

Chapitre 2

Premier niveau de sécurisation Wi-Fi

2-1

Version – 09/2017

Objectifs du chapitre

- Les faiblesses inhérentes aux réseaux sans-fil et voir comment ils sont exploités par les pirates
- Les outils d'analyse pour détecter les vulnérabilités d'un réseau sans-fil
- Stratégies de sécurité de base et des technologies de chiffrement
- Protection de base avec WEP (Wired Equivalent Privacy)
- Découvrir les points faibles de WEP

2-2

Construire un réseau Wi-Fi sécurisé



Base des protocoles MAC 802.11

Recherche des réseaux sans-fil

Analyseurs de réseau sans-fil

Mise en œuvre d'une sécurité de base avec WEP

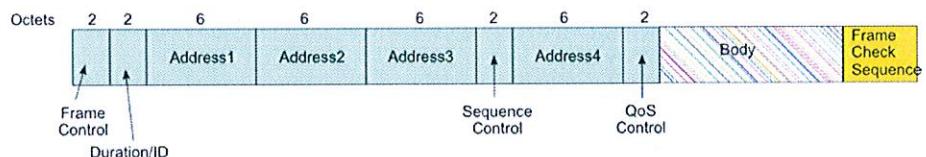
Décodage des données WEP

Résumé du chapitre

2-3

Format des trames MAC 802.11

- Adresse 1 : Destination Add (pour trame de management)
- Adresse 2 : Source Add (pour trame de management)
- Adresse 3 : BSSID (pour trame de management))
- Adresse 4 : Receiver Add seulement pour trames data (et réassociation))
- QoS control pour 802.11e



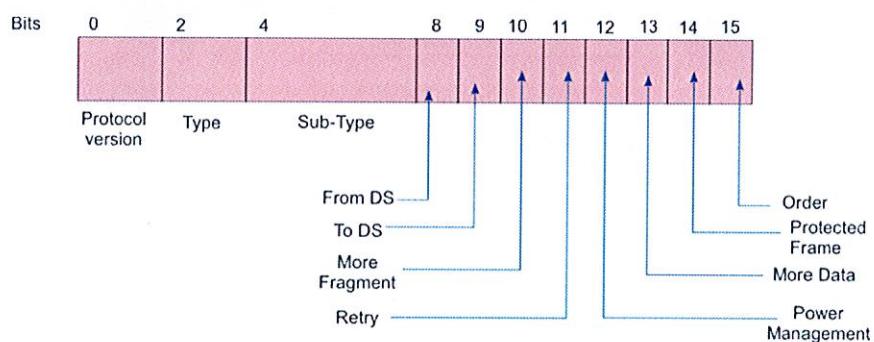
2-4

Format du champ Frame Control

- 16 Bits
- Protocol version 00
- Type : Management (00), Contrôle (01), Data (10), réservé (11)
- Sous-type 4 bits (voir exemple après)
- De Distribution System ou vers DS
- Power management (économie d'énergie 1 ou actif 0)
- Protected F (1 si WEP)
- Order (Class of Service)

Table 7-2—To/From DS combinations in data frames

To DS and From DS values	Meaning
To DS = 0 From DS = 0	A data frame direct from one STA to another STA within the same IBSS, or a data frame direct from one non-AP STA to another non-AP STA within the same BSS, as well as all management and control frames.
To DS = 1 From DS = 0	A data frame destined for the DS or being sent by a STA associated with an AP to the Port Access Entity in that AP.
To DS = 0 From DS = 1	A data frame exiting the DS or being sent by the Port Access Entity in an AP.
To DS = 1 From DS = 1	A data frame using the four-address format. This standard does not define procedures for using this combination of field values.

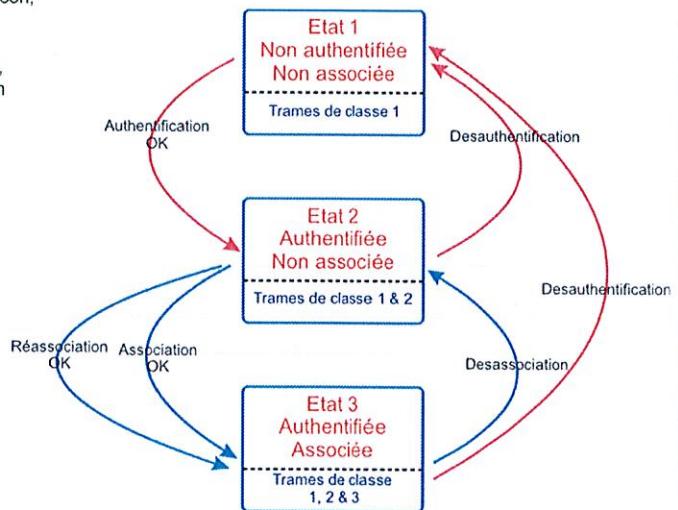


2-5

WLAN : Diagramme d'état d'une station (Automate à état)

Les états d'une station

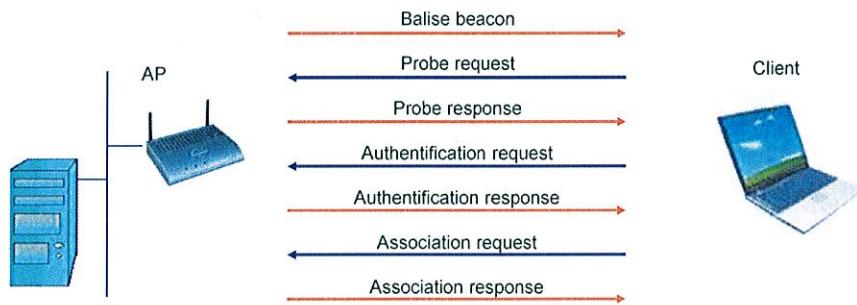
- Trames classe 1 : Probe, Beacon, Authentification et désauthentification
- Trames classe 2 : association, disassociation et réassociation
- Trames classe 3 : toutes les données



2-6

Bases du protocole MAC 802.11

Chorégraphie de base des échanges



2-7

Bases du protocole MAC 802.11

Champ type

Table 7-1—Valid type and subtype combinations

Type value b3 b2	Type description	Subtype value b7 b6 b5 b4	Subtype description
00	Management	0000	Association request
00	Management	0001	Association response
00	Management	0010	Reassociation request
00	Management	0011	Reassociation response
00	Management	0100	Probe request
00	Management	0101	Probe response
00	Management	0110-0111	Reserved
00	Management	1000	Beacon
00	Management	1001	ATIM
00	Management	1010	Disassociation
00	Management	1011	Authentication
00	Management	1100	Deauthentication
00	Management	1101	Action
00	Management	1110-1111	Reserved
01	Control	0000-0111	Reserved
01	Control	1000	Block Ack Request (BlockAckReq)
01	Control	1001	Block Ack (BlockAck)
01	Control	1010	PS-Poll
01	Control	1011	RTS
01	Control	1100	CTS
01	Control	1101	ACK
01	Control	1110	CF-End
01	Control	1111	CF-End + CF-Ack

2-8

Table 7-1—Valid type and subtype combinations (continued)

Type value b3 b2	Type descriptio	Subtype value b7 b6 b5 b4	Subty pe descripti
10	Data	0000	Data
10	Data	0001	Data + CF-Ack
10	Data	0010	Data + CF-Poll
10	Data	0011	Data + CF-Ack + CF-Poll
10	Data	0100	Null (no data)
10	Data	0101	CF-Ack (no data)
10	Data	0110	CF-Poll (no data)
10	Data	0111	CF-Ack + CF-Poll (no data)
10	Data	1000	QoS Data
10	Data	1001	QoS Data + CF-Ack
10	Data	1010	QoS Data + CF-Poll
10	Data	1011	QoS Data + CF-Ack + CF-Poll
10	Data	1100	QoS Null (no data)
10	Data	1101	Reserved
10	Data	1110	QoS CF-Ack (no data)
10	Data	1111	QoS CF-Ack + CF-Poll (no data)
11	Reserve	0000-1111	Reserve

Bases du protocole MAC 802.11

● Beacon – balise

- Trame de type management (00), sous-type (1000)
- Diffusée à intervalle régulier par l'AP.
- Permet à la station de découvrir la liste des AP dans le domaine sans fil
- Problème sérieux de sécurité, tous les SSID et les capacités des AP sont diffusés à tout arrivant – Désactiver le broadcast

● Probe request & response

- Trames de type contrôle (01), sous-type req (0100) et res(0101)
- Échange entre la station et l'AP pour approfondir leur connaissance mutuelle
- Identification
- Capacités et paramètres radio

2-9

Authentification de la station

● Ensemble d'échanges entre la STATION et l'AP

- Trame de type management (00), sous-type authentification (1011)
- STA envoie une requête d'authentification à l'AP, celui qui émet le meilleur signal si plusieurs AP ont le même SSID
- Ce processus utilise comme critère d'authentification l'adresse MAC de la STATION
- Désauthentification : notification sous-type 1100

