

Sécurité des réseaux sans fil 802.11b et authentification

OSSIR / Groupe SUR

9 Juillet 2002

Hervé Schauer
<Herve.Schauer@hsc.fr>

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



Copyright Hervé Schauer Consultants 2002 - Reproduction Interdite

Sécurité des réseaux sans fil (1/4)

Agenda

- Hervé Schauer Consultants
- Panorama et technologies des réseaux sans fils
 - Technologies de réseaux sans fil
 - Réseaux locaux
 - Réseaux personnels
 - Bus série
 - Réseaux métropolitains
 - Réseaux cellulaires
- Problématique de la sécurité
 - Intrusion
 - Déni de service sur la batterie
- Principes dans un réseau sans fil 802.11b

- Les problèmes avec les réseaux sans fils
 - Propriétés du média
 - Liberté topologique
 - Caractéristiques de la technologie
 - Caractéristiques des implémentations
 - Fonctionnalités des équipements
 - Positionnement dans l'architecture

- Les attaques contre les réseaux sans fil

- Solutions
 - Gérer ses réseaux sans fil
 - Utiliser la sécurité des bornes
 - Utiliser le mécanisme de sécurité de 802.11b : WEP
 - Auditer et surveiller les réseaux sans fil
 - Découverte de borne
 - Verbose du protocole
 - Surveillance
 - Recherche des réseaux 'sauvages'
 - Audit des réseaux locaux sans fil
 - Antennes et cartes
 - Outils d'audit

Sécurité des réseaux sans fil

Agenda

(4/4)

- Solutions (suite)
 - Authentifier les utilisateurs de réseaux sans fil
 - Portail HTTP
 - IEEE 802.1X
 - ▷ Principes
 - ▷ Protocole
 - ▷ Cadre
 - ▷ Méthodes d'authentification
 - LEAP
 - EAP-TLS
 - PEAP
 - IEEE 802.11i
 - ▷ TKIP
 - Autres possibilités
 - Architecturer correctement ses réseaux sans fil
- Conclusion
- Sélection de ressources, Acronymes, Remerciements

Hervé Schauer Consultants (1/2)

- Cabinet de consultants en sécurité Unix, Windows, TCP/IP et Internet depuis 1989
- 14 consultants
- Expérience de la sécurité Unix depuis 1987
- Expérience de la sécurité Internet depuis 1991
- Expérience de la sécurité Windows 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)

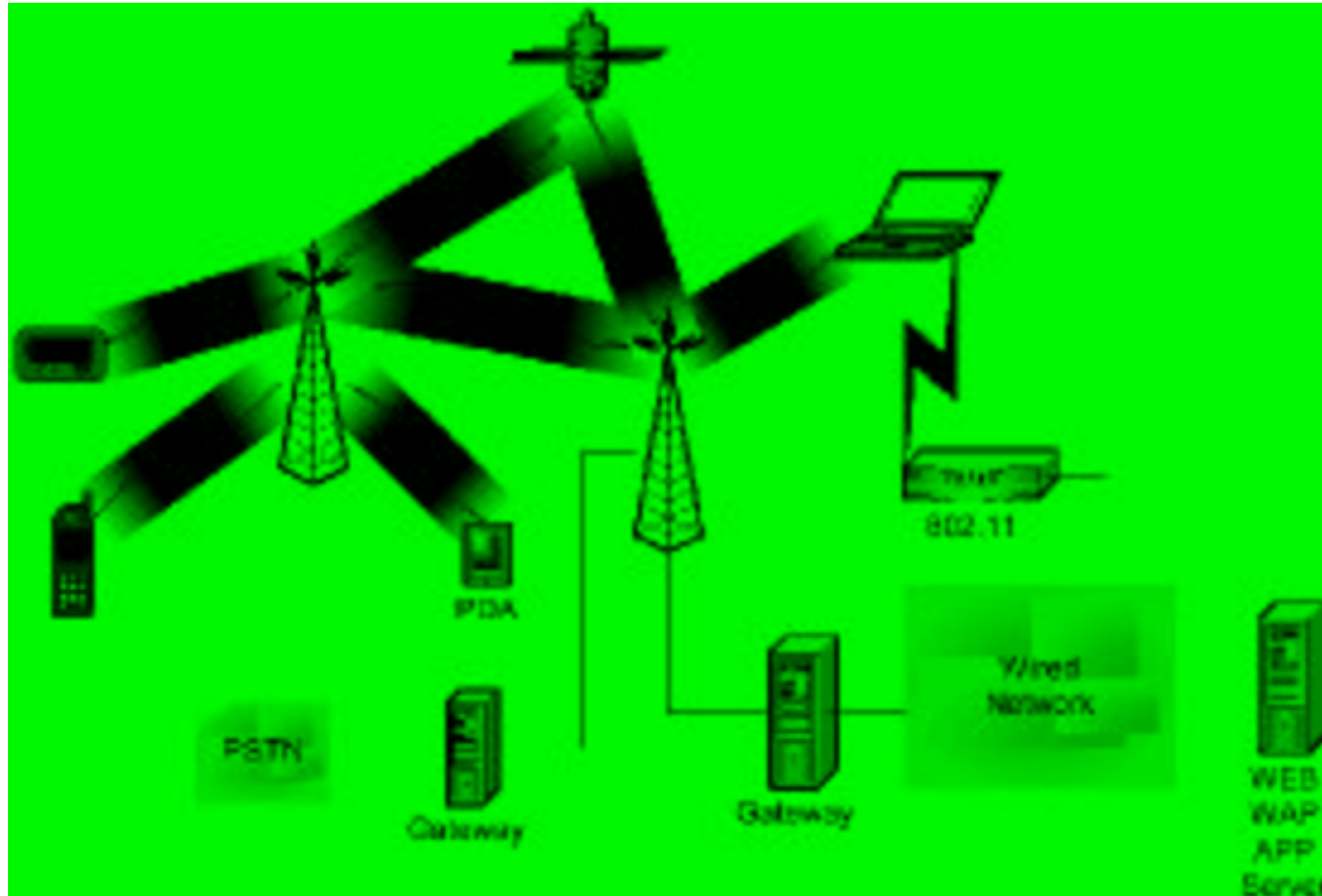
- Audits de sécurité
 - Réseaux, application, référentiels
- Enquêtes et investigations
- Tests d'intrusion
- Tests de vulnérabilités assistés : TSAR

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

- Programme complet de 17 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

Panorama global du monde sans fil



Technologies de réseaux sans fil (1/6)

Réseaux locaux sans fil (WLAN) : existant

- Equivalents d'Ethernet IEEE 802.3
- Nombreuses technologies propriétaires sur 2,4 Ghz
 - Concurrentes aux normes mais abandonnées car supplantées par 802.11
 - ▷ Exemples : Home RF d'Intel, OpenAir
 - Pour des applications spécifiques qui souhaitent éviter l'utilisation d'une norme
 - ▷ Exemple : Siemens transport
- IEEE 802.11b (WiFi), sur 2,4 GHz, 11 Mb/s
 - La principale technologie, disponible depuis 1997
 - Cartes 22 Mb/s disponibles depuis 2002, mais propriétaires 3Com
- IEEE 802.11a (WiFi5), sur 5 GHz, 54 Mb/s
 - Disponible depuis fin 2001 : Airaya, Cisco, Enterasys, Proxim, etc

Technologies de réseaux sans fil (2/6)

Réseaux locaux sans fil (WLAN) : futur

- IEEE 802.11g, IEEE 802.11e
 - Remplaceront IEEE 802.11b et IEEE 802.11a
 - Pas disponible sur le marché, 802.11g annoncé pour fin 2002
 - Possibilité de mise à jour logicielle de 802.11b vers la version de base de 802.11g
 - Possibilité de mise à jour matérielle dans un équipement existant en ajoutant une carte 802.11g ou 802.11e
 - Qualité de service définie dans IEEE 802.11f
 - Gestion dynamique de la puissance et des fréquences dans IEEE 802.11h

- ETSI Hiperlan 2, sur 5 GHz
 - Norme européenne concurrente de IEEE 802.11a et IEEE 802.11e
 - Inclu la qualité de service et la gestion dynamique des fréquences
 - Disponibilité sur le marché prévue fin 2003

Technologies de réseaux sans fil (3/6)

Réseaux personnels sans fil (WPAN)

- Réseaux personnels sans fil (WPAN) : existant
 - IEEE 802.15.1 (Bluetooth), sur 2,4 Ghz
 - Disponible depuis début 2001 en carte PCMCIA
 - Intégré en standard dans Windows XP

- Réseaux personnels sans fil (WPAN) : futur
 - IEEE 802.15.3 (Bluetooth 2), sur 2,4 Ghz
 - Débits de 11, 22, 33, 44, & 55 Mb/s
 - Sécurité de groupe, authentification, gestion de clés, confidentialité...
 - Disponibilité prévue en 2003
 - IEEE 802.15.4 (Zigbee), sur 2,4 Ghz
 - Débits de 20kb/s et 250 kb/s
 - Très basse consommation, coût du composant < 1 euro
 - Norme terminée en 2001, disponibilité prévue en 2003

Technologies de réseaux sans fil (4/6)

Bus série sans fil (WSB)

- Bus série sans fil (WSB) : existant
 - IEEE 802.15.1 (Bluetooth)
 - IEEE 1394 (FireWire ou i.Link) sur 802.11 ou Hiperlan 2

- Bus série sans fil (WSB) : futur
 - Version sans fil d'IEEE 1394
 - Nombreuses démonstrations de salons
 - Pas disponible sur le marché

Technologies de réseaux sans fil (5/6)

Réseaux métropolitains (WMAN)

- Réseaux métropolitains (WMAN) : existant
 - Nombreuses technologies propriétaires pour la BLR, 2 Mb/s
 - PMP/MMDS (1,9 GHz, 3,5 GHz, 10,5 GHz, 26 GHz)
 - LMDS (26 GHz, 28 GHz, 31 GHz, 40 GHz)
 - IEEE 802.11b, 802.11a, etc
- Réseaux métropolitains (WMAN) : futur
 - IEEE 802.16 (10 GHz à 66 GHz)
 - Disponibilité sur le marché prévue fin 2003
 - IEEE 802.16a (2 GHz à 11 GHz), 32 Mb/s à 134 Mb/s
 - Matériel basé sur le draft en cours disponible depuis fin 2001 pour 3,5 GHz : Alvarion (ex-Breezecom), Runcom
 - IEEE 802.16b, sur 5 GHz (WHUMAN, sans license)
 - Disponibilité prévue pour 2003-2004
 - Un concurrent de l'UMTS dans les zones à forte densité de population ?

