TECHN 36

Publication périodique de Smals

Août 2012

La Sécurité des Réseaux Wi-Fi

Aspects Cryptographiques

Julien Cathalo est titulaire d'un doctorat en sciences appliquées. Depuis juin 2010, il est employé comme consultant à la section Recherches de Smals. Spécialiste en cryptographie, il étudie des solutions utiles pour le secteur des soins de santé et pour la sécurité sociale. Il suit tout particulièrement la problématique de la sécurité du Cloud Computing.

Contact: 02 787 59 48

Julien.Cathalo@smals.be

Introduction

Les réseaux Wi-Fi font partie de notre quotidien. Ils permettent l'échange de données sans fil sur un réseau informatique. Qu'ils soient utilisés à des fins privées ou professionnelles, il est indispensable de les sécuriser pour protéger l'accès au réseau et la confidentialité des données transmises. Le grand public semble désormais en avoir pris conscience : en effet, selon une étude récente de la Wi-Fi Alliance réalisée aux U.S.A., 86% des utilisateurs Wi-Fi ont adopté des mesures basiques de protection[1].

Sur le plan technique, cette sécurisation comporte trois facettes : l'authentification, qui permet que seules des machines autorisées accèdent au réseau, le chiffrement, qui permet d'assurer la confidentialité des données échangées sur le réseau, et le contrôle de l'intégrité des données échangées. Pour réaliser cela, la Wi-Fi Alliance a proposés plusieurs protocoles de sécurité. Ce fut d'abord le WEP (pour « Wired Equivalent Privacy ») en 1999 dans le standard original IEEE 802.11, remplacé par WPA1 (pour « Wi-Fi Protected Access ») en 2003 puis WPA2 en 2004.

Pourquoi avoir changé deux fois de protocole ? Simplement parce que de sérieuses failles de sécurité ont été mises à jour, d'abord dans le protocole WEP puis dans WPA1.

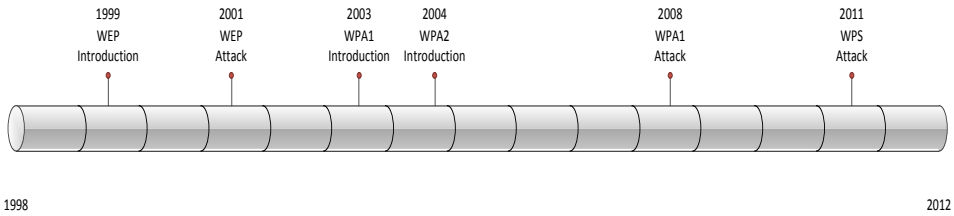

Figure 1: Historique de la sécurité du Wi-Fi

Les chapitres suivants reviennent sur cet historique en expliquant le fonctionnement cryptographique des différents protocoles et des attaques. La dernière section parle du Wi-Fi Protected Setup (WPS), qui n'est pas un protocole de cryptographie à proprement parler mais un standard de mise en œuvre simplifiée de réseaux Wi-Fi.

[1] http://www.wi-fi.org/media/press-releases/wi-fi%C2%AE-security-barometer-reveals-large-gap-between-what-users-know-and-what

