Journées
"Sécurité des nomades"

Réseaux sans fil :
Detection et écoutes passives

Jeudi 14 Novembre 2002

Jérôme Poggi
Jerome.Poggi@hsc.fr

Hervé Schauer Consultants
http://www.hsc.fr/

Plan

Reproduction INTERDITE 2002 (c) Hervé Schauer Consultants (http://www.hsc.fr/)

- *Wardriving* ou Trébucher sans fil
- Outils
- Quel type d’informations peuvent être récupérées ?
- Contre mesures
- Conclusion

Fonctionnement du *Wardriving*

Wardriving

Reproduction INTERDITE 2002 (c) Hervé Schauer Consultants (http://www.hsc.fr/)

- Origine :
  - Extension du *WarDialing*
  - Rechercher les réseaux sans fils
- Très simple à faire
- Silencieux et discret
  - Un laptop dans un sac à dos
    - absolument invisible
  - PDA
    - iPaq / Zaurus
    - Très petit
  - Connexion avec un GPS
    - Cartographie des réseaux
      - http://www.netstumbler.com/
      - http://www.nodedb.org/
      - http://www.wigle.net/
  - Utilisation d’antenne externe
    - omnidirectionnelle ou directionnelle
    - meilleure detection, moins discret

Comment est ce possible ?

Reproduction INTERDITE 2002 (c) Hervé Schauer Consultants (http://www.hsc.fr/)

- L'éther est le média
- Même avec un équipement assez loin
  - Usage d'antenne (directionnelle ou omnidirectionnelle)
- But et motivations
  - Écoutes clandestines
  - Espionnage économique
  - Fraudes
  - Piratages par rebonds
  - Surfer sur internet gratuitement
  - Jeux

Outils

Outils

Reproduction INTERDITE 2002 (c) Hervé Schauer Consultants (http://www.hsc.fr/)

- Beaucoup d’outils de détection disponibles

- Deux type :
  - Scanner passifs
    - écoute du trafic
    - théoriquement indécelable
  - Scanner actifs
    - évolution de scanner passifs
    - Deviennent actifs pour :
      - détecter plus d’informations
      - évaluer le réseau (DHCP, plages d’@, passerelle vers internet)

Sous Microsoft Windows

Reproduction INTERDITE 2002 (c) Hervé Schauer Consultants (http://www.hsc.fr/)

- Netstumbler (http://www.netstumbler.com/)
  - Fonctionne avec une carte Lucent
  - Donne peu d'informations
  - Convivial
  - Connexion avec un GPS
  - Historique ratio Signal/Bruit
- Netstumbler pour IPaq
  - Plus petit et plus discret
  - Utilisation de batterie externe fortement recommandé

Outils Linux (1/3)

Reproduction INTERDITE 2002 (c) Hervé Schauer Consultants (http://www.hsc.fr/)

- Beaucoup d’outils disponibles
- Fonctionnent avec un ou plusieurs composants suivant
  - Lucent / Agere / Orinoco / Proxim
  - Prism / Intersil
  - Cisco / Aironet

Outils Linux (2/3)

Reproduction INTERDITE 2002 (c) Hervé Schauer Consultants (http://www.hsc.fr/)

- AirTraf (http://sourceforge.net/projects/airtraf)
  - Cartes Prism et Aironet
  - Affichage en temps réel
    - Bande passante utilisée
    - Liste des clients détectés
    - Module d'IDS
  - Connexion avec une base MySQL
    - Possibilité de faire des statistiques
- Kismet (http://www.kismetwireless.net/)
  - Cartes Prism et Aironet
  - Trafic sauvegardable en format PCAP
  - Analyses des paquets de contrôle et d'administration
  - Analyses au niveau IP
  - Interface Ncurses

Outils Linux (3/3)

Reproduction INTERDITE 2002 (c) Hervé Schauer Consultants (http://www.hsc.fr/)

- WiFiScanner (http://www.hsc.fr/ressources/outils/wifiscanner/)
  - Cartes prism seulement avec le driver Linux-wlan-ng(http://www.linux-wlan.org/)
    - très performant et configurable
  - Detection et affichage de l'architecture réseau
  - Trafic entièrement sauvegardé
    - analyse hors ligne
  - Analyse de plus de 99% des trames réseaux
  - Module d'analyse et de détection d'anomalies
    - surveillance passive d'un réseau
  - Discret et quasi indétectable
    - pas de paquets radio envoyés

Démonstration

Quel type d’informations peuvent être récupérées ?

Quel type d'informations ?

