Les évolutions de sécurité des réseaux WLAN et leurs résolutions partielles avec la norme 802.11i, WPA2

EPITA - NET2

Les réseaux locaux sans fils sont apparus et se sont rapidement développés. Il a donc fallu prévoir et répondre aux problèmes de sécurité qu'ils engendraient. Coordonné par le groupe de travail 11 de l'IEEE, la norme 802.11 a été mise en place pour assurer une sécurité équivalente aux réseaux filiaires. Cette norme existe donc sous le nom de WEP pour 'Wired Equivalent Privacy'. Cependant des failles de sécurité causées par les particularitées physiques de ces réseaux sans fils (WLAN) ont été démontré et une mise à jour de la norme 802.11 à donc été mise en place. Cette nouvelle norme 802.11i à d'abord donné naissance aux technologies WPA (Wi-Fi Protected Access) comme solution temporaire puis à WPA2 comme solution finale. Ce document va mettre en lumière les aspects techniques des différentes versions des protocoles de sécurité des réseaux WLANs.

Mots clés

WLAN, 802.11i, 802.11x, CCMP (Counter Mode CBC-MAC Protocol), AES (Advanced Encryption Standard), RC4 (River Cipher 4)

1 Introduction

Le groupe de travail 11 de l'IEEE met en place la norme 803.11 et le protocole WEP pour assurer une sécurité des données qui transitent sur les réseaux WLANs. La norme est ratifié en 1999 mais dès le début des années 2000 de conséquents problèmes de sécurité sont soulevés. S'en suit alors une solution temporaire rétrocompatible avec le protocole WEP, le protocole WPA. Celui ci utilise les même mécanismes de sécurités que WEP mais en ajoute d'autre pour couvrir les failles majeures de WEP. Enfin un protocole final sera ratifié en 2004, WPA2. Alors que les deux premiers protocoles chiffraient les données avec RC4 (Rivest Cipher 4), WPA2 utilise AES réputé plus performant. Cependant la mise en place de WPA2 a necessité une amélioration matérielle. Nous allons voir dans ce document les différents stades des protocoles de sécurité des réseaux sans fils.

2 La norme 803.11 et WEP

Les problematiques majeures initiales pour les réseaux sans fil étaient d'empecher les gens de pouvoir accéder aux données qui y transitaient, d'empecher les connexions non autorisées et d'empécher la falsification des données. De la est né le mécanisme de Wired Equivalent Privacy ou WEP.

2.1 Fonctionnement

Le protocole WEP se base sur la connaissance commune d'une clée WEP de 40 bits ainsi qu'un vecteur d'initialisation (IV) de 24 bits qui est un bloc de bits généré pseudo aléatoirement. La clée WEP et le vecteur sont chiffer avec l'agorithme CR4 pour produire un 'keystream'. Avant de chiffrer la donnée à faire transiter, on utilise l'algorithme CRC pour générer des bits d'intégrité. Ces bits d'intégrités sont combiné avec la data à chiffrer et permetteront une fois le message déchiffré de vérifier si celui ci est corrompu. Ce nouveau bloc est donc chiffré avec le keystream au moyen d'un XOR. Avant d'envoyer le paquet, on rajoute le vecteur d'initialisation au début de la data chiffré. (Voir Fig. 1).

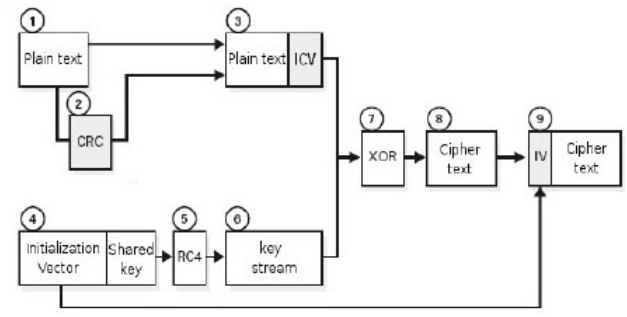

Fig. 1. Fonctionnement de WEP

2.2 Problèmes majeurs

Rapidement des failles conséquentes ont été pointé du doigt, il était possible de contourner certains aspect

sécuritaire avec des programmes open source et en quelque minutes. Le protocole WEP assure une identification de l'appareil par le point d'accès (un routeur par exemple), mais il n'y a pas d'identification du routeur par l'appareil. Un attaquant peut donc se faire passer pour le routeur et faire point de relai entre les deux machines. Un autre point est la réutilisation systèmatique de la clé WEP et du faible taux d'aléatoire du vecteur d'initialisation. Etant donné que la clée WEP ne peut prendre que 16 777 215 valeurs ($2^{24} - 1$), un attaquant qui ecoute le traffic pendant un certain temps verra des vecteurs d'initialisation se répété, le vecteur étant non chiffré, et pourra a terme déterminer la clée WEP. De plus l'algorithme d'intégrité est très faible, un attaquant qui possède la clée WEP peut donc modifier des données de façon à tromper la vérification d'intégrité.

