

Sécurité des Réseaux Wi-Fi



Présenté par :

- Ould Mohamed Lamine
- Ousmane Diouf

Table des matières

- Présentation du réseau Wi-Fi
- Configuration d'un réseau Wi-Fi
- Risques liés aux réseaux Wi-Fi
- Règles de base de Sécurité Wi-Fi
- Sécurisation avancée

Norme 802.11

- Adoption en 1997
- Bande 2.4 GHZ
- Bande 5 GHZ
- Debit allant de 1 Mbps à 54 Mbps
- Techniques de modulation différentes
- 1999 Wi-Fi Alliance

Revisions

- 802.11a
 - ◆ 8 canaux de la Bande 5
 - ◆ Debit de 54 Mbps
 - ◆ modulation OFDM
 - ◆ Portée 35m

Revisions

- 802.11b
 - ◆ 11-13 canaux de la Bande 2.4
 - ◆ Debit de 11 Mbps
 - ◆ modulation DSSS
 - ◆ Portée 70m

Revisions

- 802.11g
 - ◆ 11-13 canaux de la Bande 2.4
 - ◆ Debit de 54 Mbps
 - ◆ modulation OFDM
 - ◆ Portée 35 m

Revisions

- 802.11n
 - ◆ Attendu courant 2008
 - ◆ Probablement 2.4 et 5 GHz
 - ◆ Debit de 248×2 Mbps
 - ◆ modulation MIMO OFDM
 - ◆ Portée 200 m

Revisions

- 802.11i

Porte sur la sécurité

- ◆ Authentification
- ◆ Chiffrement des transmissions pour les normes 802.11a,802.11b,802.11g.
- ◆ Gestion et échange des clés

Modes de fonctionnement du Wi-Fi

- Mode adhoc (ISS)
- Mode infrastructure (BSS, ESS)
- Autres modes

Configuration d'un réseau Wi-Fi

- Configuration d'un point d'accès

The screenshot shows a Microsoft Internet Explorer browser window displaying the configuration page for a Linksys Wireless-G ADSL Gateway (WAG54G V.2). The browser's address bar shows the URL `http://192.168.1.1/Wireless_Basic.asp`. The page features a navigation menu with tabs for Setup, Wireless, Security, Access Restrictions, Applications & Gaming, Administration, and Status. The 'Wireless' tab is active, showing the 'Basic Wireless Settings' section. The configuration options are as follows:

- Wireless Network Mode: Mixed
- Wireless Network Name (SSID): ya_ngatcha_tech
- Wireless Channel: 11 - 2.462GHz
- Wireless SSID Broadcast: Enable Disable

At the bottom of the configuration area, there are buttons for 'Save Settings' and 'Cancel Changes'. The Linksys logo and 'A Division of Cisco Systems, Inc.' are visible in the top left, and the Cisco Systems logo is in the bottom right. The browser's status bar at the bottom shows the time as 16:34 and the system tray includes the 'démarrer' button and the 'Linux' logo.

Risques liés aux réseaux Wi-Fi

- Interception des données
- Intrusion réseau
- Brouillage radio
- Dénis de Service

Sécurisation

Règles de base de sécurité Wi-Fi

- Bon positionnement des équipements
- Eviter les valeurs par défaut
- Activation d'un cryptage (WEP ou WPA)
- Filtrage par adresse MAC
- Désactiver le DHCP, utilisation d'adresses fixes.
- Utilisation d'un pare-feu

Cryptage des données

- WEP (Wired Equivalent Privacy)
 - Clé symétrique (64 bits ou 128 bits)
 - Algorithme de cryptage RC4
 - Possibilité d'avoir jusqu'à 4 clés en rotation.

Cryptage des données

- WPA (Wireless Protected Access)
 - ◆ Adopté en 2003, WPA2 en 2004
 - ◆ Algorithmes TKIP, AES
 - ◆ Clé de 256 et de 512 bits

Mode Personnel

- Convient à l' utilisation privée
- TKIP comme algorithmme
- PSK(pre-shared Key) de 64 à 504 bits !!

