The International Journal Of Engineering And Science (IJES)
||Volume||2 ||Issue|| 4 ||Pages|| 11-21||2013||
ISSN(e): 2319 – 1813 ISSN(p): 2319 – 1805

# Attacks and Mitigations over Wireless Networks -Insecure Wireless World

Popuri Manoj Kumar
*Department of Electronics, JNTU Kakinada*

**--------------------------------------------------------Abstract---------------------------------------------------**
*Wireless Technology is increasingly being used by organizations to mediate social/business relationships and social/business transactions. Almost 70% of people are using the Wireless Networks for their online transactions or online shopping, But the problem was any one can easily compromise a wireless network and monitor the data that was transferring over that network. Here in this paper I would like to explain in detail about what are the different ways that the attacker use for compromising the wireless Networks and the Mitigations steps to take care by the user for not affected by the Attacker. This was the most Sevier problem because this wireless Networks are becoming as a part of our day to day life, So We have to Secure our Wireless World.*

***Keywords :*** *Aircrack-ng, Airmon-ng, Sniffing, WEP,WPA,WPA2, Wireshark, Web Scarab, WPA_Supplicant, Airbase-ng, EAP, PEAP.*

---------------------------------------------------------------------------------------------------------------------------------------

Date of Submission: 30 March2013 Date Of Publication: 25, April.2013

---------------------------------------------------------------------------------------------------------------------------------------

## I. INTRODUCTION

The Title Attacks and Mitigations Over Wireless Networks itself specifies My research paper deals with WLAN Security. Wireless Security is Important, As we know all of us are kind of one or more wireless devices these could be our laptops or mobile phones or our wireless keyboard and mouse, which are using internet over wireless and this is where there is a mass adoption and wireless pretty much becomes Ubiquitous. At the very same time these WIFI/WLAN are integrated in to practically all commonly used devices such as laptops, mobile phones and more embedded devices and more often these devices gives us a gateway to connect to Internet.

### 1.2 Challenges of Wireless Networks:

The Main Challenge of Wireless Network is, How to protect something we can't see/feel. And these is where there is a Wireless Network Around us But we can't see it or sense it.Another Big problem using wireless was it Extends Beyond Boundary Walls. Suppose A Company using Wireless Network It Extends to its parking lot/may be someone with a directional antenna sitting far away can able to access it. And also Because of Mobile clients. And it is also difficult to locate a Wireless Attacker because he does not have to be physically present over that network.This topic is a practical one so I will explain it by using the screenshots that was taken during my lab Experiments. And who wish to do this practically can setup there lab by following the below instructions:Install Backtrack as one of your virtual machine and brought one wireless card which can be able to sniff wireless packets over air.

## II. UNDERSTANDING THE BASICS OF WLANS

Before going into deep about Attacks and Mitigations Over Wireless Networks, We have to gain some basic understanding of what are WLANS and the Bands, channels and Sniffing[1].

### 2.1 INTRODUCTION TO IEEE 802.11

The 802.11 family consist of a series of half-duplex over-the-air modulation techniques that use the same basic protocol. The most popular are those defined by the 802.11b and 802.11g protocols, which are amendments to the original standard. 802.11-1997 was the first wireless networking standard, but 802.11a was the first widely accepted one, followed by 802.11b and 802.11g. 802.11n is a new multi-streaming modulation technique. Other standards in the family (c–f, h, j) are service amendments and extensions or corrections to the previous specifications.802.11b and 802.11g use the 2.4 GHz ISM band, operating in the United States under Part 15 of the US Federal Communications Commission Rules and Regulations. Because of this choice of frequency band, 802.11b and g equipment may occasionally suffer interference from microwave ovens, cordless telephones and Bluetooth devices. 802.11b and 802.11g control their interference and susceptibility to interference by using direct-sequence spread spectrum (DSSS) and orthogonal frequency-division multiplexing (OFDM) signaling methods, respectively. 802.11a uses the 5 GHz U-NII band, which, for much of the world, offers at least 23 non-overlapping channels rather than the 2.4 GHz ISM frequency band, where adjacent channels overlap - see list of WLAN channels. Better or worse performance with higher or lower frequencies (channels) may be realized, depending on the environment.

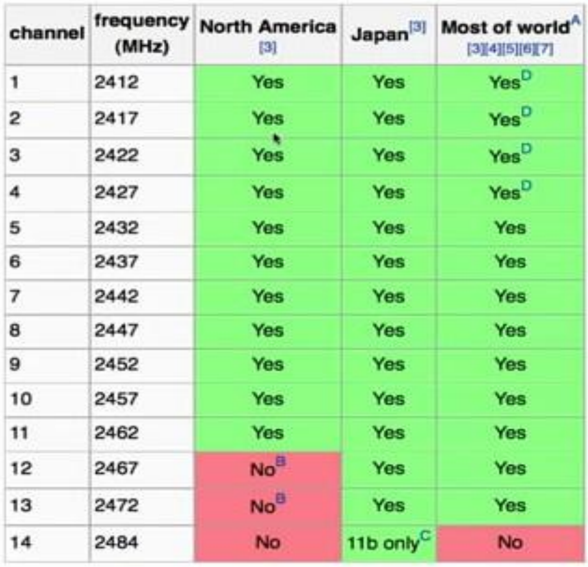
The segment of the radio frequency spectrum used by 802.11 varies between countries. In the US, 802.11a and 802.11g devices may be operated without a license, as allowed in Part 15 of the FCC Rules and Regulations. Frequencies used by channels one through six of 802.11b and 802.11g fall within the 2.4 GHz amateur radio band. Licensed amateur radio operators may operate 802.11b/g devices under Part 97 of the FCC Rules and Regulations, allowing increased power output but not commercial content or encryption[1].