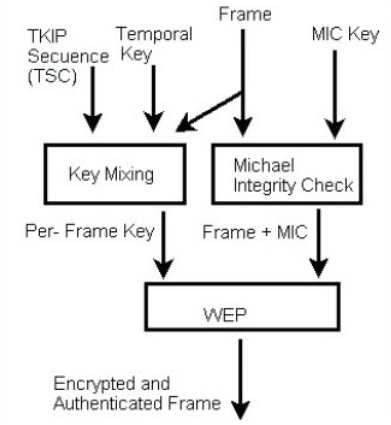

Fig. 2. Fonctionnement de WPA

3 WPA, une solution temporaire

Suite à ces nombreuses failles de sécurité, une nouvelle norme a été mise en place, la norme 803.11i. Un protocole de sécurité a aussi vu le jour comme solution de remplacement temporaire à WEP, c'est le 'Wi-Fi Protected Access' (WPA). WPA est en fait une surcouche a WEP pour palier aux problèmes majeurs.

3.1 Fonctionnement

Le protocole WPA propose un nouvel algorithme d'intégrité, Michael. Cet algorithme utilise une clée de 64 bits et est changée toute les minutes ou après une vérification d'intégrité qui a échoué. L'algorithme de chiffrement est toujours CR4. Cependant une nouvelle fonctionnalitée apparait, TKIP (Temporal Key Integrity Protocol). Le TKIP utilise une séquence de 48 bits qui change avec la même régularité que la clée d'intégrité, ensuite cette séquence est mixée avec une clée de 128 bits temporaire connue par le point d'accès (router) et le client (ordinateur). L'addresse MAC du client est aussi mixé pour obtenir une clée finale. Cette clée finale est utilisée comme clée WEP. (Voir Fig. 2). WPA propose aussi une alternative aux PSK (Pre Shared Key) qui nécessite que le client et le point d'accès partage un secret commun (un mot de passe). Il est aussi possible de configurer le point d'accès en AEP (Extensible Authentication Protocol) qui ne fonctionne plus avec un mot de passe mais une authentification du client avec un nom d'utilisateur et un mot de passe. La requête de connexion reçu par le point d'accès peut être redirigé vers un serveur d'authentification mais le routeur peut etre son propre serveur. Le WPA-AEP se base sur le protocole 802.11X. Le WPA-AEP est aussi appelé WPA-Entreprise et le WPA-PSK est aussi appelé WPA-Personal.

3.2 Limitation de WPA

WPA possède encore de potentielles failles de sécurités mais elles sont estimées très couteuses. Les fonctionnalitées de WPA sont aussi assez lourdes et impliquent une baisse de performance. La IEEE a donc continué son travail pour implémenter une version finale de WPA.

4 WPA2

WPA2 nécessite une amélioration du materiel pour amener une amélioration de l'algorithme de chiffrement. WPA2 implémente toutes les fonctionnalitées du protocole 802.11i.

4.1 Fonctionnement

WPA2 comprend toutes les fonctionnalitées de WPA, et donc le mode personnal et entreprise (IEEE 803.11X). L'algorithme de chiffrement RC4 utilisé dans WEP et WPA est remplacé par l'algorithme AES, réputé bien plus performant. De plus l'algorithme d'intégrité est lui aussi changé passant de Michael à CCM (Counter Mode CBC-MAC Protocol)

Security Method → Property ↓	**WEP**	**WPA**	**802.11i (WPA2)**
Cipher	RC4	RC4	AES
Key Size	40/104 bits	128 bits (encryption) 64 bits (authentication)	128 bits
Key Life	24-bit IV Concatenate IV to base key	48/128-bit IV TKIP mixing function	48/128-bit IV TKIP mixing function
Packet Key	Concatenated	Mixing function	Not needed
Data Integrity	CRC-32	MIC (Michael)	CCM
Replay Detection	None	Enforce IV sequencing	Enforce IV sequencing
Header Integrity	None	MIC (Michael)	CCM
Key Management	None	EAP-based (802.1X)	EAP-based (802.1X)

Fig. 3. Récapitulatif des protocoles

5 Conclusion

La sécurité des WLANs est passée par différentes étapes et différents protocole avant d'en arriver à une version relativement sécurisé. Des vulnérabilités restent potentiellement encore présentes et des améliorations ont vu le jour après la norme 802.11i comme par exemple la norme 802.11w.

6 References

1. **“Benefits and Vulnerabilities of Wi-Fi Protected Access 2 (WPA2)”,**
   Paul Arana, Fall 2006,
   https://dl.irstu.com/wp-content/uploads/Download/Education/Book/Network/Network

2. **“How does WPA and WPA2 work?”**,
   FLAMINGO Project, 16 September 2014,
   https://www.youtube.com/watch?v=-Q_WXeEf8Fw

3. **“Vulnerabilities ofWireless Security protocols (WEPand WPA2)”**,
   Vishal Kumkar, Akhil Tiwari, Pawan Tiwari, Ashish Gupta, SeemaShrawne, April 2012
   https://dl.irstu.com/wp-content/uploads/Download/Education/Book/Network/Network

4. **“The evolution of wireless security in 802.11 networks: WEP, WPA and 802.11 standards”**,
   Stanley Wong, May 20 2003,
   https://pdfs.semanticscholar.org/383a/c2849fe53714c1b64e1d23392c0789730bc4.pdf

5. **“EVOLUTION OF WIRELESS LAN SECURITY ARCHITECTURE TO IEEE 802.11i (WPA2)“**,
   Moffat Mathews, Ray Hunt,
   https://s3.amazonaws.com/academia.edu.documents/21361193/moffatmathews-evolution-of-wireless-security.pdf?response-content-disposition=inline