



HERVÉ SCHAUER CONSULTANTS

Cabinet de Consultants en Sécurité Informatique depuis 1989

Spécialisé sur Unix, Windows, TCP/IP et Internet

Les rencontres de PC Expert

Mardi 23 Mars 2004

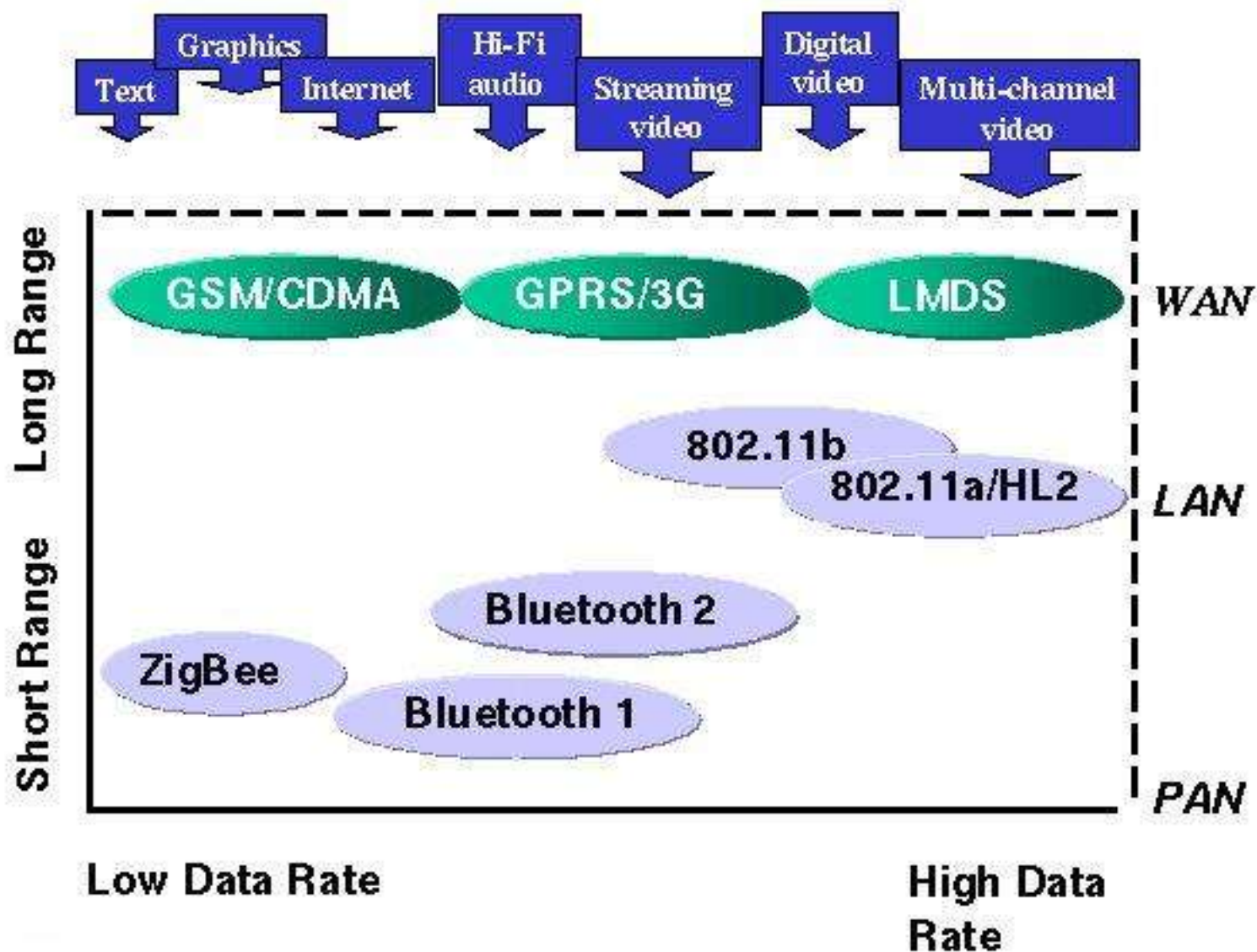
Les risques avec les réseaux sans fil


Jérôme Poggi

<Jerome.Poggi@hsc.fr>

- Présentation des réseaux sans fil
- Modes de fonctionnement des réseaux sans fil
- Problèmes des réseaux sans fil
 - Écoutes, Wardriving, débordement sur la voie publique
 - Dénis de services, brouillage
- Attaques
 - Le WEP et ses imperfections
 - Écoute avec et sans matériel spécifique
 - Verboseité du protocole
 - *Man in The Middle*
- La future norme 802.11i

