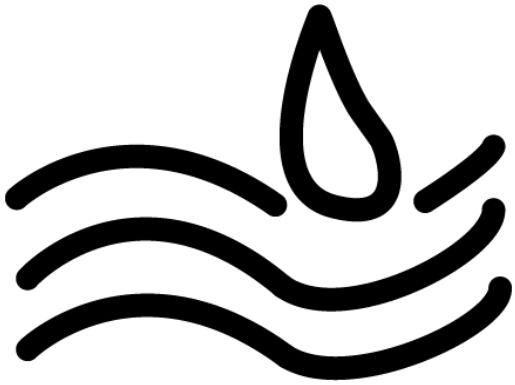
COMPARAISON

Des protocols



Assurmer
Nassim, Dorian, Remi

Table des matières

Étude Comparative des Différents Protocoles de Sécurité Wi-Fi

Introduction

Les réseaux Wi-Fi sont omniprésents dans les environnements modernes, qu'ils soient domestiques, professionnels ou publics. Avec cette popularité accrue, la sécurité des communications sans fil est devenue une préoccupation majeure. Plusieurs protocoles de sécurité ont été développés pour protéger les réseaux Wi-Fi, chacun ayant ses forces et faiblesses. Cette étude vise à comparer les principaux protocoles de sécurité Wi-Fi : WEP, WPA, WPA2 et WPA3.

WEP (Wired Equivalent Privacy)

Le WEP, introduit en 1997, est le premier protocole de sécurité Wi-Fi. Il visait à fournir un niveau de sécurité équivalent à celui des réseaux filaires. Cependant, il présente de nombreuses vulnérabilités qui le rendent obsolète.

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

WPA (Wi-Fi Protected Access)

Le WPA a été introduit en 2003 comme une solution temporaire pour combler les lacunes du WEP. Il utilise des améliorations de sécurité, mais reste vulnérable dans certaines configurations.

- Caractéristiques :
    - - Utilisation de clés dynamiques grâce au protocole TKIP.
    - - Prise en charge de l'authentification basée sur 802.1X.
- Inconvénients :
    - - TKIP est considéré comme obsolète et vulnérable.

WPA2 (Wi-Fi Protected Access 2)

Le WPA2, introduit en 2004, est une version améliorée de WPA. Il reste l'une des normes les plus utilisées aujourd'hui pour sécuriser les réseaux Wi-Fi.

- Caractéristiques :

- - Utilisation de l'algorithme AES pour le chiffrement.
- - Support de CCMP pour une meilleure intégrité des données.

- Inconvénients :
  - - Vulnérable à certaines attaques comme KRACK (Key Reinstallation Attacks).

WPA3 (Wi-Fi Protected Access 3)

Le WPA3, lancé en 2018, est la version la plus récente et la plus sécurisée. Il résout de nombreuses failles des protocoles précédents tout en introduisant de nouvelles fonctionnalités.

- Caractéristiques :
  - - Amélioration de la protection contre les attaques par force brute grâce à SAE (Simultaneous Authentication of Equals).
  - - Chiffrement individuel des données dans les réseaux publics.

- Inconvénients :
  - - Requiert du matériel compatible, limitant son adoption dans certains cas.

Tableau Comparatif

Le tableau ci-dessous résume les principales différences entre les protocoles de sécurité Wi-Fi :

Protocole	Année d'introduction	Chiffrement utilisé	Avantages	Inconvénients
WEP	1997	RC4	Facile à configurer	Vulnérabilités majeures, clés statiques, obsolète
WPA	2003	TKIP	Clés dynamiques, amélioration par rapport au WEP	TKIP vulnérable, considéré comme obsolète
WPA2	2004	AES (avec CCMP)	Sécurité renforcée, support étendu, norme dominante	Vulnérable à certaines attaques comme KRACK
WPA3	2018	AES (avec SAE)	Protection contre les attaques par force brute, chiffrement individuel	Nécessite du matériel compatible, adoption limitée pour les anciens appareils

Conclusion

Chaque protocole de sécurité Wi-Fi a joué un rôle dans l'évolution de la protection des réseaux sans fil. Toutefois, avec l'évolution des technologies et des menaces, il est crucial d'adopter les protocoles les plus récents, comme le WPA3, pour garantir un niveau de sécurité optimal.