



HERVÉ SCHAUER CONSULTANTS

Cabinet de Consultants en Sécurité Informatique depuis 1989

Spécialisé sur Unix, Windows, TCP/IP et Internet

# Sécurité des réseaux sans fil

**.: Fête de l'Internet Mobile :.**

**26 Mars 2003**

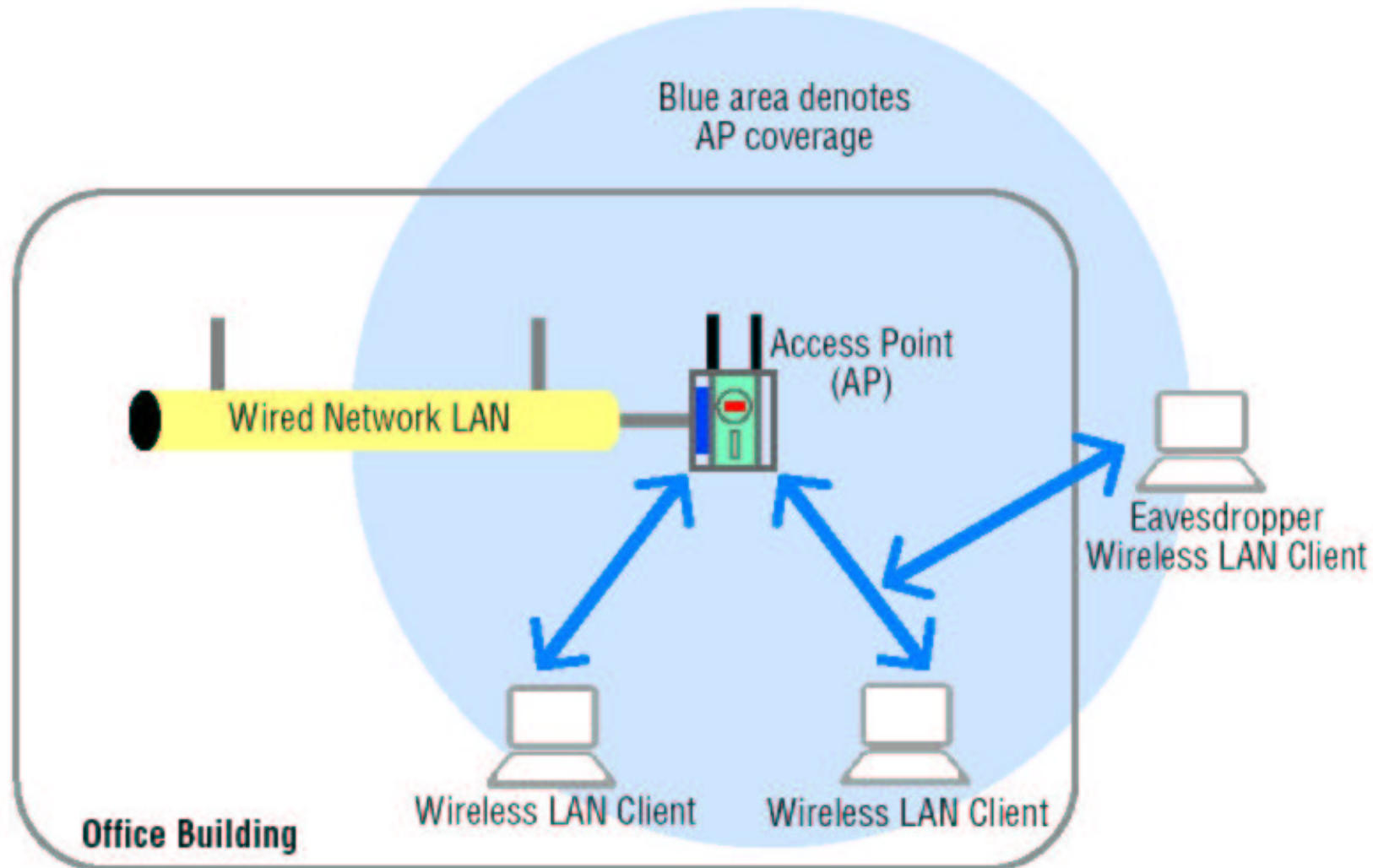


**Hervé Schauer**

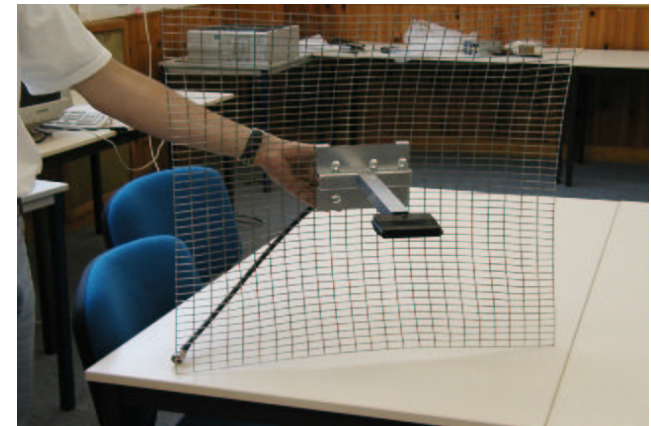
<Herve.Schauer@hsc.fr>

- × Risques liés aux réseaux sans fil
- × Sécurité dans les réseaux sans fil
  - × Deuxième génération de norme : 802.11g
- × Sécurisation des réseaux sans fil
  - × Authentification 802.1X
    - × Cadre, Principe, Pré-requis
    - × Architecture d'intégration
- × Audits de réseaux sans fil
  - × Exemple avec WifiScanner
- × Conclusion
- × Ressources et remerciements