Technologies de réseaux sans fil (6/6)

Réseaux cellulaires (WWAN) :

- Réseaux cellulaires (WWAN) : existant
 - Tetra (380 MHz, 410 MHz et 800 MHz), via un opérateur ou autonome multipoints, 9,6 Kb/s
 - CDPD (800 MHz) utilisé par Palm.net, 19,2 Kb/s
 - GSM (900 MHz, 1800 MHz, 1900 MHz aux États-Unis), 56 Kb/s avec GPRS

- Réseaux cellulaire (WWAN) : futur
 - UMTS (1,9 GHz, 2 GHz, 2,1 GHz, ou 2,5 GHz), 384 Kb/s
 - Disponibilité sur le marché prévue en 2004

- Toutes les technologies citées supportent IP

Principales technologies en réseau local

Catégorie	WSB et WPAN	WLAN	WLAN	WSB
Nom commercial	Bluetooth	WiFi	Wireless	FireWire
Norme	IEEE 802.15	IEEE 802.11b	802.11a	Wireless IEEE 1394

www.bluetooth.com www.wirelessethernet.org
www.ieee802.org/15 www.ieee802.org/11 grouper.ieee.org/groups/1394/1

Consommation électrique	très forte	faible	forte	forte
-------------------------	------------	--------	-------	-------

Débit type	0.4 Mb/s	11 Mb/s	54 Mb/s	300 Mb/s
------------	----------	---------	---------	----------

Distance type	10 m	100 m	100 m	10 m
---------------	------	-------	-------	------

Bande de fréquence	2,4 GHz	2,4 GHz	5 GHz	5 GHz ou 60 GHz
--------------------	---------	---------	-------	-----------------

Topologie type	Point-à-point	Multipoint	Multipoint	Point-à-point
----------------	---------------	------------	------------	---------------

Protocole principal	Audio et IP	L2CAP	IP	Video MPEG
Support d'IP	PPP		natif	natif
Emulation Ethernet				IETF RFC2734
IP over Bluetooth			IP over IEEE 1394	



Problématique de la sécurité (1/3)

Intrusion sur IP

- IEEE 802.11 (WiFi)
 - Support d'IP de manière native
 - Une carte allumée suffit généralement pour être attaqué
 - La connexion est permanente
- IEEE 802.15 (Bluetooth)
 - Support d'IP en natif variable
 - Natif sur Windows XP
 - Doit être configuré volontairement sur unix et les anciens Windows
 - ▷ Emulation ethernet
 - ▷ PPP
 - Une carte allumée ne suffit généralement pas pour être attaqué au niveau du système d'exploitation
 - La connexion est permanente, mais pas la session si PPP est utilisé

Problématique de la sécurité (2/3)

Intrusion sur IP

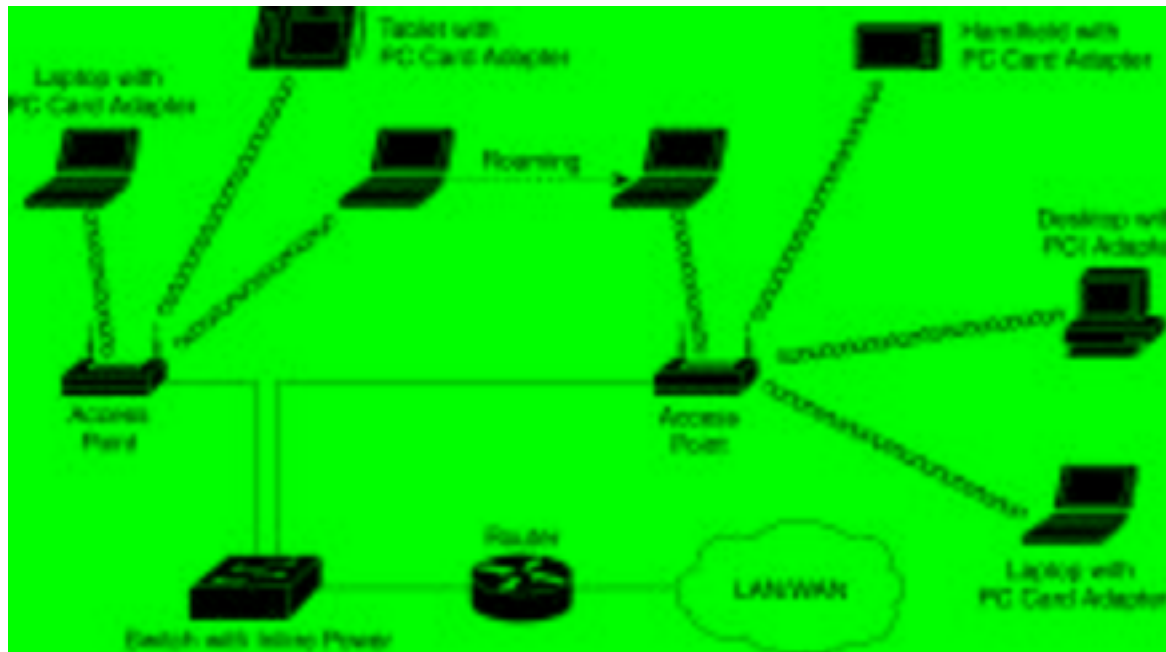
- GSM/GPRS
 - En général pas de support d'IP de manière native
 - IP doit être configuré volontairement
 - PPP
 - Possibilité de tunnels privés
 - La connexion est établie et coupée par l'utilisateur, il faut une session en cours pour être attaqué
 - Identique à tout autre accès en dialup-IP
- Une carte mixte permettant l'itinérance GSM/GPRS et IEEE 802.11b supporte IP de manière native

Problématique de la sécurité (3/3)

Déni de service sur la batterie

- IEEE 802.15 (Bluetooth)
 - Fonctionnement conçu pour une faible consommation d'énergie
 - Utilise la batterie de l'équipement hôte
 - Principale attaque : déni de service sur la batterie de l'équipement
- IEEE 802.11 (WiFi)
 - Fonctionnement consommateur d'énergie
 - Batterie propre à la carte 802.11b sur les assistants personnels
 - Pas d'attaque sur la batterie
- GSM/GPRS
 - Consommation supérieure de celle de l'usage du téléphone à la voix
 - Pas d'attaque sur la batterie

Principes dans un réseau sans fil 802.11b (1/3)



Principes dans un réseau sans fil 802.11b (2/3)

- Composants :
 - Borne ou point d'accès (AP)
 - Concentrateur sans fil
 - Potentiellement aussi un pont et un routeur
 - Carte réseau (NIC)
 - Interface Ethernet sur l'équipement
- Deux modes
 - Mode '*ad-hoc*' : dialogue direct entre deux interfaces Ethernet sans fil (point à point)
 - Mode '*infrastructure*' : dialogue entre une interface Ethernet sans fil et une borne (multipoint)
- 14 canaux
 - Plusieurs réseaux peuvent cohabiter au même endroit sur des canaux différents

Principes dans un réseau sans fil 802.11b (3/3)

- 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

Succès des réseaux sans fils

- 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

Problèmes avec les réseaux sans fils

- Les caractéristiques des réseaux sans fil qui posent problème en sécurité en ouvrant des vulnérabilités :
 - Propriétés du média
 - Liberté topologique
 - Caractéristiques de la technologie
 - Caractéristiques des implémentations
 - Fonctionnalités des équipements
 - Positionnement dans l'architecture des réseaux

Propriétés du média

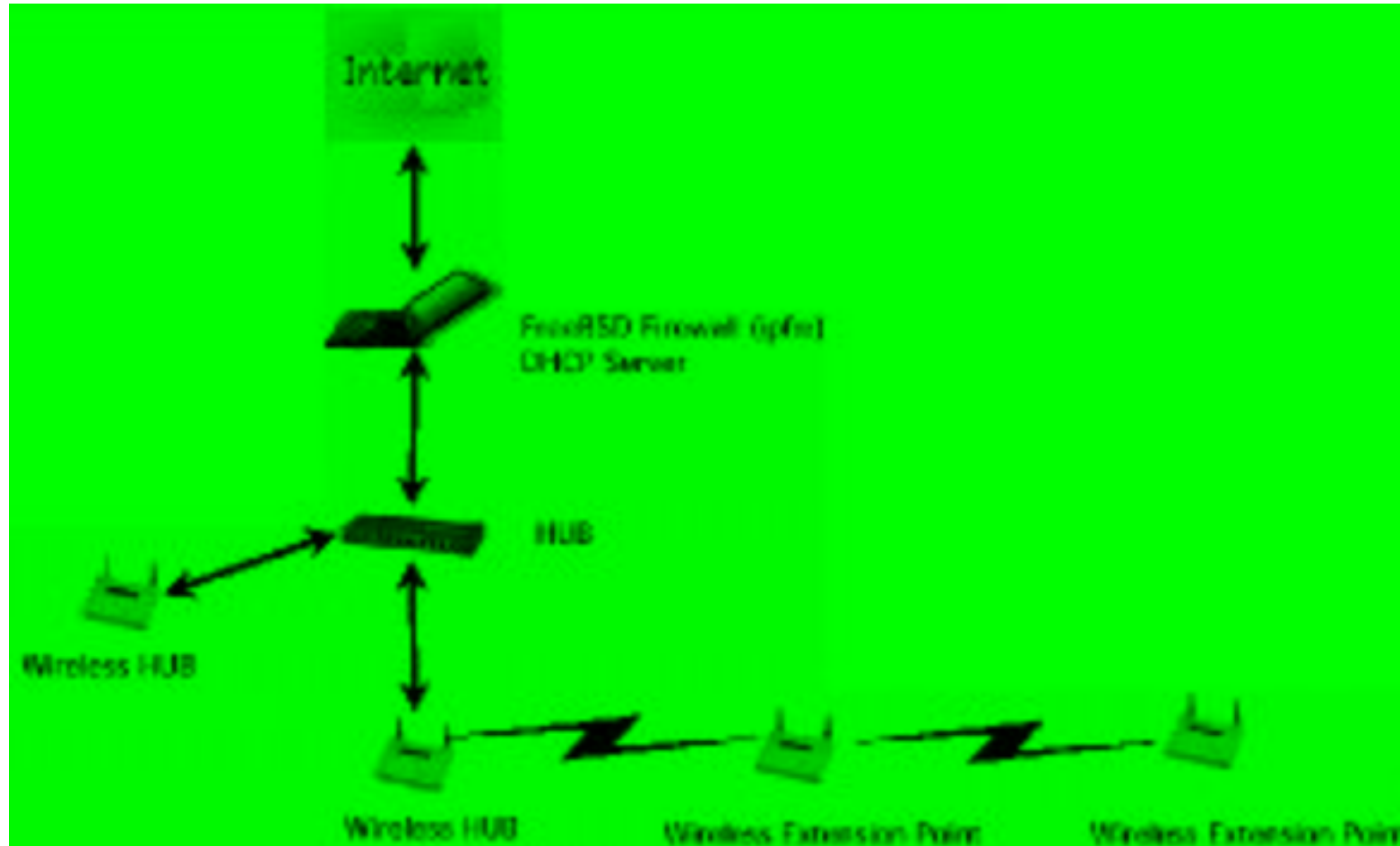
- Ondes radio-électriques
- Support pas protégé des signaux externes
 - Brouillage, déni de service
- Caractéristiques de propagation complexes
 - Dynamiques et difficiles à prévoir
 - Absorption, diffraction, réfraction, réflexion
 - Humidité, Verre, Béton, Moteurs, Fours à micro-ondes, etc
- Pas de frontière absolue ni observable
 - Ecoutes et interceptions aisées
 - Insertion de trafic possible
 - Pénétration du réseau

