Étude comparative des différents protocoles de sécurité Wi-Fi

BTS SIO SISR

Elijah B – Abdou A – Aymeric P

Planning d'exécution :

Réf	Technicien	Bref description	Dates
1	Aymeric P	Création du document	08/01/25
2	Aymeric P	Réalisation de l'étude comparatif	08/01/25
3			
4			

Relecture et validation :

	Nom	Dates	Note	Check
Auteur	Aymeric P			OK
Relecteur				
Validation				

Table des matières

1. Introduction

La sécurité des réseaux Wi-Fi est essentielle pour garantir la confidentialité et l'intégrité des données transmises. L'absence ou le choix inadéquat d'un protocole de sécurité peut exposer les utilisateurs à des cyberattaques telles que l'écoute clandestine, le piratage ou les attaques de déni de service. Cette étude détaille les principaux protocoles de sécurité Wi-Fi (WEP, WPA, WPA2 et WPA3), leurs spécifications, leurs forces et leurs faiblesses, afin de guider les administrateurs réseau dans leur choix.

2. Les protocoles de sécurité Wi-Fi

a) WEP (Wired Equivalent Privacy)

Introduction :
WEP est le premier standard de sécurité Wi-Fi, introduit en 1999 pour protéger les transmissions sans fil. Il se base sur le chiffrement pour offrir une confidentialité similaire à celle des réseaux câblés.

Caractéristiques :

- Utilisation de l'algorithme RC4 pour le chiffrement.
- Clés statiques de 64 ou 128 bits.
- Basé sur un vecteur d'initialisation (IV) pour générer des clés dynamiques, bien que ce processus ait des failles.

Avantages :

- Simplicité de configuration.
- Compatible avec les équipements Wi-Fi les plus anciens.

Limitations :

- **Sécurité faible :** La taille limitée des clés et l'utilisation répétée des vecteurs d'initialisation permettent aux attaquants de casser la clé en quelques minutes.

- **Vulnérabilité aux attaques de rejeu :** Un attaquant peut réutiliser des paquets interceptés pour accéder au réseau.
- Considéré comme obsolète depuis 2004.

Exemple d'attaque : Un pirate utilisant un outil comme Aircrack-ng peut facilement capturer les paquets Wi-Fi pour découvrir la clé WEP.

b) WPA (Wi-Fi Protected Access)

Introduction :
WPA a été introduit en 2003 pour combler les lacunes de WEP tout en maintenant la compatibilité avec les anciens matériels.

Caractéristiques :

- Utilisation du protocole TKIP (Temporal Key Integrity Protocol), qui améliore la gestion des clés.
- Ajout d'un mécanisme de contrôle d'intégrité des messages pour détecter les modifications non autorisées.
- Toujours basé sur l'algorithme RC4 pour des raisons de compatibilité.

Avantages :

- Transition facile depuis WEP grâce à une compatibilité ascendante.
- Clés de chiffrement générées dynamiquement, réduisant les risques de réutilisation.

Limitations :

- TKIP est vulnérable aux attaques ciblées, bien qu'il soit plus sécurisé que WEP.
- Faible robustesse contre les attaques par dictionnaire sur les mots de passe faibles.

Cas d'utilisation : WPA est utilisé dans les environnements nécessitant une transition rapide depuis WEP, mais il est recommandé de migrer vers WPA2 ou WPA3.

c) WPA2 (Wi-Fi Protected Access II)

Introduction :
Adopté comme standard en 2004, WPA2 améliore considérablement la sécurité en abandonnant TKIP au profit de l'AES (Advanced Encryption Standard).

Caractéristiques :

- Chiffrement AES avec des clés de 128 bits ou plus.
- Mode CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) pour l'intégrité des données.
- Support de l'EAP (Extensible Authentication Protocol), permettant des méthodes d'authentification avancées.

Avantages :

- Sécurité élevée et robustesse contre les attaques connues.
- Large adoption dans les réseaux domestiques et professionnels.

Limitations :

- Vulnérabilité à l'attaque KRACK (Key Reinstallation Attack), qui exploite une faille dans le protocole d'établissement des clés.
- Nécessite des équipements compatibles pour bénéficier de toutes ses fonctionnalités.

Cas d'utilisation : WPA2 est recommandé pour les réseaux nécessitant un compromis entre sécurité, compatibilité et performance.

d) WPA3 (Wi-Fi Protected Access III)

Introduction :
Lancé en 2018, WPA3 est le protocole de sécurité Wi-Fi le plus récent, conçu pour répondre aux menaces modernes et simplifier l'expérience utilisateur.

Caractéristiques :

- Utilisation de SAE (Simultaneous Authentication of Equals) pour éliminer les vulnérabilités aux attaques par dictionnaire.
- Chiffrement opportuniste pour les réseaux publics (Wi-Fi Enhanced Open).

- Fonctionnalités de protection IoT via Easy Connect.

Avantages :

- Protection renforcée contre les attaques par force brute et par dictionnaire.
- Sécurisation des connexions Wi-Fi publiques grâce au chiffrement individuel des sessions.
- Approprié pour les environnements où la confidentialité est cruciale.

Limitations :

- Requiert des équipements compatibles, limitant son adoption dans les réseaux utilisant des appareils plus anciens.
- Coût potentiellement élevé pour la mise à niveau des infrastructures.

3. Comparaison des protocoles

Voici un tableau comparatif des protocoles de sécurité Wi-Fi :

Protocole	**Niveau de sécurité**	**Chiffrement utilisé**	**Compatibilité**	**Limites principales**
WEP	Faible	RC4	Équipements anciens	Failles de sécurité importantes
WPA	Moyenne	TKIP	Transition WEP	Sensible aux attaques par dictionnaire
WPA2	Élevée	AES	Large adoption	Attaque KRACK
WPA3	Très élevée	AES avec SAE	Appareils récents	Nécessite des équipements modernes

4. Conclusion

En fonction de vos besoins et des équipements disponibles :

- **WPA3** est le choix privilégié pour les environnements modernes nécessitant une sécurité optimale.

- **WPA2** reste une solution viable dans les cas où la compatibilité est une priorité.
- **WPA et WEP** ne sont plus recommandés et devraient être évités.

La transition vers WPA3 doit être planifiée pour garantir une protection efficace contre les menaces actuelles.