Laboratoire Wi-Fi

Sécurité sans fil, vulnérabilités majeures et expérimentations

Projet de Mastère Spécialisé Cybersécurité
Télécom SudParis

Auteurs : Tanguy HUE
Clément LEPRETTRE

Encadrant : Olivier PAUL

7 janvier 2026

Résumé

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

Mots-clés : Wi-Fi, WPA / WPA2, WPA3, cybersécurité, attaques réseau

Table des matières

Table des figures

Liste des acronymes

AP Access Point. 3, 7–11, 13, 14

BSSID Basic Service set identifier. 3, 8

FAI Fournisseurs d'accès à Internet. 9

GTK Group Temporal Key. 9, 14

ICV Integrity Check Value. 11, 12
IV Initialization Vector. 11, 13

KCK Key Confirmation Key. 13, 14
KEK Key Encryption Key. 14

MIC Message Integrity Code. 13–15

PBKDF2 Password-Based Key Derivation Function 2. 13
PMK Pairwise Master Key. 9, 13
PRF Pseudorandom function family. 14
PSK Pre-Shared Key. 13
PTK Pairwise Transient Key. 9, 13, 14

RC4 Rivest Cipher 4. 11

SSID Service set identifier. 3, 8, 9
STA Station. 3, 8, 9, 13, 14

TK Temporal Key. 14
TKIP Temporal Key Integrity Protocol. 13
TSC TKIP Sequence Counter. 13, 15

WEP Wired Equivalent Privacy. 6, 8, 11
Wi-Fi Wireless Fidelity. 6, 7
WPA Wi-Fi Protected Access. 6, 13
WPA2 Wi-Fi Protected Access 2. 6
WPA3 Wi-Fi Protected Access 3. 6, 8

Glossaire

ANonce Authenticator Nonce : nombre aléatoire de 32 octets généré par le point d'accès lors du 4-Way Handshake pour créer la PTK. 13, 14, 16

concentrateur Équipement réseau de niveau 2, utilisé pour faire de la redirection de trame. 9

handshake Échange de messages pour authentifier et établir les clés de chiffrement. 9, 13, 14

SNonce Supplicant Nonce : nombre aléatoire de 32 octets généré par la station lors du 4-Way Handshake pour créer la PTK. 13, 14

trame Unité de données de la couche 2 transportant informations de gestion, contrôle ou données utilisateur. 8, 11

1 Introduction

Les réseaux Wireless Fidelity (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 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 Wi-Fi représentatives de la menace actuelle.

2.2 Objectifs spécifiques

— Mettre en place un laboratoire Wi-Fi complet (Kali + AP + VM Windows).
— Reproduire des attaques Wi-Fi.
— 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 principes cryptographiques, mécanismes d'intégrité plus robustes, protection des trames de gestion, et résistance 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 Principe général du Wi-Fi

Le Wi-Fi, ou norme IEEE 802.11, désigne un ensemble de standards pour les réseaux locaux sans fil (WLAN) permettant la transmission de données numériques par ondes radio (principalement 2,4 GHz, 5 GHz et 6 GHz). Développé à partir des années 1990 par le comité IEEE 802.11 pour répondre à la demande croissante de connectivité mobile sans câblage Ethernet, le premier standard a été publié en 1997, révolutionnant l'accès aux données en éliminant les contraintes physiques des réseaux filaires.

Aujourd'hui, le Wi-Fi est omniprésent : hotspots publics (cafés, aéroports, transports), entreprises, foyers. Avec Wi-Fi 7 (802.11be, 2024) et au-delà, il supporte des débits >46 Gbit/s.

Définitions générales Wi-Fi

Avant d'aborder en détail le fonctionnement des différents protocoles de sécurité, il est utile de préciser brièvement certains termes fondamentaux du Wi-Fi. Le **Service set identifier (SSID)** correspond au nom d'un réseau et permet aux dispositifs de l'identifier lors de la phase de découverte. Le **Basic Service set identifier (BSSID)**, quant à lui, désigne l'adresse MAC unique du point d'accès assurant la diffusion du réseau. Le terme **Access Point (AP)** désigne ce même point d'accès, tandis que la **Station (STA)** représente tout client Wi-Fi, qu'il s'agisse d'un ordinateur, d'un smartphone ou d'un objet connecté.

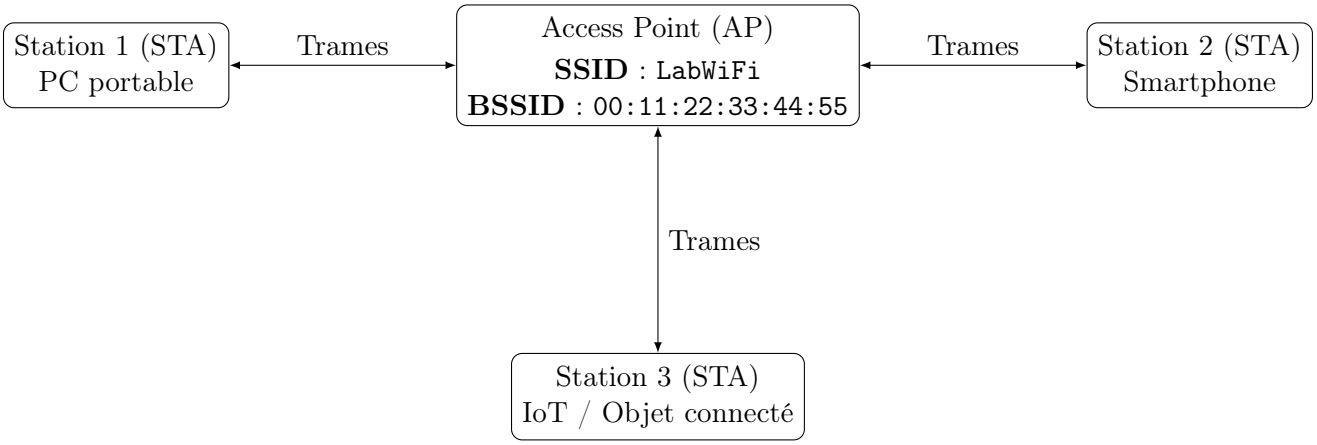

FIGURE 1 – Illustration des notions AP, STA, SSID et BSSID dans un réseau Wi-Fi

Les communications Wi-Fi reposent sur des trames qui circulent au niveau de la couche MAC du modèle 802.11. On distingue notamment les trames de *gestion*, essentielles pour l'association, l'authentification ou la déconnexion ; les trames de *contrôle*, destinées à réguler l'accès au médium ;

et les trames de *données*, qui transportent l'information utilisateur ou les paquets réseau encapsulés. La plupart des attaques Wi-Fi tirent parti de la possibilité d'observer, d'injecter ou de manipuler ces différentes catégories de trames.

Enfin, plusieurs notions cryptographiques apparaissent régulièrement dans ce chapitre. La **Pairwise Master Key (PMK)** constitue le secret partagé à partir duquel toutes les clés de session sont dérivées, tandis que la **Pairwise Transient Key (PTK)** correspond à la clé spécifique à la connexion entre un client et un point d'accès. La **Group Temporal Key (GTK)** est utilisée pour chiffrer le trafic multicast ou broadcast adressé à plusieurs stations. Ces clés sont produites ou échangées dans le cadre de mécanismes tel que le 4-Way Handshake, qui sera détaillé dans les sections suivantes.

Ces notions constituent le socle indispensable à la compréhension des protocoles de sécurisation Wi-Fi et des vulnérabilités qu'ils cherchent à prévenir.

Modes de mise en réseau [1]

Le Wi-Fi supporte plusieurs modes de mise en réseau, adaptés à des usages variés.

Mode Infrastructure Ce mode connecte les stations (STA) via un ou plusieurs points d'accès (AP) qui agissent comme des concentrateurs. Initialement utilisé en entreprise pour poser des bornes à intervalles réguliers, il nécessite un SSID commun pour la communication. L'avantage principal est le contrôle centralisé des accès : passage obligatoire par l'AP. Aujourd'hui, les routeurs fournis par les FAI aux particuliers fonctionnent en mode infrastructure, faciles à configurer.

