Wireless LAN Security: Securing Your Access Point

Sia Sie Tung , Nurul Nadia Ahmad, Tan Kim Geok
Faculty of Information Science and Technology
Multimedia University, Malaysia

Abstract

Wireless Local Area Network (WLAN) *is vulnerable to attacks due to the use of radio frequency, which encounters data revelation. This paper describes about wireless security in the physical layer, dealing namely with Access Points (AP). It is recommended to secure wireless LANs with a layered approach. Where best to begin securing the network than starting with the physical layer?*

1. Introduction

Wireless networks are totally different to wired networks, which can be physically secured. The information goes through the air, where anyone can transmit and anyone can receive. Signals are not guided by wires. WLANs are therefore essentially vulnerable to interception.

The 802.11 standard covers wireless networks. This classification actually comes from Institute of Electrical and Electronics Engineers (IEEE) where they create standards, and they number these standards in unique ways.

The 802.11 standard had two primary goals when it was initially written:-
1) ease of accessibility
2) connection
In other words, the 802.11 was developed as an 'open' standard. Bear in mind, when security is not engineered into a solution during the initial stages, the security solutions have historically been less than optimal.

There are currently a lot of worries about wireless security. Standard networks at home or at work are based on physical connectivity. With wireless there is no physical connection. Wireless access points are really radio transmitters. They use radio waves that can go through walls and buildings. This makes connecting to a local network in your home or place of employment very versatile. The downside is that connecting to your network as an intruder is a lot easier. Security considerations now have to be taken to prevent unauthorized access to your network and data.

Section 2 will describe the theoretical background of WLAN. To start securing wireless network, there are four elements that need to be addressed. Section 3 and 4 will illustrate the MAC address filtering and AP. While, Section 5 and 6 will talk about Service Set Identifier (SSID) parameter and Wired Equivalent Privacy (WEP).

2. Background

The most prominent feature about WLAN is the absence of wires and its mobility. However, as data traveled through air using radio frequency, it can easily be tapped by any one including unauthenticated personnel using a sniffer. [5]

Not paying much attention to the security of your wireless network is not a wise thing to do, designing a network with security in mind from the very beginning saves you time, effort, and perhaps money. Prevention during primary stages is always the best solution.

It does not mean that some organizations do not need to worry about wireless security if their wireless LAN deployment was not too significant. At some point, most connect with the main organization's backbone. It is possible for hackers to use the wireless LAN as a launch pad to the entire network.

To achieve complete security in wireless network seems a near impossible task. Therefore adequate deterrence should be suggested instead while designing a wireless network.

In this case it means that we need to take a hard look at the access point. The access point would be the first to look into for setting up a good secured wireless network.

Currently, there are many kinds of AP in market. An example of a decent and reasonably priced access point is the Linksys IEEE 802.11 WRT54G. To protect your data and privacy, the Wireless-G Access Point can encrypt all wireless transmissions, and supports the industrial-strength security of Wi-Fi Protected Access (WPA). The MAC Address filter lets you decide exactly who has access to your wireless network. Another interesting feature about Linksys is its ability for firm-ware updates. The ability to update firmware is beneficial because functions can be added for the access point, or if bugs do occur, the company will come up with solutions to fix the firmware.

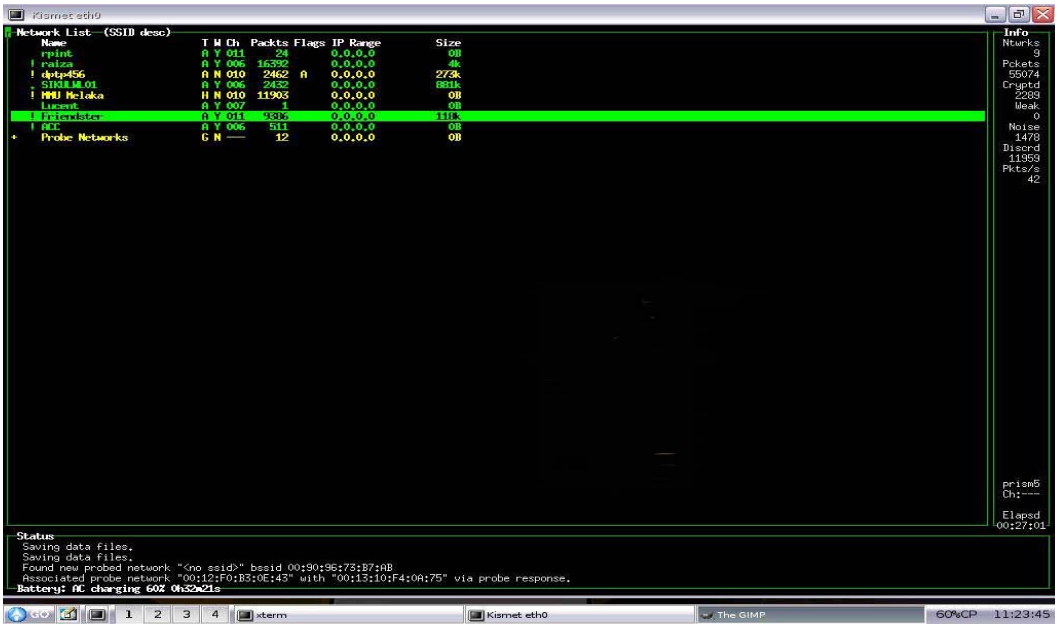
3. MAC Address Filtering

Every device that connects to a network has a unique hardware address called a MAC address (Media Access Control). This address is a 48-bit address expressed as 12 hexadecimal digits. This 12 digit hex number can be broken down even further into two fields. The first part of the MAC is a 24 bit vendor code. This identifies what vendor has made this particular network device. The last 24 bits in the MAC address is the serial number of the network interface card. [7]

So, we can identify our Access Points by the SSID, but how can we uniquely identify our wireless clients. We can identify them by their unique MAC address. So, by creating a list of unique MAC addresses we can restrict what PCs can connect to the AP. This is called MAC address filtering. If a PC with an unknown MAC address tries to connect, he will not be able to associate with the AP and thus will not be allowed to connect. This feature along with the previous SSID lockdown provides a great way to start securing your wireless network.