Reproduction INTERDITE 2002 (c) Hervé Schauer Consultants (http://www.hsc.fr/)

- Trois sortes de paquets 802.11b
  - Administration
    - recherche / signalisation
    - association / désassociation
    - authentification / désauthentification
  - Contrôle
    - gestion de la bande passante
    - accusé de reception
    - gestion de l'énergie
  - Données
    - transport
- Tous les types de paquets sont intéressants
  - Beaucoup d'informations
  - Même si du chiffrement est utilisé

Informations

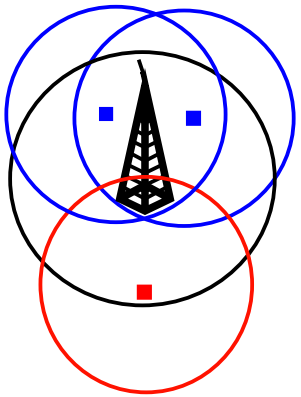
Reproduction INTERDITE 2002 (c) Hervé Schauer Consultants (http://www.hsc.fr/)

- Paquets d'administration
  - Beacon, Probe request/response
    - Facile à détecter
      - dix paquets par secondes
      - faible vitesse de transmission
      - portée importante
    - Peuvent être envoyés par
      - Bornes
      - Client en mode Ad-Hoc (P2P)
    - Contiennent
      - SSID
      - Horodatage
      - Caractéristiques système
  - Association
    - Envoyé en début de connexion
  - Authentication
    - Envoyé lors de l'établissement du protocole de dialogue

Informations

Reproduction INTERDITE 2002 (c) Hervé Schauer Consultants (http://www.hsc.fr/)

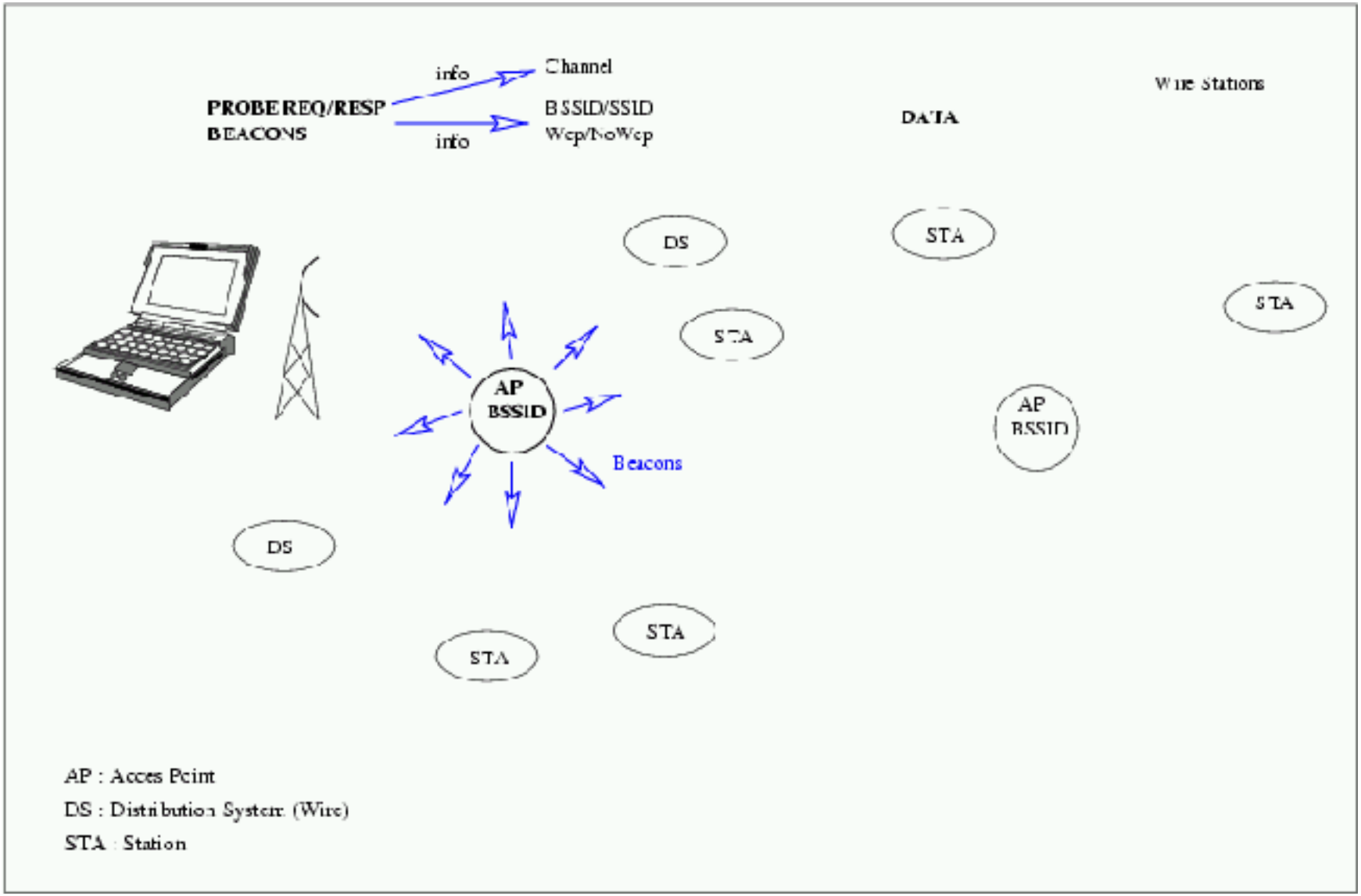
- Trames de contrôle
  - Trafic actif et existant
  - Permet de détecter des équipements en aveugle