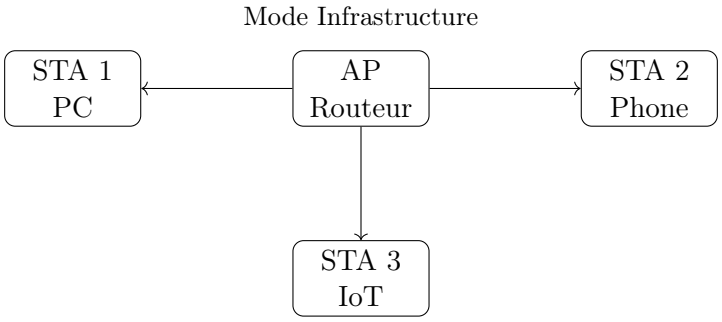

FIGURE 2 – Mode Infrastructure : STA → AP central → Internet

Mode Ad hoc Ce mode permet une connexion directe entre stations sans point d'accès intermédiaire. Idéal pour des échanges rapides (fichiers entre portables dans un train ou un café), il repose sur un SSID, un canal et une clé de chiffrement communs. Des protocoles de routage dynamique étendent la portée en mode maillé, où chaque nœud route pour les autres.

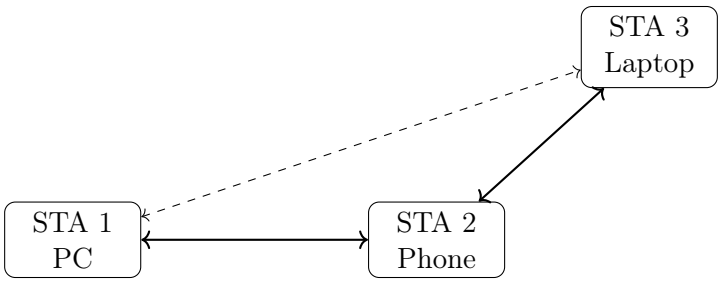

FIGURE 3 – Mode Ad hoc : communication directe sans AP

Mode Pont (Bridge) Un AP en mode pont relie d'autres AP pour étendre un réseau filaire (ex. : entre bâtiments) au niveau couche 2 OSI. Un AP racine distribue l'accès Internet, les autres se connectent en mode bridge et peuvent accueillir des clients comme en infrastructure.

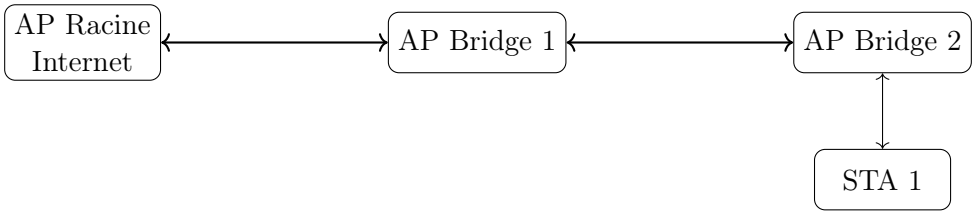

FIGURE 4 – Mode Pont : extension réseau filaire via APs

Mode Répéteur (Range-extender) Ce mode étend la couverture en répétant le signal (ex. : fond de couloir). L'interface Ethernet reste inactive, mais chaque saut augmente la latence et divise le débit par deux (réception + retransmission sur la même antenne).

FIGURE 5 – Mode Répéteur : extension portée (débit /2, +latence)

Mode	**Lien principal**	**Ethernet**	**Usage**
Infrastructure	STA → AP	✓	Internet
Ad hoc	STA ↔ STA	✗	Échange direct
Pont	AP ↔ AP (câble)	✓	Relier bâtiments
Répéteur	WiFi répété	✗	Étendre portée

TABLE 1 – Modes Wi-Fi : synthèse

Ces modes fondamentaux conditionnent les mécanismes de sécurité analysés dans la suite, particulièrement en mode infrastructure dominant.

3.2 Sécurité Wi-Fi

3.2.1 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. Son objectif était de fournir une confidentialité comparable à celle d'un réseau filaire, mais son fonctionnement 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, nommée SharedKey (40 ou 104 bits) ;
- un Initialization Vector (IV) de 24 bits, envoyé en clair ;
- concaténation `IV || clé` comme entrée de RC4 ;
- un Integrity Check Value (ICV) calculé via CRC-32, ajouté au plaintext (*texte en clair*) avant chiffrement.

Le chiffrement d'un paquet se fait ainsi :

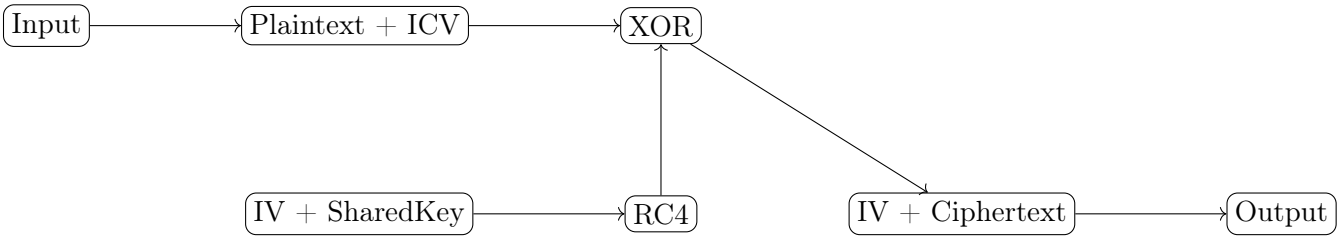

FIGURE 6 – Principe du chiffrement WEP

Format d'une trame WEP

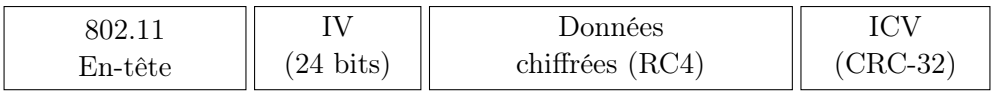

FIGURE 7 – Format d'une trame WEP

Faiblesses cryptographiques majeures Le protocole WEP présente des faiblesses structurelles fondamentales :

- **IV de 24 bits (16 777 216 valeurs possibles)** : chaque trame WEP transmet son vecteur d'initialisation en clair. Avec un trafic normal, les collisions d'IV surviennent en quelques minutes (souvent moins de 5 minutes pour un AP actif). Un attaquant peut alors combiner deux trames avec le même IV+clé pour annuler le keystream par XOR.
- **Aucun renouvellement de clé** : la clé secrète reste statique pendant des semaines/mois. Un IV réutilisé expose la même clé RC4 pendant toute la durée de vie de la clé, permettant une attaque par collecte massive de trames.
- **ICV trop faible** : L'ICV s'appuie sur un algorithme peu robuste, il est possible de modifier des trames chiffrées sans connaître la clé, en recalculant un ICV valide.

Pour mieux comprendre le problème majeur de la taille de l'IV, nous allons prendre comme exemple : un IV est utilisé 2 fois IV_0, et deux messages combinés (données | ICV) M_1 et M_2.

1. $IV_0 \rightarrow RC4(IV_0||SharedKey) \oplus M_1 = C_1$
2. $IV_0 \rightarrow RC4(IV_0||SharedKey) \oplus M_2 = C_2$
3. $C_1 \oplus C_2 = M_1 \oplus M_2$
4. En-têtes IP (IP/TCP standardardisé) connus de $M_1 \rightarrow M_2$ instantané

En pratique, avec Aircrack NG, William Arbaugh note qu'il existe 50 % de risque de collision après 4 823 paquets. [2] La documentation conseille elle 250,000 IVs pour des clés de 64 bit et 1,500,000 IVs pour des clés de 128 bit. [3]

3.2.2 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). WPA s'appuie sur un problème de chiffrement nommé Temporal Key Integrity Protocol (TKIP).