The below screenshot of the Kismet interface lists the different wireless networks that were detected by the online target laptop.

SSIDs that act as crude passwords and MAC addresses that act as personal identification numbers are often used to verify that clients are authorized to connect with an access point. Because existing encryption standards are not foolproof, knowledgeable intruders can pick off authorized SSIDs and MAC addresses to connect to a wireless LAN as an authorized user with the ability to steal bandwidth, corrupt or download files, and wreak havoc on the entire network.



```
Network List—(SSID desc)                                                    Info
     Name                        T W Ch  Packts Flags IP Range        Size  Ntwrks
     rpint                       A Y 011     24       0.0.0.0          0B        9
   ! raiza                       A Y 006  16392       0.0.0.0          4k   Pckets
   ! dptp456                     A N 010   2462  A    0.0.0.0        273k    55074
   . SIKULWL01                   A Y 006   2432       0.0.0.0        881k   Cryptd
   ! MMU Melaka                  H N 010  11903       0.0.0.0          0B     2289
     Lucent                      A Y 007      1       0.0.0.0          0B     Weak
   ! Friendster                  A Y 011   9386       0.0.0.0        118k        0
   ! ACC                         A Y 006    511       0.0.0.0          0B    Noise
 +   Probe Networks              G N ---     12       0.0.0.0          0B     1478
                                                                            Discrd
                                                                             11959
                                                                            Pkts/s
                                                                                42

                                                                            prism5
                                                                            Ch:---

                                                                            Elapsd
                                                                          00:27:01
Status
  Saving data files.
  Saving data files.
  Found new probed network "<no ssid>" bssid 00:90:96:73:B7:AB
  Associated probe network "00:12:F0:B3:0E:43" with "00:13:10:F4:0A:75" via probe response.
Battery: AC charging 60% 0h32m21s
```

Figure 1. Kismet Interface List

The network list in *Figure 1* states whether the network SSID is WEP enabled or not (the 'W' section). If the network was WEP enabled, it would state with a Y and if it wasn't an N will be stated instead. The 'Ch' section notes which channels the networks were connected on.

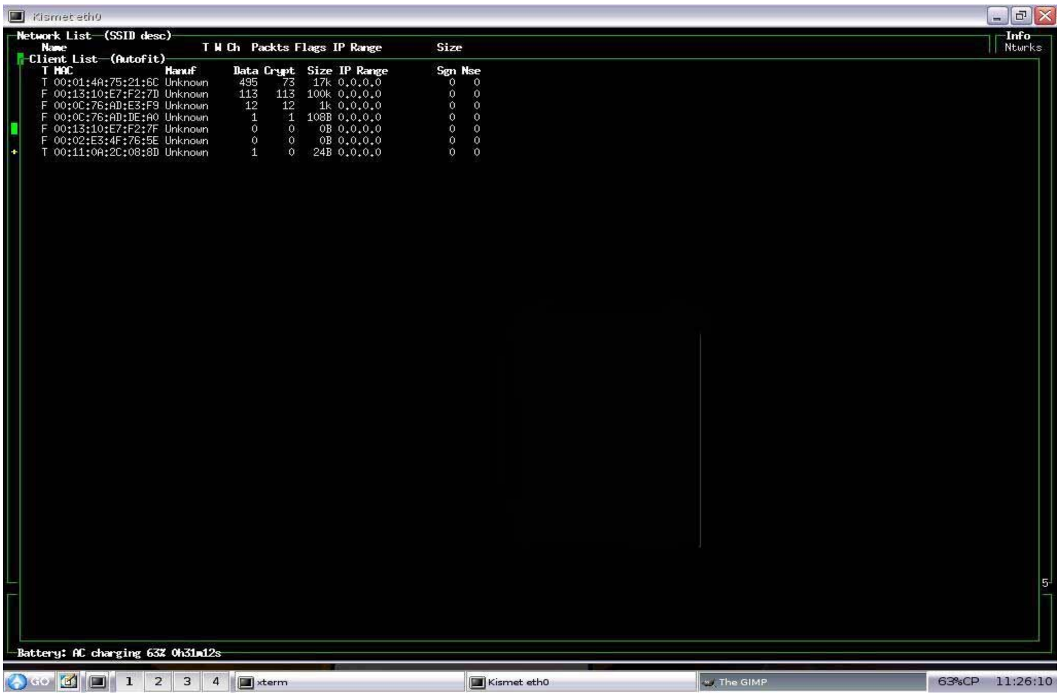
Kismet was able to detect networks that are broadcasting the SSID and those that are not, as revealed in the status section. As Kismet works passively, it does not send any loggable packets. It detects wireless APs and wireless clients, and associates them to each other.

As shown in the *Figure 2*, Kismet was able to reveal all the MAC addresses associated to the network. WRT54G is actually able to filter MAC addresses. Unfortunately, MAC filtering is trivial to bypass. The network traffic can be sniffed to determine which MAC addresses are present. MAC addresses can be changed after sniffing too.

To prove whether the AP includes Linksys IEEE 802.11 WRT54G is actually able to offer the security it features, we have acquired the Auditor Security Collection that can be downloaded from http://www.remote-exploit.org/. It provides a complete suite of wireless network discovery and penetration test tools.

Included in this suite is Kismet, an 802.11 wireless network detector, sniffer, and intrusion detection system. Kismet will work with any wireless card which supports raw monitoring (rfmon) mode, and can sniff 802.11b, 802.11a, and 802.11g traffic.

