WI-FI SECURITY

I.I.S. C. Olivetti - 5ª A Informatica - 2015
Marco Bartoli

What is  ?

The IEEE 802.11 standard

Standard	Release date	Band	Bandwidth	Throughput
802.11a	1999	5 GHz	20 MHz	11 Mbits/s
802.11b	1999	2.4 GHz	20 MHz	54 Mbits/s
802.11g	2003	2.4 Ghz	20 MHz	54 Mbits/s
802.11n	2009	2.4, 5 GHz	20, 40 MHz	600 Mbits/s
802.11ac	2014	5 GHz	40, 80, 160 Mhz	7 Gbits/s

Authentications and Encryptions

- Open

Authentications and Encryptions

- Open
- WEP

Authentications and Encryptions

- Open
- WEP
- WPA-Personal (WPA/WPA2)

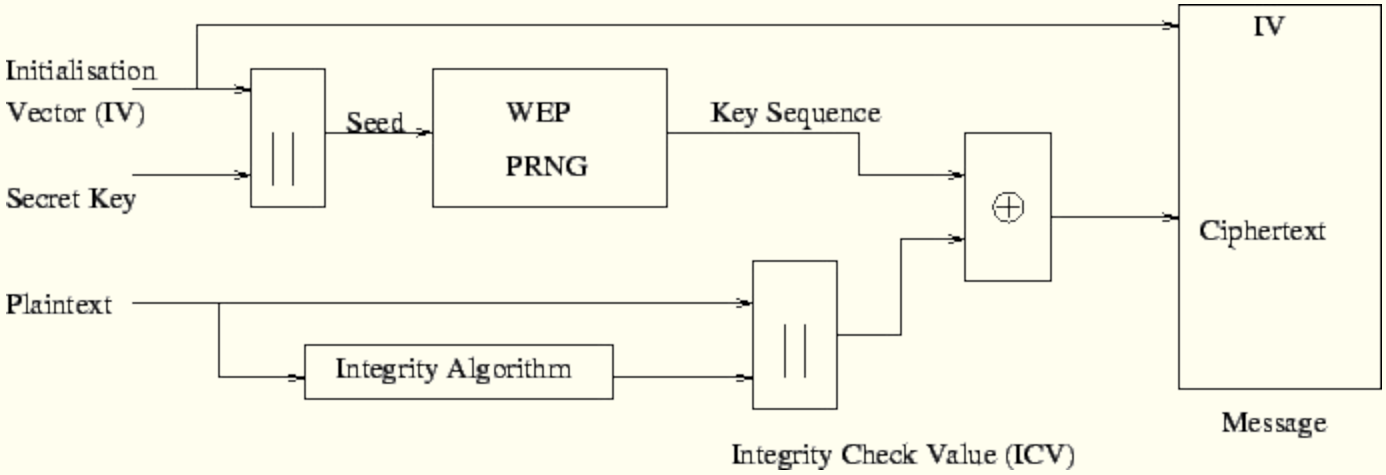
Authentications and Encryptions

- Open
- WEP
- WPA-Personal (WPA/WPA2)
- WPA-Enterprise (RADIUS)

Authentications and Encryptions

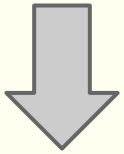
- Open
- WEP
- WPA-Personal (WPA/WPA2)
- WPA-Enterprise (RADIUS)
- WPS