Liberté topologique (1/2)

- Topologie dynamique
 - Choix du mode : '*ad-hoc*' ou '*infrastructure*'
 - En mode '*infrastructure*', choix entre les bornes.
- Utilisation des liaisons sans fil entre bornes pour l'architecture du réseau
 - La borne agit comme un répéteur
- Une carte ou une borne peuvent potentiellement dialoguer avec plusieurs autres cartes ou bornes à la fois
- Itinérance (*roaming*)

Liberté topologique (2/2)

○ Exemple de la topologie utilisée lors d'une conférence :



Caractéristiques de la technologie (1/2)

- Contraintes de placement d'une borne : courant électrique et connexion filaire
 - Antennes mal placées et mal orientées
- Envoi permanent de paquets de contrôle (*beacon*)
 - Détection toujours assurée
- Diffusion
 - Une borne sans fil est un concentrateur (*hub*) et n'est pas un commutateur(*switch*)
 - Chaque carte Ethernet reçoit tout le trafic de la borne
 - De toutes les bornes
 - Sur les 14 canaux

Caractéristiques de la technologie (2/2)

- Principe de fonctionnement avec une configuration minimale
 - Implique un protocole automatique : STP (IEEE 802.1d)
 - Possible de transformer un PC sous Linux en borne
 - opensource.instant802.com
 - people.ssh.com/jkm/Prism2/
- Utilisation de clefs de chiffrement (WEP) sans mécanisme de distribution des clefs
 - Difficile à gérer, donc faible usage du chiffrement
- Spécification du protocole ne chiffrant pas l'identificateur de réseau (SSID), ni les trames de gestion en général

Caractéristiques des implémentations (1/2)

- Avec Agere (ex-Lucent) ou Intel
 - Sur Windows : stockage des identificateurs de réseau et des clefs de chiffrement dans la base de registres en lecture pour tous
 - www.cqure.net/tools03.html
 - Sur les autres systèmes d'exploitation : stockage dans un fichier
- Avec Cisco : stockage des clefs de chiffrement dans la carte elle-même
 - Vol de la carte, vol de l'ordinateur portable avec la carte
- Sur les bornes, les clés sont stockées localement

Caractéristiques des implémentations (2/2)

- Documentation des concentrateurs Aironet publiée en Décembre 1998
- Aironet a été racheté par Cisco
 - www.personaltelco.net/download/docs/aironet.pdf

Security Features

The Ethernet or Token Ring Bridge employs Spread Spectrum Technology, previously developed for military anti-jamming and low probability of intercept radio systems. The Ethernet or Token Ring Bridge must be set to the same System Identifier (SSID) as all

other Aironet devices on the wireless infrastructure. Units with a different SSID will not be able to directly communicate with each other.

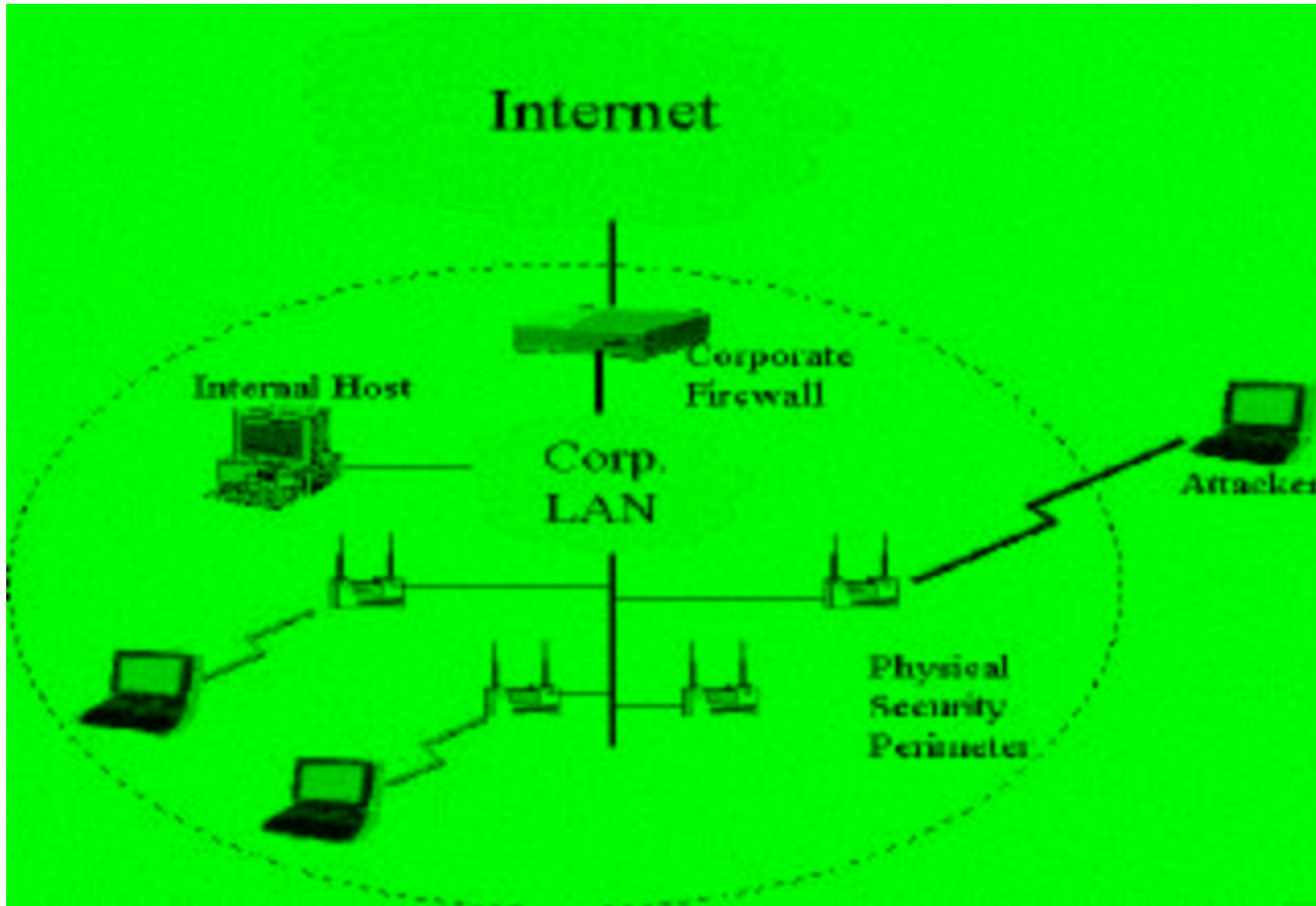
Fonctionnalités des équipements

- Equipements bon marché et faciles à mettre en oeuvre
 - Déploiement 'sauvage' de réseaux 802.11b
 - Sans que le service réseau soit consulté
 - Sans configuration appropriée ni gestion
- Bornes mises en oeuvre "par défaut", sans sécurité
 - Pas d'identificateur de réseau (SSID) ou un SSID facilement devinable
 - SSID donnant des informations sur le propriétaire du réseau
 - Pas de mise en oeuvre du chiffrement (WEP)
 - Communauté SNMP par défaut
 - Administration par une interface web ouverte à tous
 - Accessible par le réseau sans fil

Positionnement dans l'architecture

- De nombreuses bornes déployées dans le réseau interne, à l'intérieur du périmètre de l'entreprise
 - Responsables réseau ne réalisant pas les conséquences
 - Bornes individuelles connectées à la place de l'ordinateur
 - Puissance réglée au maximum
- Pas d'authentification ni sécurité appropriée
- Pas de construction d'une architecture appropriée
 - Facilité apparente de déploiement et d'installation

Attaques contre les réseaux sans fil (1/2)



Attaques contre les réseaux sans fil (2/2)

- Le *War Driving*
 - Quadrillage d'une ville avec un ordinateur portable, une carte 802.11b et une antenne externe
 - De nombreux logiciels sont disponibles
 - Un récepteurs GPS pour la localisation
- Le parking visiteurs
 - Plus de sécurité physique à outrepasser
- Conséquences
 - Ecoute de trafic
 - Insertion de trafic
 - Introduction d'une station ou d'un serveur illicite dans le réseau
 - Rebonds

Solutions

- Gérer ses réseaux sans fil
- Utiliser la sécurité des bornes
- Utiliser le mécanisme de sécurité de 802.11b : WEP
- Auditer et surveiller les réseaux sans fil
 - Surveillance, Recherche, Audit, Antennes, Outils
- Authentifier les utilisateurs de réseaux sans fil
- Architecturer correctement ses réseaux sans fil

Gérer ses réseaux sans fil (1/4)

- La sécurité est découpée entre
 - Le service du RSSI
 - Le service sécurité production ou SOC (Security Operation Center)

- Le service du RSSI :
 - Rattaché à une direction générale

- Le service sécurité production ou SOC
 - Rattaché à la direction informatique

Gérer ses réseaux sans fil (2/4)

- Le service gestion de réseau (ou NOC) gère le réseau
- Le service informatique gère les serveurs centraux
- Le service bureautique gère les PC et les serveurs bureautiques
- Le service de production sécurité ou SOC(*Security Operations Center*) gère
 - La journalisation centralisée et son analyse
 - La détection d'intrusion
 - Les interconnexions avec l'extérieur
 - Accès Internet, VPN pour accès distants, extranets, plate-forme de commerce électronique, accès par des réseaux sans fil

Gérer ses réseaux sans fil (3/4)

