Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général
de la défense
et de la sécurité nationale

*Agence nationale de la sécurité
des systèmes d'information*

Paris, le 9 septembre 2013

N° DAT-NT-005/ANSSI/SDE/NP

Nombre de pages du document
(y compris cette page) : 13

Note technique

Recommandations de sécurité relatives aux réseaux Wi-Fi

Public visé:

Développeur	
Administrateur	✓
RSSI	✓
DSI	✓
Utilisateur	✓

Informations

Avertissement

Ce document rédigé par l'ANSSI présente les « **Recommandations de sécurité relatives aux réseaux Wi-Fi** ». Il est téléchargeable sur le site www.ssi.gouv.fr. Il constitue une production originale de l'ANSSI. Il est à ce titre placé sous le régime de la « Licence ouverte » publiée par la mission Etalab (`www.etalab.gouv.fr`). Il est par conséquent diffusable sans restriction.

Ces recommandations sont livrées en l'état et adaptées aux menaces au jour de leur publication. Au regard de la diversité des systèmes d'information, l'ANSSI ne peut garantir que ces informations puissent être reprises sans adaptation sur les systèmes d'information cibles. Dans tous les cas, la pertinence de l'implémentation des éléments proposés par l'ANSSI doit être soumise, au préalable, à la validation de l'administrateur du système et/ou des personnes en charge de la sécurité des systèmes d'information.

Personnes ayant contribué à la rédaction de ce document:

Contributeurs	Rédigé par	Approuvé par	Date
BSS, LSF, BAI, FRI	LSF, BSS	SDE	9 septembre 2013

Évolutions du document :

Version	Date	Nature des modifications
1.0	30 Mars 2013	Version initiale
1.2	9 septembre 2013	Corrections mineures et ajouts concernant EAP

Pour toute remarque:

Contact	Adresse	@mél	Téléphone
Bureau Communication de l'ANSSI	51 bd de La Tour-Maubourg 75700 Paris Cedex 07 SP	communication@ssi.gouv.fr	01 71 75 84 04

Table des matières

1 Préambule 3

2 Les risques de sécurité associés au Wi-Fi 3

3 Recommandations principales à respecter 5

4 Pour en savoir plus 8

Annexe 9

A La technologie 9

A.1 La Norme . . . 9
A.2 La réglementation . . . 9

B Les vulnérabilités potentielles 9

B.1 L'accessibilité du matériel . . . 9
B.2 La portée du signal . . . 10
B.3 Les vulnérabilités logicielles . . . 10

C Les protections cryptographiques 10

C.1 Protection des communications radio . . . 10
C.2 Le WEP : une cryptographie inefficace . . . 11
C.3 WPA(TKIP) ou WPA2(AES-CCMP) ? . . . 11
C.4 L'authentification . . . 11
C.5 WPS (*Wi-Fi Protected Setup*) . . . 12

1 Préambule

Le développement des objets communiquants et leur usage quotidien sont aujourd'hui à l'origine de l'omniprésence des réseaux sans-fil Wi-Fi, tant chez les particuliers que dans le monde professionnel. Ces réseaux permettent de connecter tout type de matériel (ordinateurs portables, téléphones mobiles, consoles de jeux, télévisions, équipements électroménagers, automates industriels, etc.) à des réseaux privés ainsi qu'au réseau public Internet. Le Wi-Fi est largement utilisé au sein des réseaux domestiques (par les modems routeurs Internet et autres "Box"), mais également dans le monde professionnel pour la commodité d'accès au réseau interne de l'entreprise, ainsi que pour s'épargner le coût d'une infrastructure filaire.

Ces réseaux Wi-Fi sont toutefois souvent vulnérables, et utilisables par des personnes malveillantes afin d'intercepter des données sensibles (informations personnelles, codes de cartes de paiement, données d'entreprise etc.). Début 2013, près de la moitié des réseaux Wi-Fi n'utilisent aucun moyen de chiffrement ou utilisent un moyen de chiffrement obsolète. Force est de constater que la problématique de sécurisation des réseaux sans-fil n'est pas toujours bien appréhendée et que les risques encourus restent souvent méconnus. Pourtant, quel que soit l'usage envisagé, et si l'équipement utilisé n'est pas trop ancien, il est souvent possible de procéder assez simplement à un paramétrage robuste et sécurisé d'une borne Wi-Fi. Plusieurs aspects de configuration sont à prendre en compte. L'objet de ce document est donc de guider le lecteur dans le choix des meilleurs paramètres pour la bonne sécurisation d'un réseau Wi-Fi. Le particulier non averti y trouvera des recommandations simples à appliquer pour la mise en place d'un réseau Wi-Fi personnel, tandis que l'administrateur réseau en entreprise y trouvera des informations et recommandations complémentaires applicables à un système d'information.