- Multiple technologie
- Standard divers
- Utilisations variés
- Portée différente
- Information transportée

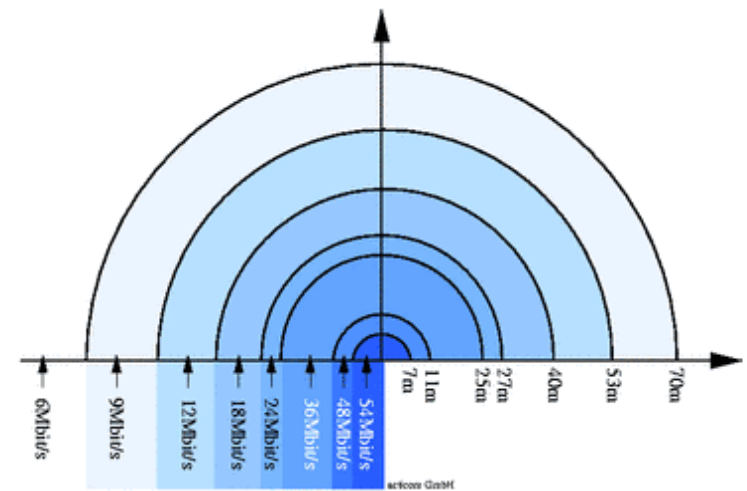


- Précisions de langage
 - WLAN : Wireless Local Area Network
 - Réseau local sans fil
 - Wi-Fi : Wireless Fidelity The Wi-Fi logo consists of the words 'Wi-Fi' in a white, sans-serif font inside a dark, rounded rectangular border.
 - Norme d'interopérabilité
 - Airport
 - Le Wi-Fi vu par Apple
 - 802.11a, 802.11b, 802.11g ...
 - Normes actuelles de l'IEEE de réseaux sans fil
 - 802.11n, 802.16, 802.20
 - Futur normes pour les réseaux sans fil

- Facilité de déploiement
 - Faibles coûts
 - Pas de frais de câblage
 - Immeubles anciens
 - Rapidité
 - Réseaux temporaires
 - Pas de démarche auprès d'un service précis de l'entreprise
- Mobilité
 - Bureau, salles de réunions, laboratoire
 - Entrepôts, usines
- Obstacles et grands sites
 - Passage de rue, de voie ferrée
- Campus, usines

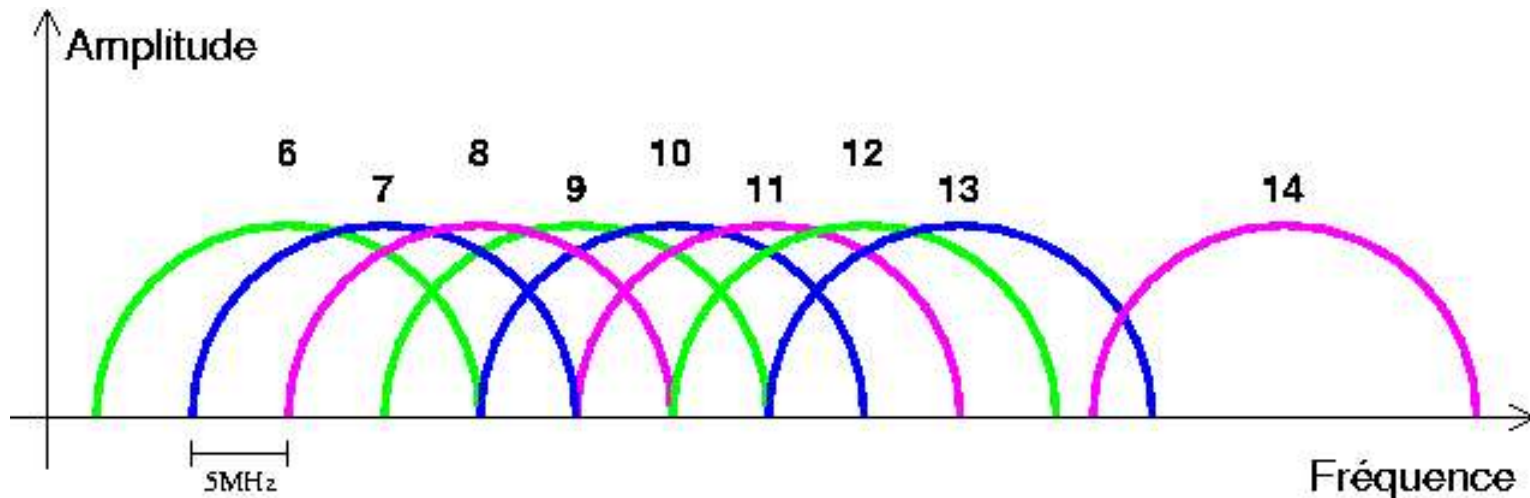
- Historique et évolution
 - 1997 : 802.11
 - 2Mbits/s max
 - porteuse non fixe
 - matériel professionnel
 - 1999 : 802.11b
 - 11Mbit/s max
 - porteuse fixe
 - début de démocratisation grand public
 - 2003 : 802.11g
 - 54Mbits/s max
 - porteuse fixe
 - démocratisé, accessible au grand public
- Autres normes
 - 802.11a : porteuse sur les 5Ghz, peu démocratisé
 - Hyperlan : porteuse sur les 5Ghz, norme Européenne