Kismet identifies networks by passively collecting packets and detecting standard named networks, detecting (and given time, decloaking) hidden networks, and inferring the presence of nonbeaconing networks via data traffic. [1]

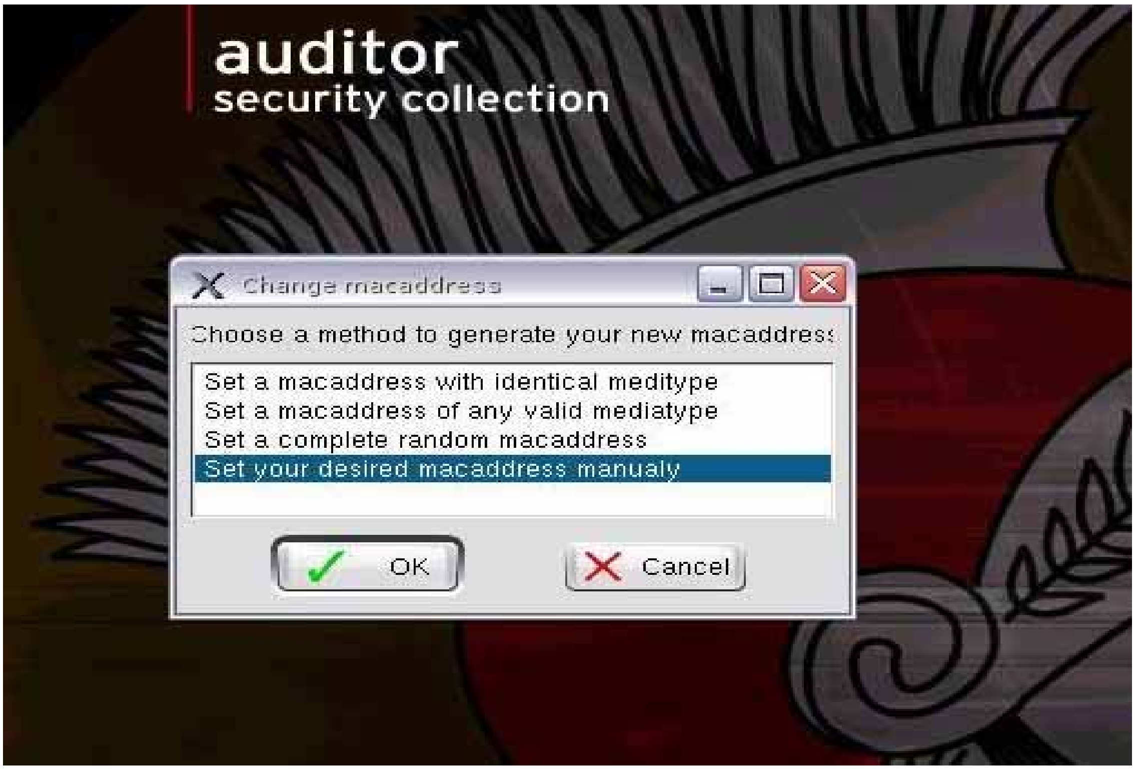


```
Network List—(SSID desc)
   Name                         T W Ch  Packts Flags IP Range         Size
 Client List—(Autofit)
   T MAC               Manuf        Data Crypt  Size IP Range          Sgn Nse
   T 00:01:4A:75:21:6C Unknown       495    73   17k 0.0.0.0             0   0
   F 00:13:10:E7:F2:7D Unknown       113   113  100k 0.0.0.0             0   0
   F 00:0C:76:AD:E3:F9 Unknown        12    12    1k 0.0.0.0             0   0
   F 00:0C:76:AD:DE:A0 Unknown         1     1  108B 0.0.0.0             0   0
   F 00:13:10:E7:F2:7F Unknown         0     0    0B 0.0.0.0             0   0
   F 00:02:E3:4F:76:5E Unknown         0     0    0B 0.0.0.0             0   0
 + T 00:11:0A:2C:08:8D Unknown         1     0   24B 0.0.0.0             0   0

Battery: AC charging 63% 0h31m12s
```

Figure 2. Kismet reveal address associated to the network

The Figure 3 below actually shows that Kismet offers the option to change MAC addresses. Many enterprises and universities secure their wireless LAN with authentication based on an authorized list of MAC addresses, such as currently deployed by Multimedia University (MMU) Malaysia. While this provides a low level of security for smaller deployments, MAC addresses were never intended to be used in this manner. As shown below, Kismet allows hackers to assume the identity of an authorized user by inserting the stolen MAC address as his own. The hacker then connects to the wireless LAN as an authorized user. However, Linkys was actually able to filter the MAC addresses.


auditor
security collection
Change macaddress
Set a macaddress with identical meditype
Set a macaddress of any valid mediatype
Set a complete random macaddress
Set your desired macaddress manualy
OK
Cancel

Choose a method to generate your new macaddres

Figure 3. Kismet Auditor Security Collection: Change MAC Address

4. Access Point (AP)

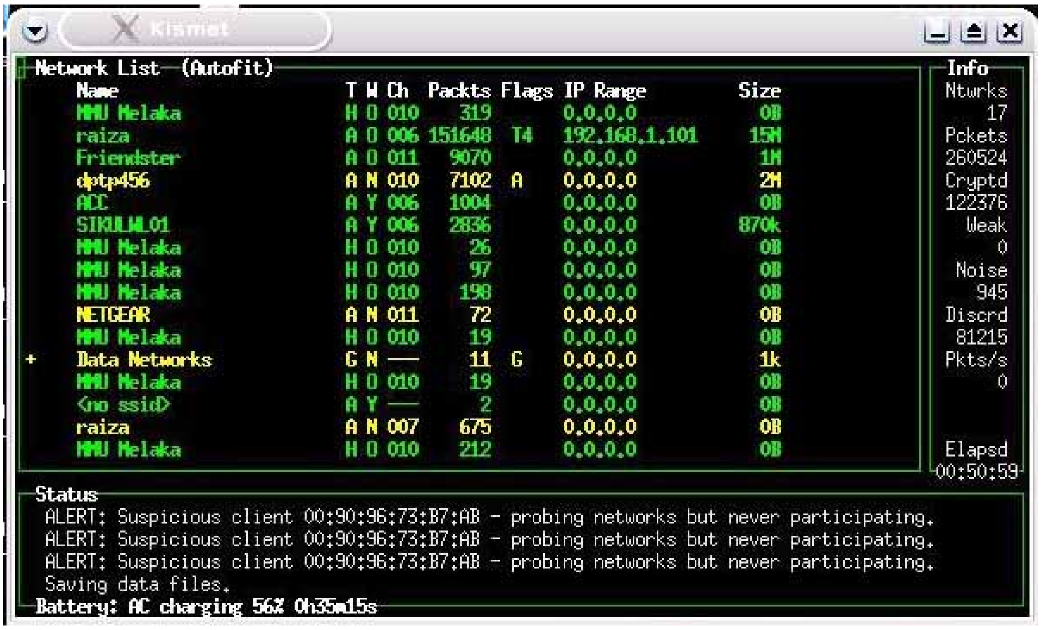
To secure wireless network, a very important factor is the choice of a good AP. The AP would be the first to look into for setting up a good secured wireless network.

