La norme IEE802.11

la norme **IEE82.11** désigne la norme Wi-Fi la plus utilisée pour les réseaux sans fil. Elle définit la couche physique dans un réseau sans fil.

C’est un ensemble de standards définissant les protocoles et spécifications techniques pour les réseaux locaux sans fil (Wi-Fi).

Etude comparative des différents protocoles de sécurité Wi-Fi

Les différents protocoles de sécurité Wi-Fi sont les suivants :
WEP, WPA, WPA2 et **WPA3**

WEP

Offre une sécurité de base contre les intrusions.
Avantages : Compatibilité avec une large gamme d'appareils plus anciens et facile à configurer.

Inconvénients : Les mesures de sécurité du WEP sont nettement dépassées par rapport aux normes contemporaines.
Son algorithme de chiffrement est vulnérable à l'attaque par force brute et au sniffing, il lui manque les mécanismes d'échange dynamique de clés trouvés dans les protocoles ultérieurs.

WPA

Développée pour résoudre plusieurs des problèmes apparus avec le WEP.

Avantages : Utilisation du TKIP ou chiffrement à clé dynamique, qui renouvelle régulièrement la clé d'accès au réseau.
Tous les appareils du réseau reconnaissent la nouvelle clé lorsqu'elle est générée.

Inconvénients : Le TKIP s'est révélé vulnérable et peut être facilement piraté.
La complexité de l'algorithme peut désormais être surmontée par la puissance de calcul moderne.
Si les utilisateurs et les administrateurs de réseau ne créaient pas de mots de passe forts, les données étaient vulnérables.
Si l'on compare le WPA au WEP, les avantages du WPA en matière de sécurité sont considérables, mais ses défauts apparaissent rapidement.

WPA2

Sert à augmenter la complexité de son prédécesseur (WPA) et constitue la norme en matière de sécurité réseau depuis plus de dix ans.
Avantages : Il offre les mêmes avantages que ceux introduits par le WPA.
Il utilise le chiffrement AES, très robuste.
Les mots de passe doivent être plus longs, ce qui renforce la sécurité.
Inconvénients : Nécessite un matériel compatible, ce qui peut poser problème pour les équipements anciens.
Vulnérable aux attaques Man-in-the-middle.

WPA3

Sert à augmenter la complexité de son prédécesseur (WPA) et constitue la norme en matière de sécurité réseau depuis plus de dix ans.
Avantages : Il offre les mêmes avantages que ceux introduits par le WPA.
Il utilise le chiffrement AES, très robuste.
Les mots de passe doivent être plus longs, ce qui renforce la sécurité.
Inconvénients : Nécessite un matériel compatible, ce qui peut poser problème pour les équipements anciens.
Vulnérable aux attaques Man-in-the-middle.