



---

# Vulnérabilités des réseaux

## WiFi

---

- Types d'attaques (passives / actives).
- Solutions proposées (internes / externes)



# Activités en ligne

Activité 1: *Wireless Security Incidents*

[https://miro.com/app/board/o9J\\_IG7Sx9c=/](https://miro.com/app/board/o9J_IG7Sx9c=/)

Activité 2: *WiFi Attacks Matching Cards*

<https://shorturl.at/blsP8>

Activité 3: *WiFi Attacks Quizz*

<https://forms.gle/1FHiHkub4fNsaetg6>

Activité 3: *Attack Types*

[https://miro.com/app/board/o9J\\_IGp8kLY=/](https://miro.com/app/board/o9J_IGp8kLY=/)

<https://miro.com/app/board/uXjVPsDp5CQ=/>



# Manque de sécurité WiFi

- Les ondes radioélectriques ont une grande capacité de :
  - Se propager dans toutes les directions
  - Atteindre une portée relativement grande
- ⇒ Impossibilité de maîtriser des ondes radio
- ⇒ Débordement de la zone de couverture radio d'un point d'accès du domaine privé d'une entreprise ou d'un particulier.
- ⇒ Difficulté de confiner les émissions d'ondes radio dans un périmètre restreint.



# Manque de sécurité WiFi (2)

- La communication se base en native sur la propagation des ondes radio
- Apprête ces réseaux à subir des attaques de type:
  - **Ecoute** (clandestine)
  - **Accès non autorisé** (Intrusion par usurpation d'identité )



# Attaques sur le réseau WiFi

- Tout adaptateur 802.11, placé à portée d'un WLAN, peut potentiellement **capturer** les trames de **données** échangées
- Une pratique consiste à **circuler** dans la ville avec un ordinateur portable équipé d'une carte réseau sans fil à la recherche de réseaux sans fil → il s'agit du **war-driving**
- Il est facile **d'écouter** sur les réseaux sans fils, voire donner même **l'accès** à des intrus aux réseaux d'infrastructure si des mesures de sécurité ne sont pas prises.



# Attaques sur le réseau WiFi (2)

- **Interception de données** : écouter les transmissions des différents utilisateurs du WLAN
  - **vol** des informations (**Eavesdropping**)
  - **Prise de connaissance** des mots de passe, de crédits de connexion,...
- **Insertion de trafic**
  - **Bombardement** du réseau
  - **Goulet d'étranglement**
- **Usurpation d'identité** : se faire passer pour un utilisateur du système
  - **Vol** et **divulcation** de l'information
  - **modification** d'informations
  - **Destruction** d'informations
  - **Injection** de code malicieux
  - Le **détournement** de connexion dont le but est d'obtenir l'accès à un réseau local ou a internet
  - Introduction de **serveur illicite** dans le réseau

# Le Wardriving

- **Wardriving** consiste à rechercher physiquement les réseaux sans fil présentant des vulnérabilités à partir d'un véhicule en mouvement et à cartographier les points d'accès sans fil.
- Equipements requis:
  - Outil d'écoute pour le Wardriving : iStumbler, KisMAC, CoWPAtty, InSSIDer, WiGLE, NetStumbler, WiFi-Where et WiFiphisher ...
  - GPS: à partir d'un smartphone ou d'un appareil autonome afin d'enregistrer l'emplacement des points d'accès sans fil.
  - Carte réseau sans fil et antenne: Une carte sans fil qui supporte le sniffing (mode monitor / promiscuous).
  - Smartphone ou ordinateur portable



© CanStockPhoto.com - csp41397336

# Le Warchalking

- **Warchalking** consiste à dessiner des des symboles dans les espaces publics pour désigner un réseau sans fil Wi-Fi ouvert dans un espace public.
- **Warchalking** fournit des informations sur le type de connexion sans fil utilisé, qui peut être un nœud ouvert, un nœud fermé ou un nœud sécurisé
- Cela peut attirer les pirates et leur faire prendre conscience du point d'accès Wi-Fi et de sa sécurité.
- Les pirates peuvent utiliser ces informations **pour attaquer le réseau Wi-Fi.**

let's warchalk..!	
KEY	SYMBOL
OPEN NODE	ssid bandwidth 
CLOSED NODE	ssid 
WEP NODE	ssid access contact  bandwidth

blackbeltjones.com/warchalking

Proposed New Signs	
Unrestricted access	AP with MAC filtering
Open access with restrictions	Pay for access AP
AP with WEP	AP with multiple access controls (not for public use)
AP with closed ESSID	Honeypot





# WiFi Chalking

## WarWalking

Les attaquants se promènent avec des ordinateurs portables WiFi pour détecter les réseaux sans fil ouverts



## WarChalking

Une méthode utilisée pour dessiner des symboles dans les lieux publics pour annoncer les réseaux WiFi ouverts



## WarFlying

Les attaquants utilisent des drones pour détecter les réseaux sans fil ouverts



## WarDriving

Les attaquants circulent avec des ordinateurs portables WiFi pour détecter les réseaux sans fil ouverts





View



Uploads



Info



Stats



Tools

Login ▾

### WiWiWa 2.46 released in Beta channel

Wed, 07 Aug 2019 23:46:45 GMT

Due to an over-aggressive bugfix for new Android releases by yours truly, 2.45 wouldn't run on Android J/K/L/M devices. 2.46 Should restore functionality on OLDDroid.

-arkasha

### Can't stop the signal, Mal

Wed, 29 May 2019 14:53:52 GMT

An update wherein this may become a developer option:

[read more...](#)

-arkasha

### Google Android 9 and up: We won't fix WiFi Scanning

Fri, 24 May 2019 18:17:21 GMT

In a blow to the networking, security, and wardriving hobbyist communities today, Google has officially marked their decision to throttle wifi scanning for non-Google software on Android 9 and up as "Won't Fix" in spite of popular community support for a configurable option.

