8802-11:1999(E); ANSI/IEEE Std 802.11, 1999 Edition; IEEE Standard for Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Higher-Speed Physical Layer Extension in the 2.4 GHz Band », Organisation internationale de normalisation, Commission électrotechnique internationale et Institute of Electrical and Electronics Engineers, 1999.
- [4] « Wi-Fi: The Standard for Wireless Fidelity », Wireless Ethernet Compatibility Alliance (WECA) Ltd. [En ligne]. Accessible à l'adresse suivante : <http://www.wirelessethernet.org>
- [5] « Wi-Fi System Interoperability Test Plan, Version 1.0 », Wireless Ethernet Compatibility Alliance, février 2000. [En ligne]. Accessible à l'adresse suivante : <http://www.wirelessethernet.org>
- [6] W. A. Arbaugh, N. Shankar et Y.J. Wan, « Your 802.11 wireless network has no clothes », University of Maryland, College Park, Maryland, mars 2001. [En ligne]. Accessible à l'adresse suivante : <http://www.cs.umd.edu/~waa/wireless.pdf>



Évaluation de la vulnérabilité des réseaux locaux sans fil (WLAN) 802.11 (ITSPSR-21A)

- [7] J. R. Walker, « Unsafe at any key size: An analysis of the WEP encapsulation », Intel Corp., Hillsboro, OR, octobre 2000. Doc.: IEEE 802.11-00/362. [En ligne]. Accessible à l'adresse suivante : <http://grouper.ieee.org/groups/802/11/Documents/DocumentHolder/0-362.zip>

- [8] J. R. Walker, « Overview of 802.11 Security », Intel Corp., Hillsboro, OR, mars 2000. Doc.: IEEE 802.15-01/154. [En ligne]. Accessible à l'adresse suivante : http://grouper.ieee.org/groups/802/15/pub/2001/Mar01/01154r0P802-15_TG3-Overview-of-802-11-Security.ppt

- [9] N. Borisov, I. Goldberg et D. Wagner, « Intercepting Mobile Communications: The Insecurity of 802.11 », UC Berkeley. Présenté à la Seventh Annual International Conference on Mobile Computing and Networking, juillet 2001. [En ligne]. Accessible à l'adresse suivante : <http://www.isaac.cs.berkeley.edu/isaac/mobicom.pdf>

- [10] W. A. Arbaugh, « An inductive chosen plaintext attack against WEP/WEP2 », University of Maryland, College Park, Maryland, mai 2001. Doc.: IEEE 802.11-01/230r1. [En ligne]. Accessible à l'adresse suivante : <http://grouper.ieee.org/groups/802/11/Documents/DocumentHolder/1-230.zip>

- [11] S. Fluhrer, I. Mantin, A. Shamir, « Weakness in the Key Scheduling Algorithm of RC4. » Eighth Annual Workshop on Selected Areas in Cryptography, août 2001.

- [12] « Network Stumbler », logiciel. [En ligne]. Accessible à l'adresse suivante : <http://www.netstumbler.com>

- [13] A. Stubblefield, J. Ioannidis, A.D. Rubin, « Using the Fluhrer, Mantin, and Shamir Attack to Break WEP », Rice University, AT&T Labs, août 2001. AT&T Tech. Report TD-4ZCPZZ. [En ligne]. Accessible à l'adresse suivante : <http://www.cs.rice.edu/~astubble/>

- [14] N. Borisov, I. Goldberg et D. Wagner, « (In)Security of the WEP algorithm », UC Berkeley. [En ligne]. Disponible à : <http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html>

- [15] « AirSnort », logiciel. [En ligne]. Accessible à l'adresse suivante : <http://airsnort.sourceforge.net>

- [16] « WEPCrack », logiciel. [En ligne]. Accessible à l'adresse suivante : <http://wepcrack.sourceforge.net>

- [17] « Sniffer Wireless Pro », logiciel. [En ligne]. Accessible à l'adresse suivante : <http://www.sniffer.com>

- [18] « AiroPeek », logiciel. [En ligne]. Accessible à l'adresse suivante : <http://www.wildpackets.com>



Évaluation de la vulnérabilité des réseaux locaux sans fil (WLAN) 802.11 (ITSPSR-21A)

- [19] B. Fleck, J. Dimov, « Wireless Access Points and ARP Poisoning: Wireless vulnerabilities that expose the wired network », Cigital, Inc. [En ligne]. Accessible à l'adresse suivante : <http://www.cigitalabs.com/resources/papers/download/arppoison.pdf>
- [20] A. Mishra, W. Arbaugh, « An Initial Analysis of the IEEE 802.1X Standard », février 2002.
- [21] « Establishing Wireless Robust Security Networks- A Guide to IEEE 802.11i », NIST Publication Number 800-97, février 2007.
- [22] Lehembre, Guillame, « Wi-Fi Security – WEP, WPA and WPA2 », juin 2005, bulletin d'information Hakin9.org .