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_lG7Sx9c=/
- 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_lGp8kLY=/
  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 maitriser 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 divulgation 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 internent
  - Introduction de serveur illicite dans le réseau

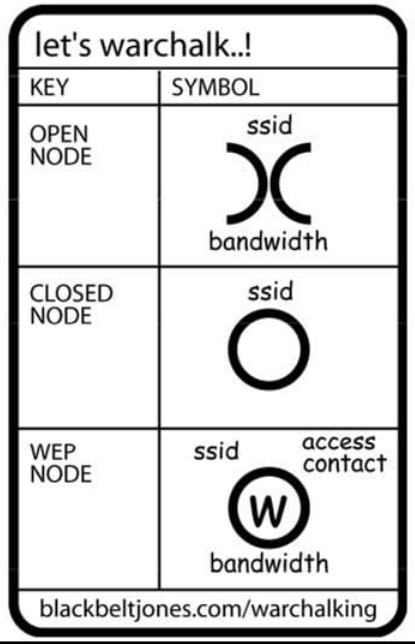
Le Wardriving

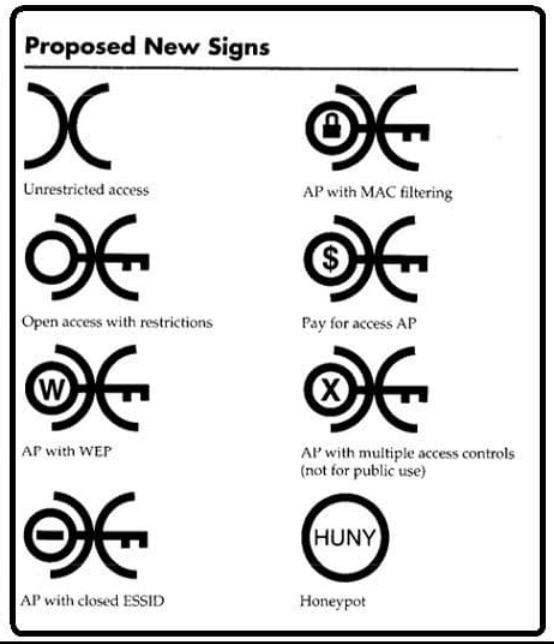
- Wardriving consiste à rechercher physiquement les réseaux sans fil présentant des vulnérabilités à partir d'un véhicule en mouvement et à cartographier les points d'accès sans fil.
- Equipements requis:
  - Outil d'écoute pour le Wardriving : iStumbler, KisMAC, CoWPAtty, InSSIDer, WiGLE, NetStumbler, 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 / promiscious).
  - Smartphone ou ordinateur portable

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.

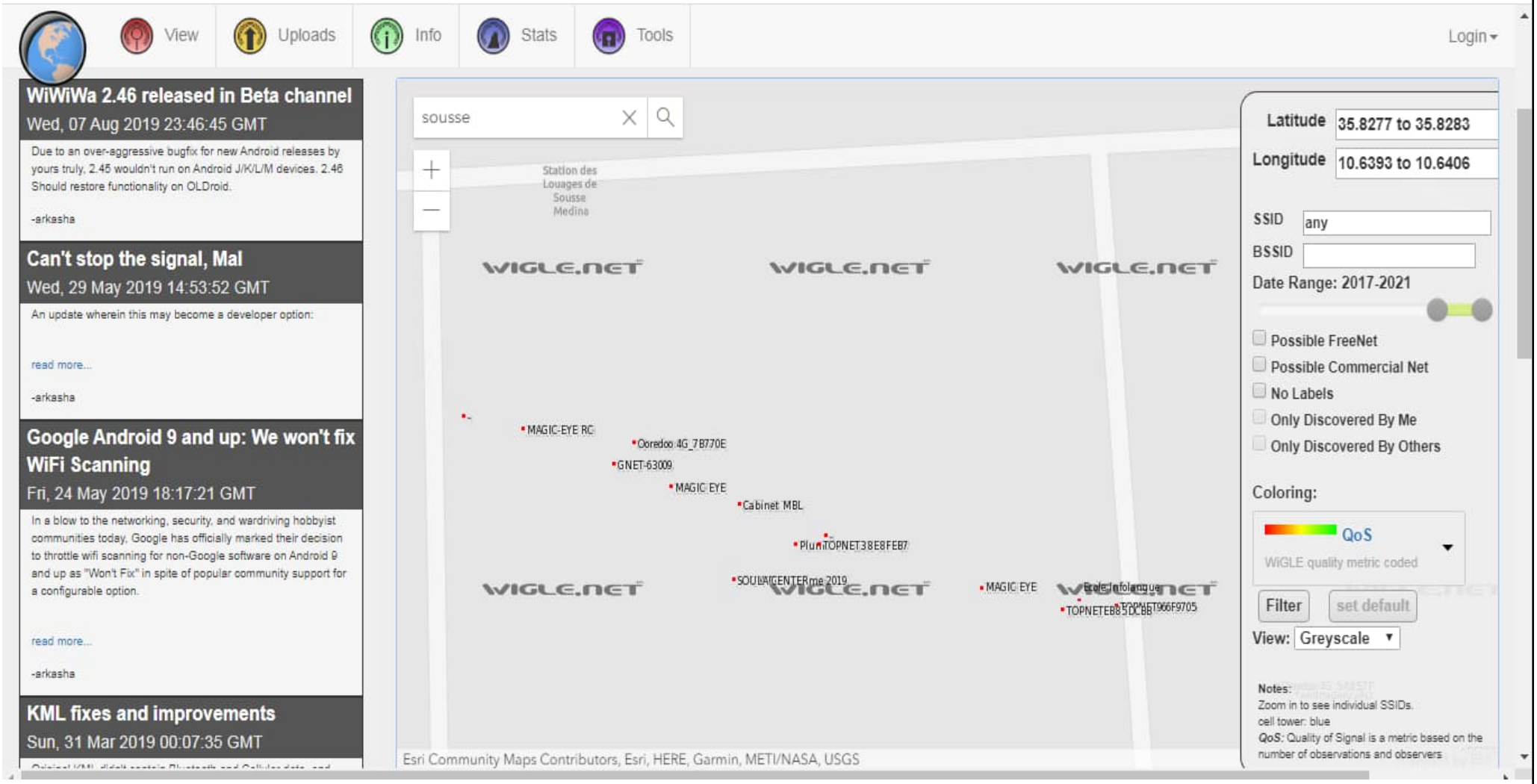
- Warchalking fournit des informations sur le type de connexion sans fil utilisé, qui peut être un nœud ouvert, un nœud fermé ou un nœud sécurisé
- Cela peut attirer les pirates et leur faire prendre conscience du point d'accès Wi-Fi et de sa sécurité.
- Les pirates peuvent utiliser ces informations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