- Le SOC gère tous les périphérique situés sur le périmètre du réseau
 - Les bornes d'accès sans fil sont sur le périmètre
- Le SOC gère l'authentification des utilisateurs de l'extérieur
 - Au minimum pour l'accès distant
- La gestion des réseaux sans fil réussi quand elle est réalisée par une équipe formée et compétente
- **Les bornes doivent être gérées par le SOC**
- Exceptions possibles
 - Bornes utilisées uniquement pour construire des liens point à point entre des réseaux distants, configurées pour n'accepter aucune connexion cliente

Gérer ses réseaux sans fil (4/4)

- Le RSSI doit
 - Ajouter les réseaux sans fil dans la sensibilisation des utilisateurs à la sécurité
 - Expliquer le danger des réseaux sans fil aux utilisateurs
 - Expliquer qu'une connexion sans fil sans authentification est un incident de sécurité devant être reporté à la sécurité
- Ajouter les audits de recherche de réseaux aux audits sur son périmètre
- Intégrer les problématiques des réseaux sans fil dans sa politique de sécurité et ses procédures
 - ISO17799 ignore l'existence des réseaux sans fil

Utiliser la sécurité des bornes (1/2)

- Gérer et superviser des bornes uniquement par l'interface filaire
- Désactiver tous les services d'administration sur l'interface sans fil
 - Interface Web
 - SNMP
 - TFTP
- Modifier les mots de passe par défaut
 - SSID
 - Clef WEP
 - Communautés SNMP
- Choisir des mots de passe forts
 - Sans lien avec le réseau ou l'entreprise

Utiliser la sécurité des bornes (2/2)

- Supprimer la diffusion du SSID
 - Le SSID du client doit correspondre à celui de la borne pour s'associer
 - Combiné avec le WEP, cela constitue une barrière vis-à-vis de certains logiciels
- Mettre à jour son *firmware* régulièrement
- Filtrage par adresse MAC (adresse Ethernet)
 - Seules les cartes enregistrées sont autorisées à utiliser le réseau
 - Gestion quotidienne lourde
 - L'adresse MAC figure en clair dans tous les trames, même si WEP est employé
 - Possible d'écouter du trafic pour repérer les adresses MAC valides
 - Génération de trames falsifiées avec une adresse MAC valide
- Filtrage IP

Mécanisme de sécurité de 802.11b: WEP (1/3)

- WEP : Wired Equivalent Privacy
- WEP première génération
 - La grande majorité des équipements actuels
 - Clef secrète partagée
 - Tout le monde possède la même clef
 - Clef statique
 - Basé sur l'algorithme de chiffrement RC4
 - Problème d'initialisation
 - Pas de gestion des clefs
 - Les clefs sont configurées et déployées manuellement
 - Rarement changées

Mécanisme de sécurité de 802.11b: WEP (2/3)

- WEP première génération (suite)
 - Attaque par dictionnaire contre la clef de chiffrement
 - www.lava.net/~newsham/wlan
 - Début 2001
 - Une clef est un mot de passe partagé potentiellement faible
 - Attaque contre le WEP statique par l'université de Berkeley
 - Février 2001
 - www.isaac.cs.berkeley.edu/isaac/wep-faq.html
 - Attaque sur l'authentification par l'université du Maryland
 - Avril 2001
 - Identifie une faille dans le schéma d'authentification 802.1X d'un constructeur
 - www.missl.cs.umd.edu/Projects/wireless/infrastructure.shtml
 - Attaque contre le WEP par Fluhrer, Mantin, et Shamir
 - *"Weaknesses in the Key Scheduling Algorithm of RC4"*
 - Juillet 2001
 - Attaque pragmatique contre le vecteur d'initialisation de RC4 tel que spécifié dans WEP

Mécanisme de sécurité de 802.11b: WEP (3/3)

- WEP première génération (suite)
 - Nombreux logiciels de mise en oeuvre des attaques
 - WEPCrack, Aircsnort, PrismSnort
 - wepcrack.sourceforge.net, aircsnort.sourceforge.net
 - Ordinateur portable sous Linux
 - Carte Ethernet sans fil équipée du chipset 'Prism II'
 - 100 Mo à 1 Go de données capturées
 - Selon la pub : quelques secondes de calcul pour déchiffrer la clef
- Le WEP première génération ne répond plus à son objectif, mais **il faut mettre en oeuvre le WEP**
 - Change complètement le niveau de sécurité du réseau
 - Permet de ralentir et complexifier les attaques
 - Impose de prendre l'habitude de la sécurité
 - Sera mieux intégré à l'avenir

Auditer et surveiller les réseaux sans fil (1/9)

Protocole 802.11b : découverte de borne



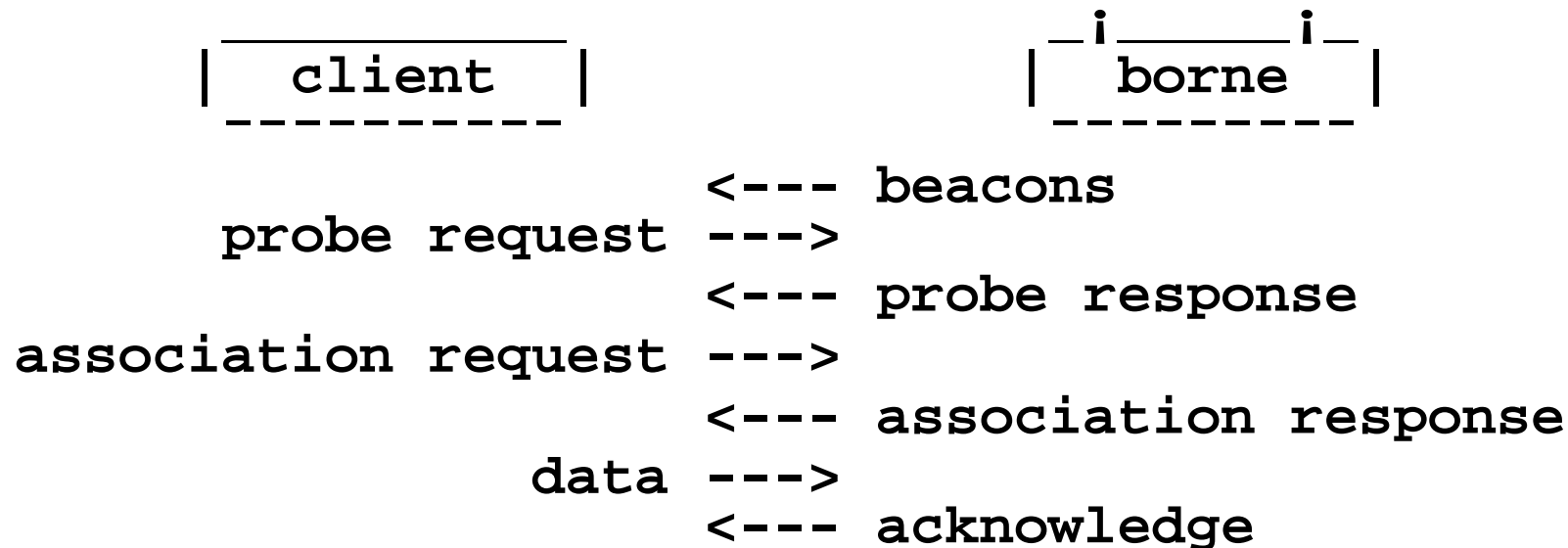
```

                                <--- beacons
probe request                   --->
                                <--- probe response
authentication request          --->
                                <--- authentication response
association request             --->
                                <--- association response
```

- Les *beacons* sont envoyés 10 fois par seconde
- La borne envoie dans sa réponse les fonctionnalités supportées
- L'authentification 802.11b est une formalité
 - Implique 4 échanges, mais toujours ouvert (*null authentication*)
- La découverte d'une borne n'utilise pas un principe passif
- Après l'association le client est connecté à la borne

Auditer et surveiller les réseaux sans fil (2/9)

La verbosité du protocole



- Les *beacons* contiennent le SSID, le nom de la borne, l'usage du WEP, des informations propriétaires
- Les trames de requêtes contiennent le SSID et les caractéristiques du réseau
 - Par défaut celles du dernier réseau rencontré
- Les trames d'association contiennent le SSID en clair
- La découverte de borne n'est pas un processus passif

Auditer et surveiller les réseaux sans fil (3/9)

La verbosité du protocole

```

      | client |
      |-----|
association request ---->
                                <---- association response
802.1X authentication ---->
                                <---- 802.1X responses
                                data ---->
                                <---- acknowledge
                                <---- data
                                acknowledge ---->
disassociation request ---->
                                <---- disassociation response
```

- Toutes les trames font l'objet d'un acquittement
- La désassociation est utilisée pour l'itinérance
 - Le client juge que le signal de la borne est devenu plus faible que le signal d'une autre borne

Auditer et surveiller les réseaux sans fil (4/9)

Surveillance

- Surveillance et détection au niveau de l'infrastructure
 - Utiliser un commutateur en apprentissage d'adresse MAC
 - Une fois les bornes branchées chaque connexion de client déclenche une alarme
 - Renvoyer les éléments émis par les bornes
 - Journalisation Syslog
 - Alarmes SNMP
 - Système de surveillance de la borne
- Surveillance du trafic au niveau sans fil (Ethernet)
 - PrismDump, AirTraf, AirIDS
 - www.guerrilla.net/gnet_linux_software.html,
sourceforge.net/projects/airtraf, www.internetcomealive.com/clients/airids
- Analyse du trafic au niveau réseau IP classique
 - Snort, Prelude
 - www.snort.org, www.prelude-ids.org

Auditer et surveiller les réseaux sans fil (5/9)

Recherche des réseaux 'sauvages'