- × Attaque de l'extérieur de l'entreprise

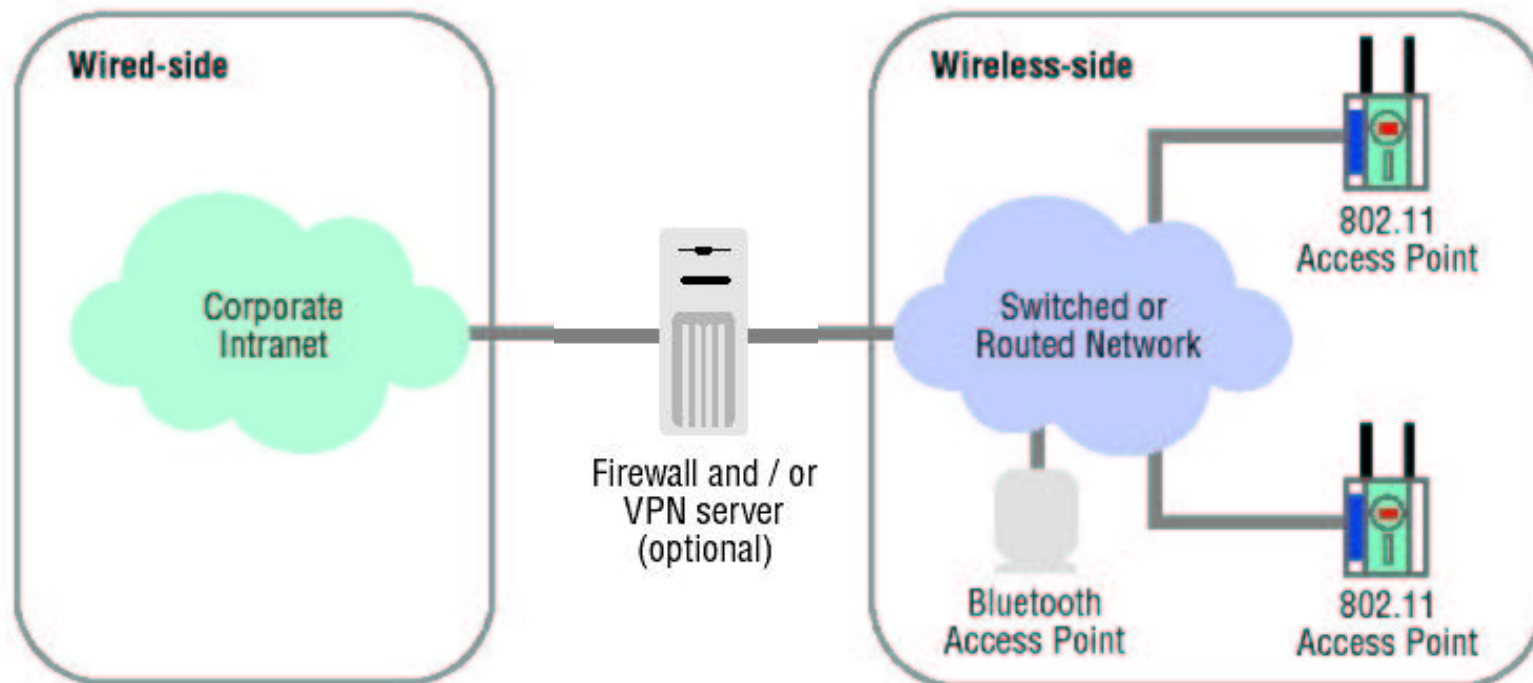


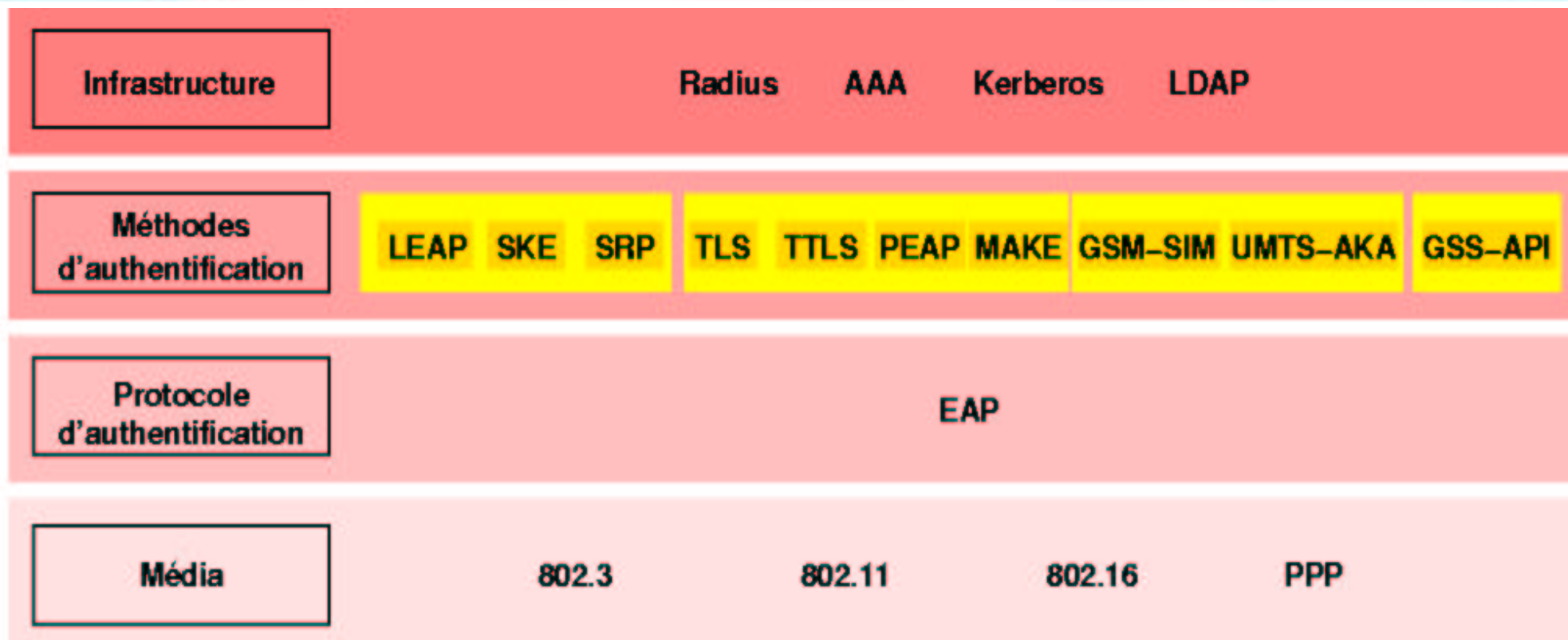
- × Connexion involontaire ou automatique sur le mauvais réseau
- × Vol de l'authentification de l'utilisateur
  - × Attaque de l'intercepteur avec une fausse borne
  - × Airjack
- × Vol d'information par écoute illégale du réseau
  - × NetStumbler
- × Intrusion pas le réseau sans fil
- × Brouillage du réseau
  - × Airjack
- × Consommation complète de la batterie de l'équipement



- × Norme IEEE 802.11g : 54 Mbits/s sur 2,4 Ghz
  - × Approuvée par le groupe de travail en février 2003
- × Norme IEEE 802.11i : sécurité dans les réseaux 802.11\*
  - × Utilise le contrôle d'accès par port d'IEEE 802.1X (avril 2001)
  - × CCMP (*Counter-Mode/CBC-MAC Protocol*)
  - × TKIP (*Temporal Key Integrity Protocol*)
    - × Génération de clefs dynamiques pour le WEP (*Wired Equivalent Privacy*)
  - × WRAP (*Wireless Robust Authenticated Protocol*)
  - × Gestion des clefs propre à l'IEEE et remplacement de RC4 par AES
  - × Dépend des normes IETF EAP et Radius
    - × Synchronisation et cohérence demandent du temps
- × Problèmes de sécurité de 802.11b (Wi-Fi) résolus dans cette nouvelle génération
- × La sécurité demeure un **choix volontaire** : il faut la configurer