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	



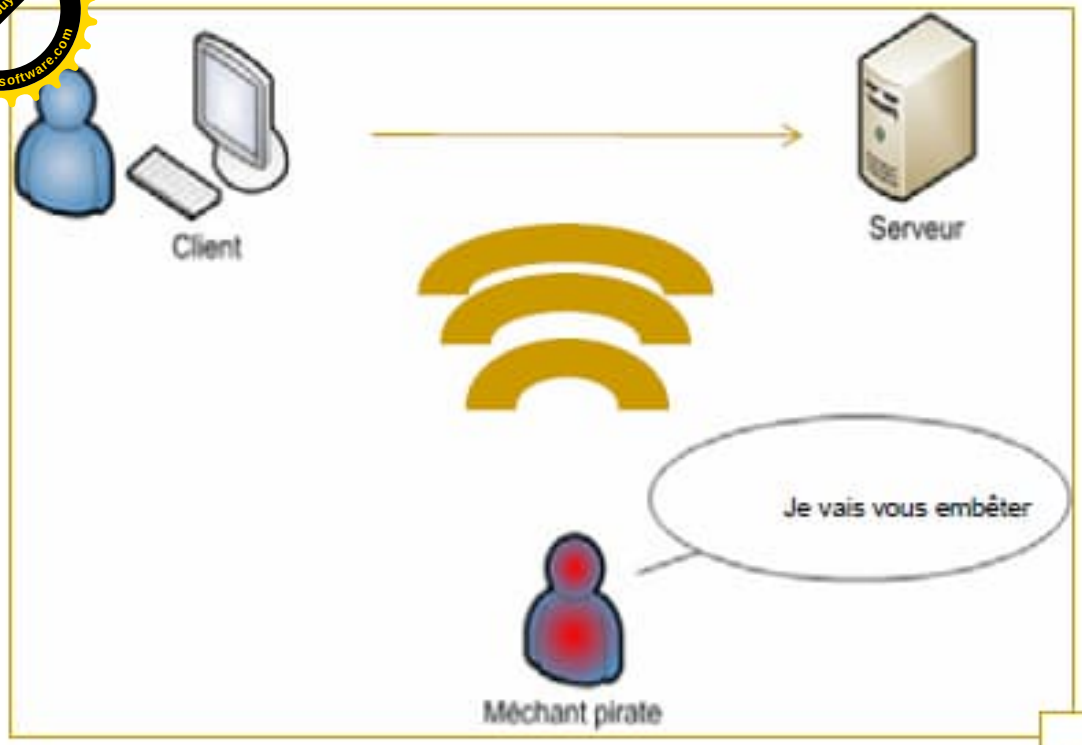
WarDriving tools

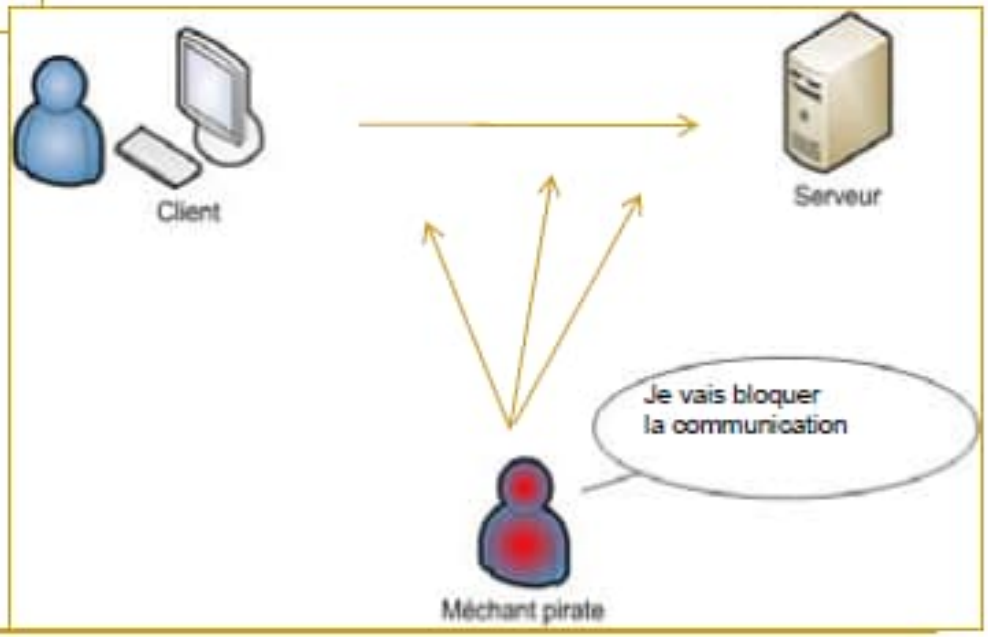
