Experimental Analysis of WLAN Security Weakness By Cracking 64 & 128 bit WEP Key

التحليل التجريبي لضعف امن الشبكات اللاسلكية المحلية بواسطة كسر مفتاح ٦٤ & ١٢٨ بت للـ(WEP)

Ali M. Alsahlany
Al-Najaf Technical College,
Foundation of Technical Education

Experimental Analysis of WLAN Security Weakness By Cracking 64 & 128 bit WEP Key

التحليل التجريبي لضعف امن الشبكات اللاسلكية المحلية بواسطة كسر مفتاح ٦٤ & ١٢٨ بت للـ(WEP)

Ali M. Alsahlany
Al-Najaf Technical College,
Foundation of Technical Education

Abstract:-

-The IEEE-802.11 encryption technique Wired Equivalent Privacy (WEP) is still widespread used today despite the numerous discussions on its insecurity. This paper demonstrates the security flaws of WLAN by cracking 64, and 128 bit WEP key. A simple practical technique used for real time decryption of data packets after attack on WLAN access point, which gives an attacker opportunity for full access to the network is presented.

I. Introduction

During the recent years, the Wireless Local Area Networks (WLANs) are experiencing a vast popularity and widespread deployment; the security evaluation of these networks is becoming more significant. Security risks in wireless networks are introduced as a result of the portability of wireless devices [1].To reduce these risks, IEEE in collaboration with many organizations worked on development various encryption standards which lower such risks to a manageable level.

One of the encryption standards widely used for encrypting wirelessly transmitted packets on WLAN is Wired Equivalent Privacy (WEP). In a WEP protected network, all packets are encrypted using the stream cipher RC4 under a common key, the

root key. The root key is shared between access point and a wireless station [2, 3]. Eavesdropping on encrypted traffics between an access point and a wireless station gives an attacker opportunity for recovery this key, then full access to the network and encrypted confidential information.

There are numerous researches have discussed flaws and weaknesses of WEP [2 - 4]. They have shown possibility attacks and recover WEP key analytically.

In practice, the real network attack after capturing enough encrypted data worked in Ref [5, 6].They have been demonstrated that the attack are reported only for a cracking 64 bit WEP Key.

In this paper, an active attack on the WEP protocol to recover a 64 and 128 bit WEP key using less than 50,000 distinctive IV packets is performed practically.

The rest of this paper is outlined as follows. Section II describes the WEP operation within the context of WLAN. Hardware and software used in the attacking process given in section III. Section IV presents the experimental details i.e. the measurement setup and procedure. Results and discussion are presented in section V. Finally the conclusions are drawn to section VI.

II. Wired Equivalent Privacy (WEP) Operation

WEP is the security protocol in use since the earlyIEEE802.11 standard. It is based on a stream cipher encryptionalgorithm called "RC4"[٧]. WEP is used to control access tothe WLAN and to encryptconfidential information.Fig. 1 illustrates the process of encryption. At first, the secret key used in WEP algorithm and a 24-bit initialization vector (IV) are concatenated as the encryption/decryption key. Secondly, the resulting key acts as the seed to generate the key sequence. Then, plain text

message, along with its ICV, is combined with key sequence. After a bitwise XOR process, we get the cipher text. A final encrypted frame is made by attaching the IV in front of the cipher text.

The decrypting process is the reverse process of theencrypting process. Firstly, the receiver generates key sequenceby shared key and IV. Then, the initial plaintext can beresumed by XOR operation between the key sequence and thecipher text. Next, data integrity is checked. The plaintext goesto Integrity Algorithm to make a new ICV (ICV') and finallywe should compare the ICV' and ICV to determine the dataintegrity.

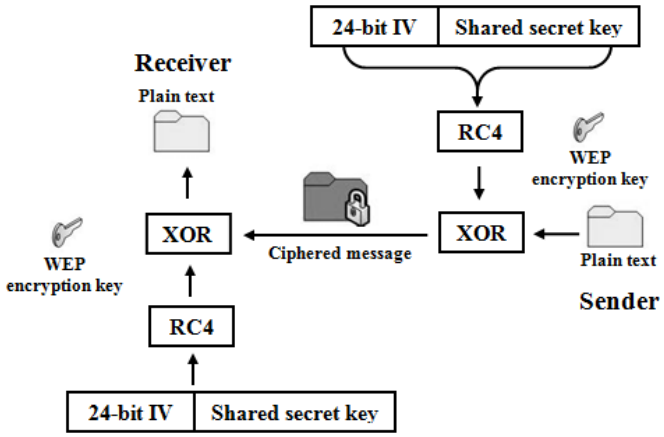

Fig. 1: Schematics of the WEP protocol used to control access to the WLAN and to encrypt confidential information.