● Type d'authentification

- *Système ouvert ou null*
 - Toutes les requêtes d'authentification des clients sont acceptées pourvu que le SSID soit correct
 - La plupart des équipements 802.11 utilisent ce mode d'authentification par défaut
- *Clé partagée*
 - Le client émet la requête d'authentification
 - Le point d'accès envoie un challenge au client : il doit prouver qu'il connaît la clé secrète

2-10

Association

- Échanges entre STATION et AP
 - STATION envoie une requête d'association
 - Trame de management (00), sous-type (0000)
 - Avec Capacité, débit, éventuellement Qos demandée
 - Le point d'accès retourne une réponse d'association
 - Trame de management (00), sous-type (0001)
 - Acceptant ou refusant l'association avec code statut et code raison
- Le driver du client affiche souvent le statut comme associé ou connecté
- Le client peut s'authentifier auprès de plusieurs points d'accès
 - Mais ne peut s'associer qu'avec un seul AP à la fois
- La mobilité consiste à changer de point d'accès
 - En passant de la zone de couverture d'un point d'accès à une autre
 - Réassociation – adresse de STATION et adresse ancien AP et nouveau AP et ESSID
 - Désassociation notification – sous-type (1010)

2-11

Construire un réseau Wi-Fi sécurisé

Base des protocoles MAC 802.11



Recherche des réseaux sans-fil

Analyseurs de réseau sans-fil

Mise en œuvre d'une sécurité de base avec WEP

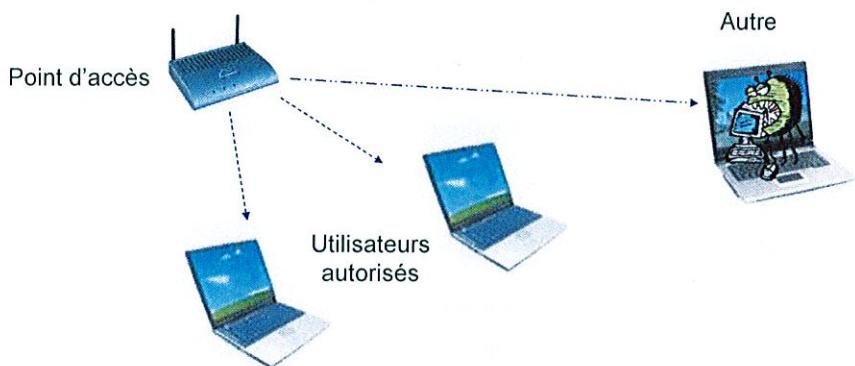
Décodage des données WEP

Résumé du chapitre

2-12

Risques de sécurité des réseaux sans-fil

- La sécurité est cruciale pour tous les réseaux et plus particulièrement les réseaux radios
 - Les signaux Wi-Fi peuvent être interceptés dans l'air
 - Les logiciels analyseurs de réseau peuvent extraire les paquets de données
 - Les réseaux Wi-Fi sont non chiffrés par défaut
 - Par défaut, le SSID du point d'accès est diffusé
 - Sans sécurité, espions et pirates peuvent se connecter à leur guise



2-13

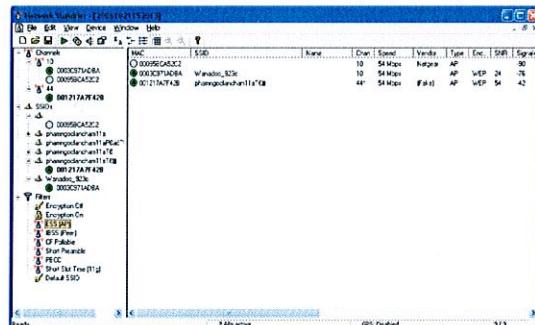
Scan

- Consiste à écouter pour savoir si un LAN est dans la portée
- Balayage passif
 - Écoute les balises (beacon) sur chaque canal pendant une courte période
- Les balises sont diffusées par le point d'accès (toutes les 100 ms)
 - Elles contiennent le SSID du réseau par défaut
- La station cherchant activement à rejoindre un réseau émet une trame « probe request »
 - La « probe request » spécifie un SSID spécifique ou un SSID diffusé
 - Seuls certains AP répondent si le SSID est spécifié
 - Tous les AP accessibles répondent à une demande de SSID diffusé

2-14

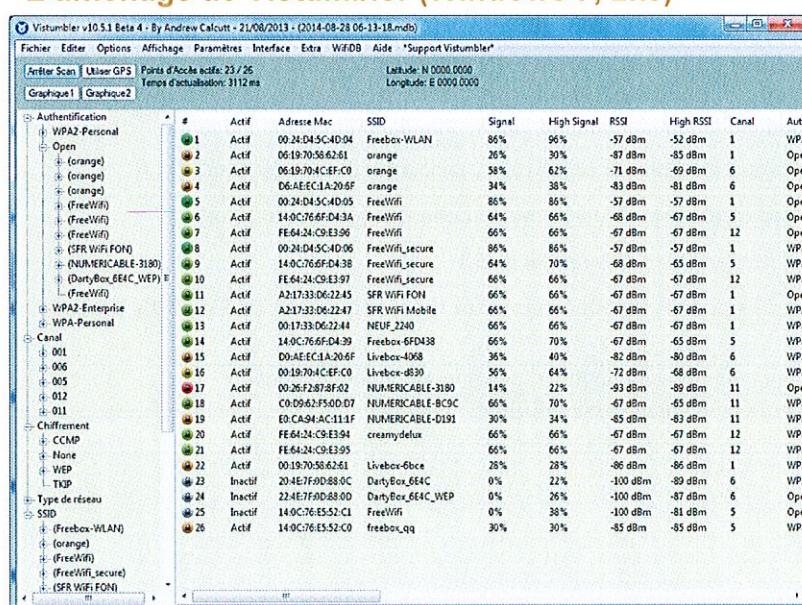
NetStumbler (Windows XP/2003) – version 0.4.0 Vistumbler (Windows 7, 2k8)

- ❖ Outil simple de balayage pour les réseaux sans-fil
 - Téléchargeable www.stumbler.com
- ❖ Balaye le spectre Wi-Fi, surveillant diffusions et balises
- ❖ Affiche SSID, canaux, puissance du signal du point d'accès
- ❖ Déetecte les points d'accès non configurés, présentant des failles de sécurité
 - Point d'accès ayant conservé le SSID par défaut
 - Réseaux non chiffrés
- ❖ Pas d'évolution depuis plusieurs années.
- ❖ Vistumbler : évolution pour systèmes 64 bits
 - Téléchargeable <http://www.vistumbler.net/>



2-15

L'affichage de Vistumbler (Windows 7, 2k8)



2-16

- ❖ Plus grand support (802.11n, détection types de WPA, ...)

- ❖ Vues construites en fonction de la recherche

- Canal : affiche et trie les AP détectés sur des canaux particuliers
- SSID affiche la liste des AP par SSID

L'affichage de Vistumbler (Windows 7, 2k8)