Mode Entreprise

- Convient à l' utilisation professionnelle
- Basée sur la norme 802.1x et EAP
- AES comme algorithme
- **Gestion dynamique des clés de 256 ou de 512 bits**

Sécurisation

Outils de piratage

- Airodump

Outil d'ecoute qui nous permet l'obtention :

- ◆ ESSID et BSSID des APs
- ◆ Adresses Mac de clients (à utiliser pour usurpation)
- ◆ Mode de cryptage utilisé
- ◆ Canaux de fréquence utilisés
- ◆ Paquets IVs

Outils de piratage

- Airodump

www.Mcours.com
Site N°1 des Cours et Exercices Email: contact@mcours.com

```
Shell - Konsole
Shell

BSSID          PWR  Packets  LAN IP / # IVs  CH  MB  ENC  ESSID
B2:B3:54:76:BF:9A  8      52
00:14:BF:6D:C0:20  27    1039
1E:84:C4:83:B2:C3   5     997
                406   11   54  WEP  wifi-rtn
                11    48  OPN  bombolong

BSSID          STATION          PWR  Packets  ESSID
00:14:BF:6D:C0:20 00:0A:79:47:A0:40  46    423  wifi-rtn
1E:84:C4:83:B2:C3 00:12:17:15:F0:8E   9     508  bombolong

wH0x
livesecurityresource
http://iwh0x.net
```

Aircrack

Pour décrypter la clé WEP Aircrack utilise les Ivs :

- **Environ 300 000 IVs pour une clé de 64 bits**
- **Environ 1 000 000 IVs pour une clé de 128 bits**

Aireplay

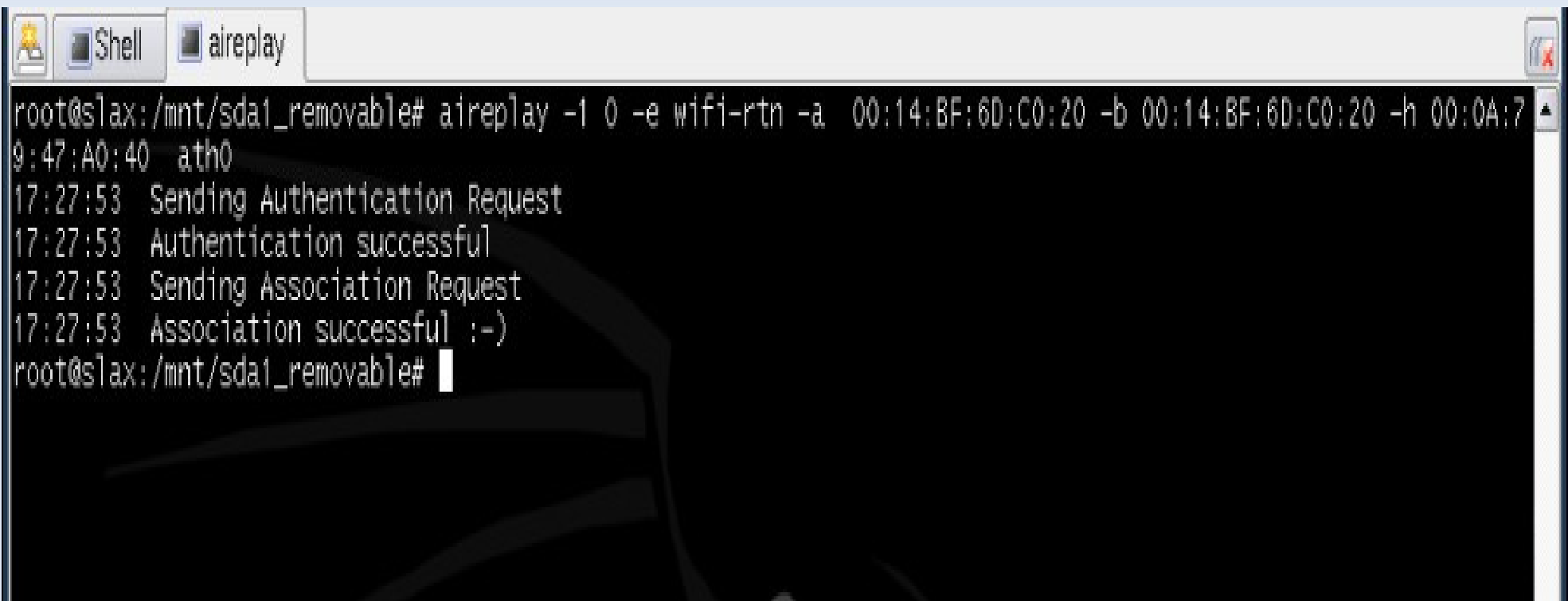
- Fausse authentification par adresse MAC
- Injection de paquets pour augmenter le trafic

