

# WI-FI SECURITY



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

What is  <sup>TM</sup> ?

# 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

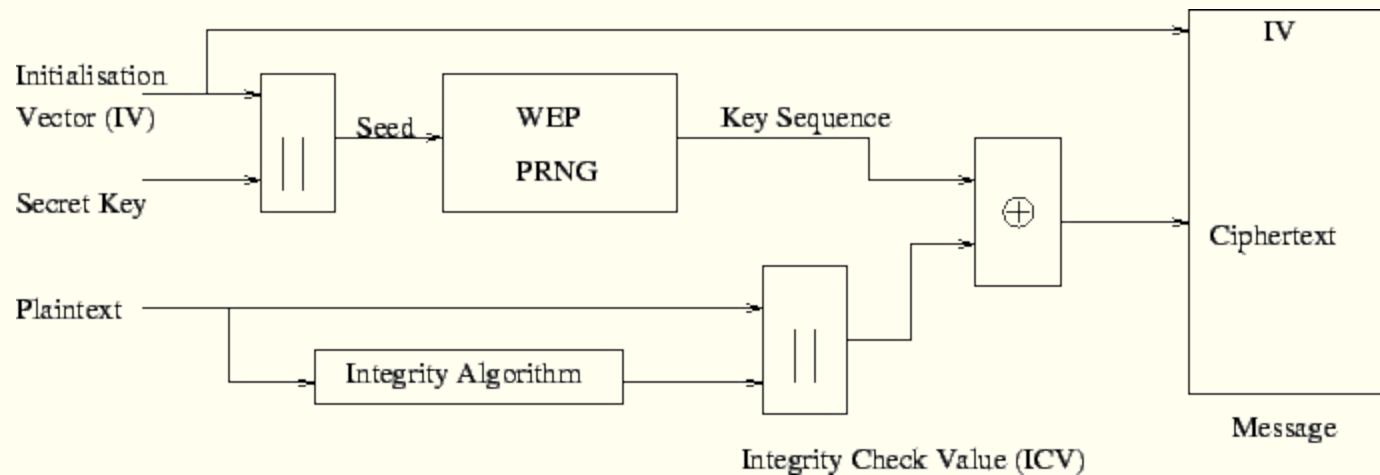
- Open
- WEP
- WPA-Personal (WPA/WPA2)
- WPA-Enterprise (RADIUS)

# Authentications and Encryptions

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



# WEP Weakness



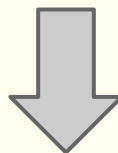
# Aircrack Magics

```
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)

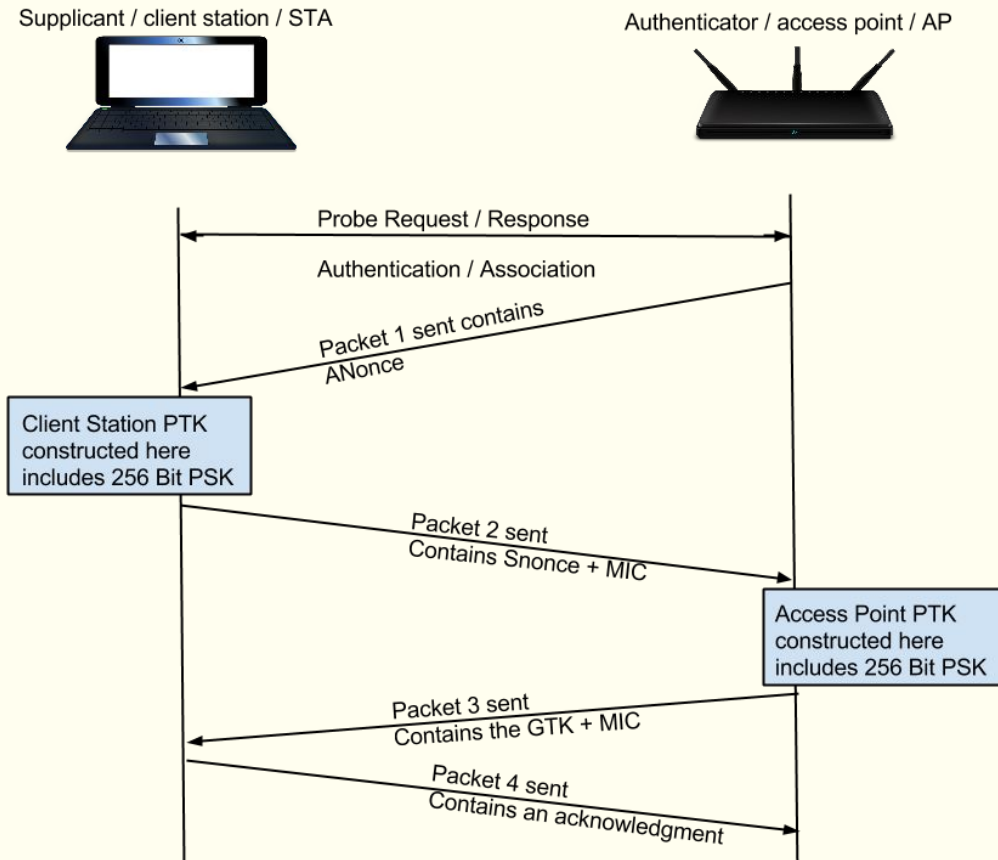
```
KEY FOUND! [ 28:E6:6B:E9:D3:B6:20:95:DD:E9:2F:BE:37 ]
```

```
Decrypted correctly: 100%
```

```
WSX ~ $
```

# WPA-Personal Weakness



# WPS Cracking

```
Reaver v1.4 WiFi Protected Setup Attack Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnetsol.com>