2 Les risques de sécurité associés au Wi-Fi

La compromission d'un réseau sans-fil donne accès à l'ensemble des flux réseaux qui y sont échangés, ce qui inclut bien évidemment les données sensibles. Or, l'interception des flux peut être réalisée assez simplement. De par la multitude d'outils prévus à cet effet et disponibles librement, elle ne nécessite souvent aucune connaissance particulière.

L'accès illégitime à un réseau Wi-Fi par une personne malveillante lui confère une situation privilégiée lui permettant de s'attaquer plus facilement à d'autres ressources du système d'information (postes de travail, serveurs, équipements réseaux) et indirectement d'accéder à d'autres données sensibles.

Par manque de robustesse, les mécanismes cryptographiques intrinsèques aux réseaux Wi-Fi n'apportent parfois qu'une fausse impression de sécurité. Fin 2012, les principaux profils de sécurité sont, par ordre d'apparition :

- le WEP, dont la clé (mot de passe d'accès) est cassable en moins d'une minute ;
- le WPA, de robustesse variable en fonction du paramétrage utilisé ;
- le WPA2, particulièrement robuste ;
- et plus récemment le WPS qui simplifie l'authentification d'un terminal sur un réseau WPA2 (par code PIN par exemple) mais ré-introduit une vulnérabilité importante qui en réduit fortement le niveau de sécurité.

De quoi dépend la sécurité d'un réseau Wi-Fi ?

Les préconisations que l'on peut trouver dans les guides de bonnes pratiques en matière de sécurité Wi-Fi ne sont pas universelles. Certains déploiements peuvent exiger l'activation de paramétrages spécifiques qui, de fait, influeront différemment sur le niveau de sécurité global du réseau sans-fil et des matériels qui s'y connectent.

La simple présence de la technologie Wi-Fi dans un terminal ou un équipement peut suffire à ce qu'il présente des risques de sécurité. Il est donc préférable de se passer de cette technologie lorsqu'elle ne répond à aucun besoin concret. À défaut et lorsque l'utilisation d'un réseau sans-fil est incontournable, la sécurité et la robustesse d'un réseau Wi-Fi et du matériel supportant cette technologie dépendent en général :

- de l'accessibilité du réseau, c'est à dire de la portée des signaux électromagnétiques qui propagent le signal Wi-Fi ;
- des mécanismes d'authentification utilisés afin d'identifier les utilisateurs du réseau de manière univoque et sûre ;
- des mécanismes cryptographiques mis en oeuvre afin de protéger les communications sans-fil, lesquels sont souvent dérivés des mécanismes d'authentification ;
- des mécanismes d'administration et de supervision des points d'accès du réseau et des terminaux utilisant le réseau ;
- d'autres éléments de configuration des points d'accès Wi-Fi.

Sensibilité des données échangées et disponibilité des réseaux.

La technologie Wi-Fi repose sur un lien radio dont les ondes sont par nature sujettes à l'interception et aux interférences (brouillage des ondes accidentel ou intentionnel). En l'absence de moyens de protection complémentaires conformes à la réglementation, il convient alors de ne pas utiliser de lien Wi-Fi pour faire transiter des données sensibles ou critiques comme, par exemple :

- des informations classifiées de défense. Leur protection en confidentialité doit impérativement être assurée par des équipements agréés par l'ANSSI (IGI 1300 [1]) ;
- des informations sensibles à caractère confidentiel ;
- des informations non confidentielles mais dont la disponibilité et l'intégrité sont critiques pour des infrastructures industrielles ou d'importance vitale.

Dans ces contextes, quel que soit le niveau de sécurité des réseaux Wi-Fi pouvant être mis en œuvre, il reste préférable d'utiliser des connexions filaires. À défaut, la confidentialité des informations devra être assurée par l'utilisation de moyens de chiffrement complémentaires tels qu'IPsec ou TLS.

1. http ://www.ssi.gouv.fr/archive/fr/reglementation/igi1300.pdf

Politique de sécurité.