Attaques actives

- **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*.





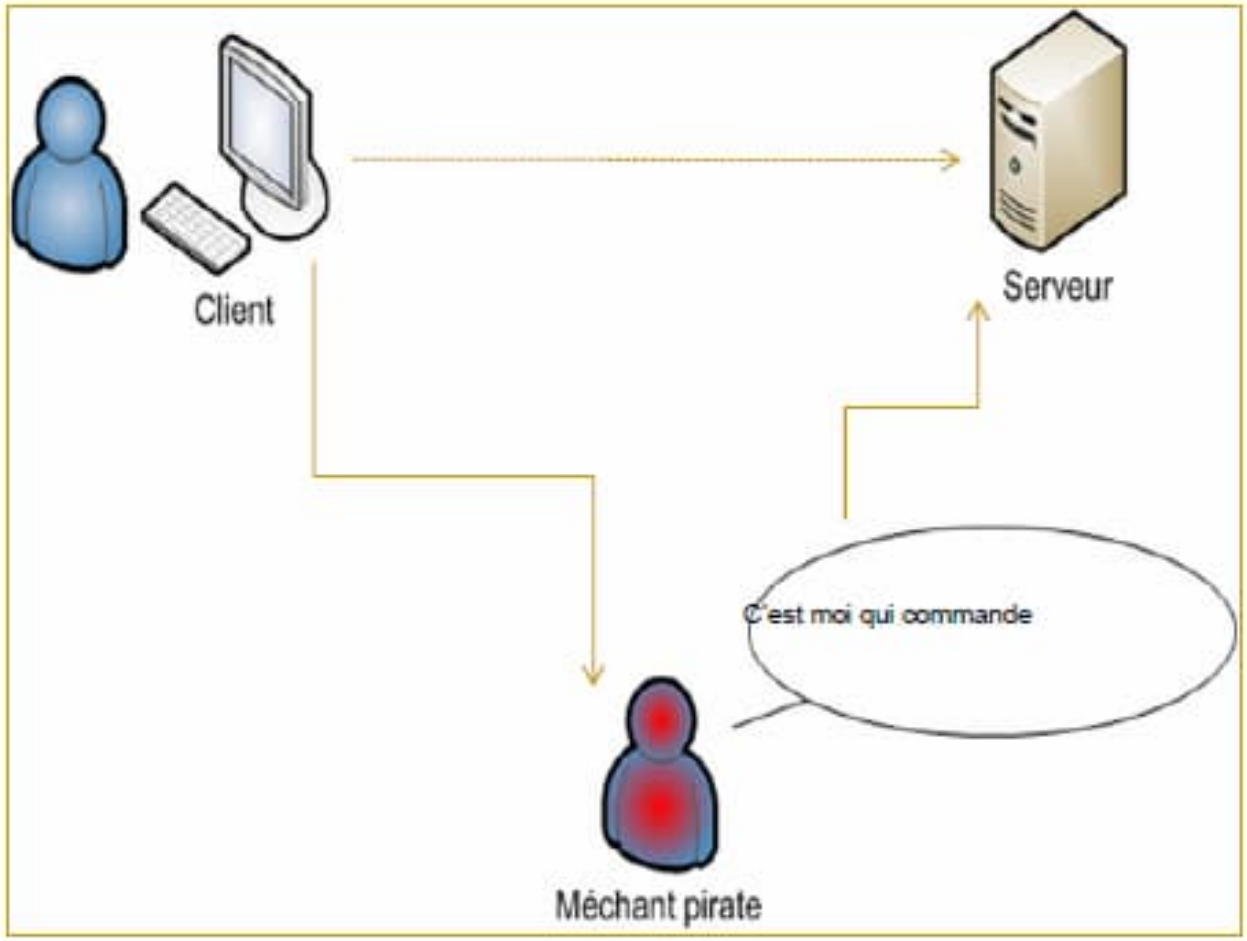
DoS (Denial Of Service)