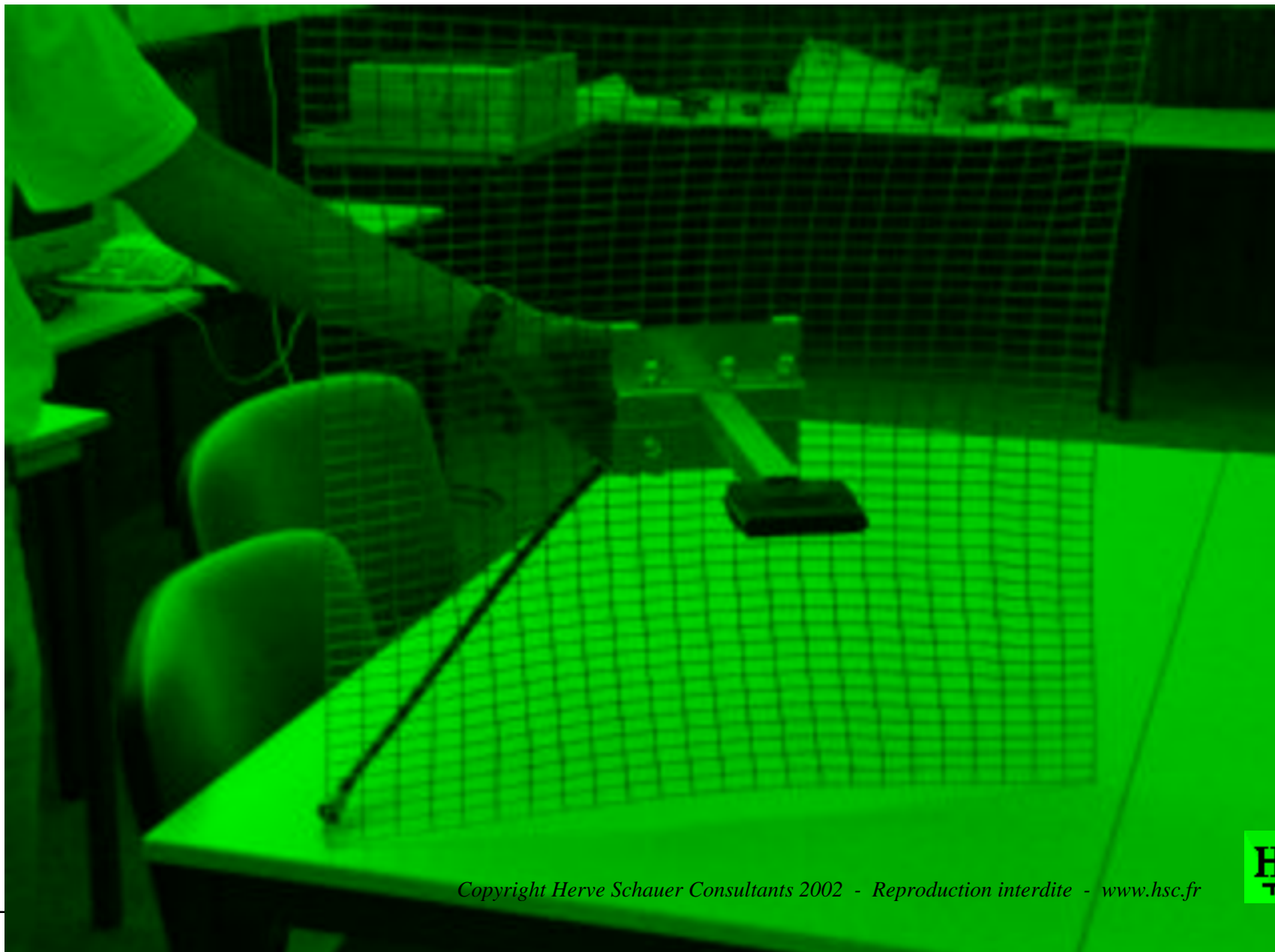
- Les réseaux sauvages peuvent être le fait :
 - D'employés inconscients pour des réseaux temporaires ou de test
 - D'employés indéclicats pour leur usage
 - D'intrus pour renvoyer le trafic du réseau privé plus loin, hors des limites physiques
- Il faut vérifier s'il n'y a pas de réseaux déployés 'sauvages'
 - Technique similaire à celle des intrus
 - Outils de gestion distribuée d'une telle recherche peu disponibles

Auditer et surveiller les réseaux sans fil (6/9)

Audit de réseaux locaux sans fil

- Objectifs
 - Détecter les réseaux sans fil IEEE 802.11b sauvages
 - Détecter les stations mal ou auto-configurées
 - Evaluer la sécurité des réseaux sans fil
- Méthodologie
 - Parcours du périmètre avec un équipement portable
 - Ordinateur ou assistant personnel
 - Utilisation d'antennes pour amplifier la réception
 - Recherche de SSID, de clef WEP, des mots de passe des bornes, ...
 - Eventuellement poursuivre avec des tests d'intrusion au travers des réseaux sans fil
 - Bien vérifier à qui les réseaux appartiennent en préalable

Auditer et surveiller les réseaux sans fil (7/9)



Auditer et surveiller les réseaux sans fil (8/9)

- Cartes avec connexion d'antenne externe



Auditer et surveiller les réseaux sans fil (9/9)

Outils d'audit

- Nombreux outils disponibles
 - NetStumbler Windows www.netstumbler.org
 - AirTraf Linux sourceforge.net/projects/airtraf
 - GtkScan/PerlSkan Linux sourceforge.net/projects/wavelan-tools/
 - Kismet Linux www.kismetwireless.net
 - PrismStumbler Linux prismstumbler.sourceforge.net
 - Wardrive Linux www.thehackerschoice.com
- **WifiScanner** Linux www.hsc.fr/ressources/outils/wifiscanner/
 - Détecte les clients et les bornes 802.11b
 - Ecoute alternativement sur les 14 canaux en temps réel
 - Peut rechercher les bornes et leurs clients pour en générer la visualisation de l'architecture réseau avec GraphViz www.graphviz.org
 - Utilise le format standard *libpcap* pour enregistrer le trafic réseau
 - Fonctionne avec les cartes basées sur le composant PrismII

Authentifier les utilisateurs de WLAN

- L'élément le plus important dans un réseau sans fil

- Nombreuses possibilités
 - Portail HTTP
 - IEEE 802.1X : *Port Based Network Access Control*
 - Introduction
 - Principes
 - Protocole
 - Cadre
 - Méthodes d'authentification
 - LEAP
 - EAP-TLS
 - PEAP
 - IEEE 802.11i
 - TKIP
 - Autres possibilités

Portail HTTP

- Méthode la plus simple
- Usurpation de la première connexion en HTTP
- L'authentification peut
 - Etre propre au portail HTTP
 - Utiliser un serveur d'authentification Radius
 - Technique utilisée par les fournisseurs de service d'accès à l'Internet pas ré seau sans fil
- Pas de logiciel spécifique à déployer sur le poste client
- Pas de gestion des clés WEP
- NoCatAuth
 - www.nocat.net

IEEE 802.1X (1/10) : Introduction

- IEEE 802.1X : *Port Based Network Access Control*
 - standards.ieee.org/getieee802/802.1.html
 - Norme développée à l'origine pour les VLAN
 - Commune à toutes les normes 802.3 (Ethernet), 802.5 (Token Ring), etc
- Cadre permettant l'élaboration de mécanismes
 - D'authentification et d'autorisation pour l'accès au réseau
 - De distribution des clés de session
- Utilise le protocole d'authentification EAP (*Extensible Authentication Protocol*) pour authentifier le client
 - Directement au-dessus du réseau local : EAPOL (*EAP over LANs*)
 - EAP peut encapsuler toute forme de méthode d'authentification
 - Mot de passe, biométrie, cartes à puce, calculatrice, clé publique, etc

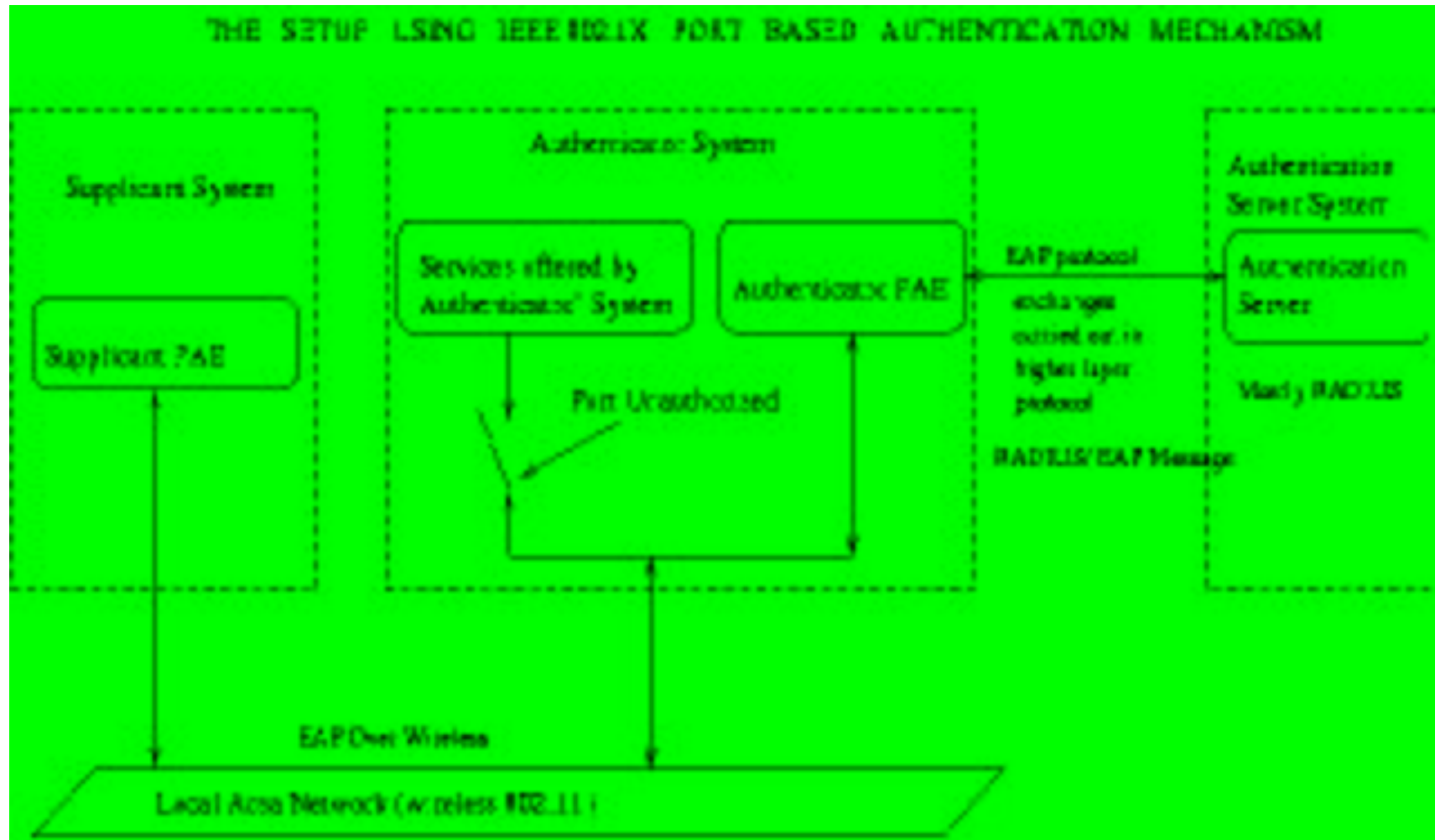
IEEE 802.1X (2/10) et 802.11

- IEEE 802.1X permet d'obtenir dans le cadre du 802.11 :
 - L'authentification de l'utilisateur depuis le poste client
 - Le contrôle d'accès à la borne
 - La distribution des clés WEP
- 802.1X avec 802.11 permet beaucoup de possibilités, peu d'interopérabilité
 - Toujours bien regarder ce qui est implémenté dans le matériel proposé
- Disponibilité sur les clients :
 - Standard dans Windows XP
 - Auprès des fournisseurs de bornes pour Windows, Mac, Unix
 - Logiciel libre disponible pour Linux : Xsupplicant
 - www.missl.cs.umd.edu/1x