- Trames de données
  - Identification
  - Mots de passe
  - Courrier électronique
  - Fichiers
  - "weak IV" (cassage du WEP)
  - Trames "broadcast" venant du réseau filaire
  - Informations ARP

Informations

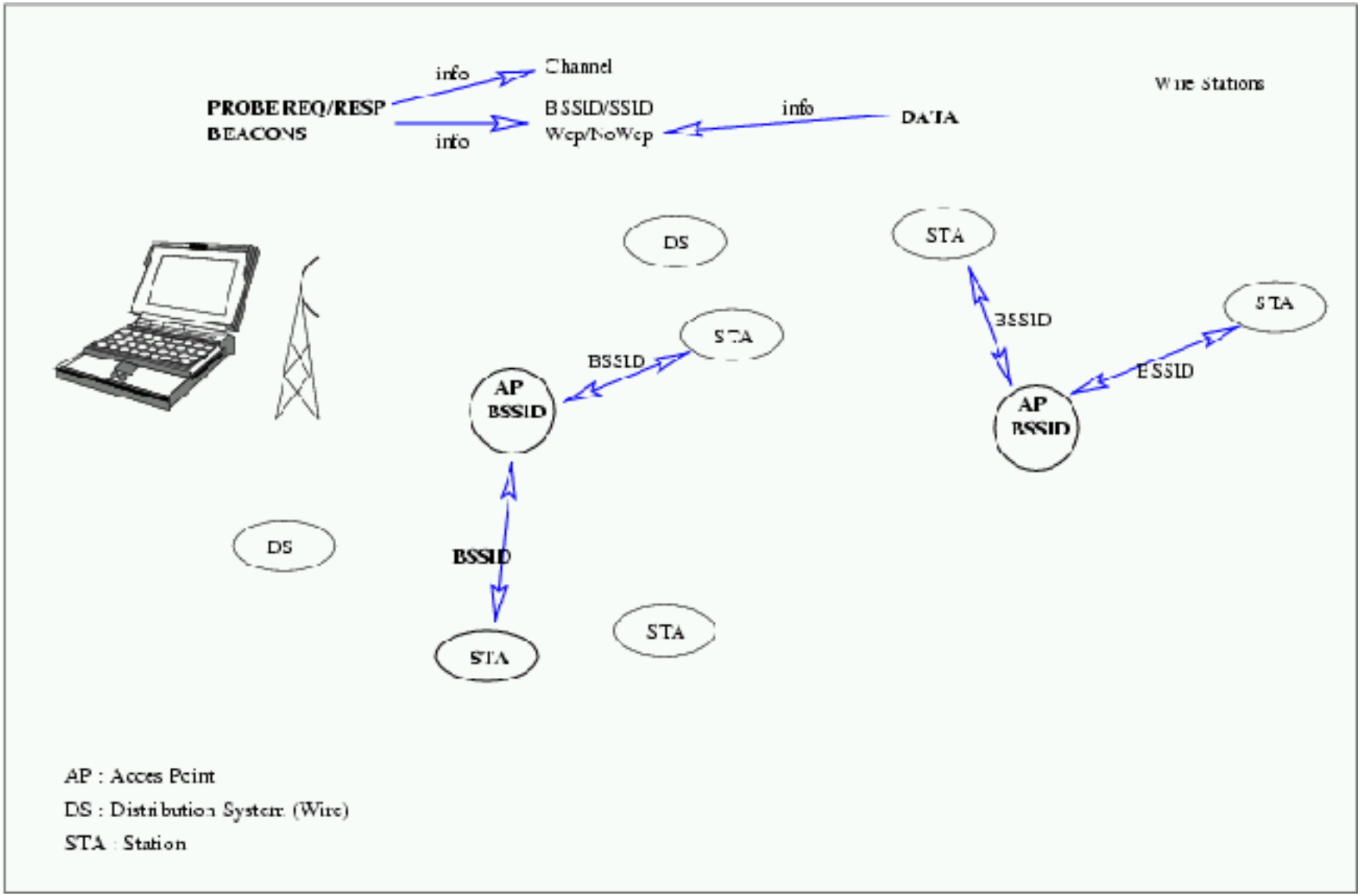
Reproduction INTERDITE 2002 (c) Hervé Schauer Consultants (http://www.hsc.fr/)