La définition d'une politique de sécurité pour un réseau Wi-Fi est une opération complexe mais primordiale pour un organisme mettant en oeuvre cette technologie. Cette politique doit être ajustée le plus précisément possible, à l'issue d'une analyse de risques, afin de bien identifier les objectifs de sécurité à satisfaire et de lister les mesures de sécurité qui en découlent. Qu'elles soient techniques et/ou organisationnelles, elles ne doivent pas imposer des contraintes irréalistes pour les utilisateurs qui motiveraient ces derniers à les contourner.

Dans tous les cas, la mise en place du Wi-Fi pouvant être une vulnérabilité majeure dans la réalisation du système d'information de l'organisme, cette politique doit être validée au plus haut niveau de l'organisme par une autorité en mesure d'assumer les risques résiduels.

3 Recommandations principales à respecter

L'ANSSI estime qu'il est primordial d'appliquer les 23 recommandations suivantes afin de conserver la maîtrise et le bon usage des réseaux Wi-Fi. Lorsque les points d'accès, les terminaux et plus généralement les systèmes d'information utilisés le permettent, ces recommandations doivent être imposées techniquement. Cela concerne notamment les aspects d'authentification, de protection cryptographique et de mise à jour des terminaux.

Sur tout type de terminaux, personnels ou professionnels :

R1	N'activer l'interface Wi-Fi que lorsqu'elle celle-ci doit être utilisée.

R2	Afin de garder le contrôle sur la connectivité du terminal, désactiver systématiquement l'association automatique aux points d'accès Wi-Fi configurés dans le terminal.

R3	Maintenir le système d'exploitation et les pilotes Wi-Fi du terminal en permanence à jour des correctifs de sécurité.

R4	Éviter tant que possible de se connecter à des réseaux sans fil inconnus ou qui ne sont pas de confiance.

R5	Bloquer, par configuration du pare-feu local, les connexions entrantes via l'interface Wi-Fi.

Sur les terminaux à usage professionnel :

R6	Respecter la politique de sécurité de l'entité, en particulier s'agissant des moyens cryptographiques d'authentification ainsi que de protection en confidentialité et en intégrité qui doivent être mis en oeuvre.

R7	Ne pas brancher de bornes Wi-Fi personnelles sur le réseau de l'entité.

R8	En situation de mobilité, lors de toute connexion à des points d'accès Wi-Fi qui ne sont pas de confiance (par exemple à l'hôtel, la gare ou l'aéroport), préalablement à tout échange de données, utiliser systématiquement des moyens de sécurité complémentaires (VPN IPsec par exemple).

R9	Plus largement, lorsque des données sensibles doivent être véhiculées via un réseau Wi-Fi, l'utilisation d'un protocole de sécurité spécifique, tel que TLS ou IPsec, doit être mis en oeuvre.

Note : L'ANSSI a publié des recommandations de sécurité relatives à IPsec [2] qu'il convient de suivre pour une mise en oeuvre sécurisée de ce protocole.

Sur les points d'accès Wi-Fi :

R10	Configurer le point d'accès pour utiliser un chiffrement robuste. le mode WPA2 avec l'algorithme de chiffrement AES-CCMP est fortement recommandé. Pour les points d'accès personnels, utiliser le mode d'authentification WPA-PSK (WPA-Personnel) avec un mot de passe long (une vingtaine de caractères par exemple) et complexe, d'autant plus que ce dernier est enregistré et n'a pas besoin d'être mémorisé par l'utilisateur.

Note : L'utilisation d'un mot de passe faible peut réduire à néant la sécurité du réseau Wi-Fi. La notion de complexité d'un mot de passe est abordée dans les recommandations de sécurité relatives aux mots de passe [3].
Note : L'usage d'un réseau Wi-Fi ouvert, c'est à dire sans authentification ni chiffrement, peut toutefois s'avérer opportun s'il donne uniquement accès à des équipements permettant de monter un VPN (tunnel IPsec par exemple). Dans ce cas précis, l'authentification et la confidentialité des communications est assurée par le tunnel.

R11	Lorsque l'accès au réseau Wi-Fi n'est protégé que par un mot de passe (WPA-PSK), il est primordial de changer régulièrement ce dernier mais également de contrôler sa diffusion. En particulier, il convient de : – ne pas communiquer le mot de passe à des tiers non autorisés (prestataires de services par exemple) ; – ne pas écrire le mot de passe sur un support qui pourrait être vu par un tiers non autorisé ; – changer le mot de passe régulièrement et lorsqu'il a été compromis.

