WLAN Security Flaw: Cracking 64 bit WEP Key

Anil Kumar Singh[1], Bharat Mishra[2] and Sandeep Singh[3]

[1] Jagran Institute of Management,
Kanpur- 208014 (India)

[2]MGCGV, Chitrakoot
Satna (M.P.) India

[3]Jagran Institute of Management,
Kanpur-208014 (India)

Abstract

We put on display an active attack on the WEP protocol that is able to recover a 64-bit WEP key using 5000 capture packets with a success probability of 90%. In order to succeed 100% in all cases, more than 5000 packets are needed. The IV of these packets can be randomly chosen. This is an improvement in the number of required frames by more than an order of level over the best known key-recovery attacks for WEP.

In this paper we demonstrate the security flaws of Wireless LAN by cracking 64 bit WEP key on Wi-Fi access points using Backtrack, a live Linux distribution. We attack the Wi-Fi AP, making it generate packets for our cracking effort, finally cracking the WEP key successfully.

Key words - WLAN, Wi-Fi, MAC address, radio waves, WEP Key, Access Point and IV.

Introduction

Wired Equivalent Privacy (WEP) is used to keep wireless connections secure from sniffing attacks. You've probably heard that it's not very secure. It is a protocol for encrypting wirelessly transmitted packets on IEEE802.11networks. In a WEP protected network, all data packets are encrypted using the stream cipher RC4 under a common key, the root key [1]. The root key is shared by all radio stations [2][1]. A successful recovery of this Key gives an attacker full access to the network.

WEP is a part of the IEEE802.11 wireless standard ratified in 1999 [3]. It was designed to provide confidentiality on wireless communications by using RC4. In order to simplify the key setup, WEP uses preinstalled fixed keys. The first analysis of the WEP standard was done in 2001 by Borisov, Goldberg and Wagnerin [4]. They demonstrated major

security flaws revealing that WEP does not provide confidentiality, integrity and Access control.

Material and methods

The research was carried out to reveal WLAN Security Flaw: Cracking 64 bit WEP Key.

The work was conducted at Department of Information Technology, Jagran Institute of Management, affiliated to GBT University, Uttar Pradesh. Details of materials used and the procedures employed are as follows:

We can design a scenario after understanding the theory of WEP cracking. We have taken the cracking software Back Track 3.0 [5]. Hardwares picked for the purpose were: HCL Desktop, Compaq Laptops, AP (D-Link 3200 Series Access Point) and Wireless card (D-Link DWA 510); and softwares picked were: Operating System (Windows XP) and other application softwares. A client is used to communicate with Access Point while User Datagram Protocol (UDP) flooding is used to send data. Another client is used to keep track of the network traffic as a hacker and listens to the WLAN. AP is linked to LAN with wires. Figure 1 is the illustration of the WEP cracking job.

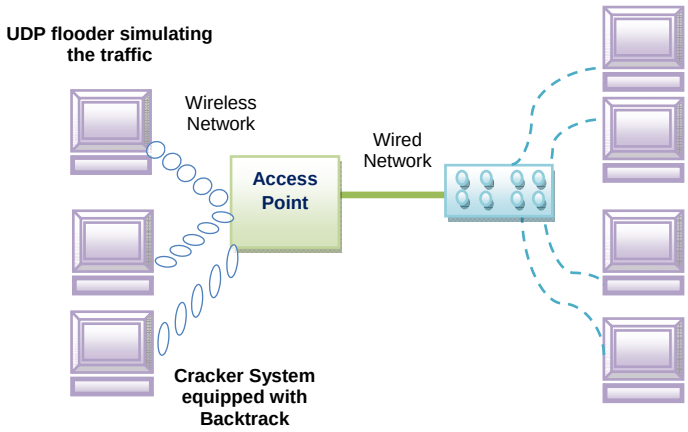

Figure - 1 WEP gears cracking lab setup

After booting with Back Track CD we open the console window and we find out the Wireless Network Interface Card (WNIC).

bt ~ # airmon-ng

MAC-Media Access Control address provided by the manufacturer at the time of manufacturing. It is a unique 48 bit, hexadecimal form, hardware address of WNIC. We here change the MAC address of WNIC. Before changing the MAC address it should be noticed that WNIC should be down.