• Suite de la description de l'environnement sans fil

Authentification	Chiffrement	Type de réseau	Latitude	Longitude	Fabricant	Type de Lst (dd mm ss)	Lon (dd mm ss)	Taux base (Mbit/s)	Autres taux (Mbit/s)	Première activité	Dernière actualisation
WPA2-Personal	CCMP	Infrastructure	N 0.000000	E 0.000000	FREEBOX SA	802.11n N0°0'0"0.0000"	E0°0'0"0.0000"	1,2,5,5,1,22	6,9,12,18,24,36,48,54	28-08-2014 06:13:25...	28-08-2014 06:16:31...
Open	None	Infrastructure	N 0.000000	E 0.000000	Inconnu	802.11n N0°0'0"0.0000"	E0°0'0"0.0000"	1,2,5,5,11	6,9,12,18,24,36,48,54	28-08-2014 06:13:25...	28-08-2014 06:16:31...
Open	None	Infrastructure	N 0.000000	E 0.000000	Inconnu	802.11n N0°0'0"0.0000"	E0°0'0"0.0000"	1,2,5,5,11	6,9,12,18,24,36,48,54	28-08-2014 06:13:25...	28-08-2014 06:16:31...
Open	None	Infrastructure	N 0.000000	E 0.000000	Inconnu	802.11n N0°0'0"0.0000"	E0°0'0"0.0000"	1,2,5,5,11	6,9,12,18,24,36,48,54	28-08-2014 06:13:25...	28-08-2014 06:16:31...
Open	None	Infrastructure	N 0.000000	E 0.000000	FREEBOX SA	802.11n N0°0'0"0.0000"	E0°0'0"0.0000"	1,2,5,5,11,22	6,9,12,18,24,36,48,54	28-08-2014 06:13:25...	28-08-2014 06:16:31...
Open	None	Infrastructure	N 0.000000	E 0.000000	FREEBOX SAS	802.11n N0°0'0"0.0000"	E0°0'0"0.0000"	1,2,5,5,11,22	6,9,12,18,24,36,48,54	28-08-2014 06:13:25...	28-08-2014 06:16:31...
Open	None	Infrastructure	N 0.000000	E 0.000000	Inconnu	802.11g N0°0'0"0.0000"	E0°0'0"0.0000"	1,2,5,5,11	6,9,12,18,24,36,48,54	28-08-2014 06:13:25...	28-08-2014 06:16:31...
WPA2-Enterprise	CCMP	Infrastructure	N 0.000000	E 0.000000	FREEBOX SA	802.11n N0°0'0"0.0000"	E0°0'0"0.0000"	1,2,5,5,11,22	6,9,12,18,24,36,48,54	28-08-2014 06:13:25...	28-08-2014 06:16:31...
WPA2-Enterprise	CCMP	Infrastructure	N 0.000000	E 0.000000	FREEBOX SAS	802.11n N0°0'0"0.0000"	E0°0'0"0.0000"	1,2,5,5,11,22	6,9,12,18,24,36,48,54	28-08-2014 06:13:25...	28-08-2014 06:16:31...
WPA2-Enterprise	CCMP	Infrastructure	N 0.000000	E 0.000000	Inconnu	802.11g N0°0'0"0.0000"	E0°0'0"0.0000"	1,2,5,5,11	6,9,12,18,24,36,48,54	28-08-2014 06:13:25...	28-08-2014 06:16:31...
Open	None	Infrastructure	N 0.000000	E 0.000000	Inconnu	802.11g N0°0'0"0.0000"	E0°0'0"0.0000"	1,2,5,5,11,18,24,36,54	6,9,12,18,24,36,48,54	28-08-2014 06:13:25...	28-08-2014 06:16:31...
WPA2-Enterprise	CCMP	Infrastructure	N 0.000000	E 0.000000	Inconnu	802.11g N0°0'0"0.0000"	E0°0'0"0.0000"	1,2,5,5,11,18,24,36,54	6,9,12,18,24,36,48,54	28-08-2014 06:13:25...	28-08-2014 06:16:31...
WPA-Personal	CCMP	Infrastructure	N 0.000000	E 0.000000	SFR	802.11g N0°0'0"0.0000"	E0°0'0"0.0000"	1,2,5,5,11,18,24,36,54	6,9,12,18,24,36,48,54	28-08-2014 06:13:25...	28-08-2014 06:16:31...
WPA-Personal	CCMP	Infrastructure	N 0.000000	E 0.000000	FREEBOX SAS	802.11n N0°0'0"0.0000"	E0°0'0"0.0000"	1,2,5,5,11,22	6,9,12,18,24,36,48,54	28-08-2014 06:13:25...	28-08-2014 06:16:31...
WPA2-Personal	CCMP	Infrastructure	N 0.000000	E 0.000000	Alpha Networks...	802.11n N0°0'0"0.0000"	E0°0'0"0.0000"	1,2,5,5,11	6,9,12,18,24,36,48,54	28-08-2014 06:13:25...	28-08-2014 06:16:31...
WPA2-Personal	CCMP	Infrastructure	N 0.000000	E 0.000000	Z-Corn, Inc.	802.11n N0°0'0"0.0000"	E0°0'0"0.0000"	1,2,5,5,11	6,9,12,18,24,36,48,54	28-08-2014 06:13:25...	28-08-2014 06:16:31...
Open	WEP	Infrastructure	N 0.000000	E 0.000000	Netgear	802.11g N0°0'0"0.0000"	E0°0'0"0.0000"	1,2,5,5,11,18,24,36,54	6,9,12,48	28-08-2014 06:13:25...	28-08-2014 06:16:31...
WPA2-Personal	CCMP	Infrastructure	N 0.000000	E 0.000000	Akey Computer...	802.11n N0°0'0"0.0000"	E0°0'0"0.0000"	1,2,5,5,11,18,24,36,54	6,9,12,48	28-08-2014 06:13:25...	28-08-2014 06:16:31...
WPA2-Personal	CCMP	Infrastructure	N 0.000000	E 0.000000	Akey Computer...	802.11n N0°0'0"0.0000"	E0°0'0"0.0000"	1,2,5,5,11,18,24,36,54	6,9,12,48	28-08-2014 06:13:25...	28-08-2014 06:16:31...
WPA-Personal	CCMP	Infrastructure	N 0.000000	E 0.000000	Inconnu	802.11g N0°0'0"0.0000"	E0°0'0"0.0000"	1,2,5,5,11	6,9,12,18,24,36,48,54	28-08-2014 06:13:25...	28-08-2014 06:16:31...
WPA2-Personal	CCMP	Infrastructure	N 0.000000	E 0.000000	Inconnu	802.11g N0°0'0"0.0000"	E0°0'0"0.0000"	1,2,5,5,11,22	6,9,12,18,24,36,48,54	28-08-2014 06:13:25...	28-08-2014 06:16:31...
WPA2-Personal	CCMP	Infrastructure	N 0.000000	E 0.000000	Z-Corn, Inc.	802.11n N0°0'0"0.0000"	E0°0'0"0.0000"	1,2,5,5,11	6,9,12,18,24,36,48,54	28-08-2014 06:13:25...	28-08-2014 06:16:31...
WPA-Personal	Tkip	Infrastructure	N 0.000000	E 0.000000	NETGEAR	802.11g N0°0'0"0.0000"	E0°0'0"0.0000"	1,2,5,5,11,18,24,36,54	6,9,12,48	28-08-2014 06:14:04...	28-08-2014 06:16:13...
Open	WEP	Infrastructure	N 0.000000	E 0.000000	Inconnu	802.11g N0°0'0"0.0000"	E0°0'0"0.0000"	1,2,5,5,11,18,24,36,54	6,9,12,48	28-08-2014 06:14:07...	28-08-2014 06:16:13...
Open	None	Infrastructure	N 0.000000	E 0.000000	FREEBOX SAS	802.11n N0°0'0"0.0000"	E0°0'0"0.0000"	1,2,5,5,11,22	6,9,12,18,24,36,48,54	28-08-2014 06:14:20...	28-08-2014 06:16:20...
WPA-Personal	CCMP	Infrastructure	N 0.000000	E 0.000000	FREEBOX SAS	802.11n N0°0'0"0.0000"	E0°0'0"0.0000"	1,2,5,5,11,22	6,9,12,18,24,36,48,54	28-08-2014 06:16:25...	28-08-2014 06:16:25...

2-17

Guide de référence NetStumbler/Vistumbler

• Cercle indiquant le statut

- Vert, jaune et rouge pour un signal décroissant
- Gris pour les signaux interceptés mais maintenant hors de portée
- Le cercle porte un symbole de verrou pour les signaux chiffrés



• MAC Address

- Adresse sur 6 octets de l'AP transmise par la trame de la balise, peut être différente de l'adresse réelle

• SSID affiche à la fois les points d'accès et les réseaux ad hoc

• Signal, High Signal : Qualité du signal, Meilleure qualité du signal

• RSSI, High RSSI : Force du signal en dBm (-100 dBm=pas de signal)

• Canal (1-14, 802.11b,g) ou (36-161, 802.11a)

• Authentication : Open, WPA/WPA2-Personnal – Type de sécurité

• Chiffrement : Type de protocole pour la protection (None, WEP, TKIP, CCMP)

• Type de réseau : Infrastructure ou Ad-Hoc

2-18

Guide de référence NetStumbler/Vistumbler

• Latitude, Longitude

- Position quand l'AP est entré dans la portée
- Si GPS (Global Positioning System) est installé et configuré

• Fabricant

- Nom du fabricant de l'AP s'il peut être déterminé, pas celui du chipset

• Type

- 802.11a, b ou n

• Lat, Lon

- Latitude/longitude

• Taux base, Autres taux

- Taux de transmission qui peuvent être négociés en fonction de la qualité de réception du signal

• Première activité, dernière activité

- Heure locale de première et dernière détection du SSID

2-19

Wardriving

• Localisation des connexions réseau sans-fil

- En conduisant dans une ville, une zone industrielle, ou une zone à forte densité de population
- On intercepte les réseaux sans-fil qui dépassent la portée des bâtiments
- Pour détecter les points d'accès et analyser la sécurité des réseaux

• Équipement nécessaire

- Ordinateur portable ou PDA
- Antenne directionnelle à gain élevé pour détecter les réseaux à distance
- NetStumbler/Vistumbler ou autre outil d'analyse de protocole sans-fil