IEEE 802.1X (3/10) : Principe

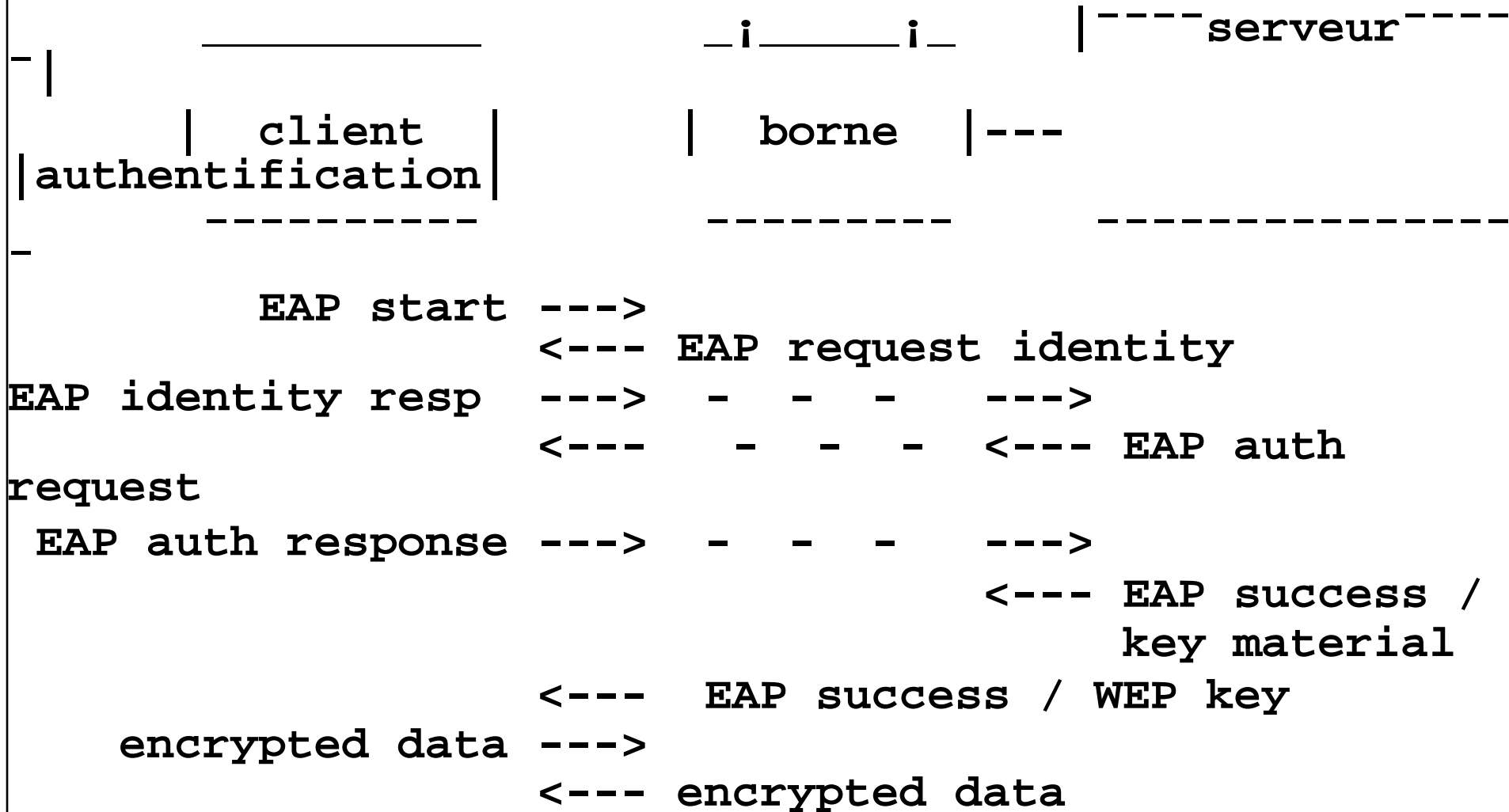
- 802.1X découpe les ports physiques d'un commutateur ou les ports virtuels d'une borne sans fil en deux ports logiques appelés PAE (*Port Access Entity*)
 - PAE d'authentification (*Authenticator PAE*) : toujours ouvert
 - PAE de service ou port contrôlé : ouvert après authentification
- Le PAE du client (*Supplicant PAE*) demande l'accès au PAE de service et il est bloqué par la borne
- Le PAE d'authentification de la borne renvoie ses trames vers un serveur d'authentification
 - La borne encapsule EAP dans RADIUS
- Après l'authentification la borne déploie le PAE du client sur le PAE de service

IEEE 802.1X (4/10) : Principe



IEEE 802.1X (5/10) : Protocole

Protocole 802.11b : authentication 802.1X



○ Suivant les méthodes d'authentification utilisées dans EAP, les trames 802.1X contiennent

Copyright Herve Schauer Consultants 2002 - Reproduction interdite - www.hsc.fr

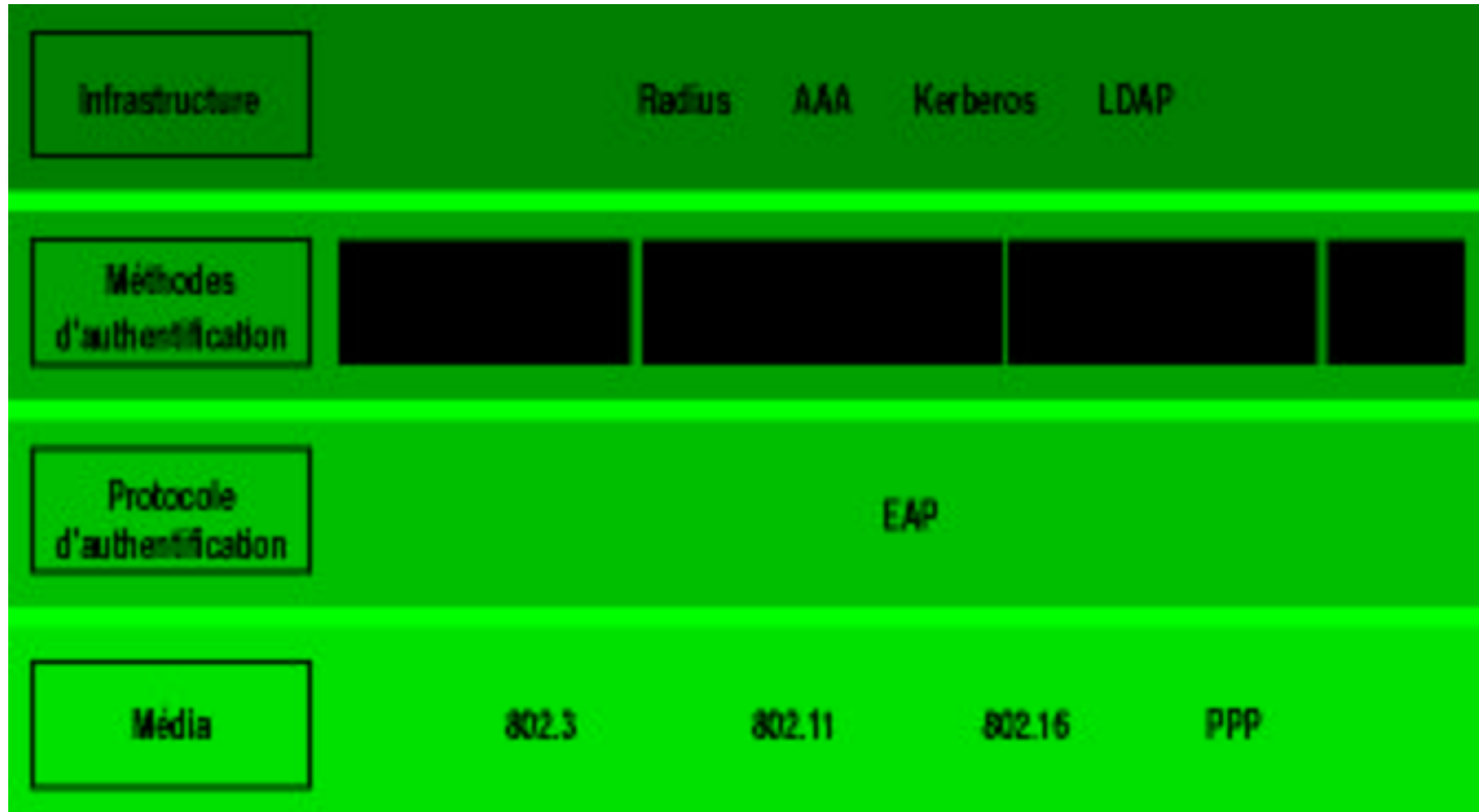


○ Le nom et mot de passe de l'utilisateur en clair ou chiffré

IEEE 802.1X (6/10) : Cadre

- IEEE 802.1X est un cadre qui intègre :
 - Une couche infrastructure
 - Serveurs d'authentification (Radius, AAA, Kerberos)
 - Annuaire
 - Une couche méthodes d'authentification
 - Basées sur des mots de passes
 - Basées sur des certificats
 - Utilisant des cartes ou caleuses
 - Génériques
 - Une couche protocole d'authentification
 - Toujours EAP
 - Une couche média
 - Ethernet 802.3, 802.11, 802.16, PPP, etc

IEEE 802.1X (7/10) : Cadre



802.1X (8/10) : Méthodes d'authentification

- Méthodes basées sur des mots de passes
 - EAP-MD5
 - Condensat du nom et mot de passe
 - Pas d'authentification mutuelle
 - LEAP (*Lightweight Extensible Authentication Protocol*)
 - Également renommé récemment Cisco-EAP par Cisco
 - EAP-SKE (*Shared Key Exchange*)
 - Authentification mutuelle
 - Itinérance entre des réseaux de différents fournisseurs
 - EAP-SRP (*Secure Remote Password*)
 - Implémentation pour EAP du protocole SRP [RFC2945]
www.ietf.org/internet-drafts/draft-ietf-pppext-eap-srp-03.txt