Aireplay

- Fausse authentification par adresse MAC
- Injection de paquets pour augmenter le trafic

Aireplay

Fausse Association avec un BSSID obtenu avec Airodump



```
root@slax:/mnt/sda1_removable# aireplay -i 0 -e wifi-rtn -a 00:14:BF:6D:C0:20 -b 00:14:BF:6D:C0:20 -h 00:0A:79:47:A0:40 ath0
17:27:53 Sending Authentication Request
17:27:53 Authentication successful
17:27:53 Sending Association Request
17:27:53 Association successful :-)
```

The image shows a terminal window titled 'Shell' and 'aireplay'. The user is running the command `aireplay -i 0 -e wifi-rtn -a 00:14:BF:6D:C0:20 -b 00:14:BF:6D:C0:20 -h 00:0A:79:47:A0:40 ath0`. The output shows a successful authentication and association process.

Outils de piratage

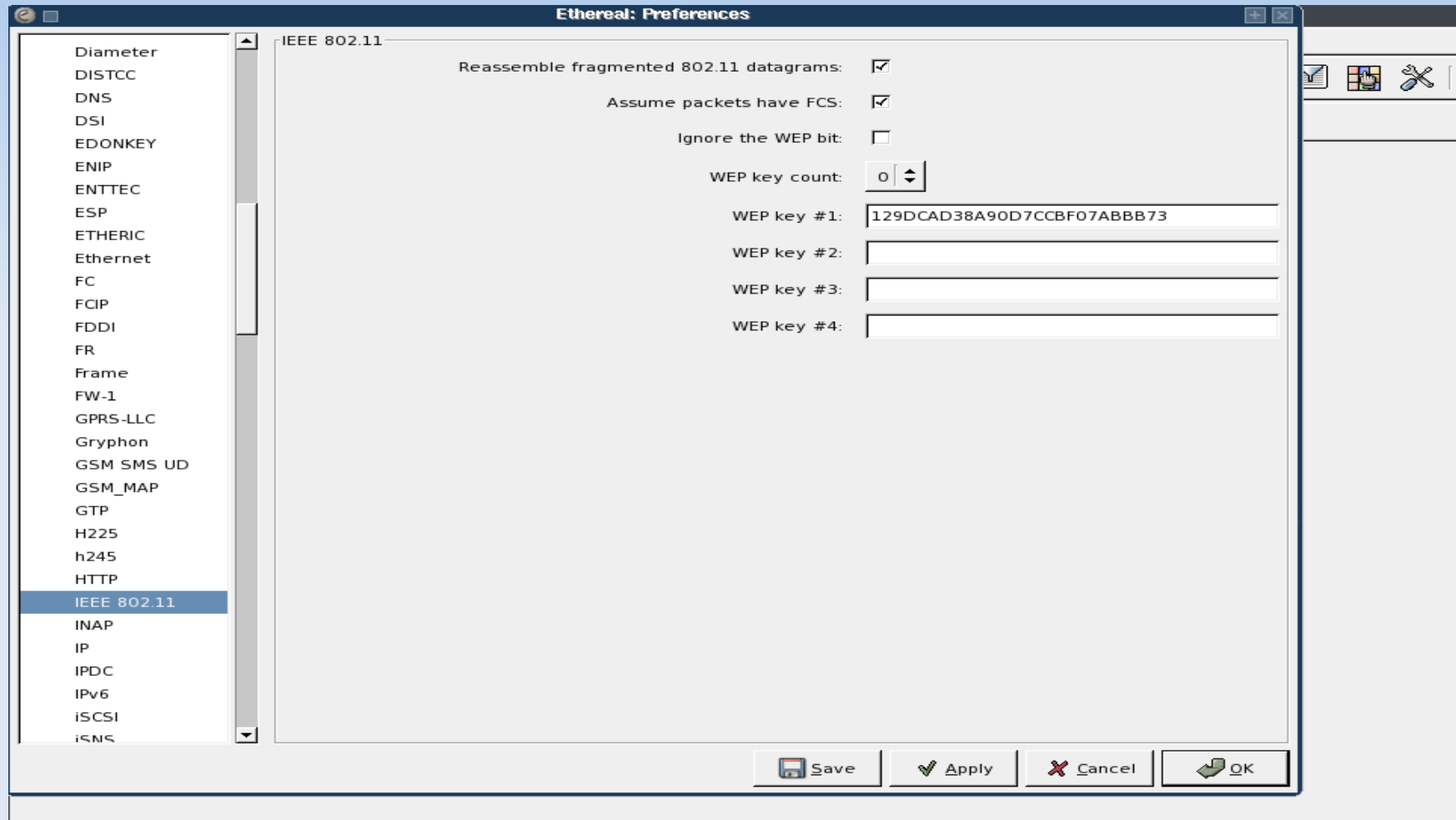
- Les informations recueillies après écoute sont utilisées pour cracker une clé avec aircrack(par exemple).

```
aircrack-ng  
9 0/ 20 07( 114) 04( 90) 2D( 77) 3C( 33) 89( 27) 55( 21)  
10 2/ 4 AB( 83) 19( 62) 3D( 41) 00( 33) 87( 30) A5( 27)  
11 0/ 4 BB( 448) 96( 208) A5( 85) 6D( 66) 65( 43) C4( 42)  
12 0/ 7 73( 540) A9( 253) A3( 123) 79( 105) 80( 94) 7F( 64)  
  
KEY FOUND! [12:9D:CA:D3:8A:9D:D7:CC:BF:07:AB:BB:73 ]
```