## III. BANDS, CHANNELS, AND SNIFFING

Generally these WLANS operates in three different Frequency ranges

[1] 2.4GHz(802.11b/g/n)
[2] 3.6GHz(802.11y)
[3] 4.9/5.0GHz(802.11a/h/j/n)

Each of these ranges are divided into multiple channels, every country has allowed channels, users and maximum power levels.



| channel | frequency (MHz) | North America [3] | Japan[3] | Most of world[A] [3][4][5][6][7] |
|---|---|---|---|---|
| 1 | 2412 | Yes | Yes | Yes[D] |
| 2 | 2417 | Yes | Yes | Yes[D] |
| 3 | 2422 | Yes | Yes | Yes[D] |
| 4 | 2427 | Yes | Yes | Yes[D] |
| 5 | 2432 | Yes | Yes | Yes |
| 6 | 2437 | Yes | Yes | Yes |
| 7 | 2442 | Yes | Yes | Yes |
| 8 | 2447 | Yes | Yes | Yes |
| 9 | 2452 | Yes | Yes | Yes |
| 10 | 2457 | Yes | Yes | Yes |
| 11 | 2462 | Yes | Yes | Yes |
| 12 | 2467 | No[B] | Yes | Yes |
| 13 | 2472 | No[B] | Yes | Yes |
| 14 | 2484 | No | 11b only[C] | No |

Fig: sample list of 802.11b/g/n channels allowed in various countries.

**3.1 Understanding of Wireless Sniffing:** Generally we are aware of wired sniffing and the concept is very similar Akin to wired side "promiscuous" mode ,similarly in wireless we put our wireless device in monitor mode . There are couple of tools in Bt which will help us to put our device into monitor mode and i am using Aircrack-ng now.To understand this in detail We have to place our Wireless Card into monitor mode. Follow the commands to make the wireless card into monitor mode.

```
root@SecurityWizard:~#iwconfig
```

The above command show is our wireless card is connected to the machine or not.

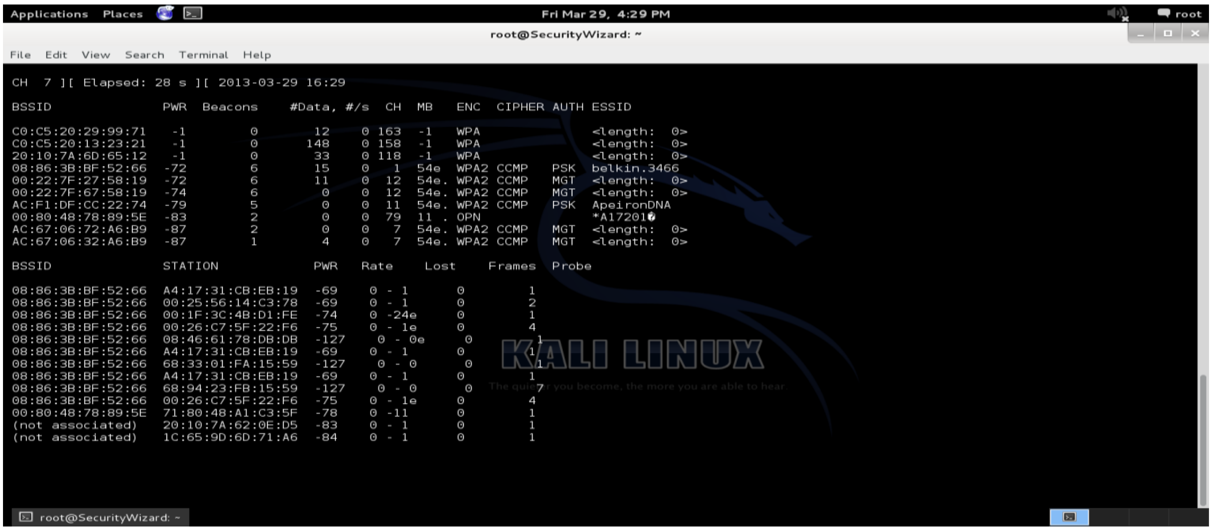
```
root@SecurityWizard:~#airmon-ng start wlan0
```

Airmon-ng is a Tool by Aircrack sweat of tools which creates a monitor mode for WLAN0(MON0), Now our Wireless card is in monitor mode and can able to sniff the data over Air. and our wireless card is only a single radio it would be on only one channel *at* a time.