[read more...](#)

-arkasha

### KML fixes and improvements

Sun, 31 Mar 2019 00:07:35 GMT

Original KML default controls. Bluetooth and Cellular data, and

sousse



Station des Louages de Sousse Medina

WIGLE.NET

WIGLE.NET

WIGLE.NET

MAGIC-EYE RC

Coredoor 4G\_78770E

GNET-63009

MAGIC-EYE

Cabinet MBL

PLUANTOPNET38E8FE87

WIGLE.NET

SOUVAIGNERme 2019

WIGLE.NET

MAGIC-EYE

WIGLE.NET

TOPNETER85DCBET966F9705

Esri Community Maps Contributors, Esri, HERE, Garmin, METI/NASA, USGS

Latitude 35.8277 to 35.8283

Longitude 10.6393 to 10.6406

SSID any

BSSID

Date Range: 2017-2021

- Possible FreeNet
- Possible Commercial Net
- No Labels
- Only Discovered By Me
- Only Discovered By Others

Coloring:

QoS

WIGLE quality metric coded

Filter

set default

View: Greyscale ▾

Notes:

Zoom in to see individual SSIDs.

cell tower: blue

QoS: Quality of Signal is a metric based on the number of observations and observers



# WarDriving tools



**Airbase-ng**

<http://aircrack-ng.org>



**MacStumbler**

<http://www.macstumbler.com>



**ApSniff**

<http://www.monolith81.de>



**WiFi-Where**

<http://www.threejacks.com>



**WiFiFoFum**

<http://www.wififofum.net>



**AirFart**

<http://airfart.sourceforge.net>



**MiniStumbler**

<http://www.netstumbler.com>



**AirTraf**

<http://airtraf.sourceforge.net>



**WarLinux**

<http://sourceforge.net>



**802.11 Network Discovery Tools**

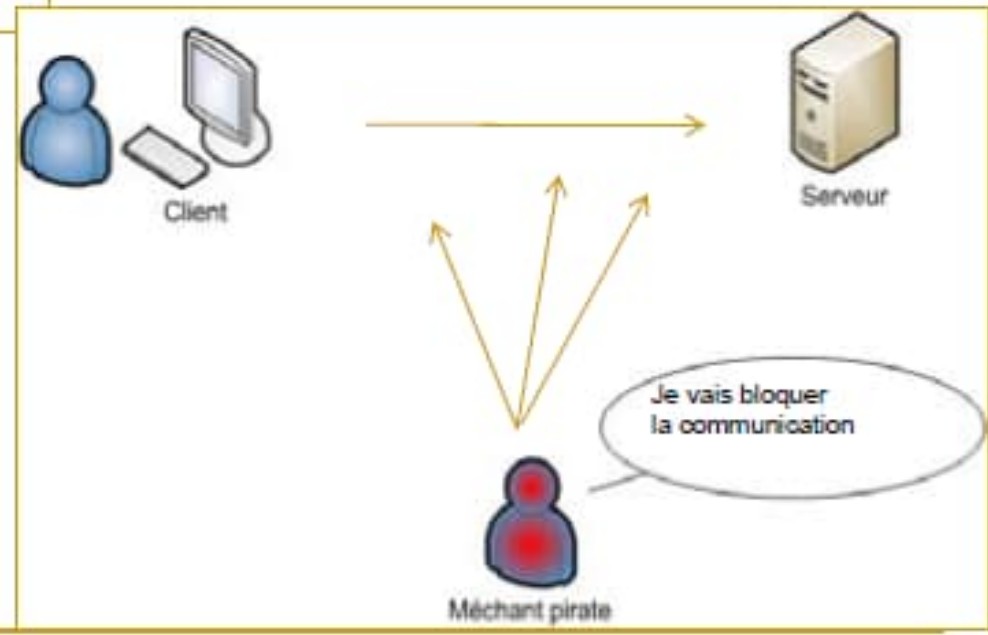
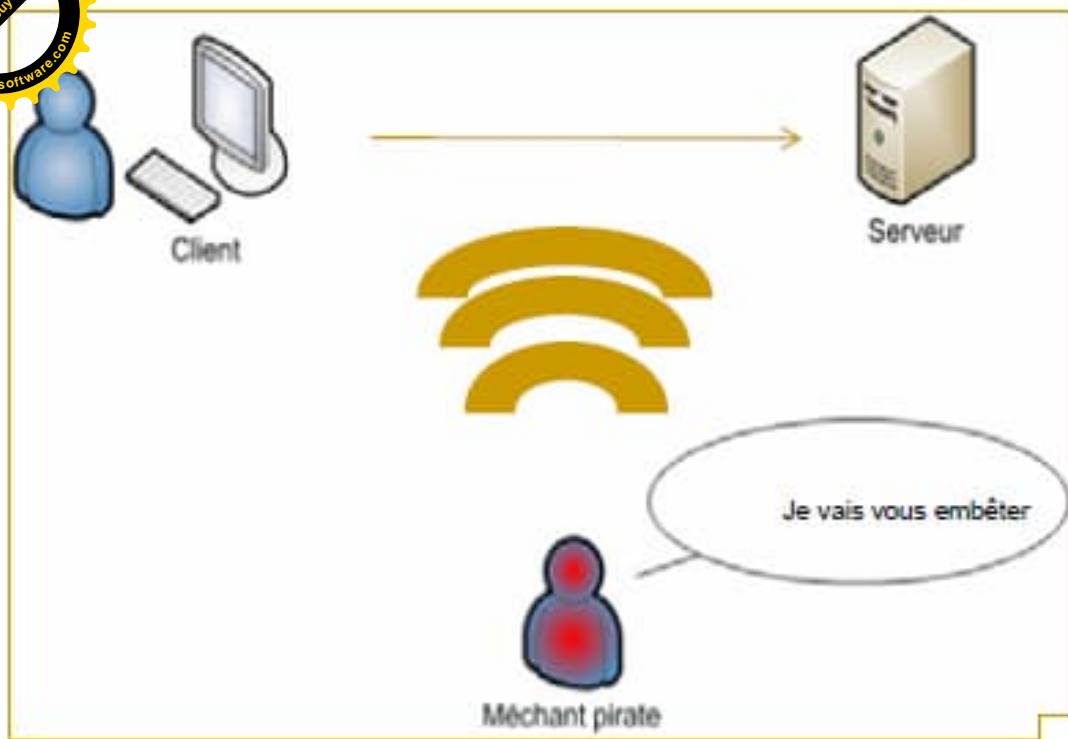
<http://wavelan-tools.sourceforge.net>