- Le transport de l'information se fait sur la radio
 - Sur une bande de fréquence définie : 2,4Ghz pour 802.11b/g
 - Protocole CSMA/CA : évitement de collision
 - Les équipements respectent le média
 - Pas de transmission anarchique
 - Débit variable suivant la qualité de la communication
 - Plus le rapport Signal/Bruit est grand plus la communication est rapide
 - Exemple : pour le 802.11g
- 2 modes de fonctionnement
 - Centralisé : Infrastructure
 - Une borne gère tout
 - Décentralisé : Ad-Hoc
 - Liaison multi-point
 - Chaque noeud est de poids égal



- Chaque réseau est identifié par un SSID : identificateur du réseau
 - Plusieurs réseaux avec des SSID différents peuvent cohabiter au même endroit sur le même canal
- Une interface Ethernet sans fil 802.11 est similaire à une interface Ethernet filaire 802.3
 - 802.11b : CSMA/CA, 802.3 : CSMA/CD
 - Vision identique pour les ordinateurs et pour TCP/IP
 - Adressage MAC identique
 - Adresses des bornes en plus : 4 adresses MAC au lieu de 2 dans la trame
- WEP (*Wired Equivalent Privacy*)
 - Permet (en théorie) d'assimiler un réseau Ethernet sans fil à un réseau Ethernet filaire en assurant une sécurité équivalente à celle d'un câble
 - Implémentation faite sans consultation préalable avec des cryptographes

- 14 canaux : 14 porteuses (2412 Mhz à 2484Mhz)
 - Espacés de 5Mhz
 - Utilisation de 22Mhz par canaux
 - Recouvrements de canaux
 - Pas de recouvrement entre les canaux 1, 6 et 11
 - Législation Française : <http://www.art-telecom.fr/dossiers/rlan/menu-gal.htm>
 - utilisation à l'intérieur des bâtiments : libre, PIRE <100mW
 - utilisation à l'extérieur : 1-7 < 100 mW, 8-13 < 10 mW



- Support non fiable
 - Perturbable, partagé
 - DECT, Micro-ondes, Vidéo de surveillance, partage vidéo ...
 - Libre
 - Bande de fréquence IMS (Industrial, Medical, Scientific)
 - Utilisé par les radio amateur
 - De plus en plus de bornes déployées
- Facilement écoutable, détectable
 - Émission radio
- Chiffrement WEP non fiable
 - Possibilité de déchiffrer le trafic
 - En ligne et Hors ligne
 - Programmes de cassage du WEP disponibles sur internet

- Accessible au grand public
 - Beaucoup d'endroits sont équipés
- Connexions non contrôlées
 - Connexion sur la borne du voisin plutôt que sur la borne de l'entreprise
 - Contournement de la politique de sécurité
- Traverse les murs, diffusion spatiale
 - Pas de limitation physique simple
 - Traverse les murs, fenêtres ...
 - Peu de maîtrise du périmètre radio
 - Réflexion, diffusion ...
- Caractéristique de propagation variable suivant l'environnement
 - Stoppés par tout ce qui est à base d'eau
 - Arbres, humains, brouillard ...

