Security Protection Under the Environment of WiFi

Zihui Ren[1, a *], Cheng Chen[2,b] and Lijun Zhang[3,c]

[1]No.120 science avenue, Hefei high - tech industrial development zone, Anhui province, China

[2]No.120 science avenue, Hefei high - tech industrial development zone, Anhui province, China

[3]No.120 science avenue, Hefei high - tech industrial development zone, Anhui province, China

[a]26089314@qq.com, [b]3412246@qq.com, [c]290046305@qq.com

Keywords: Security vulnerabilities; Attack form; Countermeasures

Abstract. Wireless network technology is one of the important symbols of the development of global information technology in twenty-first Century. Wireless access. wireless lan and other technologies have been flourishing in recent years. But the security problem has become increasingly prominent. Such as security vulnerabilities WPA and WPA2 protocol of session key agreement in the foreign media recently. These vulnerabilities can lead to the WPA/WPA2 protocol to solve key heavy attack. WPA/WPA2 encryption protocol and the corresponding network intrusion. For a while, WiFi security problem has become a new research topic of wireless network. This paper starts with analyzing the structure and attack form of wireless network, summarizes and analyzes the potential security risks of WiFi's different application scenarios and puts forward countermeasures.

WiFi Application Status

According to the different application environment of WiFi. WiFi is divided into two application scenarios. One is home WiFi which is characterized by the user password to join the WiFi wireless network. Then the user gets the address, and then can access the Internet normally, two is the commercial WiFi which is characterized by the unified management and allocation of the front end of a plurality of wireless devices using a wireless controller and uses portal+radius authentication method. When the user reaches the wireless hot spot. It gets the address first but it can't go online properly. After the portal is popped out and the authentication is completed. The user can go online.

WiFi Security Risks

In view of the above two application scenarios of WiFi. According to the statistics and extensive field research of China's public WiFi security report in the first half of 2017. WiFi mainly has the following ways of attack.

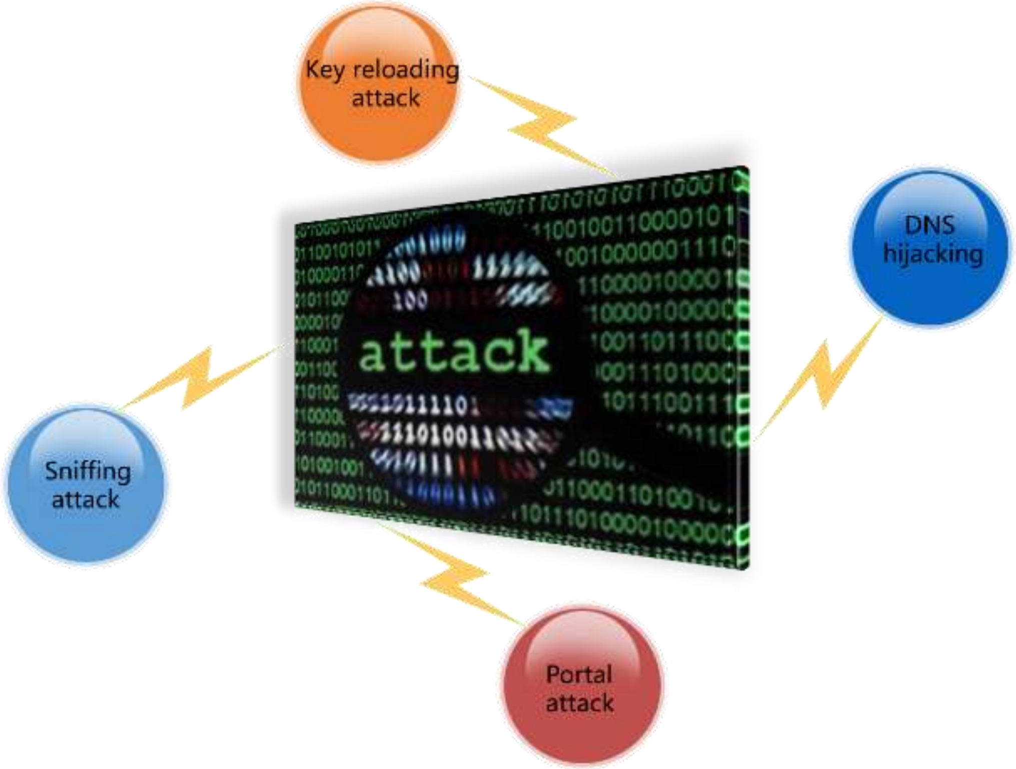

Figure 1. Attack form of wireless network

WiFi Sniffer Attack. The WiFi wireless packet is transmitted in the air. Using the 802.11b/g/n/ac protocol and any wireless network card can be received within the coverage. If an illegal hacker holds a special network card, it can intercept the packets that are transmitted in the entire network. Once the hacker sniffing the monitored equipment received and sent to all network packets, it is possible to attack the target to initiate all kinds of intrusion and attack, such as session hijacking, as the name suggests is the victim of the ongoing operation can be hijacked to their wireless devices, and realize the remote control of the victims even implanted Trojan to steal the identity card number , personal income, bank card number, and other sensitive information. You can also launch script injection attacks, data tampering, and thus distort the victim information sent or received information, even by a simple sniffer can crack wireless air interface encryption algorithm, and further access to other network account and password.