Fonctionnement interne

WPA introduit plusieurs mécanismes :
— un mélange de clés élaboré (phase 1 et phase 2) ;
— un Initialization Vector de taille doublée (24 à 48 bits) ;
— un TKIP Sequence Counter (TSC) pour de l'anti-replay ;
— un Message Integrity Code (MIC) pour de l'intégrité et de la signature ;
— une rotation des clés fréquente.

Phases de WPA

Le protocole s'appuie sur une clé connue (appelée passphrase) par les STA et l'AP, nommée Pre-Shared Key (PSK). Il peut également, dans le cadre de *WPA-Enterprise*, être généré via un serveur RADIUS. Ici, nous ne développerons que la méthode avec une passphrase connue par les deux parties.

WPA corrige WEP par 3 étapes distinctes :

— **Phase 1 (PBKDF2 4096 itérations)** : passphrase → Pairwise Master Key (PMK) résistante plus robuste. Cette clé n'est jamais utilisée directement, elle ne sert qu'à générer une clé temporaire.
La fonction PBKDF2 utilise le SSID comme sel cryptographique et applique 4096 itérations de HMAC-SHA1. Ce mécanisme ralentit volontairement les tentatives de brute force, mais n'empêche pas les attaques hors ligne si la passphrase est faible et que le 4-Way Handshake est capturé.

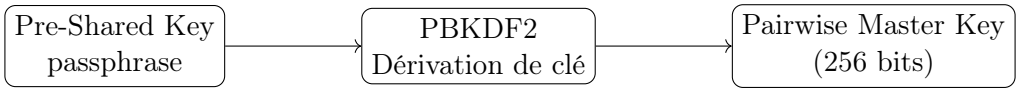

FIGURE 8 – Phase 1 : Sécurisation de la clé

— **Phase 2 (4-Way Handshake)** : PMK → PTK échangée sans jamais transmettre la clé (ANonce/SNonce + MIC protègent).
Les nonces (ANonce, générée par l'AP et SNonce, générée par la STA) garantissent l'unicité de la PTK à chaque association, même si la PMK reste identique. Le MIC, calculé à l'aide de la clé Key Confirmation Key (KCK), assure l'intégrité et l'authenticité des messages du handshake.

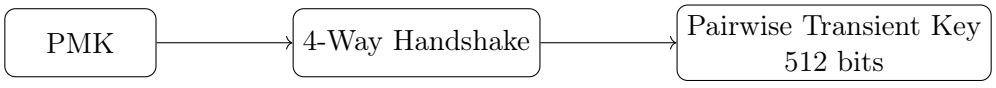

FIGURE 9 – Phase 2 : Création d'une clé unique en AP et STA

Le **4-Way Handshake** assure 3 objectifs critiques :

— **Preuve mutuelle PMK** : STA et AP prouvent qu'ils connaissent la même PMK sans jamais la transmettre.
— **PTK (Pairwise Transient Key, 512 bits)** : clé unique unicast STA ↔ AP. Utilise une Pseudorandom function family (PRF), pour faire cette dérivation :

$$PTK = PRF(PMK, \min(MAC_{AP}, MAC_{STA}) \,||\, \max(MAC_{AP}, MAC_{STA}) \,||\, \min(ANonce, SNonce) \,||\, \max(ANonce, SNonce))$$

.
— **GTK (Group Temporal Key)** : clé broadcast/multicast partagée par TOUS les clients du réseau (trafic groupe). L'AP l'envoie chiffrée avec la PTK du client.

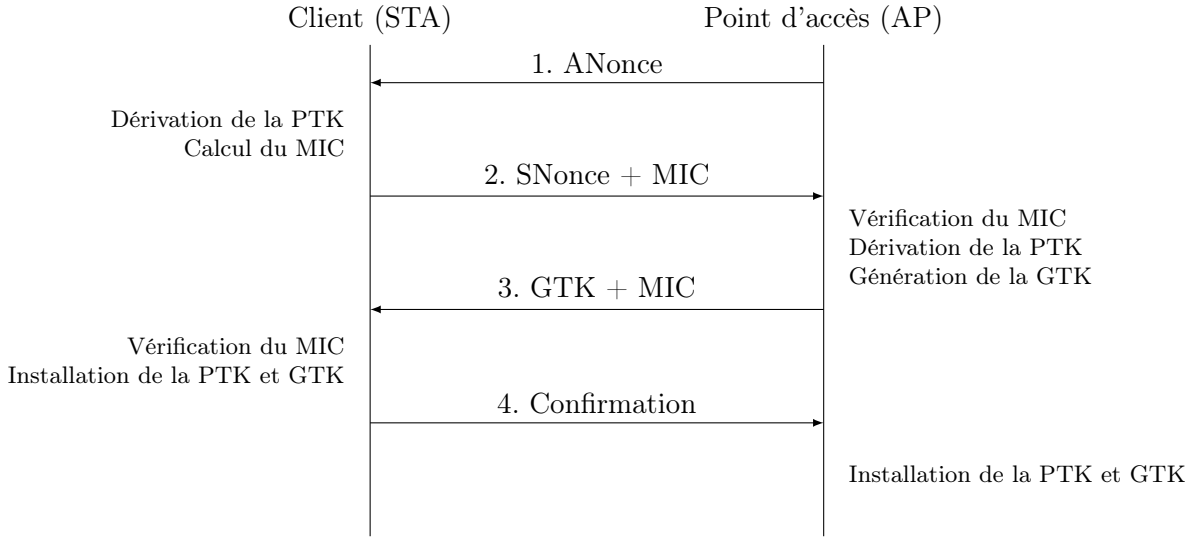

FIGURE 10 – 4-Way Handshake WPA/WPA2

La *Pairwise Transient Key* (PTK) est en pratique un trousseau de sous-clés spécialisées : la KCK est utilisée pour l'authentification et la protection des messages du 4-Way Handshake, la KEK pour chiffrer et distribuer la clé de groupe GTK, et la TK pour chiffrer le trafic de données unicast entre la STA et le point d'accès.

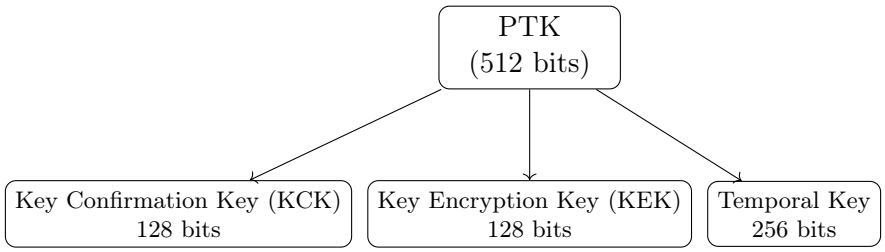

FIGURE 11 – Décomposition de la PTK en sous-clés KCK, KEK et TK.

Durant le 4-Way Handshake, les messages ne sont pas chiffrés. Leur sécurité repose sur l'utilisation de la clé KCK, dérivée de la PTK, permettant le calcul d'un MIC garantissant l'intégrité et l'authenticité des échanges. La clé KEK est quant à elle utilisée pour chiffrer la clé de groupe GTK transmise par le point d'accès.