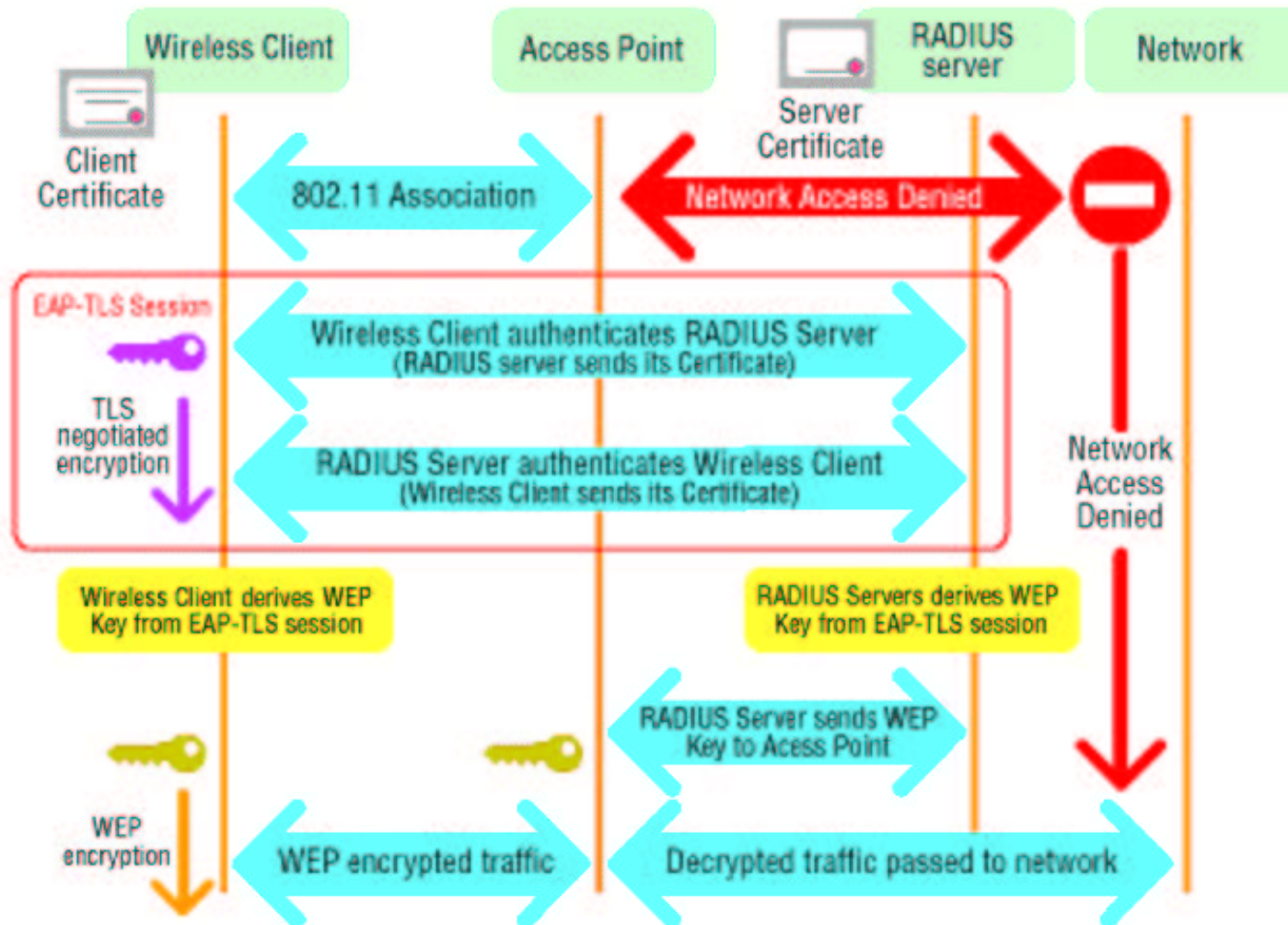
- × Cloisonner le réseau sans fil par rapport aux réseaux filaires
- × Mettre en œuvre un contrôle d'accès au réseau sans fil
- × Authentifier par le réseau les postes ayant accès au réseaux sans fil
  - × Norme IEEE 802.1X : contrôle d'accès par authentification par port





