



HERVÉ SCHAUER CONSULTANTS

Cabinet de Consultants en Sécurité Informatique depuis 1989

Spécialisé sur Unix, Windows, TCP/IP et Internet

Identifier les dangers liés à Internet

Mécanismes Wi-Fi et risques techniques

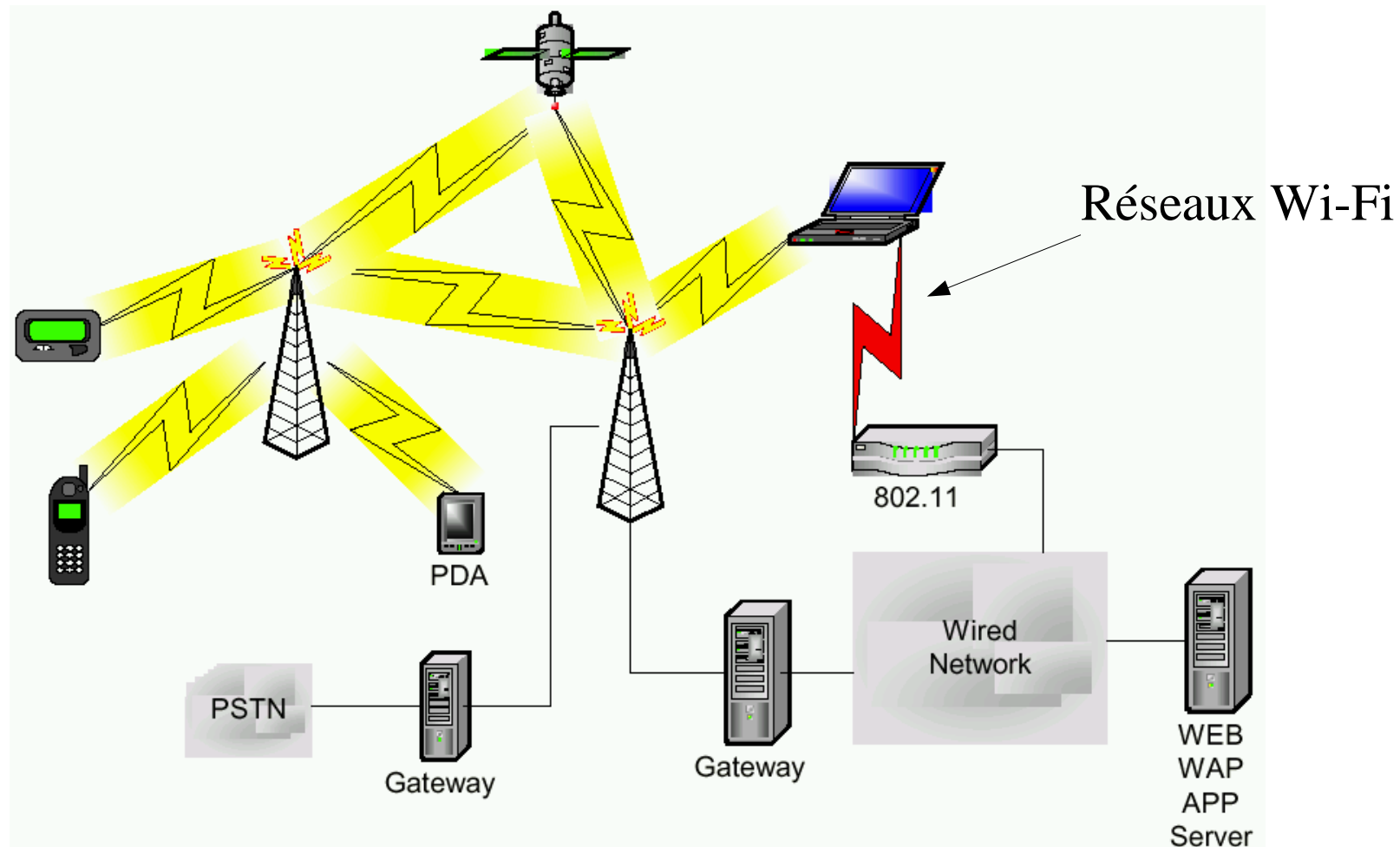
Jérôme Poggi

<Jerome.Poggi@hsc.fr>

Plan

- Principe des réseaux sans fil
 - Technologies
- Risques des réseaux sans fil
 - Attaques radio
 - Attaques réseaux
- Méthodes de détections
- Outils
- Antennes