But we can View the traffic of all the channels by using another tool Airodump from aircrack.

```
root@SecurityWizard:~#airodump-ng mon0
```

Makes MON0 to sniff among various channels.



```
CH  7 ][ Elapsed: 28 s ][ 2013-03-29 16:29

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

C0:C5:20:29:99:71   -1        0       12    0 163  -1   WPA              <length:  0>
C0:C5:20:13:23:21   -1        0      148    0 158  -1   WPA              <length:  0>
20:10:7A:6D:65:12   -1        0       33    0 118  -1   WPA              <length:  0>
08:86:3B:BF:52:66  -72        6       15    0   1  54e  WPA2 CCMP   PSK  belkin.3466
00:22:7F:27:58:19  -72        6       11    0  12  54e. WPA2 CCMP   MGT  <length:  0>
00:22:7F:67:58:19  -74        6        0    0  12  54e. WPA2 CCMP   MGT  <length:  0>
AC:F1:DF:CC:22:74  -79        5        0    0  11  54e. WPA2 CCMP   PSK  ApeironDNA
00:80:48:78:89:5E  -83        2        0    0  79  11 . OPN              *A17201�
AC:67:06:72:A6:B9  -87        2        0    0   7  54e. WPA2 CCMP   MGT  <length:  0>
AC:67:06:32:A6:B9  -87        1        4    0   7  54e. WPA2 CCMP   MGT  <length:  0>

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

08:86:3B:BF:52:66  A4:17:31:CB:EB:19  -69    0 - 1     0        1
08:86:3B:BF:52:66  00:25:56:14:C3:78  -69    0 - 1     0        2
08:86:3B:BF:52:66  00:1F:3C:4B:D1:FE  -74    0 -24e    0        1
08:86:3B:BF:52:66  00:26:C7:5F:22:F6  -75    0 - 1e    0        4
08:86:3B:BF:52:66  08:46:61:78:DB:DB  -127    0 - 0e    0        1
08:86:3B:BF:52:66  A4:17:31:CB:EB:19  -69    0 - 1     0        1
08:86:3B:BF:52:66  68:33:01:FA:15:59  -127    0 - 0     0        1
08:86:3B:BF:52:66  A4:17:31:CB:EB:19  -69    0 - 1     0        1
08:86:3B:BF:52:66  68:94:23:FB:15:59  -127    0 - 0     0        7
08:86:3B:BF:52:66  00:26:C7:5F:22:F6  -75    0 - 1e    0        4
00:80:48:78:89:5E  71:80:48:A1:C3:5F  -78    0 -11     0        1
(not associated)   20:10:7A:62:0E:D5  -83    0 - 1     0        1
(not associated)   1C:65:9D:6D:71:A6  -84    0 - 1     0        1
```

Fig: Displaying the Result of Airodump

Then Switch your wireshark and configure it to MON0, then we can capture the data over all channels and if we configure brupsuite, we can actually made a man-in-the-middle attack by changing the data as our wish.

## IV. WEP IN DEPTH

Before actually talking about WEP cracking I would like to describe you a little basics about WEP cracking. Here we discuss Wired Equivalent Privacy Encryption And how an Attacker take chance to exploit these WEP[2].

**4.1 Wired Equivalent Privacy** (**WEP**) is a security algorithm for IEEE 802.11 wireless networks. Introduced as part of the original 802.11 standard ratified in September 1999, its intention was to provide data confidentiality comparable to that of a traditional wired network. WEP, recognizable by the key of 10 or 26 hexadecimal digits, is widely in use and is often the first security choice presented to users by router configuration tools[2].And from the date IEEE proposed WEP Encryption, many researchers came with the vulnerabilities in WEP. And youtube contains a lot many videos about WEP cracking, But those are skit kiddy's how use those techniques. But still I don't know for whatever the reason the Access point manufacturers continue to ship it with WEP and still used by home users and some marts. Why marts was they use some scanning devices which has the less hardware capability and can only use WEP.

**4.2 Wep Encryption Schme:**

The WEP packet is in the following format[3].

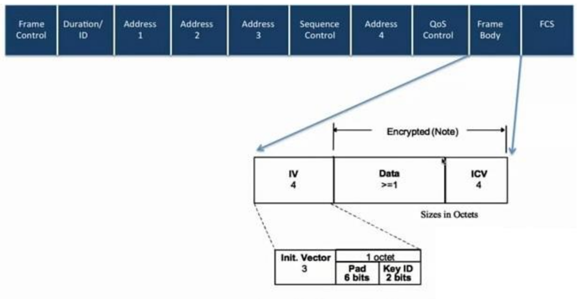


Fig: WEP Internals

Let me put it in perspective of Wireless LAN Packet. If we want to encrypt the Data with WEP. WEP is typically consider with Frame body.

Frame Body contains IV which is of 4bytes which is not encrypted and pretended with the data and ICV. The DATA is Encrypted using RC4 encryption Algorithm along with ICV which is Integrity Check.

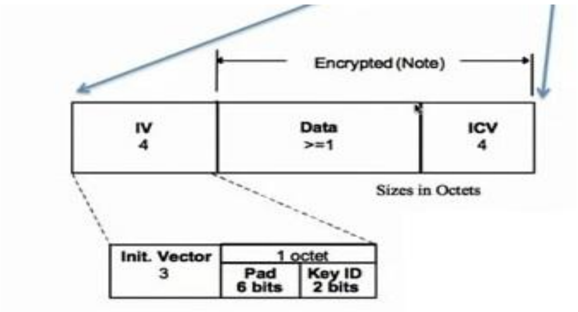


Fig: IV in Detail

The IV consists of Initialization Vector of 3 bytes and 6 bits of padding and 2 bits of key ID. IV is a Random 24 bit value and generated per packet basis. And the Access point pretends the WEP key of 40/104 bit to the IV. Which goes as input to RC4 Algorithm which generates a random key stream.