Clé	**Taille**	**Usage**	**Phase**	**Renouvellement**
PSK	Variable	Passphrase partagée	Pré-Phase	Manuel
PMK	256 bits	Clé maître dérivée (PBKDF2)	Phase 1	À chaque authentification
PTK	512 bits	Clé transitoire unicast	Phase 2	À chaque 4-Way Handshake
KCK	128 bits	Intégrité du handshake (MIC)	Phase 2	À chaque 4-Way Handshake
KEK	128 bits	Chiffrement de la GTK	Phase 2	À chaque 4-Way Handshake
TK	256 bits	Chiffrement des données unicast	Phase 3	Clé par paquet (via TSC)
GTK	128 bits	Trafic broadcast/multicast	Phase 2	Périodique / Reconnexion

Table 2 – Récapitulatif des clés utilisées dans WPA-TKIP

— **Phase 3 (TKIP par trame)** : une fois les clés installées, chaque trame de données est chiffrée indépendamment à l'aide de l'algorithme TKIP. Contrairement à WEP, une clé unique est générée pour chaque paquet.
Pour chaque trame, les éléments suivants sont utilisés :
— la clé temporaire TK ;
— l'adresse MAC de l'émetteur ;
— le TKIP Sequence Counter (TSC) (compteur anti-rejeu de 48 bits).
TKIP applique un **mélange de clés en deux phases** :
— **Phase 1** : combine la TK, la MAC source et les 32 bits de poids fort du TSC pour produire une clé intermédiaire ;
— **Phase 2** : intègre les 16 bits de poids faible du TSC afin de générer la clé RC4 finale spécifique au paquet.
Un MIC est ensuite calculé sur les données en clair avant chiffrement, puis l'ensemble est chiffré à l'aide de RC4 et transmis.

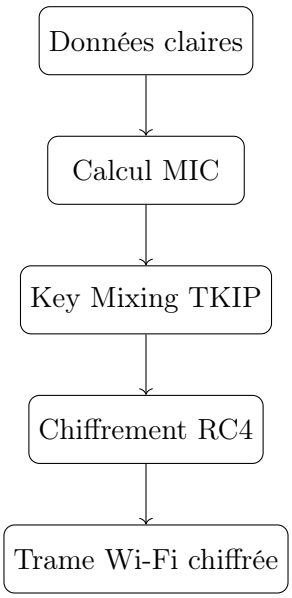

Figure 12 – Chiffrement d'une trame WPA-TKIP

Bien que RC4 soit toujours utilisé, WPA réduit significativement les risques d'attaque sans néanmoins les éliminer.

3.2.3 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 (*Pairwise Master Key* : clé maitresse) = PBKDF2(*Password-Based Key Derivation Function 2* : basée sur une passphrase et le SSID).
— **WPA2-Enterprise** : PMK fournie via un serveur RADIUS et une authentification EAP.

3.2.4 Dérivation des clés

Au-delà de l'échange de messages représenté dans la Figure 10, le 4-Way Handshake repose sur un mécanisme de dérivation de clés particulièrement structuré. L'ensemble du processus débute avec la PMK (Pairwise Master Key), qui constitue la base cryptographique partagée entre le client et le point d'accès. Dans le cas d'un réseau WPA2-PSK, cette PMK résulte directement de l'application d'une fonction de dérivation (PBKDF2) sur la passphrase et le SSID ; dans un environnement Enterprise, elle est fournie après l'authentification EAP par un serveur RADIUS. L'objectif du handshake n'est donc pas de négocier une nouvelle clé, mais de prouver que les deux entités possèdent bien cette PMK sans jamais la transmettre.

À partir de cette PMK, les deux parties vont dériver une clé plus large appelée PTK (Pairwise Transient Key). La construction de la PTK repose sur plusieurs éléments : l'adresse MAC du point d'accès, celle du client, ainsi que deux valeurs aléatoires appelées ANonce (envoyée par l'AP) et SNonce (envoyée par la station). Ces quatre paramètres garantissent que la PTK générée est unique pour chaque session, même si la PMK reste identique : une propriété essentielle pour éviter la réutilisation de clés et limiter les risques d'attaque par rejeu ou par corrélation.

La PTK n'est pas utilisée directement ; elle est découpée en trois sous-clés distinctes, chacune remplissant un rôle spécifique dans la sécurisation du lien. La première est la KCK (Key Confirmation Key), employée pour calculer les MIC (Message Integrity Code) des messages du handshake. Elle permet à chaque partie de vérifier que l'autre possède bien la PTK correcte, et donc implicitement la PMK. La deuxième sous-clé est la KEK (Key Encryption Key), utilisée par l'AP pour chiffrer la GTK (Group Temporal Key) transmise dans le message 3. Cette clé assure que seul un client légitime peut recevoir ou mettre à jour la clé de diffusion. Enfin, la dernière composante est la TK (Temporal Key), qui servira au chiffrement effectif du trafic unicast échangé entre la station et l'AP après la fin du handshake.

Un autre élément important est la présence de la GTK, envoyée par le point d'accès lors du message 3 du 4-Way Handshake. Contrairement à la PTK, qui est propre à une paire client–AP, la GTK est partagée entre tous les clients d'un même réseau et sert au chiffrement des trames multicast et broadcast. Sa transmission protégée par la KEK garantit qu'un attaquant passif ne peut pas l'intercepter, tandis que son renouvellement régulier limite les risques de compromission en cas d'écoute prolongée.

Ainsi, le 4-Way Handshake ne se réduit pas à un simple échange de valeurs nonces, mais constitue un véritable protocole d'initialisation cryptographique. Il assure simultanément la preuve de possession du secret initial, la dérivation de clés fraîches, l'établissement d'un canal chiffré sécurisé et la synchronisation des compteurs de trames. L'ensemble du mécanisme repose sur des propriétés formelles destinées à garantir la confidentialité et l'intégrité des échanges, tout en minimisant les risques liés à la réutilisation ou à la dérivation incorrecte des clés.

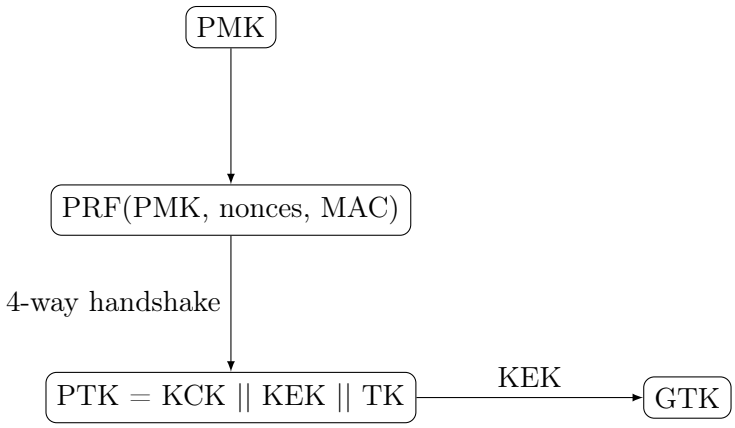

FIGURE 13 – Dérivation cryptographique PMK → PTK → GTK

Format d'une trame CCMP (WPA2)

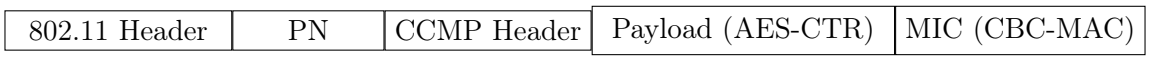

FIGURE 14 – Structure d'une trame CCMP

3.2.5 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)

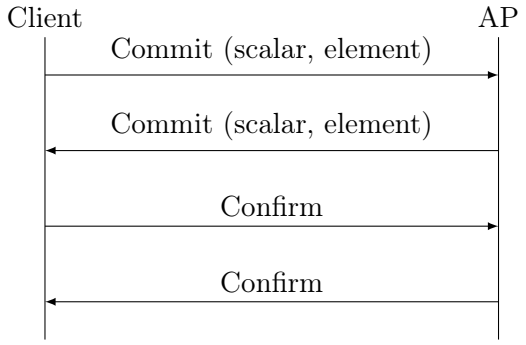

FIGURE 15 – Handshake SAE (WPA3)

3.3 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.

3.3.1 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.

3.3.2 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.