- 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)

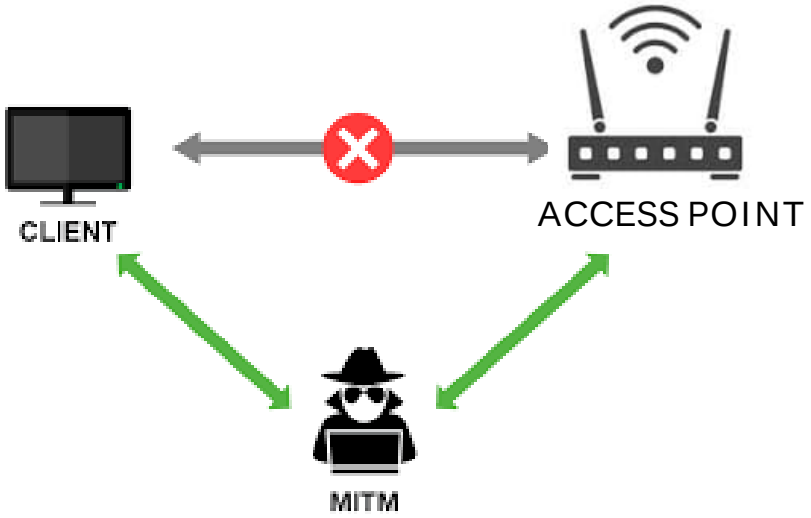
  Consiste à disposer un point d'accès étranger dans à proximité des autres PA légitimes. Les stations désirant se connecter au réseau livreront au PA intrus leurs informations nécessaires à la connexion. Ces informations pourront être utilisées par une station pirate. Il suffit tout simplement à une station 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.



