Laboratoire WiFi

Sécurité sans fil, vulnérabilités majeures et expérimentations

Projet de Mastère Spécialisé Cybersécurité
Télécom SudParis

Auteurs : Tanguy HUE
Clément LEPRETTRE

Encadrant : Olivier PAUL

27 novembre 2025

Résumé

Ce rapport présente un état de l'art complet de la sécurité des réseaux WiFi contemporains, une analyse détaillée des vulnérabilités majeures encore exploitables ainsi qu'une mise en pratique expérimentale basée sur un environnement virtualisé.

Mots-clés : WiFi, WPA2, WPA3, cybersécurité, attaques réseau

Table des matières

1 Introduction

Les réseaux Wi-Fi sont devenus un élément incontournable des infrastructures numériques modernes. Que ce soit dans les environnements personnels, professionnels ou industriels, ils assurent une connectivité permanente et flexible, mais exposent également les systèmes à des risques spécifiques liés à la nature même des communications sans fil. Contrairement aux réseaux filaires, un réseau Wi-Fi dépasse toujours les limites physiques du bâtiment ou de l'organisation qui l'utilise, ce qui permet à un attaquant de s'y connecter ou de l'observer sans jamais avoir à pénétrer physiquement dans les locaux. Cette caractéristique en fait une cible privilégiée et un vecteur d'attaque largement exploité.

Les mécanismes de sécurité Wi-Fi ont pourtant beaucoup évolué au fil des années. Après les faiblesses majeures de WEP et les limites de WPA, WPA2 a longtemps été considéré comme un standard robuste, jusqu'à l'apparition d'attaques protocolaires comme KRACK. Plus récemment, WPA3 a introduit de nouveaux mécanismes destinés à renforcer l'authentification et la confidentialité, mais même cette version moderne a connu ses premières vulnérabilités dès sa diffusion. Cette succession d'avancées et de contournements montre que la sécurité Wi-Fi est un domaine en évolution constante, dans lequel chaque amélioration technique entraîne l'apparition de nouvelles attaques ciblées.

Malgré les améliorations successives des protocoles et l'apparition de WPA3, les réseaux Wi-Fi restent vulnérables. Beaucoup d'équipements utilisent encore des standards anciens ou sont configurés avec des options de rétrocompatibilité qui affaiblissent la sécurité. Les implémentations varient d'un constructeur à l'autre, certaines protections dépendent du comportement du client, et les attaques théoriques se révèlent parfois très simples à reproduire en pratique. La problématique centrale de ce travail est donc de comprendre quelles attaques restent réellement efficaces aujourd'hui, comment elles peuvent être mises en œuvre dans un environnement réaliste, et quelles implications elles ont sur la sécurité globale d'un réseau Wi-Fi.

Dans ce contexte, ce projet s'intéresse à la compréhension des principales failles affectant les réseaux Wi-Fi actuels et à l'analyse des attaques réellement exploitables sur le terrain. Il s'agit d'étudier comment un attaquant peut contourner les protections en place, quelles conditions pratiques rendent ces attaques possibles, et quelles sont leurs conséquences concrètes sur la confidentialité, l'intégrité et la disponibilité des communications. L'objectif n'est pas uniquement théorique : il s'agit de reproduire ces attaques dans un environnement maîtrisé afin d'observer leur fonctionnement, d'en comprendre les mécanismes internes et d'évaluer leur pertinence vis-à-vis des architectures modernes.

2 Objectifs du projet

2.1 Objectif général

Étudier, analyser et reproduire des attaques WiFi représentatives de la menace actuelle.

2.2 Objectifs spécifiques

— Mettre en place un laboratoire WiFi complet (Kali + AP + VM Windows).
— Reproduire des attaques WiFi.
— Capturer, analyser et expliquer les traces réseau.
— Évaluer les conséquences et proposer des contre-mesures.

3 Fonctionnement des Protocoles Wi-Fi

La sécurité des réseaux Wi-Fi repose sur une succession de mécanismes cryptographiques introduits progressivement pour corriger les vulnérabilités de leurs prédécesseurs. Depuis WEP en 1997 jusqu'à WPA3 en 2018, chaque protocole a apporté des évolutions majeures : nouveaux algorithmes, nouvelles primitives cryptographiques, mécanismes d'intégrité plus robustes, protection des trames de gestion, et résistance accrue aux attaques hors ligne. Cette section propose une analyse approfondie de ces mécanismes, de leur logique interne, de leurs limites, ainsi que des structures de trames qu'ils manipulent.

3.1 WEP : Wired Equivalent Privacy

WEP (1997) constitue la première tentative de sécuriser les communications Wi-Fi. Il a été conçu à une époque où la cryptographie grand public était encore émergente, et souffre aujourd'hui de nombreuses limitations structurelles. Son objectif était de fournir une confidentialité comparable à celle d'un réseau filaire, mais son architecture s'est révélée profondément vulnérable.