• Les professionnels de la sécurité pratique l'audit de sites par cette méthode

- Identification des failles de sécurité et de la vulnérabilité aux pirates
- La détection des réseaux ne viole aucune loi en elle-même
- L'audit de sites implique une cartographie et une mesure de la portée des points d'accès

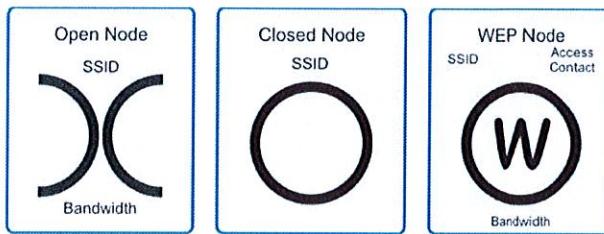
• Les pirates les imitent pour détecter et exploiter les réseaux non protégés

- Obtenir un accès gratuit à Internet
- Intercepter des mots de passe et du trafic en clair
- Accéder potentiellement aux dossiers d'une entreprise

2-20

Warchalking

- ▶ Symboles placés à l'extérieur des bâtiments pour montrer l'existence de réseaux Wi-Fi
 - Symboles dessinées à la craie sur les murs et les trottoirs par les fans de Wi-Fi et les pirates



2-21

Construire un réseau Wi-Fi sécurisé

Base des protocoles MAC 802.11

Recherche des réseaux sans-fil



Analyseurs de réseau sans-fil

Mise en œuvre d'une sécurité de base avec WEP

Décodage des données WEP

Résumé du chapitre

2-22

Outils d'analyse de réseau

Les outils d'analyse de réseau sont utilisés pour

- Audit de sites, mesure du signal et des interférences
- Dépannage et audit de sécurité
- Analyse des configurations

Problématiques renouvelées

- Du fait du BYOD (*Bring your own device*)

Fonctions disponibles

- Balayage pour afficher les canaux utilisés et la force du signal
- Détails des points d'accès et SSID dans la portée
- Détection des fonctions de sécurité mal configurées ou désactivées
- Capture de paquets, enregistrement, affichage et analyse des protocoles

Exemples d'outils existants

- AirMagnet (AirMagnet WiFi Analyzer PRO)
- CommView® for WiFi v.7.0
- Fluke WaveRunner
- AiroPeek/OmniPeek
- Wireshark ...

2-23

AirMagnet : Capture de paquets

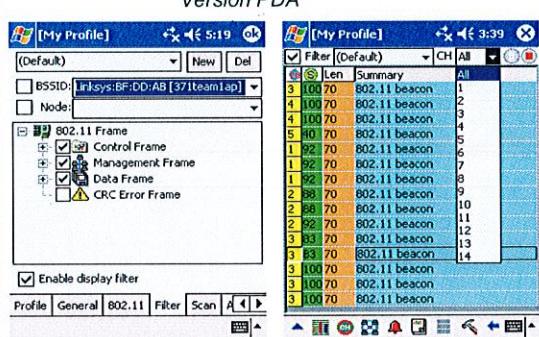
AirMagnet permet de capturer et de décoder des paquets en temps réel

- En plus des fonctionnalités d'audit

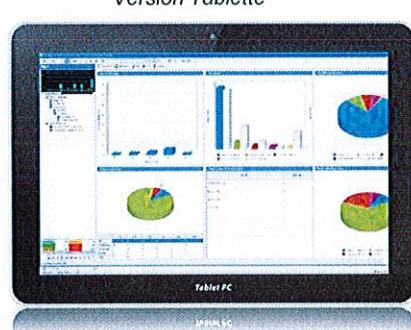
Configurer les filtres pour cibler un canal ou un point d'accès particulier

- On peut également filtrer par type de paquet

Version PDA



Version Tablette

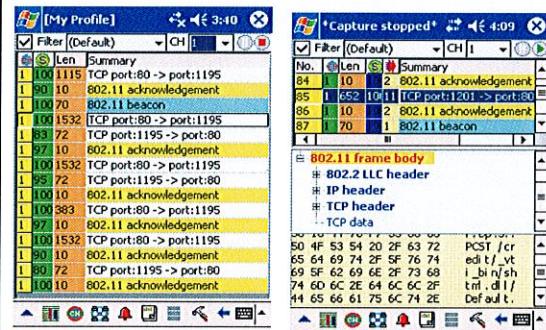


2-24

AirMagnet : Capture de paquets

- Sélectionner un paquet pour afficher les détails
- Comprend le décodage des en-têtes de protocole de niveau 2, 3 et 4
- Les données peuvent être affichées en hexadécimal
- Le texte lisible est affiché
- Preuve d'un risque significatif pour la sécurité !

Version PDA



2-25

Version Tablette



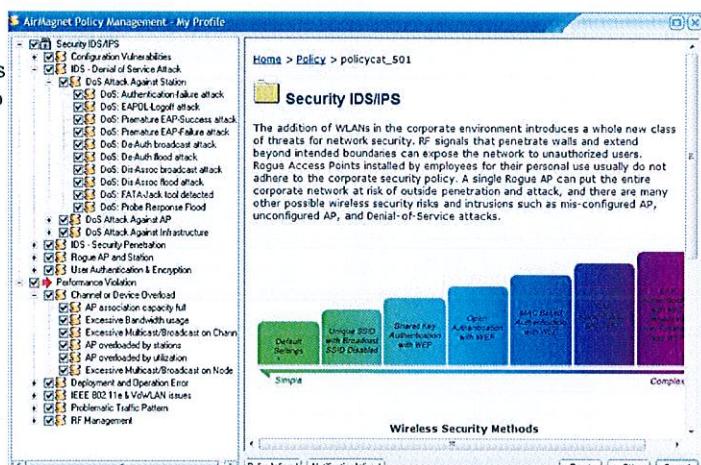
Alertes de sécurité avec AirMagnet

- Balaye les points d'accès pour détecter les failles de sécurité

- Points d'accès non configurés
- chiffrement désactivé
- Attaques DoS
- Impostures et intrusions
- Alertes de sécurité auto

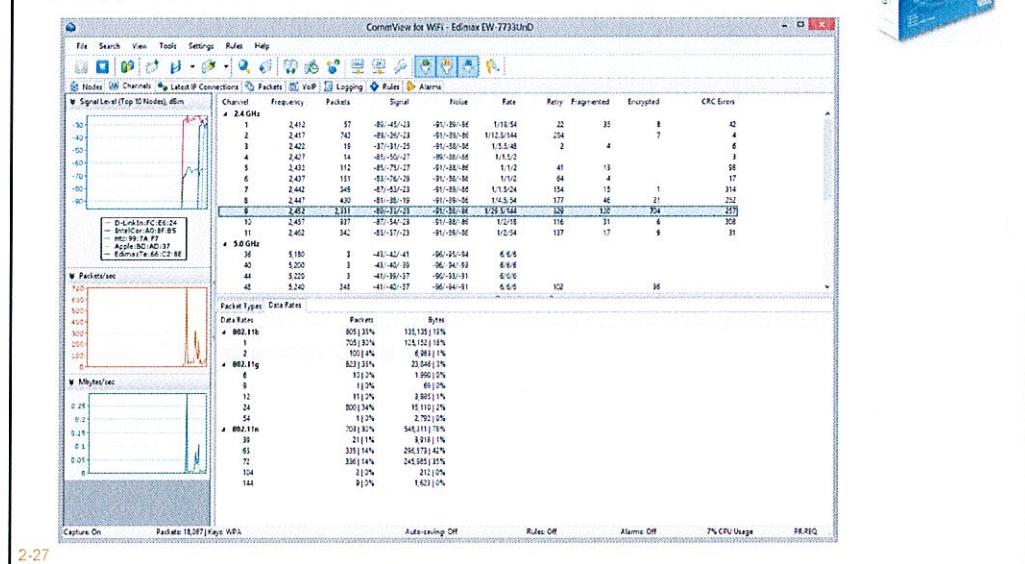


2-26



CommView® for WiFi v.7.0

• Support de canaux multiples

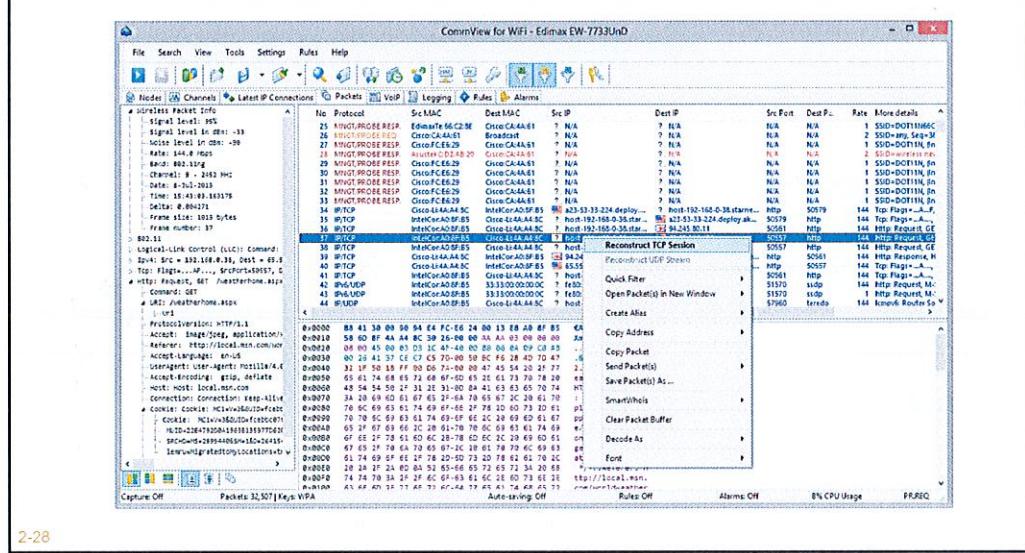


2-27

CommView® for WiFi v.7.0

Scanneur et analyseur de réseau

- Décodage automatique des paquets chiffrés WPA/WEP si la clé est connue



2-28

WaveRunner (Fluke)