WEP Weakness



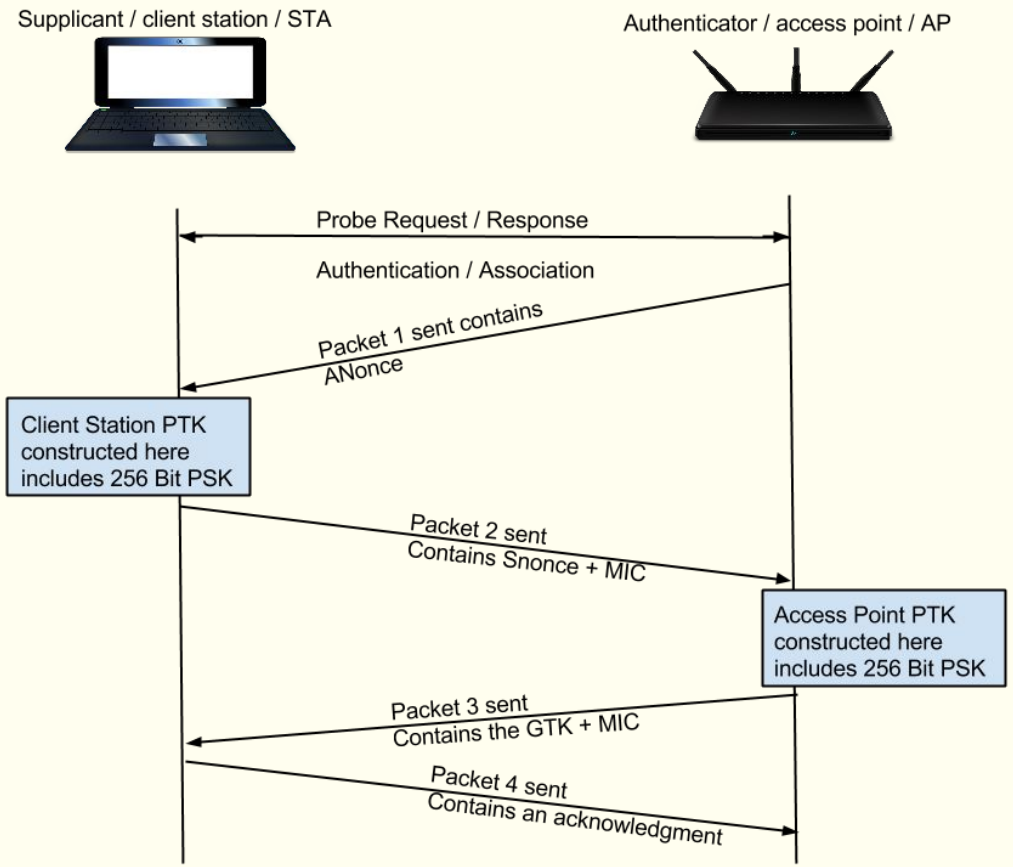
Aircrack Magics

```
CH  6 ][ Elapsed: 1 min ][ 2015-06-16 22:41 ][ resumed output

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

C4:6E:1F:C9:CF:08  -31 100      677        0    0   6  54e. WEP  WEP         Maturita2015

BSSID              STATION            PWR   Rate    Lost    Frames  Probe
```