Fonctionnement interne

WEP repose sur l'algorithme de chiffrement par flot RC4. Le mécanisme de chiffrement est simple :

— une clé secrète partagée statique (40 ou 104 bits) ;
— un vecteur d'initialisation (IV) de 24 bits, envoyé en clair ;
— concaténation `IV || clé` comme entrée du KSA de RC4 ;
— un ICV (Integrity Check Value) calculé via CRC-32, ajouté au plaintext avant chiffrement.

Le chiffrement d'un paquet se fait ainsi :

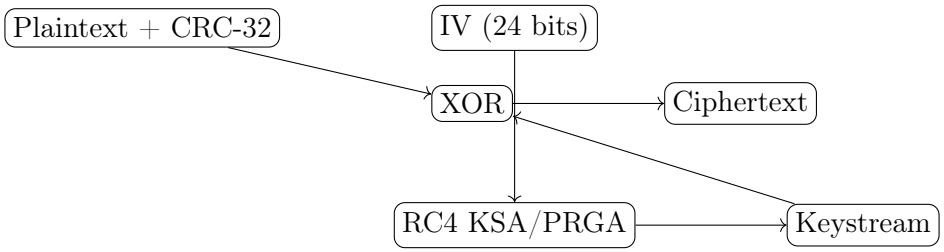

FIGURE 1 – Principe du chiffrement WEP

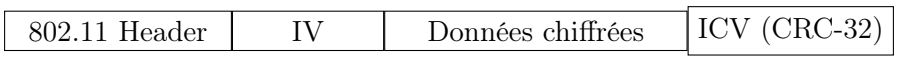

FIGURE 2 – Format d'une trame WEP

Format d'une trame WEP

Faiblesses cryptographiques majeures

— IV de 24 bits : collisions quasi certaines en quelques minutes.
— RC4 présente des biais initiaux exploités par les attaques FMS, KoreK et PTW.
— CRC-32 n'est pas une fonction d'intégrité cryptographique : vulnérable au bit-flipping.
— Pas de renouvellement de clé : longue exposition.

Ces vulnérabilités rendent WEP totalement compromis : casser une clé WEP prend moins d'une minute dans des conditions favorables.

3.2 WPA : Wi-Fi Protected Access

Face à la crise WEP, la Wi-Fi Alliance introduit en 2003 WPA comme correctif transitoire, visant à remplacer les composants vulnérables tout en conservant le matériel existant (compatibilité ascendante).

Fonctionnement interne

WPA introduit plusieurs mécanismes :
— un mélange de clés élaboré (phase 1 et phase 2) ;
— un compteur TSC (TKIP Sequence Counter) antipiratage ;
— un MIC (Message Integrity Code) ;
— une rotation des clés fréquente.
Bien que RC4 soit toujours utilisé, WPA réduit significativement les risques d'attaque sans néanmoins les éliminer.

3.3 WPA2 : AES-CCMP et le 4-Way Handshake

WPA2 apporte une amélioration profonde : l'abandon de RC4 au profit d'un chiffrement moderne AES-CCMP.

Modes d'authentification

— **WPA2-PSK** : la PMK = PBKDF2(passphrase, SSID).
— **WPA2-Enterprise** : PMK fournie via un serveur RADIUS et une authentification EAP.

Le 4-Way Handshake

Le handshake assure :
— la preuve de possession mutuelle de la PMK ;
— la génération de la PTK ;
— la distribution de la GTK.