Méthode de détection des informations

Informations

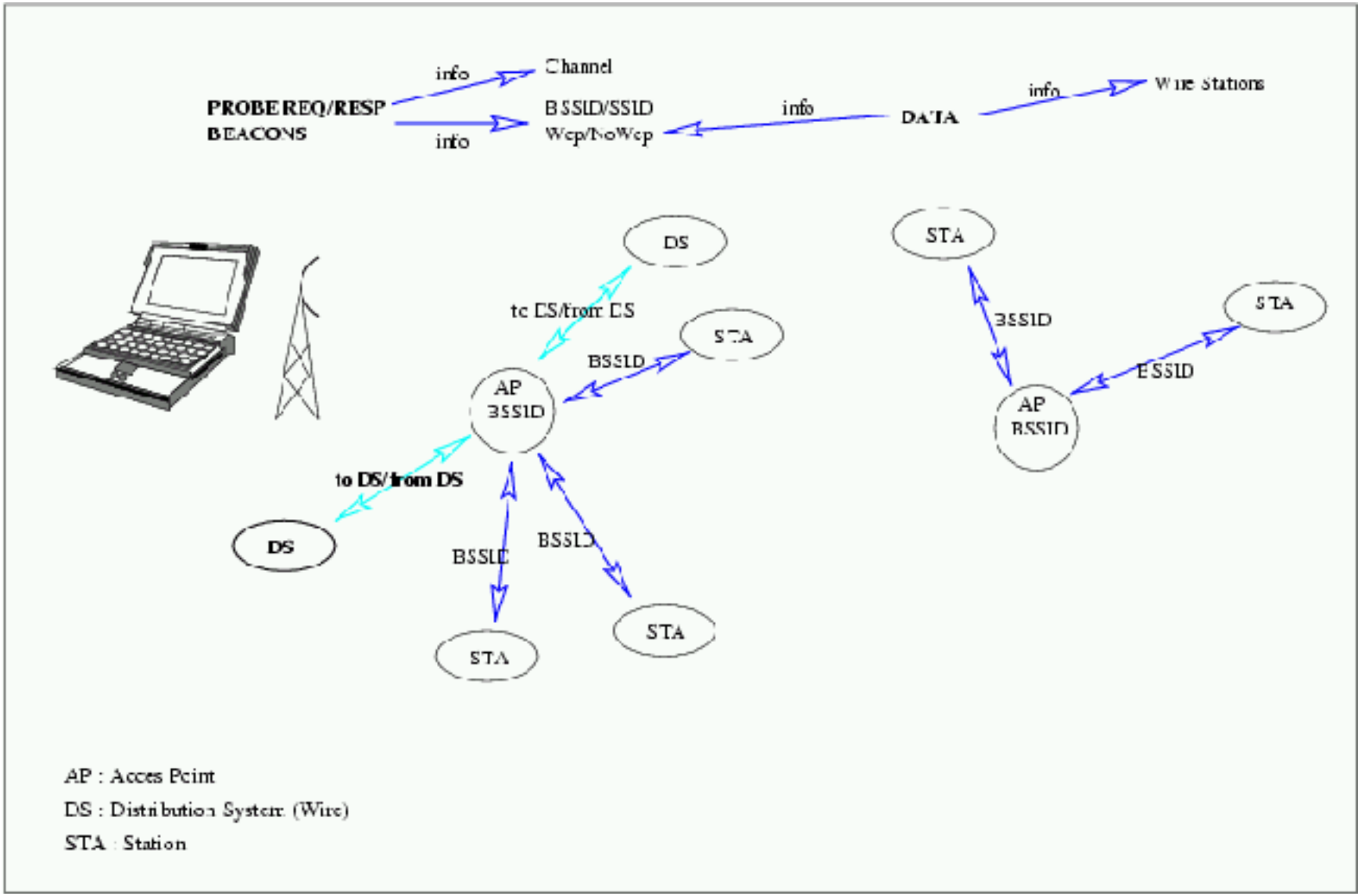
Reproduction INTERDITE 2002 (c) Hervé Schauer Consultants (http://www.hsc.fr/)