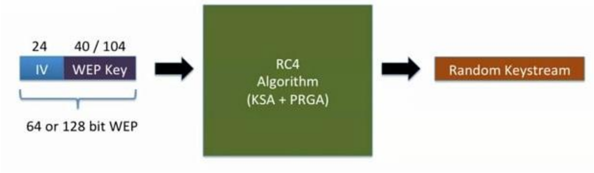


Fig: Generating the Key stream

The data is passed through the CRC32 algorithm which generates an ICV.

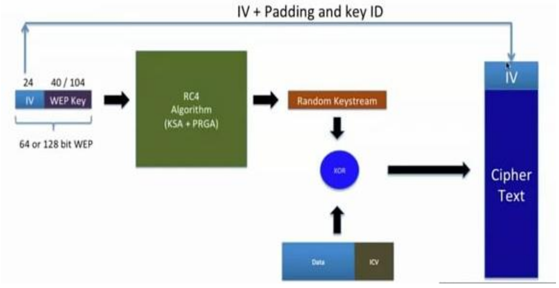


Fig: Encryption of WEP key

These Data along With ICV is XORED with the Random Keystream which can be converted to a Cipher Text. These cipher text is pretended with unencrypted IV and used as a KEY during Authentication.And one thing we have to observe from above description was the IV is not encrypted and can be generated per packet basis. And by collecting these IVS we can crack the WEP key because these IVs contains the WEP key. When we cracked the WEP key we can Decrypt all the encrypted data which leads to a most Sevier problem.

### 4.3 WEP Cracking:

Generally a lot many videos are there on youtude for WEP cracking, but here I we will use aircrack-ng. The Oldest one is finding "Weak IVs" which reveal Information About WEP Key. Once we can collect a large number of Weak IVs we can crack the WEP key. And these Weak IVs are not uniformly distributed in the IV space.

### 4.4 Techniques:

-Passive Way(Wait--Wait--Wait)

The Advantage of Passive way was it was Undetectable.Actually Using Directional Antenna one can monitor the data the flaw in wireless was any one can scilently monitor the packets over network. The disadvantage Was We have to Wait for Long time to Collect the IVs.-Active Way(Patience is Not your Virtue)Replay Attacks Which simulates the Network to send encrypted Data packets.

ARP Reply which sends ARP request and sends ARP Responces.

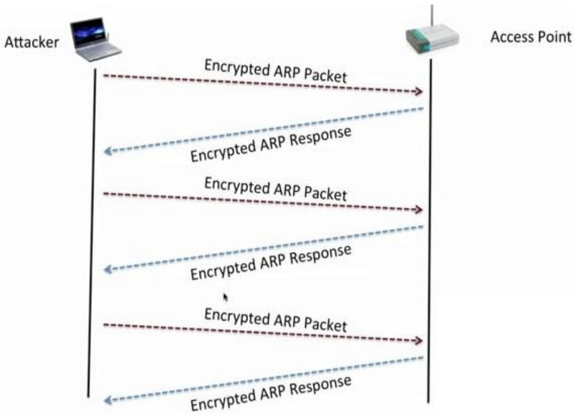
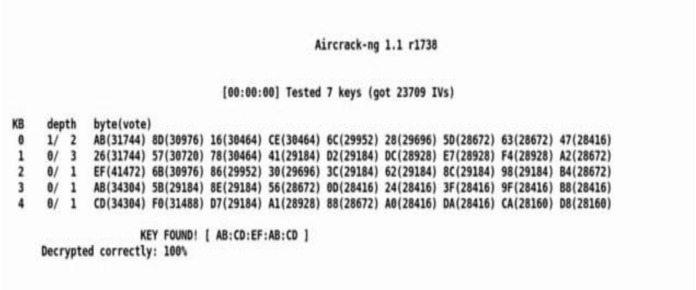


Fig: ARP Replay-Replay Packets to AP.

The First Step is Actually to spot the Wireless Networks over air using Airodump and then Save the IVs into a pcap file and by just running a aircrack on the pcap file of 30-45 thousand of IVs we can cracking.



```
                              Aircrack-ng 1.1 r1738


                   [00:00:00] Tested 7 keys (got 23709 IVs)

KB    depth   byte(vote)
 0    1/  2   AB(31744) 8D(30976) 16(30464) CE(30464) 6C(29952) 28(29696) 5D(28672) 63(28672) 47(28416)
 1    0/  3   26(31744) 57(30720) 78(30464) 41(29184) D2(29184) DC(28928) E7(28928) F4(28928) A2(28672)
 2    0/  1   EF(41472) 6B(30976) 86(29952) 30(29696) 3C(29184) 62(29184) 8C(29184) 98(29184) B4(28672)
 3    0/  1   AB(34304) 5B(29184) 8E(29184) 56(28672) 0D(28416) 24(28416) 3F(28416) 9F(28416) B8(28416)
 4    0/  1   CD(34304) F0(31488) D7(29184) A1(28928) 88(28672) A0(28416) DA(28416) CA(28160) D8(28160)

                  KEY FOUND! [ AB:CD:EF:AB:CD ]
    Decrypted correctly: 100%
```

Fig:Sample Output of Aircrack-ng

## V. CAFFE LATTE ATTACK:

In previous Discussion we cracked the WEP key using ARP Replay attack. These Caffe Latte Include the Message Injection Attack. The WEP has a Flaw That Message Modification And Injection, Now there was a paper Written very earlier called "Intercepting Mobile Communication-The Insecurity of 802.11" this paper includes several attacks over 802.11.