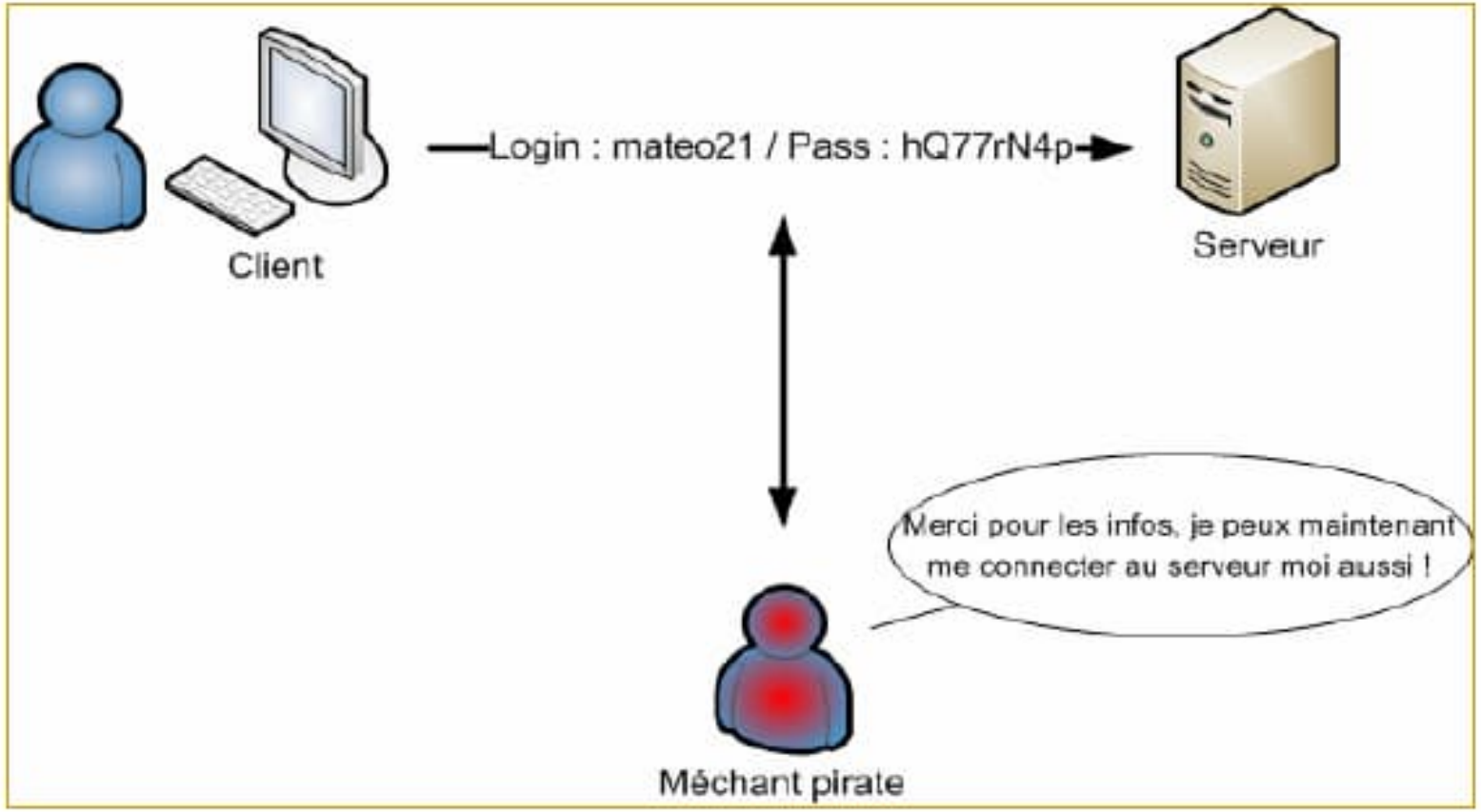
Man-In-The-Middle Attack

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

Brute Force

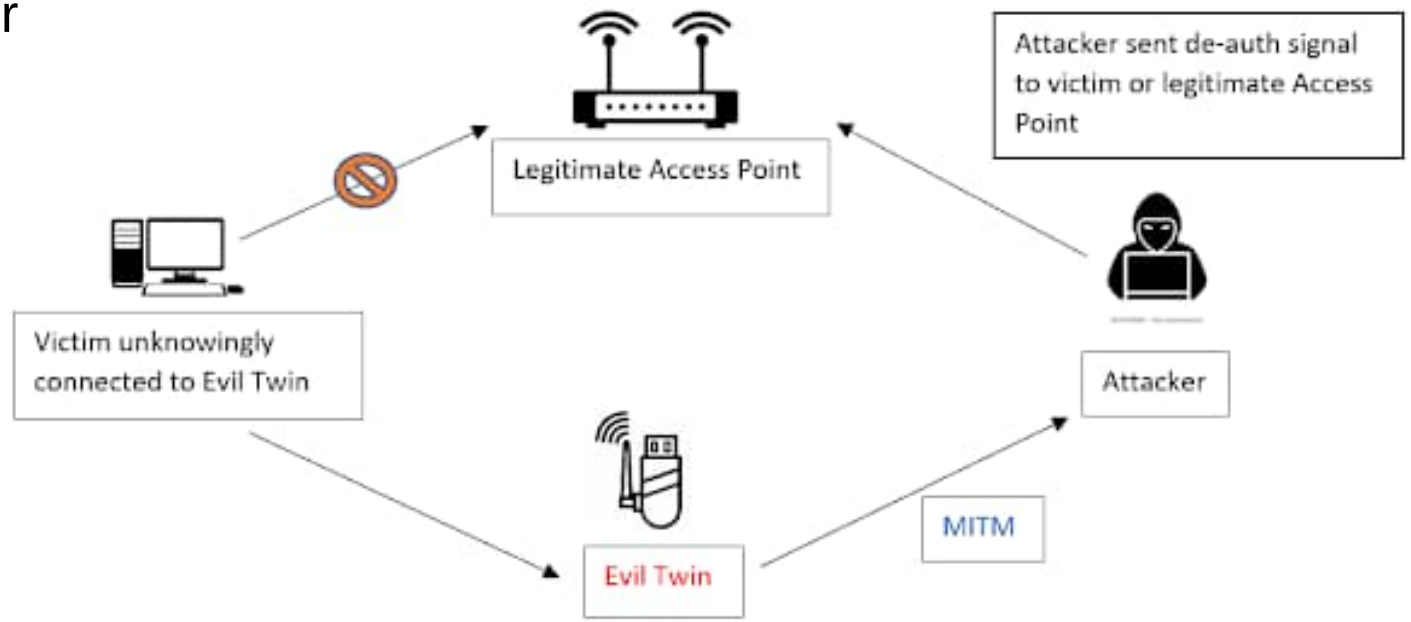
- Le Brute force est un piratage cryptographique qui consiste à deviner les combinaisons possibles d'un mot de passe, clé, code,…. ciblé jusqu'à ce que le code ciblé correct soit découvert.
- Efficacité selon la longueur / complexité du mot de passe / clé / code,…
- Peut prendre beaucoup de temps
- Quelques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

