**Wireless Security**

**Info 402**

**Sommaire**

* Introduction ………………………………………….2
* WEP et son vulnerabilité ..………………..…..3
* WPA et son vulnerabilité ..………………..….10
* WPA2 et son vulnerabilité ……………………13
* Conclusion ..……………………………..……….…15

**Introduction**

Les technologies sans fil (wireless) sont plus vulnerables aux attaques en raison de la nature des transmissions du reseau qui sont pas physiquement contraintes dans les limites d’un batiment.

Au plus les pirates informatiques realisent que les reseaux sans fil peuvent souvent etre insecurises et exploites comme une passerelle vers les reseaux cables relativement surs au-dela d’eux.

Chaque algorithme de chiffrement présente des avantages et des inconvénients et comme un laboratoire doit pénétrer ces algorithmes comprennet bien.

**WEP et son vulnerabilité :**

**Le protocole WEP (Wired Equivalent Privacy) :** est un protocole du protéger et une partie de la norme IEEEE 802.11 objectif initial standard était d’assurer la confidentialité des données dans les réseaux sans fil à la vie privée équivalente de niveau dans les réseaux filaires.

Dans les réseaux sans fil peuvent accéder au réseau sans contact physique avec elle, donc en utilisant le mécanisme de chiffrement dans la couche de liaison de données afin de réduire l’accès non autorisé au réseau sans fil était qui crypte les données en utilisant symétrique algorithme de chiffrement RC4.

**Comment ça marche WEP :**

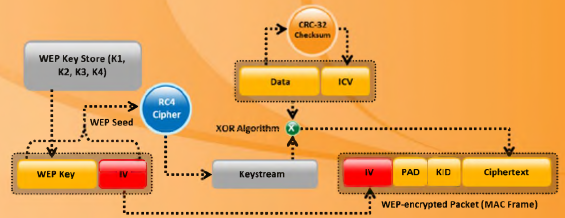
Le chiffrement se décompose en plusieurs phases :

• La création de la graine

• La création du keystream

• Le calcul ICV

• La constitution du message final et son encapsulation dans une trame



a) La création de la graine :

Le vecteur d’initialisation (IV – Initialization Vector) est une séquence de bits qui change régulièrement (à chaque trame envoyée si l’implémentation est bonne). Combiné à la clé statique, il introduit une notion aléatoire au chiffrement. Ainsi, deux messages identiques ne donneront pas le même contenu chiffré, puisque l’IV est dynamique.

Comme la clé, le IV doit être connu à la fois de l’émetteur et du récepteur. Le IV est donc transporté en clair dans les trames.

Deux longueurs de clé WEP peuvent être choisies sur les équipements Wi-Fi :

- 40 bits, soit 5 octets

- 104 bits, soit 13 octets

La clé K est concaténée à l’IV en position de poids faible généralement. On obtient alors une clé de 64 bits (8 octets) ou 128 bits (16 octets) que l’on appelle graine, germe, plaintext ou encore seed : IV || K.

b) La création du keystream :

Une table de 256 octets (généralement) est formée. Elle est initialisée en reportant la graine autant de fois que nécessaire. A partir de la même clé, on obtient donc la même table à l’issue de la phase d’initialisation. On appellera ce tableau S (comme seed) par la suite.

Par permutation et autres manipulations, les cellules sont ensuite mélangées. On initialise une table d’états T (qui sera le masque appliqué sur le texte clair) avec T[i]=i pour 0 ≤ i ≤ longueur(T)-1. Ce procédé porte le nom de Key Scheduling Algorithm (KSA) ou encore module de mise à la clé. A son issue, tous les éléments de la table auront été permutés.

Une fois la table T mélangée, on peut fabriquer des PRNs ou « Pseudo Random Numbers » à l’aide d’un générateur PRGA ou « Pseudo Random Generator Algorithm » qui fonctionne sur le même principe que le module KSA mais sans faire appel à la clé K.

La clé de chiffrement utilisée est une séquence de bits extraite de cette table à partir du PRGA. On appelle cette séquence pseudo aléatoire, suites-clé, masque ou encore **keystream**.

c) Le calcul ICV**:**

Le WEP prévoit un mécanisme nommé Integrity Check Value (ICV), destiné à contrôler l’intégrité des séquences WEP dites trames (frames en anglais). Pour cela, un code équivalent au CRC32 (i.e. sur 32 bits) est calculé. Il résulte du message en clair M et non du contenu chiffré. Le CRC32 correspond en fait au reste dans la division en binaire du message par un diviseur fixé à l’avance.

