HACK UTT

WORKSHOP

THÈME : WIFI HACKING

23/04/2025

18h-20h

Arthur BIDET

SOMMAIRE

1. LE WIFI

Wireless Fidelity : technologie qui permet de **connecter** des appareils entre eux et à Internet sans fil, via des **ondes radio**.

Normes : **802.11**a/b/g/n/ac/ax...

Sécurités : WEP, WPA, WPA2, WPA3, ...

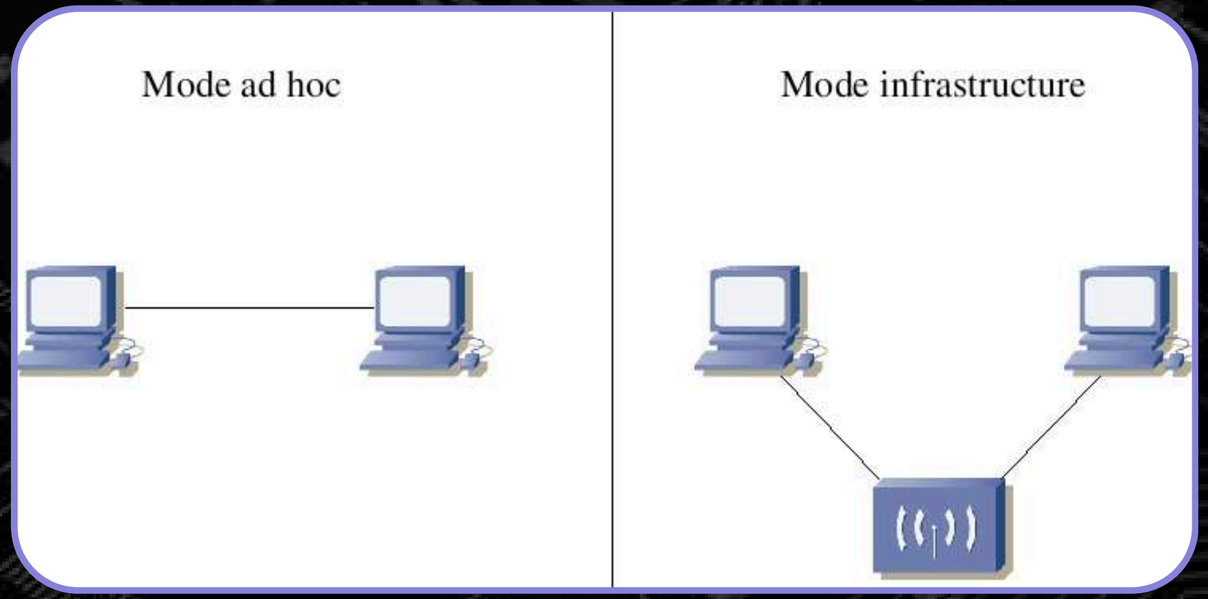
Portée : quelques dizaines de mètres jusqu'à plusieurs kilomètres