802.1X (9/10) : Méthodes d'authentification

- Méthodes basées sur des certificats
 - EAP-TLS (*Transport Layer Security*)
 - EAP-TTLS (*Tunneled-TLS*)
 - Extention d'EAP-TLS utilisant la connexion TLS pour échanger des informations complémentaires
www.ietf.org/internet-drafts/draft-ietf-pppext-eap-ttls-00.txt
 - Protège l'identité de l'utilisateur
 - Disponible chez Funk Software, LeapPoint Technologies et Meetinghouse Data Communications pour tous les systèmes clients et les bornes Agere (ex-Lucent)
- PEAP (*Protected Extensible Authentication Protocol*)
- EAP-MAKE (*Mutual Authentication Protocol*)
 - authentification par un mécanisme basé sur Diffie-Hellman
 - clé symétrique commune dérivée
 - impose une PKI

802.1X (10/10) : Méthodes d'authentification

- Méthodes utilisant des cartes ou calculettes
 - EAP-SIM (*Subscriber Identity Module*)
 - Utilise la carte à puce SIM du GSM
 - Authentification de l'utilisateur
 - Distribution d'une clé de session
 - Implémenté par Nokia

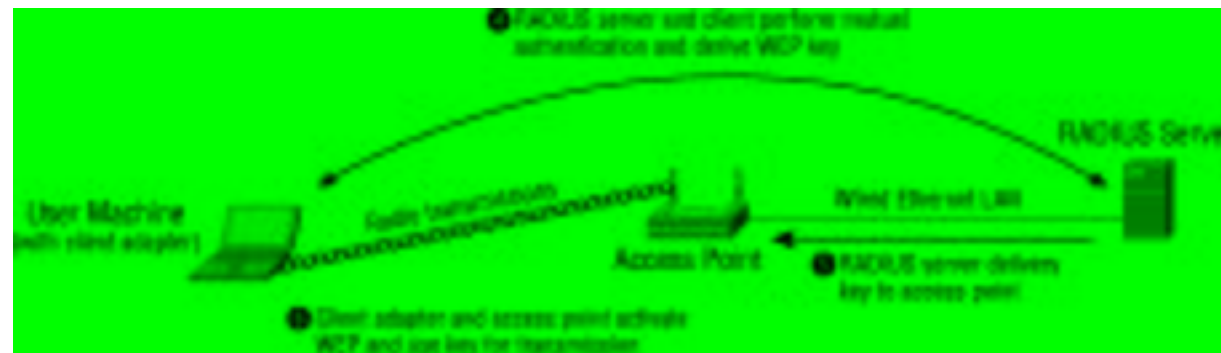
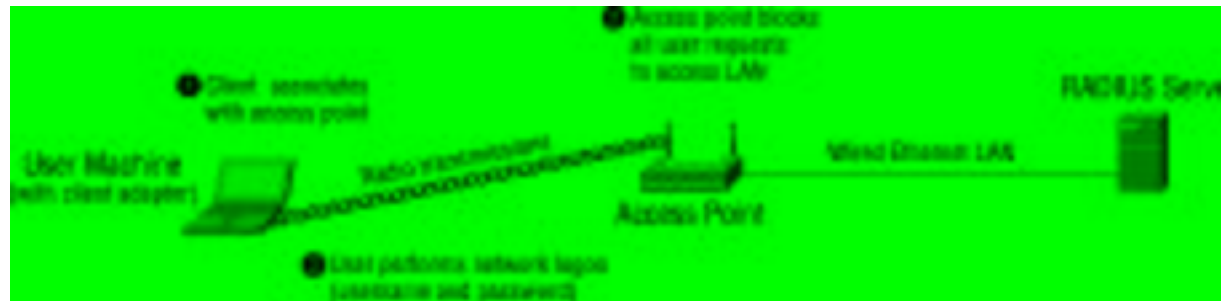
www.ietf.org/internet-drafts/draft-haverinen-mobileip-gsmsim-02.txt
 - EAP-AKA
 - utilise le système d'authentification AKA de l'UMTS
 - AKA utilise la carte à puce SIM de l'UMTS et est compatible avec la SIM du GSM
- Méthode générique
 - GSS-API
 - support de multiples méthodes d'authentification
 - clef publique, carte à puce, Kerberos, Mot de passe à usage unique, etc

LEAP (1/2)

- LEAP : *Lightweight Extensible Authentication Protocol*
- Système implémenté dans les bornes Cisco uniquement
- Basé sur le cadre 802.1X
- Première implémentation viable de 802.1X dans le cadre des réseaux sans fil 802.11b
- Protocole d'authentification entre le client et la borne
- Utilise un serveur Radius
- Basé sur le protocole d'authentification EAP
- Supporte de multiples mécanismes d'authentification
- Génère et distribue des clés WEP dynamiques
- Disponible pour les clients Windows, MacOS 9 et Linux

LEAP (2/2)

○ Principe de LEAP



EAP-TLS

- Basé sur le cadre 802.1X
- RFC2716 expérimental pour EAP-TLS pour PPP
- Système implémenté dans les bornes 3Com, Agere, Proxim
- Disponible dans de nombreux serveurs d'authentification Radius dont FreeRadius
 - www.freeradius.org
- Authentification mutuelle entre le client et le serveur d'authentification par le *handshake* TLS
- Utilisation possible d'un certificat client si une PKI existe
- Génère et distribue des clés WEP dynamiques
 - Par utilisateur
 - Par session
 - Par nombre de paquets transmis
- Disponible en standard dans Windows XP, avec Xsupplicant sur Linux, et dans de nombreux logiciels clients commerciaux

PEAP

- Implémentation annoncée dans les bornes Agere, Cisco et Enterasys
- Basé sur le cadre 802.1X
- Défini dans :
 - www.ietf.org/internet-drafts/draft-josefsson-pppext-eap-tls-eap-02.txt
- Application d'EAP dans TLS dans EAP
- Authentification mutuelle
 - Coté serveur par TLS
 - Coté client par EAP (au minimum)
- Génération des clés de session en itinérance
- Impose un serveur Radius supportant TLS
- Support dans Windows XP et Windows .net annoncé fin 2001 pour le 2ième trimestre 2002
- Disponibilité réelle sans doute fin 2002

IEEE 802.11i (1/3)

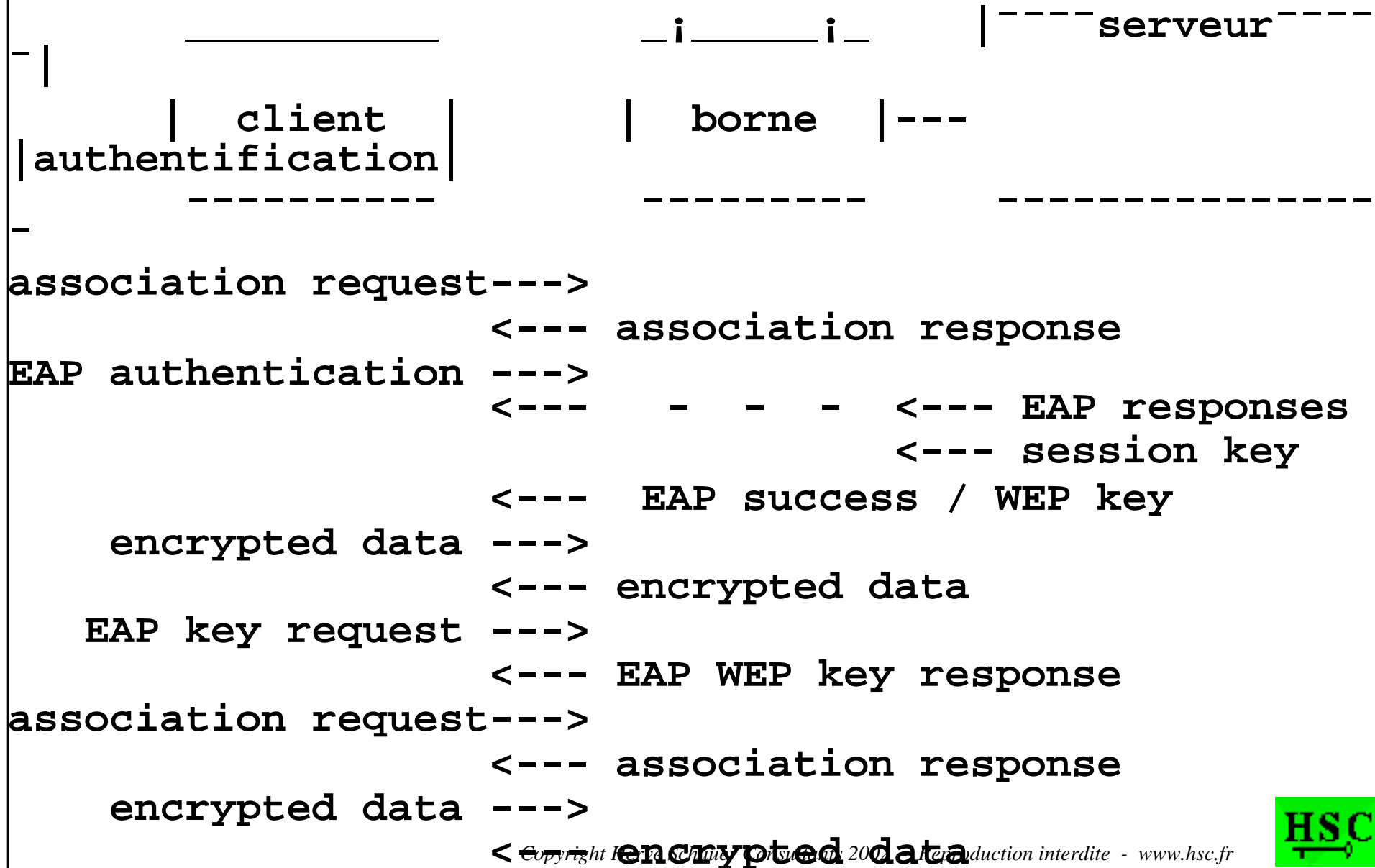
- Groupe de travail IEEE dédié pour adresser la sécurité
- IEEE 802.11i est obligatoire dans IEEE 802.11g et IEEE 802.11e
 - Sera inclu dans la certification WiFi de la WECA en 2003
- Deux niveaux :
 - Solution de transition compatible avec le matériel existant
 - Nouveau protocole de gestion des clés : TKIP
 - Promu par la WECA
 - Solution définitive incompatible avec le matériel existant
 - RC4 remplacé par AES
 - Utilisation de 802.1X
- Génère et distribue des clés WEP dynamiques