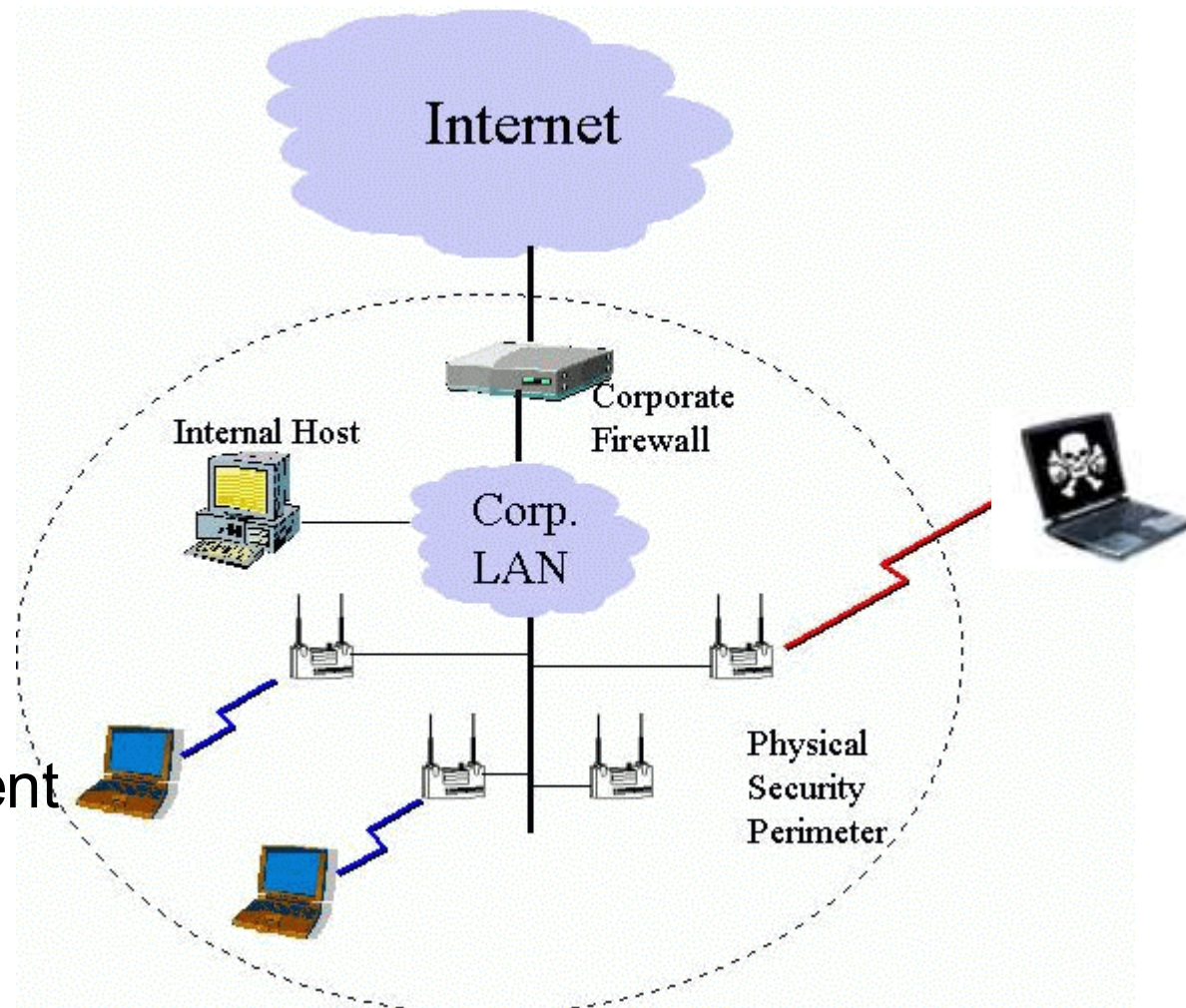
- Utiliser du réseau sans fil = Avoir une prise Ethernet sur le parking
- Il faut sécuriser en connaissance de cause
- Wardriving :
 - Rechercher le maximum de bornes ouverte ou non
 - Cartographier ces bornes
 - « Sport » à la mode et illégale
- Le protocole est très verbeux
 - Beaucoup d'informations sont disponibles juste en écoutant
- Beaucoup d'outils gratuits disponibles
 - Sous tous les OS
 - Netstumbler, Kismet, Airtraf, wifiscanner ...





