ESIEE [it]
L'école de l'expertise numérique

PRESENTATION WIFI

Auteurs : *Carvalho Tom, Bagassien Stephen, Dez Sofiane*

Référence : *Assurmer*

Date : *10/02/2024*

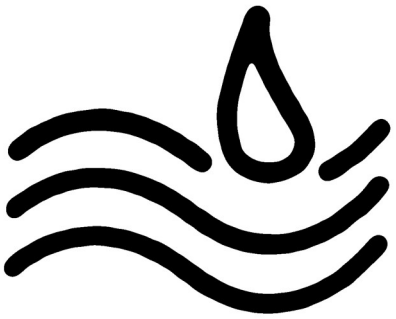

Table des matières

Étude comparative des différents protocoles de sécurité WIFI

Qu'est-ce que le WIFI ?

Le WIFI, acronyme de "Wireless Fidelity", est une technologie sans fil qui permet la transmission de données entre des appareils électroniques via des ondes radio. Elle élimine la nécessité de câbles physiques, offrant ainsi une connectivité flexible et pratique dans divers environnements.

Principes Fondamentaux du WIFI :

Le fonctionnement du WIFI repose sur la norme IEEE 802.11, établissant les protocoles et les règles pour les réseaux locaux sans fil (WLAN). Les périphériques compatibles WIFI, tels que les ordinateurs, les smartphones, et les objets connectés, communiquent entre eux via des points d'accès sans fil, souvent intégrés à des routeurs.

Modes de Fonctionnement :

Le WIFI opère principalement dans deux modes : l'infrastructure et l'adhoc. Dans le mode infrastructure, les appareils se connectent à un point d'accès central, tandis que le mode adhoc permet la communication directe entre les appareils sans nécessiter d'infrastructure supplémentaire.

Bande Fréquence :

Les réseaux WIFI utilisent différentes bandes de fréquences, notamment 2,4 GHz et 5 GHz. La bande de 2,4 GHz offre une meilleure portée, tandis que la bande de 5 GHz offre des vitesses de transmission plus élevées avec moins d'interférences.

Protocoles de Sécurité WIFI :

La sécurité est une préoccupation majeure dans les réseaux WIFI. Les protocoles tels que WEP (Wired Equivalent Privacy), WPA (WIFI Protected Access), et WPA2/WPA3 sont utilisés pour chiffrer les données et protéger les réseaux contre les accès non autorisés.

Avantages du WIFI :

Mobilité : Le WIFI offre une connectivité sans fil, permettant aux utilisateurs de se déplacer librement tout en restant connectés au réseau.

Connectivité Multiple : Plusieurs appareils peuvent se connecter simultanément à un réseau WIFI, favorisant le partage de ressources.

Flexibilité : Les réseaux WIFI peuvent être déployés dans divers environnements, tels que les domiciles, les entreprises, les cafés, et les espaces publics.

Applications du WIFI :

Accès à Internet : La connexion WIFI est largement utilisée pour l'accès à Internet, offrant une alternative pratique aux connexions filaires.

Réseaux Domestiques et Professionnels : Les réseaux WIFI sont essentiels dans les foyers et les entreprises, permettant le partage de fichiers, d'imprimantes, et d'autres ressources.

Présentation de sécurité WIFI

La sécurité sans fil vise à empêcher tout accès non autorisé aux réseaux WIFI et à garantir la confidentialité des données transitant sur ces réseaux. Plusieurs protocoles de sécurité ont été développés pour répondre à ces préoccupations croissantes.

Les Protocoles de Sécurité WIFI les Plus Courants

WEP (Wired Equivalent Privacy) : Introduit en 1997, le WEP était le premier protocole de sécurité WIFI. Cependant, il a rapidement montré des failles importantes, le rendant obsolète et non recommandé pour une utilisation sécurisée.

WPA (WIFI Protected Access) : Lancé en 2003 pour pallier les faiblesses du WEP, le WPA introduit des améliorations significatives, mais présente également des vulnérabilités, notamment liées au protocole TKIP.

WPA2 (WIFI Protected Access 2) : Introduit en 2004, le WPA2 a renforcé la sécurité en remplaçant le protocole TKIP par le protocole AES. Malgré ses améliorations, des vulnérabilités subsistent, en particulier dans les points d'accès utilisant encore le WEP.

WPA3 (WIFI Protected Access 3) : Lancé en 2018, le WPA3 apporte des améliorations majeures, renforçant la confidentialité des données et introduisant des fonctionnalités avancées de protection. Son adoption progresse pour remplacer progressivement le WPA2.

Tableau de comparaison de type de sécurité WIFI

Caractéristiques de Sécurité WIFI	WEP (Wired Equivalent Privacy)	WPA (WIFI Protected Access)	WPA2 (WIFI Protected Access 2)	WPA3 (WIFI Protected Access 3)
Année d'introduction	1997	2003	2004	2018
Protocole de Chiffrement	RC4	TKIP (Temporal Key Integrity Protocol), AES (Advanced Encryption System)	CCMP (Counter Mode Cipher Block Chaining Message Authentication Code Protocol), AES	SAE (Simultaneous Authentication of Equals), WPA3-Personal, WPA3-Enterprise
Longueur de Clé (bits)	64 bits (WEP-64), 128 bits (WEP-128)	256 bits (WPA2)	192 bits, 256 bits (WPA2-AES)	192 bits, 384 bits (WPA3-Personal), 192 bits, 384 bits, 512 bits (WPA3-Enterprise)
Vulnérabilités Notables	Faiblesse face aux attaques par clé statique, vulnérable aux attaques par réinjection de paquets	Failles liées à TKIP, WIFI Protected Setup (WPS)	Certaines attaques contre WPA2-PSK (Pre-Shared Key)	Les versions précédentes de WPA3-Personal peuvent être sujettes à des attaques de type bruteforce
Méthode d'Authentification	Clé partagée (Partagée entre les utilisateurs)	PSK (Pre-Shared Key), Entreprise (utilise un serveur d'authentification)	PSK, Entreprise	PSK, SAE (Simultaneous Authentication of Equals), Entreprise
Principales Améliorations	X	Amélioration de la clé de chiffrement (TKIP), ajout du WPA2-PSK	Remplacement du TKIP par le CCMP (AES), renforcement de la sécurité	Amélioration de la confidentialité des données, protocole de chiffrement SAE, renforcement de la protection contre les attaques par force brute
Utilisation Recommandée	Non recommandé, obsolète	Utilisé comme transition de WEP à WPA2, mais désormais dépassé par WPA2/WPA3	Recommandé, largement utilisé	En cours de déploiement, devrait progressivement remplacer WPA2

Bibliographie

1. https://www.avast.com/fr-fr/c-wep-vs-wpa-or-wpa2
2. https://www.avg.com/fr/signal/wep-wpa-or-wpa2
3. https://community.fs.com/fr/article/wep-vs-wpa-vs-wpa2-vs-wpa3.html
4. https://cyber.gouv.fr/publications/securiser-les-acces-wi-fi