IEEE 802.11i (2/3) : TKIP

- Clés WEP dynamiques par session
- Vecteur d'initialisation de 48 bits
 - Au lieu de 24 bits dans 802.11b actuel
 - Réinitialisation à l'établissement de la clé de session
 - Règle stricte de séquençage
- Dérivation d'une clé par trame
 - Avec clé de session + vecteur d'initialisation + adresse MAC
- MIC (*Message Integrity Code*) ajouté à chaque trame
 - Au lieu d'un CRC32 sur les données et rien sur les en-têtes dans 802.11b actuel
 - Sera inutile avec AES à la place de RC4
- Sur le papier, interdit 100% des attaques connues

IEEE 802.11i (3/3) : TKIP

Distribution des clés WEP de session



Autres possibilités

- Autres extensions propriétaires au niveau 2
 - Agere : WEPplus
 - Meilleurs vecteurs d'initialisation des clés
 - 3COM : DSL (*Dynamic Security Link*)
 - Gestion de clés dynamiques dans la borne

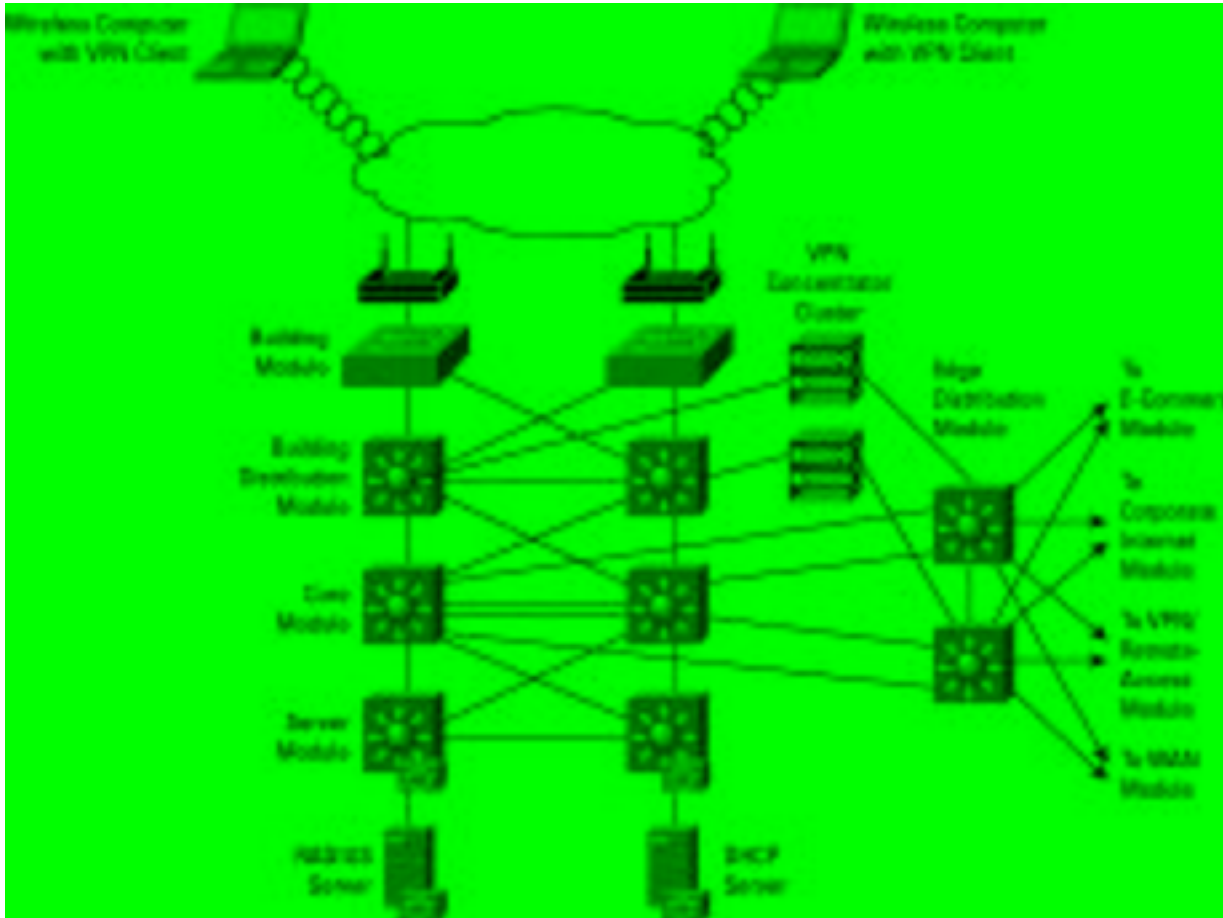
- Solutions au niveau 3 ou 4 indépendantes de la technologie du réseau sans fil
 - Authentification et chiffrement
 - SSH
 - SSL
 - Tunnels IPsec
 - Authentification "client" IPsec identique à celle d'un accès distant

Architecturer correctement ses WLAN (1/2)

- Considérer les bornes 802.11 comme des équipements sensibles
 - Choisir des bornes dont le *firmware* peut être mis à jour
 - Correctifs de sécurité
 - Nouvelles fonctionnalités
- Travailler la sécurité physique des ondes dans l'espace
 - Choisir consciencieusement l'emplacement des bornes
 - Ou des antennes, voir :
www.hsc.fr/ressources/presentations/wlan02b/mgp00028.html
 - Régler la puissance des bornes au plus juste
- Considérer les flux 802.11b comme des flux extérieurs (ie Internet)
 - Les bornes doivent être placées derrière une passerelle
 - Les flux doivent être filtrés au niveau de la passerelle
 - Les utilisateurs doivent être authentifiés

Architecturer correctement ses WLAN (2/2)

- Exemple en utilisant des tunnels



Conclusion

- Les réseaux locaux sans fil sont déjà déployés chez vous
- Les réseaux locaux sans fil sont là pour toujours
- Il faut s'organiser pour les gérer et minimiser les risques
 - Authentifier, contrôler, surveiller

Questions / Réponses

Les transparents sont disponibles sur
www.hsc.fr

Sélection de ressources (1/3)

- 802.11 (WiFi)
 - Les normes IEEE 802.11
 - standards.ieee.org/getieee802/802.11.html
 - Detecting and eavesdropping on WLANs: feasibility and countermeasures
 - www.hsc.fr/ressources/presentations/wlan02b/
 - Exemple d'utilisation en liaison point à point sur 2000 m
 - www.wifi-france.net/htm/autrans2002
 - Comparatif de la consommation des cartes Ethernet sans fil
 - www.synack.net/wireless/consumption.html
 - Camera vidéo équipée en 802.11b
 - www.dlink.com/products/DigitalHome/DigitalVideo/dcs1000w/
 - Wireless LAN Security in Depth
 - www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safwl_wp.htm
 - Securing The Maginot Line of Wireless LANs
 - www.bluesocket.com/magnotLine.html

Sélection de ressources (2/3)

- 802.11 (WiFi) (suite)
 - La réponse de Cisco aux vulnérabilités de 802.1X
 - www.cisco.com/warp/public/cc/pd/witc/ao350ap/prodlit/1680_pp.htm
- 802.15 (Bluetooth)
 - La spécification de Bluetooth 1.1 (la norme 802.15 est en draft)
 - www.bluetooth.com/dev/specifications.asp
 - Draft IETF "IP over Bluetooth"
 - www.normos.org/ietf/draft/draft-akers-atwal-btooth-01.txt
 - Le groupe de travail 802.15.3
 - www.ieee802.org/15/pub/TG3.html
 - Introduction à la sécurité de 802.15.3
 - www.securemulticast.org/GSEC/gsec3_ietf53_Singer.pdf

Sélection de ressources (3/3)

- Mixte
 - Introduction aux réseaux sans fil
 - www.guill.net/reseaux/Sansfil.html
 - Un prototype de borne mixte 802.11b et GPRS sous Linux
 - www.linuxdevices.com/articles/AT6271269832.html
 - Une borne faisant à la fois 802.11b et 802.11a : Cisco Aironet 1200
 - www.cisco.com/warp/public/cc/pd/witc/ao1200ap/prodlit/casap_ds.htm
- Administration et régulation en France
 - Synthèse de la consultation publique sur la technologie RLAN
 - www.art-telecom.fr/publications/index-rlanreponse.htm
 - Réseaux locaux sans fil
 - www.atika.pm.gouv.fr/dossiers/documents/reseaux_locaux_sans_fil.shtml

Acronymes (1/3)

AP Access Point, borne d'un réseau sans fil

BLR Boucle Locale Radio

BNEP Bluetooth Network Encapsulation Protocol

CSMA/CD Carrier Sense Multiple Access / Collision Detection

CSMA/CA Carrier Sense Multiple Access / Collision Avoidance

EAP Extensible Authentication Protocol [RFC2284]

GPRS General Packet Radio Service

GSS-API Generic Security Service API [RFC1508]

IP Internet Protocol

L2CAP Logical Link Control and Adaptation Protocol (Bluetooth)

LAN Local Area Network

LEAP Lightweight Extensible Authentication Protocol

LMDS Local Multipoint Distribution Service ou System

MAN Metropolitan Area Network

Acronymes (2/3)

MMDS Microwave Multichannel Distribution System

Multipoint Microwave Distribution System

Multichannel Multipoint Distribution Service

NAP Network Access Point

NIC Network Interface Card

NOC Network Operations Center

PAE Port Access Entity

PAN Personal Area Network

PEAP Protected Extensible Authentication Protocol

PMP Point Multi-Points

PPP Point-to-Point Protocol [RFC1548]

SB Serial Bus

SIM Subscriber Identity Module

SNMP Simple Network Management Protocol

SOC Security Operations Center

SSID Service Set Identifier, ou System Identifier, le nom du réseau

STP Spanning Tree Protocol

Acronymes (3/3)

TFTP Trivial File Transfer Protocol

TKIP Temporal Key Integrity Protocol

TLS Transport Layer Security protocol

VLAN Virtual Local Area Network

WAN Wide-Area Network

WAP Wireless Access Point

WECA Wireless Ethernet Compatibility Alliance

www.wirelessethernet.org

WEP Wired Equivalent Privacy

souvent prit pour Wireless Encryption Protocol

WHUMAN Wireless High-speed Unlicensed Metropolitan Area Network

WLAN Wireless Local Area Network

WMAN Wireless Metropolitan Area Network

WPAN Wireless Personal Area Network

WSB Wireless Serial Bus

WWAN Wireless Wide-Area Network

Remerciements

- William Arbaugh et Arunesh Mishra, Université de Maryland, et Phil Cox, System Experts, pour leur schémas
- Jérôme Poggi, Ghislaine Labouret et l'ensemble des consultants pour leur expérimentations
- Yann Berthier, Ghislaine Labouret, Denis Ducamp et Jérôme Poggi pour leur relecture
- Jérôme Poggi et Thomas Seyrat pour leurs photos