Ethereal

- Ethereal est utile pour obtenir l'adresse IP d'un AP
- Faire des attaques de dictionnaire sur différents types de protocoles.

Ethereal



Ethereal

ath0: Capturing - Ethereal

File Edit View Go Capture Analyze Statistics Help

Filter: (wlan.bssid==00:14:BF:6D:C0:20) && (tcp) + Expression...

No. ↓	Time	Source	Destination	Protocol	Info
1023	31.418705	213.189.84.13	192.168.1.13	TCP	4662
1024	31.773423	213.189.84.13	192.168.1.13	TCP	4662

Sécurisation avancée

Méthodes d'authentification

■ Portail captif

Le portail captif est composé de plusieurs fonctionnalités

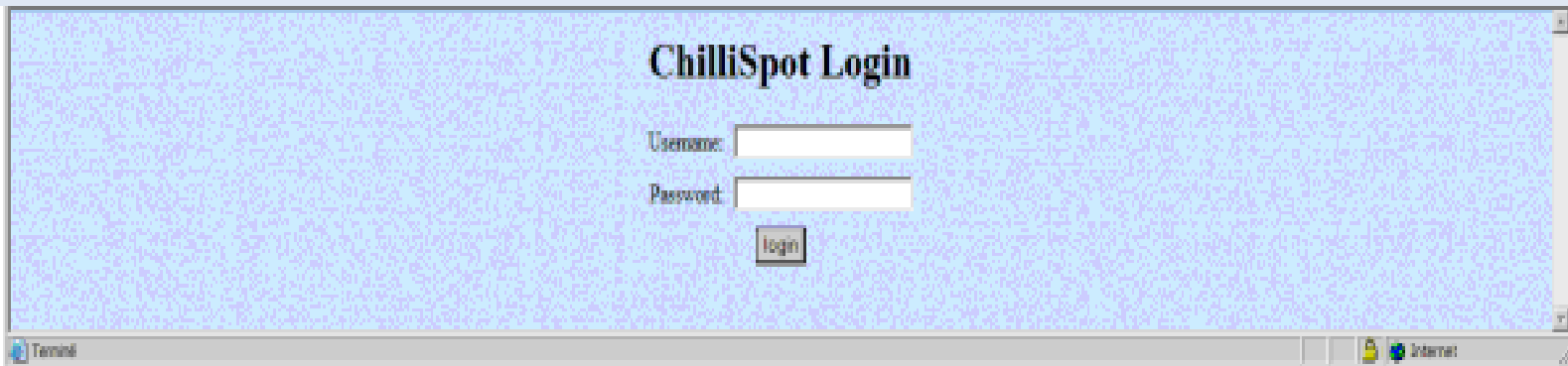
- Une passerelle entre plusieurs réseaux, équipée d'un filtre « firewall », pilotée par le portail http.

- Un portail http permettant la saisie de l'identité de l'utilisateur.

- Une base d'authentification contenant la liste des utilisateurs

Exemple portail captif(ChilliSpot)

- Toute requête http est redirigée vers une page d'authentification.