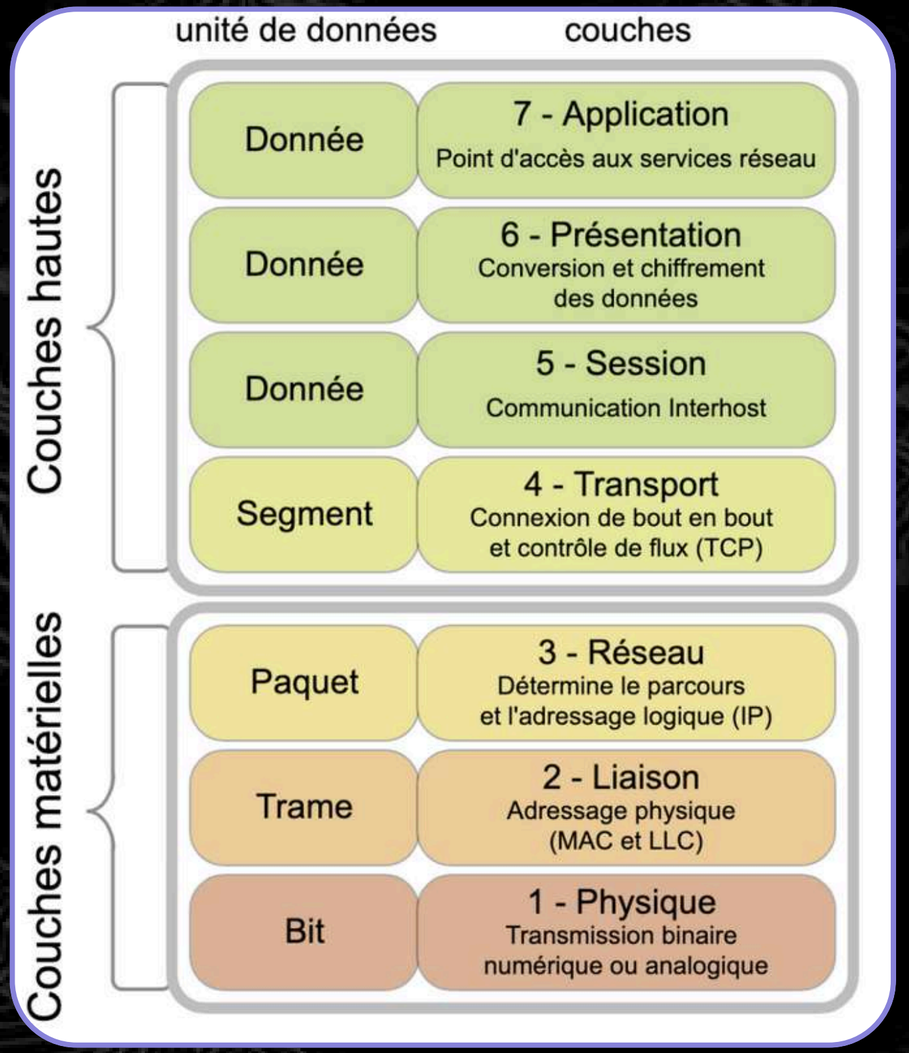
Appareils : **Routeurs**, répéteurs, **ordinateurs**, **téléphones**, objets connectés, ...

1. LE WIFI

Et au niveau réseau ?