Méthode de détection des informations

Informations

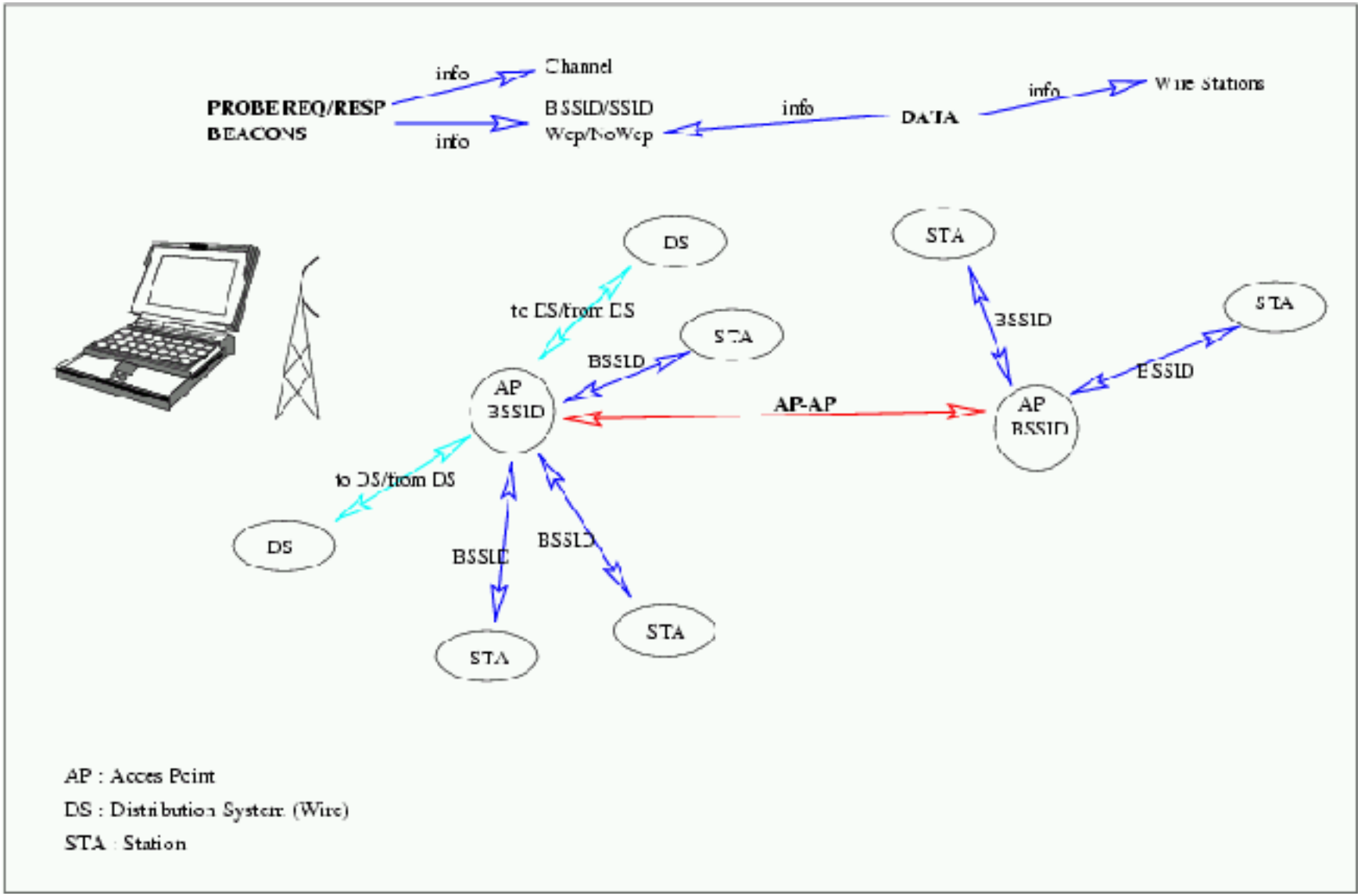
Reproduction INTERDITE 2002 (c) Hervé Schauer Consultants (http://www.hsc.fr/)



Méthode de détection des informations

Informations

Reproduction INTERDITE 2002 (c) Hervé Schauer Consultants (http://www.hsc.fr/)



Méthode de détection des informations

Beacon de borne

Reproduction INTERDITE 2002 (c) Hervé Schauer Consultants (http://www.hsc.fr/)

```
Frame 64 (75 on wire, 75 captured)
    Arrival Time: Feb 19, 2002 11:50:33.579712000
    Packet Length: 75 bytes
IEEE 802.11
    Type/Subtype: Beacon frame (8)
    Frame Control: 0x0080
        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.. = Fragments: No fragments
            .... 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
            0... .... = Order flag: Not strictly ordered
    Duration: 0
    Destination address: FF:FF:FF:FF:FF:FF (FF:FF:FF:FF:FF:FF)
    Source address: 00:40:05:48:53:43 (00:40:05:48:53:43)
    BSS Id: 00:40:05:48:53:43 (00:40:05:48:53:43)
    Fragment number: 0
    Sequence number: 1649
IEEE 802.11 wireless LAN management frame
    Fixed parameters (12 bytes)
        Timestamp: 0x000000153AE7F191
        Beacon Interval: 0.102400 [Seconds]
        Capability Information: 0x0015
            .... ...1 = ESS capabilities: Transmitter is an AP
            .... ..0. = IBSS status: Transmitter belongs to a BSS
            ...1 .... = Privacy: AP/STA can support WEP
            ..0. .... = Short Preamble: Short preamble not allowed
            .0.. .... = PBCC: PBCC modulation not allowed
            0... .... = Channel Agility: Channel agility not in use
            CFP participation capabilities: Point coordinator at AP for delivery and polling (0x0001)
    Tagged parameters (35 bytes)
        Tag Number: 0 (SSID parameter set)
        Tag length: 10
        Tag interpretation: WLAN
        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: 11
        Tag Number: 4 (CF Parameter set)
        Tag length: 6
        Tag interpretation: CFP count 0, CFP period 1, CFP max duration 0, CFP Remaining 0
        Tag Number: 5 ((TIM) Traffic Indication Map)
        Tag length: 4
        Tag interpretation: DTIM count 0, DTIM period 1, Bitmap control 0x0, (Bitmap suppressed)
```

