Analytical Review of Security of Wireless Network

Anuradha Sharma 1, Amandeep Chouksey 2,

Amity School of engineering & Technology, Amity University, Lucknow Campus

ABSTRACT: The computers have become more and more sophisticated these days thus; it has become difficult to ensure security only by inspection and intuition . Standard methods of analyzing different aspects of the area have been developed; aiming to identify and apply key principles of the area. But the area of security analysis is constantly developing as new secure designs (and way of breaking into them) are invented. In many cases, systems are now so complex, and feature so much non-deterministic behavior that it is impossible to find an absolutely secure solution, and instead improvements to the problem and counter-measures to ensure security must be aimed at.

The wireless network or popularly known as Wi-Fi is used most widely to connect various devices over the network. The communication over the wireless networks requires delivery of packets from the source or the sender to the receiver. Though wireless networks have got a large number of advantages over other networks as its economical, feasible, mobile etc., they are prone to large number of attacks due to security issues with the wireless channels. This paper presents how easily and with not that much technical knowledge one can penetrate into a secured wireless network easily and can perform various kinds of attacks from spoofing there IP to steals packets that are travelling over the network . It's a matter of great concern as most of the institutes in any arena are using wireless networks to provide connectivity to there devices, hence it is extremely important to keep the data secure and to maintain the integrity and confidentiality of the data.

Index terms: Brute Force, Beacons, ESSID, BSSID, deauth, Channel

I. INTRODUCTION

1.1 BRIEF INTRODUCTION

So, what is the importance of learning security analytics?

Security analytics is a valuable in demand skill today, including penetration testing, information security as companies continue to advance online, they continue to need help with keeping their websites and online tools secure. The idea is that people and companies put websites online apps put tools online for the people to use that then can be exploited and taken down by hackers. If one is willing to be one of the white hat hackers or in general terms the good hackers he/she can help these companies and people find vulnerabilities in their websites, apps ,tools etc. and secure them before anyone else takes advantage of them and can get paid really well to do this.

Wireless Local Area Network also referred to as WLAN or Wi-Fi are widely used technology for communication. People use Wi-Fi at home, office, college , coffee shop, airports and many other places. Enterprises, college campuses, airports, home users are using wi-fi increasingly. Soon governments are deciding to cover complete cities, trains over wi-fi. Wi-Fi provides easiest way to connect different devices over wireless and to internet .Nowadays from home to enterprises networks are moving from wired to wireless network as ease of its use.

In wireless pentesting one should follow standard methodology to carry out the assessment. The methodology /standard will provide roadmap for your assessment. It may include following:

a. Identify targets for assessment.

b. Define timeline , process and plan.

c. Taking legal approval from client.

d. Conducting assessment and providing report to client .

II. PREREQUISITES

Curiosity is the first and the basic step in the field of security analysis. There are basically three prerequisites for security analysis which are as follows:

1.A linux based computer system .

2. A high speed internet connection .

3. A working wireless access card(all laptops after 2008 have an inbuilt wireless access card).

2.1Brute Force

Brute force password cracking attempts all possibilities of all the letters, number, special characters that might be combined for a password and attempts them. As you might expect, the more computing horsepower you have, the more successful you will be with this approach.

Although it might seem contrary to common sense, one often start by trying to brute force very short passwords. Although brute force of long passwords can be very time consuming (days or weeks), very short passwords can be brute forced in a matter of minutes.

One starts by trying to brute force passwords of six characters or less. Depending upon my hardware, this can usually be accomplished in a matter of minutes or hours. In many environments, this will yield at least a few passwords.

Number passwords are the easiest to crack. An 8-character numeric password only requires that we try 100 million possibilities, and even a 12-character number password only requires 1 trillion possibilities. With powerful hardware, we can do this with barely breaking a sweat.

2.2Aircrack-ng

Aircrack-ng is a wireless network security analytics suite that is complete in itself.

The areas of wireless security analytics on which this suite focuses are as follows:

- Monitoring: This area focuses on the capturing of packet and then exporting the data into text files or other suitable format files which could be further used and processed by the third party tools and applications.
- Attacking: This area focuses on the replaying of the attacks performed , the deauthentication done by the programmer , fake access points and many more through injection of packets.
- Testing: This area focuses on the Checking wireless cards of the various devices and driver capabilities that includes capturing and injection.
- Cracking: This area focuses on the cracking of the Wired Equivalent Privacy and Wireless Protected Access Pre Shared Key (both 1 and 2).