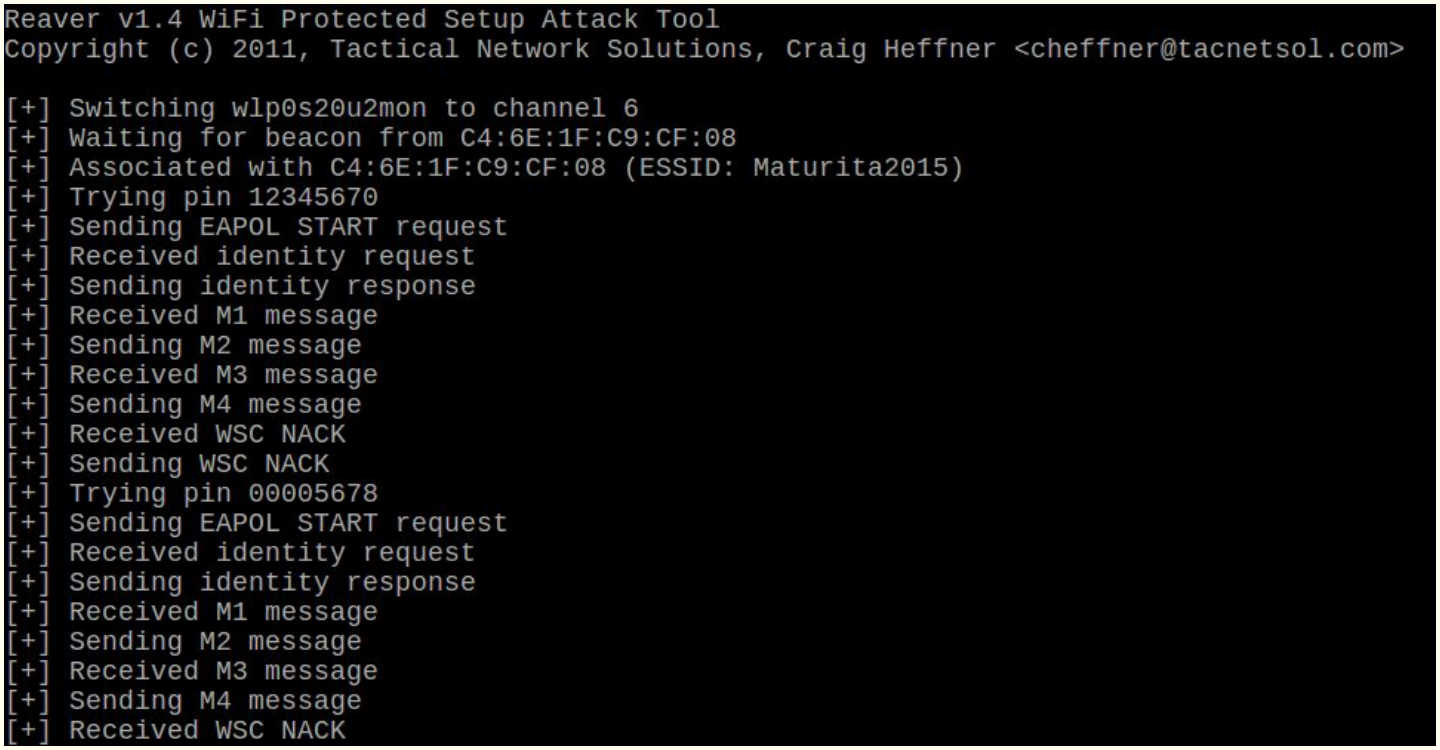


```
                              Aircrack-ng 1.2 rc2


                  [00:00:00] Tested 861 keys (got 50459 IVs)

  KB    depth   byte(vote)
   0    0/ 13   28(63744) A8(60928) 86(58880) C7(58880) 3D(58624)
   1    0/  1   57(76544) 0F(60928) 34(59392) 5B(58880) D4(57856)
   2    1/  2   1E(61952) A8(59648) 67(59136) 03(58624) 5F(58368)
   3    0/  1   B4(75264) 31(61184) 7F(60416) 66(58112) 83(57856)
   4    9/  4   F9(58368) 07(57856) EF(57856) FF(57856) 3B(57600)

              KEY FOUND! [ 28:E6:6B:E9:D3:B6:20:95:DD:E9:2F:BE:37 ]
         Decrypted correctly: 100%


WSX  ~  $
```