Norme 802.11 qui concerne les couches 1 et 2 du modèle OSI

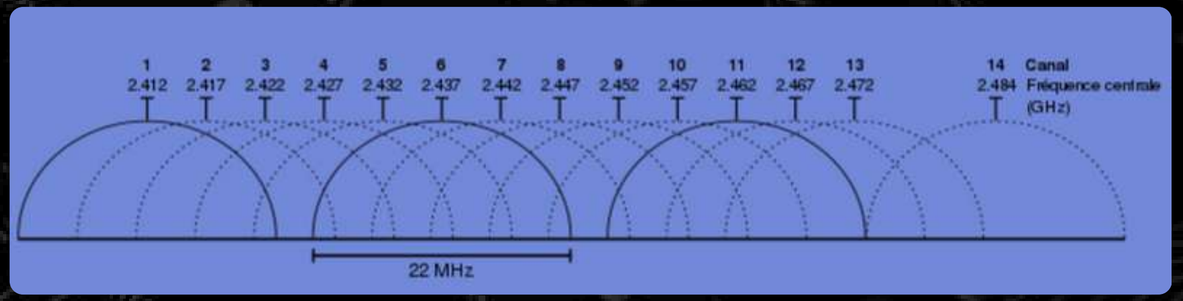




1. LE WIFI

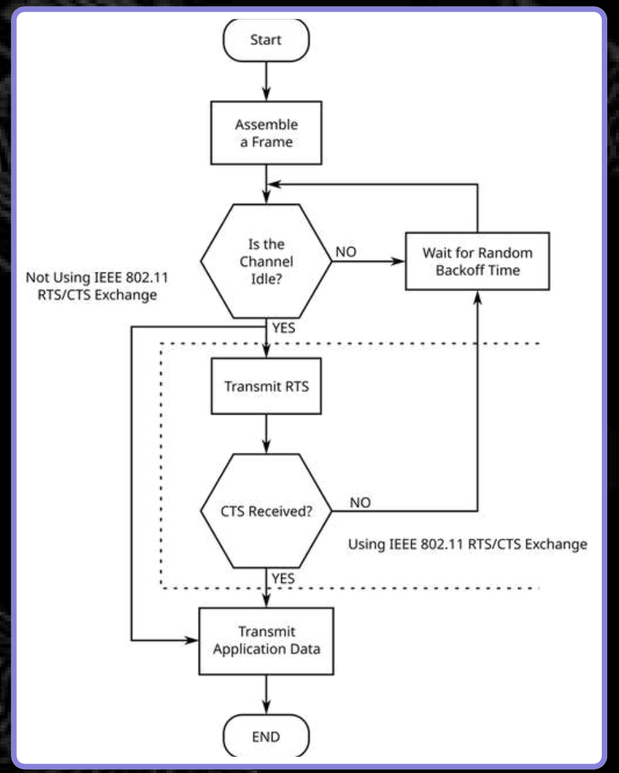
OFDM

- Technique de **modulation** où un **signal** est divisé en plusieurs **sous-porteuses orthogonales**.
- Les **canaux** représentent des **bandes de fréquences** sur lesquelles les appareils communiquent



CSMA/CA

Colision avoidance = On peut avoir plusieurs appareils qui communiquent sur le même canal



2. LES OBJECTIFS

Types d'attaques :

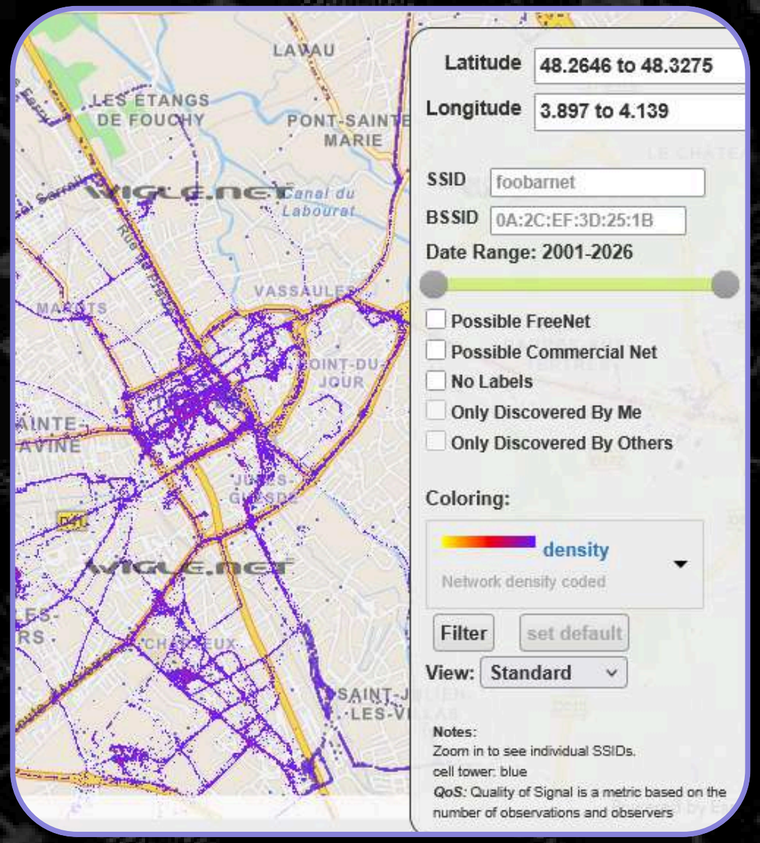
- Faiblesses des protocoles (mots de passe)
- Rogue Access Points 
- Brouillage 
- DoS 
- MITM 

