



PROJET ASSURMER

AUTEURS :

DE CARVALHO LOPES Bruno
BELAHA Sidahmed
LE CLAINCHE Killian

DATE :

07/01/2025

2024

Sommaire

Etude comparative des différents protocoles de sécurité wifi	3
Introduction	3
Protocoles de sécurité Wi-Fi analysés	3
Critères de comparaison	3

Etude comparative des différents protocoles de sécurité wifi

Introduction

Le Wi-Fi est une technologie omniprésente qui connecte des milliards d'appareils dans le monde. Cependant, sa nature sans fil l'expose à des risques importants, notamment :

- **Intrusions non autorisées** : Accès à un réseau par des attaquants non légitimes.
- **Vol de données** : Interception des communications entre un appareil et le point d'accès.
- **Déni de service (DoS)** : Saturation du réseau par des attaquants.

Cette étude vise à analyser et comparer les principaux protocoles de sécurité Wi-Fi pour identifier les options les plus adaptées selon les besoins spécifiques.

Protocoles de sécurité Wi-Fi analysés

Les protocoles Wi-Fi ont évolué au fil des ans pour répondre aux nouvelles menaces :

1. **WEP (Wired Equivalent Privacy)** : Premier protocole standardisé pour la sécurité des réseaux Wi-Fi.
2. **WPA (Wi-Fi Protected Access)** : Une solution transitoire pour corriger les failles de WEP.
3. **WPA2 (Wi-Fi Protected Access 2)** : Une amélioration majeure apportant des algorithmes de chiffrement robustes.
4. **WPA3 (Wi-Fi Protected Access 3)** : Le protocole actuel, conçu pour offrir une sécurité avancée adaptée aux nouveaux usages.

Critères de comparaison

Voici les critères d'analyse retenus pour cette étude :

1. **Chiffrement et authentification** : Algorithmes et processus utilisés pour sécuriser les données.
2. **Vulnérabilités connues** : Failles d'exploitation publiées ou détectées.
3. **Performance** : Impact sur les ressources matérielles et la vitesse de transmission.
4. **Compatibilité** : Prise en charge par les appareils récents et anciens.
5. **Facilité de mise en œuvre** : Simplicité pour les utilisateurs finaux ou les administrateurs.
6. **Cas d'utilisation recommandé** : Contextes où le protocole est le plus pertinent.