WPA-Personal Weakness



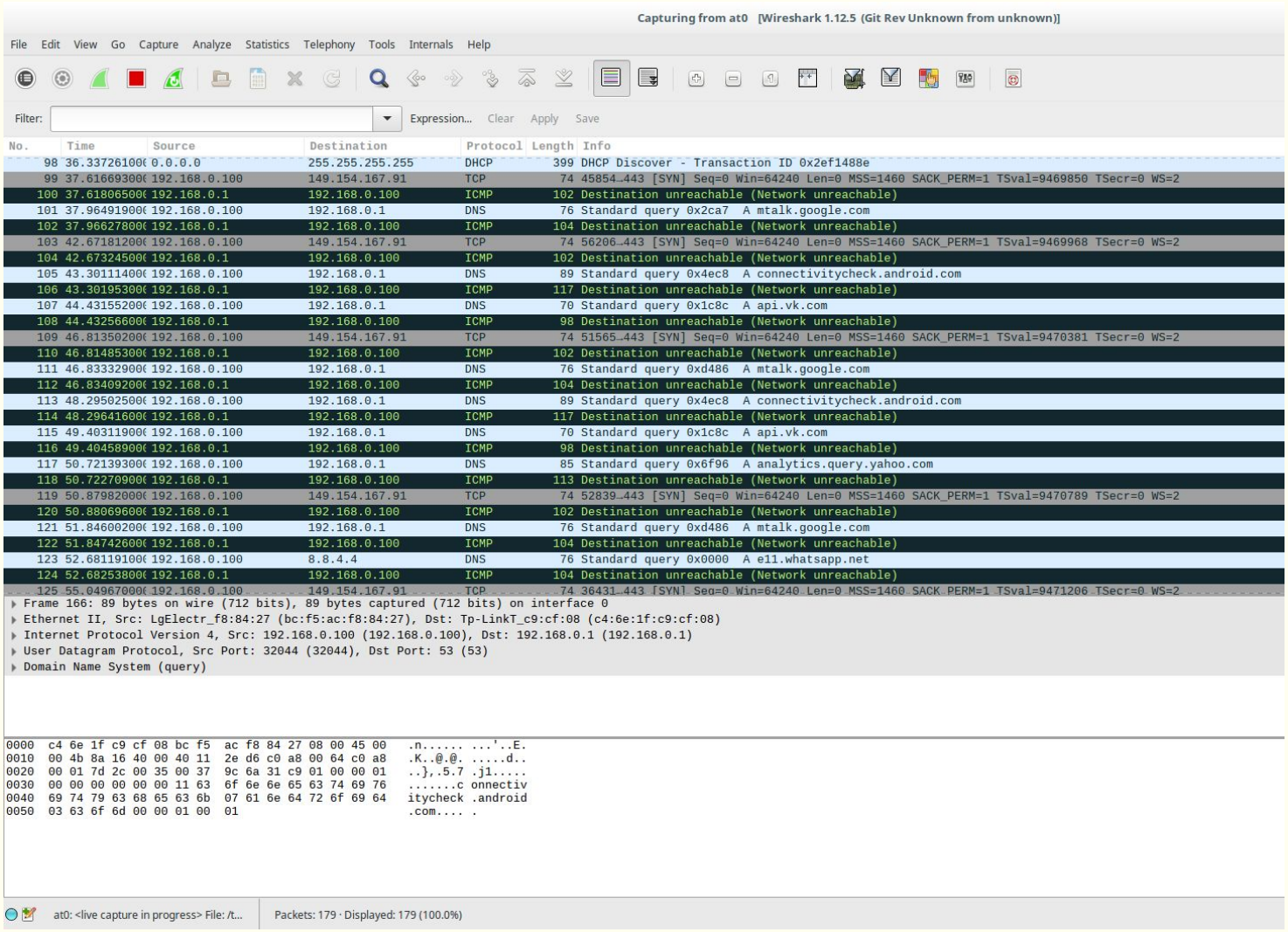
WPS Cracking



Further hacking methods

- MITM attack

MITM example using Wireshark



Further hacking methods

- MITM attack
- Denial of Service attack

Further hacking methods

- MITM attack
- Denial of Service attack
- Network injection

Further hacking methods

- MITM attack
- Denial of Service attack
- Network injection
- MAC spoofing

Additional protection techniques

- Filter MAC addresses

Additional protection techniques

- Filter MAC addresses
- Hide SSID

Additional protection techniques

- Filter MAC addresses
- Hide SSID
- Static IP addressing (disable DHCP)

Additional protection techniques

- Filter MAC addresses
- Hide SSID
- Static IP addressing (disable DHCP)
- RF shielded walls

Real security? Cables