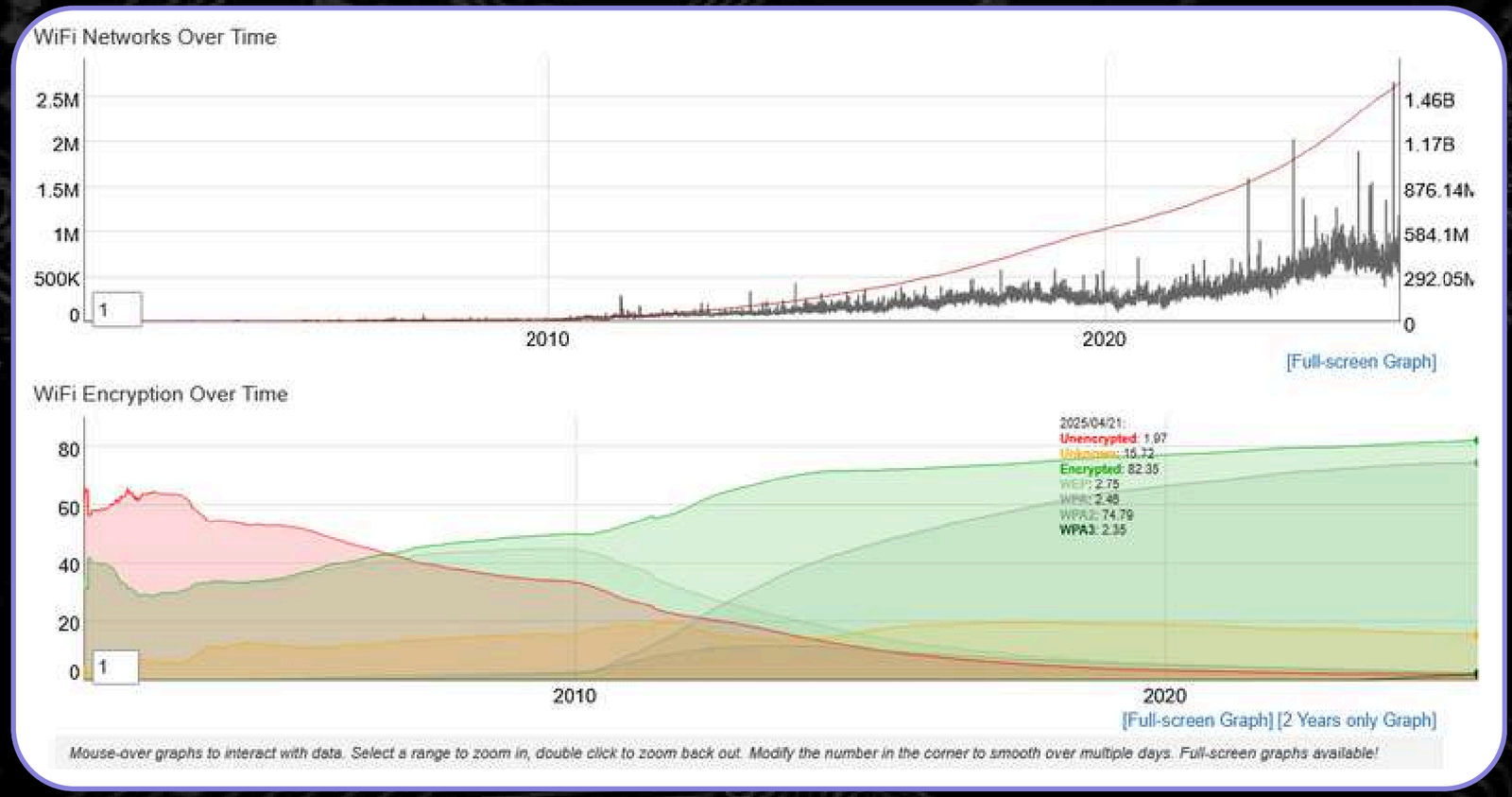
Pourquoi ?