© Copyright Hervé Schauer Consultants 2002

- × Méthodes pour réseaux d'entreprises
  - × Passé : LEAP, Présent : EAP-TLS, Futur : PEAP
- × Méthodes pour opérateurs
  - × Présent : mot de passe + usurpation HTTP/HTTPS, Futur : EAP-SIM



- × AP n'ouvre le port que pour EAPOL
- × AP transforme EAPOL en EAP dans Radius
- × AP ouvre la session TLS vers serveur Radius
- × Authentification réussie, AP reçoit la clef WEP et ouvre le port totalement

- × Avoir ou mettre en place un service de gestion des utilisateurs
- × Déployer des bornes supportant les fonctionnalités 802.1X
- × Avoir ou déployer sur tous les postes clients l'authentification 802.1X
  - × Même quand 802.1X est disponibles en standard, la méthode d'authentification souhaitée ne l'est pas toujours
  - × Logiciels tiers existent pour tous les clients
- × Maîtriser les effets induits
  - × Temps de connexion au réseau plus lent pour les utilisateurs
  - × Incompatibilités entre l'authentification et l'itinérance

## × Entreprise

- × Mettre en place une infrastructure de réseau sans fil IEEE 802.11b/g
  - × Meilleur moyen de lutter contre les bornes sauvages et la connexion accidentelle au voisin
- × Considérer l'infrastructure sans fil comme un réseau externe
- × Segmenter l'infrastructure de réseau sans fil avec des VLAN
  - × Séparer réseau sans fil pour l'entreprise et réseau de *HotSpot*
  - × Détecter les intrus par les adresses MAC
  - × Tester l'étanchéité des VLAN sans fil
- × Travailler la sécurité physique des ondes dans l'espace
  - × Régler la puissance des bornes et positionner les antennes de manière appropriée
- × Sécuriser les bornes et appliquer les correctifs de sécurité
- × Déployer les logiciels d'authentification sur les clients
- × Considérer les technologies alternatives à IEEE 802.11b/g (WiFi)
  - × Réseaux sur courants porteurs, IEEE 802.15.3 (Bluetooth 2), IEEE 802.11a (WiFi5), IEEE 802.16a, IEEE 802.16b (réseaux métropolitains)



- × Opérateur de *HotSpots*
  - × Utiliser les authentications à base de carte SIM (EAP-SIM, EAP-AKA)
  - × Utiliser HTTPS pour l'authentification par usurpation HTTP
  - × Sécuriser les flux d'authentification Radius depuis les bornes quand ils doivent passer sur Internet
    - × Tunnel chiffré IPsec si la borne ou l'équipement local le permet
  - × Mettre en place si possible une infrastructure d'authentification et de comptage hors du réseau d'accès à l'Internet
  - × Cloisonner comme pour tout ISP sa propre infrastructure de celle offrant Internet
  - × Intégrer le caractère unique à un endroit donné d'un réseau 802.11b

## × Objectifs

- × Détecter les réseaux sans fil IEEE 802.11b sauvages
- × Détecter les stations clientes mal ou auto-configurées
- × Evaluer la sécurité des réseaux sans fil
- × Valider les mécanismes de contrôle d'accès mis en place

## × Méthodologie

- × Parcours du périmètre avec un équipement portable
- × Utilisation d'antennes pour amplifier la réception
- × Recherche de SSID, de clef WEP, des mots de passe des bornes
- × Réalisation de tests d'intrusion

## × Outils d'audit

- × Kismet, WifiScanner





La sécurité des réseaux sans fil est possible

Questions ?

[www.hsc.fr](http://www.hsc.fr)

- × <http://www.hsc.fr/ressources/themes.html#wireless>
  - × Ensemble des ressources liées au sujet des réseaux sans fil
- × <http://www.hsc.fr/ressources/presentations/jtr2002-802.11b/>
  - × Présentation et vidéo en ligne, octobre 2002
- × <http://www.hsc.fr/ressources/outils/wifiscanner/>
  - × Logiciel d'audit de réseaux sans fil
- × [http://www.hsc.fr/ressources/articles/securisation\\_802.11b/](http://www.hsc.fr/ressources/articles/securisation_802.11b/)
  - × Article sur la sécurité des réseaux sans fil, juillet 2002
- × <https://www.clusif.asso.fr/fr/infos/event/pdf/RSF.pdf>
  - × Réseaux sans fil : menaces, enjeux et parades, Clusif, février 2003

- × Christophe Serda pour les schémas de Madge
  - × *Réutilisés avec autorisation*
- × Jérôme Poggi et Thomas Seyrat pour leurs photos
- × Jérôme Poggi et Alexandre Fernandez pour leur relecture