Beacon de client Ad-Hoc

Reproduction INTERDITE 2002 (c) Hervé Schauer Consultants (http://www.hsc.fr/)

```
Frame 415 (65 on wire, 65 captured)
    Arrival Time: Feb 19, 2002 11:19:07.829280000
    Packet Length: 65 bytes
IEEE 802.11
    Type/Subtype: Beacon frame (8)
    Frame Control: 0x0080
        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.. = Fragments: No fragments
            .... 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
            0... .... = Order flag: Not strictly ordered
    Duration: 0
    Destination address: FF:FF:FF:FF:FF:FF (FF:FF:FF:FF:FF:FF)
    Source address: 00:40:96:68:73:63 (00:40:96:68:73:63)
    BSS Id: 66:00:03:03:A5:02 (66:00:03:03:A5:02)
    Fragment number: 0
    Sequence number: 422
IEEE 802.11 wireless LAN management frame
    Fixed parameters (12 bytes)
        Timestamp: 0x0000000000BB866A
        Beacon Interval: 0.102400 [Seconds]
        Capability Information: 0x0012
            .... ...0 = ESS capabilities: Transmitter is a STA
            .... ..1. = IBSS status: Transmitter belongs to an IBSS
            ...1 .... = Privacy: AP/STA can support WEP
            ..0. .... = Short Preamble: Short preamble not allowed
            .0.. .... = PBCC: PBCC modulation not allowed
            0... .... = Channel Agility: Channel agility not in use
            CFP participation capabilities: Station is not CF-Pollable (0x0000)
    Tagged parameters (25 bytes)
        Tag Number: 0 (SSID parameter set)
        Tag length: 10
        Tag interpretation: WLAN
        Tag Number: 1 (Supported Rates)
        Tag length: 4
        Tag interpretation: Supported rates: 1.0(B) 2.0 5.5 11.0 [Mbit/sec]
        Tag Number: 3 (DS Parameter set)
        Tag length: 1
        Tag interpretation: Current Channel: 6
        Tag Number: 6 (IBSS Parameter set)
        Tag length: 2
        Tag interpretation: ATIM window 0x0
```