R12	Pour les réseaux Wi-Fi en environnement professionnel, mettre en oeuvre WPA2 avec une infrastructure d'authentification centralisée en s'appuyant sur WPA-Entreprise (standard 802.1x et protocole EAP), ainsi que des méthodes d'authentification robustes.

Note : Un abonné à un réseau Wi-Fi protégé par WPA-PSK peut très simplement intercepter les données échangées par un autre abonné de ce même réseau. L'utilisation de WPA-PSK ne permet donc pas de garantir la confidentialité des flux entre terminaux connectés à un même réseau Wi-Fi. En environnement professionnel, EAP reste alors à privilégier.

2. http ://www.ssi.gouv.fr/IMG/pdf/NP_IPsec_NoteTech.pdf
3. http ://www.ssi.gouv.fr/IMG/pdf/NP_MDP_NoteTech.pdf

Note : Différentes méthodes d'authentification basées sur le protocole EAP peuvent être utilisées, mais certaines sont à éviter car elles peuvent présenter des vulnérabilités. Parmi les méthodes d'authentification EAP les plus robustes associées au label WPA-Entreprise, figurent :

- EAP-TLS, qui exige toutefois une Infrastructure de Gestion de Clés (IGC), avec clé privée et certificat à déployer auprès de chaque utilisateur. Lorsqu'EAP est utilisé, il convient par ailleurs que les clients vérifient l'authenticité du serveur d'authentification ;
- EAP-TTLS, qui ne nécessite que le déploiement de certificats X509 serveurs et peut donc s'avérer plus pratique lorsqu'il est difficile de déployer des certificats clients. Ceux-ci s'authentifient alors généralement par couple utilisateur/mot de passe. Le support EAP-TTLS n'étant pas natif sous Windows, il convient de s'assurer qu'il est pris en charge par les clients Wi-Fi potentiels ;
- PEAP, similaire à EAP-TTLS mais nativement pris en charge par Windows.

R13	Configurer le *Private VLAN* invité en mode *isolated* lorsque que le point d'accès Wi-Fi prend en charge cette fonctionnalité.

Note : La fonction de *Private VLAN* contribue à la protection en confidentialité des flux entre terminaux connectés à un même réseau Wi-Fi. Chaque client est alors comme dans un VLAN qui lui est propre, empêchant ainsi les communications entre clients.

R14	Ne pas conserver un nom de réseau (SSID) générique et proposé par défaut. Le SSID retenu ne doit pas être trop explicite par rapport à une activité professionnelle ou une information personnelle.

Note : Conserver un SSID par défaut peut fortement réduire la sécurité d'un réseau Wi-Fi en mode WPA-PSK.

R15	Désactiver systématiquement la fonction WPS (Wi-Fi Protected Setup) des points d'accès.

Note : WPS simplifie l'authentification d'un terminal sur un réseau WPA2 (par code PIN par exemple) mais ré-introduit une vulnérabilité importante qui en réduit fortement l'intérêt du point de vue de la sécurité. Cette fonctionnalité est détaillée en annexe.

R16	Sécuriser l'administration du point d'accès Wi-Fi, en : – utilisant des protocoles d'administration sécurisés (HTTPS par exemple) ; – connectant l'interface d'administration à un réseau filaire d'administration sécurisé, *a minima* en y empêchant l'accès aux utilisateurs Wi-Fi ; – utilisant des mots de passe d'administration robustes.

R17	Configurer le point d'accès pour que les évènements de sécurité puissent être supervisés. En environnement professionnel, il est préférable de rediriger l'ensemble des évènements générés par les points d'accès vers une infrastructure centrale de supervision.

R18	Maintenir le micrologiciel des points d'accès à jour.

Concernant l'architecture réseau :

R19	Ne jamais sous-estimer la zone de couverture d'un réseau Wi-Fi. Ne jamais penser être à l'abri de tout risque du fait de l'isolement géographique du point d'accès Wi-Fi.

Note : L'usage d'antennes directionnelles ou le réglage de la puissance des antennes permettent de contrôler la zone de couverture.

