



**CLEAR CHANNEL**

---

## Réseaux locaux sans fil et sécurité



**Net Focus ♦ 25 juin 2003**

runo Kerouanton ♦ Responsable SNT ♦ CISSP



# Sommaire

---

- Présentation des RLAN
- Vulnérabilités et menaces
- Parades possibles
- L'audit de sécurité des RLANs
- Aspects juridiques
- Conclusion



# Qu'est ce que la sécurité ?

---

- Confidentialité
  - Éviter le vol d'informations confidentielles
- Intégrité
  - Conserver les informations intactes
- Disponibilité
  - Pouvoir accéder aux informations en permanence



# Différents types de réseaux ~~sans fil~~

---

- Réseaux personnels (PAN)

*Débit moyen, portée et consommation faibles.*

Ex. : Bluetooth

- Réseaux locaux (RLAN)

*Haut débit, portée moyenne.*

Ex. : Wi-Fi (802.11)

- Réseaux étendus (WAN)

*Haut débit, longue portée.*

Ex. : satellite, boucle locale



# Les réseaux IEEE 802.11

	Bande de fréquence	Débit maximum
802.11 b	2,4 GHz	11 Mbit/s
802.11 a	5 GHz	54 Mbit/s
802.11 g	2,4 GHz	54 Mbit/s

Moins répandu :

- Norme IEEE 802.11 d'origine (1 ou 2 Mbit/s)
- Extensions propriétaires (ex. : 802.11b en 22 Mbit/s)
- Autres normes (HiperLan, HomeRF, ...)



# Vulnérabilités et menaces

---

- Failles de conception
- Attaques du WEP
- Attaques courantes
- Autres facteurs



# Quels sont les problèmes ?

- La norme 802.11 a été créée sans le conseil d'experts en sécurité.
- La technologie radio en elle-même facilite les attaques.
- L'explosion du marché et la facilité de mise en œuvre amplifient le phénomène.



# Failles de conception du 802.11

---

- Norme « permissive » laissant le choix d'implémentation aux constructeurs.
- Mécanismes d'authentification insuffisants.
- Failles dans le mécanisme de chiffrement (WEP).



# Les principales failles du 802.11

---

- Le SSID (Service Set Identifier) est toujours transmis en clair.
- Le point d'accès envoie en permanence des trames de contrôle (beacon frames).
- L'authentification est contournable (adresses MAC), voire inexistante.
- La gestion des clefs est inexistante, les clefs sont statiques.



# Les principales failles du WEP

---

- Mécanisme d'intégrité (ICV) contournable
  - Algorithme linéaire.
- Vecteur d'Initialisation (IV) trop court
  - Existence de dictionnaires.
- Failles dans l'algorithme RC4
  - Prédicibilité de la séquence pseudo aléatoire.
  - Attaque « texte en clair » (écoute passive).
- Authentification mal implémentée
  - Facilite l'attaque « texte en clair » !
  - Contournable.



# Différentes menaces

---

- Confidentialité
  - Découverte de la topologie des points d'accès.
  - Ecoute passive du réseau, capture des informations.
- Intégrité
  - Intrusion, accès et maintien frauduleux sur le réseau.
  - Suppression ou modification de données.
- Disponibilité
  - Perturbation des fréquences radio.
  - Déni de service sur les points d'accès.



# Cas typiques de malveillance

Types de profils :

- **Le « script kiddie »**  
Pas de méthode ni de but précis.
- **Le pirate**  
Objectif défini, individu déterminé.
- **Le (mal)chanceux**  
S'introduit par erreur sur le RLAN !



# A.1- Découverte des points d'accès

---

- Wardriving

- Utilisation d'un ordinateur portable : en voiture, en transports, voire en avion !
- Ou d'un assistant personnel (PDA) pour localiser les points d'accès.