Key Recovery

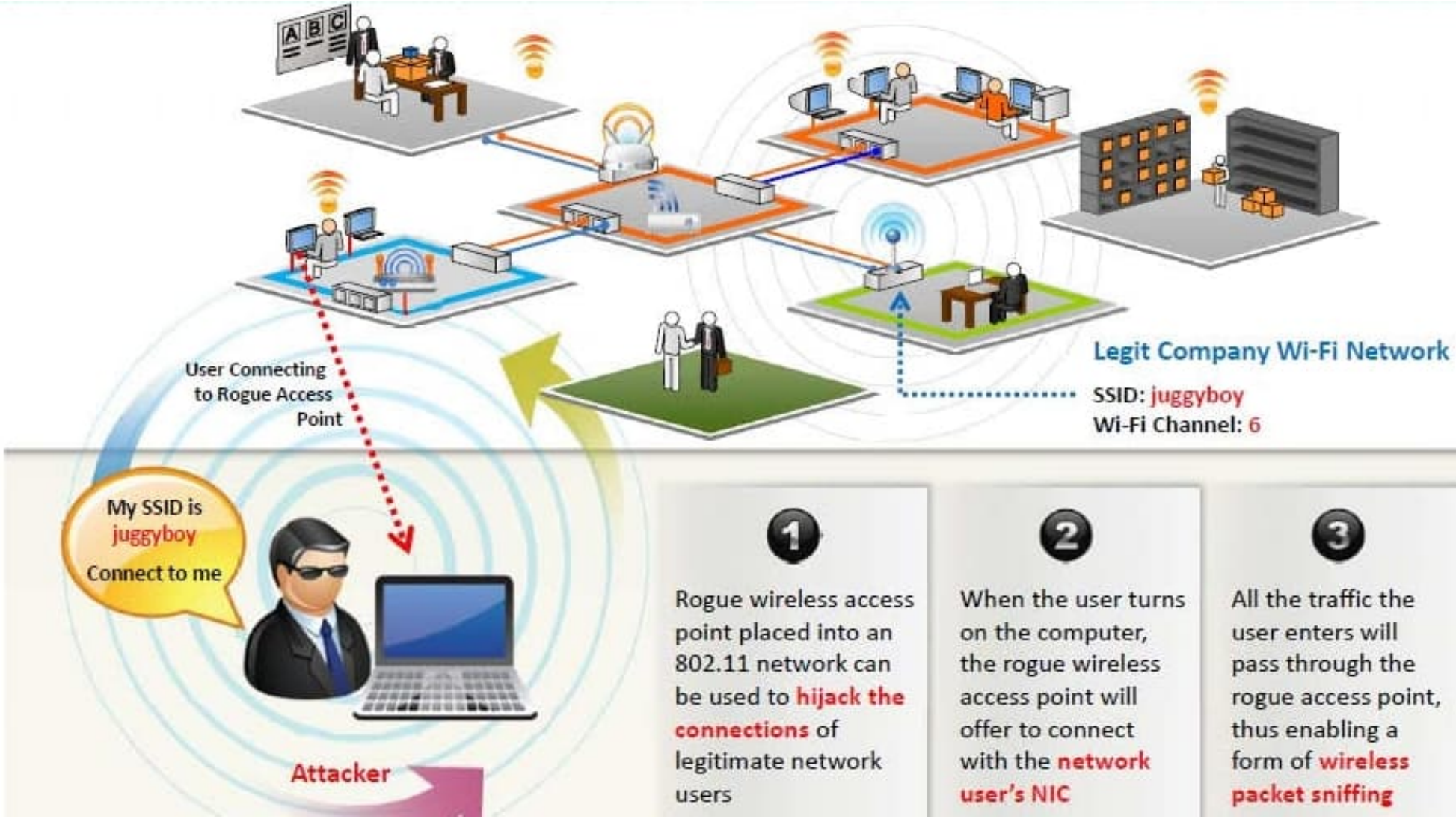
- Consiste à récupérer la clé pré-partagée utilisée pour s'associer à un réseau
- Peut âtre appelée sous d'autres noms: Key Crack, Key hack, …
- Plusieurs techniques:
  - Exploiter les vulnérabilités d'un mécanisme d'authentification entre le client et le point d'accès
  - Analyse statistique sur le 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