3.3.3 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 16 – Structure d'une trame GCMP (WPA3)

3.4 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 3 – Comparaison des protocoles de sécurité Wi-Fi

4 État de l'art sur la sécurité Wi-Fi

La sécurité des réseaux Wi-Fi constitue un domaine d'étude central en cybersécurité, en raison de l'omniprésence des technologies sans fil dans les environnements professionnels, industriels et domestiques. Depuis l'introduction du standard IEEE 802.11 en 1997, la surface d'attaque associée aux réseaux Wi-Fi n'a cessé de croître, sous l'effet conjugué de l'évolution des protocoles, de la diversité des implémentations matérielles et logicielles, et de la généralisation des usages mobiles.

Contrairement aux réseaux filaires, les communications Wi-Fi reposent sur un médium radio ouvert, accessible à toute entité située dans la zone de couverture du point d'accès. Cette caractéristique intrinsèque expose les échanges à des menaces spécifiques telles que l'écoute passive, l'injection de trames, l'usurpation d'identité réseau, ou encore les attaques de type *Man-in-the-Middle*. La sécurité des réseaux Wi-Fi ne dépend donc pas uniquement de la robustesse des mécanismes cryptographiques employés, mais également de la qualité des implémentations, des configurations retenues et des pratiques opérationnelles adoptées.

L'histoire de la sécurité Wi-Fi illustre une succession de mécanismes de protection introduits progressivement pour corriger les vulnérabilités des protocoles précédents. Chaque nouvelle génération de protocoles a apporté des améliorations significatives en matière de confidentialité, d'intégrité et d'authentification, mais a également donné naissance à de nouvelles catégories d'attaques exploitant des faiblesses cryptographiques, protocolaires ou humaines. Ainsi, les attaques statistiques ayant compromis WEP ont laissé place à des attaques ciblant les mécanismes d'authentification de WPA, puis à des attaques protocolaires plus subtiles contre WPA2, avant l'émergence de vulnérabilités liées aux implémentations et aux canaux auxiliaires dans les versions les plus récentes.

Cet état de l'art se concentre exclusivement sur les attaques Wi-Fi, les protocoles ayant été présentés dans la section précédente. Il propose une analyse structurée des principales familles d'attaques, de leur fonctionnement interne, de leur contexte d'apparition et de leur pertinence actuelle. L'objectif est de fournir une vision claire et synthétique des menaces réellement exploitables aujourd'hui, afin de justifier le choix des attaques étudiées et reproduites dans la suite de ce projet.

4.1 Évolution historique des attaques contre les réseaux Wi-Fi

L'évolution des attaques contre les réseaux Wi-Fi est étroitement liée à celle des protocoles de sécurité déployés pour protéger les communications sans fil. Dès l'apparition du protocole WEP (*Wired Equivalent Privacy*), introduit avec la première version du standard IEEE 802.11 en 1997, de nombreuses vulnérabilités ont été mises en évidence, révélant les limites des mécanismes cryptographiques alors utilisés.

WEP repose sur l'algorithme de chiffrement par flot RC4, combiné à des vecteurs d'initialisation (IV) de seulement 24 bits. Cette taille réduite entraîne une réutilisation fréquente des IV sur des réseaux actifs, ouvrant la voie à des attaques statistiques permettant de récupérer progressivement la clé de chiffrement. Les travaux de Fluhrer, Mantin et Shamir ont démontré qu'il était possible d'exploiter certaines faiblesses du générateur de clés RC4 pour reconstruire la clé WEP à partir d'un volume suffisant de trafic capturé. Ces attaques ont été rapidement automatisées par des outils spécialisés, rendant la compromission d'un réseau WEP accessible avec des moyens limités. Face à ces vulnérabilités structurelles, WEP a été officiellement déclaré obsolète au début des années 2000.

Afin de répondre à l'urgence sécuritaire sans imposer un renouvellement massif des équipements, la Wi-Fi Alliance a introduit WPA (*Wi-Fi Protected Access*) comme solution transitoire. WPA s'appuie sur le protocole TKIP (*Temporal Key Integrity Protocol*), qui conserve RC4 mais introduit un mécanisme de renouvellement dynamique des clés, un compteur de séquence et un code d'intégrité des messages. Bien que WPA ait significativement élevé le niveau de sécurité par rapport à WEP,

plusieurs attaques ont montré que cette solution restait vulnérable, notamment en raison de son héritage cryptographique et de certaines faiblesses dans la gestion de l'intégrité des trames.

La normalisation de WPA2 en 2004, dans le cadre du standard IEEE 802.11i, marque une étape majeure dans la sécurisation des réseaux Wi-Fi. WPA2 abandonne RC4 au profit de l'algorithme AES dans le mode CCMP, offrant une protection complète en matière de confidentialité, d'intégrité et de protection contre les attaques par rejeu. Pendant plusieurs années, WPA2 a été considéré comme un mécanisme de sécurité robuste, largement déployé dans les environnements professionnels et grand public. Toutefois, la découverte de l'attaque KRACK en 2017 a mis en évidence une faiblesse conceptuelle du protocole, exploitant la possibilité de rejouer certaines étapes du *4-Way Handshake* afin de forcer la réinstallation de clés de chiffrement déjà utilisées.

Ces travaux ont démontré que, même en l'absence de failles cryptographiques directes, des erreurs de conception protocolaire peuvent conduire à des vulnérabilités exploitables. En réponse à ces constats, WPA3 a été introduit en 2018 avec des mécanismes d'authentification renforcés, notamment l'utilisation du protocole SAE (*Simultaneous Authentication of Equals*) et l'obligation des *Protected Management Frames*. Néanmoins, la coexistence prolongée de WPA2 et WPA3 dans des environnements mixtes maintient une surface d'attaque significative, justifiant l'étude approfondie des attaques visant les protocoles encore largement déployés.

4.2 Attaques contre WEP : premières vulnérabilités des réseaux Wi-Fi

Le protocole WEP (*Wired Equivalent Privacy*) a constitué la première tentative de sécurisation des réseaux Wi-Fi lors de l'introduction du standard IEEE 802.11. Conçu pour offrir un niveau de confidentialité comparable à celui des réseaux filaires, WEP repose sur l'algorithme de chiffrement par flot RC4, combiné à une clé secrète partagée et à un vecteur d'initialisation (IV) de 24 bits transmis en clair dans chaque trame. Cette conception s'est rapidement révélée inadaptée face aux contraintes spécifiques des réseaux sans fil.

La principale faiblesse de WEP réside dans la gestion des vecteurs d'initialisation. En raison de leur taille réduite, les IV sont rapidement réutilisés sur des réseaux actifs, ce qui permet à un attaquant passif de collecter un grand nombre de trames chiffrées utilisant des clés de flot identiques. Cette réutilisation constitue le fondement des attaques statistiques visant à reconstruire la clé secrète sans jamais la deviner directement.

Les travaux de Fluhrer, Mantin et Shamir ont mis en évidence une vulnérabilité structurelle du générateur de clés de RC4 lorsqu'il est utilisé avec des IV faiblement aléatoires. L'attaque dite FMS exploite des corrélations entre certains octets du flot de clés et la clé secrète, permettant, après l'analyse d'un volume suffisant de trafic, de reconstituer progressivement la clé WEP. Cette attaque a démontré qu'un chiffrement théoriquement solide pouvait être compromis par une mauvaise intégration protocolaire.

D'autres attaques ont rapidement émergé pour exploiter les faiblesses de WEP. Les attaques par fragmentation tirent parti de la capacité du protocole 802.11 à fragmenter les trames, permettant à un attaquant de récupérer des portions de flot de chiffrement et de forger des paquets arbitraires. L'attaque ChopChop repose quant à elle sur une technique itérative consistant à tronquer progressivement une trame chiffrée et à observer les réponses du point d'accès afin de déduire le contenu en clair octet par octet. Ces attaques démontrent que WEP ne garantit ni la confidentialité ni l'intégrité des données transmises.

L'automatisation de ces techniques par des outils tels qu'AirSnort ou Aircrack-ng a rendu le cassage de clés WEP accessible avec des moyens matériels limités et dans des délais très courts, souvent de l'ordre de quelques minutes. Face à l'accumulation de ces vulnérabilités, WEP a été officiellement déclaré obsolète, et son utilisation est aujourd'hui considérée comme totalement insecure.