Scanneur et analyseur portable, incluant un iPAQ

- Concurrent d'AirMagnet mais avec de nouvelles fonctionnalités
- Meilleur pour le balayage et les audits de sites

2-29

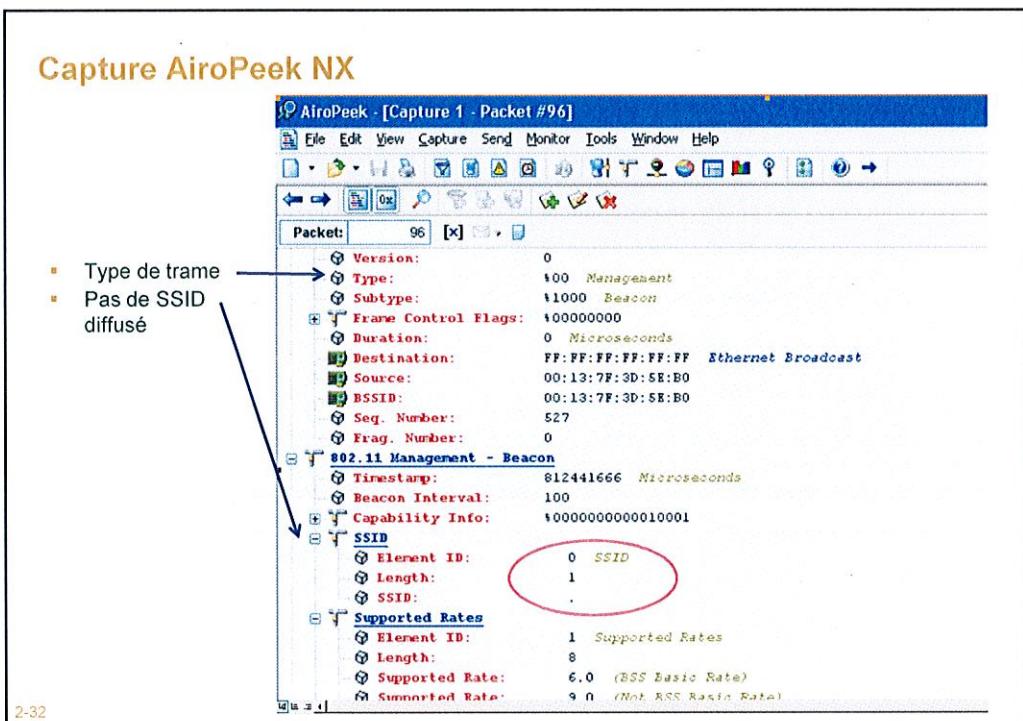
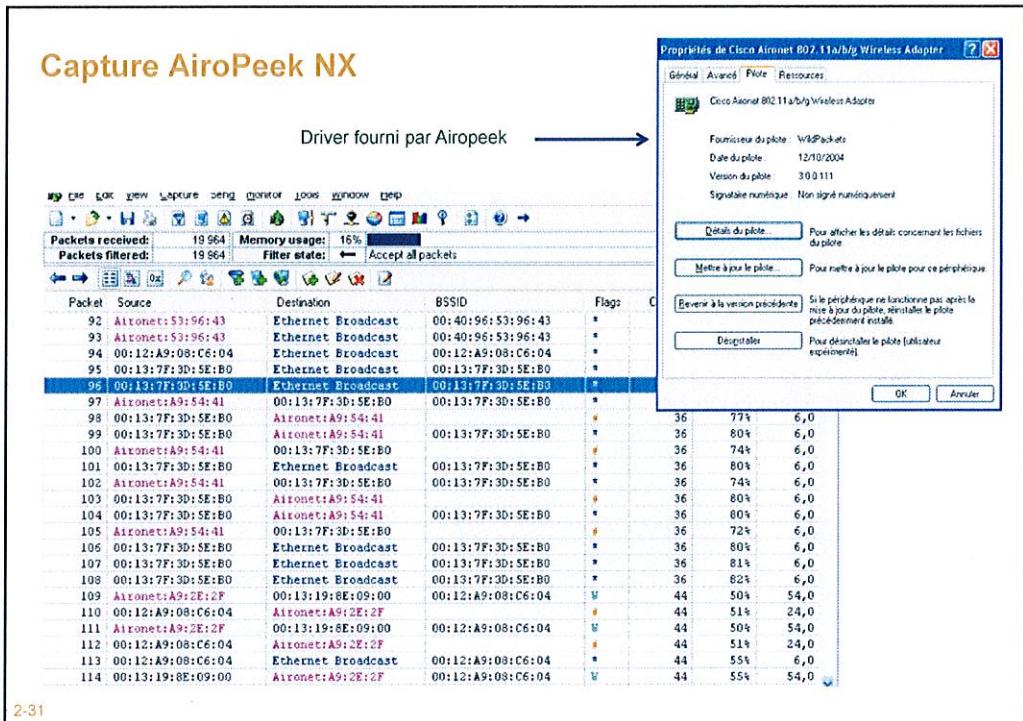
AiroPeek/OmniPeek

Analyseur de protocoles sans-fil de niveau expert

- Produit commercial de www.wildpackets.com
- Caractéristiques d'un analyseur de protocoles Ethernet, mais dédié sans-fil
- Surveillance en temps réel, analyse des captures et affichage du trafic 802.11b
- Filtrage, journalisation, détection des intrusions, analyse avancée
- La jauge est excellente pour surveiller le trafic et l'utilisation du réseau



2-30



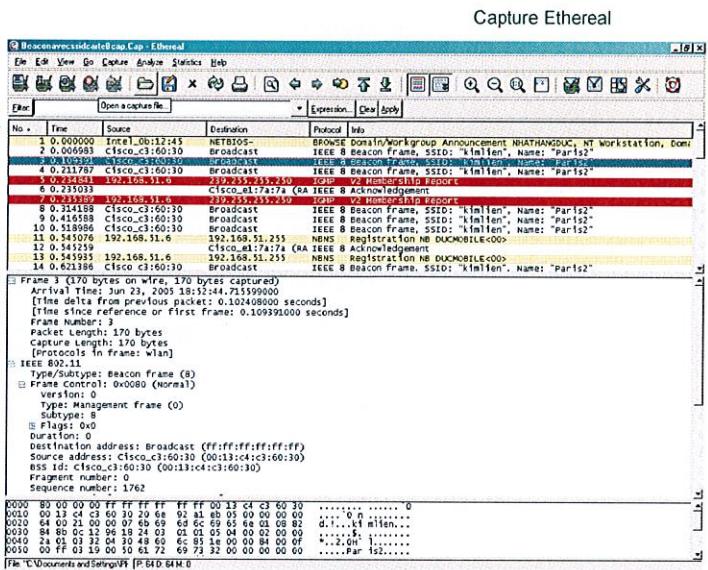
Wireshark (anciennement Ethereal)

Outil d'analyse de protocole répandu

- Logiciel *open source*
- www.wireshark.org/
- Pour Linux, Windows, Mac OS X

Ne capture pas les paquets 802.11 sous Windows

- Sous Windows, ne fonctionne que pour l'analyse des réseaux Ethernet car on ne peut pas mettre la carte en mode rfmon
- Intéresse avant tout les experts en sécurité utilisant Linux



2-33

Construire un réseau Wi-Fi sécurisé

Base des protocoles MAC 802.11

Recherche des réseaux sans-fil

Analyseurs de réseau sans-fil



Mise en œuvre d'une sécurité de base avec WEP

Décodage des données WEP

Résumé du chapitre

2-34

Politiques de sécurité de base

5 classes de service de sécurité

- Authentification
- Intégrité
- Non-répudiation
- Disponibilité
- Confidentialité

Deux parties dans la sécurité des réseaux sans-fil

- Qui est qui ? Comment s'assurer de qui est l'interlocuteur ? Par l'adresse MAC ?
=> Authentification
- Que doit on protéger ? Tout le trafic ou seulement les échanges applicatifs ?
=> Confidentialité (+ Intégrité)

Authentification, Autorisation

- Machine ou Utilisateur ? Une clef identique pour tous ou par utilisateur ?