First thing to be considered is the physical walkthrough, the signal strength and access point placement. For the physical walkthrough, things that need to be considered is the metal objects, open distances, building construction, window glass and all the material that can effect the signal strength.

The second component is access point; it is better to name access point properly so that it can be tracked down easily during trouble shooting event. Access point must be installed in a potential service location where it is a common place for users to reach. If access point is installed outdoors, make sure the equipment is properly secured, discouraging tampering.

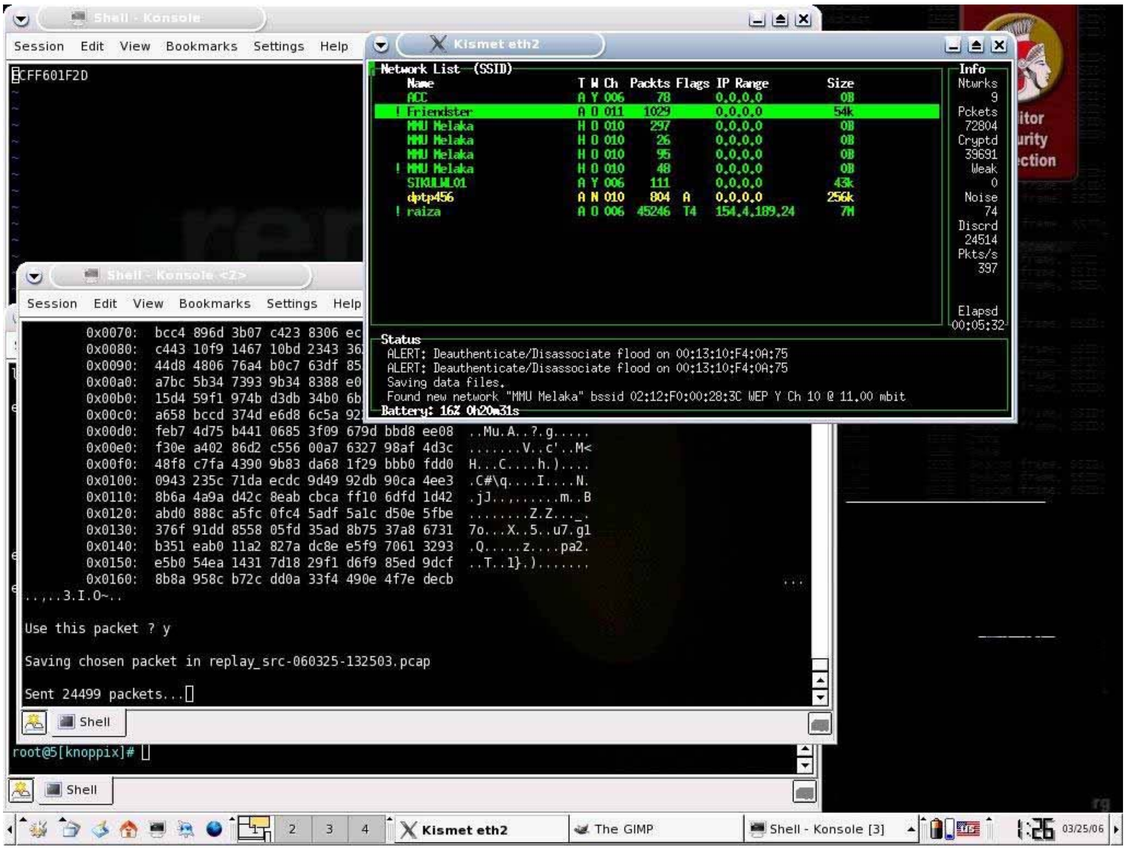
Figure 4 below shows a multiplicity of certain network. The attacker creates an access point, which has the same name as the original wireless network. The fake access point could be stronger or have greater signal should the attacker was able to be closer to its target. Usually stations would automatically select access points, which are greater; therefore the target may confuse and select the attacker's fake access point by mistake. A fake access point or more commonly known as a rogue access point is one that the organization having a wireless network does not authorize for operation. Linksys WRT54G is unable to prevent rogue access point.

The AP is secure if packets move slowly as shown in the following Figure 5. This means that Linksys WRT54G prevents replay attacks. Replay is an active attack on integrity where an intruding party resends information that is sent from the source entity to the destination entity. Replay attacks can be used to crack WEP as well.



```
Network List (Autofit)                                                          Info
    Name                        T W Ch  Packts Flags IP Range        Size       Ntwrks
    MMU Melaka                  H O 010    319       0.0.0.0          0B            17
    raiza                       A O 006 151648  T4   192.168.1.101   15M        Pckets
    Friendster                  A O 011   9070       0.0.0.0          1M        260524
    dptp456                     A N 010   7102  A    0.0.0.0          2M        Cryptd
    ACC                         A Y 006   1004       0.0.0.0          0B        122376
    SIKULWL01                   A Y 006   2836       0.0.0.0        870k          Weak
    MMU Melaka                  H O 010     26       0.0.0.0          0B             0
    MMU Melaka                  H O 010     97       0.0.0.0          0B         Noise
    MMU Melaka                  H O 010    198       0.0.0.0          0B           945
    NETGEAR                     A N 011     72       0.0.0.0          0B        Discrd
    MMU Melaka                  H O 010     19       0.0.0.0          0B         81215
 +  Data Networks               G N ---     11  G    0.0.0.0          1k        Pkts/s
    MMU Melaka                  H O 010     19       0.0.0.0          0B             0
    <no ssid>                   A Y ---      2       0.0.0.0          0B
    raiza                       A N 007    675       0.0.0.0          0B
    MMU Melaka                  H O 010    212       0.0.0.0          0B        Elapsd
                                                                              00:50:59
Status
 ALERT: Suspicious client 00:90:96:73:B7:AB - probing networks but never participating.
 ALERT: Suspicious client 00:90:96:73:B7:AB - probing networks but never participating.
 ALERT: Suspicious client 00:90:96:73:B7:AB - probing networks but never participating.
 Saving data files.
Battery: AC charging 56% 0h35m15s
```