Bien que WEP ne soit plus déployé dans les environnements modernes, l'étude de ses attaques reste pertinente d'un point de vue pédagogique. Elles illustrent les conséquences d'une mauvaise gestion des aléas cryptographiques et constituent le point de départ historique des attaques Wi-Fi, ayant directement influencé la conception des protocoles de sécurité ultérieurs.

4.3 Attaques contre WPA et TKIP : limites des solutions transitoires

Face à l'obsolescence rapide de WEP, la Wi-Fi Alliance a introduit en 2003 le protocole WPA (*Wi-Fi Protected Access*) comme mécanisme de sécurisation transitoire, dans l'attente de la finalisation du standard IEEE 802.11i. L'objectif principal de WPA était de corriger les faiblesses les plus critiques de WEP tout en restant compatible avec les équipements existants, via une mise à jour logicielle. Pour ce faire, WPA repose sur le protocole TKIP (*Temporal Key Integrity Protocol*), qui conserve l'algorithme RC4 mais en modifie profondément l'usage.

TKIP introduit plusieurs améliorations majeures par rapport à WEP. Il met en œuvre un mécanisme de mélange de clés visant à produire une clé de chiffrement distincte pour chaque trame, à partir d'une clé maîtresse partagée et de paramètres dynamiques. Il ajoute également un compteur de séquence étendu afin de prévenir les attaques par rejeu, ainsi qu'un code d'intégrité des messages, appelé MIC (*Message Integrity Code*), destiné à détecter les modifications non autorisées des trames.

Malgré ces améliorations, WPA/TKIP conserve des faiblesses structurelles héritées de WEP, en particulier l'utilisation de RC4 et certaines limitations dans la conception du mécanisme d'intégrité. Plusieurs attaques ont démontré que TKIP ne garantissait pas une sécurité cryptographique suffisante face à des attaquants déterminés. L'attaque Beck-Tews, publiée en 2008, exploite une faiblesse dans le traitement des paquets QoS pour permettre le déchiffrement et l'injection de trames de petite taille. Cette attaque combine une variante de l'attaque ChopChop avec l'exploitation des limites du MIC, rendant possible la falsification de trafic chiffré en un temps relativement court.

Ces attaques ont mis en évidence le caractère fondamentalement transitoire de WPA. Bien que plus robuste que WEP, WPA/TKIP ne constitue pas une solution pérenne, en raison de ses choix cryptographiques contraints par la rétrocompatibilité matérielle. La découverte de vulnérabilités exploitables a conduit à l'interdiction progressive de TKIP dans les déploiements modernes et à son déclassement au profit de mécanismes reposant sur des algorithmes de chiffrement par bloc plus robustes.

L'étude des attaques contre WPA et TKIP demeure néanmoins pertinente, car elle illustre les limites des approches correctives incrémentales en matière de sécurité. Elle souligne également l'importance de concevoir des protocoles reposant sur des fondations cryptographiques solides plutôt que sur des adaptations de mécanismes déjà fragilisés, un principe qui guidera la conception de WPA2 et des protocoles ultérieurs.

4.4 Attaques contre WPA2 : exploitation du *4-Way Handshake*

La standardisation de WPA2 en 2004, dans le cadre du protocole IEEE 802.11i, a marqué une étape majeure dans la sécurisation des réseaux Wi-Fi. En remplaçant RC4 par l'algorithme AES utilisé dans le mode CCMP, WPA2 apporte une amélioration significative en matière de confidentialité, d'intégrité et de protection contre les attaques par rejeu. WPA2 s'est ainsi imposé comme le mécanisme de sécurité de référence pour les réseaux sans fil pendant plus d'une décennie. Toutefois, malgré la robustesse de ses primitives cryptographiques, plusieurs attaques ont montré que la sécurité globale du protocole pouvait être compromise par des faiblesses liées aux mécanismes d'authentification et d'établissement des clés.

Le fonctionnement de WPA2 repose sur un échange en quatre étapes, appelé *4-Way Handshake*,

destiné à établir des clés de session uniques entre le client et le point d'accès. À partir d'une clé maîtresse partagée (PMK), dérivée soit d'une phrase de passe dans le mode *WPA2-Personal*, soit des paramètres d'authentification 802.1X dans le mode *WPA2-Enterprise*, le protocole permet de générer une clé temporaire de session (PTK) utilisée pour chiffrer les communications unicast. Cet échange assure également la synchronisation des compteurs et des nonces nécessaires à la sécurité du chiffrement.

Dans le cas du mode *WPA2-Personal*, l'attaque la plus répandue consiste à capturer le *4-Way Handshake* lors de l'authentification d'un client légitime, puis à effectuer un craquage hors ligne de la phrase de passe. Cette attaque ne nécessite aucune interaction supplémentaire avec le réseau cible après la capture du handshake, ce qui la rend particulièrement discrète. La faisabilité de l'attaque dépend principalement de la complexité du mot de passe utilisé. Les phrases de passe courtes ou basées sur des dictionnaires peuvent être compromises en quelques heures à l'aide d'outils exploitant des capacités de calcul parallèles, notamment via des processeurs graphiques.

Bien que le protocole WPA2-Enterprise repose sur une authentification individuelle et offre une résistance accrue face aux attaques par dictionnaire, il n'est pas exempt de menaces. Des configurations incorrectes, telles que l'absence de validation du certificat du serveur d'authentification par les clients, peuvent permettre des attaques de type *Evil Twin*, conduisant à l'interception des identifiants ou à l'usurpation de sessions.

En 2017, la découverte de l'attaque KRACK (*Key Reinstallation Attack*) a profondément remis en question la sécurité de WPA2. Cette attaque exploite une faiblesse protocolaire du *4-Way Handshake*, en forçant la retransmission de certains messages afin de provoquer la réinstallation d'une clé de chiffrement déjà utilisée. Cette réinitialisation entraîne la réutilisation de nonces et la remise à zéro des compteurs de rejeu, permettant à un attaquant situé à portée radio d'intercepter ou de manipuler les communications chiffrées.

L'attaque KRACK a démontré que la sécurité d'un protocole ne repose pas uniquement sur la solidité de ses algorithmes cryptographiques, mais également sur la rigueur de sa conception protocolaire et de ses implémentations. Bien que des correctifs logiciels aient été rapidement déployés pour atténuer cette vulnérabilité, KRACK a mis en évidence des limites structurelles de WPA2 et a constitué un facteur déterminant dans le développement et l'adoption de WPA3.

Malgré ces vulnérabilités, WPA2 demeure largement déployé dans de nombreux environnements, en particulier dans les réseaux domestiques et les petites infrastructures professionnelles. Ce constat justifie l'étude approfondie des attaques ciblant WPA2, qui restent aujourd'hui parmi les menaces les plus réalistes et les plus exploitables dans un contexte opérationnel.

4.5 Focus sur WPA3 et les attaques Dragonblood

WPA3 a été introduit afin de renforcer la sécurité des réseaux Wi-Fi, notamment en remplaçant le mécanisme d'authentification basé sur une clé pré-partagée par le protocole SAE (*Simultaneous Authentication of Equals*). Ce choix vise en particulier à supprimer les attaques par dictionnaire hors ligne qui affectent les déploiements *WPA2-Personal*, en rendant l'attaque dépendante d'interactions actives et en limitant les tentatives possibles. WPA3 impose également l'usage des *Protected Management Frames* (PMF), réduisant l'efficacité des attaques reposant sur la falsification de trames de gestion, comme la désauthentification.

Toutefois, la robustesse théorique d'un protocole ne garantit pas l'absence de vulnérabilités pratiques. En 2019, une famille de failles, regroupées sous le nom de *Dragonblood*, a été publiée par Mathy Vanhoef et Eyal Ronen. Ces vulnérabilités ne remettent pas en cause le principe cryptographique de SAE, mais ciblent principalement des aspects d'implémentation et des choix d'intégration, notamment la phase de dérivation de la clé et certaines possibilités de repli (*downgrade*) dans des

environnements de compatibilité.

