PROJET ASSURMER

2024

AUTEURS :

DE CARVALHO LOPES Bruno
BELAHA Sidahmed
LE CLAINCHE Killian

DATE :

07/01/2025

Sommaire

Analyse détaillée des protocoles

WEP (Wired Equivalent Privacy)

- **Résumé historique** : Introduit en 1997 avec la norme IEEE 802.11 pour offrir une sécurité équivalente à celle des réseaux filaires.
- **Technologie utilisée** :
    - Chiffrement basé sur RC4.
    - Longueur des clés : 40 bits (standard) ou 104 bits (amélioré).
    - Utilisation d'un vecteur d'initialisation (IV) de 24 bits.
- **Forces** :
    - Compatibilité étendue, même sur les équipements très anciens.
    - Facile à configurer.
- **Faiblesses** :
    - Le chiffrement RC4 est obsolète et vulnérable.
    - Le vecteur d'initialisation est trop court, entraînant des collisions fréquentes.
    - Vulnérabilités : FMS (Fluhrer, Mantin et Shamir), cracking rapide avec des outils comme Aircrack-NG.
- **Statut actuel** : Complètement abandonné par la Wi-Fi Alliance et déconseillé dans tous les cas.

WPA (Wi-Fi Protected Access)

- **Résumé historique** : Introduit en 2003 comme une solution temporaire à WEP.
- **Technologie utilisée** :
  - Chiffrement TKIP (Temporal Key Integrity Protocol) basé sur RC4.
  - Mise à jour dynamique des clés pour empêcher les attaques de rejouement.
- **Forces** :
  - Corrige certaines failles de WEP, notamment les collisions d'IV.
  - Relativement facile à déployer sur les équipements WEP avec mise à jour logicielle.
- **Faiblesses** :
  - Le protocole RC4 reste faible par conception.
  - Vulnérable à des attaques comme Michael (exploit des checksum) et attaques par dictionnaire.
- **Vulnérabilités majeures** :
  - Vulnérable aux attaques par brute force sur le protocole PSK (Pre-Shared Key).
  - Man-in-the-Middle et attaques par replay possibles.
- **Statut actuel** : Obsolète, bien que toujours en usage sur des équipements anciens.

WPA2 (Wi-Fi Protected Access 2)

- **Résumé historique** : Standard depuis 2004, introduisant des améliorations majeures.
- **Technologie utilisée** :
    - Chiffrement AES (Advanced Encryption Standard) avec CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol).
    - Deux modes d'utilisation : **PSK** (clé partagée) pour les environnements domestiques et **EAP** (Extensible Authentication Protocol) pour les entreprises.
- **Forces** :
    - Protection contre les attaques par replay.
    - AES est une norme de chiffrement robuste et largement adoptée.
    - Adapté aux environnements professionnels et domestiques.
- **Faiblesses** :
    - Vulnérable à certaines attaques (exemple : KRACK - Key Reinstallation Attack, découvert en 2017).
    - Les clés PSK faibles (courtes ou simples) peuvent être crackées via brute force.
- **Statut actuel** : Toujours utilisé, mais en transition vers WPA3.

WPA3 (Wi-Fi Protected Access 3)

- **Résumé historique** : Lancement en 2018 pour répondre aux failles de WPA2.
- **Technologie utilisée** :
    - Chiffrement renforcé basé sur SAE (Simultaneous Authentication of Equals).
    - Chiffrement individualisé pour chaque session utilisateur (chiffrement opportuniste).
    - Améliorations pour les appareils IoT via Wi-Fi Easy Connect.
- **Forces** :
    - Résistance accrue aux attaques par force brute (avec SAE, une attaque réussie nécessite d'attaquer chaque mot de passe individuellement).
    - Protection contre les attaques de désauthentification.
    - Adapté aux environnements modernes (domotique, IoT).
- **Faiblesses** :
    - Moins de compatibilité avec les anciens appareils.
    - Coût potentiellement plus élevé pour la mise à niveau des infrastructures.
- **Statut actuel** : Recommandé pour toutes les nouvelles installations.

Tableau comparatif

Protocole	Année	Chiffrement	Forces	Faiblesses	Statut actuel
WEP	1997	RC4	Simplicité, Compatibilité	Extrêmement vulnérable	Abandonné
WPA	2003	TKIP/RC4	Corrige WEP, clé dynamique	Faible sécurité, attaques possibles	Dépassé
WPA2	2004	AES/CCMP	Sécurité fiable, largement adopté	Vulnérabilités comme KRACK	Standard courant
WPA3	2018	AES/SAE	Sécurité avancée	Compatibilité limitée, plus coûteux	Standard recommandé

Conclusion

- **WEP** et **WPA** sont à éviter en raison de leur obsolescence et de leur faible sécurité.
- **WPA2** reste adapté à de nombreux contextes, mais il est impératif de l'utiliser avec des mots de passe robustes et de déployer des correctifs pour les vulnérabilités connues (ex. KRACK).
- **WPA3** est la meilleure option pour les nouvelles installations, offrant des améliorations substantielles en termes de sécurité et d'efficacité.