# Attaques actives

## ■ DoS (Denial of Service) :

Cette attaque a pour but d'empêcher des utilisateurs légitimes d'accéder à des services en saturant de fausses requêtes ces services.

- ✓ Brouillage du signal radio par une émission ayant une fréquence proche (four micro-onde,...).
- ✓ Bloquer le PA en :
  - l'inondant de requêtes de désassociation (programme de type Airjack)
  - provoquant une surconsommation d'énergie de telle manière à rendre l'appareil temporairement inutilisable, c'est ce que l'on appelle un *déni de service sur batterie*.



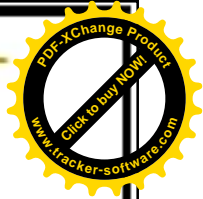


# DoS (Denial Of Service)

- ▶ Vise à rendre le réseau WiFi **indisponible**
- ▶ Plusieurs techniques:
  - ▶ **Jamming** ( brouillage) afin de perturber la transmission radio et créer des interférences
  - ▶ **Bombarder** l'AP (ou la STA victime) avec des trames:
    - ▶ D'association / d'authentification
    - ▶ De désauthentification
    - ▶ De Probe
    - ▶ ...

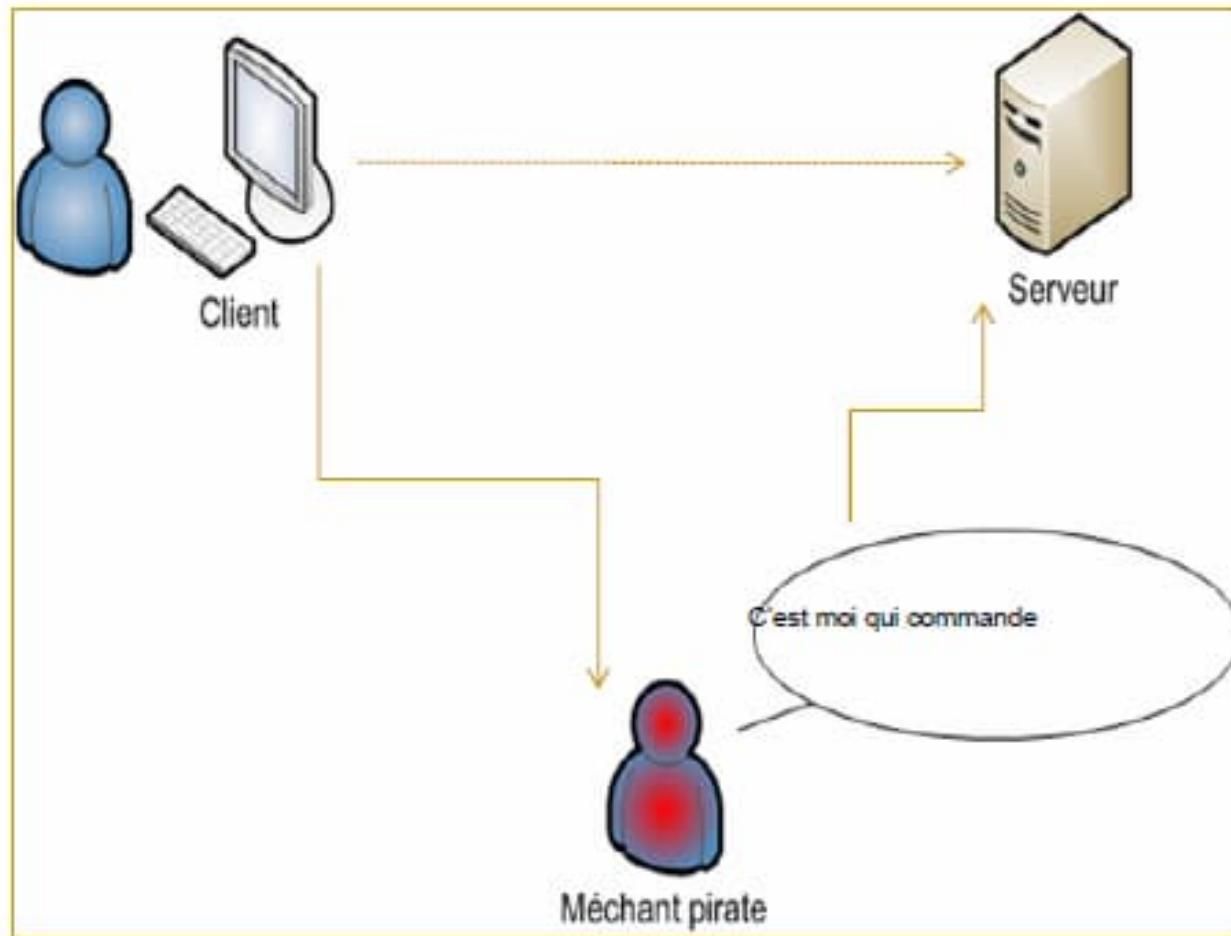
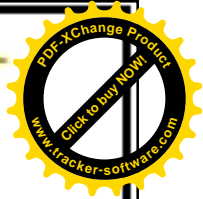