III. Hardware/Software Used in the Attacking

The equipments used in this evaluation are:

1. Router:

- TP-LINK TL-WR941ND Wireless N300 Home Router.

2. Wireless LAN card:

- (D-Link DWA 135)

- 802.11b/g/n compatible.

3. Dell Desktop with a Windows 7 operating system installed in it.

- Intel Pentium, Dual CPU 1.8GHz with 1GB RAM.

4. Dell Laptop with a Linux - Wifiway operating system [8] (Wifiway version 3.4) installed in it.

- Dell Vostro 1540, Intel (R) 2.4GHz with 3GBRAM.

Application softwares that will be mentioned later in this paper can be found preinstalled in the operating system. A desktop is used to communicate with Router to ensure continue packet exchange. The laptop is used to sniff the network traffic as an Attacker. The router is linked to WAN port with 1 Gbit/Sec Ethernet wires. Fig. 2 is the illustration of the WEP cracking job.

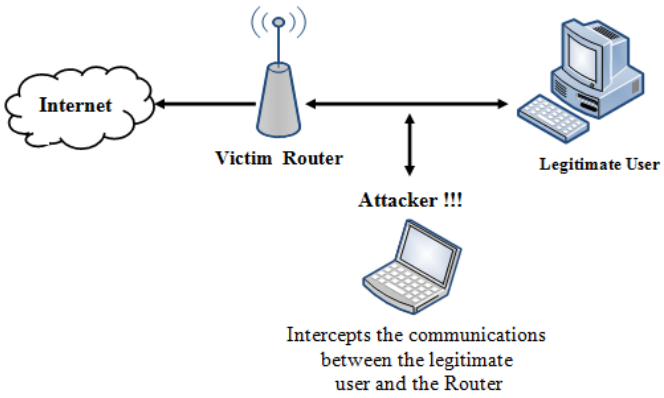

Fig. 2: Illustration of a Wired Equivalent Privacy (WEP) weakness. The attacker can monitor encrypted transmissions and captures IVs,lookup the corresponding WEP key and easily decrypts the transmitted data.

IV. Experimental Procedures for a WEP-Cracking

At Desktop computer, open the Internet explorer and type the IP of the router 192.168.1.1 in the address bar and press enter,

click on wireless tab, wireless setting; Router will display the following window, write the SSID address as shown in Fig. 3- a, and b.

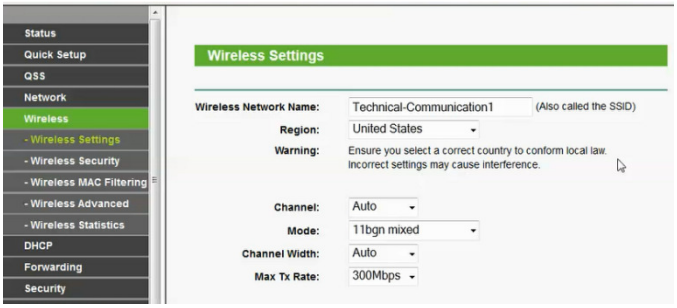

Fig. 3-a: Define SSID address asTechnical-Communication1 for WEP key 128 bit.

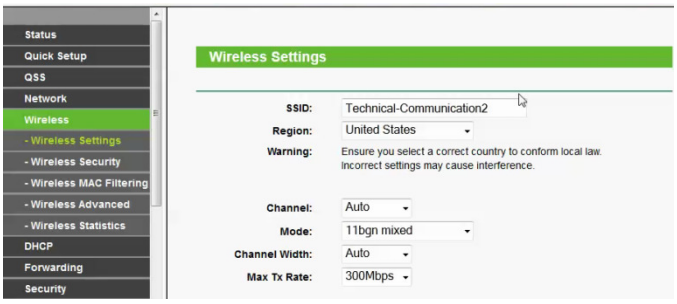

Fig. 3-b: Define SSID address as Technical-Communication2 for WEP key 64 bit.