bt ~ # ifconfig wlan0 down

bt ~ #macchanger –mac 00:11:22:33:44:55 wlan0

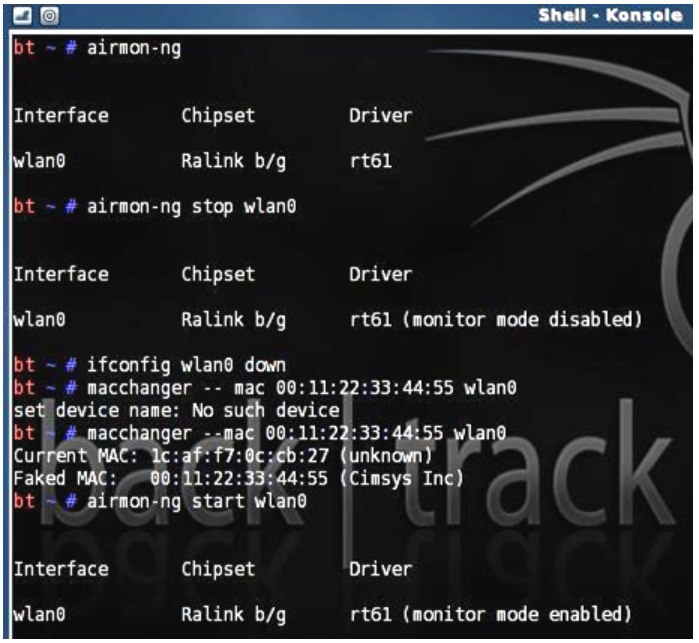

Figure – 2 showing the fake MAC address

bt ~ #airmon-ng start wlan0

Find out the Access Point and their MAC addresses, Data, Channel, Speed in MB, Encryption, Cipher, Authentication and ESSID. We type the following command in console window.

bt ~ #airodump-ng wlan0

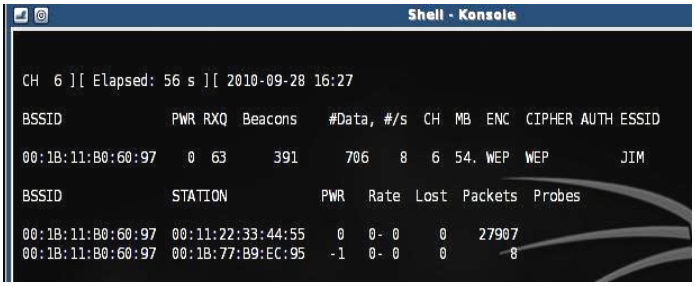

Figure – 3 showing the MAC of AP, their Channel No. Speed, Encryption, Cipher and ESSID

bt ~ # airodump-ng -c <channel No.> -w [pokemon] --bssid <MAC address of the Access Point>

After execution of the above command, the output data which will be stored in the file pokemon; you can put any name of the file as you wish. This file will be offered for the WEP Crack program when we are ready to crack the WEP key. Open another shell and put down the previous command running. Now we need to generate some fake packets to the access point to speed up the data output. Test the access point by issuing the following command:

bt ~ #aireplay-ng -1 0 -a <MAC address of the AP> -h <Fake MAC address of the WLAN> WLAN0

If the above command is successfully executed, then we will have to generate many packets on the target network so that we can crack the WEP Key.

bt ~ #aireplay-ng -3 -b <MAC address of the AP> -h <Fake MAC address of the WLAN> WLAN0

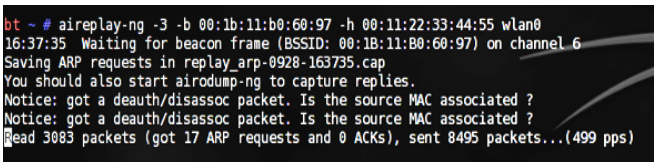

Figure – 4 showing the speed of capturing packets

It will force the Access Point to send out a bunch of packets which we can then use to crack the WEP key.

