Réalisation Professionnelle n°8 : Comparaison protocoles WIFI

Assurmer

Mathieu URGIN
Clément MONTMAYEUR

BTS SIO SISR 2B

Janvier 2024

Sommaire

Comparaison des protocoles de sécurité Wi-Fi

1.1 Introduction

Les protocoles de sécurité Wi-Fi jouent un rôle essentiel pour protéger les réseaux sans fil contre les intrusions et les cyberattaques. Depuis l'introduction de la norme IEEE 802.11, plusieurs protocoles de sécurité ont été développés pour faire face à l'évolution des menaces. Cette étude comparative analyse les différents protocoles, leurs forces, leurs faiblesses et leur pertinence dans les environnements modernes.

1.2 WEP (Wired Equivalent Privacy)

Le WEP est introduit avec la norme IEEE 802.11, il a été le premier protocole de sécurité Wi-Fi. Le WEP utilise une clé de cryptage RC4[1] de 64 bits ou 128 bits pour protéger les données transmises, il est assez simple à configurer et compatible avec les équipements les plus anciens mais souffre de grandes faiblesses. Le WEP est vulnérable à des attaques comme le cracking de clés et il manque de mécanismes de gestion de clés sécurisés, il est fortement déconseillé de nos jours.

1.3 WPA (Wi-Fi Protected Access)

Le WPA améliore la sécurité grâce à l'utilisation du protocole TKIP[2], le protocole TKIP renforce la gestion des clés et des vecteurs d'initialisation ce qui réduit les risques d'attaques. Il est facilement implantable sur du matériel existant et offre une sécurité accrue par rapport à WEP. Le protocole TKIP reste cependant vulnérable à certaines attaques à faible niveau. WPA a surtout été conçu comme solution temporaire en attendant WPA2.

1.4 WPA2 (Wi-Fi Protected Access 2)

WPA2 a marqué un grand pas en avant avec l'implémentation obligatoire d'AES pour le cryptage. Il propose deux modes d'authentification : personnel (PSK) et entreprise (EAP). WPA2 offre un haut niveau de sécurité et une compatibilité étendue avec les appareils modernes ce qui en fait la norme la plus utilisée à ce jour. Toutefois, certaines vulnérabilités comme KRACK montrent ses limites.
En mode personnel, un mot de passe unique partagé entre tous les utilisateurs est utilisé pour authentifier les connexions, ce mode est simple à configurer et adapté aux réseaux domestiques ou de petites entreprises. De l'autre côté, le mode entreprise repose sur un serveur d'authentification (généralement un serveur RADIUS) qui valide chaque utilisateur individuellement. Cela offre un contrôle total des accès et une sécurité renforcée mais nécessite une infrastructure plus complexe à mettre en place.

---

[1] **RC4 :** Algorithme de chiffrement de flux rapide et simple, utilisé dans des protocoles comme WEP, il est désormais considéré comme obsolète en raison de ses nombreuses vulnérabilités.
[2] **TKIP (Temporal Key Integrity Protocol) :** Protocole de sécurité utilisé avec WPA, qui améliore la gestion des clés et protège contre les attaques interceptant ou manipulant les données, mais reste vulnérable face à certaines failles avancées.

1.5 WPA3 (Wi-Fi Protected Access 3)

WPA3 vise à résoudre les limitations de WPA2, il introduit l'échange de clés basé sur le protocole SAE qui améliore la sécurité contre les attaques par force brute. Chaque session bénéficie d'un cryptage indépendant renforçant la confidentialité des données, sa simplicité et sa sécurité en font un choix idéal pour l'Internet des objets. Cependant, WPA3 souffre encore d'une compatibilité limitée avec les anciens appareils et son implémentation est encore en cours dans de nombreux environnements.

1.6 Conclusion

L'évolution des protocoles de sécurité Wi-Fi montre les efforts constants pour s'adapter aux nouvelles menaces tout en offrant des solutions fiables et accessibles. Bien que WEP et WPA soient aujourd'hui obsolètes, WPA2 reste largement utilisé tandis que WPA3 s'impose progressivement comme le standard de référence pour les réseaux modernes.