Click on the wireless security tab, write the WEP key of legitimate users.

Fig. 4-a: Configuration WEP key as 128 bit (i.e. 13 ASCII characters 6AYC}3Z] U>f} u) for Technical-Communication1 network.

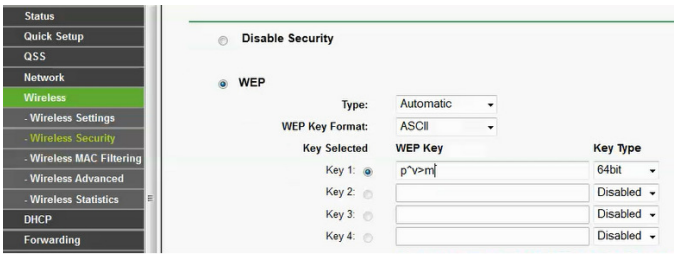

Fig. 4-b: Configuration WEP key as 64 bit (i.e. 5 ASCII characters p^v>m) forTechnical-Communication2 network.

Now going to access the WLAN which SSID address is displayed above.

At Laptop computer, after booting with Wifiway operating system, open the terminal window of Airoscript Viejo program and make scanning for an available wireless network by selecting the first command of terminal window as shown in Fig. 5. After scanning process the available Routers and their MAC addresses , Data, Channel, Speed in MB, Encryption, Cipher, Authentication and ESSID will display.

Fig. 5: Showing the main terminal window of Airoscript Viejo program.

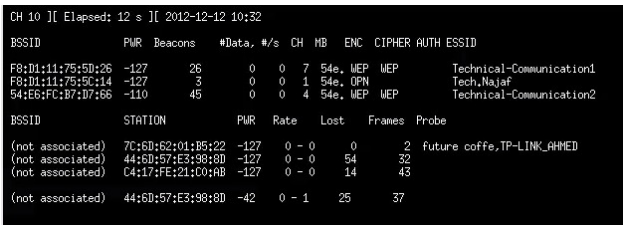

Fig. 6: Showing the MAC of AP, their Channel No. Speed, Encryption, Cipher and ESSID

Select the objective network **(i.e. Technical-Communication1 for WEP key 128 bit, and Technical-Communication2 for WEP key 64 bit one by one)** by return to the main terminal window and selected the second command.

Now we need to generate some fake packets to the router to speed up the data output. Test the router by issuing the third command of terminal window. The attack process forobjective network is begin after choosing attack commands. If the above commands are successfully executed, then we will have to generate many packets on the target network so that we can crack the WEP Key.

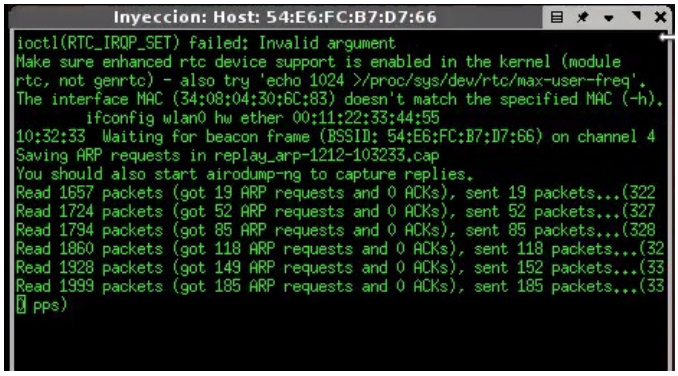

Fig. 7: Showing the speed of capturing packets.

It will force the Router to send out a bunch of packets, which can then use to crack the WEP key.

Cracking the WEP key after capturing the 5000 – 10000 IVs can be starting by select the cracking command.

Fig. 8-a: Showing the decrypted 128 bit WEP key.

