



# Sécurité des Réseaux WIFI

Par Stéphane Puybareau – Rotomalug  
[stephane@puybareau.com](mailto:stephane@puybareau.com)

# Le WIFI

- Norme de réseau sans fils haut débit
- Standard IEEE802.11
- Apparue en 1999
- Aujourd'hui, disponible partout

# Les systèmes sans fils

- PAN (Périphériques, faible portée (~10m))
  - Bluetooth  1 Mbps (3 Mbps)
  - WUSB  60MBps
- LAN (Ordinateurs, portée moyenne (~500m))
  - Wifi 54MBps
- MAN (Personnes, longue portés (>5km))
  - GSM / UMTS 64kBps / 384kBps
  - WIMAX 70MBps



# Avantages du WIFI

- Sans fil
- Facile à mettre en œuvre
- Portée adaptée à un petit bâtiment
- Débit comparable à un réseau local ethernet

# Inconvénients du WIFI

- Porté : supporte mal les obstacles
- Mobilité : problème de batterie, roaming...
- Sécurité

# La sécurité

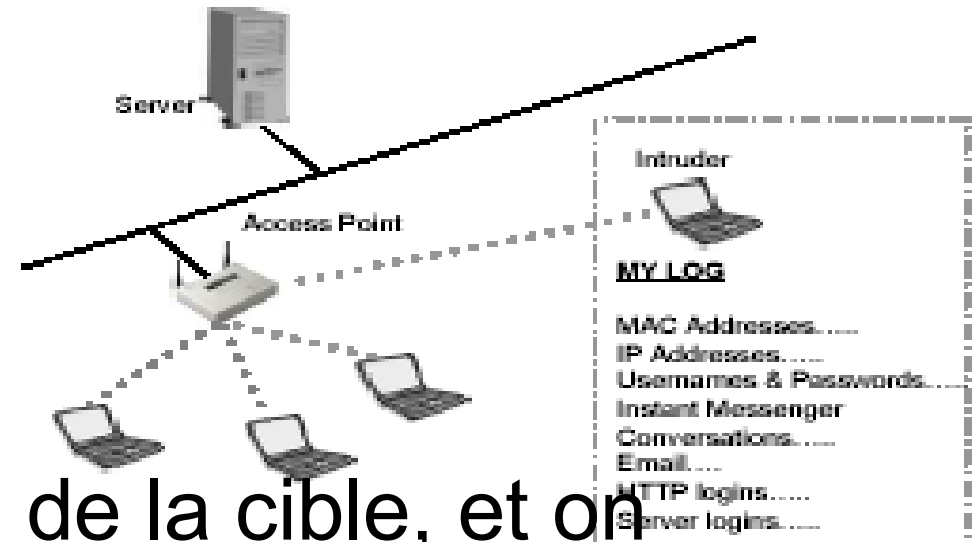
- Le problème :
  - On ne contrôle pas la diffusion des ondes

# Les risques possibles

- L'écoute passive
- L'accès aux ressources
- Le dénie de service
- Usurpation d'identité

# Les risques

- L'écoute passive



- On se met a proximité de la cible, et on écoute ses secrets

- Comme à la terrasse d'un café

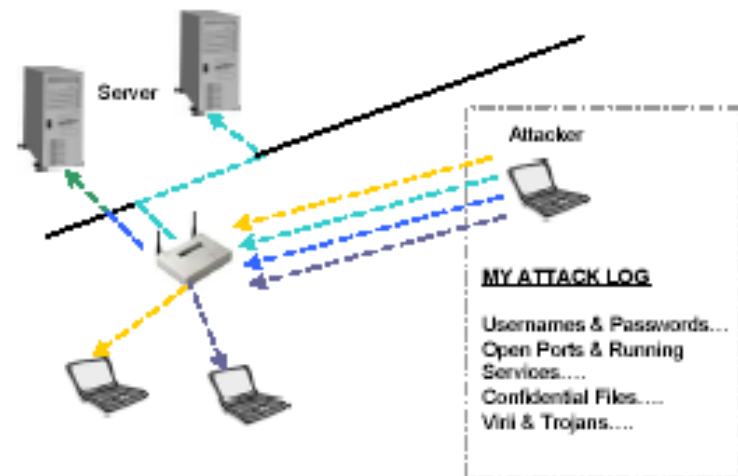
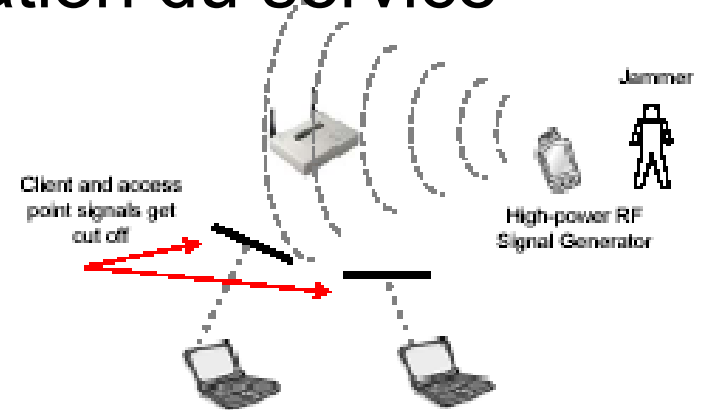
# Les risques