Figure 4. Kismet Network List (Autofit): No weak IVs



```
CFF601F2D
```

```
Network List  (SSID)
    Name                      T W Ch  Packts Flags IP Range        Size
    ACC                       A Y 006     78       0.0.0.0           0B
  ! Friendster                A O 011   1029       0.0.0.0          54k
    MMU Melaka                H O 010    297       0.0.0.0           0B
    MMU Melaka                H O 010     26       0.0.0.0           0B
    MMU Melaka                H O 010     95       0.0.0.0           0B
  ! MMU Melaka                H O 010     48       0.0.0.0           0B
    SIKULWL01                 A Y 006    111       0.0.0.0          43k
    dptp456                   A N 010    804  A    0.0.0.0         256k
  ! raiza                     A O 006  45246  T4   154.4.189.24      7M

Info
Ntwrks
 9
Pckets
 72804
Cryptd
 39691
Weak
 0
Noise
 74
Discrd
 24514
Pkts/s
 397
Elapsd
00:05:32

Status
 ALERT: Deauthenticate/Disassociate flood on 00:13:10:F4:0A:75
 ALERT: Deauthenticate/Disassociate flood on 00:13:10:F4:0A:75
 Saving data files.
 Found new network "MMU Melaka" bssid 02:12:F0:00:28:3C WEP Y Ch 10 @ 11.00 mbit
Battery: 16% 0h20m31s
```

```
        0x0070:  bcc4 896d 3b07 c423 8306 ec
        0x0080:  c443 10f9 1467 10bd 2343 36
        0x0090:  44d8 4806 76a4 b0c7 63df 85
        0x00a0:  a7bc 5b34 7393 9b34 8388 e0
        0x00b0:  15d4 59f1 974b d3db 34b0 6b
        0x00c0:  a658 bccd 374d e6d8 6c5a 92
        0x00d0:  feb7 4d75 b441 0685 3f09 679d bbd8 ee08  ..Mu.A..?.g.....
        0x00e0:  f30e a402 86d2 c556 00a7 6327 98af 4d3c  .......V..c'..M<
        0x00f0:  48f8 c7fa 4390 9b83 da68 1f29 bbb0 fdd0  H...C....h.)....
        0x0100:  0943 235c 71da ecdc 9d49 92db 90ca 4ee3  .C#\q....I....N.
        0x0110:  8b6a 4a9a d42c 8eab cbca ff10 6dfd 1d42  .jJ..,.......m..B
        0x0120:  abd0 888c a5fc 0fc4 5adf 5a1c d50e 5fbe  ........Z.Z..._.
        0x0130:  376f 91dd 8558 05fd 35ad 8b75 37a8 6731  7o...X..5..u7.g1
        0x0140:  b351 eab0 11a2 827a dc8e e5f9 7061 3293  .Q.....z....pa2.
        0x0150:  e5b0 54ea 1431 7d18 29f1 d6f9 85ed 9dcf  ..T..1}.).......
        0x0160:  8b8a 958c b72c dd0a 33f4 490e 4f7e decb                  ...
..,..3.I.O~..

Use this packet ? y

Saving chosen packet in replay_src-060325-132503.pcap

Sent 24499 packets...
```

```
root@5[knoppix]#
```

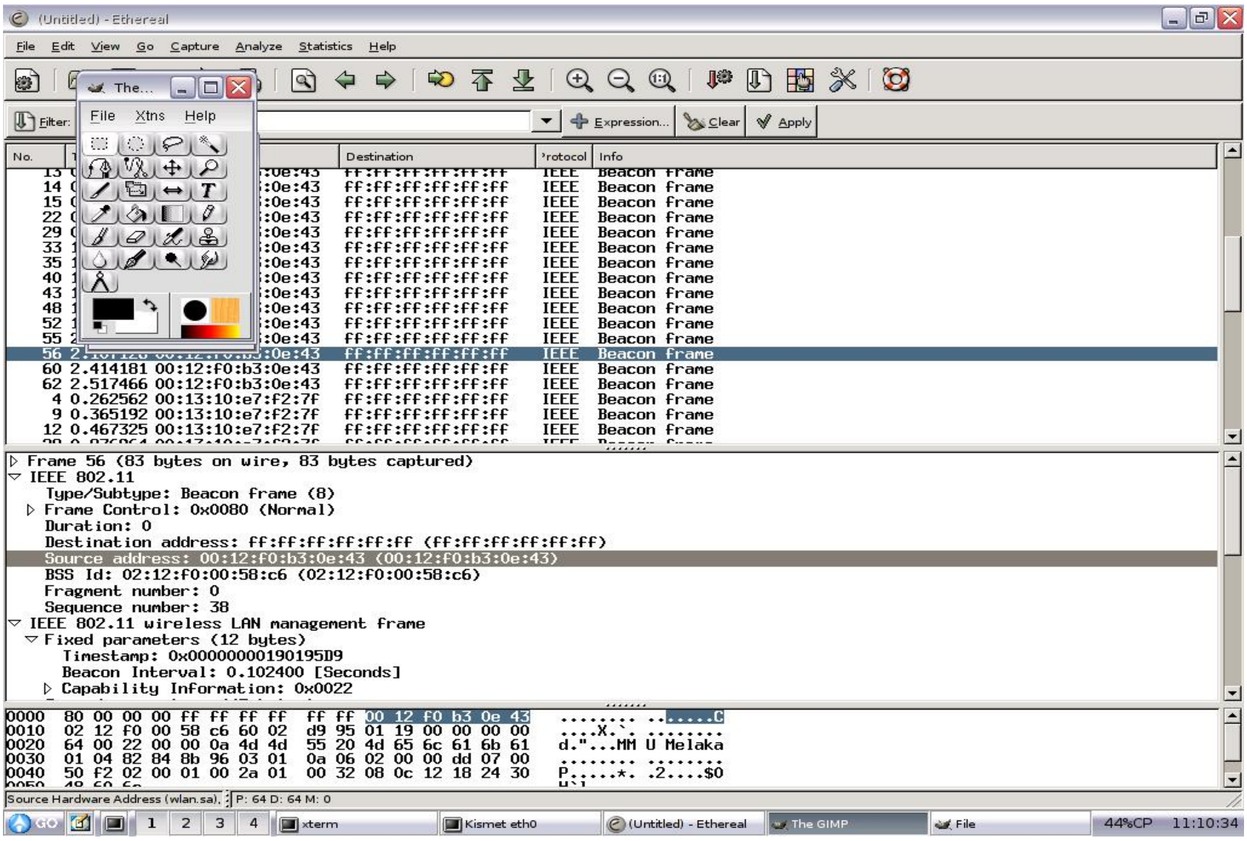
Figure 5. Linksys WRT54G: Prevent reply attack