Le résultat du calcul d’intégrité: ICV(M) est ensuite concaténé au payload M : M||ICV(M), puis chiffré avec la clé. La clé WEP est donc indispensable pour l’interpréter.

La modification de la trame chiffrée semble inconcevable sans la clé puisque le résultat de l’ICV changerait.

d) La constitution du message final et son encapsulation dans une trame :

On détient dans la trame deux informations en clair : le KeyID et l’IV. On récupère la graine en concaténant la clé WEP indiquée par le Key ID avec l’IV qui se trouve en clair dans la trame. On peut retrouver alors le keystream utilisé pour le chiffrement. On opère un XOR entre le cryptogramme et le keystream et on récupère ainsi le payload et le CRC. Prenons un message chiffré C, un plaintext P et une graine G, on a :

C + RC4(G) = (P + RC4(G)) + RC4(G) = P

On applique alors l’algorithme de contrôle d’intégrité et on peut dès lors comparer les résultats. Si les résultats coïncident, la trame est acceptée, sinon elle est rejetée et supprimée. La probabilité qu’un contrôle d’intégrité se révèle positif alors que la clé utilisée serait invalide est considérée comme nulle.

Wep vulnerabilities :

1-Plaintext attack:

Wep utilise RC4 cryptage qui est stream cipher qui fait XOR entre plaintext et le keystream pour obtenu ciphertext alors si un pirate peut comparer le text chiffre (les donnles données WEP) à l’équivalent en texte brut. Tous ce qu’ils auraient à faire est de brancher les deux valeurs dans l’algorithme RC4 utilise par WEP pour decouvrir le flux de clès utilise pour chiffrer les données.

2- Vulnerabilité de l’algorithme RC4 :

Une autre vulérabilité de WEP est qu’elle utilise RC4, un chiffrement de flux développé par RSA pour chiffrer les données.

En 1994 un utilisateur anonyme à poste l’algorithme RC4, republie dans un certain nombre de groupe de discussion usenet avec le titre « RC4 algorithme revele ».

En 2001 un article intitule « faiblesses dans l’algorithme RC4 » a été publie qui a demontre qu’un certain nombre de clès utilises dans RC4 étaient faibles et vulnerables au compromis.

Après, un certain nombre d’outils open-source apparus ce fait our casser RC4. Deux de ces outils pour craquer WEP sont Airsnort et WepCrack.

3- *Stream Cipher Vulnerability:*

Un problème central avec le WEP est le potential de reutilization de IV. Une vulnerabilite bien connue des chiffrement des flux est la reutilization d’une clè pour crypter deux messages.

Lorsque cela se produit, les deux messages chiffres peuvent entre XOR entre eux pour annuler le « key stream » et le resultat sera XOR entre les deux plaintext original.

Alors si l’attaquant connait le contenu d’un de ces messages en plaintext il peut facilement obtenir le plaintext de l’autre message.

En plus on à 16,777,216 combinaisons possibles pour le IV, c’est un nombre relativement faible surtout sur un reseau sans fil occupe.

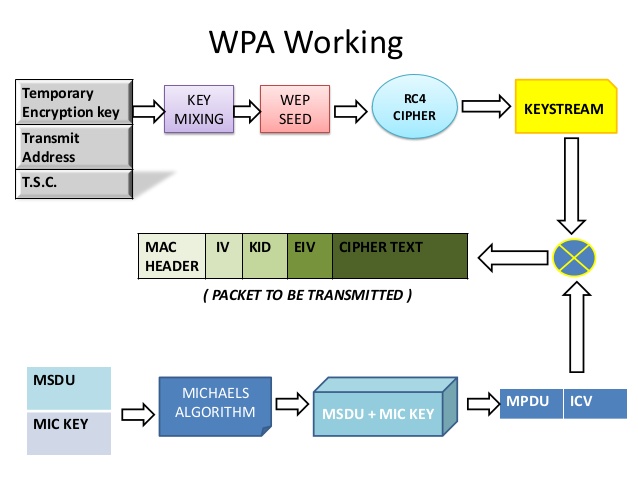
Une fois qu’un attaquant a rassemble suffisament de cardes qui utilise des IV en double, il peut conclure le clè secrete partagée.

**WPA et son vulnerabilité :**

Wi-Fi Protected Access était réponse directe et le remplacement de l’Alliance Wi-Fi à la vulnérabilité de plus en plus apparentes de la norme WEP. Il a été officiellement adopté en 2003, un an avant WEP a été officiellement pris sa retraite. La configuration la plus courante WPA est WPA-PSK (Pre-Shared Key). Les clés utilisées par WPA sont 256 bits, une augmentation significative par rapport aux clés de 64 bits et 128 bits utilisés dans le système WEP.

