ISBN 978-981-11-0008-6
Proceedings of 2016 6th International Workshop on Computer Science and Engineering (WCSE 2016)
Tokyo, Japan, 17-19 June, 2016, pp. 256-260
doi: 10.18178/wcse.2016.06.040

The Research on Attacks and Protections of WLAN Based on Wired Equivalent Privacy (WEP)

Feng Yuan [1], Shang Zhihui [1], Zhang Jianwei [2 +], Cai Zengyu [1] and Ma Linlin [1]

[1] School of Computer and Communication Engineering, Zhengzhou University of Light Industry, Zhengzhou 450002, China

[2] Software Engineering College, Zhengzhou University of Light Industry, Zhengzhou 450002, China

Abstract. Firstly this paper summarizes the defects of Wireless Local Area Network (WLAN) based on Wired Equivalent Privacy(WEP), such as the problem of access security, hardware device lost, security defects of access control mechanism and password cracking. Then it discusses the attacks methods to WEP mechanism. On this basis, the password cracking method of WLAN based on WEP is described, include the principle of cracking, the environment of cracking and the steps of cracking the passwords of WEP. At last, the security solutions from the physical, technological and management aspects for WLAN based on WEP is presented. Our research can give advantage for using WLAN securely.

Keywords: WLAN, WEP, security, password crack.

1. Introduction

With the rapid popularization of WLAN, its security risk is causing more and more attention of people [1]. WEP is the part of the IEEE 802.11 standard through in September 1999, which prevents unauthorized users wiretapping wireless network information by encrypting the data between two devices and mainly provides access control and data encryption mechanism, allowing users holding correct WEP key to have access to networks and decrypt data flow. But due to the problem on design, there are many kinds of safety defects about WEP [2]-[6], which caused the attention of researchers. In this paper, we proposed the security and protection program of WLAN based on WEP on the basis of security of WLAN based on WEP, in order to provide references for building secure WLAN based on WEP.

2. Analysis of the Safety Defects of WLAN Based on WEP

2.1. Analysis of the Defects of WLAN Based on WEP Mechanism

False access point: IEEE802.11b shared key authentication table using one-way authentication, rather than mutual authentication. Access point need to authenticate the user, but the user cannot identify the access point. If a fake access point is placed within the wireless LAN, it can hijack legitimate user's client adapter or a denial of service attack.

Security issue of Hardware device lost: Statically assigned WEP key is usually stored in the card's non-volatile memory, so when the card is lost or stolen, the user can take advantage of this illegal unauthorized access to the network card.

The security defects of access control mechanism: Closed network access control mechanism: Management information includes the network name or SSID, and the message is the access point and the user broadcast in the network, does not have any obstacles.

[+] Corresponding author. Tel.: + 86-37186609559.
E-mail address: mailfengy@163.com.

Ethernet MAC address access control list: The MAC address is easy for an attacker to sniff. If activated the WEP, MAC address must also be exposed. And most of the wireless network card can use software to change the MAC address.

2.2. Method of Attack Against WEP Mechanism

The attack method of WEP mechanism can be divided into two categories, one is independent of RC4 attack, the other is related to RC4 attack. Associated with RC4 attack is mainly aimed at WEP environment or class of RC4 WEP environment. The target of the attack is to obtain the key, not just for the pseudo random sequence. The main attack way including PTW [3] \ FMS attack [4], KoreK attack [5] and Klein first round attack [6].

Has nothing to do with the RC4 attack has the following four categories: (1) Packet injection attacks. The attacker to capture WEP network packets, and replay after a period of time, to realize injection attacks. (2)Authentication attack. An attacker would have to capture the mobile station (STA) and control the access point(AP) between the authentication data exchange package, construct new legal certification. (3)Chopchop attack. The attack using WEP weakness in the process of to check with CRC - 32. (4)Piecewise attack. The attacker was encrypted with m long pseudo random sequence, the segmentation of the data can send a length of 16(M-4) data load, and then obtain the long 16m-60m encryption using pseudo random sequence. Since IEEE802.11 allows up to 2304 Byte load, most applications are limited to a load of 1500 Byte. Attacker sends 34 fragment, can get 1504 Byte long encrypted with a pseudo random sequence. Because the AP will replace the IV value, segmented attack, so the attacker can establish a IV dictionary, pseudo random sequence corresponding to different IV.