Contre-mesures

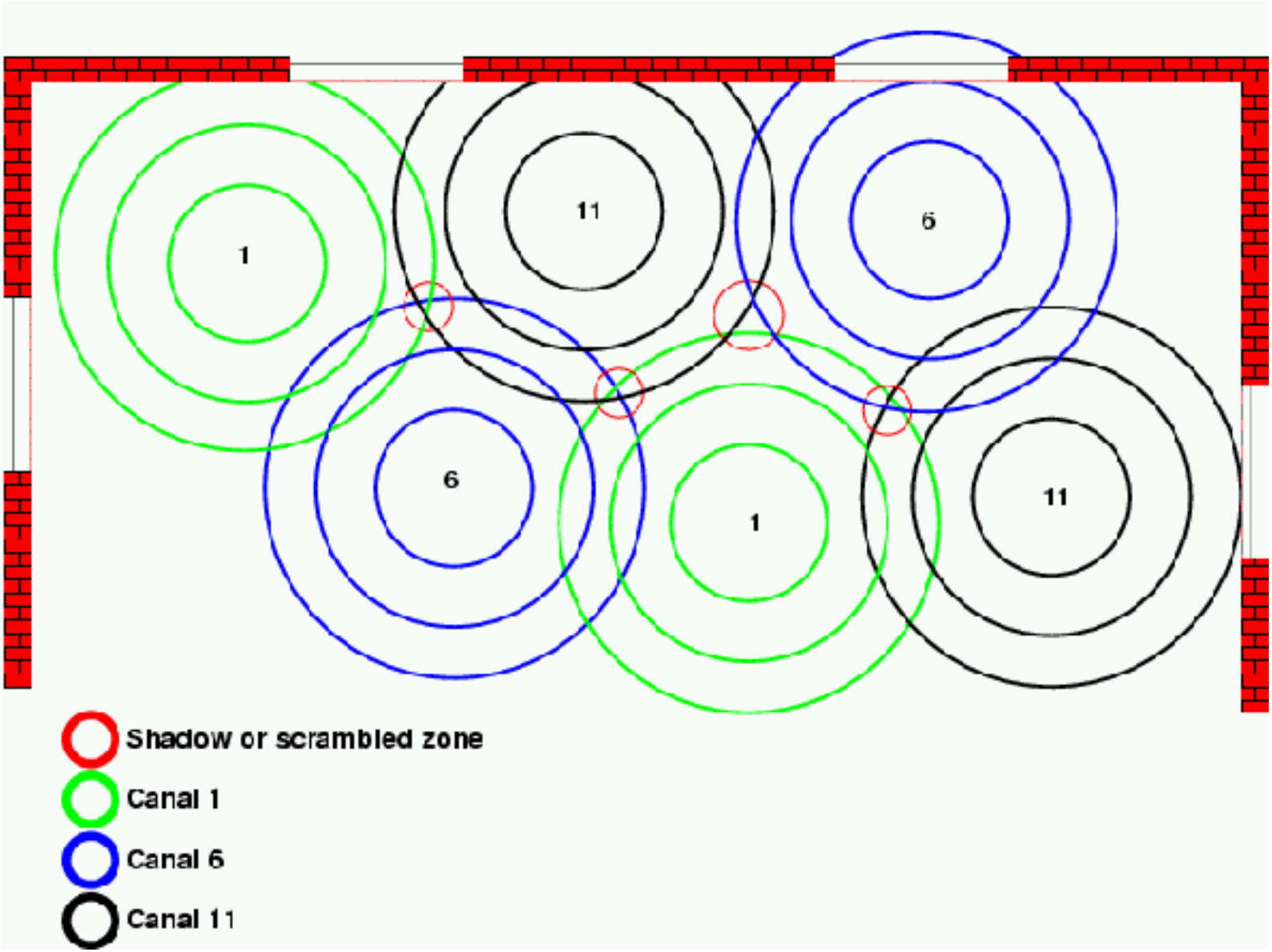
Contre-mesures physique

Reproduction INTERDITE 2002 (c) Hervé Schauer Consultants (http://www.hsc.fr/)

- Il existe des contre-mesures matériels :
  - Utilisation d'antenne sectoriel
    - antenne patch (180°)
    - antenne secteur (90°, 180°...)
  - Utilisation de l'environnement
    - béton armé, murs épais
    - fenêtres blindées ou réfléchissante
    - grillage
    - arbres ...
  - Réduction de la puissance d'émission
    - de la borne
    - des clients

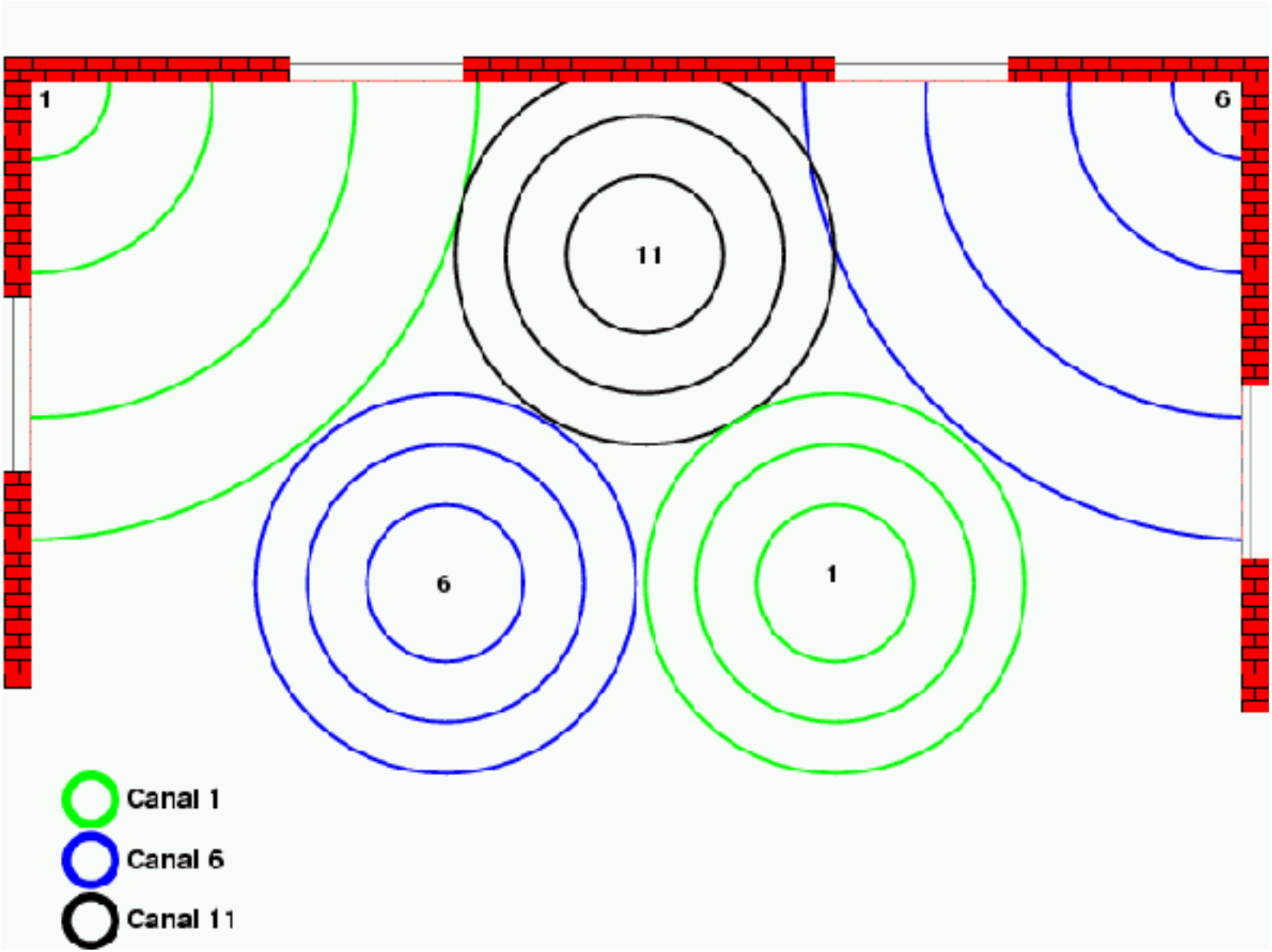
Utilisation correct d’antennes

Reproduction INTERDITE 2002 (c) Hervé Schauer Consultants (http://www.hsc.fr/)