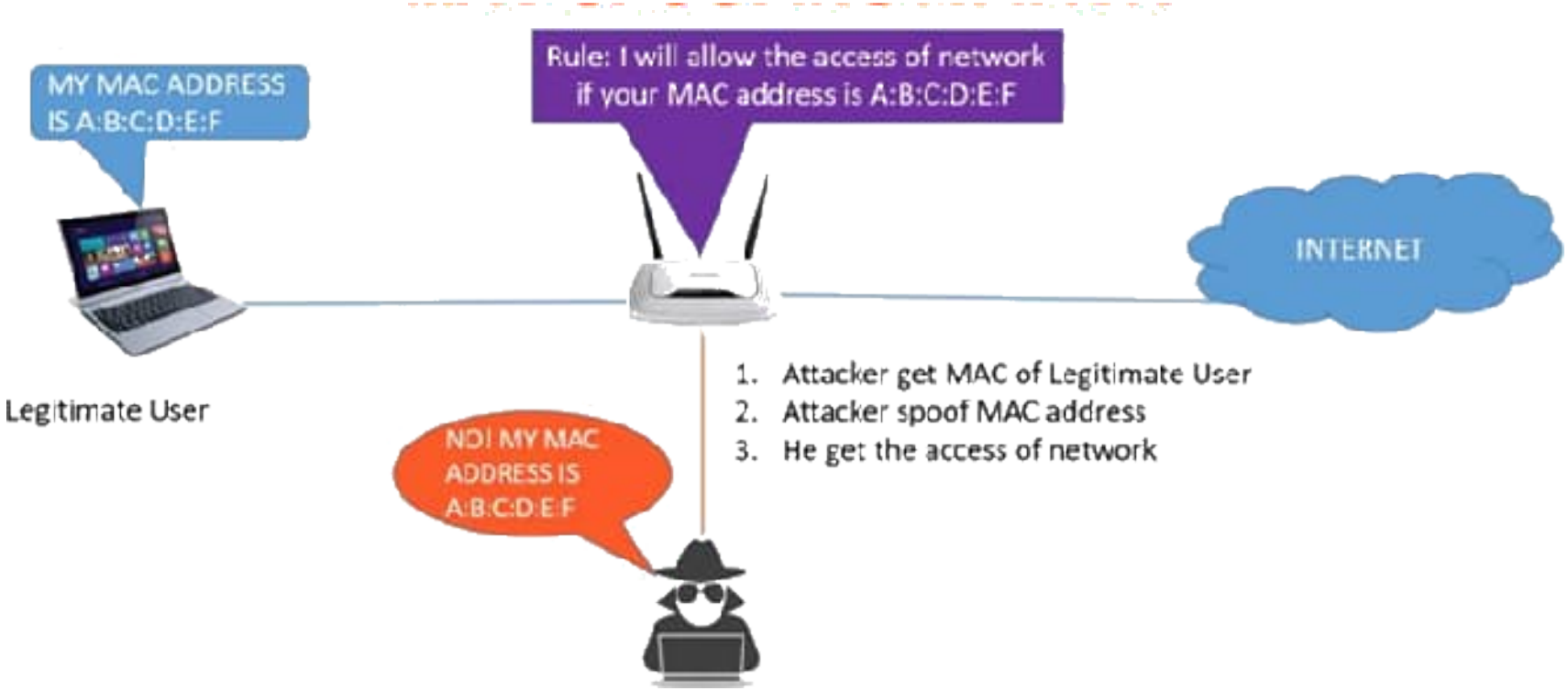
Rogue AP Attack



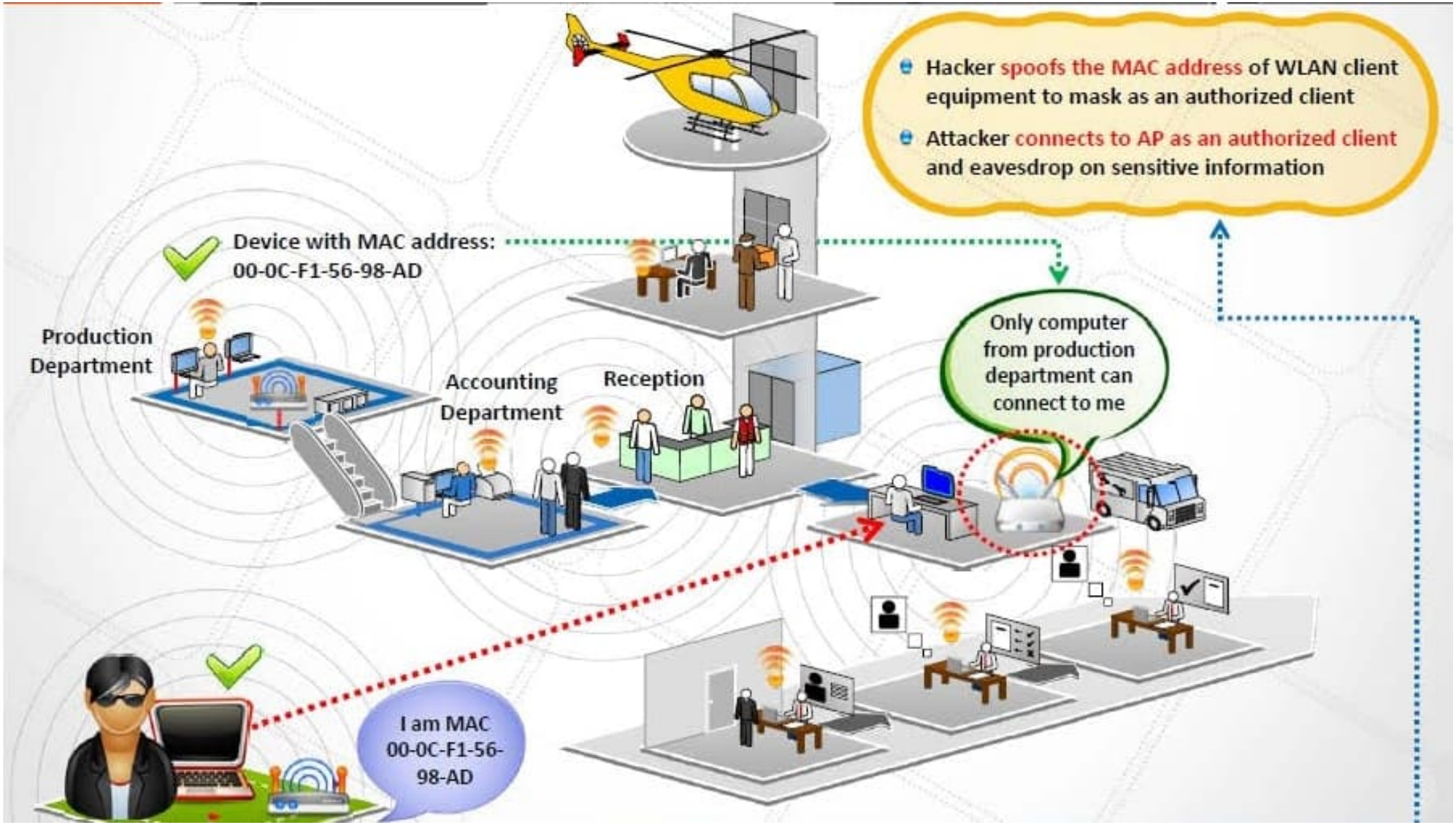
1. Rogue wireless access point placed into an 802.11 network can be used to **hijack the connections** of legitimate network users
2. When the user turns on the computer, the rogue wireless access point will offer to connect with the **network user's NIC**
3. All the traffic the user enters will pass through the rogue access point, thus enabling a form of **wireless packet sniffing**