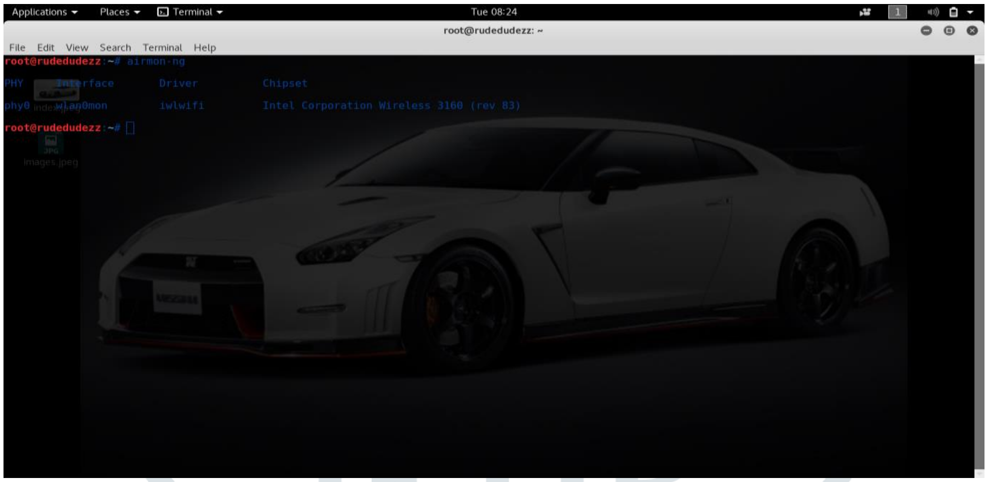
The tools that have been defined in this suite follows command line interface which allows the programmer to use heavy scripting techniques. It is this feature that has given many graphical user interfaces large number of advantages. This suite works mainly on the Linux environment as it is open source operating system but on the other hand this suite is also compatible to Windows Operating system , FreeBSD, OpenBSD, NetBSD, along with it in Solaris and even in the eComStation 2.

2.3Airmon-ng

Airmon-ng is one the first and foremost tool that is needed in almost each and every wireless hack, because it transforms the wireless access card of the device into a assorted mode wireless card which in turn enables the programmer to perform his attack.

When the wireless network card of the device is in the assorted mode, this means that the wireless network card can view and receive all the network traffic that is flowing over the wireless. In general, the wireless network cards of the devices will receive only those packets that are intended for that device (as ordained by the Media Access Control address of the Network Identity Card), but when a programmer is using the airmon-ng suite , the wireless network card will receive all the wireless traffic flowing in the wireless no matter whether the traffic is intended for that device or not.

This network analytics tool responds to the action with some sort of key information on the wireless adapter of the device that the programmer is working on which includes the chipset and the driver of the device . Along with it the most important aspect of this suite is that it has altered the state for the wireless adapter of the device used by the programmer to mon0 from wlan1.



```
root@rudedudezz:~# airmon-ng

PHY     Interface       Driver          Chipset

phy0    wlan0mon        iwlwifi         Intel Corporation Wireless 3160 (rev 83)

root@rudedudezz:~# 
```

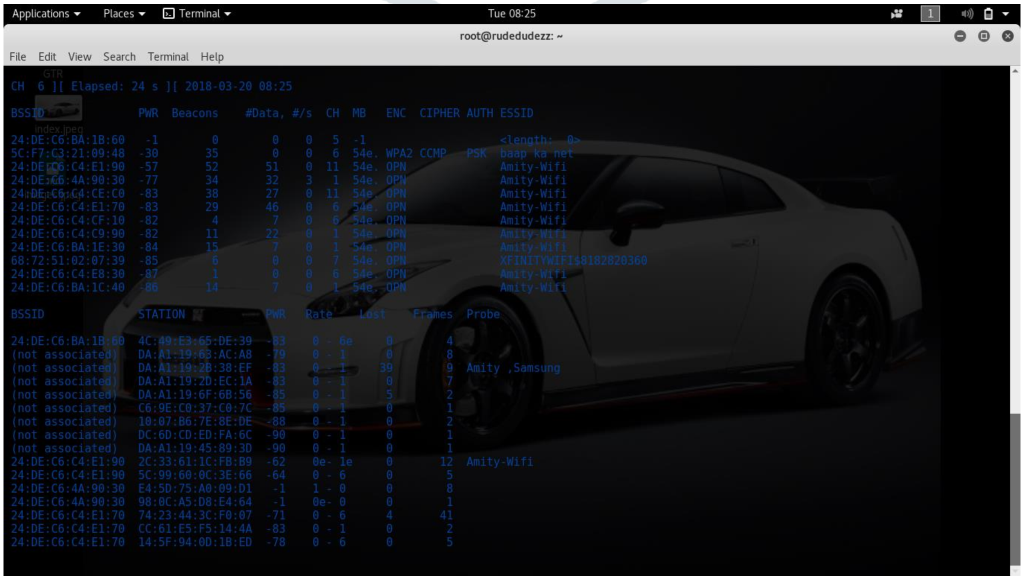
Initializing the monitor mode .