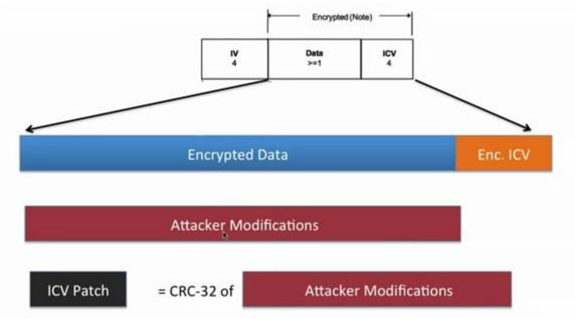


Fig: Creating Bit mask without knowing plain text.

Therefore using these Msg injection without knowing data we can create a Modified encrypted data and corresponding ICV.

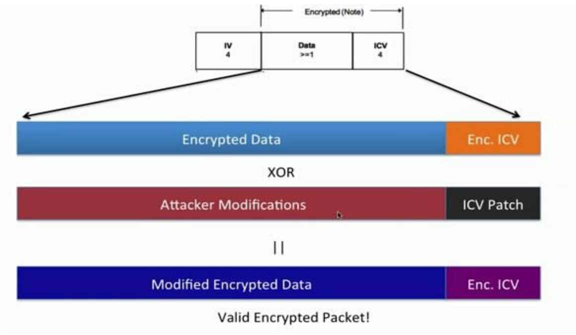


Fig: Patching A Valid Packet

By Performing the XOR operation between the Encrypted Data and Attacker Modifications we can get the Modified Encrypted Data and the Encrypted ICV, Which is used as a original data.

**5.1 Mitigations For Securing WEP:** Although the IEEE 802.11 standard upon which Wi-Fi wireless LAN networks are based addressed security somewhat with the Wired Equivalent Privacy (WEP) protocol in its first instantiation, WEP proved relatively easy to crack. Fortunately, the IEEE 802.11 group became aware of the issues with WEP early on and on June 24 of 2000 the IEEE Standards Association approved an amendment to the original IEEE 802.11 specification that addresses these issues. The culmination of three and a half years of work by the IEEE 802.11i Task Group, the amendment adds stronger encryption, authentication, and key management strategies that go a long way toward guaranteeing data and system security.

The IEEE 802.11i effort actually started with a task group intended to address both quality of service and security, namely IEEE 802.11e. However, it quickly became apparent that security needed special attention and so that group was split into IEEE 802.11e, which continues to work on quality of service, and IEEE 802.11i, which focused on security. The resulting IEEE 802.11i amendment has many components, the most obvious of which are the two new data-confidentiality protocols, TKIP and CCMP. IEEE 802.11i also uses IEEE 802.1X's key-distribution system to control access to the network.

## VI. WPA/WPA2

After the IEEE Came to Know that the WEP is Completely insecure, It was decided to design a strong encryption standard.

**6.1 Wi-Fi Protected Access:** IEEE 802.1xAuthentication Server- LEAP, EAP/TLS,PEAP or PSK(Pre- Shared Key). RC4 stream cipher with a 128 bit key and 48 bit initialization vector(IV). Temporary Key Integrity Protocol(TKIP). Message integrity protocol(MIC)[4].

**6.2 WPA-PSK:** In WPA-PSK a Pass phrase or a shared secret key is used. Pre shared key is generated by combining the Service set identifier with a passphrase(An ASCII string 8-63 characters). A passphrase less than 64 characters must be insecure. The management is handled on the Access point and this WPA-PSK is vulnerable to dictionary Attacks.

**6.3 Temporal Key Integrity Protocol(TKIP):**

Fixes Flaws of Key reuse in WEP-comprised of three parts, guarantees clients different keys.
-128 bit temporal key shared by clients and Access points.
-MAC of client
-48 bit IV Describes packet sequence number.

Increments the value of IV to Ensure Every Frame has a different Value. Changes temporal key for every 10,000 packets, uses RC4 like WEP if only Firmware upgrade required.

**6.4 Michael Message Integrity Check:** Message integrity check(MIC) is a 64 bit message calculated using "Micheal" algorithm inserted in TKIP packet to detect content alteration. Here the Message is concatenated with the secret key and the result is hashed, Which protects both the Data and Header. It Implements a Frame counter, Which discourages Replay Attacks.

The main drawback of WEP is it uses static keys for encrypting data. Where in WPA/WPA2 uses Dynamic keys.