Utilisation correct d’antennes

Reproduction INTERDITE 2002 (c) Hervé Schauer Consultants (http://www.hsc.fr/)

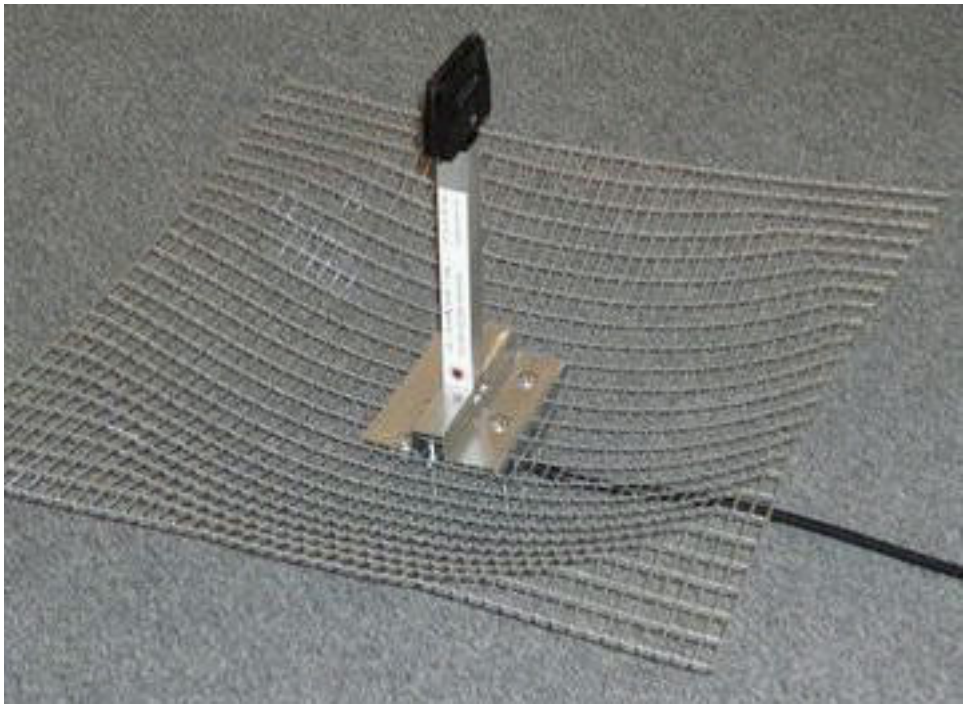


avec des antennes secteurs

Mais...

Reproduction INTERDITE 2002 (c) Hervé Schauer Consultants (http://www.hsc.fr/)

Avec du matériel pas cher et une antenne, il est très aisé d'écouter des équipements éloignés



Conclusion

Conclusion

Reproduction INTERDITE 2002 (c) Hervé Schauer Consultants (http://www.hsc.fr/)

- Considérer que tout le trafic en écoutable
  - <==> mettre une prise réseau à disposition !
- Les SSID sont toujours en clair
  - même avec du chiffrement
  - même s'il est "non diffusé"
- Ne pas négliger l'environnement
- Maîtriser l'environnement radio
  - aussi correctement que possible
- Ajouter une couche de chiffrement

Questions / Réponses

Jérôme Poggi
Hervé Schauer Consultants
http://www.hsc.fr/

Merçi

Jérôme Poggi
Hervé Schauer Consultants
http://www.hsc.fr/

Hervé Schauer Consultants (1/2)

Reproduction INTERDITE 2002 (c) Hervé Schauer Consultants (http://www.hsc.fr/)

- Cabinet de consultants en sécurité Unix, Windows, TCP/IP et Internet depuis 1989
- 12 consultants
- Expérience de la sécurité Unix depuis 1987
- Expérience de la sécurité Internet depuis 1991
- Expérience de la sécurité WNT depuis 1997
- Conception et architecture
  - Sécurité Internet/Intranet
  - Détection d'intrusion
  - Commerce électronique et services en ligne
- Mise en place de systèmes de sécurité

Hervé Schauer Consultants (2/2)

Reproduction INTERDITE 2002 (c) Hervé Schauer Consultants (http://www.hsc.fr/)

- Audits de sécurité
  - Réseaux, application, référentiels
- Enquêtes
- Tests d'intrusion
- Tests de vulnérabilités assistés : TSAR

- Veille en vulnérabilités
- Veille technologique de l'actualité en sécurité

- Programme complet de 15 formations en sécurité

- Plus de 30 produits de sécurité maîtrisés
- Plus de 150 références dans tous les secteurs d'activités et sur tous les continents