Quelques définitions

- Un *système de chiffrement symétrique* est un système avec lequel la même clé est utilisée pour chiffrer et pour déchiffrer des messages. On rencontre principalement deux types de systèmes de chiffrement symétriques : les « block ciphers » et les « stream ciphers ».
- Un *block cipher* est un système de chiffrement symétrique qui fonctionne en chiffrant des blocs de message clair d'une taille fixée (par exemple, 128 bits). Le block cipher le plus connu est le standard AES (Advanced Encryption Standard) ainsi que son prédécesseur (désormais obsolète et pas sûr) DES.
- Un *stream cipher* ou chiffrement à flots est un type système de chiffrement symétrique basé sur la génération d'une chaîne de bits pseudo-aléatoires. Le chiffrement consiste à générer, à partir de la clé, une chaîne de bits pseudo-aléatoires, puis à calculer le XOR entre cette chaîne et le message clair. Le résultat est le message chiffré. Pour déchiffrer, on génère cette même chaîne de bits à partir de la clé, puis on calcule le XOR entre cette chaîne et le message chiffré. Le résultat est le message clair. L'algorithme RC4 est l'un des stream ciphers les plus connus et utilisés.
- Le *counter mode* est une méthode de stream cipher qui utilise comme composant un block cipher. Il fonctionne en utilisant le block cipher pour chiffrer les valeurs successives d'un compteur afin de générer une chaîne de bits pseudo-aléatoires. Ensuite, cette chaîne est utilisée comme dans un stream cipher pour chiffrer le message clair.
- Un *code de redondance cyclique* (CRC) est un système utilisé pour détecter des changements accidentels dans des données.
- Un *Message Authentication Code* (MAC) est un algorithme d'authentification à clé secrète.
- Dans ce texte nous utiliserons les termes « *client* » et « *point d'accès* » pour désigner respectivement l'appareil qui se connecte au réseau et l'appareil qui permet l'accès au réseau.

WEP : Wired Equivalent Privacy

Le protocole « Wired Equivalent Privacy » ou WEP faisait partie du premier standard Wi-Fi IEEE 802.11. Son nom promettait une sécurité équivalente à une connection filaire, nous verrons que ce n'est pas du tout le cas.

Le WEP utilise les algorithmes suivants :

- Le stream cipher RC4 pour chiffrer les données et authentifier le client auprès d'un point d'accès.
- Le code de redondance CRC32 pour vérifier l'intégrité des donnéees.

Le chiffrement WEP fonctionne de la manière suivante.

Le client et le point d'accès sont munis d'une même clé, la Pre-Shared Key ou PSK. Plusieurs tailles de clés pour PSK sont possibles : 40 bits, 104 bits et 232 bits.

L'algorithme RC4 va, à partir de cette clé et d'un IV (« initialization vector ») aléatoire de 24 bits, générer des bits aléatoires. Un nouvel IV est tiré aléatoirement pour chaque paquet, ainsi la chaîne de bits aléatoires sera différente à chaque fois. Le message chiffré est obtenu en calculant le XOR entre cette chaîne aléatoire et le message clair.

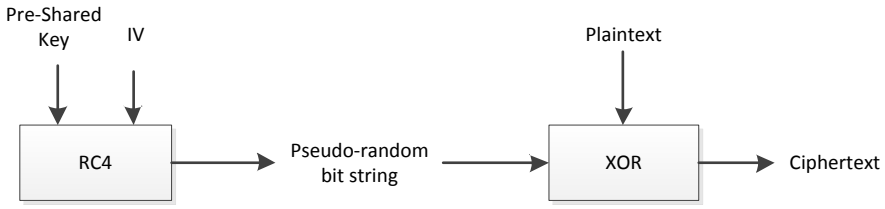

Figure 2: Chiffrement WEP

Le message chiffré est ensuite envoyé au destinataire ainsi que l'IV.

Le déchiffrement consiste simplement à générer la même chaîne aléatoire à partir de la PSK et de l'IV, puis de calculer le XOR entre le message chiffré et la chaîne aléatoire pour reconstituer le message clair.

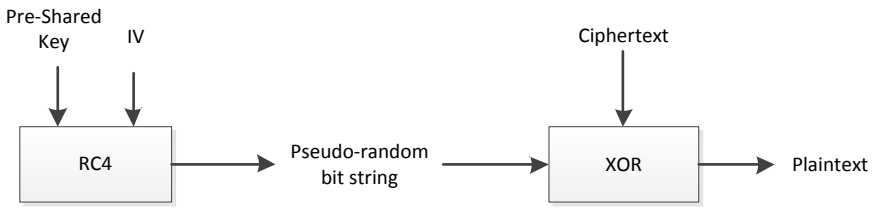

Figure 3: Déchiffrement WEP

Failles de sécurité du WEP

On peut déjà noter une première faiblesse de ce système : la taille des IV (24 bits) n'est pas suffisante. Au bout de 5000 chiffrements effectués, il y a en moyenne 50% de chances pour que le même IV ait été utilisé deux fois et cela implique que ce sera la même chaîne pseudo-aléatoire qui a été générée… On a donc deux paires de messages (*cm1*,*em1*) et (*cm2*,*em2*) où *cm* signifie message clair (« clear message ») et *em* signifie message chiffré (« encrypted message »), tels que :

