3.5. WPA3 (Wi-Fi Protected Access 3)

Introduit en 2018.

Caractéristiques principales :
Protège contre les attaques par force brute grâce au protocole SAE (Simultaneous Authentication of Equals).
Chiffrement des données même sur les réseaux ouverts (OWE, Opportunistic Wireless Encryption).
Introduit le 192-bit security suite pour les environnements professionnels nécessitant une sécurité élevée.

Forces :
SAE empêche la réutilisation des clés et renforce la sécurité des mots de passe faibles.
Protection accrue contre les attaques passives et actives.
Compatibilité avec les anciens équipements en mode transition WPA2/WPA3.

Faiblesses :
Pas encore universellement adopté (nécessite des équipements compatibles).
Les attaques de type downgrade (forcer un passage à WPA2) peuvent encore exister si les deux protocoles sont activés.

Statut actuel :
Recommandé pour les nouveaux réseaux, en particulier dans les environnements critiques.

4. Présentation du fonctionnement d'une solution RADIUS et certificats

Le protocole RADIUS (Remote Authentication Dial-In User Service) centralise l'authentification, l'autorisation, et la gestion des comptes d'accès dans un réseau. Il est souvent utilisé pour sécuriser l'accès Wi-Fi dans des environnements professionnels.

4.1. Principes de base

Client RADIUS : Le point d'accès Wi-Fi relaye les requêtes d'authentification.
Serveur RADIUS : Vérifie les identifiants ou certificats dans une base de données centralisée (ex. Active Directory).
Réponse : Autorisation ou refus d'accès au réseau selon les règles définies.

RADIUS avec certificats :
Utilise des certificats numériques au lieu des mots de passe, via une infrastructure à clé publique (PKI).
Basé sur des protocoles comme EAP-TLS pour une authentification mutuelle (client et serveur).
Protège contre les attaques par écoute et les compromissions de mots de passe.

Avantages :
Sécurité élevée : Supprime les mots de passe, empêche le phishing.
Gestion centralisée : Un point de contrôle unique pour gérer les accès.
Adaptabilité : Idéal pour les réseaux d'entreprise ou universitaires.

En somme, RADIUS associé aux certificats garantit un accès réseau sécurisé et bien adapté aux environnements nécessitant une forte sécurité.