MAC Spoofing

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

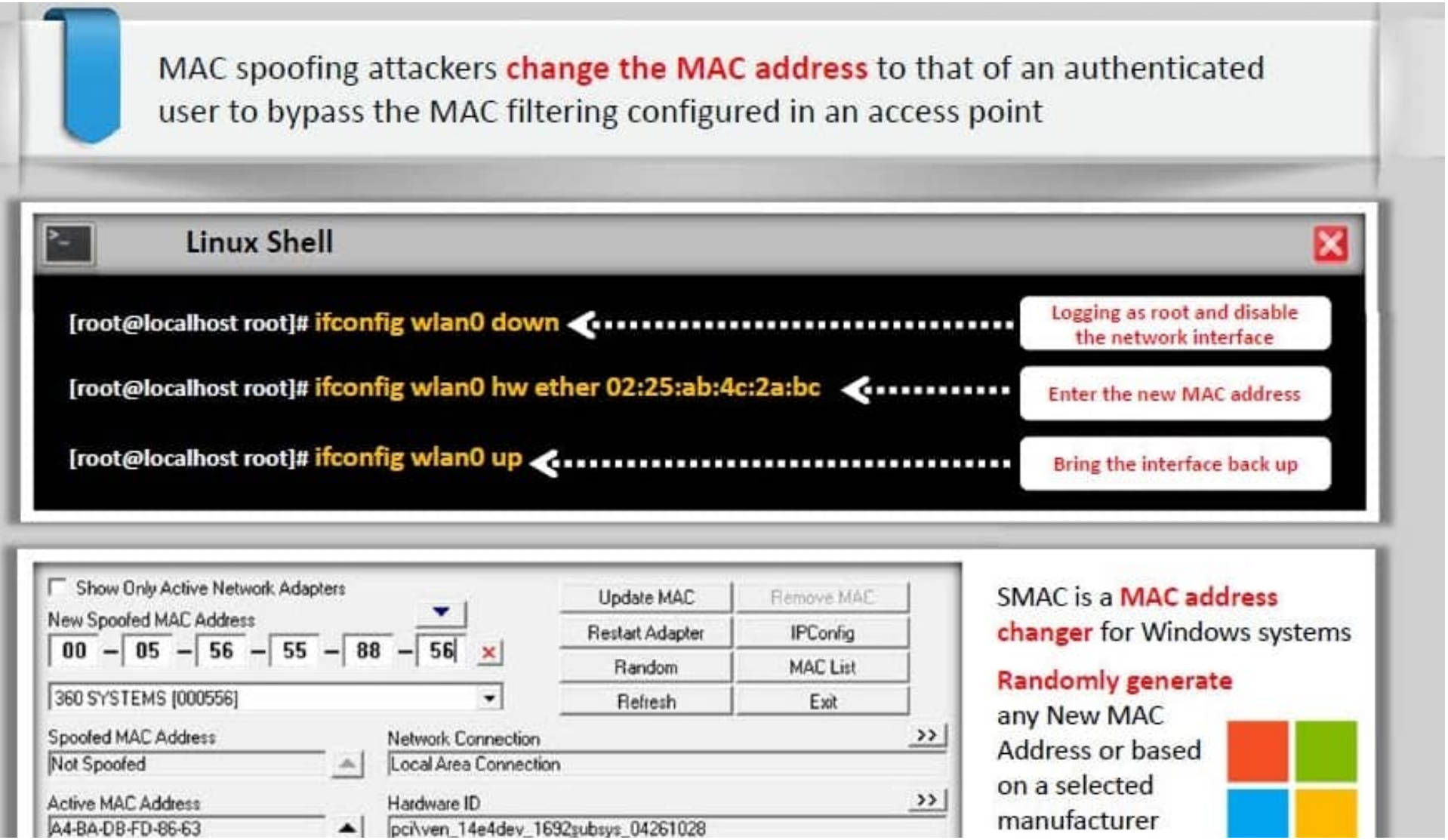


MAC Spoofing Attack



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



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

Type	Locaux à desservir
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_qnau4d9yO_0jskxIMwjEmDs&t=match

- Activité 2: Security Mindmap

  https://miro.com/app/board/o9J_IG7Sx9c=/