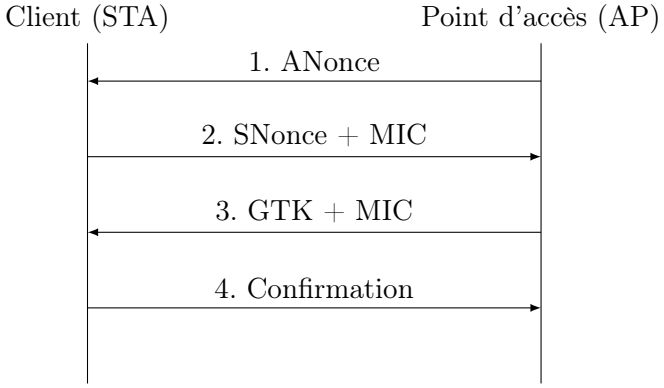

FIGURE 3 – 4-Way Handshake WPA/WPA2

3.4 Dérivation des clés : PMK, PTK et GTK

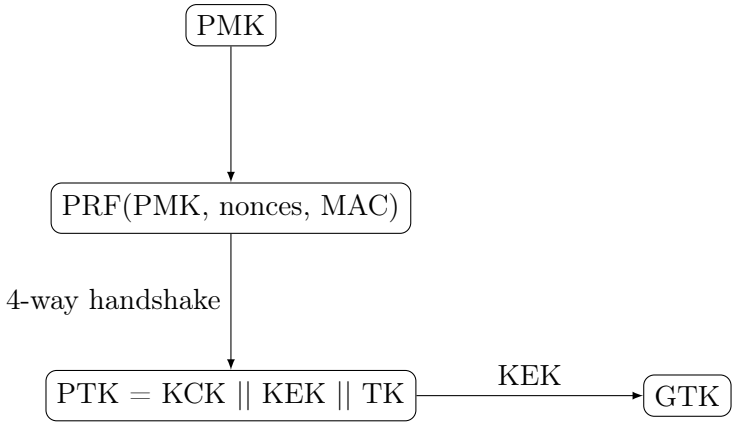

FIGURE 4 – Dérivation cryptographique PMK → PTK → GTK

Format d'une trame CCMP (WPA2)

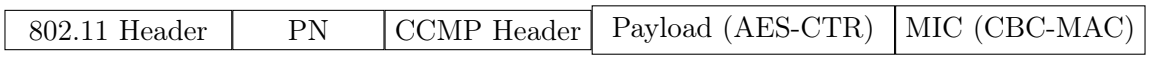

FIGURE 5 – Structure d'une trame CCMP

3.5 WPA3 : SAE, Dragonfly, GCMP et PMF

WPA3 corrige des failles structurelles de WPA2, notamment KRACK, en introduisant SAE (Dragonfly), OWE, PMF obligatoire, et le support obligatoire de GCMP dans certaines suites.

Handshake SAE (Dragonfly)

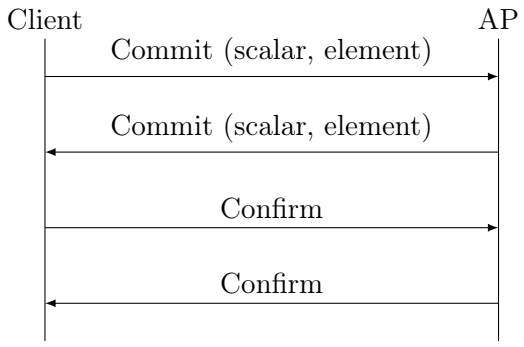

FIGURE 6 – Handshake SAE (WPA3)

3.6 Mécanismes cryptographiques avancés

Les protocoles de sécurité modernes du Wi-Fi reposent sur des mécanismes cryptographiques plus élaborés que ceux utilisés par les générations précédentes. Contrairement à WEP et TKIP, qui n'offraient qu'une protection minimale contre l'écoute, l'injection ou la manipulation des trames, WPA2 et surtout WPA3 reposent sur des constructions cryptographiques complètes, conçues pour

fournir à la fois confidentialité, intégrité, résistance aux attaques par rejeu et garanties formelles sur la sécurité de la session. Trois mécanismes occupent une place centrale : AES-CCMP, GCMP et SAE (aussi appelé Dragonfly). Ces primitives ne jouent pas le même rôle, mais constituent ensemble la base de la sécurité Wi-Fi contemporaine.

3.6.1 AES-CCMP

AES-CCMP est devenu la norme de chiffrement par défaut avec WPA2. Son objectif est d'aller bien au-delà du simple masquage des données transportées : il assure simultanément la confidentialité des informations, l'intégrité des trames et la protection contre les attaques par rejeu.

Pour y parvenir, CCMP combine deux éléments complémentaires. D'une part, il utilise AES en mode compteur (CTR) pour le chiffrement. Ce mode transforme le bloc AES en générateur de flot chiffrant, permettant de chiffrer efficacement des paquets de taille variable sans introduire de structure exploitable. De l'autre, CCMP associe ce chiffrement à un code d'authentification basé sur CBC-MAC, un mécanisme cryptographique destiné à garantir que les données n'ont subi aucune altération. Cette combinaison forme une construction dite *AEAD* (Authenticated Encryption with Associated Data), dans laquelle confidentialité et intégrité sont assurées simultanément par une même clé, ce qui évite un grand nombre de vulnérabilités présentes dans les générations antérieures.

L'ensemble repose également sur un numéro de paquet (Packet Number, PN) utilisé comme nonce unique. Toute réutilisation est interdite, ce qui empêche un attaquant de rejouer ou de réinjecter des trames chiffrées. En pratique, AES-CCMP constitue encore aujourd'hui une référence en matière de chiffrement pour les réseaux Wi-Fi.

AES-CCMP combine :

— AES en mode CTR pour le chiffrement ;

— CBC-MAC pour l'intégrité (authentification).

C'est une construction AEAD robuste, largement testée.