[+] Switching wlp0s20u2mon to channel 6
[+] Waiting for beacon from C4:6E:1F:C9:CF:08
[+] Associated with C4:6E:1F:C9:CF:08 (ESSID: Maturita2015)
[+] Trying pin 12345670
[+] Sending EAPOL START request
[+] Received identity request
[+] Sending identity response
[+] Received M1 message
[+] Sending M2 message
[+] Received M3 message
[+] Sending M4 message
[+] Received WSC NACK
[+] Sending WSC NACK
[+] Trying pin 00005678
[+] Sending EAPOL START request
[+] Received identity request
[+] Sending identity response
[+] Received M1 message
[+] Sending M2 message
[+] Received M3 message
[+] Sending M4 message
[+] Received WSC NACK
```

# Further hacking methods

- MITM attack

# MITM example using Wireshark

Capturing from at0 [Wireshark 1.12.5 (Git Rev Unknown from unknown)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
98	36.33726100	0.0.0.0	255.255.255.255	DHCP	399	DHCP Discover - Transaction ID 0x2ef1488e
99	37.61669300	192.168.0.100	149.154.167.91	TCP	74	45854.443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=9469850 TSecr=0 WS=2
100	37.61806500	192.168.0.1	192.168.0.100	ICMP	102	Destination unreachable (Network unreachable)
101	37.96491900	192.168.0.100	192.168.0.1	DNS	76	Standard query 0x2ca7 A mtalk.google.com
102	37.96627800	192.168.0.1	192.168.0.100	ICMP	104	Destination unreachable (Network unreachable)
103	42.67181200	192.168.0.100	149.154.167.91	TCP	74	56206.443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=9469968 TSecr=0 WS=2
104	42.67324500	192.168.0.1	192.168.0.100	ICMP	102	Destination unreachable (Network unreachable)
105	43.30111400	192.168.0.100	192.168.0.1	DNS	89	Standard query 0x4ec8 A connectivitycheck.android.com
106	43.30195300	192.168.0.1	192.168.0.100	ICMP	117	Destination unreachable (Network unreachable)
107	44.43155200	192.168.0.100	192.168.0.1	DNS	70	Standard query 0x1c8c A api.vk.com
108	44.43256600	192.168.0.1	192.168.0.100	ICMP	98	Destination unreachable (Network unreachable)
109	46.81350200	192.168.0.100	149.154.167.91	TCP	74	51565.443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=9470381 TSecr=0 WS=2
110	46.81485300	192.168.0.1	192.168.0.100	ICMP	102	Destination unreachable (Network unreachable)
111	46.83332900	192.168.0.100	192.168.0.1	DNS	76	Standard query 0xd486 A mtalk.google.com
112	46.83409200	192.168.0.1	192.168.0.100	ICMP	104	Destination unreachable (Network unreachable)
113	48.29502500	192.168.0.100	192.168.0.1	DNS	89	Standard query 0x4ec8 A connectivitycheck.android.com
114	48.29641600	192.168.0.1	192.168.0.100	ICMP	117	Destination unreachable (Network unreachable)
115	49.40311900	192.168.0.100	192.168.0.1	DNS	70	Standard query 0x1c8c A api.vk.com
116	49.40458900	192.168.0.1	192.168.0.100	ICMP	98	Destination unreachable (Network unreachable)
117	50.72139300	192.168.0.100	192.168.0.1	DNS	85	Standard query 0x6f96 A analytics.query.yahoo.com
118	50.72270900	192.168.0.1	192.168.0.100	ICMP	113	Destination unreachable (Network unreachable)
119	50.87982000	192.168.0.100	149.154.167.91	TCP	74	52839.443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=9470789 TSecr=0 WS=2
120	50.88069600	192.168.0.1	192.168.0.100	ICMP	102	Destination unreachable (Network unreachable)
121	51.84600200	192.168.0.100	192.168.0.1	DNS	76	Standard query 0xd486 A mtalk.google.com
122	51.84742600	192.168.0.1	192.168.0.100	ICMP	104	Destination unreachable (Network unreachable)
123	52.68119100	192.168.0.100	8.8.4.4	DNS	76	Standard query 0x0000 A e11.whatsapp.net
124	52.68253800	192.168.0.1	192.168.0.100	ICMP	104	Destination unreachable (Network unreachable)
125	55.04967000	192.168.0.100	149.154.167.91	TCP	74	36431.443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=9471206 TSecr=0 WS=2

Frame 166: 89 bytes on wire (712 bits), 89 bytes captured (712 bits) on interface 0  
Ethernet II, Src: LgElectr\_f8:84:27 (bc:f5:ac:f8:84:27), Dst: Tp-LinkT\_c9:cf:08 (c4:ce:1f:c9:cf:08)  
Internet Protocol Version 4, Src: 192.168.0.100 (192.168.0.100), Dst: 192.168.0.1 (192.168.0.1)  
User Datagram Protocol, Src Port: 32944 (32044), Dst Port: 53 (53)  
Domain Name System (query)

0000 c4 6e 1f c9 cf 08 bc f5 ac f8 84 27 08 00 45 00 .n.....'...E.  
0010 00 4b 8a 16 40 00 40 11 2e d6 c9 a8 00 64 c9 a8 .K.@@. ....d..  
0020 00 01 7d 2c 00 35 00 37 9c 6a 31 c9 01 00 00 01 .}.5.7. .jl.....  
0030 00 00 00 00 00 00 11 63 6f 6e 6e 63 74 69 76 .....c connectiv  
0040 69 74 79 63 68 65 63 6b 07 61 6e 64 72 6f 69 64 itycheck .android  
0050 03 63 6f 6d 00 00 01 00 01 ..... .com.....

at0: <live capture in progress> File: /t... Packets: 179 · Displayed: 179 (100.0%)

# 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