R20	En environnement professionnel, isoler le réseau Wi-Fi du réseau filaire et mettre en place des équipements de filtrage réseau permettant l'application de règles strictes et en adéquation avec les objectifs de sécurité de l'organisme. Comme pour le point d'accès, l'équipement de filtrage doit être paramétré pour que puissent être supervisés les évènements de sécurité.

R21	Si un réseau Wi-Fi "visiteurs" doit être mis en place, il est recommandé de déployer une infrastructure dédiée à cet usage, isolée des autres et ne donnant accès à aucune ressource du réseau interne. Ce réseau doit par ailleurs avoir sa propre politique de sécurité beaucoup plus restrictive.

En environnement Active Directory :

R22	Mettre en oeuvre les GPO nécessaires à l'application de stratégies de sécurité verrouillant les configurations Wi-Fi des postes clients Windows, de manière à appliquer techniquement différentes recommandations indiquées dans ce document.

R23	Afin de ne pas les communiquer aux utilisateurs, déployer sur les postes Windows les informations de connexion au Wi-Fi par GPO (nom de réseau, clé d'accès, certificats éventuels si la méthode EAP le nécessite, etc.).

4 Pour en savoir plus

Pour approfondir le sujet de la sécurisation des réseaux Wi-Fi et disposer ainsi de plus d'éléments justifiant ces recommandations, le lecteur est invité à lire l'annexe de ce document qui est une mise à jour de la note d'information CERTA-2002-REC-002 [4] publiée en 2002 et actualisée en 2008.

4. http ://www.certa.ssi.gouv.fr/site/CERTA-2002-REC-002/

Annexe

A La technologie

A.1 La Norme

Le Wi-Fi est une technologie de transmission d'information sans-fil, standardisée par l'IEEE sous la norme 802.11. Il permet de transporter des données numériques, c'est à dire des datagrammes IP, de la même manière qu'un réseau filaire Ethernet mais sans les mêmes garanties de confidentialité, d'intégrité, et de disponibilité.

Ses variantes sont :

- 802.11a : transmission sur la bande de fréquences à 5 GHz, utilisation de l'OFDM (*Orthogonal Frequency Division Multiplexing*) avec modulation simple des sous-porteuses ;
- 802.11b : transmission sur la bande de fréquences à 2.4 GHz, utilisation d'une modulation simple après étalement spectral ;
- 802.11g : transmission sur la bande de fréquences à 2.4 GHz, utilisation de l'OFDM avec une modulation optimisée des sous-porteuses.
- 802.11n : optimisation des mécanismes de transmission radio, notamment avec le MIMO (*Multiple Input Multiple Output*) ;
- 802.11ac : récente optimisation du 802.11n ;
- 802.11i : profils de sécurité pour l'authentification, le chiffrement et le contrôle d'intégrité des liaisons Wi-Fi.

La Wi-Fi Alliance délivre les labels aux produits supportant les éléments importants de la norme IEEE.

A.2 La réglementation

Ce document n'a pas vocation à couvrir les aspects réglementaires. Néanmoins, certaines réglementations qui s'appliquent aux réseaux Wi-Fi sont à prendre en compte, en particulier :

- le "code des postes et des communications électroniques" qui réglemente l'utilisation des différentes bandes de fréquences radio et, sur les bandes autorisées, les niveaux maximum de puissance d'émission ;
- la loi "informatique et liberté" qui s'applique aux traitements de données à caractère personnel.

B Les vulnérabilités potentielles

B.1 L'accessibilité du matériel

Les interfaces Wi-Fi des matériels traitent les données Wi-Fi dès qu'elles sont activées. Elles recherchent par exemple les points d'accès Wi-Fi disponibles en réalisant des balayages des bandes de fréquences, et répondent aux sollicitations (trame de type *PROBE REQUEST*) venant d'autres interfaces Wi-Fi. Il est ainsi possible de détecter les interfaces Wi-Fi dans une zone donnée, puis via leur adresse MAC (identifiant unique associé à la carte) de déterminer leur fabricant, modèle et numéro de série.

D'autre part, lorsqu'une interface Wi-Fi est configurée pour se connecter automatiquement à des réseaux connus, celle-ci va scanner régulièrement les fréquences Wi-Fi à la recherche des SSID de ces réseaux Wi-Fi. Il est par conséquent possible, en étant dans la même zone de couverture, de connaître les réseaux Wi-Fi auxquels un terminal accède régulièrement.