2.4Airodump-ng

Airodump-ng is yet another tool that is contained in this wireless network security analytics tool that is used by the coder to enable the device to capture the packets that are flowing in the wireless network and which are of the coders specification . This tool is extremely important and a very helpful in the cracking of the passwords.

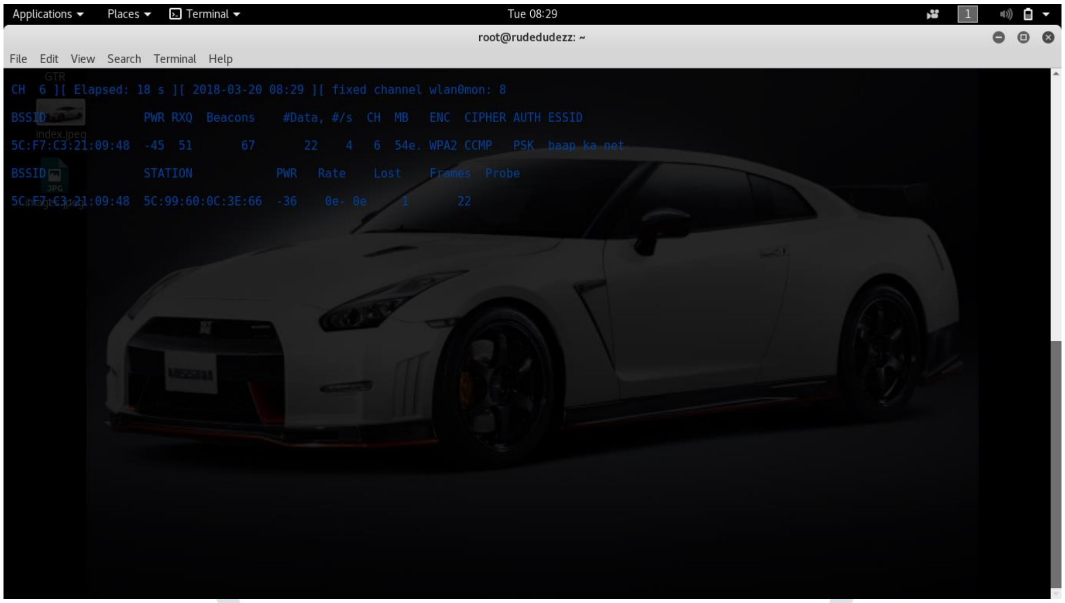
One can easily figure it out in the screenshot shown below , the airodump-ng tool shows all the access points that is the devices that are in the range of the coders device along with the basic service set identifier that is the media access control address , the strength of the access points , the exact number of the beacon frames , the total number of the data packets flowing in the wireless , the channel of the access point, the speed available for the flow of data between the devices , the type of encryption method used , the type of cipher method used, along with the authentication method used and the ESSID of the devices or the access points within the range of the chipset of the device of the programmer .