- Vol de données (mots de passe, information sensibles, ...)
- Contrôle (accès au réseau privé, ...)
- Multitude de motivations possibles

BONUS : WIGLE.NET

*“WiGLE (Wireless Geographic Logging Engine) is a website for collecting information about the different **wireless hotspots** around the world.”*





3. LE WEP

Une sécurité historique

- Mécanisme de **sécurité** pour réseaux sans-fil **majoritairement utilisé** de **2000 à 2015**, désormais considéré comme obsolète.
- Intégrité : le WEP utilise la somme de contrôle **CRC32** pour assurer l'**intégrité**
- Confidentialité : utilisation du **chiffrement par flot RC4**

RC4 est conçu en 1987 par Ronald Rivest, l'un des inventeurs de l'algorithme de cryptographie asymétrique RSA

Son fonctionnement

Vecteur d'Initialisation (IV)

Séquence de bits qui change régulièrement, à chaque trame si l'implémentation est bonne. Il est combiné à la clé statique, ce qui introduit une notion d'aléatoire dans le chiffrement.

Clé WEP statique

La clé partagée peut être de **40 bits** ou de **104 bits**. En la concaténant à l'IV, on obtient la **seed**, elle de **64 bits** ou **128 bits**.

Keystream

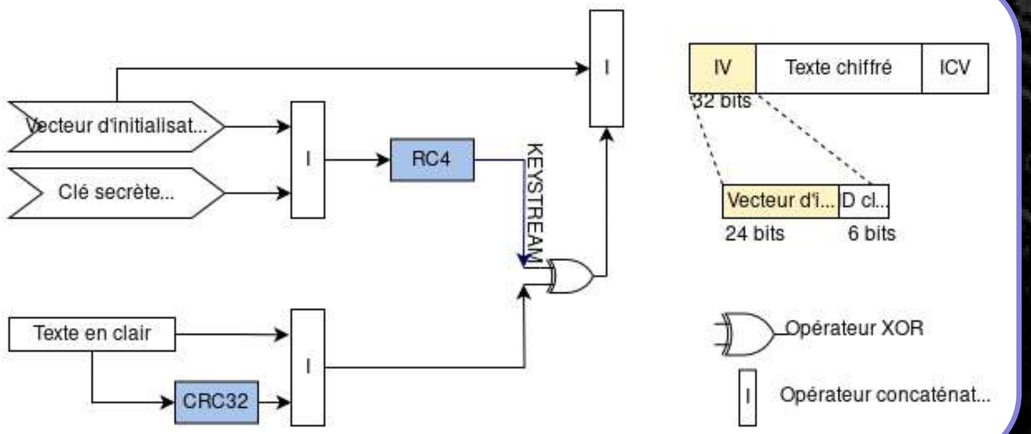
Le **keystream** est le message à envoyer. Il est chiffré par **RC4** en utilisant la **graine** (seed).