B.2 La portée du signal

La norme et la réglementation sont faites pour obtenir un réseau sans fil de faible portée avec un signal exploitable jusqu'à 100 mètres environ en ligne directe. En réalité, il est possible d'aller bien au-delà de cette distance en utilisant :

- un émetteur/récepteur Wi-Fi disposant d'une bonne sensibilité et d'une puissance d'émission accrue [5] ;
- une antenne à fort gain sur la bande de fréquences visée.

Nota Bene : Il est rappelé que l'emploi de moyens particuliers dans le but d'accéder frauduleusement à un système d'information et/ou d'intercepter des correspondances est pénalement répréhensible.

B.3 Les vulnérabilités logicielles

Même si les interfaces Wi-Fi s'appuient sur une puce matérielle radio, elles restent pilotées grâce à du code logiciel :

- microcode embarqué dans la puce matérielle ;
- code installé sur le système d'exploitation hôte de l'interface Wi-Fi (le pilote, entre autres).

Ces briques logicielles peuvent souffrir de bogues et de failles de sécurité. Étant donné qu'elles s'exécutent dans la majorité des cas avec le plus haut privilège du système, l'exploitation de telles vulnérabilités peut mettre en péril la sécurité des terminaux et des données qui y résident, ainsi que la sécurité des point d'accès Wi-Fi.

C Les protections cryptographiques

C.1 Protection des communications radio

Les technologies de communications sans-fil répondent à des normes précises à des fins d'interopérabilité. Par défaut, elles sont peu souvent protégées contre des écoutes ou modifications illégales.

Lors de sa publication initiale en 1997, le norme IEEE 802.11 n'incluait pas de profils de protection cryptographique. Aujourd'hui encore, on peut trouver de nombreux réseaux Wi-Fi qui ne proposent pas de protection cryptographique. Les protocoles radio et les mécanismes de modulation et de codage Wi-Fi peuvent sembler complexes, mais force est de constater qu'il est extrêmement facile de reconfigurer n'importe quel matériel à bas coût pour pouvoir écouter des canaux radio Wi-Fi et ainsi, intercepter les communications transportées sur des canaux Wi-Fi non chiffrés.

5. En France, la limite de puissance d'émission maximale autorisée est de 100 mW en rayonnement isotrope.

C.2 Le WEP : une cryptographie inefficace

La norme Wi-Fi prévoit des profils de protection cryptographique afin de répondre à la problématique de confidentialité et d'intégrité des liaisons radio. La norme WEP (*Wired Equivalent Privacy*) avait tout d'abord été mise en place. Cependant, ses caractéristiques cryptographiques sont mauvaises :

- elle ne propose pas de méthode d'authentification efficace, ni de méthode automatique de renouvellement de clé de chiffrement ;
- elle s'appuie sur l'algorithme de chiffrement par flot RC4 et l'utilise de manière peu sécurisée (en particulier au niveau de son initialisation) ;
- elle ne propose pas de séparation cryptographique entre les utilisateurs d'un même point d'accès.

Lorsque WEP est activé sur un point d'accès, en s'appuyant sur une connexion légitime en cours, un attaquant peut aujourd'hui découvrir la clé de chiffrement en moins d'une minute. Il peut ainsi accéder au réseau Wi-Fi ciblé et, potentiellement, déchiffrer toutes les communications Wi-Fi prises en charge par ce point d'accès. L'usage de WEP doit donc être prohibé.

C.3 WPA(TKIP) ou WPA2(AES-CCMP) ?

TKIP utilisé par WPA (*Wi-Fi Protected Access*) a été pensé en tant qu'évolution du WEP et introduit dans la norme IEEE 802.11i. Entre autres, il continue de s'appuyer sur l'algorithme de chiffrement à flot RC4, la méthode d'initialisation de RC4 étant entièrement revue. Cette évolution a été bénéfique, et même si TKIP souffre toujours de quelques failles de sécurité mineures, comparées aux failles du WEP, elle a apporté une réponse sérieuse aux problèmes de sécurité rencontrés avec WEP.

Cependant, depuis plusieurs années, l'algorithme de chiffrement et de contrôle d'intégrité AES-CCMP (utilisé par WPA2 basé sur l'algorithme de chiffrement par bloc AES) également introduit dans 802.11i est supporté par la quasi-totalité des matériels Wi-Fi. Il est considéré comme robuste et aucune attaque cryptographique réaliste de AES-CCMP n'existe au jour de publication de ce document. Il s'agit donc de l'algorithme à privilégier afin de protéger la confidentialité et l'intégrité des communications Wi-Fi. Il est supporté par le matériel labellisé WPA2.