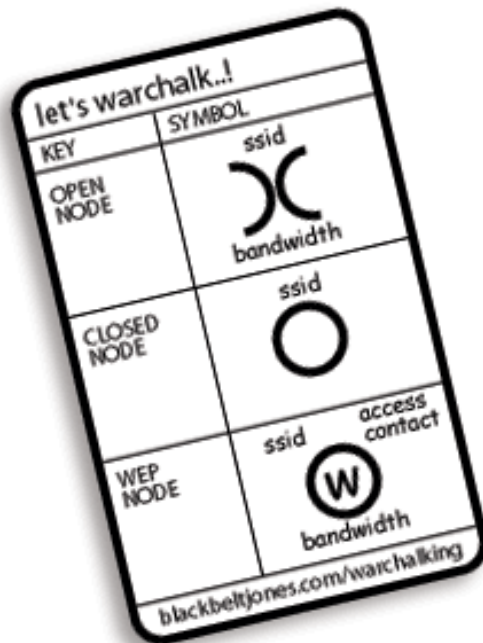
- Ingénierie sociale

- Se faire passer pour un technicien de maintenance, par exemple.



# A.2- Découverte des points d'accès

---



- Sites web avec listes de points d'accès (cartographie GPS)
- Graffitis à proximités des points d'accès (Warchalking)

# B.1- Cassage du chiffrement WEP

---

- **Problèmes :**
  - Les clefs WEP sont statiques.
  - Souvent identiques sur tout le réseau.
  - Et relativement faciles à « casser ».
- **Méthodologie :**
  - Outils simples et répandus (Airsnort, ...)
  - Ecoute passive du trafic : indétectable.
  - Prend de quelques heures à quelques jours selon le trafic.
- **Permet à l'attaquant :**
  - L'écoute du trafic en clair.
  - L'intrusion dans le réseau d'entreprise.
  - La mise en place de points d'accès illégaux.



## B.2- L'attaque

---

- Usurpation d'identité
  - Intrusion dans le réseau d'entreprise.
- Attaques « Man-in-the-Middle »
  - Utilisation de points d'accès illégaux (Rogue Access-Points).



## B.3- Les déni de service

---

- Bloquage des points d'accès par saturation radio.
- Envoi répété d'ordres de désassociation.
- Épuisement des batteries des systèmes nomades.
- Phénomènes indépendants  
(Fours à micro-ondes, foudre, interférences radio, ...)



# Autres facteurs d'insécurité

- Simplicité d'installation : employés installant leur propre point d'accès sans préavis.
- Difficulté de configuration et de maintenance des points d'accès si ils sont nombreux.
- Nouvelles technologies : assistants personnels et ordinateurs portables avec réseaux sans fil intégrés.



# Comment se protéger ?

---

- ✓ Sécuriser l'existant
  - Procédures de base.
  
- ✓ L'Audit de sécurité RLAN
  - Interne ou externe.
  
- ✓ Prévoir l'avenir
  - nouveaux standards, nouvelles attaques).



# 1. Sécurisation : les bases

---

1. Installer la dernière version de microcode.
2. Changer le mot de passe d'administration.
3. Changer le SSID.
4. Activer le WEP.
5. Désactiver la transmission du « beacon ».
6. Activer le filtrage par MAC adresses.



## 2. Sécurisation : la suite...

... et si possible :

2. Mettre des clefs wep dynamiques.
3. Authentifier à l'aide d'un serveur RADIUS.
4. Activer le filtrage par adresses IP.
5. Mettre en place un serveur de logs.
6. Mettre en place un tunnel VPN chiffré.



## 3. Sécurisation : Pour aller plus loin

---

- Dissuader le « war-driver ».
  - Simulation de faux points d'accès (Fake-AP).
- Surveiller les réseaux RLAN.
  - Détection d'intrusion des réseaux sans fil.
- Centraliser la gestion des points d'accès.
  - Optimisation de la maintenance.



# L'audit de sécurité des RLAN

---

- Peut être externalisé ou bien effectué en interne.
- Outils de tests facilement disponibles.
- Attention aux résultats :
  - Pérennité de l'audit.
  - Mauvaise interprétation.