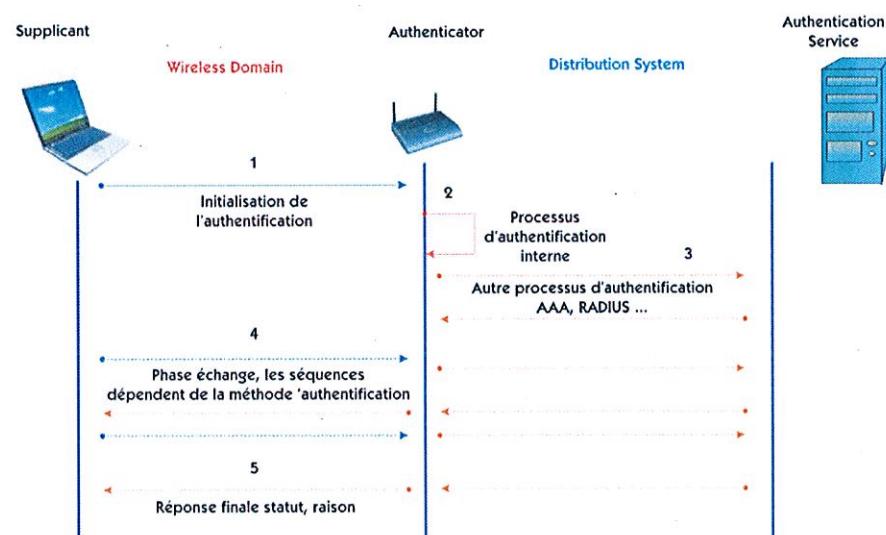
Chiffrement et Intégrité des données

- Quel type ou niveau OSI de chiffrement des données ?
- Quelle méthode de chiffrement ?

2-35

Principe de l'authentification

Les éléments d'un modèle tri-partie

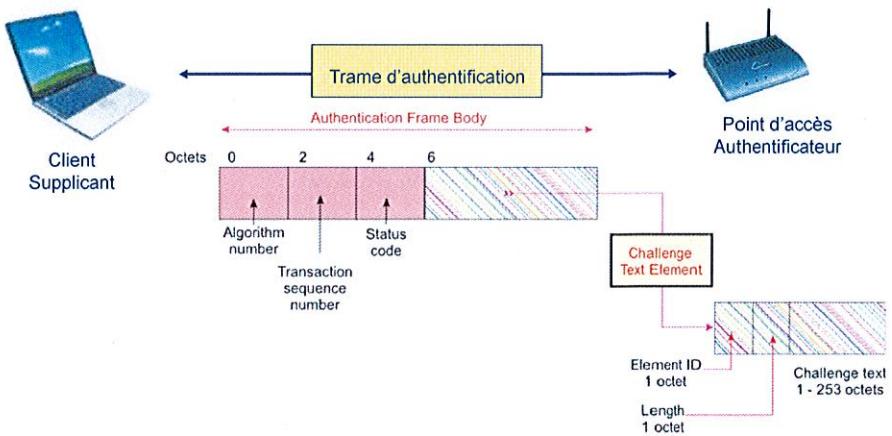


2-36

Authentification de base

Deux Algorithmes d'authentification

- Open Authentication - algorithm number = 0
- Shared-key authentication – algorithm number = 1
- Challenge text Element ID = 16

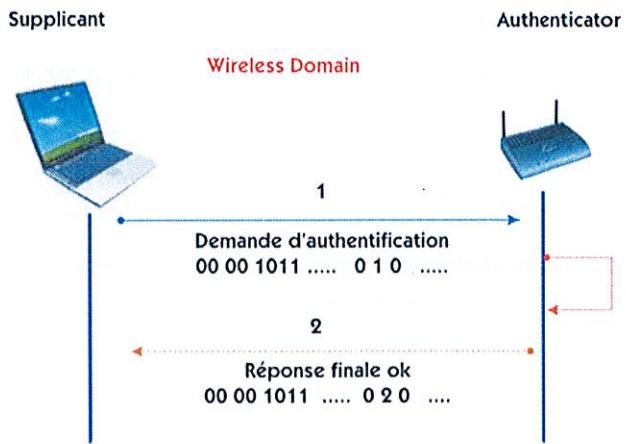


2-37

Authentification de base

Authentification open

- Simple échange de messages entre le supplicant et l'authentificateur
- Authentification nulle : on croit à priori tous ceux qui veulent s'associer, pourvu qu'ils connaissent le SSID

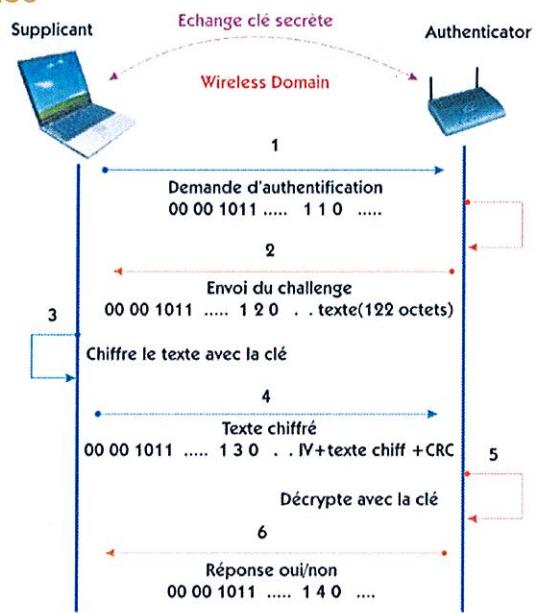


2-38

Authentification de base

Authentification à clé partagée – Shared-key

- Méthode basée sur un protocole de type challenge – réponse : 6 étapes et 4 messages
- Shared-key authentication a besoin des mécanismes WEP
- Il est donc nécessaire de mettre en place une infrastructure WEP
- Cette méthode n'établit que les deux parties connaissent (et partagent) la même clé secrète.



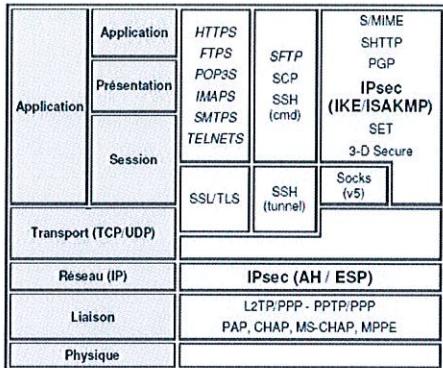
2-39

Politiques de sécurité de base

- Adopter des pratiques élémentaires pour contrecarrer les efforts des pirates occasionnels
- Changer le SSID par défaut sur tous les points d'accès
 - Ex : transformer linksys, tsumani, WLAN en quelque chose d'autre
- Changer le SSID en quelque chose de sibyllin
 - Ne pas utiliser le nom de l'entreprise ou du service
 - Ex : ap0zn30 au lieu de wifi
- Désactiver la diffusion du SSID
 - Un système fermé ne transmet pas le SSID dans les balises
 - Les clients doivent configurer le SSID explicitement
 - Un client ne découvrira donc pas automatiquement le réseau
 - N'empêche pas NetStumbler de détecter les réseaux
 - Pour ce faire, il intercepte le trafic des clients vers l'AP pour découvrir le SSID
 - Toutefois sans le SSID, il est impossible de débuter une attaque
- Activer le chiffrement WEP (Wired Equivalent Protocol) – au minimum

2-40

Chiffrement et intégrité des données



Chiffrement, mais de quel niveau ?

- Chiffrement sur couche applicative, transport, réseau ou liaison possible...

=> Niveau Applicatif

=> Niveau Liaison WEP, WPA/WPA2

Principe des réseaux ouverts (Hotspot)

- Chiffrement sur couche applicative, pas d'authentification particulière, sauf sur le hotspot au moyen d'un portail captif

Principe des réseaux domestiques/d'entreprise

- Chiffrement sur couche liaison, authentification sur un élément réseau (AP ou Serveur)

2-41

Chiffrement et intégrité des données

Le chiffrement consiste à brouiller un message *clair* pour produire un *texte chiffré*

- Lorsqu'un pirate intercepte le texte chiffré, il ne peut pas en déduire le texte original
- Seul le destinataire prévu doit pouvoir décoder le message
- NB : décrypter signifie qu'on ne connaît pas la clé, déchiffrer qu'on la connaît

DES (Data Encryption Standard)

- U.S. National Institute of Standards and Technology (NIST), 1977
- Basé sur une clé de 64 bits; dont 56 bits générés de façon aléatoire, et 8 bits de parité, (1 bit pour chaque bloc de 7 bits)

Triple DES (3DES)

- Alternative à DES : 3DES prend un bloc de 64 bits de données, crypte, décrypte et crypte de nouveau. 3DES peut utiliser pour ces opérations une deux ou trois clés différentes. L'avantage d'utiliser une clé unique est la compatibilité avec DES.

