COMPARAISON DES DIFFERENTS PROTOCOLES DE SECURITE WI-FI

WEP/WPA (1/2/3)

ASSURMER

Montpellier, Occitanie, France

Ezequiel-junior VARELA-MONTEIRO
Kévin BOULIER
SISR 2B

Version	Date version	Auteur	Validateur et date	Destinataires	Diffusion document	Nbr. de pages	Commentaires
1	13/01/24	Ezequiel-junior VARELA MONTEIRO	Aucun	Service DSI	Interne via Teams	4	

Table des matières

Introduction

La sécurité des réseaux Wi-Fi est un enjeu majeur pour les entreprises et les particuliers. Plusieurs protocoles de sécurité ont été développés au fil du temps pour protéger les données et garantir la confidentialité des communications. Ce document présente une analyse comparative des différents protocoles, en mettant en avant leurs forces et leurs faiblesses.

Description des protocoles

1. **WEP (Wired Equivalent Privacy)** :
   - Introduit en 1997, il s'agissait du premier standard de sécurité pour les réseaux Wi-Fi.
   - Chiffrement faible basé sur l'algorithme RC4 et des clés statiques, ce qui le rend vulnérable.
   - Désormais considéré comme obsolète et à éviter.
2. **WPA (Wi-Fi Protected Access)** :
   - Introduit pour remédier aux failles de WEP.
   - Utilise TKIP (Temporal Key Integrity Protocol) pour générer des clés dynamiques.
   - Bien que plus sécurisé que WEP, il reste vulnérable aux attaques modernes.
3. **WPA2** :
   - Chiffrement avancé avec AES (Advanced Encryption Standard).
   - Introduction de l'authentification 802.1X pour une sécurité renforcée.
   - Norme encore largement utilisée aujourd'hui, bien qu'elle présente des failles potentielles (ex : attaque KRACK).
4. **WPA3** :
   - Dernier standard en date, conçu pour résoudre les faiblesses de WPA2.
   - Amélioration de la protection contre les attaques par force brute grâce à SAE (Simultaneous Authentication of Equals).
   - Offre un chiffrement plus robuste et une meilleure confidentialité des données.

Comparaison

Protocole	Année d'introduction	Niveau de sécurité	Points forts	Limites
WEP	1997	Faible	Premier standard Wi-Fi	Vulnérabilité extrême
WPA	2003	Modéré	Clés dynamiques avec TKIP	Toujours vulnérable
WPA2	2004	Fort	Chiffrement AES performant	Susceptible à certaines attaques
WPA3	2018	Très fort	SAE, protection renforcée	Compatibilité matérielle limitée

Conclusion

En conclusion le choix du protocole de sécurité doit s’adapter à la situation et aux besoins spécifiques de chaque organisation :

WPA3 est la solution la plus appropriée pour les environnements modernes disposant d'équipements compatibles. Il offre une sécurité robuste grâce à SAE et une protection accrue contre les attaques par force brute, en faisant le choix idéal pour les entreprises et les utilisateurs souhaitant une connectivité optimale.

WPA2 reste une alternative fiable pour les réseaux utilisant des appareils plus anciens. Afin de limiter les risques, il est crucial de mettre en place des mots de passe forts et de s'assurer que toutes les mises à jour de sécurité disponibles ont été appliquées.

WEP et WPA ne doivent jamais être utilisés en raison de leurs failles de sécurité critiques.