- Utilisation de vos ressources :
  - Puissance de calculs
  - Données
  - Connexion Internet
- C'est un classique vol

# Les risques

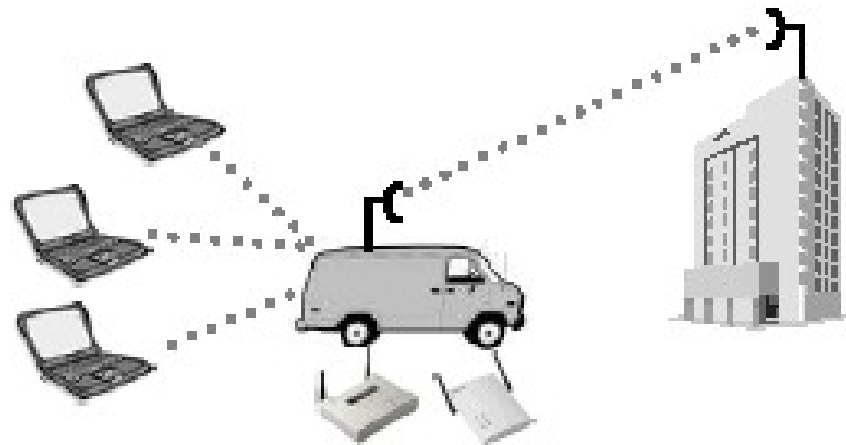
- Le dénie de service
  - Objectif : empêcher l'utilisation du service

- Méthodes :
  - Brouillage des fréquences
  - Déconfiguration



# Les risques

- Usurpation d'identité
  - Souvent dans le but de commettre un autre délit
  - Vols d'identité personnel
    - Connexion Internet
    - Données (Clé privé de signature)
  - Type "Man In the Middle"



# La loi

- En France :
  - LOI NUMERO 88-19 DU 5 JANVIER 1988  
RELATIVE A LA FRAUDE INFORMATIQUE

*"Quiconque, frauduleusement, aura accédé ou se sera maintenu dans tout ou partie d'un système de traitement automatisé de données sera puni d'un emprisonnement de 2 mois à un an et d'une amende de 2 000 F à 50 000 F ou de l'une de ces 2 peines seulement."*

# La loi

- On ne peut pas se connecter à un réseau sans y être invité
- Même si ce réseau n'est pas protégé

# Protections

- Évaluer la valeur de la cible pour bien évaluer le risque
- Exemple : un particulier risque rarement plus que le vol d'identité ou de connexion
- Exemple : une entreprise risque le vols de données, le vandalisme, le dénie de service

# Protections

- La meilleur des méthodes :
  - Rester en filaire !

# Protections

- Limiter la zone de couverture WIFI
  - Êtes vous sûr que vos commerciaux travaillent depuis le parking de votre entreprise ?
- Comment ?
  - Bien positionner les points d'accès
  - Utilisation d'antenne directionnel
  - Tapisser les murs de plomb ;-)

# Protections – Le Cryptage

- Plusieurs solutions :
  - Cryptage intégré au WIFI
  - Cryptage au dessus du WIFI
- Protège contre :
  - L'écoute passive
  - Le vol de ressources

# Protections – Le cryptage

## Cryptage intégré au WIFI

- Nécessite un matériel compatible
  - WEP :
    - Compatible avec tout
    - Cassé
  - WPA :
    - Plus sûr
    - Attention à la compatibilité

# Protections – Le cryptage

## Cryptage au dessus du WIFI

- On garde le WIFI non crypté, mais on crypte les données que l'on envois dessus
  - VPN
  - IPSec
  - SSL
- Sûr
- Nécessite de changer l'infrastructure

# Protections – L'authentification

- S'assurer de l'identité de la personne avec qui on communique
- Protège contre :
  - Le vol d'identité
  - Le vol de ressource

# Protections – L'authentification

- Solutions :
  - Par cryptage
  - Par adresse MAC :
    - Facilement contournable
  - Par 802.1X :
    - Compatibilité du matériel
  - Par sécurisation des applications :
    - Attention au vol de mot de passes ou de cookies

# Protections

- Le bien a protéger vaut-il l'énergie dépensé pour le protéger ?
  - Coût de mise en place de la protection
  - Coût d'utilisation au quotidien

# Merci

- Questions ?
  - Réponses ?
- Vous pouvez me contacter à l'adresse suivante :  
stephane@puybureau.com