C.4 L'authentification

Deux modes d'authentification principaux sont décrit dans la norme 802.11i : l'authentification par clé partagée WPA-PSK, et l'authentification déléguée WPA-Entreprise qui s'appuie sur les protocoles 802.1x et EAP (*Extensible Authentication Protocol*).

Le mode d'authentification par clé partagée WPA-PSK convient particulièrement pour sécuriser un point d'accès Wi-Fi unique, sans contrainte de confidentialité des flux entre terminaux du réseau Wi-Fi. Lorsqu'on configure un mot de passe pour WPA-PSK, il convient de choisir un mot de passe robuste en accord avec les recommandations précédemment indiquées. Dans ce mode, lorsque le SSID du point d'accès est un SSID générique qui ne semble pas unique (par exemple, le nom du constructeur du point d'accès, ou du fournisseur d'accès Internet), il convient de le changer pour un SSID personnalisé et unique. En effet, lors de la configuration WPA-PSK, le mot de passe est condensé et dérivé avec le SSID afin de produire une clé de 256 bits, qui sera ensuite stockée comme clé maîtresse pour l'authentification, le chiffrement et le contrôle d'intégrité Wi-Fi. Lorsqu'est conservé un SSID standard avec une authentification WPA-PSK, un attaquant peut disposer de tables pré-calculées lui permettant

de fortement accélérer la recherche du mot de passe. Dans tous les cas, veiller à ne pas choisir un SSID qui est en relation avec une activité sensible (nom d'entreprise ou de site industriel, type d'activité...).

Le mode d'authentification WPA-Entreprise est quant à lui à utiliser pour sécuriser un réseau de points d'accès Wi-Fi, et à privilégier en environnement professionnel. Il met en jeu EAP qui décorrèle le protocole réseau Wi-Fi et la méthode d'authentification. Différentes méthodes d'authentification basées sur le protocole EAP peuvent ainsi être utilisées, mais certaines sont à éviter car elles peuvent présenter des vulnérabilités. Les méthodes d'authentification EAP les plus robustes sont décrites en note de la recommandation R12. L'utilisation d'EAP avec une de ces trois méthodes d'authentification permet entre autres :

- d'imputer chaque connexion à un utilisateur dûment authentifié et autorisé ;
- de supprimer les droits d'accès au réseau Wi-Fi pour un utilisateur précis, en révoquant simplement son certificat ou ses droits d'accès, sans qu'il soit nécessaire de changer une clé partagée ;
- de s'assurer que le client valide le certificat serveur et ne puisse donc se connecter qu'aux réseaux Wi-Fi d'entreprise dont le certificat à été délivré par une autorité racine de confiance de l'entreprise.

Nota Bene : En environnement Active Directory, les certificats utilisateurs peuvent être automatiquement générés et distribués aux utilisateurs, de même que la configuration d'accès sur les postes clients. Le déploiement à grande échelle d'un Wi-Fi sécurisé par authentification WPA-Entreprise s'en trouve alors grandement simplifié.

C.5 WPS (*Wi-Fi Protected Setup*)

Plus récemment, la Wi-Fi Alliance a introduit le mécanisme WPS, avec l'intention de faciliter la mise en place de configuration WPA2, en particulier pour des terminaux ne disposant pas d'interfaces de saisie ergonomiques. Quatre méthodes différentes sont proposées pour permettre d'effectuer un transfert à priori sécurisé de la configuration WPA2 du point d'accès vers le terminal.

Malheureusement, la méthode principale, qui consiste à entrer dans le terminal un code PIN inscrit sur le point d'accès, souffre d'une vulnérabilité très importante. Lorsque WPS est activé sur un point d'accès, un attaquant peut connaître la configuration WPA2 en obtenant le code PIN WPS du point d'accès, ce qui revient à découvrir deux combinaisons, de 4 puis 3 chiffres par recherche en "force brute". Cette recherche peut prendre de quelques minutes à quelques heures mais ne nécessite pas de s'appuyer sur une connexion existante (contrairement aux attaques sur WEP). Par sécurité, le mode WPS doit donc être systématiquement désactivé des points d'accès Wi-Fi.