# Méthodologie pour l'audit

---

## 1. Découverte de la topologie réelle :

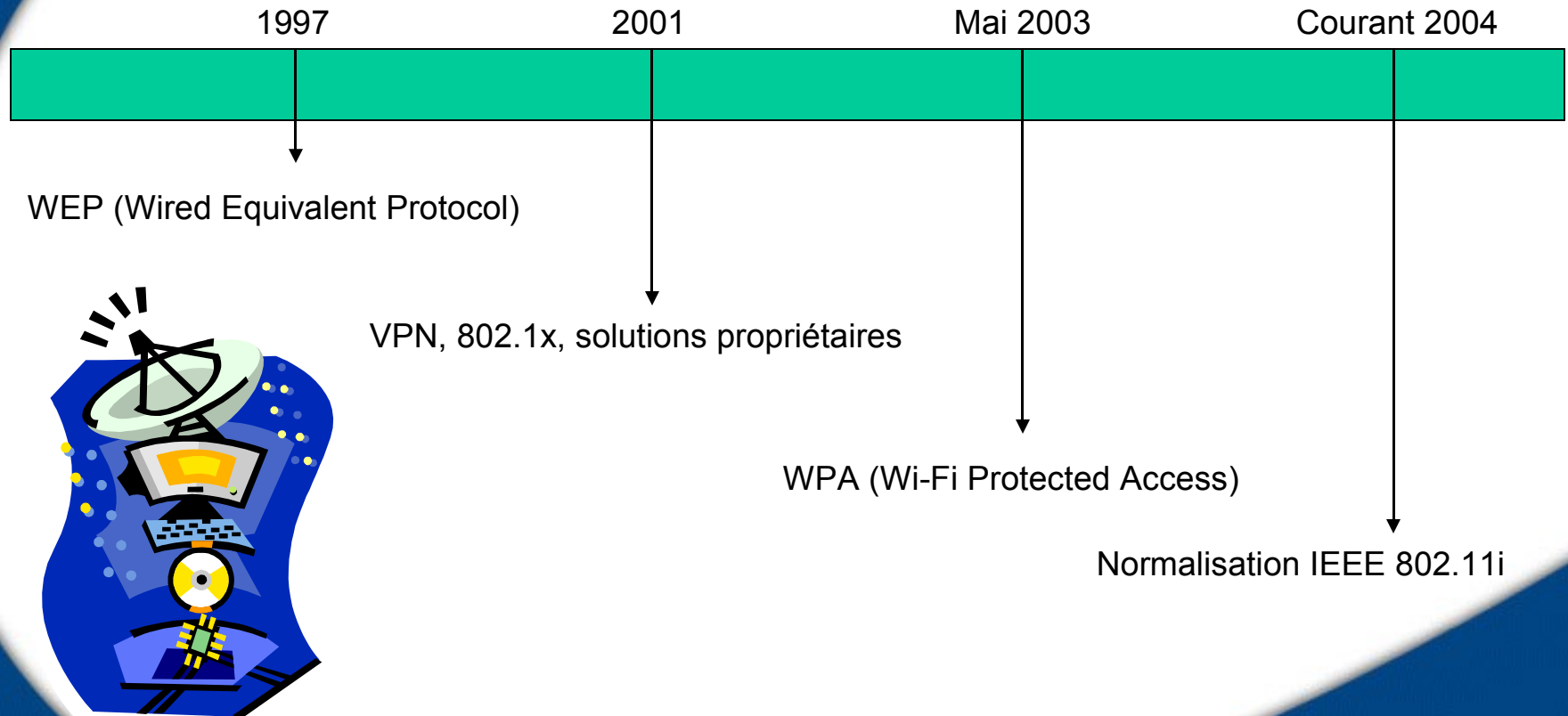
- En « scannant » le périmètre de l'entreprise à l'aide d'un ordinateur portable ou d'un PDA (war-driving).
- Recherche visuelle de points d'accès non déclarés (antennes, bornes, war-chalking, ...).
- Etude des journaux des serveurs DHCP, DNS, IDS.

## 2. Résultats :

- Périmètre de couverture radio.
- Liste des points d'accès non sécurisés.
- Liste des points d'accès non déclarés.