- Brouillage
 - Brouillage entre bornes
 - Canaux trop proche
 - Densité de borne trop grande
 - Brouillage par d'autres équipements
 - DECT, Micro-ondes, ...
 - Vidéo surveillance, ...
- Dénis de service
 - Inondation du réseau avec des trames d'administration usurpées
 - Dé-Authentification
 - Dé-Association
 - Aucune solution existante présente
 - Le 802.11i permet d'identifier les trames d'administration

- Plus besoin d'être dans la société
 - Attaque depuis l'extérieur
- Usurpations de borne, de clients
 - Simple à effectuer
- L'écoute est simple
- Tous les équipement connectés à la borne reçoivent les données
- Attaques simple et évoluées
 - Ex: *Virtual Carrier-sense Attack*



- Le WEP est imparfait :
 - Attaque contre la confidentialité
 - Faiblesse de RC4 (*key scheduling algorithm weakness*)
 - Réutilisation du flux de codons (*keystream reuse*)
 - Attaque exhaustive
 - Attaque contre l'intégrité
 - Modification de paquets
 - Injection de faux paquets
 - Attaque contre l'authentification auprès de l'AP
 - Fausse authentification (*authentication spoofing*)
- Le WEP est toujours utilisé dans :
 - WPA et les solutions d'authentification basées sur 802.1X
 - Mais quasiment toutes les failles sont en partie corrigées ou supprimées

- Écoutes sans matériel spécifique :

- Un PC, une Carte PCMCIA 802.11b et un logiciel
 - Windows : NetStumbler
 - Linux : Kismet, wifiscanner, ...



- Écoutes avec matériel spécifique :

- Un PC, une carte PCMCIA 802.11b, un logiciel d'écoute
- Une ou plusieurs antennes

```

dragom@gir.jan.nerv-un.net:~/dragom
┌─Networks--(Autofit)─┐ Info
├─ Name                T W Ch Packts Flags          Ntwrks
├─ St Francis          G N 07 324          0.0.0.0
├─ VBHJLUND            A Y 11 48           0.0.0.0
├─ Cerhud-PDK          G N 06 339          0.0.0.0
├─ <no ssid>           A N 01 1508 U3      10.132.112.0
├─ cvsretail           A N 14 1001         0.0.0.0
├─ IBM-PDK
├─ pserwap003
├─ linksys
├─ <no ssid>
├─ tsunami3624t
├─ <no ssid>
├─ default
├─ arlington
├─ linksys
├─ LucHomeNet
├─ linksys
├─ CPT_Wireless
├─ WLAN
└─ Status
  Detected new network
  Detected new network
  Detected new network
  Detected new network
  ────────────────────
  MFIScanner v0.7.2beta1 (C) 2002 Hervé Schauer Consultants (jerome.poggil@hsc-18es.com)
  ┌─ Summary ─┐
  └─ IP        ─┘
  └─ STA      ─┘
  └─ REGION   ─┘
  └─ SSID     ─┘
  └─ Channel  ─┘
  └─ Invalid  ─┘
  └─ Cracked  ─┘
  └─ Weak     ─┘
  └─ Last ID  ─┘
  └─ Packets  ─┘
  └─ Scan     ─┘
  └─ 000000001111 ─┘
  └─ 1234567890123 ─┘
  └─ IDB is OFF ─┘

FrameType=080 (typeID subtypeID)
S-Ctrl=06
02/05/2003 16:19:120.370,"ssidlah",06(+),---,AP,02L,000,FF1FF1FF1FF1FF1FF,001801C81821D01E4,001801C81821D01E4,2M/s,AP Base (dedicated)
IDB OF PACKET PROCESSING ---
Packet number: 154
rcvlen = 39
Hex:
000000 - 8000 0000 FFFF FFFF FFFF 0006 2571 CEE3 .....Rg...
000006 - 0006 2571 CEE3 00E3 00E1 9800 3152 0000 .....Rg.....
00000C - 6400 1100 0000 0104 8284 0161 0301 0608 d.....
000012 - 0400 0000 00FF FFFF FF.....
Process Management Frame
IDB1FF1FF1FF1FF1FF Src:0010612571C81E3 Bssid:0010612571C81E3
Fragment number: 0x0000
Sequence number: 1 0x02E4
Timestamp: 0x00002818046F18A
Reason: IdleCh3: 1 0x04
Capabilities: 1 0x12
SN: 1 0x00
TagTypeLen = 00(00),01(04),03(01),05(04),
Res_TypeOfClient:3
FrameType=000 (typeID subtypeID)
S-Ctrl=06
02/05/2003 16:19:120.410,"06(+)",Map,AP,030,000,FF1FF1FF1FF1FF1FF,0010612571C81E3,0010612571C81E3,2M/s,AP Base (dedicated),Rad
to only BEACON
IDB OF PACKET PROCESSING ---
    
```