# Attaques actives (2)



- Man in the middle (home au milieu)

Consiste à disposer un point d'accès étranger dans à proximité des autres PA légitimes. Les stations désirant se connecter au réseau livreront au PA intrus leurs informations nécessaires à la connexion. Ces informations pourront être utilisées par une station pirate. Il suffit tout simplement à une station pirate écoutant le trafic, de récupérer l'adresse MAC d'une station légitime et de son PA, de générer une requête de désassociation et de s'intercaler au milieu.

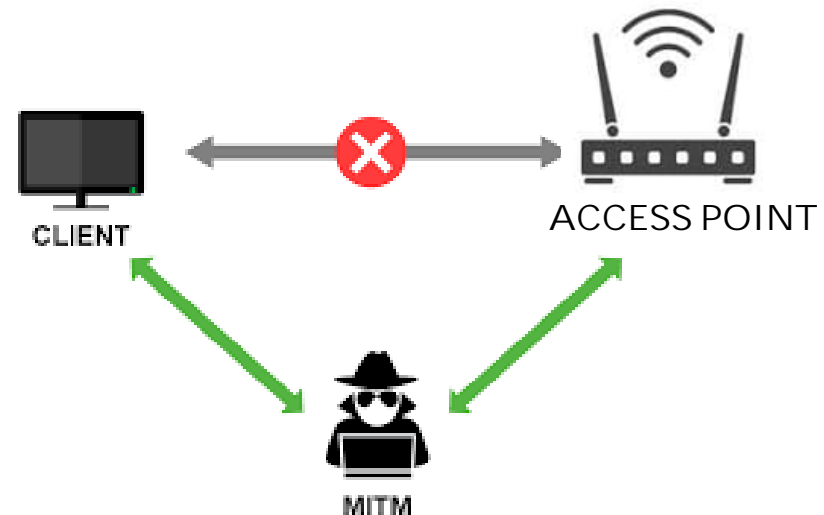




# MITM (Man In The Middle)

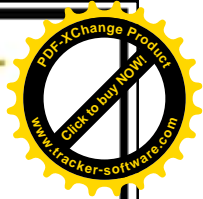
- ▶ L'attaquant **s'intercale** au milieu de la connexion entre l'AP et le client
- ▶ L'attaquant **relaie** les paquets entre le point d'accès et un client

➔ Il peut **écouter** le trafic, **d'injecter** des trames, de les **modifier** et **empêcher** les paquets d'atteindre leur destination.