5. Service Set Identifier (SSID)

The SSID is the first parameter that gets talked about when wireless LAN security is discussed. This is a 1 to 32 alphanumeric character string that is used to identify membership to an access point (AP) in a wireless local area network (WLAN). [6]

The beacon frame, which is a type of management frame, provides the "heartbeat" of a wireless LAN, enabling stations to establish and maintain communications in an orderly fashion.[3] When a device transmits a beacon frame, which can occur several times per second, it is advertising itself to the world in hopes of finding something else to communicate with. When a device receives a beacon frame, it has all the information it needs to communicate with the transmitting device; namely, the SSID.

These frames were captured using Ethereal’s network packet analyzer which can be downloaded from www.ethereal.com. By sniffing a beacon frame, one can find the SSID information as shown in the Figure 6. SSID information can be filtered by some APs. Linksys WRT54G provides the option of enabling/disabling SSID broadcasts. This can act as some kind of password to the wireless network, therefore filtering SSID can be considered as a type of password. A good SSID would not have a name that is related to that organization. Another good example is an unnamed SSID, anonymity is better as shown in the following Figure 7.



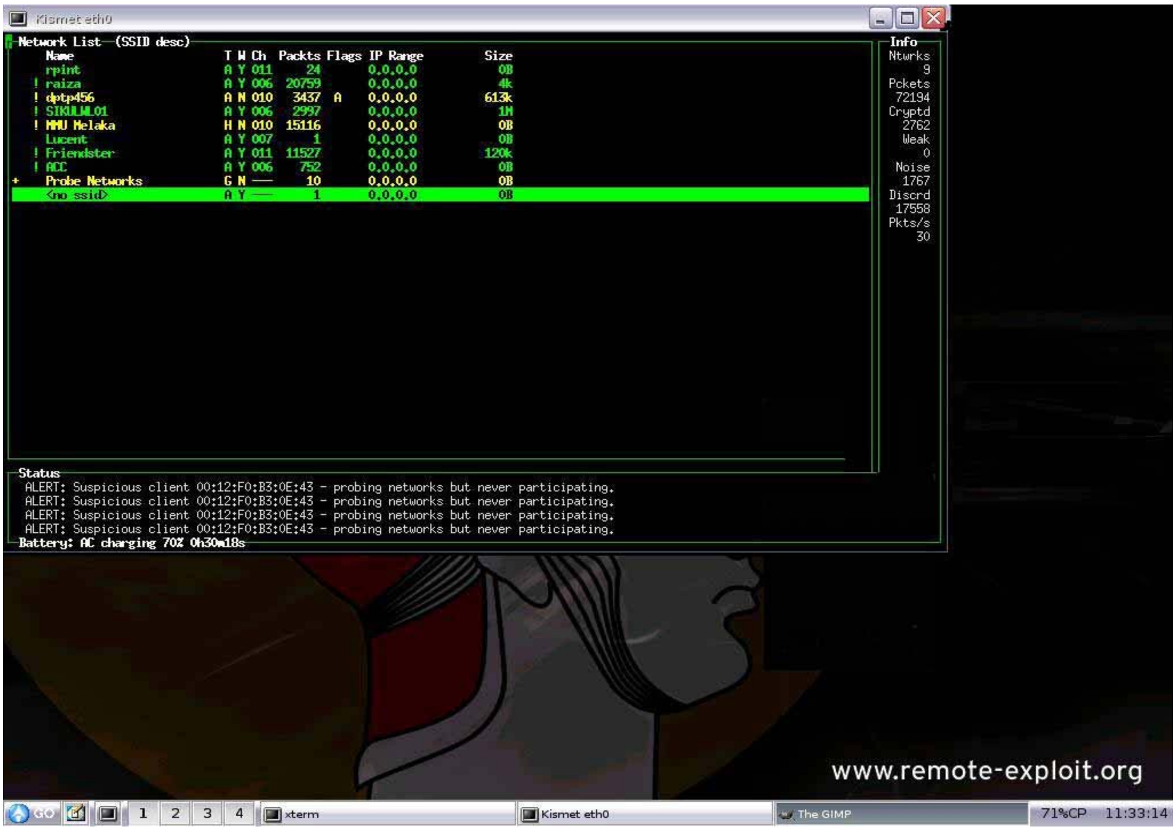
```
No.  T                        Destination         'rotocol  Info
 13 (              :0e:43  ff:ff:ff:ff:ff:ff   IEEE   Beacon frame
 14 0              :0e:43  ff:ff:ff:ff:ff:ff   IEEE   Beacon frame
 15 0              :0e:43  ff:ff:ff:ff:ff:ff   IEEE   Beacon frame
 22 0              :0e:43  ff:ff:ff:ff:ff:ff   IEEE   Beacon frame
 29 0              :0e:43  ff:ff:ff:ff:ff:ff   IEEE   Beacon frame
 33 1              :0e:43  ff:ff:ff:ff:ff:ff   IEEE   Beacon frame
 35 1              :0e:43  ff:ff:ff:ff:ff:ff   IEEE   Beacon frame
 40 1              :0e:43  ff:ff:ff:ff:ff:ff   IEEE   Beacon frame
 43 1              :0e:43  ff:ff:ff:ff:ff:ff   IEEE   Beacon frame
 48 1              :0e:43  ff:ff:ff:ff:ff:ff   IEEE   Beacon frame
 52 1              :0e:43  ff:ff:ff:ff:ff:ff   IEEE   Beacon frame
 55 2              :0e:43  ff:ff:ff:ff:ff:ff   IEEE   Beacon frame
 56 2.             :0e:43  ff:ff:ff:ff:ff:ff   IEEE   Beacon frame
 60 2.414181 00:12:f0:b3:0e:43  ff:ff:ff:ff:ff:ff   IEEE   Beacon frame
 62 2.517466 00:12:f0:b3:0e:43  ff:ff:ff:ff:ff:ff   IEEE   Beacon frame
  4 0.262562 00:13:10:e7:f2:7f  ff:ff:ff:ff:ff:ff   IEEE   Beacon frame
  9 0.365192 00:13:10:e7:f2:7f  ff:ff:ff:ff:ff:ff   IEEE   Beacon frame
 12 0.467325 00:13:10:e7:f2:7f  ff:ff:ff:ff:ff:ff   IEEE   Beacon frame

▷ Frame 56 (83 bytes on wire, 83 bytes captured)
▽ IEEE 802.11
    Type/Subtype: Beacon frame (8)
  ▷ Frame Control: 0x0080 (Normal)
    Duration: 0
    Destination address: ff:ff:ff:ff:ff:ff (ff:ff:ff:ff:ff:ff)
    Source address: 00:12:f0:b3:0e:43 (00:12:f0:b3:0e:43)
    BSS Id: 02:12:f0:00:58:c6 (02:12:f0:00:58:c6)
    Fragment number: 0
    Sequence number: 38
▽ IEEE 802.11 wireless LAN management frame
  ▽ Fixed parameters (12 bytes)
      Timestamp: 0x00000000190195D9
      Beacon Interval: 0.102400 [Seconds]
    ▷ Capability Information: 0x0022

0000  80 00 00 00 ff ff ff ff  ff ff 00 12 f0 b3 0e 43   ........ .......C
0010  02 12 f0 00 58 c6 60 02  d9 95 01 19 00 00 00 00   ....X.`. ........
0020  64 00 22 00 00 0a 4d 4d  55 20 4d 65 6c 61 6b 61   d."...MM U Melaka
0030  01 04 82 84 8b 96 03 01  0a 06 02 00 00 dd 07 00   ........ ........
0040  50 f2 02 00 01 00 2a 01  00 32 08 0c 12 18 24 30   P.....*. .2....$0

Source Hardware Address (wlan.sa), | P: 64 D: 64 M: 0
```