- Le protocole 802.11 est très verbeux
 - Une trame annonçant la borne est diffusé 10 fois par secondes
 - Contient énormément d'informations
 - Pas toujours officielles
 - Données non documentées
 - Données spécifique par constructeurs
 - Tout est documentée dans la norme
 - Plus de 150 pages
 - Les trames d'administrations ne sont
 - Ni authentifiées, ni chiffrées
 - L'information est toujours en clair

```
Frame 1 (62 bytes on wire, 62 bytes captured)
  Arrival Time: Mar  1, 2004 19:05:28.950052000
  Time delta from previous packet: 0.000000000 seconds
  Time since reference or first frame: 0.000000000 seconds
  Frame Number: 1
  Packet Length: 62 bytes
  Capture Length: 62 bytes
IEEE 802.11
  Type/Subtype: Beacon frame (8)
  Frame Control: 0x0080 (Normal)
    Version: 0
    Type: Management frame (0)
    Subtype: 8
    Flags: 0x0
      DS status: Not leaving DS or network is operating in AD-HOC mode (To DS: 0  From DS: 0)
(0x00)
      .... .0.. = More Fragments: This is the last fragment
      .... 0... = Retry: Frame is not being retransmitted
      ...0 .... = PWR MGT: STA will stay up
      ..0. .... = More Data: No data buffered
      .0.. .... = WEP flag: WEP is disabled
      1... .... = Order flag: Not strictly ordered
  Duration: 0
  Destination address: ff:ff:ff:ff:ff:ff (ff:ff:ff:ff:ff:ff)
  Source address: 00:04:23:79:df:60 (00:04:23:79:df:60)
  BSS Id: 02:04:23:b8:77:9f (02:04:23:b8:77:9f)
  Fragment number: 0
  Sequence number: 3811
  Frame check sequence: 0xffffffff (incorrect, should be 0x52b20719)
```

HSC Beacon 1/2

IEEE 802.11 wireless LAN management frame

Fixed parameters (12 bytes)

Timestamp: 0x000000006DAE2227

Beacon Interval: 0.102400 [Seconds]

Capability Information: 0x0022

.... 0 = ESS capabilities: Transmitter is a STA
.... 1 = IBSS status: Transmitter belongs to an IBSS
.... 00.. = CFP participation capabilities: Station is not CF-Pollable (0x0000)
.... 0 = Privacy: AP/STA cannot support WEP
.... 1. = Short Preamble: Short preamble allowed
.... .0.. = PBCC: PBCC modulation not allowed
.... 0... = Channel Agility: Channel agility not in use
.... .0.. = Short Slot Time: Short slot time not in use
..0. = DSSS-OFDM: DSSS-OFDM modulation not allowed

Tagged parameters (22 bytes)

Tag Number: 0 (SSID parameter set)

Tag length: 7

Tag interpretation: NETGEAR

Tag Number: 1 (Supported Rates)

Tag length: 4

Tag interpretation: Supported rates: 1.0(B) 2.0(B) 5.5(B) 11.0(B) [Mbit/sec]

Tag Number: 3 (DS Parameter set)