When the main motive of the coder if to hack a wireless network of , then the most essential and significant fields that are displayed by this command are basic service set identifier and the channel of the access point .



```
CH  6 ][ Elapsed: 24 s ][ 2018-03-20 08:25

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

24:DE:C6:BA:1B:60   -1        0        0    0   5  -1                    <length:  0>
5C:F7:C3:21:09:48  -30       35        0    0   6  54e. WPA2 CCMP   PSK  baap ka net
24:DE:C6:C4:E1:90  -57       52       51    0  11  54e. OPN              Amity-Wifi
24:DE:C6:4A:90:30  -77       34       32    3   1  54e. OPN              Amity-Wifi
24:DE:C6:C4:CE:C0  -83       38       27    0  11  54e. OPN              Amity-Wifi
24:DE:C6:C4:E1:70  -83       29       46    0   6  54e. OPN              Amity-Wifi
24:DE:C6:C4:CF:10  -82        4        7    0   6  54e. OPN              Amity-Wifi
24:DE:C6:C4:C9:90  -82       11       22    0   1  54e. OPN              Amity-Wifi
24:DE:C6:BA:1E:30  -84       15        7    0   1  54e. OPN              Amity-Wifi
68:72:51:02:07:39  -85        6        0    0   7  54e. OPN              XFINITYWIFI$8182820360
24:DE:C6:C4:E8:30  -87        1        0    0   6  54e. OPN              Amity-Wifi
24:DE:C6:BA:1C:40  -86       14        7    0   1  54e. OPN              Amity-Wifi

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

24:DE:C6:BA:1B:60  4C:49:E3:65:DE:39  -83    0 - 6e     0        4
(not associated)   DA:A1:19:63:AC:A8  -79    0 - 1      0        8
(not associated)   DA:A1:19:2B:38:EF  -83    0 - 1     39        9  Amity ,Samsung
(not associated)   DA:A1:19:2D:EC:1A  -83    0 - 1      0        7
(not associated)   DA:A1:19:6F:6B:56  -85    0 - 1      5        2
(not associated)   C6:9E:C0:37:C0:7C  -85    0 - 1      0        1
(not associated)   10:07:B6:7E:8E:DE  -88    0 - 1      0        2
(not associated)   DC:6D:CD:ED:FA:6C  -90    0 - 1      0        1
(not associated)   DA:A1:19:45:89:3D  -90    0 - 1      0        1
24:DE:C6:C4:E1:90  2C:33:61:1C:FB:B9  -62    0e- 1e     0       12  Amity-Wifi
24:DE:C6:C4:E1:90  5C:99:60:0C:3E:66  -64    0 - 6      0        5
24:DE:C6:4A:90:30  E4:5D:75:A0:09:D1   -1    1 - 0      0        8
24:DE:C6:4A:90:30  98:0C:A5:D8:E4:64   -1    0e- 0      0        1
24:DE:C6:C4:E1:70  74:23:44:3C:F0:07  -71    0 - 6      4       41
24:DE:C6:C4:E1:70  CC:61:E5:F5:14:4A  -83    0 - 1      0        2
24:DE:C6:C4:E1:70  14:5F:94:0D:1B:ED  -78    0 - 6      0        5
```

It displays the name of all the access points , there BSSID's , beacon frames , channel on which they are operating, speed , encryption method , there ESSID's .



```
CH  6 ][ Elapsed: 18 s ][ 2018-03-20 08:29 ][ fixed channel wlan0mon: 8

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

5C:F7:C3:21:09:48  -45  51       67       22    4   6  54e. WPA2 CCMP   PSK  baap ka net

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

5C:F7:C3:21:09:48  5C:99:60:0C:3E:66  -36    0e- 0e     1       22
```

Tracking the desired access point from those which are availabl .

2.5Aireplay-ng

Aireplay-ng is one of the most powerful tool in the aircrack-ng wireless cracking suite , as it can be utilized to generate, alternate or accelerate the traffic on the given access point . This wireless network security analytics tool is specially useful when the programmer is performing attacks as in a deauth attack which will bump all the everybody off the access point , Wireless Equivalent Privacy and Wireless Protected Access 2 password attacks , along with the Address Resolution Protocol injection and in the replay attacks .

This wireless network security analytics tool can have access to the packets mainly from the two sources:

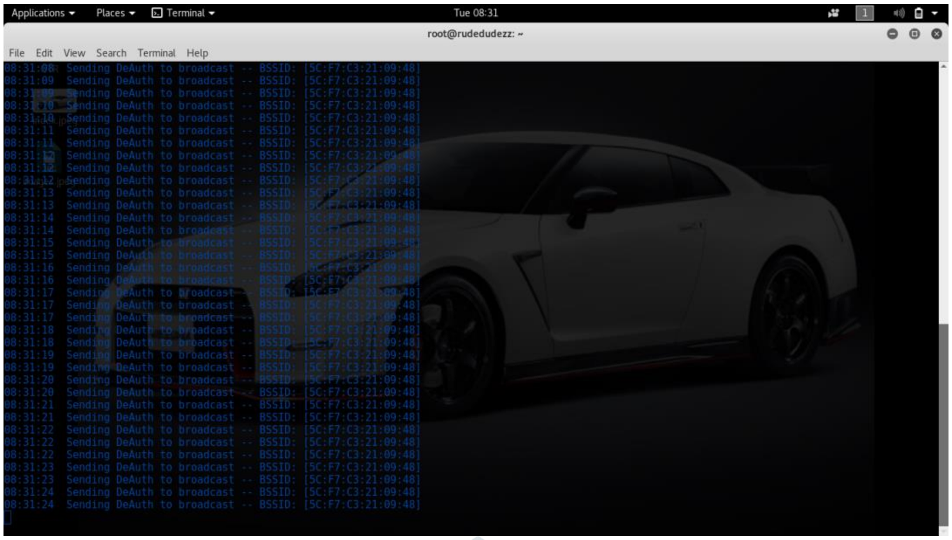
1. Packets from the live stream and ,
2. A pcap file that has already been captured .