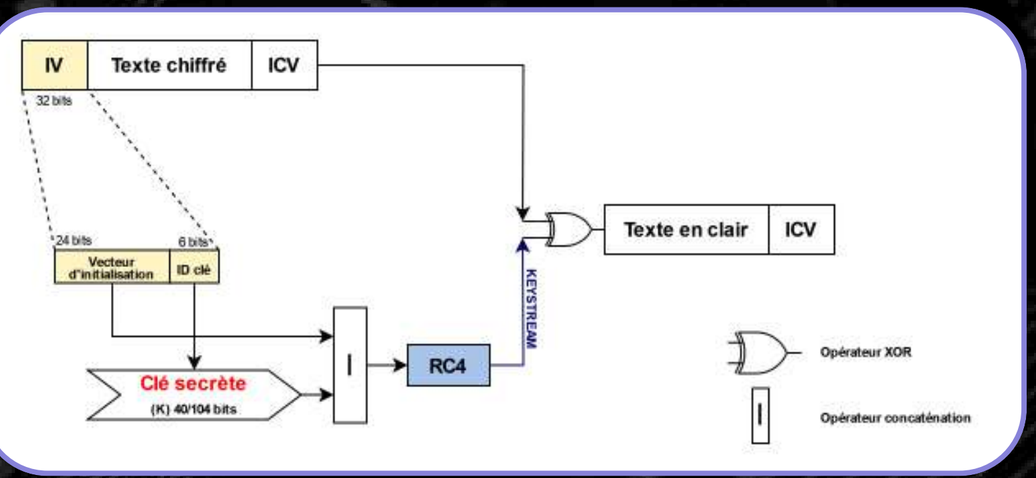
Checksum

La **checksum** est calculée en utilisant la fonction **CRC32**. Elle permet de vérifier l'**intégrité** du message une fois déchiffré.

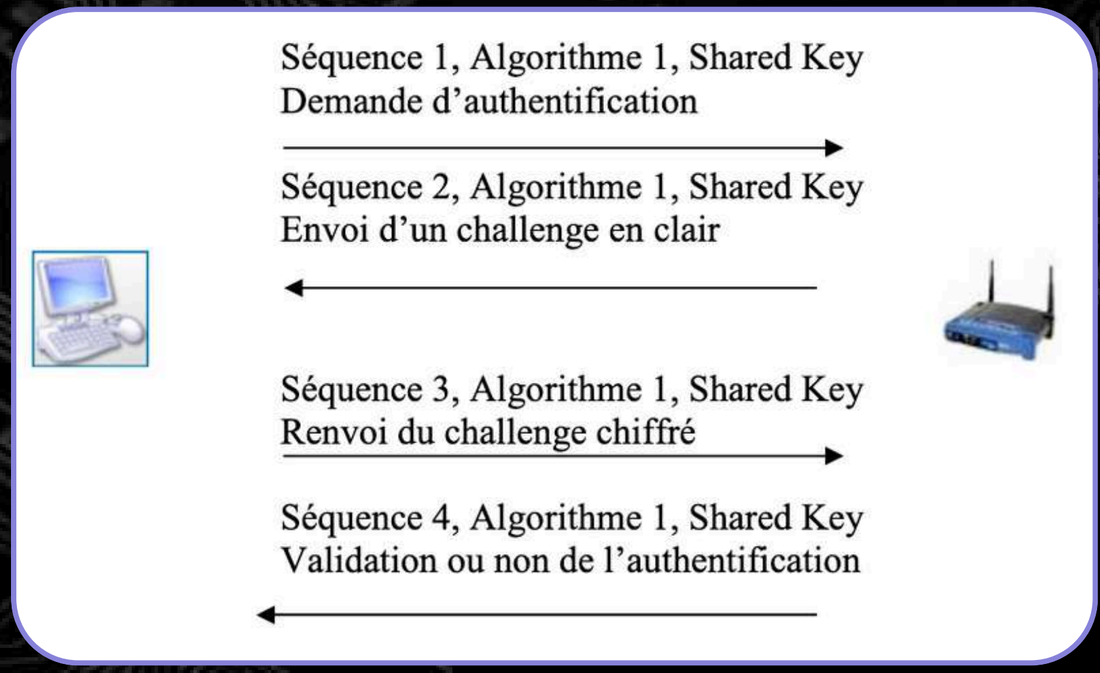
3. LE WEP

Chiffrement et déchiffrement





Authentification



DISCLAIMER POUR LES SCRIPTKIDDIES

1. Les attaques doivent se faire sur des environnement contrôlés (votre réseau), comprenez vos actions
2. Les attaques passives étant généralement indétectables, c'est votre devoir de filtrer les réseaux
3. Un antécédent de cyberattaque ? dites au revoir aux employeurs