# Man-In-The-Middle Attack



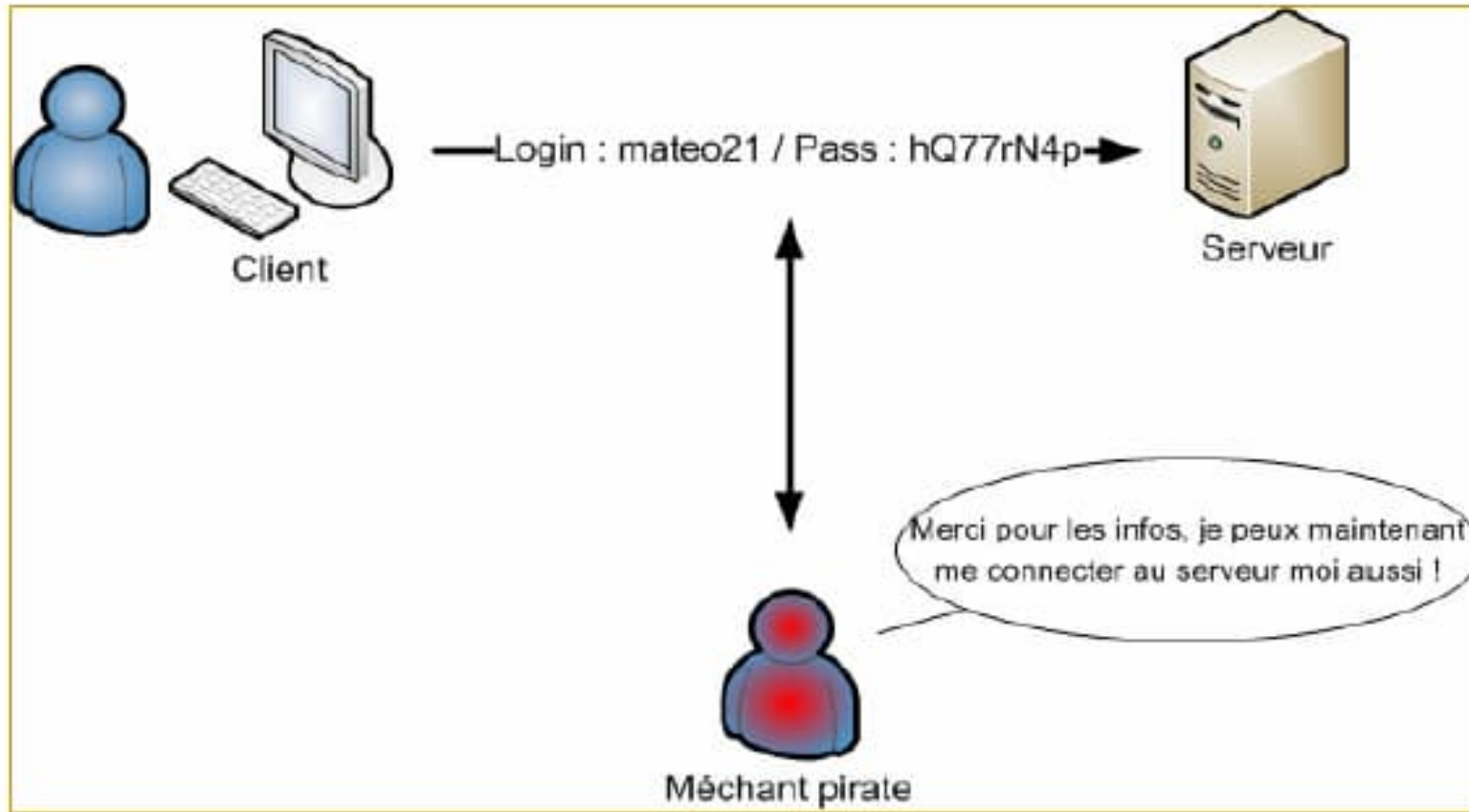


# Attaques actives (3)

- Spoofing (usurpation d'identité) :

Consiste à envoyer à une machine des paquets semblant provenir d'une adresse IP autre que celle de la machine du pirate (mascarade).

# Session Hijacking Attack



# Mauvaise configuration des AP



**SSID Broadcast**

Access points are configured to **broadcast SSIDs** to authorized users

**Weak Password**

To verify authorized users, network administrators **incorrectly use the SSIDs as passwords**

**Configuration Error**

SSID broadcasting is a configuration error that assists intruders to **steal an SSID** and have the AP assume they are allowed to connect

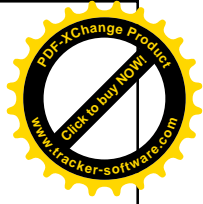
Connecting to **juggyboy**  
No password,  
Lucky Me!

**Attacker**



# Brute Force

- Le **Brute force** est un piratage cryptographique qui consiste à deviner les combinaisons possibles d'un mot de passe, clé, code,.... ciblé jusqu'à ce que le code ciblé correct soit découvert.
- Efficacité selon la longueur / complexité du mot de passe/clé/code,...
- Peut prendre beaucoup de temps
- Quelques outils de brute-forcing:
  - Aircrack-ng
  - John the Ripper
  - L0phtCrack
  - RainbowCrack

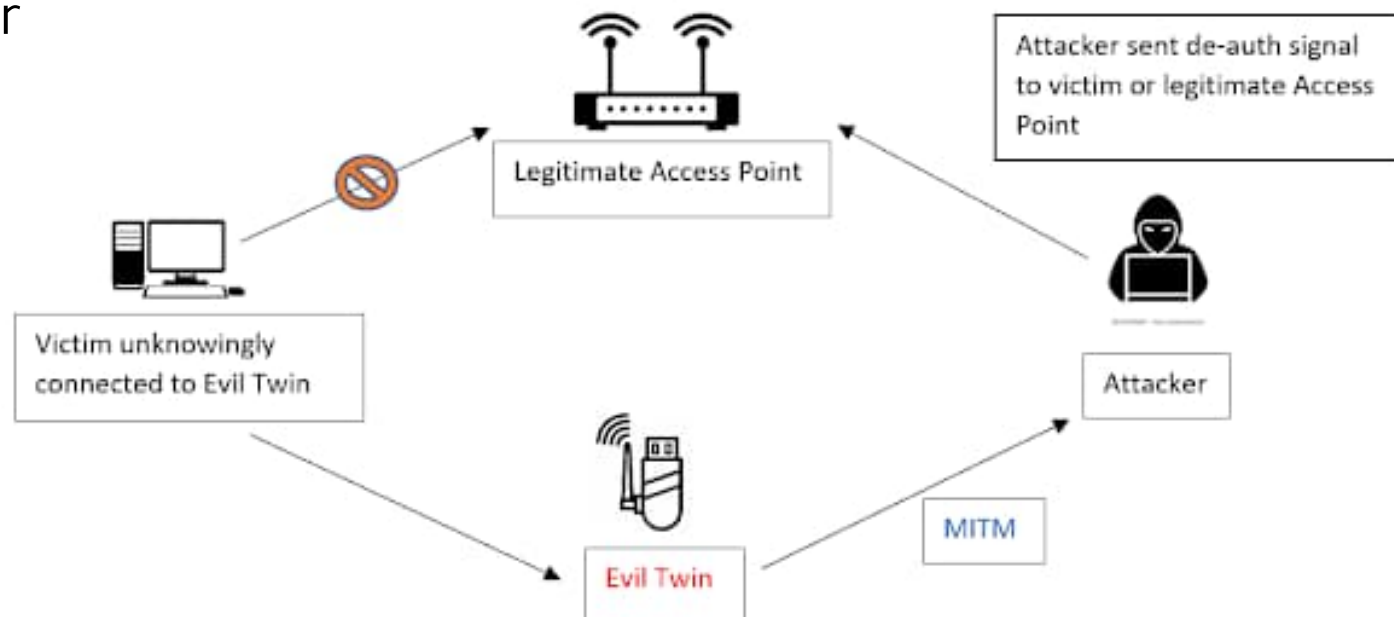


# Key Recovery

- Consiste à récupérer **la clé pré-partagée** utilisée pour s'associer à un réseau
- Peut être appelée sous d'autres noms: **Key Crack**, **Key hack**, ...
- Plusieurs techniques:
  - Exploiter les vulnérabilités d'un mécanisme d'authentification entre le client et le point d'accès
  - Analyse statistique sur le trafic de données cryptées à partir des trames capturées