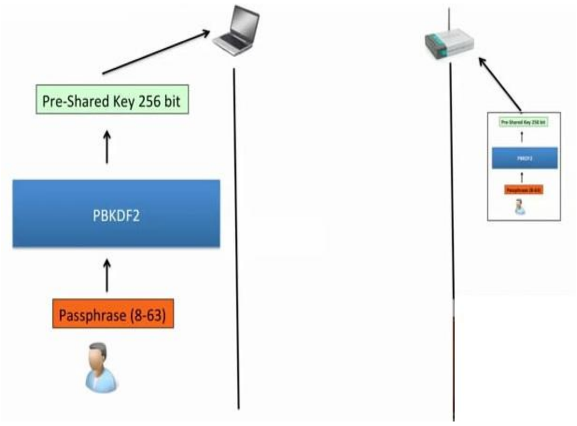


Fig: WPA Pre-Shared Key

Here the PBKDF2 is a Password Based key Derivation Function which uses RFC2898 algorithm. These PBKDF2 consists of Passphrase,SSIDssidlen,4096,256. Where 256 is the Integrity key length of PSK.

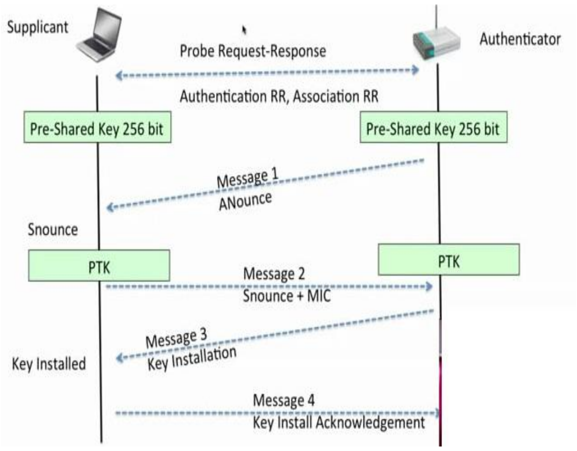


Fig: WPA/WPA2 $ way handshake

Here in WPA-PSK the Pre shared key present at both Supplicant and the Authenticator And the 4 way hand shake takes place by Transmitting the 4 messages among them. The first msg is the Anounce which is also known a Authenticator nounce, msg 2 consists of the Snounce and the MIC and finally after key installation Followed by Acknowledgement packet.

**6.5 WPA-PSK Cracking:** Here in WPA-PSK if We capture the Handshake with which we can able to crack WPA-PSK. Lets first examine how WPA-PSK works.

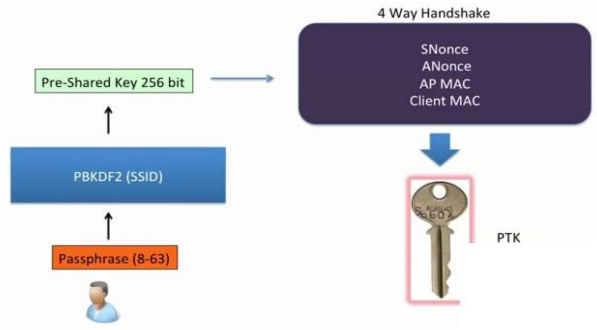


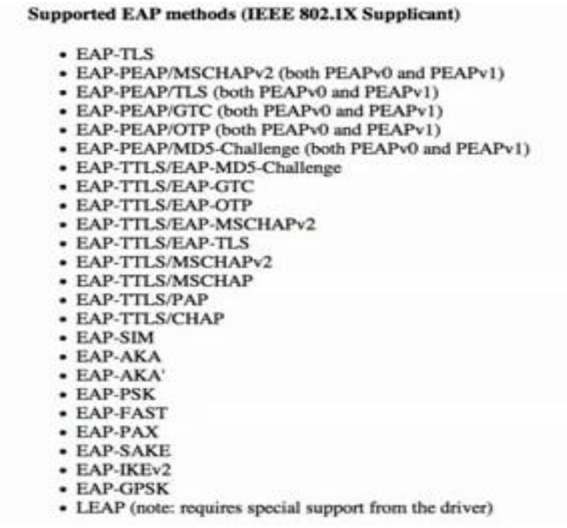
Fig: Block Diagram for 4 way handshake.

And know by simply capturing the Hand shake between the Access point and the client an attacker can able to perform a dictionary attack and crack the Key.

But this need a very high Database of passwords to crack WPA-PSK as Rainbow tables. And we can crack he WPA-PSK using either the 1,3 handshake packets or 2,4 handshake packets. Actually the Attacker can create a fake access point pointing to the same name that the client was authenticated know, and he then sends the deauth packets to the client and make the client connects to his fake access point , this was the type of attacks that was increasing rapidly now a days.

**6.6 WPA2-PSK Cracking:** Here for the WPA2-psk cracking the exactly same principals apply as WPA-PSK cracking, the only difference is that the signature based algorithm are different. The same four way handshake exists and we can crack the key by using the aircrack-ng[5].These Handshake is captured using airodump-ng and captured handshake is given to the aircrack-ng along with the rainbow table list of keys.Then it checks for all the possibilities and Replay back if any key matchs. These WPA/WPA2 Cracking was not as easy as WEP Cracking, But one with the rich set of rainbow tables can hack the WPA/WPA2 easily.

**6.7 WPA Supplicant:** WPA_Supplicant is the de-factoo tool, which is used to connect to network from the linux based kernals. These WPA_supplicant is a cross platform. And these WPA Supplicant is a Open source which specifies if you are a code hacker you can do lot of interesting stuff with WPA_Supplicant[6].