Une première catégorie d'attaques identifiée dans *Dragonblood* concerne les attaques par canaux auxiliaires (*side-channel attacks*). SAE s'appuie sur une procédure dite de *Hunting and Pecking* pour dériver un élément de groupe à partir du mot de passe. Certaines implémentations vulnérables présentent des variations mesurables (temps d'exécution, accès mémoire, consommation de ressources) lors de cette dérivation. Un attaquant capable d'observer ces variations peut réduire l'espace de recherche du mot de passe et accélérer une attaque par dictionnaire, en éliminant une partie des candidats. Bien que ces attaques soient plus contraignantes que le craquage hors ligne classique de WPA2, elles soulignent l'importance de contre-mesures d'implémentation, telles que l'exécution en temps constant et la réduction des fuites d'information.

Une seconde catégorie mise en évidence concerne des attaques de repli (*downgrade attacks*). Dans certains scénarios de transition ou de compatibilité, un point d'accès peut être configuré pour accepter à la fois WPA2 et WPA3 (*WPA3 Transition Mode*). Dans ce contexte, un attaquant peut tenter d'influencer la négociation afin de forcer l'usage de mécanismes moins robustes (par exemple un retour vers WPA2) ou de paramètres cryptographiques plus faibles, réintroduisant des vulnérabilités connues. Ces attaques rappellent que la coexistence de standards hétérogènes, fréquente dans les environnements réels, constitue une source de risque importante et peut limiter l'efficacité des améliorations introduites par les nouveaux protocoles.

L'existence de *Dragonblood* montre ainsi que l'adoption de WPA3 ne supprime pas instantanément toutes les menaces, mais déplace une partie du risque vers des aspects plus spécifiques : sécurité des implémentations, choix de configuration et gestion de la compatibilité. En pratique, les contre-mesures recommandées reposent sur l'application des correctifs fournis par les constructeurs, l'évitement du *Transition Mode* lorsque cela est possible, l'utilisation de paramètres cryptographiques robustes, ainsi que le maintien de bonnes pratiques de sécurité (notamment des phrases de passe longues et non prédictibles). Cette perspective est cohérente avec l'idée que, même lorsque les protocoles évoluent, la sécurité effective d'un réseau Wi-Fi dépend fortement de son déploiement opérationnel.

4.6 Attaques PMKID : compromission sans client connecté

Les attaques PMKID constituent une évolution significative des techniques de compromission des réseaux WPA2, en ce qu'elles permettent de lancer une attaque par dictionnaire sans nécessiter la capture préalable du *4-Way Handshake* ni la présence d'un client déjà authentifié sur le réseau. Cette attaque, révélée en 2018, exploite une fonctionnalité optionnelle du protocole IEEE 802.11i liée à l'identification de la clé maîtresse partagée.

Le PMKID (*Pairwise Master Key Identifier*) est une valeur dérivée de la clé maîtresse PMK et transmise par le point d'accès dans certaines trames EAPOL lors de l'initialisation d'une connexion. Il est calculé à partir d'une fonction de hachage cryptographique incluant la PMK, les adresses MAC du point d'accès et du client, ainsi qu'une chaîne constante. Dans certaines configurations, notamment lorsque des mécanismes de roaming rapide sont activés, cette valeur peut être transmise avant même l'établissement complet du *4-Way Handshake*.

Un attaquant peut exploiter ce comportement en envoyant une simple requête d'initiation de connexion au point d'accès, sans qu'aucun client légitime ne soit connecté. La réponse du point d'accès contient alors le PMKID, que l'attaquant peut capturer passivement. Cette information suffit à lancer une attaque hors ligne par dictionnaire ou force brute sur la clé maîtresse, de manière similaire aux attaques basées sur le *4-Way Handshake*, mais sans nécessiter d'attaque active préalable telle qu'une désauthentification.

L'attaque PMKID présente un avantage opérationnel majeur : elle est plus discrète que les

attaques classiques reposant sur la capture du handshake, car elle ne génère ni déconnexion de clients ni trafic suspect perceptible par les utilisateurs. Elle est également plus rapide à mettre en œuvre, puisqu'elle ne dépend pas du comportement des clients légitimes. Des outils dédiés permettent d'automatiser la capture du PMKID et sa conversion dans un format exploitable par des logiciels de craquage hors ligne utilisant des capacités de calcul parallèles.

Comme pour les attaques par capture du *4-Way Handshake*, la réussite de l'attaque PMKID dépend essentiellement de la robustesse de la phrase de passe utilisée. Les réseaux reposant sur des mots de passe faibles ou prévisibles restent vulnérables, indépendamment de l'absence de clients connectés. Cette attaque souligne ainsi une faiblesse fondamentale des modes *WPA2-Personal*, fondés sur des clés pré-partagées.

Les contre-mesures face aux attaques PMKID incluent l'utilisation de phrases de passe longues et complexes, la désactivation des fonctionnalités de roaming non nécessaires, ainsi que la migration vers WPA3. En remplaçant l'échange de clés par le protocole SAE, WPA3 supprime la possibilité d'attaques hors ligne de ce type et offre une meilleure résistance face aux tentatives de compromission passives.

4.7 Attaques par désauthentification et déni de service

Les attaques par désauthentification figurent parmi les attaques actives les plus anciennes et les plus fondamentales visant les réseaux Wi-Fi. Elles exploitent une caractéristique du standard IEEE 802.11 selon laquelle certaines trames de gestion, notamment les trames de désauthentification et de désassociation, peuvent être envoyées par un point d'accès ou un client afin d'indiquer la fin légitime d'une session sans fil.

Dans les premières versions du standard, ces trames de gestion ne sont ni chiffrées ni authentifiées, y compris lorsque les communications de données sont protégées par WEP, WPA ou WPA2. Un attaquant situé à portée radio peut ainsi forger des trames de désauthentification en usurpant l'adresse MAC du point d'accès ou du client cible, et forcer la rupture de la connexion sans disposer d'aucune clé cryptographique.

L'attaque par désauthentification peut être utilisée comme une attaque par déni de service, en envoyant de manière répétée des trames de désauthentification afin d'empêcher toute connexion stable des clients légitimes. Toutefois, son intérêt principal réside dans son rôle de prérequis pour de nombreuses autres attaques Wi-Fi. En forçant la déconnexion d'un client, l'attaquant provoque une reconnexion automatique, générant ainsi un *4-Way Handshake* pouvant être capturé à des fins de craquage hors ligne. Cette technique est largement utilisée pour accélérer les attaques contre les réseaux WPA/WPA2-Personal.

Les attaques par désauthentification sont également exploitées pour révéler des SSID prétendument cachés. Lorsqu'un client se reconnecte à un réseau dont le SSID n'est pas diffusé dans les trames balises, il inclut le nom du réseau dans certaines trames de gestion, permettant à un attaquant passif d'identifier le SSID réel. De manière plus générale, la désauthentification facilite la mise en œuvre d'attaques de type *Evil Twin*, en forçant les clients à se reconnecter à un point d'accès malveillant présentant un signal plus fort ou une configuration trompeuse.

La simplicité de mise en œuvre de ces attaques, combinée à leur efficacité, explique leur large diffusion. Des outils spécialisés permettent d'automatiser l'envoi massif de trames de désauthentification en ciblant un point d'accès, un client spécifique ou l'ensemble des clients associés à un réseau donné. Cette facilité d'exploitation rend les attaques par désauthentification particulièrement accessibles, même pour des attaquants disposant de compétences techniques limitées.