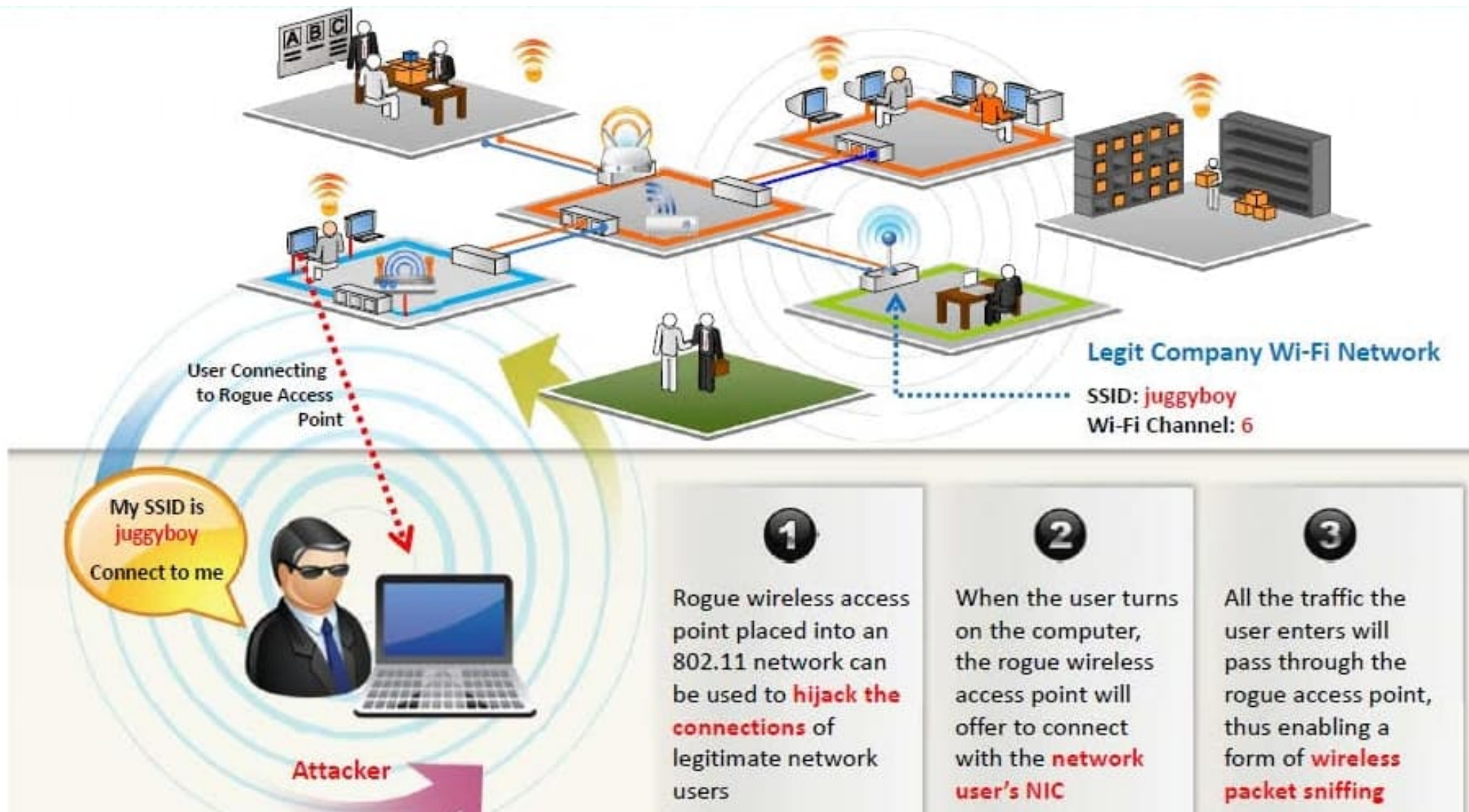
# Rogue AP

- ▶ L'attaquant met en place un point d'accès **non autorisé** ou **factice** (**Fake AP**) qui semble légitime à la station victime.
- ▶ On parle d'attaque **Evil Twin**, lorsque le réseau malveillant utilise le mêmes **MAC**, **BSSID** et **SSID** que le réseau cible
- ▶ L'attaquant amplifie le signal de manière à ce que la victime se connecte automatiquement au point d'accès non autorisé en raison de son balisage plus rapide et de sa portée élevée.
- ▶ L'attaquant envoie une trame de **désauthentification** pour obliger les clients de s'y connecter