- *em1* = *cm1* XOR RC4(PSK,IV)
- *em2* = *cm2* XOR RC4(PSK,IV)

En calculant le XOR entre les deux lignes, et grâce au fait que RC4(PSK,IV) XOR RC4(PSK,IV) = 0000000000, on obtient que *em1* XOR *em2* = *cm1* XOR *cm2*. On voit donc qu'un attaquant, qui ne connaît pas la clé PSK, qui repère deux messages chiffrés avec la même IV peut obtenir le XOR entre les deux messages clairs correspondants. L'attaquant a donc récupéré beaucoup d'information sur les deux messages clairs (mais pas ces messages eux-mêmes, ni la clé).

L'insécurité du WEP va plus loin et la première véritable attaque a été réalisée en 2001 et décrite dans un article publié par Fluhrer, Mantin et Shamir[2].

L'attaque exploite des faiblesses dans l'algorithme RC4. En observant plusieurs paquets chiffrés, un attaquant peut découvrir la clé PSK. Le système est donc considéré comme complètement cassé. L'attaque peut être mise en œuvre à l'aide du logiciel aircrack-ng à condition de disposer d'une carte Wi-Fi compatible (toutes les cartes ne le sont pas, cela dépend en fait du chipset de la carte).

Le WEP est donc considéré comme cryptographiquement cassé : l'utiliser pour protéger sa connexion Wi-Fi est donc déconseillé car il n'offre pas une protection suffisante.

WPA1 : Wi-Fi Protected Access

Le standard WPA ou WPA1 (« Wi-Fi Protected Access »), aussi appelé TKIP pour (« Temporal Key Integrity Protocol »), a été proposé par la Wi-Fi Alliance en 2003. La raison de sa création était que le WEP était désormais cassé et il fallait donc un nouveau protocole de sécurité. Il fallait en plus que ce nouveau protocole soit compatible avec les cartes Wi-Fi existantes.

Il a donc été proposé comme une solution de transition, en attendant que le standard IEEE 802.11i soit terminé. Ces contraintes expliquent pourquoi WPA1 a été aussi vite attaqué : les conditions n'étaient pas réunies pour que la Wi-Fi Alliance propose un protocole avec une sécurité validée par des tiers.

WPA, tout comme son successeur WPA2, existe en deux modes d'opération :

- WPA-Enterprise, mode dans lequel les clients doivent s'authentifier auprès d'un serveur pour recevoir leurs codes d'accès au réseau
- WPA-Personal, mode dans lequel les clients utilisent tous une « passphrase » commune

WPA-Enterprise nécessite la mise en œuvre d'un serveur d'authentification 802.1X et a donc été conçu plutôt pour les grandes entreprises ; WPA-Personal est une solution plus légère, plus facile à mettre en place, prévue pour les particuliers et les petites entreprises.

Le protocole WPA1 utilise un « MIC » (Message Integrity Code) appelé Michael et une fonction de hachage appelée simplement « hash ». Pour chiffrer et authentifier un message, on utilise une méthode assez complexe.

1. A partir d'une clé appelée « pre-shared key », on dérive deux clés : une clé de chiffrement K et une clé d'intégrité K*.
2. Avec la clé K et un vecteur d'initialisation IV, on calcule une « packet key ». A partir de cette clé, on dérive un flux de bits avec l'algorithme RC4.
3. Avec la clé K* et l'algorithme Michael, on calcule un code à partir du message clair. Ensuite on découpe le résultat (formé du message clair et du code) en fragments. Pour chaque fragment, on calcule son CRC32.

Le message chiffré est constitué du XOR entre le flux de bits et l'ensemble des fragments concaténés avec leur CRC32.