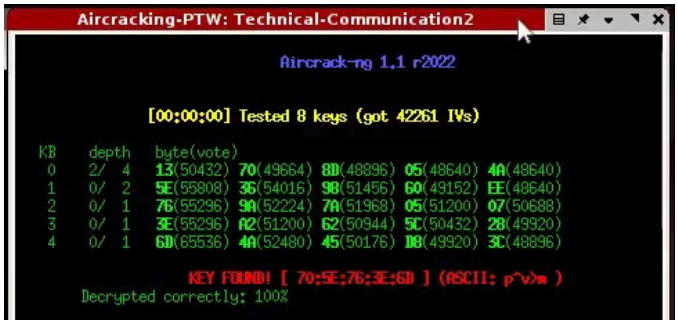

Fig. 8-b : Showing the decrypted 64 bit WEP key.

V. Experimental Results

The experiment presented in the previous section is used to emphasize that the WEP at any key size is an exposed encryption and shouldn't be the used to secure WLAN.

When TP-LINK TL-WR941ND Series as Router (Center Point) and D-Link DWA 135 Series Client as a client, it will generate 5000 - 74233 distinctive Packets in 2-3 minutes. And Wifiway can crack WEP key successfully every time within less than 40 second.

The number of distinctive IV packets capturing is normally distributedas shown in Fig. 7. The capturing number will increase as time passes. The cracking will become easier if the number of IVs generated is more.

Figure 8-a, and b demonstrate an active attack on the WEP protocol thatis able to recover a 64 and 128 bit WEP key using less than 50,000 frames with asuccess probability of 100%.

VI. Conclusions

WLANs being the most spread technology over the world is vulnerable to the threats of hacking. It is very important to protect a network from the hackers in order to prevent exploitation of confidential data. Based on experimental results, the current implementation of WEP has proven to be flawed. Suggestions for improvement and tighten security of WLAN

changing static WEP to the latest wireless encryption suit such as enterprise WPA2, or combination of enabling WEP key and MAC address filter security mechanism.

الخلاصة:ـ

التحليل التجريبي لضعف امن الشبكات اللاسلكية المحلية بواسطة كسر مفتاح ٦٤ & ١٢٨ بت للـ(WEP)

تقنية التشفير (WEP) لا تزال واسعة الاستخدام اليوم على الرغم من مناقشات عديدة بشأن انعدام الأمن فيها. هذا البحث يوضح ثغرات الأمن للشبكات ألاسلكية المحلية عن طريق كسر مفتاح ٦٤ & ١٢٨ بت للـ(WEP)، استخدمت تقنية عملية بسيطة لفك تشفير واقعي وحقيقي لرزم البيانات بعد الهجوم على نقطة الوصول للشبكة اللاسلكية المحلية المستهدفة والتي تعطي المهاجم الفرصة للوصول الكامل إلى الشبكة.

REFERENCES

[1]Ahmed M. Al Naamany , Ali Al Shidhani, HadjBourdoucen, "IEEE 802.11 Wireless LAN Security Overview," *IJCSNS International Journal of Computer Science and Network Security*, Vol.6, No.5B, pp. 138-155, May 2006.

[2] E. Tews, R. P. Weinmann and A. Pyshkin, "Breaking 104 bit WEP in lessthan 60 seconds," IACR Eprint Server, http://eprint.iacr.org/ 2007/120.pdf , number 2007/120, Accessed April 1, 2007.

[3] Lazar Stošić, Milena Bogdanović," RC4 stream cipher and possible attacks on WEP," *(IJACSA) International Journal of Advanced Computer Science and Applications*, Vol. 3, No. 3, pp. 110-114, 2012.

[4] Anil Kumar Singh, Bharat Mishra and Sandeep Singh "WLAN Security Flaw: Cracking 64 bit WEP Key," *IJCSI International Journal of Computer Science* Issues, Vol. 7, Issue 6, pp. 296-299, Nov. 2010.

[5] A. Bittau, M. Handley, and J. Lackey, "The final nail in WEP's coffin," In IEEE Symposium on Security and Privacy", pp. 386-400, IEEE Computer Society, 2006.

[6] S Vinjosh Reddy, "Wireless Hacking - A WiFi Hack By Cracking WEP," *Proceedings of the 2nd International Conference on Education Technology and Computer (ICETC),* pp 189-193, IEEE, 2006.

[7]Ying Wang, Zhigang Jin and Ximan Zhao, "Practical Defence against WEP and WPA-PSK Attack for WLAN," *Proceedings of the 6th International Conference on Wireless Communications Networking and Mobile Computing (WiCOM)*, IEEE, 2010.

[8] http://www.wifiway.softonic.com/linux.