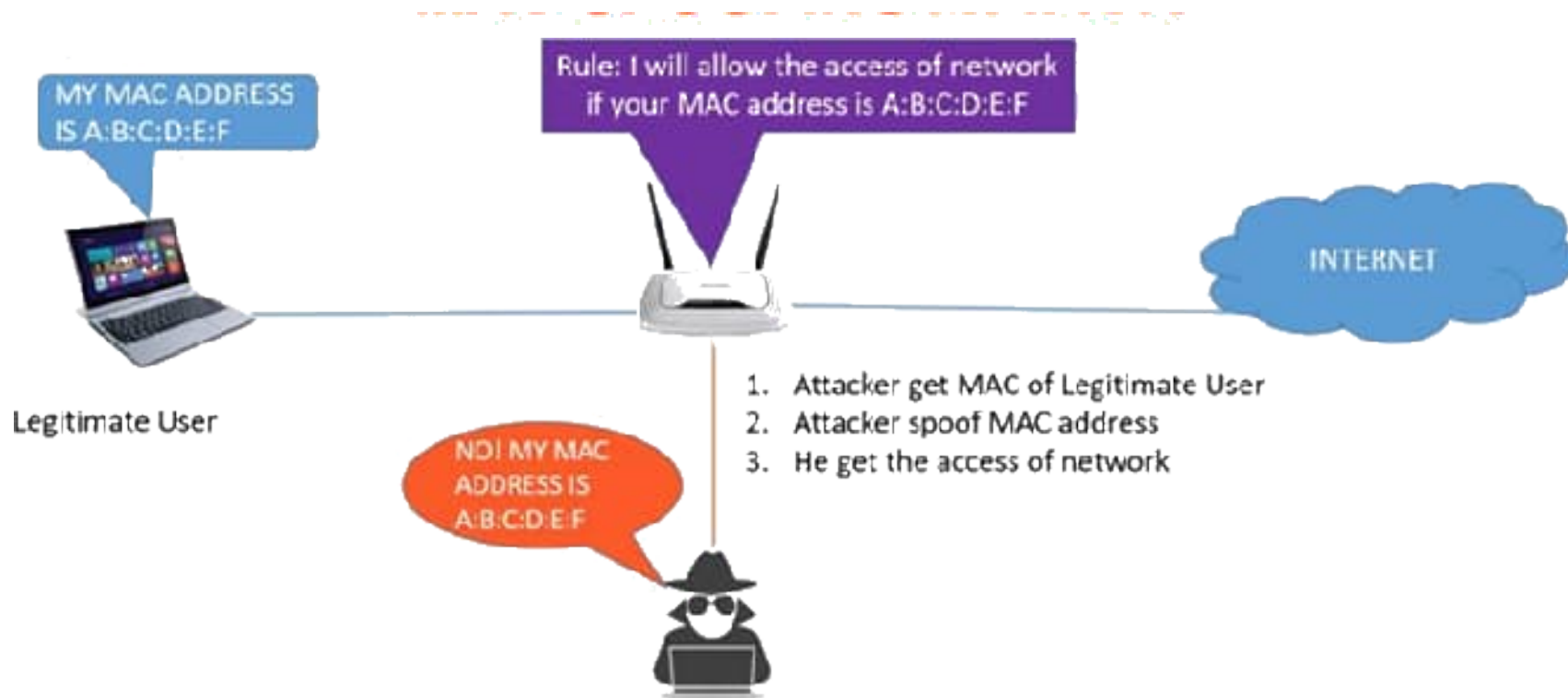


# Rogue AP Attack

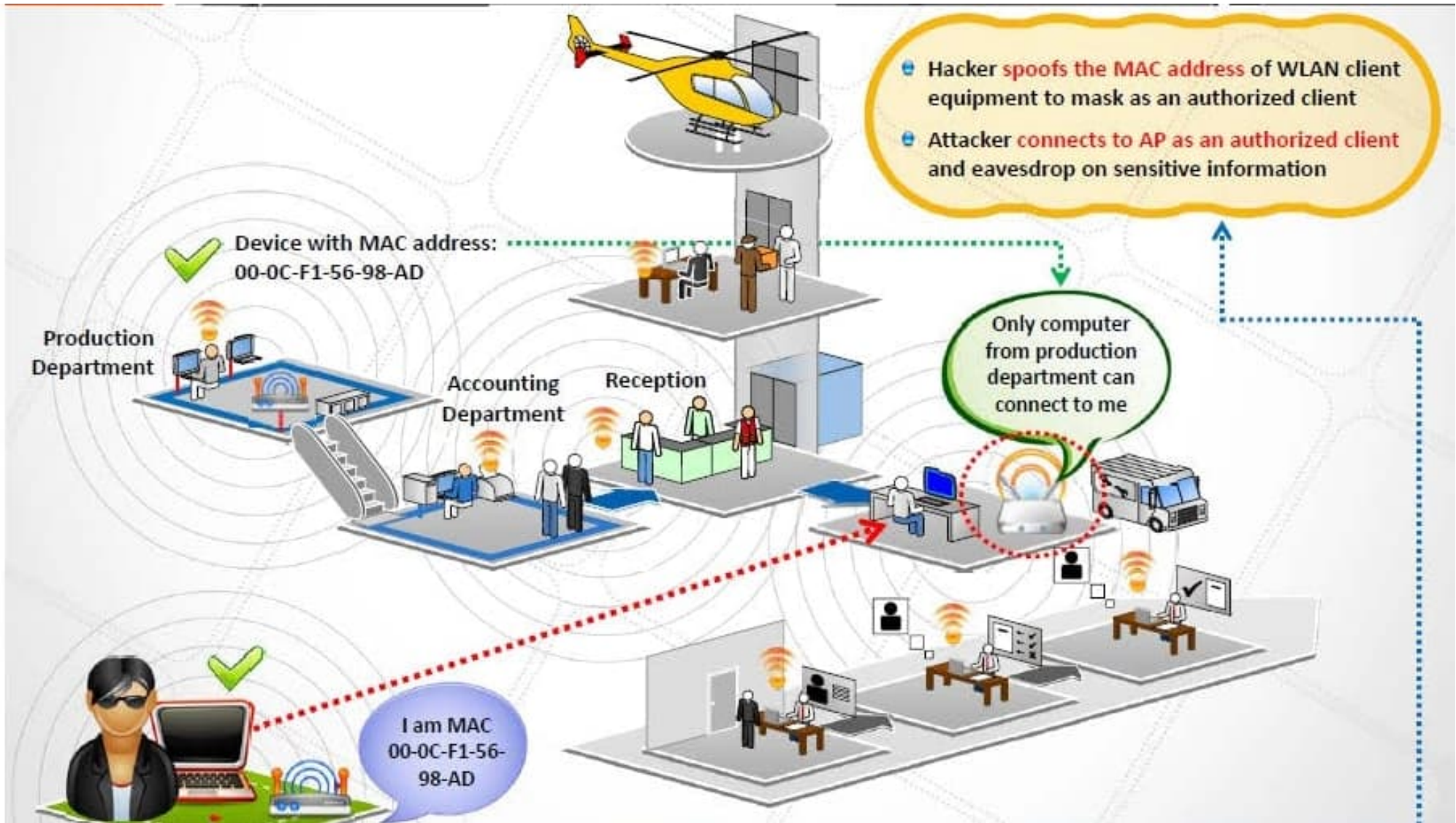


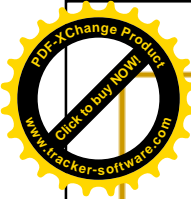
# MAC Spoofing

- ▶ Consiste à voler l'identité (adresse MAC) d'un client légitime



# MAC Spoofing Attack





# MAC Spoofing Attack (2)

MAC spoofing attackers **change the MAC address** to that of an authenticated user to bypass the MAC filtering configured in an access point

```
Linux Shell
[root@localhost root]# ifconfig wlan0 down
[root@localhost root]# ifconfig wlan0 hw ether 02:25:ab:4c:2a:bc
[root@localhost root]# ifconfig wlan0 up
```

Logging as root and disable the network interface

Enter the new MAC address

Bring the interface back up

Show Only Active Network Adapters

New Spoofed MAC Address: 00 - 05 - 56 - 55 - 88 - 56

360 SYSTEMS [000556]

Spoofed MAC Address: Not Spoofed

Active MAC Address: A4-BA-DB-FD-86-63

Network Connection: Local Area Connection

Hardware ID: pci\ven\_14e4dev\_1692subsys\_04261028

Update MAC	Remove MAC
Restart Adapter	IPConfig
Random	MAC List
Refresh	Exit

SMAC is a **MAC address changer** for Windows systems

**Randomly generate** any New MAC Address or based on a selected manufacturer





# Danger des stations nomades

- Les connexions aux hotspots sont généralement insécurisées
  - ➔ Les PCs mobiles connectés deviennent des proies faciles pour un pirate à proximité.
  - ➔ Deviennent d'excellents relais pour des attaques sur le site central.

Il est donc impératif de protéger es stations nomades pour se protéger elles-mêmes et pour protéger le site central (firewall individuel, communication à travers un VPN,...).



# Ethical Wireless Hacking Tools...





# Solutions élémentaires pour la sécurité

- Positionner intelligemment les points d'accès selon la zone que l'on souhaite couvrir.
- Protéger physiquement les PA (contre le vol, connexion directe, R.à.z,...)
- Réduire la puissance de la borne d'accès afin d'adapter sa portée à la zone à couvrir  
→ Bien choisir le type d'antenne utilisée

<u>Type</u>	<u>Locaux à desservir</u>
Verticale	Salles de réunion, bureaux
Dipôle	Couloirs (zones étroites et longues)
Sectorielle	Salles de réunion ou halls d'entrée
Yagi	Liaison entre bâtiments proches