A pcap file is basically a standard file type that is related with the tools that capture packet such as libpcap and winpcap .

An aireplay command from the airmon-ng suite used for wireless network security analytics can filter all the Basic Service Set Identifier of any of the specific access point, the Media Access Control address of both the source and the destination, the length of the packets both minimum and maximum etc. On the same hand the coder can also view few of attack options that exist for that access point using the aireplay-ng command .

These include deauth, fake deauth, interactive, arpreplay (necessary for fast WEP cracking), chopchop (a form of statistical technique for WEP packet decrypting without cracking the password), fragment, caffe latte (attacking the client side), and others .

These four tools in the aircrack-ng suite are our Wi-Fi hacking work horses . We'll use each of these in nearly every Wi-Fi hack . Some of our more hack-specific tools include airdecap-ng, airtun-ng, airolib-ng and airbase-ng .



```
08:31:08  Sending DeAuth to broadcast -- BSSID: [5C:F7:C3:21:09:48]
08:31:09  Sending DeAuth to broadcast -- BSSID: [5C:F7:C3:21:09:48]
08:31:09  Sending DeAuth to broadcast -- BSSID: [5C:F7:C3:21:09:48]
08:31:10  Sending DeAuth to broadcast -- BSSID: [5C:F7:C3:21:09:48]
08:31:10  Sending DeAuth to broadcast -- BSSID: [5C:F7:C3:21:09:48]
08:31:11  Sending DeAuth to broadcast -- BSSID: [5C:F7:C3:21:09:48]
08:31:11  Sending DeAuth to broadcast -- BSSID: [5C:F7:C3:21:09:48]
08:31:12  Sending DeAuth to broadcast -- BSSID: [5C:F7:C3:21:09:48]
08:31:12  Sending DeAuth to broadcast -- BSSID: [5C:F7:C3:21:09:48]
08:31:12  Sending DeAuth to broadcast -- BSSID: [5C:F7:C3:21:09:48]
08:31:13  Sending DeAuth to broadcast -- BSSID: [5C:F7:C3:21:09:48]
08:31:13  Sending DeAuth to broadcast -- BSSID: [5C:F7:C3:21:09:48]
08:31:14  Sending DeAuth to broadcast -- BSSID: [5C:F7:C3:21:09:48]
08:31:14  Sending DeAuth to broadcast -- BSSID: [5C:F7:C3:21:09:48]
08:31:15  Sending DeAuth to broadcast -- BSSID: [5C:F7:C3:21:09:48]
08:31:15  Sending DeAuth to broadcast -- BSSID: [5C:F7:C3:21:09:48]
08:31:16  Sending DeAuth to broadcast -- BSSID: [5C:F7:C3:21:09:48]
08:31:16  Sending DeAuth to broadcast -- BSSID: [5C:F7:C3:21:09:48]
08:31:17  Sending DeAuth to broadcast -- BSSID: [5C:F7:C3:21:09:48]
08:31:17  Sending DeAuth to broadcast -- BSSID: [5C:F7:C3:21:09:48]
08:31:17  Sending DeAuth to broadcast -- BSSID: [5C:F7:C3:21:09:48]
08:31:18  Sending DeAuth to broadcast -- BSSID: [5C:F7:C3:21:09:48]
08:31:18  Sending DeAuth to broadcast -- BSSID: [5C:F7:C3:21:09:48]
08:31:19  Sending DeAuth to broadcast -- BSSID: [5C:F7:C3:21:09:48]
08:31:19  Sending DeAuth to broadcast -- BSSID: [5C:F7:C3:21:09:48]
08:31:20  Sending DeAuth to broadcast -- BSSID: [5C:F7:C3:21:09:48]
08:31:20  Sending DeAuth to broadcast -- BSSID: [5C:F7:C3:21:09:48]
08:31:21  Sending DeAuth to broadcast -- BSSID: [5C:F7:C3:21:09:48]
08:31:21  Sending DeAuth to broadcast -- BSSID: [5C:F7:C3:21:09:48]
08:31:22  Sending DeAuth to broadcast -- BSSID: [5C:F7:C3:21:09:48]
08:31:22  Sending DeAuth to broadcast -- BSSID: [5C:F7:C3:21:09:48]
08:31:22  Sending DeAuth to broadcast -- BSSID: [5C:F7:C3:21:09:48]
08:31:23  Sending DeAuth to broadcast -- BSSID: [5C:F7:C3:21:09:48]
08:31:23  Sending DeAuth to broadcast -- BSSID: [5C:F7:C3:21:09:48]
08:31:24  Sending DeAuth to broadcast -- BSSID: [5C:F7:C3:21:09:48]
08:31:24  Sending DeAuth to broadcast -- BSSID: [5C:F7:C3:21:09:48]
```