Afin de remédier à ces vulnérabilités, le standard IEEE 802.11w a introduit les *Protected Management Frames* (PMF), visant à chiffrer et authentifier certaines trames de gestion critiques. Lorsque

PMF est activé, les trames de désauthentification et de désassociation ne peuvent plus être forgées sans disposer des clés cryptographiques appropriées. Bien que PMF soit optionnel dans WPA2, il devient obligatoire avec WPA3, réduisant significativement l'efficacité de ces attaques. Néanmoins, la persistance de réseaux n'implémentant pas PMF maintient les attaques par désauthentification parmi les menaces les plus répandues dans les environnements Wi-Fi actuels.

4.8 Attaques Evil Twin et usurpation de points d'accès

Les attaques de type *Evil Twin* reposent sur l'usurpation de l'identité d'un point d'accès Wi-Fi légitime afin de tromper les utilisateurs et intercepter leurs communications. Contrairement aux attaques purement cryptographiques, les attaques Evil Twin exploitent principalement les mécanismes de gestion du réseau sans fil ainsi que le comportement des clients, ce qui les rend particulièrement efficaces dans des environnements réels tels que les réseaux publics ou d'entreprise.

Le principe fondamental d'une attaque Evil Twin consiste à créer un faux point d'accès reproduisant les caractéristiques visibles d'un réseau légitime, notamment son SSID et, dans certains cas, son adresse MAC. L'attaquant configure généralement ce point d'accès malveillant avec une puissance d'émission plus élevée que celle du point d'accès authentique, ou combine l'attaque avec des trames de désauthentification afin de forcer les clients à se reconnecter. Les terminaux privilégient alors automatiquement le point d'accès offrant le signal le plus fort, sans être en mesure de distinguer le réseau légitime de sa copie.

Une fois la connexion établie entre la victime et le point d'accès malveillant, l'attaquant se place en position d'homme du milieu (*Man-in-the-Middle*). Il peut alors intercepter, modifier ou rediriger le trafic réseau, capturer des données sensibles ou déployer des attaques complémentaires. Dans le cas des réseaux ouverts ou protégés par WPA/WPA2-Personal, l'attaquant peut mettre en place un portail captif frauduleux imitant une page de connexion légitime afin de récupérer des identifiants ou des phrases de passe Wi-Fi.

Les attaques Evil Twin sont particulièrement efficaces contre les réseaux utilisant des clés prépartagées, car la victime ne dispose d'aucun mécanisme permettant de vérifier l'authenticité du point d'accès. Même lorsque la phrase de passe saisie est correcte, celle-ci peut être capturée par l'attaquant et réutilisée ultérieurement pour se connecter au réseau légitime. Dans les environnements *WPA2-Enterprise*, ces attaques restent possibles en cas de mauvaise configuration des clients, notamment lorsque ceux-ci ne vérifient pas le certificat du serveur d'authentification, permettant ainsi l'usurpation du rôle du serveur RADIUS.

Les conséquences d'une attaque Evil Twin peuvent aller bien au-delà de la simple interception du trafic Wi-Fi. En contrôlant la passerelle réseau, l'attaquant peut lancer des attaques de type *SSL Stripping*, des redirections DNS malveillantes, ou injecter du contenu frauduleux dans les flux applicatifs. Ces attaques combinées permettent de compromettre des identifiants applicatifs, des sessions web ou des données sensibles, même lorsque des protocoles de sécurité supérieurs sont partiellement déployés.

Les contre-mesures face aux attaques Evil Twin reposent sur une combinaison de mécanismes techniques et organisationnels. L'utilisation de WPA2-Enterprise ou WPA3-Enterprise avec authentification mutuelle basée sur des certificats numériques constitue la protection la plus efficace, à condition que les clients valident correctement le certificat du serveur d'authentification. L'activation des *Protected Management Frames* limite l'efficacité des attaques par désauthentification utilisées pour faciliter ces scénarios. Enfin, le déploiement de systèmes de détection d'intrusion sans fil (WIDS/WIPS) et la sensibilisation des utilisateurs aux risques des réseaux Wi-Fi non fiables complètent les mesures de défense contre ce type d'attaque.

4.9 Attaques par compromission applicative : Man-in-the-Middle et SSL Stripping

Les attaques de type *Man-in-the-Middle* (MITM) constituent une catégorie d'attaques transversales exploitant une position intermédiaire entre la victime et les services auxquels elle accède. Dans un contexte Wi-Fi, cette position est fréquemment obtenue à la suite d'attaques de désauthentification ou d'attaques *Evil Twin*, qui permettent à l'attaquant de contrôler le point d'accès ou la passerelle réseau utilisée par les clients.

Une fois en position MITM, l'attaquant est en mesure d'intercepter, de modifier ou de rediriger le trafic réseau de la victime de manière transparente. Cette capacité ouvre la voie à de nombreuses attaques visant les couches supérieures du modèle OSI, en particulier les protocoles applicatifs reposant sur HTTP et HTTPS. Contrairement aux attaques ciblant directement les mécanismes de sécurité Wi-Fi, ces attaques exploitent des hypothèses de confiance implicites dans les communications réseau.

Parmi les attaques MITM les plus connues figure le *SSL Stripping*, qui consiste à empêcher la transition d'une connexion HTTP vers HTTPS. De nombreux utilisateurs accèdent initialement à un service web via une URL non chiffrée, s'en remettant à la redirection automatique vers HTTPS effectuée par le serveur. En position d'homme du milieu, l'attaquant intercepte cette redirection et maintient une connexion chiffrée légitime avec le serveur distant, tout en présentant à la victime une connexion HTTP non chiffrée. La victime perçoit alors une interface apparemment normale, tandis que les données sensibles transmises, telles que des identifiants ou des informations personnelles, circulent en clair entre le client et l'attaquant.

Les attaques MITM peuvent également s'appuyer sur des techniques complémentaires telles que l'empoisonnement ARP, la falsification de réponses DNS ou l'injection de certificats frauduleux, lorsque les mécanismes de validation côté client sont insuffisants. Dans un environnement Wi-Fi compromis, ces attaques sont particulièrement difficiles à détecter pour l'utilisateur final, car elles ne nécessitent pas la compromission directe du terminal.

Les contre-mesures face aux attaques MITM et SSL Stripping reposent principalement sur le renforcement de la sécurité aux couches supérieures. L'utilisation systématique de HTTPS, combinée à des mécanismes tels que HSTS (*HTTP Strict Transport Security*), empêche le downgrade vers HTTP et neutralise efficacement les attaques de type SSL Stripping. La validation rigoureuse des certificats TLS par les clients est essentielle pour prévenir l'usurpation de serveurs légitimes. En complément, l'utilisation de réseaux privés virtuels (VPN) permet de chiffrer l'ensemble du trafic utilisateur, réduisant l'impact d'une compromission du réseau Wi-Fi sous-jacent.

Ces attaques illustrent la nécessité d'une approche de sécurité globale, dépassant la seule protection du lien radio. Même lorsque les mécanismes Wi-Fi sont correctement configurés, une mauvaise sécurisation des couches applicatives ou des comportements utilisateurs peut conduire à des compromissions sévères. Elles justifient pleinement l'étude conjointe des attaques Wi-Fi et des attaques applicatives dans une démarche de défense en profondeur.

5 Méthodologie

5.1 Environnement expérimental

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

6 Attaques Wi-Fi étudiées et reproduites

7 Conclusion

Références

[1] C. aux projets Wikimedia, "Wi-fi — wikipédia," 8 2003, [Online ; accessed 2026-01-06]. [Online]. Available : https://fr.wikipedia.org/wiki/Wi-Fi#Modes_de_mise_en_r%C3%A9seau

[2] C. to Wikimedia projects, "Aircrack-ng - wikipedia," 5 2006, [Online ; accessed 2026-01-06]. [Online]. Available : https://en.wikipedia.org/wiki/Aircrack-ng#WEP

[3] A. N. darkAudax, "simple_wep_crack [aircrack-ng]," 3 2018, [Online ; accessed 2026-01-06]. [Online]. Available : https://www.aircrack-ng.org/doku.php?id=simple_wep_crack

Annexes

A Captures Wireshark

B Scripts utilisés