**Supported EAP methods (IEEE 802.1X Supplicant)**

- EAP-TLS
- EAP-PEAP/MSCHAPv2 (both PEAPv0 and PEAPv1)
- EAP-PEAP/TLS (both PEAPv0 and PEAPv1)
- EAP-PEAP/GTC (both PEAPv0 and PEAPv1)
- EAP-PEAP/OTP (both PEAPv0 and PEAPv1)
- EAP-PEAP/MD5-Challenge (both PEAPv0 and PEAPv1)
- EAP-TTLS/EAP-MD5-Challenge
- EAP-TTLS/EAP-GTC
- EAP-TTLS/EAP-OTP
- EAP-TTLS/EAP-MSCHAPv2
- EAP-TTLS/EAP-TLS
- EAP-TTLS/MSCHAPv2
- EAP-TTLS/MSCHAP
- EAP-TTLS/PAP
- EAP-TTLS/CHAP
- EAP-SIM
- EAP-AKA
- EAP-AKA'
- EAP-PSK
- EAP-FAST
- EAP-PAX
- EAP-SAKE
- EAP-IKEv2
- EAP-GPSK
- LEAP (note: requires special support from the driver)

Fig: Supported EAP Methods by WPA Supplicant.

These WPA_Supplicant configuration file requires one or more allowed networks.

## VII. MITIGATIONS FOR SECURING WPA/WPA2:

Don't use weak Passphrase. Check your network setting regularly, as your APs are saved into the computer the client always searches for the becon frames of the known networks, If it found one then connects to by supplying the credentials saved into it.So can easily know what are the access points that the client was searching for and can create the same, let it connect to it. Don't Add exceptions for not trusted certificates.

## VIII. EAP-MD5 BASICS

As in the WPA Enterprise these EAP consists of a Client, Access point and a Radius Server[7].

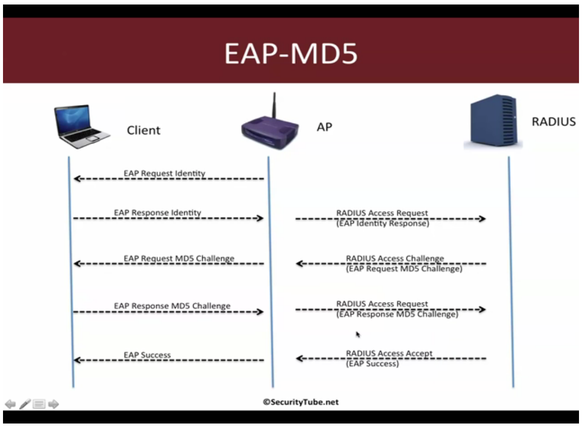

EAP-MD5
Client
AP
RADIUS
EAP Request Identity
EAP Response Identity
RADIUS Access Request (EAP Identity Response)
EAP Request MD5 Challenge
RADIUS Access Challenge (EAP Request MD5 Challenge)
EAP Response MD5 Challenge
RADIUS Access Request (EAP Response MD5 Challenge)
EAP Success
RADIUS Access Accept (EAP Success)
©SecurityTube.net

Fig: EAP-MD5 authentication

That the client is requested to EAP Identity and in response the clients send the response identity to the Ap Which intern send to the radius server, then the server requests for a MD5 Challenge in response the client sends the response md5 challenge, then the server verifies the challenge and send EAP Success to the Client.

**8.1 Setting up a Radius Server:** To Setup a Radius server, Add username/password in users file and make EAP-MD5 the default EAP in eap.conf. Ensure that the shared secret is correct for the AP-RADIUS Server in clients.conf. We can configure the Radius server in our virtual meachine for demo/practice purposes.

**8.2 CRACKING PEAP:** PEAP primarily works with the server side certificates, the problem here was it was easy to create a rouge radius server which creates fake certificates. Here the clients may not prompt/user may accept invalid certificates.

**8.3 Setting Up a Honeypot With FreeRadius-WPE:** The client connects to our FreeRadius-WPE and gives the Credentials of the server, Accept the Fake certificates and send authentication details over MSCHAPv2 in the TLS tunnel.The Attackers radius server logs these credentials and applies the dictionary attack to crack the challenge text.

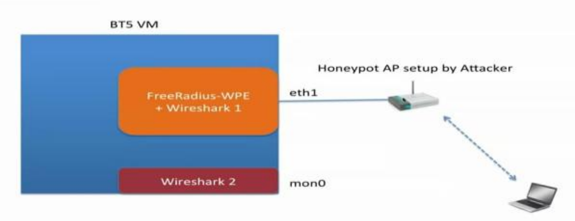
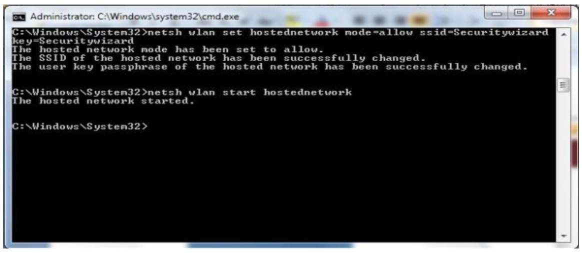


Fig : Network Architecture

But we as a security conscious persons when sees these fake certificates understands that it was fake server, but while considering the client he may think that he has to accept the fake certificate and adds these fake certificate to his list. And tries to Authenticate to the network. Here We use Airport tool to create a fake Honeypot for a freeradius server.

