Comparaison des Protocoles de Sécurité Wi-Fi

Assurmer
Tom

Table des matières

1. Introduction

Les réseaux Wi-Fi sont présents partout, tant dans les environnements domestiques que professionnels. Cette omniprésence rend cruciale la sécurité des connexions. Différents protocoles ont été mis au point pour assurer cette sécurité. Ce document présente une étude comparative entre les protocoles WEP, WPA, WPA2 et WPA3.

2. WEP (Wired Equivalent Privacy)

Le protocole WEP, lancé en 1997, visait à fournir une sécurité équivalente aux réseaux filaires. Cependant, ses nombreuses failles en ont rapidement limité l'utilisation.

- Caractéristiques :
    - - Clés statiques de 40 ou 104 bits
    - - Utilisation de l'algorithme RC4
- Inconvénients :
    - - Vulnérable aux attaques par cryptanalyse
    - - Faible complexité des clés

3. WPA (Wi-Fi Protected Access)

Le WPA, introduit en 2003, comble les lacunes du WEP avec l'utilisation de clés dynamiques et le protocole TKIP.

- Caractéristiques :
    - - Clés dynamiques (TKIP)
    - - Authentification 802.1X
- Inconvénients :
    - - TKIP obsolète et vulnérable

4. WPA2 (Wi-Fi Protected Access 2)

WPA2, adopté en 2004, est encore aujourd'hui une norme largement utilisée, avec l'intégration de l'AES pour un chiffrement plus sécurisé.

- Caractéristiques :
    - - Chiffrement AES
    - - Support de CCMP
- Inconvénients :

- - Sensible aux attaques KRACK

5. WPA3 (Wi-Fi Protected Access 3)

WPA3 est le protocole le plus récent (2018) avec des mécanismes de sécurité plus robustes comme SAE et le chiffrement individualisé en réseau public.

- Caractéristiques :
  - - SAE pour contrer les attaques par force brute
  - - Chiffrement individuel en public
- Inconvénients :
  - - Nécessite un matériel compatible

6. Tableau Comparatif

Protocole	Année	Chiffrement	Avantages	Inconvénients
WEP	1997	RC4	Facile à configurer	Failles majeures, obsolète
WPA	2003	TKIP	Clés dynamiques, amélioration du WEP	TKIP vulnérable
WPA2	2004	AES (CCMP)	Sécurité renforcée, norme dominante	Vulnérable à KRACK
WPA3	2018	AES (SAE)	Protection accrue, chiffrement individuel	Matériel requis

7. Conclusion

Chaque protocole a contribué à l'évolution de la sécurité Wi-Fi. Aujourd'hui, WPA3 représente le standard à privilégier pour assurer un niveau de sécurité adapté aux menaces actuelles.