Tag length: 1

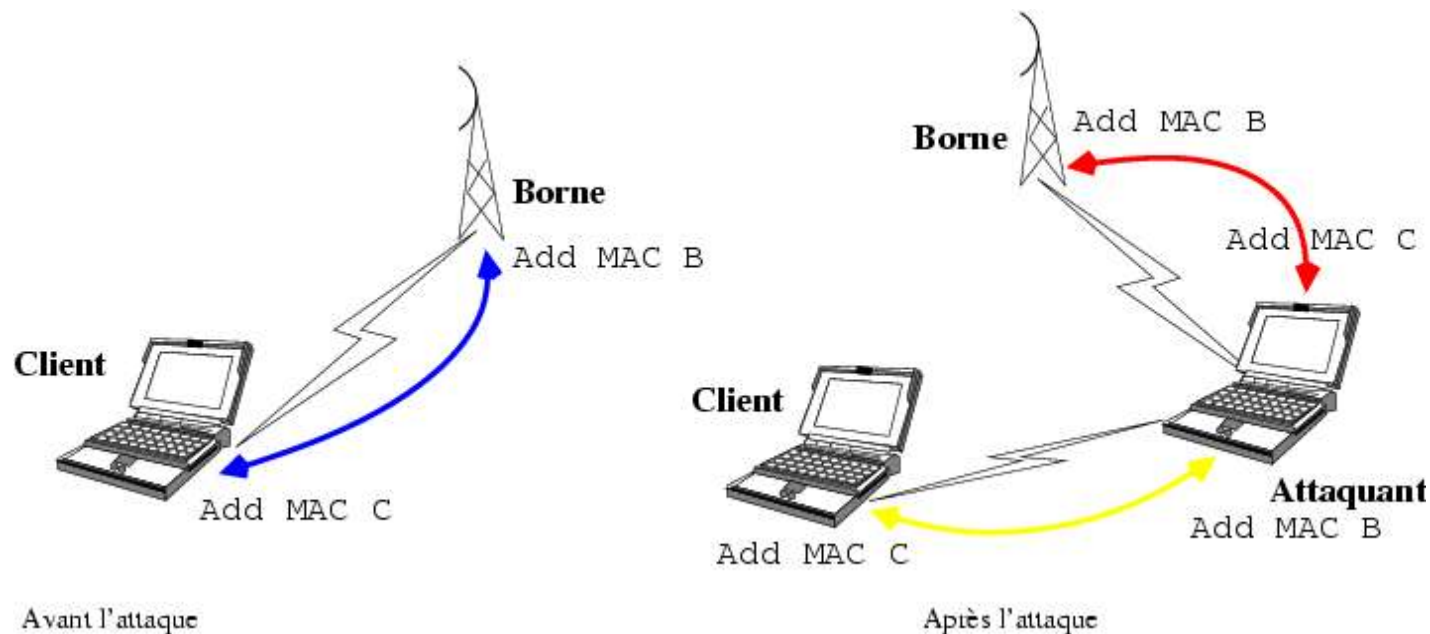
Tag interpretation: Current Channel: 10

Tag Number: 6 (IBSS Parameter set)

Tag length: 2

Tag interpretation: ATIM window 0x0

- *Man in the Middle* : Interception et insertion dans la communication
- Usurpation de la borne
- Interception de toutes les communications
- Le client s'attache toujours à la borne qu'il reçoit le mieux



- WPA : Profil de 802.11i promu par le WECA
 - Permet de combler une partie des problèmes du WEP
 - Utilisation de TKIP : changement des clefs de chiffrement de façon périodique
 - Vecteur d'initialisation de 48bits (281 474 976 710 656 possibilités)
 - Impossibilité de réutiliser un même IV avec la même clef
 - Utilisation du MIC qui est un contrôle d'intégrité de tout le message
- Le WPA n'intègre pas les sécurisation que le 802.11i apporte :
 - La sécurisation des réseaux multi-point Ad-Hoc
 - La sécurisation des paquets de dés-authentification/dés-association
 - Permet de stopper la plupart des attaques et dénis de services
 - N'implémente pas AES comme algorithme de chiffrement
 - chiffrement CCMP : AES en mode chaîné sur blocs de 128 bits

- Déployez les réseaux sans fil avant vos utilisateurs
 - Maîtrise des utilisateurs et de la technologie
- Considérez les réseaux sans fil comme des accès Internet
 - Filtrage, authentification, DMZ ...
- Utilisez le 802.11g qui est compatible avec le 802.11b
 - Le 802.11b est dépassé
- Pas de solution propriétaire
 - Souvent opaque, pas certifiable
- Utilisez des solutions éprouvées ou d'avenir
 - Authentification 802.1X
 - WPA, 802.11i
- Auditez et/ou faites auditer votre infrastructure

Merci de votre attention

Questions ?