[2] Scott R. Fluhrer, Itsik Mantin, Adi Shamir: Weaknesses in the Key Scheduling Algorithm of RC4. Selected Areas in Cryptography 2001: 1-24

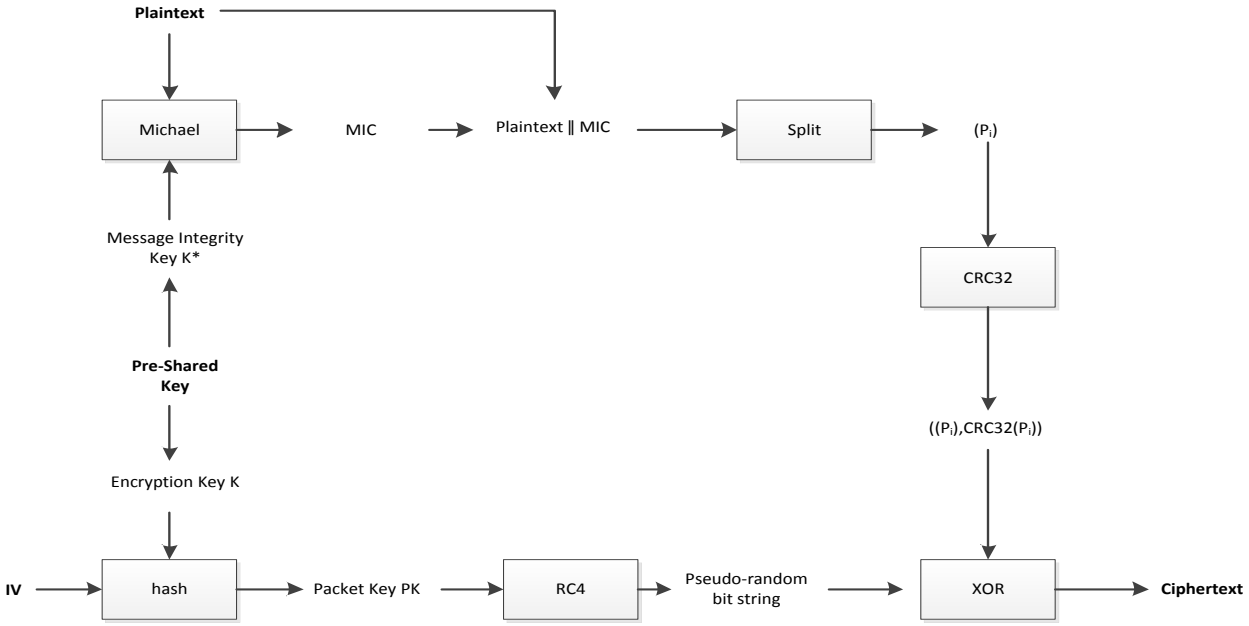

Figure 4: Chiffrement et authentification WPA1

Pour assurer la compatibilité avec le hardware Wi-Fi existant, on a construit un système basé sur les mêmes composants (RC4, CRC32) que le WEP mais en les utilisant autrement afin d'éviter les problèmes de sécurité de celui-ci.

Failles de sécurité du WPA1

Des faiblesses de WPA1 ont été remarquées dès son introduction. Mais la première attaque efficace publiée contre WPA1 date de 2008 et est due aux chercheurs Beck et Tews[3]. Leur attaque permet de retrouver le message clair à partir d'un message chiffré, et peut aussi falsifier le message. C'est donc à la fois la confidentialité et l'authenticité qui sont cassées. Leur attaque se limite aux implémentations de WPA1 qui supportent des fonctionnalités QoS (Quality of Service) du standard IEE802.11e. Un an plus tard, Ohigashi et Morii développent une nouvelle attaque, plus efficace et qui n'a plus la contrainte du QoS.

[3] Martin Beck, Erik Tews: Practical attacks against WEP and WPA. IACR Cryptology ePrint Archive 2008: 472 (2008)

WPA2 : Wi-Fi Protected Access 2

WPA2 utilise le protocole de chiffrement CCMP. Le principe de CCMP consiste à utiliser l'algorithme de chiffrement AES en mode CCM (Counter with CBC-MAC) dont le fonctionnement est expliqué dans la suite. Le but est d'assurer aussi bien la confidentialité que l'authenticité.