2-42

Standards de chiffrement

• AES (Advanced Encryption Standard)

- Publié par le NIST en 1998
- Clés de 128, 192, et 256 bits pour chiffrer des blocs de 128, 192 ou 256 bits (toutes les 9 combinaisons de longueur de clés et de longueur de blocs sont possibles)
- Mieux adapté pour du chiffrement hardware (plus rapide)

• RC4

- Rivest Cipher 4 : Inventé par Ron Rivest et promu par RSA Data Security
- RC4 est souvent utilisé avec une clé de 128 bits
- Chiffrement par flux : la clé est un flux opérant sur le texte qui devient un texte chiffré
- RC4 est utilisé par WEP
- La même clé pour chiffrer et déchiffrer

2-43

WEP

• Wired Equivalent Privacy

- Conçu pour fournir un niveau de sécurité à peu près équivalent à celui d'un réseau câblé (!)
- L'authentification préliminaire est l'équivalent de la trace laissée au moment de la connexion à la prise réseau filaire.

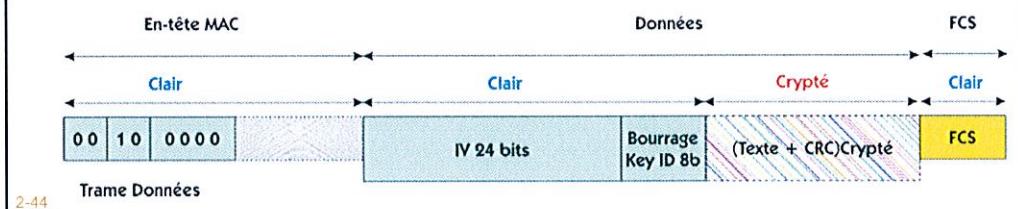
• Outil substantiel de dissuasion contre les attaques les plus courantes

- Le chiffrement empêche les espions d'intercepter des données en clair
- L'authentification associée empêche les utilisateurs non autorisés d'accéder au réseau

• WEP est un compromis entre la performance et la sécurité de base

- Mais la méthode de chiffrement présente des faiblesses

• Format d'une trame de données chiffrée avec WEP



2-44

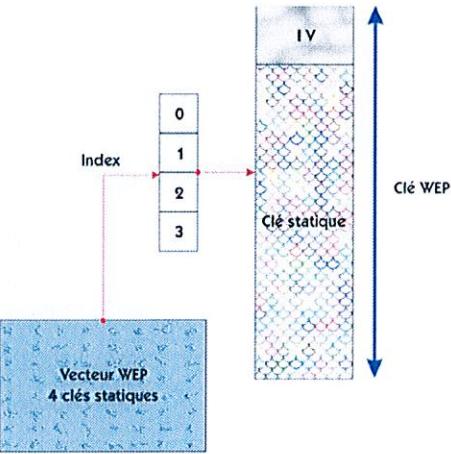
Le modèle WEP

WEP utilise l'algorithme RC4

- En Deux phases :
 - Génération de la clé
 - chiffrement

Émetteur et récepteur partagent une clé secrète

- La clé WEP de 64 ou 128 bits est composé de:
 - Clé statique – preshared key : WEP définit un vecteur qui contient 4 clés numérotées de 0 à 3 – Key ID. Clés de 40 ou 104 bits configurées par l'utilisateur (en général en hexadécimal ou avec une passphrase).
 - Un vecteur d'initialisation (IV), appelé germe (Seed). Ce IV est en principe généré de façon aléatoire, et incrémenté pour chaque paquet successif. Certains constructeurs démarrent l'IV à 0 et incrémenté de 1 à chaque passe. IV est en clair dans la trame.

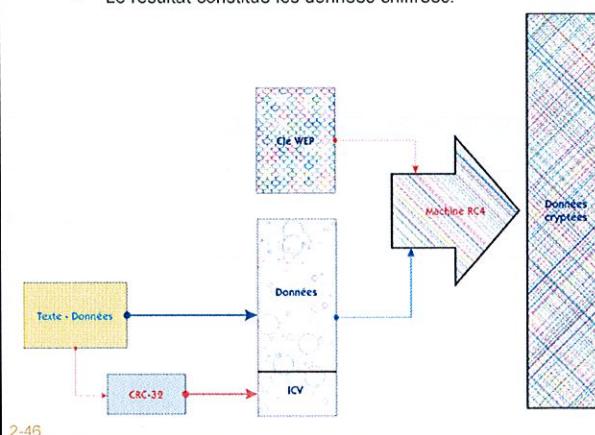


2-45

Le modèle WEP

chiffrement des données

- En fonction des données, l'algorithme CRC-32 génère un ICV (Integrity Check Value) de 4 octets. Cet ICV est rajouté aux données.
- Cet ensemble est confié à la machine RC4 en même temps que la clé WEP.
- Le résultat constitue les données chiffrées.

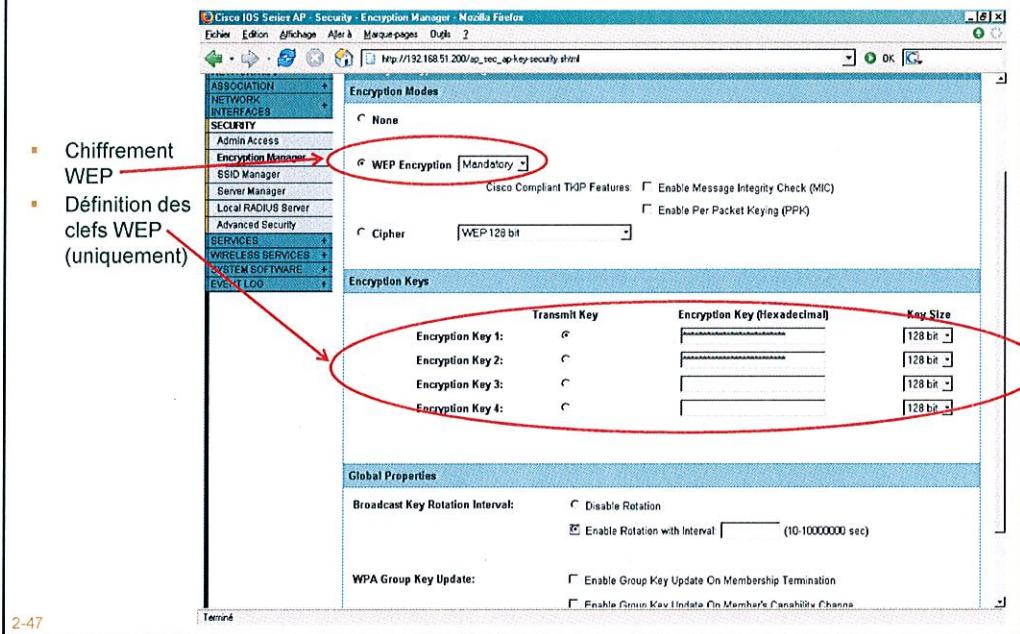


2-46

- Trame WEP -

Flags:	0x00
Status:	0x01
Packet Length:	104
Timestamp:	18:00:47.562683 04/04/2001
Data Rate:	22 11.0 Mbps
Channel:	6 2437 MHz
Signal Level:	74
802.11 MAC Header	
Version:	0
Type:	0x10 Data
Subtype:	0x0000 Data Only
To DS:	0
From DS:	1
More Frag.:	0
Retry:	0
Power Mgmt:	0
More Data:	0
WEP:	1
Order:	0
Duration:	218 Microseconds
Destination:	00:40:96:40:53:5B
BSSID:	00:A0:F8:8B:20:1F
Source:	00:A0:C5:E2:6D:A8
Seq. Number:	2952
Frag. Number:	0
802.11 WEP Data	
WEP IV:	0xF10000
WEP Key Index:	1 Key ID=2
WEP Data:	
Data: (68 bytes)	0x2FF0665F
WEP ICV:	0x2FF0665F
FCS - Frame Check Sequence	
FCS (Calculated):	0x16A5D2BA