Localisation des réseaux sans fil dans le paysage numérique



Technologies WLAN

- IEEE 802.11b (Wi-Fi), sur 2,4 GHz, 11 Mb/s
 - La principale technologie, disponible depuis 1997
- IEEE 802.11a (Wi-Fi5), sur 5 GHz, 54 Mb/s
 - Disponible depuis fin 2001
- IEEE 802.11g, IEEE 802.11e
 - Remplaceront respectivement IEEE 802.11b et IEEE 802.11a
 - Non disponible sur le marché
 - 802.11g prévue fin 2002
 - Possibilité de mise à jour logicielle de 802.11b vers 802.11g
 - Qualité de service définie dans IEEE 802.11f
 - Gestion dynamique puissance / fréquences dans IEEE 802.11h

Rappel de loi et vocabulaire



- Avertissement :

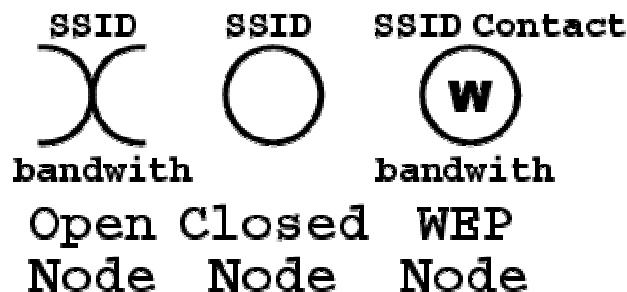
Auditer, surveiller, écouter, faire du wardriving sur un réseau, qui ne vous appartient pas, est illégal.

- Warchalking

- Marquage de réseau sans fil

- Wardriving

- Extension du WarDialing
- Recherche de réseaux sans fil depuis une voiture



Risques

Interception du trafic

- Avec un scanner passif
 - Kismet, WifiScanner, PrismStumbler ...
- Avec un scanner actif
 - Netstumbler, dstumbler
 - Outils commerciaux
- Avec une simple carte PCMCIA
 - Association à la borne
 - Écoute classique du réseau
 - Tcpcap, ethereal ...
- Vol d'informations

Risques

- Introduction illicite dans le système d'information
 - Comment ?
 - Association
 - Simple, avec usurpation d'identité
 - Attaque d'un poste autorisé
 - Pénétration des système d'information par rebond
 - Attaque de l'intercepteur (*man in the middle*)
 - Utilisation de AirJack (<http://802.11ninja.net/>)
 - Fausse borne
- Vol d'informations, destructions, modifications ...
- Dégradation de l'image de marque

Risques

Attaque par rebond

- Responsabilité juridique du dernier tiers identifiable

Dénis de services

- Perturbation des fréquences
 - Micro-ondes, moteurs, ...
 - Bornes avec antenne
- Perturbation du fonctionnement du réseau
 - Usurpation de borne
 - Usurpation de signaux de contrôle ou d'administration

Auditer et surveiller

- Auditer les réseaux sans fil
 - Détection des équipements non maîtrisés
 - Ordinateur portable avec carte intégré
 - Borne sauvage ou pirate
 - Mobilité désiré
 - Passerelle de transport d'information hors du périmètre
- Surveiller ses équipements et réseaux
 - Comptabiliser ses équipements
 - Être réactif et détecter
 - Tentative d'attaques
 - Utilisation de sondes

Surveillance et recherche

Comment surveiller ?

- Détecter toute évolution du périmètre radio
 - Nouveaux équipements
- Détecter les événements « anormaux »
 - Recherche d'équipements radio
 - Signature de certains logiciels
 - Netstumbler
 - Dstumbler
 - Windows XP
 - Usurpations d'identité
 - Étude des champs 802.11b
 - Emplacement géographique des équipements

Surveillance et recherche

Quoi surveiller ?

- **Trafic réseau filaire**
 - Débits anormaux, Scans de ports
 - Signatures d'attaque
 - Partie filaire des équipements radio
- **Trafic réseau sans fil**
 - Association / Désassociation
 - Échecs d'authentification
 - Tentatives de connexions aux équipements radio
 - Bornes
 - Tentatives de connexion aux équipements d'authentification
 - Radius, Passerelle Web ...

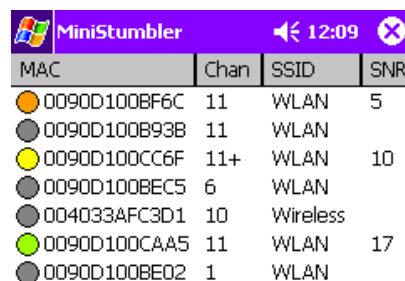
Surveillance et recherche

Quand ?

