AP 8 : COMPARAISON DES PROTOCOLES DE SÉCURITÉ WIFI	HUYNH Michael SAKO Bah FRANÇAIS Benjamin 2B-SISR

ASSURMER

Version	Auteur	Date	Nombre de pages	À l'attention de	Mode de diffusion	Validateur
1.0	HUYNH Michael	08/01/2025	8	Assurmer-IT	Document PDF	Aucun

COMPARAISON DES PROTOCOLES DE SÉCURITÉ WIFI

Table des matières

Introduction à la comparaison des protocoles WiFi

La sécurité des réseaux Wi-Fi est une préoccupation majeure pour les entreprises et les particuliers, en raison de la transmission de données sensibles sur des canaux sans fil susceptibles d'être interceptés. Au fil des années, plusieurs protocoles de sécurité ont été développés pour protéger ces communications, chacun offrant des niveaux de protection variés. Nous ferons une analyse comparative des principaux protocoles de sécurité Wi-Fi **WEP**, **WPA**, **WPA2** et **WPA3** en mettant en lumière leurs caractéristiques, leurs forces et leurs faiblesses respectives. Cette comparaison nous permettra d'avoir une compréhension claire de l'évolution des mesures de sécurité sans fil et à guider notre choix du protocole le plus adapté à notre infrastructure.

Description des différents protocoles de sécurité WiFi

La sécurité des réseaux Wi-Fi a évolué à travers plusieurs générations de protocoles, chacun introduisant des améliorations significatives pour répondre aux vulnérabilités identifiées. Voici une analyse détaillée des principaux protocoles, classés par ordre chronologique.

1. WEP (Wired Equivalent Privacy - 1997)

Le protocole WEP, introduit en 1997, est le premier standard de sécurité conçu pour les réseaux Wi-Fi. À l'époque, il visait à offrir un niveau de confidentialité équivalent à celui des réseaux filaires.

Il repose sur l'algorithme de chiffrement RC4 et des clés statiques de 64 ou 128 bits.

Bien que novateur à son lancement, WEP est rapidement devenu obsolète en raison de faiblesses majeures, notamment la réutilisation des clés d'initialisation (IV) qui le rend vulnérable aux attaques par force brute ou par cryptanalyse.

WEP est aujourd'hui considéré comme non sécurisé et n'est plus recommandé. Son usage a été largement abandonné au profit de standards plus robustes.

2. WPA (Wi-Fi Protected Access - 2003)

WPA a été introduit en 2003 comme une solution temporaire pour combler les lacunes de WEP, avant le développement de WPA2.

Il utilise le protocole TKIP (Temporal Key Integrity Protocol), qui génère des clés dynamiques pour chaque session afin de renforcer la sécurité.

Bien que plus sécurisé que WEP, WPA reste vulnérable à certaines attaques modernes, comme celles exploitant des failles dans TKIP.

WPA est considéré comme obsolète, bien qu'il puisse être rencontré dans des réseaux plus anciens ou pour des appareils moins performants.

3. WPA2 (2004)

En 2004, WPA2 est devenu le nouveau standard de sécurité pour les réseaux Wi-Fi, intégrant des améliorations majeures par rapport à WPA.

Il s'appuie sur le chiffrement AES (Advanced Encryption Standard) pour protéger les données, et introduit le protocole d'authentification 802.1X pour une gestion granulaire des accès réseau.

Bien que largement utilisé, WPA2 présente des vulnérabilités, comme l'attaque KRACK (Key Reinstallation Attack), qui exploite des failles dans la gestion des clés.

WPA2 reste une option fiable pour de nombreux réseaux, bien qu'il commence à être remplacé par WPA3 dans les environnements exigeants.

4. WPA3 (2018)

Lancé en 2018, WPA3 est la dernière évolution des standards de sécurité Wi-Fi, conçue pour résoudre les failles de WPA2 et offrir une protection accrue face aux menaces modernes.

Il introduit le protocole SAE (Simultaneous Authentication of Equals), qui renforce la résistance aux attaques par force brute et améliore la confidentialité des données échangées.

WPA3 offre une meilleure protection pour les réseaux ouverts (sans mot de passe) grâce à **OWE** (Opportunistic Wireless Encryption) et prend en charge le chiffrement individualisé des sessions.

Bien que très sécurisé, WPA3 nécessite des équipements compatibles, ce qui peut limiter son adoption immédiate dans certains environnements.

WPA3 est fortement recommandé pour les réseaux modernes disposant d'équipements compatibles.

Protocole	Année	Technologie principale	Forces
WEP	1997	RC4, clés statiques	Premier protocole standard pour Wi-Fi- Simple à configurer
WPA	2003	TKIP	Génération dynamique des clés pour réduire les failles de WEP- Compatibilité avec les anciens équipements
WPA2	2004	AES, 802.1X	Chiffrement avancé avec AES- Support des protocoles EAP et 802.1X- Sécurité robuste et largement adoptée
WPA3	2018	SAE, OWE, chiffrement avancé	Résistance accrue aux attaques par force brute grâce à SAE- Protection renforcée des réseaux ouverts (OWE)- Chiffrement individualisé des sessions

Faiblesses	Environnements adaptés	Recommandations actuelles
Clés statiques réutilisées (faiblesse fondamentale)- Vulnérable aux attaques par force brute et par cryptanalyse- Obsolète	Aucun : totalement obsolète	Ne doit jamais être utilisé, même sur des réseaux fermés
Sensible aux attaques modernes- Chiffrement TKIP moins robuste qu'AES- Faiblesses structurelles héritées de WEP	Réseaux anciens avec limitations matérielles	Transition immédiate vers WPA2 ou WPA3
Attaques par réinstallation de clés (KRACK)- Nécessite des configurations avancées pour maximiser la sécurité	Réseaux domestiques et professionnels standards	Utilisation encore valable, mais une migration vers WPA3 est fortement conseillée
Nécessite des équipements récents- Compatibilité limitée avec les anciens appareils	Réseaux modernes et critiques Environnements nécessitant une sécurité élevée	Standard recommandé pour tous les nouveaux réseaux et déploiements

Conclusion

Le choix du protocole de sécurité Wi-Fi doit s’adapter aux besoins spécifiques de chaque organisation et à la compatibilité de ses équipements. WPA3 représente aujourd’hui la solution la plus robuste, grâce à des technologies avancées comme SAE, qui renforcent la protection contre les attaques par force brute et garantissent une confidentialité accrue des données. Pour les environnements où les appareils compatibles avec WPA3 ne sont pas encore disponibles, WPA2 demeure une alternative fiable, à condition de maintenir des mots de passe complexes et de veiller à appliquer toutes les mises à jour de sécurité.

En revanche, WEP et WPA doivent être évités en raison de leurs failles critiques qui exposent les réseaux à des risques élevés d’intrusion. Pour sécuriser efficacement les réseaux, il est essentiel d’adopter des protocoles modernes, de renforcer les pratiques de sécurité (telles que le renouvellement régulier des mots de passe) et de planifier une transition progressive vers WPA3 pour bénéficier des dernières avancées en matière de protection des données.

Webographie

Security Boulevard

Cisco

NetSpot