## IX. WIRELESS BACKDOORS WITH HOSTED NETWORKS

-Creating an access point on a client device, Till now we have created various access points on Unix system(Backtrack), using custom software HostAPd and Airbase-ng. Can't we create these access points on a Most used platform(Windows), Yes we can Using the Microsoft "Hosted Network" feature , Which is available on Windows 7 and server 2008 Onwards.With these Hosted Network feature, a windows computer can use a single physical wireless adapter to connect as a client to the hardware access point(AP), While at the same time acting as a software AP allowing other wireless capable devices to connect to it.The objective of this feature is to allow creation of wireless personal area network(PAN). And then do Internet connection sharing on all of the Wireless capable devices, known as Network connection sharing(ICS).



```
C:\Windows\System32>netsh wlan set hostednetwork mode=allow ssid=Securitywizard
key=Securitywizard
The hosted network mode has been set to allow.
The SSID of the hosted network has been successfully changed.
The user key passphrase of the hosted network has been successfully changed.


C:\Windows\System32>netsh wlan start hostednetwork
The hosted network started.


C:\Windows\System32>
```

Fig: Starting Hosted Network on Windows.

C:\Windows\System32>netsh wlan set hostednetwork mode=allow ssid=secrutiywizard key=securitywizard

[1] The hosted network mode has been set to allow.
[2] The SSID of the hosted network has been successfully changed.
[3] The user key passphrase of the hosted network has been successfully changed.

Then start the Hostednetwork, But in windows we can configure the access point on our won as open/WEP/WPA/WPA2 . It was set to WPA2 by default.But using this Hostednetwork there is no need of external Wireless card, we can use our wireless adapter for both as client and to create an access point.

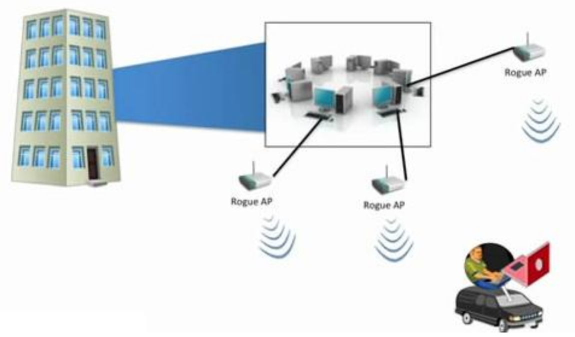


Fig: Rouge AP in a Enterprise Network.

Rouge Aps are the APs created by these hosted networks, this means every single windows 7 system can able to create a rouge AP. The threat level of these issue is more because if an malicious insider of an organization have created these rouge AP, by which the outside attacker can easily enter in to the Enterprise Network. And these rouge AP are the painful task for the Administrators. An attacker sitting in the parking lot can able to enter into the network using this rouge AP. Here the attacker has a chance to connect to victim over the wireless network which was created by the victim at some point of time. Victim will never notice anything unusual unless he visits his network settings. As the attacker is connecting to the victim over a private network, it was difficult to detect even the attack is going on. Abusing legitimate feature, not picked up by AVs, Anti Malware.Now by this Anyone with Windows 7 os can create a Wireless Backdoor without using any tools further.

Tips To Secure your Wireless World:

[1] Always disable your hosted Network.
[2] Check your Network settings Regularly
[3] Don't Connect to open APs.
[4] Don't commit any transactions over WEP.
[5] If you are Still using WEP u are in a big danger, Upgrade your firmware to WPA/WPA2.

Don't accept fake certificates, If the browser says that the certificate is not trusted simply get out of it and check your network settings.

## X. CONCLUSION

Here by I conclude that WEP,WPA/WPA2 Personal and Enterprise, PEAP, and EAP can be cracked. My Motive here is to make an awareness about how wireless can be cracked if we are not aware of it, but not to let u know how to crack the Wireless. So Make your Wireless world Much secure and don't make your organization or yourself to be the Backdoors for the Attackers.

However please be warned that the above methods are just to show the insecurity of Wireless and make you aware of it. Practicing these on a Private Network could be illegal.

## XI ACKNOLEDGEMENTS

I would like to thank my Professor Vivek Ramachandran, Freelancer, Wireless Security for giving me such an exposure to the Wireless Security and guiding me throughout my research.

## REFFERENCES

[1] Wireless LAN from Wikipedia
[2] http://en.wikipedia.org/wiki/Wireless_LAN
[3] Wired Equivalent Privacy by IEEE
[4] http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=5444462&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D5444462
[5] Wired Equivalent Privacy from Wikipedia
[6] http://en.wikipedia.org/wiki/Wired_Equivalent_Privacy
[7] Wi-Fi Protected Access from Wikipedia
[8] http://en.wikipedia.org/wiki/Wi-Fi_Protected_Access
[9] IEEE_802.11i-2004/WPA2
[10] http://en.wikipedia.org/wiki/IEEE_802.11i-2004
[11] WPA_Supplicant by epitest
[12] http://hostap.epitest.fi/wpa_supplicant/
[13] Extensible Authentication Protocol
[14] http://en.wikipedia.org/wiki/Extensible_Authentication_Protocol