Configurer des clés WEP sur l'AP Cisco



2-47

Configurer des clés WEP sur les postes clients

Activez WEP sur chaque client

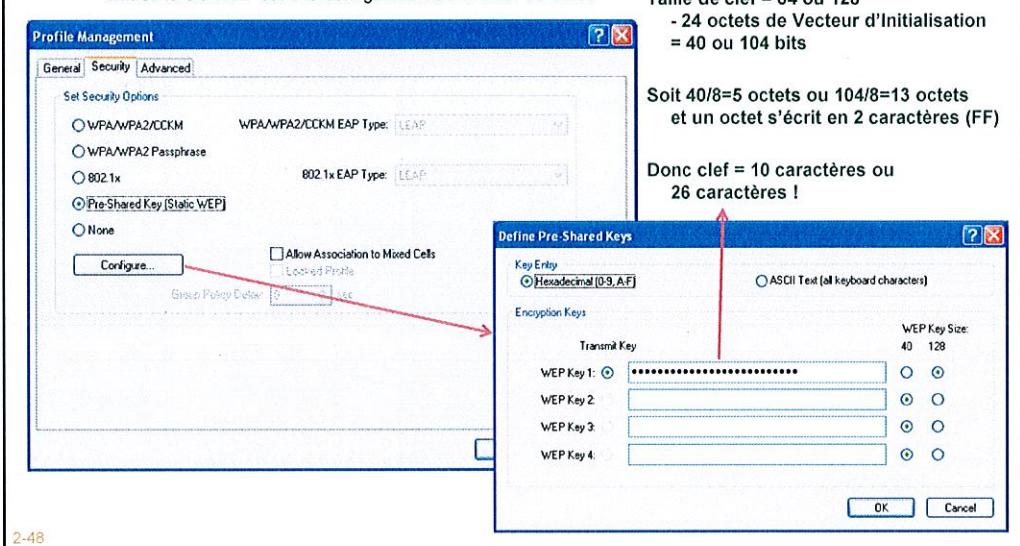
- Entrez la clé WEP dans la configuration de la carte du client

Clef WEP

Taille de clef = 64 ou 128
- 24 octets de Vecteur d'Initialisation
= 40 ou 104 bits

Soit $40/8=5$ octets ou $104/8=13$ octets
et un octet s'écrit en 2 caractères (FF)

Donc clef = 10 caractères ou
26 caractères !



2-48

Points faibles de WEP

- De multiples facteurs rendent WEP facile à craquer
 - Sur un réseau très actif, un pirate peut craquer une clé WEP en quelques heures / minutes
- 1. La clé WEP est statique
- 2. LE VI est visible et transmis dans chaque trame *en clair*
- 3. Le VI est un nombre supposé aléatoire mais sous-dimensionné, autorisant les *répétitions*
- 4. Presque tous les paquets chiffrés contiennent des informations d'en-tête similaires
 - Le craquage exploite la répétition des données et des VI
- 5. Certains constructeurs donnent des valeurs de VI faciles au craquage et non aléatoires

2-49

Exploiter WEP

- WEP était raisonnablement satisfaisant pour les faibles trafics, les réseaux domestiques
 - Mais ne prends que quelques minutes à casser !
- En dépit de ses faiblesses, utiliser WEP quand même ?
 - Un peu de chiffrement vaut mieux que pas de chiffrement du tout !
 - Choisir des clés de 128 bits
 - Mais ne pas compter sur WEP pour résister à une personne disposant des outils nécessaires
- Mais surtout : Utiliser d'autres technologies de chiffrement sur des couches supérieures (VPN, SSL, etc ...)

2-50

Construire un réseau Wi-Fi sécurisé

Base des protocoles MAC 802.11

Recherche des réseaux sans-fil

Analyseurs de réseau sans-fil

Mise en œuvre d'une sécurité de base avec WEP



Décodage des données WEP

Résumé du chapitre

2-51

Vue d'ensemble des outils des pirates

• Outils qui s'avèrent plus centrés sur l'extraction de données et l'exploitation des failles que sur la protection et la performance

- Les responsables de la sécurité doivent savoir qu'ils existent

• Kismet

- Analyseur de paquets sous Linux
- Similaire à NetStumbler avec des fonctions supplémentaires
 - Journalisation des paquets faibles sur le plan cryptographique
 - Démasquage des SSID cachés
 - Identification du fabricant
 - Décodage des paquets WEP à l'exécution

• WEPCrack, AirSnort

- Décodage des paquets au chiffrement faible

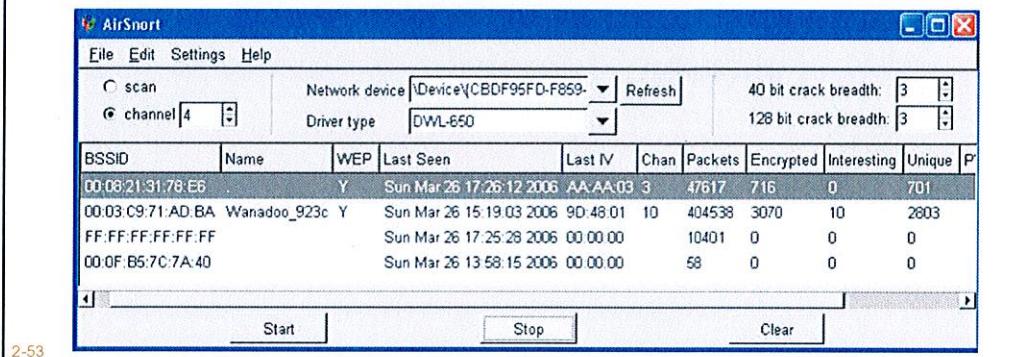
• Suite Aircrack-ng

- Solution logicielle la plus performante

2-52

Craquer WEP avec AirSnort

- AirSnort scanne les fréquences et capture les paquets comme un sniffer. Néanmoins, AirSnort a pour but de repérer les paquets WEP qui utilisent un Initialization Vector (IV) "faible". Si le paquet utilise un IV faible, alors il est conservé et noté comme paquet intéressant "Interesting Packet".
 - Ainsi, une personne peut cracker une clef WEP de 40 bit avec AirSnort 02.1.b en collectant 3693 "interesting packets" sur 10,000,000 de paquets envoyés. Il faudrait 6 heures pour générer les paquets en lançant environ 250 ping simultanément.
 - Il s'agit d'un scan, et donc cette méthode ne peut pas faire "planter" l'AP

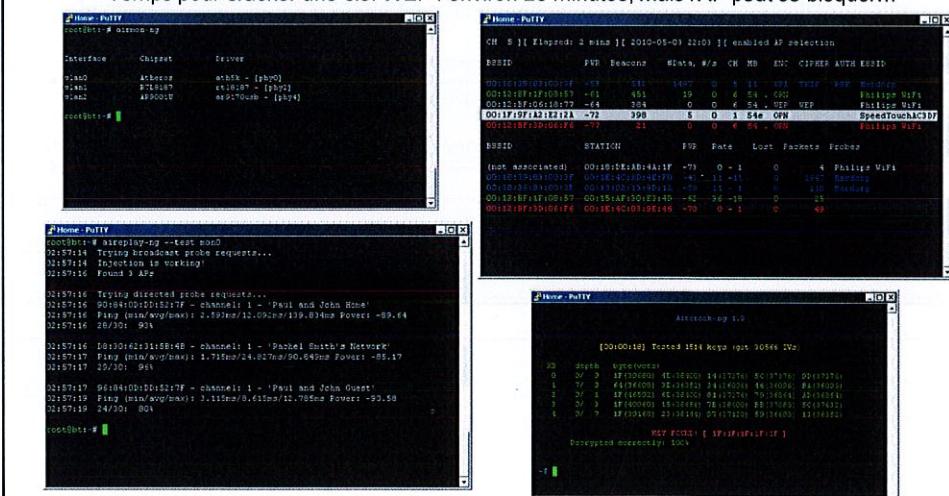


2-53

Aircrack-ng

- Suite logicielle la plus courante, fonctionne par injection

- Composé principalement de : Airmon-ng, Airodump-ng, Aireplay-ng , Aircrack-ng
 - Temps pour cracker une clef WEP : environ 20 minutes, mais l'AP peut se bloquer....



2-54

Construire un réseau Wi-Fi sécurisé

Base des protocoles MAC 802.11

Recherche des réseaux sans-fil

Analyseurs de réseau sans-fil

Mise en œuvre d'une sécurité de base avec WEP

Décodage des données WEP



Résumé du chapitre

2-55

Résumé du chapitre

• Dans ce chapitre, nous avons

- Étudié les faiblesses inhérentes aux réseaux sans-fil et vu comment elles sont exploitées par les pirates
- Utilisé des outils d'analyse pour détecter les vulnérabilités d'un réseau sans-fil
- Mise en œuvre des stratégies de sécurité de base et des technologies de chiffrement
- Appliqué une protection de base avec WEP (Wired Equivalent Privacy)
- Découvert les points faibles de WEP

2-56