Sécurisation d'une borne wifi

Étude comparative des différents protocoles de sécurité Wi-Fi

DRIF WASSIM
CHAMMAH GUILLAUME
LEGROS KYLIAN

Table des matières

Étude comparative des différents protocoles de sécurité Wi-Fi

Qu'est-ce que le Wi-Fi ?

Le Wi-Fi est un ensemble de protocoles de communications sans fil régi par les normes du groupe IEEE 802.11. C'est une onde radio (bandes de fréquences hertziennes) qui permet de relier plusieurs appareils informatiques au sein d'un même réseau pour permettre un échange de données entre eux.

Quelle est la différence entre tous ces paramètres qui varient dans les différentes normes Wi-Fi ?

Chaque norme possède une certaines :

- Puissance de signal
- Portée du signal
- Fréquence sur laquelle le signal se diffuse (Hz)

La puissance du signal se compte en bits par seconde. Il s'agit de la vitesse de transfert de l'information. Plus la puissance du signal est forte, plus les téléchargements, les accès aux sites webs ou bien les vidéos seront plus rapides d'accès.

La portée du signal est la portée maximale que le signal peut émettre. Les obstacles peuvent également freiner la diffusion de l'onde et donc sa puissance et sa portée. Plus la bande de fréquence est élevée, plus le réseau sera sensible aux obstacles et aura une faible portée.

La fréquence fait référence à la bande de fréquences radio utilisée pour transmettre des données sans fil entre les périphériques connectés au réseau Wi-Fi et la borne d'accès. Les deux fréquences principales utilisées dans les réseaux sont 2.4 GHz et 5 GHz. Ces deux différentes fréquences peuvent affecter la portée, la vitesse et la capacité à traverser les obstacles physiques tels que les murs.

Qu'est-ce qu'un protocole de sécurité Wi-Fi ?

Un protocole de sécurité Wi-Fi est un ensemble de règles et de procédures conçues pour protéger les réseaux sans fil (Wi-Fi) contre les accès non autorisés et les attaques. Ces protocoles permettent d'assurer la confidentialité des données, à sécuriser les communications entre les dispositifs connectés au réseau Wi-Fi et à garantir l'authentification des utilisateurs.

Listes des protocoles de sécurité Wifi les plus courant :

- WEP (Wired Equivalent Privacy) : C'était l'un des premiers protocoles de sécurité Wi-Fi qui est un chiffrement de 40, 64, 128 et 256 bits mais il est maintenant obsolète et très vulnérable aux attaques possédant des technologies surpassant le protocole WEP.

- WPA (Wi-Fi protected Access) : WPA est le successeur de WPE pour remédier aux faiblesses de WEP. Ce protocole respecte la majorité de la norme IEEE 802. 11i et il est compatible 802. 11b et 802. 11g. Il fonctionne donc avec les matériels ne supportant que ces normes. La plupart des application modernes utilisent une clé pré-partagée (PSK) (c'est une clé qui est utilisé pour authentifier les utilisateurs sur les réseaux locaux sans fil en entreprise ou à la maison) ou appelé WPA Personal et le protocole d'intégrité de clé temporelle ou TKIP pour le chiffrement. Il est compatible avec EAP (Extensible Authentication Protocol)

qui est un infrastructure d'authentification qui permet l'utilisation de différentes méthodes d'authentification pour les technologies d'accès réseau sécurisées (Wi-Fi, VPN etc…). Il s'agit d'une infrastructure sur le client d'accès et sur le serveur d'authentification. EAP possède de nombreuses méthodes d'authentification comme EAP-TLS, EAP-TTLS, EAP-MSCHAPv2 etc… qui permettent une meilleure sécurité pour l'authentification. (en encapsulant pour la plupart)

- WPA2 (Wi-Fi Protected Access version 2) : WPA2 est le successeur de WPA2 et il est compatible 100% avec IEEE 802.11i. Il fonctionne avec une clé pré-partagée PSK (comme son aïeul WPA) et pour cela il utilise la norme de chiffrement avancé AES (Advanced Encryption Standard). (L'AES est un algorithme de chiffrement symétrique que l'on utilise très souvent, par exemple pour le chiffrement de fichiers ou le disque (bloc). Il est considéré comme étant plus sûr et remplace TKIP. WPA2 est vulnérable aux attaques par bruteforce, ainsi la longueur du mot de passe Wi-Fi est très important. WPA2 est également éligible au protocole EAP et PEAP.

- WPA3 (Wi-Fi Access version 3) : WPA3 utilise une nouvelle norme qui crypte en 128 bits en mode WPA3-Personal et 192 bits en mode WPA3-Enterprise. WPA3 remplace également PSK par SAE (Simultaneous Authentication of Equals) basé sur Diffie-Hellman key exchange c'est-à-dire avec des mots de passe secrets pour empêcher ces types d'attaques. En utilisant SAE, les appareils peuvent établir une connexion Wi-Fi sécurisée sans nécessiter de pré-partage de clé statique, ce qui améliore la sécurité globale du réseau sans fil.

- WPA3-Enterprise (Wi-Fi Protected Access version 3 - Enterprise) : Le WPA3-Enterprise utilise une norme avancée qui crypte les données en 192 bits, offrant un niveau de sécurité supérieur, conforme à la suite cryptographique CNSA (Commercial National Security Algorithm). Ce mode est spécifiquement conçu pour les environnements professionnels et les réseaux critiques. WPA3-Enterprise repose sur le protocole 802.1X et utilise un serveur RADIUS pour une authentification centralisée, basée sur des certificats numériques ou des identifiants uniques. Ce mécanisme renforce la sécurité en exigeant une validation stricte des utilisateurs et des appareils. Grâce à ces améliorations, le WPA3-Enterprise protège efficacement contre les attaques par interception, les attaques par dictionnaire et les accès non autorisés, tout en garantissant une sécurité réseau robuste et fiable pour les entreprises

Comparaison des différents protocoles de sécurité

Ces tableaux nous indiquent les principales différences entre plusieurs protocoles de sécurité.

Fonctionnalités	Méthode de chiffrement	Gestion des clés	Compatibilité	Niveau de sécurité
WPA	TKIP	PSK et EAP	Appareils plus anciens	Modérés
WPA2	AES	PSK et EAP	Appareils plus modernes	Élevée
WPA3	AES et SAE	PSK, EAP et SAE	Appareils plus récents	Très élevée
WPA3-ENTREPRISE	AES-192	EAP via 802.1X.	Appareils récents et réseaux professionnels nécessitant une infrastructure avancée.	Très élevée

Protocole de sécurité	Avantages	Inconvénients
WPA	Compatible avec les appareils les plus anciens, meilleure sécurité par rapport à WEP	Moins sécurisé que WPA2 et WPA3, sensibles aux attaques, compatible qu'avec certaines normes
WPA2	Cryptage fort (AES), compatible avec de nombreux appareils	Nécessite plus de puissance de traitement, problèmes de compatibilité avec les appareils plus anciens, moins sécurisé que WPA3
WPA3	Fonctionnalités de sécurité améliorées, bonne résistances aux attaques par dictionnaire hors-ligne	Nécessite un matériel moderne, WPA3 n'est pas encore adopté partout
WPA3-Entreprise	Sécurité renforcée grâce au chiffrement AES-192 et à la gestion centralisée des utilisateurs.	Coûts élevés pour la mise en place et la maintenance.