Certains des changements importants mis en œuvre avec WPA inclus des contrôles d’intégrité de message (pour déterminer si un attaquant avait capturé ou modifié des paquets transmis entre le point d’accès et le client) et le Temporal Key Integrity Protocol (TKIP).

TKIP utilise un système de clé par paquet qui est radicalement plus sûr que la clé fixe utilisée dans le système WEP. TKIP a ensuite été remplacé par Advanced Encryption Standard (AES).



Malgré ce que WPA amélioration significative était sur WEP, le fantôme du WEP hanté WPA. TKIP, un composant de base de WPA, a été conçu pour être facilement déployé par l’intermédiaire du firmware des mises à niveau sur des appareils WEP activé existants. En tant que tel, il doit recycler certains éléments utilisés dans le système WEP qui, en fin de compte, ont également été exploitées.

WPA, WEP comme son prédécesseur, a été démontré par les deux manifestations publiques preuve de concept et appliquées comme vulnérables à l’intrusion. Fait intéressant, le processus par lequel WPA est habituellement violé est pas une attaque directe sur l’algorithme de WPA (bien que ces attaques ont été démontrées avec succès), mais par des attaques sur un système supplémentaire qui a été déployé avec l’installation de WPA, Wi-Fi Protected (WPS), conçu pour le rendre facile de relier des dispositifs aux points d’accès modernes.

Il ya deux attaques connues contre TKIP :

* Attaque de Beck-Tews
* Ohigashi-Morii attaque (qui est une amélioration sur l'attaque Beck-Tews)

Ces deux attaques ne pouvaient décrypter que de petites portions de données, compromettant la confidentialité. Ce qu'ils ne peuvent pas vous donner, c'est l'accès au réseau. Pour vous donner une idée de combien de données peuvent être récupérées, une seule trame ARP prendrait environ 14-17 minutes pour obtenir le texte brut. Obtenir des informations utiles avec ce type d'attaque est très improbable (mais pas impossible) compte tenu du taux de récupération.La seule attaque connue, en plus des défauts dans le micrologiciel de certains routeurs, est brute forçant la clé WPA. En général, la clé est générée comme suit

Key = PBKDF2(HMAC−SHA1,passphrase, ssid, 4096, 256).

WPA prend également en charge AES (qui peut être utilisé à la place de RC4). Alors que AES est plus sûr que RC4 le plus gros problème de WPA est toujours présent, à savoir le contrôle d'intégrité est toujours fait en utilisant TKIP-MIC.

**WPA2 et son vulnerabilité :**

WPA a, en 2006, été officiellement remplacé par WPA2. L’un des changements les plus importants entre WPA et WPA2 était l’utilisation obligatoire des algorithmes AES et l’introduction de CCMP (Mode Cipher Compteur avec Block Chaining message Authentication Protocol Code) en remplacement de TKIP (encore préservé dans WPA2 comme un système de secours et interopérabilité avec WPA).

À l’heure actuelle, la vulnérabilité de sécurité primaire au système de WPA2 réelle est un obscur (et nécessite l’attaquant d’avoir déjà accès au réseau Wi-Fi sécurisé afin d’avoir accès à certaines touches, puis perpétuer une attaque contre d’autres périphériques sur le réseau ). En tant que tel, les implications de sécurité des vulnérabilités WPA2 connues sont limitées presque entièrement à des réseaux de niveau d’entreprise et méritent peu à aucune considération pratique en matière de sécurité du réseau domestique.

Malheureusement, la même vulnérabilité qui est le plus grand trou dans l’armure WPA, le vecteur d’attaque à travers la configuration Wi-Fi Protected (WPS), reste dans les points d’accès modernes WPA2-capable. Bien que la rupture dans un réseau WPA / WPA2 sécurisé en utilisant cette vulnérabilité nécessite partout de 2-14 heures d’effort soutenu avec un ordinateur moderne, il est encore une légitime préoccupation et WPS sécurité doivent être désactivés (et, si possible, le firmware de l’accès point devrait être flashé à une distribution qui n’a même supporte pas WPS de sorte que le vecteur d’attaque est entièrement enlevée).

Conclusion

* Wep est plus vulnerable que les autres.
* Wpa plus meilleur de wep car le cle dynamique.
* Wpa2 est le meilleur en utilisant AES et pas rc4.