# Amélioration des normes de sécurité



# VPN, 802.1x, solutions propriétaires

---

- VPN (Réseaux privés virtuels)
  - PPTP, L2TP, IPSEC,...
- IEEE 802.1x (Port based Access Control)
  - Authentification préalable lors de la connexion.
- EAP (Extensible Authentication Protocol)
  - Serveur d'authentification (Radius, Kerberos).
- Solutions propriétaires
  - Souvent basées sur EAP et 802.1x.
  - Peu interopérables.



# Wi-Fi Protected Access (WPA)

- **Solution palliative « interopérable »**
  - Origine : consortium Wireless Fidelity Alliance.
  - Possible uniquement sur matériels Wi-Fi.
  - Mise à jour logicielle : peu coûteux.
  
- **Améliorations :**
  - TKIP (Temporal Key Integrity Protocol) :
    - Vecteur d'Initialisation 48 bits.
    - Clefs de chiffrement dynamiques et renforcées.
    - Nouveau mécanisme d'intégrité.
  - Infrastructure de distribution des clefs.
  - Mécanisme d'authentification amélioré.
  - Prise en charge d'EAP et 802.1x.



# La norme IEEE 802.11i

---

- La norme définitive du groupe IEEE
  - Egalement appelée WPA Version 2.
  - Disponibilité courant 2004.
- Tous les avantages de WPA, plus :
  - Algorithme de chiffrement AES CCMP.
  - Mécanisme de pré-authentification.
  - Sécurité des communications point-à-point.
- Mais... tout le matériel devra être remplacé !



# Sanctions pénales

---

- **Perturbation des radio-fréquences**

*Article L.39-1 du Code des Postes  
et Télécommunications*

- **Accès frauduleux**

Articles 323-1 et suivants  
du Code Pénal (loi Godfrain)



# Sanctions pénales - Perturbation

## Article L.39-1 du Code des Postes et Télécommunications

Est puni d'un emprisonnement de six mois et d'une amende de 200 000 F le fait :

- 1° D'établir ou de faire établir un réseau indépendant, sans l'autorisation prévue à l' article L.33-2, ou de le maintenir en violation d'une décision de suspension ou de retrait de cette autorisation ;
  
- 2° De perturber, en utilisant une fréquence ou une installation radioélectrique sans posséder l'attestation de conformité ou l'autorisation prévue à l' article L.89 ou en dehors des conditions réglementaires générales prévues à l'article L.33-3, les émissions hertziennes d'un service autorisé, sans préjudice de l'application de l'article 78 de la loi n° 86-1067 du 30 septembre 1986 précitée.



# Sanctions pénales - Intrusions

---

## Article 323-1 du Code Pénal (loi Godfrain)

Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni d'un an d'emprisonnement et de 15000 euros d'amende. Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de deux ans d'emprisonnement et de 30000 euros d'amende.

## Article 323-2 du Code Pénal

Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de trois ans d'emprisonnement et de 45000 euros d'amende.

## Article 323-3 du Code Pénal

Le fait d'introduire frauduleusement des données dans un système de traitement automatisé ou de supprimer ou de modifier frauduleusement les données qu'il contient est puni de trois ans d'emprisonnement et de 45000 euros d'amende.



# Conclusion

---

- Les RLAN : Une réalité à prendre en compte dans l'entreprise.
- Peu de sécurité, mais cela est en train de changer.
- Il existe actuellement des solutions de sécurité intermédiaires pour les réseaux RLAN déjà en service.



# Quelques sources d'informations

---

- **802.11 et les réseaux sans fil**
  - *Par Paul Mühlethaler – Editions Eyrolles*
- **Etude de la DCSSI**
  - *Présentation synthétique*  
<http://www.ssi.gouv.fr/fr/actualites/synthwifi.pdf>
  - *Analyse des risques et recommandations*  
[http://www.ssi.gouv.fr/fr/actualites/Rec\\_WIFI.pdf](http://www.ssi.gouv.fr/fr/actualites/Rec_WIFI.pdf)
- **Synthèse du CLUSIF**
  - *« menaces, enjeux, parades »*  
<https://www.clusif.asso.fr/fr/infos/event/pdf/RSF.pdf>





**CLEAR CHANNEL**

---

**Merci pour votre  
attention**