3. LE WEP

Les situations

Scenarios	Open	SKA
Connected clients	sniffing + arpreplay (with client spoofing) + deauth + cracking	sniffing + arpreplay (with client spoofing) + deauth + cracking
No clients	sniffing + fake auth + fragmentation or chopchop + cracking	😳

https://www.thehacker.recipes/radio/wi-fi/wep/

Noms des attaques

- FMS/KOREK
- fausse authentification
- Chop-Chop
- Clair connu

Exemple : SKA avec clients

Identifier le client

airmon-ng start wlan0
airodump-ng wlan0mon
Noter le BSSID (mac ap), canal (1-11), station (mac client)

Capturer le handshake SKA

airodump-ng --channel 6 --bssid AA:BB:CC:DD:EE:FF -w output.pcapng wlan0mon #capture les communications avec l'AP
aireplay-ng -0 X -a AA:BB:CC:DD:EE:FF -c 11:22:33:44:55:66 wlan0mon #deauth attaque → X = nb de paquets de deauth

Récupération des IV

aireplay-ng -3 -b AA:BB:CC:DD:EE:FF wlan0mon #-3 = arp replay

Craquer la clé WEP

aircrack-ng output.pcapng

4. LE WPA2 - PSK

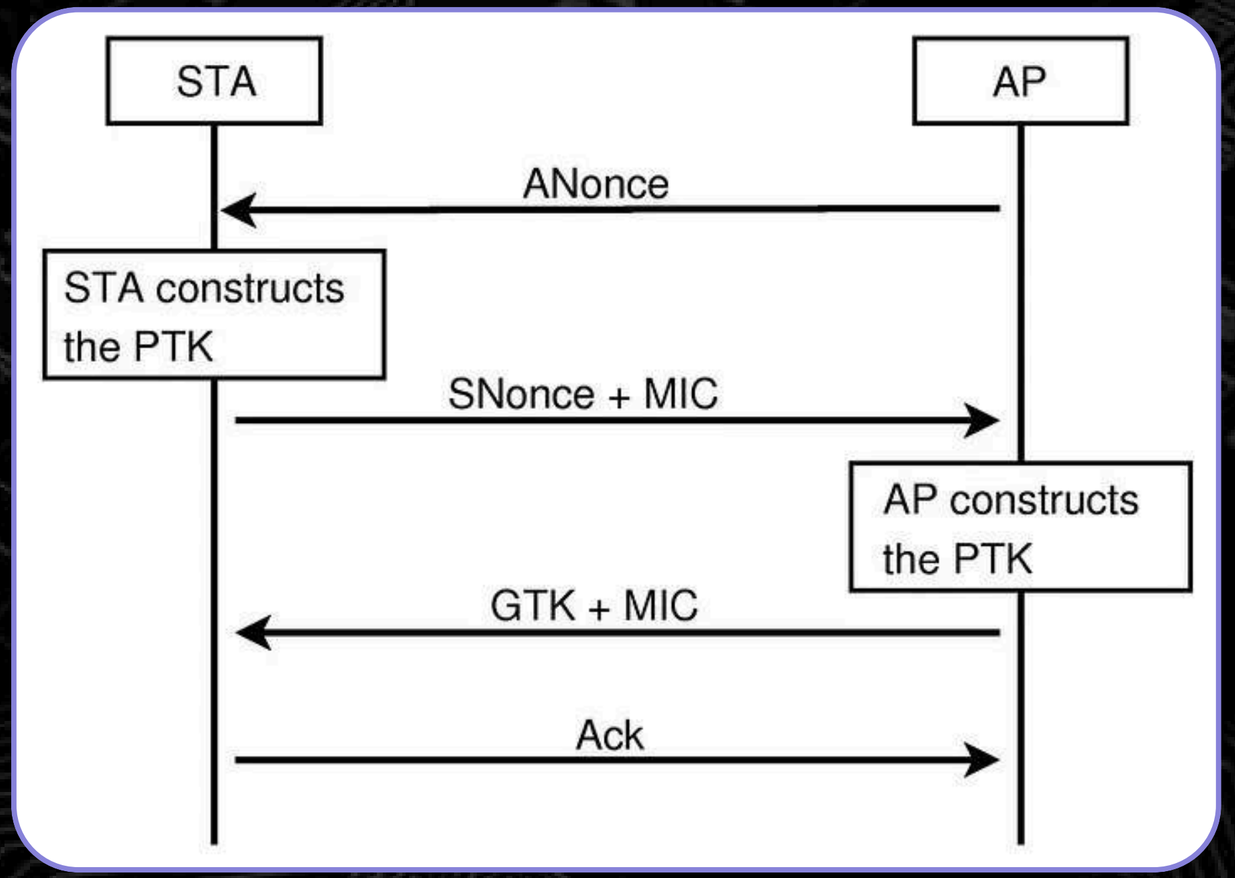
Concepts

WPA2 est la version de la norme 802.11i certifiée par la Wi-Fi Alliance. Elle impose de prendre en charge le protocole CCMP, qui s'appuie sur AES, et qui est considéré comme totalement sécurisé.

Le 4-way handshake

L'authentification est basée sur un 4-way handshake. Cet échange permet de vérifier l'identité du client et de l'AP. Il permet aussi à chacun de négocier les clés de chiffrement pour la sécurisation des communications, ainsi que d'assurer l'intégrité et la confidentialité.

```
- PSK = mot de passe
- PMK = PBKDF2(HMAC-SHA1, PSK, SSID, SSID length, 4096, 256 bits)
- PTK = PRF-512(PMK, "Pairwise key expansion", Min(AA, SPA) || Max(AA,
SPA)||Min(ANonce, SNonce) || Max(ANonce, SNonce))
- GTK = dépend de l'AP
- MIC = HMAC-SHA1(PTK, Data)
```