Figure 6. Ethereal: Network packet analyzer



```
Network List—(SSID desc)                                                       Info
     Name                       T W Ch  Packts Flags IP Range       Size      Ntwrks
     rpint                      A Y 011     24       0.0.0.0          0B           9
   ! raiza                      A Y 006  20759       0.0.0.0          4k      Pckets
   ! dptp456                    A N 010   3437  A    0.0.0.0        613k       72194
   ! SIKULWL01                  A Y 006   2997       0.0.0.0          1M      Cryptd
   ! MMU Melaka                 H N 010  15116       0.0.0.0          0B        2762
     Lucent                     A Y 007      1       0.0.0.0          0B        Weak
   ! Friendster                 A Y 011  11527       0.0.0.0        120k           0
   ! ACC                        A Y 006    752       0.0.0.0          0B       Noise
 +   Probe Networks             G N ---     10       0.0.0.0          0B        1767
     <no ssid>                  A Y ---      1       0.0.0.0          0B      Discrd
                                                                               17558
                                                                              Pkts/s
                                                                                  30
Status
 ALERT: Suspicious client 00:12:F0:B3:0E:43 - probing networks but never participating.
 ALERT: Suspicious client 00:12:F0:B3:0E:43 - probing networks but never participating.
 ALERT: Suspicious client 00:12:F0:B3:0E:43 - probing networks but never participating.
 ALERT: Suspicious client 00:12:F0:B3:0E:43 - probing networks but never participating.
Battery: AC charging 70% 0h30m18s
```