802.1x et EAP

- Standard mis en place en 2001
- Authentification dès l'accès physique au réseau.
- 802.1x s'appuie sur le protocole EAP(Extensible Authentication Protocol).

802.1x et EAP

- Principe général basé sur 3 entités:
 - ◆ système à authentifier(en général poste de travail)
 - ◆ système authentificateur(système relais:point d'accès en Wi-Fi)
 - ◆ serveur authentificateur(determine les services accessibles au demandeur:en général Serveur RADIUS)

Mécanismes d'authentification avec EAP

- Méthodes avec mots de passe
- Méthodes avec certificats
- Méthodes avec cartes à puce

Méthodes avec mots de passe

- **LEAP** (lightweight Extensible Authentication Protocol): A la base solution propriétaire Cisco, gère dynamiquement les clés WEP.
- **EAP-MD5** utilise MD5, authentification par login et mot de passe du client seul (pas d'authentification du serveur)
- **EAP-SKE** (EAP-Shared Key Exchange): permet une authentification mutuelle entre le client et le serveur.
- **EAP-PSK** (EAP Secure Remote Password)
sécurise la communication des mots de passe.

Méthodes avec certificats

- EAP-TLS(EAP-Transport Layer Security) basée sur SSL(Secure Socket Layer), authentication mutuelle entre le client et le serveur à travers des certificats. Le serveur possède une copie du certificat du client et vis-versat.
- EAP-TTLS(EAP-Tunneled TLS) extension de EAP-TLS génère des clés aléatoires protégées par un tunnel IPSec.

Méthodes avec certificats

- PEAP(Protected Extensible Authentication Protocol) crée d'abord un tunnel TLS, authentification par certificat niveau du serveur et par login/mot de passe pour le client.

Il existe d'autres méthodes d'authentification par certificats mais celles citées sont les plus utilisées.

Méthodes avec cartes à puce

- EAP-SIM(Subscriber Identity Module) utilise la carte SIM du GSM.
- EAP-AKA(Authentication and Key Agreement)utilise la carte USIM de l'UMTS.

Serveur d'authentification RADIUS

- la norme 802.1x effectue l'authentification sur un serveur qui est en général un serveur RADIUS.
- Un serveur RADIUS(Remote Authentication Dial In User Service) est un serveur AAA(Authentication Autorization Accounting) fonctionnant en mode client/serveur.

Serveur d'authentification RADIUS

- Le serveur AAA est chargé de 3 tâches:
 - ◆ Vérifier l'identité des clients stockés dans un fichier texte, une base de données, un annuaire LDAP,.... (authentification)
 - ◆ Définir les droits du client (authorization)
 - ◆ Archiver l'utilisation des ressources réseau du client

Serveur d'authentification RADIUS

- L'authentification entre le serveur et le NAS(Network Access Server):le point d'accès en Wi-Fi se fait grâce à un mot de passe partagé qui n'est jamais envoyé sur le réseau.
- Le mot de passe partagé sert à crypter les échanges entre le serveur et le point d'accès.

Exemple Serveur RADIUS:Freeradius

- Freeradius est gratuit et libre,tourne sous Linux.
- supporte de nombreux EAP et permet d'authentifier les utilisateurs selon plusieurs moyens :mots de passe UNIX,bases de données,annuaires LDAP ou Active Directory....



- Utilise le port UDP 1812 pour l'authentification et le port 1813 pour la gestion des comptes.

Quelle solution de Sécurité Wi-Fi choisir ?

- Côté cryptage des données:
 - ♦ le WEP a montré ses faiblesses et ne résiste pas aux attaques.
 - ♦ le WPA/TKIP est une solution acceptable en mode personnel, en évitant des mots de passe courts, se trouvant dans un dictionnaire....
 - ♦ WPA2 avec AES pour les entreprises.

Quelle solution de Sécurité Wi-Fi choisir ?

- Côté authentification:
 - ♦ le portail captif serait une solution pour un campus, un cyber espace libre mais protégé par un minimum d'authentification afin de ne pas surcharger le réseau.
 - ♦ Un serveur d'authentification avec 802.1x/EAP sera nécessaire pour les entreprises, notamment avec les certificats (PEAP EAP-TLS TTLS ...)

Quelle solution de Sécurité Wi-Fi choisir ?

- Ces solutions sont évoquées à titre d'orientation mais il est évident que chaque cas nécessite une étude spécifique tenant compte de la sensibilité des applications, des moyens disponibles, des contraintes....