Pour chiffrer et authentifier un message M avec AES en mode CCM avec une clé K, on procède de la manière suivante :

- On calcule un tag T avec un MAC à partir du message M et de la clé K avec AES en mode CBC-MAC
- On chiffre le message M ainsi que le tag T avec AES en mode compteur avec la clé K.

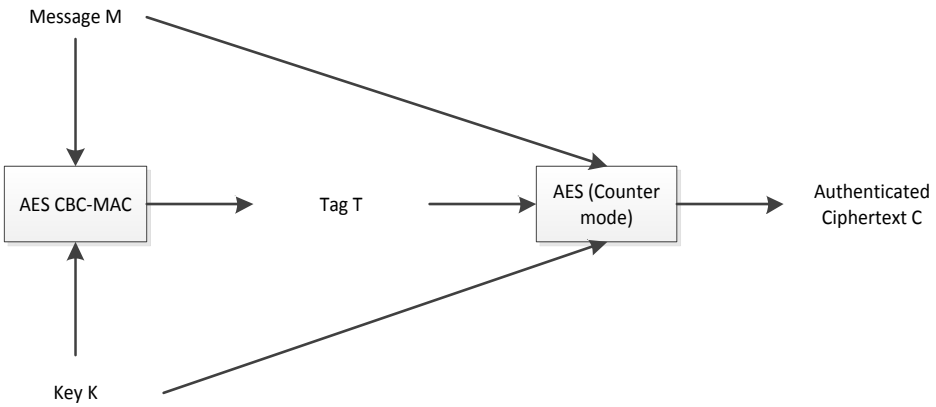

Figure 5: Chiffrement et authentification CCMP

Depuis 2006, tout matériel qui veut porter la marque déposée Wi-Fi doit obligatoirement supporter WPA2.

Sécurité du WPA2

A la différence de ses prédécesseurs, le standard WPA2 repose sur des méthodes éprouvées en cryptographie. La sécurité de la méthode CCMP utilisée a été prouvée formellement, ce qui signifie que cette méthode est sûre sous certaines hypothèses ; pour un expert en cryptographie, cela implique que la méthode est robuste et bien construite. L'algorithme de chiffrement AES est un standard du NIST (National Institute of Standards and Technology) depuis 2001 et la NSA approuve son utilisation pour des informations classées top secret. Sa sécurité n'est pas prouvée mathématiquement, mais a été étudiée à de nombreuses reprises par des chercheurs sans qu'aucun ne trouve une attaque exploitable en pratique.

Ces éléments inspirent donc confiance dans la sécurité de WPA2, même s'ils ne permettent pas une garantie à 100% que le protocole soit inviolable. En particulier, les utilisateurs doivent prendre soin de choisir un mot de passe suffisamment long et complexe pour

résister à une attaque de type « brute force » qui consiste simplement à essayer de très nombreux mots de passe jusqu'à trouver le bon.

A propos du "Wi-Fi Protected Setup" (WPS).

Le Wi-FI Protected Setup (WPS) est un standard de la Wi-Fi Alliance, créé en 2007, qui a pour but de mettre en œuvre de manière simplifiée et sécurisée une connexion Wi-Fi. Ce n'est pas un système de chiffrement et d'authentification ; il ne faut donc pas le mettre sur le même plan que le WEP, WPA1 ou WPA2. Il est en fait destiné à être complémentaire.

Si la simplicité est bien garantie, la sécurité ne l'est pas, comme nous verrons plus loin. Avec cette méthode, on évite à l'utilisateur de déterminer une méthode de sécurisation et de choisir un mot de passe complexe. Ce mode est activité par défaut dans la plupart des routeurs Wi-Fi récents. Plusieurs options existent pour ajouter un client au réseau :

1. *Client PIN Method*. Un PIN est inscrit sur le client Wi-Fi (via un écran ou un autocollant) et doit être tapé par l'utilisateur sur le point d'accès.
2. *Router PIN Method*. Alternativement, le PIN est inscrit sur le point d'accès et doit être entré sur le client.
3. *Push-Button-Method*. L'utilisateur doit appuyer sur un bouton (éventuellement virtuel) sur le client et sur le point d'accès.