3. The Cracking of Passwords of Wireless LAN Based on WEP

The attacks on wireless networks in general can be divided into two categories: one kind of attack is related to the network access control, protection of data confidentiality and data integrity, such as traffic analysis, passive eavesdropping and active eavesdropping, unauthorized access, session interception and replay attack and so on. This kind of attack can occur in a wired network environment. The other kind of attack is based on the wireless communication network design, deployment and the unique way of maintenance, such as the detection of AP, the cracking of WEP, the breakthrough of limits of AP, the forging of base station, wireless phishing etc. The security of wireless network is on the basis of traditional cable network having added new security threats. This paper mainly focused on the research of the cracking solutions of secret key of WLAN based on WEP.

The Back Track 4, shorted as "BT4, is a portable Linux environment system,which can be started by being put in the U disk or CD, having no impact on the hard disk itself, no needing of the local installation, a good packaged Linux operating system, being internally installed a large number of network safety detection tools and hacker decoding software, etc. This paper conducted the practice of the cracking of the passwords of Wireless LAN based on WEP by using the Back Track 4.

3.1. The Principle of Cracking

The cracking of WEP is generally conducted by Airodump - ng tool collecting a large number of data packets produced by legitimate online clients and then using Aircrack - ng tools to crack, but the cracking is based on that there are target AP having active client connection. If there is no client or no client on the Internet, then it will be unable to collect enough iV data packets, and then cannot crack the password. Of course, passwords can also be cracked without clients by the attacks of Chopchop,Fragment and ARP+Deauth. But these processes are relatively complicated.

3.2. The Environment of Cracking

The testing environment consists of a TD-W89541G wireless routers of TP-LINK and two personal computers with wireless network card. The wireless network card is Intel WiFi Link 5100AGN. The attacker is installed Intel WiFi Link 5100AGN. The topology structure is showed in Fig. 1. With the continuous correspondence of the communication computer and WIFI routers, the attacker can gain the passwords of WEP by performing attack steps.

3.3. The Steps of Cracking the Passwords of WEP

(1) To restart the computer after putting the Backtrack 4 Linux system disk into the disk drive and then enter the BackTrack4 system desktop;

(2) Open the network function: input the order "/etc/init.d/NetworkManager start" in the shell window;

(3) Activate the wireless card as the pattern of monitor: input the order "airmon-ng start wlan0 6";

(4) Scanning the wireless Ap by Airodump-ng tool: input the order "airodump-ng --ivs -w wep -c 6 mon0";

(5) After gaining enough data packets, and using "Aircrack -ng"for synchronous cracking, it can crack the passwords of WEP in a certain period of time.

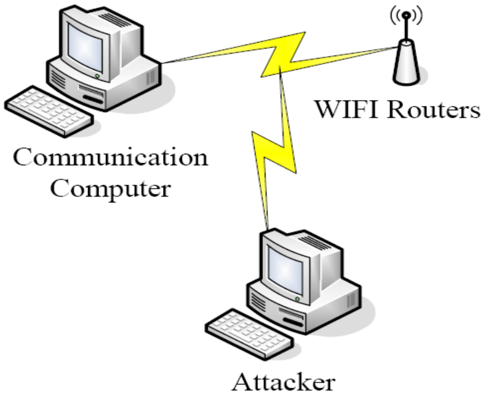

Fig. 1: Topology graph of testing attacks on WEP.

3.4. The Results of Testing

By many times of cracking tests through the use of the WEP password of different length of the secret Key and different bit length of key, for different length of the password, we can get the required time to obtain a WEP password. It is shown in Table 1. As we can see, the degree of security of WEP is low, even though the complicate WEP password also cannot defense the cracking attack. According to this, we can know that the degree of security of WEP is low. However, there are still a lot of people holding the ingrained misconceptions: 1. they think that the degree of security can be increased by high bits of password. 2. a complicated WEP password can ensure the safety of the wireless communication. 3. Attacks can be avoided by setting special character on the SSID of AP.