- Surveillance constante
 - Remontée d'alarme
 - Plan d'intervention
 - Informatique
 - Bloquer les accès
 - Éviter le dénis de service
 - Physique
 - Rechercher la source
 - Dépôts de plainte
 - Intervention d'un cabinet extérieur compétant
- Détection ponctuelle
 - Utilisation d'assistants personnels

Outils d'audit

- Solutions portable
 - IPacq
 - Windows CE
 - MiniStumbler
 - Kit batterie
 - Sharp Zaurus
 - Linux
 - Kismet
 - Batterie supplémentaire
- Discret



MAC	Chan	SSID	SNR
0090D100BF6C	11	WLAN	5
0090D100B93B	11	WLAN	
0090D100CC6F	11+	WLAN	10
0090D100BEC5	6	WLAN	
004033AFC3D1	10	Wireless	
0090D100CAA5	11	WLAN	17
0090D100BE02	1	WLAN	



Outils d'audit

```
dragom@gir.lan.nerv-un.net:~$ nmap
Networks--(Autofit)--
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| Name      | T W Ch | Packets | Flags |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| + St Francis | G N 07 | 324     |      | 0.0.0.0 |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |
| VBHOUND     | A Y 11 | 48      |      | 0.0.0.0 |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |
| + Cenhud-PDK | G N 06 | 339     |      | 0.0.0.0 |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |
| <no ssid>   | A N 01 | 1508    | U3    | 10.132.112.0 |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |
| cvsretail   | A N 11 | 1091    |      | 0.0.0.0 |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |
| + IBM-PDK    | G Y 00 | 432     |      | 0.0.0.0 |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |
| pserwap003  | A Y 07 | 56      |      | 0.0.0.0 |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |
| linksys     | A Y 06 | 155     |      | 0.0.0.0 |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |
| <no ssid>   | A Y 11 | 175     |      | 0.0.0.0 |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |
| tsunamisgt3624t | A N 06 | 4       |      | 0.0.0.0 |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |
| <no ssid>   | A Y 06 | 58      |      | 0.0.0.0 |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |
| default     | A N 11 | 284     |      | 0.0.0.0 |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |
| arlington   | A N 06 | 15      |      | 0.0.0.0 |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |
| linksys     | A Y 06 | 91      |      | 0.0.0.0 |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |
| LucHomeNet  | A Y 06 | 1107    |      | 0.0.0.0 |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |
| . linksys   | A N 02 | 107     |      | 0.0.0.0 |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |
| ! CPT_Wireless | A N 01 | 170     |      | 0.0.0.0 |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |
| ! WLAN     | A N 11 | 22      |      | 0.0.0.0 |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| Info:      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |
| Ntwrks    | 22   |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |
| Pckets    | 6148 |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |
| Cryptd    | 386  |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |
| Weak      | 0    |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |
| Noise     | 0    |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |
| Discrd    | 1448 |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| Elapsed   | 000203 |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
Status:
Detected new network "WaveLAN Network" bssid 00:02:2D:22:86:C1 WEP N Ch 10 @
Detected new network "WLAN" bssid 00:90:D1:00:D9:57 WEP N Ch 11 @ 11.00 mbit
Detected new network "CPT_Wireless" bssid 00:02:2D:0D:D4:C0 WEP N Ch 1 @ 11.
Detected new network "linksys" bssid 00:04:5A:DD:56:0F WEP N Ch 2 @ 11.00 mb
```

- Windows
 - Netstumbler
 - Kismet (avec Cygwin)

- *BSD

- BSDairtools
 - Dstumbler
 - Dwepcrack
 - Prism2dump

```
ATERM<9>
> [10] nss (linksys) bssid:00:04:5a:dd:56:0f
  bssid: 00:04:5a:dd:56:0f
  mfg: Linksys
  Channel: 10 11.0/100
  Signal/Noise: 87/114/27
  First Seen: 3:25:36
  Last Seen: 3:27:52

> [109090] (lucme) bssid:00:02:2d:0d:d4:c0
  [373390] (nss) bssid:00:02:2d:0d:d4:c0
  basic navigation ]
+/-] up/down
</>] node up/down
u/d] page up/down
e/h] end/home
n/s] next/sort
a/r] refresh/resolve
o/l] open/audio
n/k] next/fresh
c/] comment/comment

file commands:
[1/b] load/dump
[q] quit

[ dstumbler v1.0 by hikari - (c) Dachboden Labs 2001 ]
```