3.6.2 GCMP (AES-GCM)

GCMP, introduit avec les standards 802.11ac et repris dans WPA3-Enterprise, reprend les principes d'AES-CCMP mais s'appuie cette fois sur AES-GCM. Cette construction fait partie des modes de chiffrement AEAD les plus étudiés et les plus robustes. AES-GCM associe un chiffrement en mode CTR à la fonction d'authentification GHASH, reposant sur des opérations arithmétiques dans un corps de Galois. Cette approche permet de calculer l'intégrité et le chiffrement de façon quasi parallèle, ce qui rend GCMP particulièrement performant sur les architectures modernes.

L'intérêt principal de GCMP réside donc dans sa rapidité : il offre un débit supérieur à CCMP, ce qui le rend bien adapté aux environnements à forte charge ou aux réseaux professionnels nécessitant des débits élevés. Il reste néanmoins sensible aux erreurs d'implémentation, comme l'ont montré certaines variantes des attaques Dragonblood qui ciblaient directement GCMP-128 lorsque les nonces n'étaient pas utilisés correctement. Malgré cela, GCMP demeure une brique cryptographique robuste lorsqu'il est correctement mis en œuvre.

3.6.3 SAE / Dragonfly

Contrairement à AES-CCMP et à GCMP, qui sont des mécanismes de chiffrement et d'intégrité utilisés *après* l'établissement de la connexion, SAE (Simultaneous Authentication of Equals) intervient au moment de l'authentification. SAE n'est pas un algorithme de chiffrement mais un protocole d'échange de clés sécurisé, faisant partie de la famille des PAKE (Password-Authenticated Key Exchange).

L'enjeu de SAE est de résoudre l'un des problèmes fondamentaux des versions antérieures : avec WPA2-PSK, un attaquant pouvait capturer un 4-Way Handshake puis tenter hors ligne de retrouver le mot de passe par dictionnaire. Dans SAE, ce type d'attaque est impossible. Le protocole s'appuie sur un échange Diffie–Hellman (sur groupes modp ou courbes elliptiques), dans lequel le mot de passe n'est jamais transmis ni dérivé sous forme exploitable. Chaque tentative d'authentification nécessite une interaction en temps réel avec le point d'accès, ce qui empêche les attaques hors ligne et limite naturellement la vitesse des tests possibles.

SAE offre également la propriété de *Forward Secrecy* : même si un mot de passe venait à être compromis ultérieurement, les sessions passées resteraient inexploitables, car la clé de session résulte d'un secret éphémère renouvelé à chaque connexion. Cette approche corrige l'une des failles conceptuelles les plus importantes de WPA2 et constitue la principale amélioration de WPA3-Personal.

Pour résumer, ses caractériques principales sont les suivantes :

— s'appuie sur Diffie-Hellman (modp ou ECC) ;
— offre Forward Secrecy ;
— empêche les attaques hors-ligne ;
— protège contre attaques dictionnaires massives.

Format d'une trame GCMP

Figure 7 – Structure d'une trame GCMP (WPA3)

3.7 Synthèse comparative approfondie

Protocole	Crypto	Auth	Intégrité	Résistance
WEP	RC4	Clé statique	CRC-32	Nulle
WPA	RC4	PSK	MIC	Faible
WPA2	AES-CCMP	PSK/802.1X	CBC-MAC	Forte (hors KRACK)
WPA3	AES-CCMP/GCMP	SAE/802.1X	PMF	Très forte
OWE	Diffie-Hellman	Aucune	CCMP/GCMP	Élevée

Table 1 – Comparaison des protocoles de sécurité Wi-Fi

4 État de l'art sur la sécurité Wi-Fi

La surface d'attaque des réseaux Wi-Fi n'a cessé d'évoluer depuis 1997. Les vulnérabilités historiques et contemporaines exploitent indifféremment : les faiblesses cryptographiques intrinsèques, les défauts d'implémentation, les erreurs de configuration, et les mécanismes d'interaction entre utilisateurs et points d'accès. Cet état de l'art se concentre exclusivement sur les **attaques**, désormais que les protocoles ont été décrits dans la section précédente, et présente une analyse détaillée des vecteurs connus, de leur fonctionnement interne et de leur pertinence actuelle.

4.1 Évolution historique des attaques contre les réseaux Wi-Fi

L'évolution des attaques Wi-Fi suit logiquement celle des protocoles eux-mêmes. Chaque nouvelle protection a donné naissance à un nouveau type d'attaque : statistiques pour WEP, cryptanalytiques pour WPA, protocolaires pour WPA2 et side-channels pour WPA3.

5 Méthodologie

5.1 Environnement expérimental

— Hôte Windows + VirtualBox
— VM Kali Linux avec carte WiFi compatible monitor/injection
— VM Lubuntu configurée en point d'accès WiFi

6 Attaques WiFi étudiées et reproduites

7 Conclusion

Références

Annexes

A Captures Wireshark

B Scripts utilisés