Capturing the handshake in order to obtain the encrypted password .

2.6Aircrack-ng

Aircrack-ng is wireless network security analytics suite that is complete in itself . After obtaining the encrypted password in a file , the next step is to run this file over the aircrack-ng using any password directory or file of our choice . The time duration to successfully obtain the password depends on a number of factors such as **-** the length of the password , size of the password file etc.

When the password matches with that present in the file then it is displayed on the screen . The soul efficiency of this attack totally depends on the efficiency of the password file that has been used and the performance of the device that is being used for the attack .

III. CONCLUSION

Adaptable has wind up being basic bit of our life. Their present change is the aftereffect of diverse flexible periods. This paper presents how easily and with not that much technical knowledge one can penetrate into a secured wireless network easily and can perform various kinds of attacks from spoofing there IP to steals packets that are travelling over the network . The best and the most easiest way to avoid such attacks is to make a 32 bit password and keep on changing regularly, as it would take more than a month for the brute force mechanism to rack the password. Along with it, it should keep a track of the regular deauthentication and authenticationn of a connected device over the network. The most effective of all would be to keep a complicated password and not to share it with anyone who seems to be vulnerable .For greater security over the network one can create a strong router pin and also can set MAC filtering over the network.

REFERENCES

1. Flickenger, R. *Wireless Hacks*. Cambridge, Massachusetts: O'Reilly; 2003.
2. Vladimirov, A.A., Gavrilenko, K.V., and Mikhailovsky, A.A. *Wi-Foo: The Secrets of Wireless Hacking*. Reading, Massachusetts: Addison-Wesley Professional; 2004.
3. Arbaugh, W.A., An Inductive Chosen Plaintext Attack Against WEP/WEP2, Submission to the IEEE-802.11. doc# IEEE 802.11-01/230.
4. Bellardo, J. and Savage , 802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions, , S. Proceedings of the USENIX Security Symposium,
5. Fluhrer, S., Mantin, I., and Shamir, Weaknesses in the Key Scheduling Algorithm of RC4, A. In Proc. 8th Workshop on Selected Areas in Cryptography. LNCS 2259.
6. Stubblefield, A., Ioannidis, J., and Rubin , Using the Fluhrer, Mantin, and Shamir Attack to Break WEP, Revision 2, , A.D. AT&T Labs. www.uninett.no/wlan/download/wep_attack.pdf. August 21, 2001.
7. Walker, J., Unsafe at Any Key Size: An Analysis of the WEP Encapsulation, IEEE doc# 802.11-00/362. October 2000.
8. Aboda, B., Blunk, L., Vollbrecht, J., Carlson, J., and Levkowetz, H. IETF., **RFC 3748,** Extensible Authentication Protocol (EAP), ftp://ftp.rfc-editor.org/in-notes/rfc3748.txt. June 2004.
9. Wi-Fi Protected Access: Strong, standards-based, interoperable security for today's Wi-Fi networks, www.wi-fi.org/membersonly/getfile.asp?f=Whitepaper_Wi-Fi_Security4-29-03.pdf. Wi-Fi Alliance. April 2003.
10. "Deploying Wi-Fi Protected Access (WPA™) and WPA2™ in the Enterprise." www.wi-fi.org/membersonly/getfile.asp?f=WFA_02_27_05_WPA_WPA2_White_Paper.pdf. Wi-Fi Alliance. March 2005.
11. Anuradha Sharma, Puneet Misra, A Security Framework for e-business applications, International Journal of computer Applications, ISSN: 0975 – 8887) Volume 102– No.7, September 2014