Parabolique	Liaison entre immeubles éloignés

*Les différents types d'antennes pour réseaux sans fil*

# Types d'antennes



yagi



Verticale



Dipole



Sectorielle



Parabolique directionnelle





# Solutions élémentaires pour la sécurité(2)

- Eviter les valeurs par défaut :
    - ✓ mot de passe de l'administrateur pour la configuration du PA.
    - ✓ SSID afin de ne pas donner des éléments d'information sur la marque ou le modèle du PA.
    - ✓ Désactiver le DHCP.
    - ✓ Modifier le plan d'adressage...
  
  - Désactiver la diffusion de la beacon frame ➔ réseau fermé, cependant:
    - ✓ on ne peut pas fermer un réseau ad hoc
    - ✓ lors de l'association, le nom du SSID est transmis en clair.
  
  - Séparer le WLAN du reste du réseau (mise en place d'un firewall).
-



# Filtrage des adresses MAC

- Chaque PA permet de gérer une liste de droits d'accès (appelée ACL) basée sur les adresses MAC des équipements autorisés à se connecter au réseau sans fil.
- ☹ Ne résoud pas le problème de la confidentialité des échanges.
- ☹ Facilement contournable pour un utilisateur expérimenté (possibilité d'usurpation d'@ MAC pour certains pilotes de cartes réseau).



# Les mesures de sécurité WiFi

- ▶ Approfondir l'étude de **couverture** WiFi
  - ▶ Bien placer les AP
  - ▶ Réduire la puissance d'émission
  - ▶ Choisir les bonnes antennes radio
- ▶ Eviter les **valeurs par défaut**
  - ▶ Modifier **SSID, mots de passe admin**, adresse IP, DHCP, ...
  - ▶ Désactiver le Beacon Broadcast
- ▶ **Filtrage d'adresse MAC**
  - ▶ Configurer une liste d'adresses MAC autorisées / non autorisées au niveau du AP
  - ▶ Facilement contournable par un **MAC spoofing**
- ▶ Isoler le réseau WiFi du reste du réseau filaire (à travers des firewalls)
- ▶ Utiliser des systèmes de détection d'intrusion (IDS/WIDS : **Wireless Intusion Detection System**)



# Quelques éléments de sécurité

- ▶ Activité 1: Security Services Flashcards

[https://www.flippity.net/fc.php?k=15CX6tpEwLFZavgPNdSt\\_qna\\_u4d9yO\\_0jskxIMwjEmDs&t=match](https://www.flippity.net/fc.php?k=15CX6tpEwLFZavgPNdSt_qna_u4d9yO_0jskxIMwjEmDs&t=match)

- ▶ Activité 2: Security Mindmap

[https://miro.com/app/board/o9J\\_IG7Sx9c=](https://miro.com/app/board/o9J_IG7Sx9c=/)