Table 1: The Test Results of WEP

Test of WEP	Key bit length	Length of password	password	Time of cracking (second)
The first time	64bit	5	67890	12
The second time	64bit	5	hezfn	10
The third time	128bit	13	hezfnhechmust	78
The forth time	128bit	13	Ha,ha.123#456	113
The fifth time	128bit	13	JaKG*#@Mn/s89	87
The sixth time	152bit	16	cjchrkercoecjrrt	41

4. Security and Protection Program of Wireless LAN Based on WEP

According to the analysis, we designed the Security and protection program of Wireless LAN based on WEP. This program mainly includes the protection of technology and management. The technical protection is referred to introduce more advance technology, overcome the safety problem of WEP mainly including the replacement of WEP with WPA2, the adoption of 802.1x system and the using of VPN and dividing of VLAN etc. the protection of management is referred to protect the security of WEP network on the basis of using WEP through more strict management measures and means, such as reinforcing the physical protection, isolating AP and upgrading hardware devices in time etc.

Replace WEP with WPA2: 802.11 TKIP encryption technology was first used by WPA. WPA2 is the further upgrade of WPA. It can greatly solve the problems existing in 802.11 using the original WEP security.

Using 802.1x system: 802.11x introduces extensible authentication protocol (EAP). As the extensible authentication protocol, EAP can be used MD5, a one-time password, smart card, public key certification mechanism, which provide a higher level of security. It is defined by the ppp protocol. In terms of user authentication, 802.11 x client authentication request can also be through external RADIUS server for authentication.

Using VPN and dividing VALN: VPN can be used to ensure the confidentiality, integrity and authentication in the data communication network. IPSec can also be used to ensure the safety of WLAN, and the safety is far greater than the traditional PPTP VPN. VLAN ,a switched network,is divided on logic according to the function, the project team or application ,rather than physical or geographical division. One can use VLAN to achieve the purpose of reconfiguring the network through software instead of removing the charge mobile devices and circuit in the house.

Physical protection: Develop a comprehensive security policy and firm manner to ensure that the wireless AP and wireless network card's security. Because almost all of the wireless devices with reset button to reset the function of AP, makes a stolen AP can easily be reused by other people . Therefore, the AP can be placed in a position not easy contact, you can also lock the device and the bracket directly. In addition, the use of a built-in wireless network card desktop computers should also avoid wireless card is lost or the whole computers be stolen.

Isolation of AP: By reducing the AP transmission power, change the low gain wireless way can be AP signal coverage to the office area, can be completely isolated all the wireless client device, so can only access AP connection of the fixed network. For the special department, the wireless signal working range can be strictly limited.

Upgrading hardware devices in time: As a wireless security managers should often browse wireless equipment manufacturers website, view the latest vulnerability and related patch announcement, and in a timely manner for the safety of the equipment installation manufacturers released update or upgrade programs.

5. Conclusion

This paper analyzes the existed problems of security of Wireless LAN based on WEP mechanism, offers the methods of cracking the passwords of WEP, and provides the corresponding security solutions based on this. The research shows that there are severe security problems of Wireless LAN based on WEP mechanism and they bring safety loopholes for the users of wireless. In order to solve the security problems, we can build the solid solution from the physical, technological and management aspects. The use of more advanced WPA would overcome the disadvantages of WEP and 802.1 x system, but also brings new security issues. The security of wireless LAN Based on the IEEE 802.1 x system will be our next research emphasis.

6. Acknowledgements

This work is Supported by 2016 Outstanding Youth Science and Technology Innovation Project of Henan Province: research of the macro scenario fitting routing technology centering on content, Zhengzhou science and technology development plan（153PKJGG26）and the Graduate,s Scientific Research Foundation of Zhengzhou University of Light Industry.

7. References

[1] Saini N, Mandal S. Wireless LAN Security[J]. International Journal of Research, 2015, 2(5): 33-37.

[2] Zhao P, Liu J, Wang S. A Scheme of Trusted and Secure Access to WLAN[C]//Proceedings of the 2012 International Conference on Electronics, Communications and Control. IEEE Computer Society, 2012: 2711-2714.

[3] Tews E, Ralf-Philipp W, Pyshkin A. Breaking 104 Bit WEP in Less than 60 Seconds[EB/OL]. (2007-12-13). http://eprint.iacr.org/.

[4] Fluhrer S R, Mantin I, Shamir A. Weaknesses in the Key Scheduling Algorithm of RC4[M]//Vaudenay S, Youssef

A M. Selected Areas in Cryptography 2001. [S. l.]: Springer, 2001.

[5] Kore K. Next Generation of WEP Attacks?[EB/OL]. (2004-10-25).
http://www.netstumbler.org/showpost.php?p=93942&postcount35.

[6] Klein A. Attacks on the RC4 Stream Cipher[J]. Designs, Codes and Cryptography, 2008, 48(3): 269-286.