Failles de sécurité du Wi-Fi Protected Setup

En décembre 2011, des chercheurs, Stefan Viehböck et Craig Heffner, ont indépendamment découvert une vulnérabilité dans WPS[4]. Cette vulnérabilité concerne la méthode "Router PIN Method" avec laquelle le PIN inscrit sur le point d'accès est entré sur le client que l'on veut ajouter au réseau. L'attaque part du constat qu'un accès physique au point d'accès n'est pas nécessaire et que le seul élément nécessaire pour l'authentification est la connaissance du PIN. A priori, comme le PIN fait huit chiffres, il y a 10^8 = 100 000 000 PINs à tester pour une recherche exhaustive (ou attaque "brute force"). Si l'on s'arrête à cette observation, on peut penser qu'une recherche exhaustive est infaisable en pratique, ce nombre étant trop grand.

Cependant, le point d'accès vérifie d'abord les 4 premiers chiffres. On peut donc commencer par tester toutes les combinaisons possibles de ces 4 premiers chiffres puis tester le reste, soit 10^4+10^4 = 20000 combinaisons à tester en tout. De plus, le dernier chiffre du PIN est une checksum des 7 chiffres précédents ; le nombre de combinaisons à tester devient donc 10^4+10^3 = 11000.

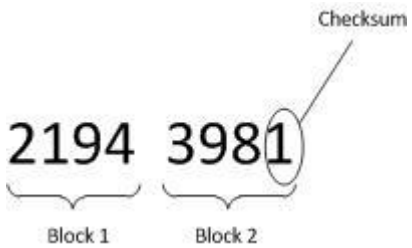

Figure 6: Format d'un PIN WPS

[4] http:// www.h-online.com/open/news/item/Wi-Fi-Protected-Setup-made-easier-to-brute-force-Update-1401822.html

L'attaque consiste donc à lancer un WPS en choisissant la Router Pin Method avec un point d'accès auquel on veut se connecter puis tester ces combinaisons jusqu'à réussir à se connecter. Certains points d'accès se verrouillent après plusieurs essais erronés de PIN, mais cela n'empêche pas l'attaque, cela la ralentit seulement.

Les outils wpscrack et Reaver implémentent cette attaque et retrouvent le PIN en quelques heures.

Il n'y a pas beaucoup de possibilités pour protéger son propre réseau Wi-Fi contre cette attaque : il faut désactiver le WPS sur son point d'accès lorsque cela est possible, et mettre à jour le firmware du point d'accès Wi-Fi lorsque des mises à jour seront disponibles. C'est d'ailleurs ce que recommande le CERTA (Centre d'expertise gouvernemental de réponse et de traitement des attaques informatiques), organisme gouvernemental français[5].

Suite à la publication de cette attaque, plusieurs constructeurs ont publié des guides pour expliquer à leurs utilisateurs comment désactiver le WPS.

Conclusion

L'histoire de la sécurité des réseaux Wi-Fi est mouvementée et est marquée par les attaques successives contre les différents standards de la Wi-Fi Alliance. A l'heure actuelle, la seule option recommandable est d'utiliser WPA2. En effet, seul ce système offre un niveau de protection suffisant pour un réseau Wi-Fi. Les autres protocoles (WEP et WPA1) ne sont pas sûrs.

Par ailleurs, le Wi-Fi Protected Setup est lui aussi faillible et doit être désactivé sur les points d'accès. L'utilisation de WPA2 ne garantit pas à elle seule un bon niveau de sécurité, et l'utilisateur doit être vigilant ; en particulier il doit choisir soigneusement son mot de passe[6].

[5] http://www.certa.ssi.gouv.fr/site/CERTA-2012-ACT-001/CERTA-2012-ACT-001.html

[6] Voir à ce sujet l'article de Kristof Verslype sur le blog de la section Recherches : http://blogresearch.smalsrech.be/?p=4078