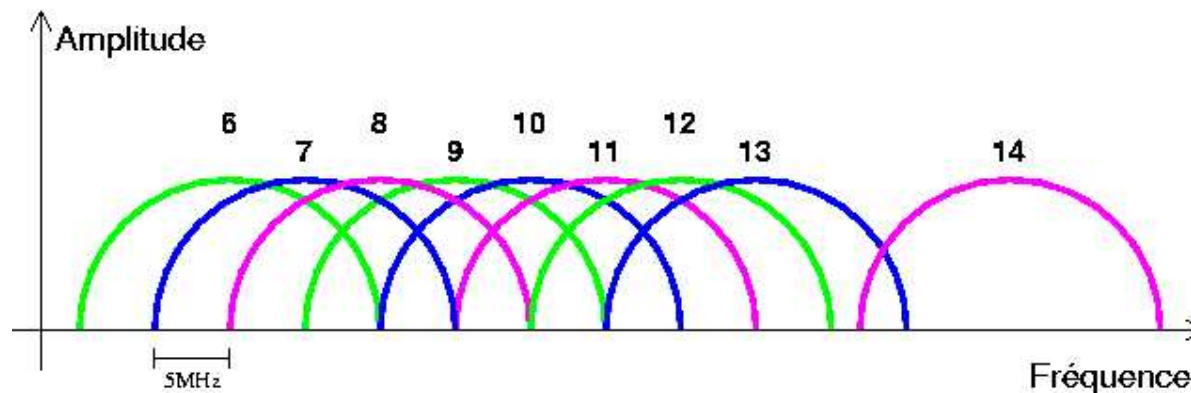
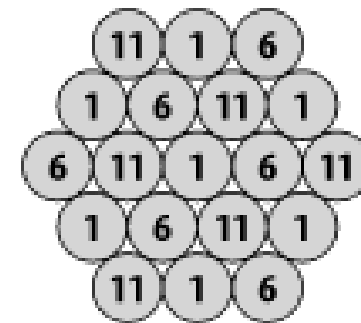
Outils d'audit Linux

- Kismet
 - <http://www.kismetwireless.net/>
- WiFiScanner
 - <http://wifiscanner.sf.net/>
- Mognet (java)
 - <http://chocobospore.org/mognet/>
- Airtraf
 - <http://airtraf.sf.net/>
- Wellenreiter (perl)
 - <http://www.remote-exploit.org/>

Répartition du spectre

14 Canaux / 14 fréquences de porteuse

- Espacement de 5 Mhz entre les canaux
- Porteuse de 2412 Mhz à 2484 Mhz
 - Canal 14 et 13 espacé de 12 Mhz
 - Bande passante de 22Mhz
- Réglementation stricte en France



Antennes

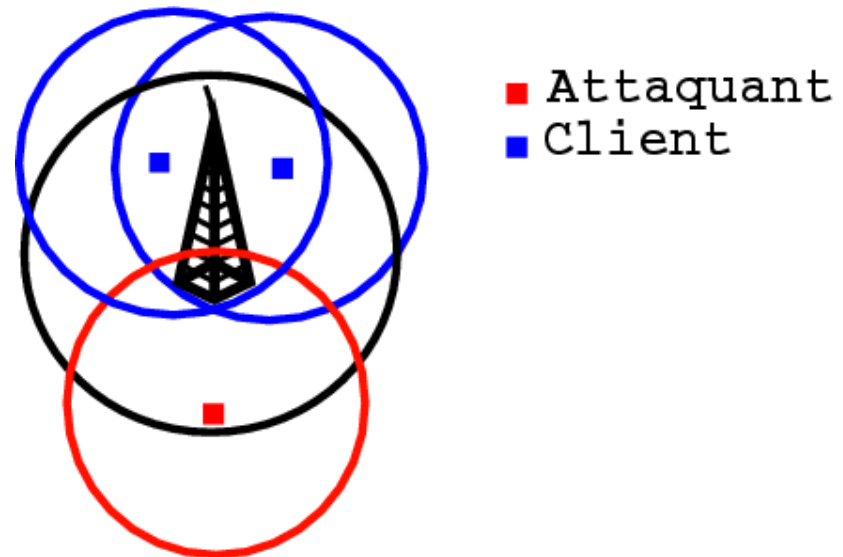
- Utilisation de GPS
 - Géolocalisation
- Utilisation d'antennes
 - Amélioration du signal et des résultats
 - Différents type d'antennes
 - Omnidirectionnelles
 - Directionnelles
 - Secteur et patch
- Détection à très longue portée



Détection en aveugle

- Attention à la détection en aveugle
 - Équipements détectés hors de portée radio
 - Détectés par l'intermédiaire d'un équipement tiers
 - Analyse des trames 802.11b

client -> borne
borne -> client
-> attaquant



Conclusion

- Les réseaux sans fil nécessitent de l'attention
 - Il faut les surveiller
 - Les considérer comme des points d'entrée pour des attaquants
- Il faut les sécuriser
 - les mettre dans une DMZ
- Auditer et rechercher
 - Une tâche à ne pas négliger

Merci



HERVÉ SCHAUER CONSULTANTS

<http://www.hsc.fr/>