After about capturing the 5000-10000 IVs We start cracking the WEP key by typing the following:

aireplay-ng -b <MAC address of the Access Point> pokemon-01.cap [6].

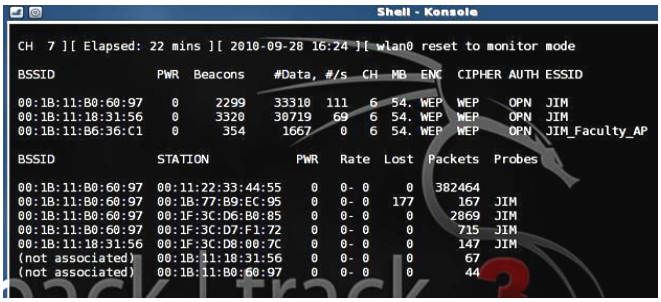

Figure – 5 showing the associated AP

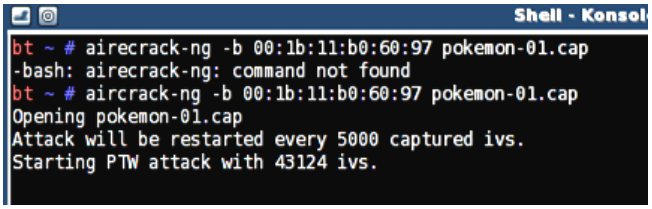

Figure - 6 showing the attack with IVs

Figure – 7 showing the decrypted WEP key

Experimental Results

The number of remarkable packets capturing is normally distributed l as shown in Figure 3. First, the capturing number will increase and then it will decrease as time passes.

When D-link DWL-3200 series AP as AP (Center Point) and D-Link DWA 550 Series Client as client, it will generate 5000-43124 repeat IV Packets in 2-3 minutes. And Back Track can crack WEP key successfully every time within 30-40 seconds.

The results of this experiment shows: First, the cracking will become easier if the number of IVs generated is more.

Secondly, the experiment paves way for the security up gradation of D-Link AP (Wireless device).

Conclusion

WLANs are largely used in education, healthcare, financial industries, and various public places such as airline lounges, coffee shops, and libraries. Although the technology has been standardized for many years, providing wireless network security has become a critical area of concern. Due to the broadcast nature of the wireless communication, it becomes easy for an attacker to capture wireless communication or to disturb the normal operation of the network by injecting additional traffic.

Security is of ultimate importance to the global communication and information networks. The data, which are encrypted with WEP Key, are also insecure [7]. WLAN is also prone to an authorized intervention by hackers because of its weakness analysed above.

References

1. **Tews Erik et. al.** ,Breaking104 bit WEP in less than 60 seconds, TU Darmstadt, FB Informatik Hochschulstrasse 10, 64289 Darmstadt, Germany.
2. **Shaheen Jaleel et. al. (2007),** Confidential and secure broadcast in wireless sensor networks, The18th Annual IEEE International Symposium on Personal, Indoor and Mobile Radio Communications.
3. **IEEE:** ANSI/IEEE standard802.11b: Wireless LAN Medium Access Control, (MAC) and Physical Layer (phy) Specifications (1999).
4. **N. Borisov et. al. (2001) -** Intercepting mobile communications the Insecurity of 802.11. In MOBICOM.180–189.
5. **Download backtrack 3.0** by http://www.topsofts.com/linux/download/236/247/109317/backtrack.html
6. **Maz , 19 Aug.** Tutorial: Cracking WEP Using Backtrack 3
7. **Ye Peisong, and Yue Guangxue (2010),** Security Research on WEP of WLAN, Proceedings of the Second International Symposium on Networking and Network Security (ISNNS ’10) p.p. 039-042

Anil Kumar Singh, MCA – Asst. Professor, Jagran Institute of Management, Kanpur. Currently pursuing the Doctoral programme in WLAN Security Vulnerability Threats and Alternative S*olution*.
at MGCV Satna (M.P.)

Dr. Bharat Mishra, Ph.D., Dept of Physical Science. MGCGV Satna (M.P.)

Sandeep Singh, PGDCA, Dept. of Information technology, Jagran Institute of Management, Kanpur.