Figure 7. Unnamed SSID

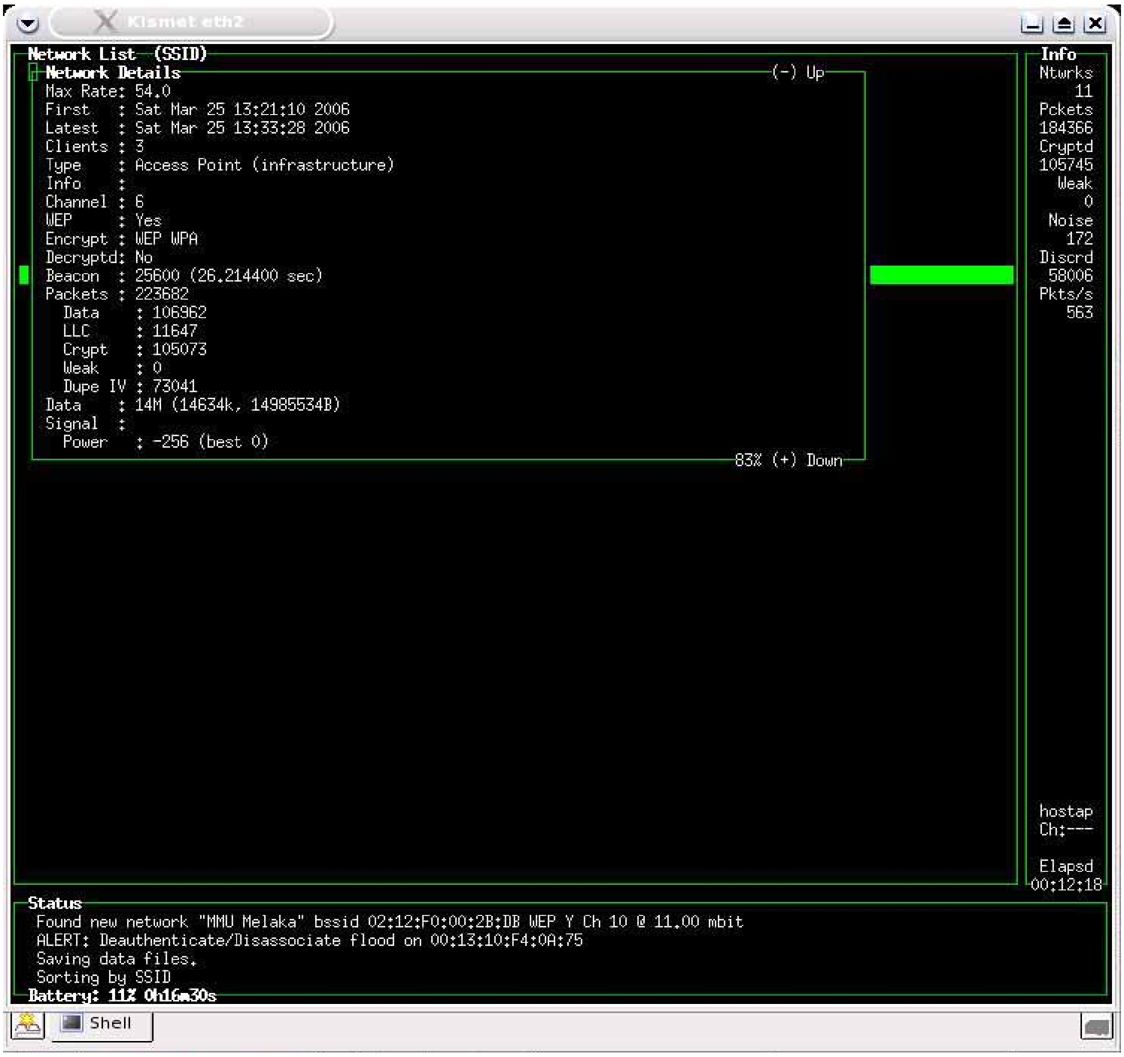
6. Wired Equivalent Privacy (WEP)

Wired Equivalent Privacy (WEP) is the privacy protocol specified in IEEE 802.11 to provide wireless LAN users protection against casual eavesdropping. [2]

Among the features of WEP are:

- Uses stream cipher RC4 for confidentiality
- Uses CRC-32 checksum for integrity
- Has 2 Key sizes: 40 bit and 104 bit + (24 bit) IV
- The same traffic key must never be used twice

To attack WEP, the authentication key will be sniffed by the attacker, and replay attack will be conducted to collect interesting initialization vectors (IVs) that will help to crack the WEP. The above Figure 8 shows that Linksys is able to withstand an attack on WEP as there were insufficient IVs that could be collected from the particular network. While, as stated in the following Figure 4, there were no weak IVs available in the network for collection to crack WEP (Weak: 0). Even if they are protected by WEP (which still remains the most common security counter measure on 802.11 LANs), the vulnerabilities of WEP are very well publicized and known to practically anyone with a minimal interest in wireless networking.



```
Network List (SSID)                                                          Info
 Network Details                                            (-) Up           Ntwrks
  Max Rate: 54.0                                                                 11
  First   : Sat Mar 25 13:21:10 2006                                         Pckets
  Latest  : Sat Mar 25 13:33:28 2006                                         184366
  Clients : 3                                                                Cryptd
  Type    : Access Point (infrastructure)                                    105745
  Info    :                                                                    Weak
  Channel : 6                                                                     0
  WEP     : Yes                                                               Noise
  Encrypt : WEP WPA                                                             172
  Decryptd: No                                                               Discrd
  Beacon  : 25600 (26.214400 sec)                                             58006
  Packets : 223682                                                           Pkts/s
    Data    : 106962                                                            563
    LLC     : 11647
    Crypt   : 105073
    Weak    : 0
    Dupe IV : 73041
  Data    : 14M (14634k, 14985534B)
  Signal  :
    Power   : -256 (best 0)
                                                        83% (+) Down

                                                                             hostap
                                                                             Ch:---

                                                                             Elapsd
                                                                           00:12:18
Status
 Found new network "MMU Melaka" bssid 02:12:F0:00:2B:DB WEP Y Ch 10 @ 11.00 mbit
 ALERT: Deauthenticate/Disassociate flood on 00:13:10:F4:0A:75
 Saving data files.
 Sorting by SSID
Battery: 11% 0h16m30s
```

Figure 8. Kismet Network List (SSID): Insufficient IVs

7. Conclusion

As previously stated before, it is suggested to secure wireless LANs with a layered approach, beginning with the physical layer. The importance of Layer 1 security should not be taken too lightly.

Good access points are a main factor to achieve decent security for the wireless network. We do not need expensive, high-end access points to stay secure, decently priced ones are usually adequate. Simple defensive methodologies should always be taken account into, such as SSID and protocol filtering.

Nonetheless, it is still important to continue implementing the correct methods for the other layers in the network to achieve the most secure and optimal wireless network.

References

[1] Kismet. *http://www.kismetwireless.net/*

[2] Wireless LAN Security Interoperability Lab: What’s Wrong With WEP?. *http://www.ilabs.interop.net/WLANSec/What_is_wrong_with_WEP-lv03.pdf*

[3] Jim Geier. 802.11 Beacons Revealed. *http://www.wi-fiplanet.com/tutorials/article.php/1492071*

[4] Remote-exploit.org. *http://www.remote-exploit.org/*

[5] Wen Chuan Hsieh, Chi Chun Lo, Jing Chi Lee & Li Tsung Huang, The Implementation of a Proactive Wireless Intrusion Detection System, IEEE 2004.

[6] Joe Scolamiero, Securing Your Wireless Access Point: What Do All Those Settings Mean Anyways, SANS Institute 2004.

[7] Cisco System Press, edited by Laura Chappell, Introduction to Cisco Router Configuration, Macmillan Technical Publishing, 1999