4. LE WPA2 - PSK

Méthode d'attaques :

1. Récupération d'informations (adresse mac AP et client, canal)
2. Capturer les échanges avec l'AP
3. Déconnecter un client pour récupérer un handshake
4. Filtrer les résultats et casser le mot de passe

Outils :

1. Scan : airodump-ng, iwlist, hcxdumptool
2. Capture : airodump-ng, hcxdumptool
3. Déconnexion : **airplay-ng**
4. Mot de passe : arcrack-ng, JohnTheRipper, **Hashcat**

https://www.notion.so/Wifi-d3eb7668fd2942d2bd1e7e7344053220?pvs=4

5. LE WPA2 - PMKID

Le **PMKID** (Pairwise Master Key Identifier) est un identifiant unique utilisé par le **point d'accès** (AP) pour suivre la clé **PMK** (Pairwise Master Key) utilisée lors de la connexion d'un client.
En gros, c'est une **empreinte** qui permet d'identifier la clé PMK entre un client et un AP **sans devoir refaire toute l'authentification**.

PMKID = HMAC-SHA1-128(PMK, "PMK Name" | MAC_AP | MAC_STA)

L'attaque du PMKID :

1. Ne nécessite pas de 4-way handshake
2. Ne nécessite pas de client connecté à l'AP

Méthode :

1. Calculer des PMK candidats par bruteforce
2. Calculer le PMKID correspondant et le comparer avec celui capturé

https://www.notion.so/Wifi-d3eb7668fd2942d2bd1e7e7344053220?pvs=4

6. ET APRÈS ?

Autres méthodes

- Rogue access points (WPA2, WPA2-Entreprise)
- Evil Twin AP (usurpation)
- Déni de service
- Brouillage

Post exploitation

- Reconnaissance du réseau (machines, services)
- Recherche de cibles intéressantes
- Sniffing et MITM (Man-in-the-Middle)
- Accès à des ressources
- Utilisation du réseau comme rebond

THE END

MERCI À TOUS D'ÊTRE VENUS !

Retrouvez toute la partie technique, des explications détaillées et des attaques supplémentaires sur mon Notion :
https://www.notion.so/Wifi-d3eb7668fd2942d2bd1e7e7344053220?pvs=4