Key Reloading Attack. The WPA/WPA2 encryption protocol vulnerability used to protect WiFi security is called "key reinstall attack" (KRACK), which affects almost all computers, cell phones, routers and other WiFi devices. The attack takes place 4 times when the terminal is connected to an encrypted WiFi network. The 4 handshakes were designed to verify whether the password was correct or not to allow the device to be allowed to access the network. Using this vulnerability, hackers can manipulate and replay encrypted handshake information with the aid of the fishing AP in order to deceive the victim to reinstall the key that has already been used. When the victim restores the key, such as Nonce and Replaycounter will be reset to the initial value. As a result, the same encryption key may be random value used has been used, resulting in the encrypted data packet when the repeated use of key stream, so that the key can be a random value to decrypt the message, hackers can monitor data communications to the wireless terminal, to steal user privacy.

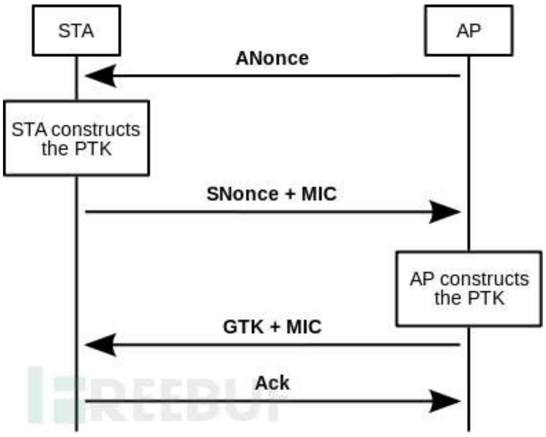

Figure 2. Four time handshake protocol in WPA2 encryption mode

Portal Attack. This attack mainly exists in the need to access the certification page of commercial WiFi, mostly uses the Portal server to the user authentication before Web Portal redirects, due to the Web Portal server can be all network users to access the Internet, so there are "tampering, denial of service attacks website security threats, which is related to hackers by means of tampering the web page address will access authentication, user login interface intercepted to other web pages, or use illegal means to occupy the host or network in most of the resources, causes the network user cannot effectively use.

Dns Hijacking Attack. No matter home or commercial WiFi equipment, some network equipment manufacturers have left the back door in the management firmware for the convenience of the later maintenance and management. It also brings a hidden danger to device security. If WiFi device or wireless controller is invaded by the outside, the attacker can easily change the configuration of the device, destroy the user's wireless network, and make the user unable to access the Internet. In addition, hackers can also add additional configurations, such as DNS, to achieve DNS hijacking. After the DNS hijacking, the hijackers' access to the Internet, the login account and the passwords for the plaintext will be easily obtained by the hijackers.

Countermeasures

For security risks above domestic and commercial WiFi, we can take to improve the network security policy level, deployment of safety protection equipment and system, network equipment selection to improve their own system of wireless network security defense security level, high safety and high reliability for household and commercial WiFi.

For Sniffer Attacks. Because of the difference of WiFi access and authentication mechanism between home and business, the ways of prevention are also different.

Table 1 Sniffer attack defense method

Application scene	Home Wifi	Commercial WiFi
Defense measures	Hide your own SSID Configuring MAC white list Enhanced password management Watch out for network attacks at any time Using encrypted network resources	Using radius advanced authentication methods To enhance the security of the empty packet Configuring the AP isolation strategy

Home WiFi. The first, you can hide your SSID, configure the MAC white list, regularly replace and use strong passwords, that is, more than 8 digits and more complex passwords that contain upper and lower letters, numbers and symbols. In addition to the empty data encryption transmission, wireless access, increasing the difficulty of hackers to crack up hackers from the source control. The MAC white list function allows only the trusted devices to connect to WiFi, and the non trusted devices refuse to connect to WiFi. The second, when we find ourselves slow down, it may represent sniffing attacks. At this time, you should write off and exit the network account and emptying the cookies of the wireless terminal and revise the wireless password. At last, It is suggested that you choose to use encrypted network resources, such as a web site that supports "HTTPS".

Commercial WiFi. One is to use radius advanced authentication method and combine security audit to realize legitimate users access to legal network. Even if the hacker attacks, also can accomplish positioning and tracking; the two is to enhance the empty packet decryption difficulty, to ensure the communication content can not be eavesdropping; three is to configure the AP isolation and user isolation, to prevent illegal users from sniffing behavior from the source.

For Key Reloading Attack. Whether it is home WiFi or commercial WiFi can be from two aspects of prevention. One is the need to update the client operating system to avoid driving; two is to open the illegal AP detection and positioning function, timely detection of fishing and fishing AP, AP resistance, users don't trust related non fishing signal AP; or related, users will continue to drop or can not normally access.

For Portal Attack. This attack is a way of attack by commercial WiFi. For this attack, we can deploy firewall, anti DDOS, webpage tampering and other security protection system at the front of server, so as to ensure the high security of Web Portal server.

For Dns Hijacking. The prevention measures of home WiFi and commercial WiFi are basically the same. One is to start from the source of prevention, it is recommended not to buy there are loopholes in the router; two is always pay attention to security updates issued by a manufacturer, will be updated to the latest version of the firmware of the device, try to repair the known vulnerabilities; three is to modify the WiFi device admin password and WiFi, and not the same password, use the same 8 suggestions above, high strength and small letters containing password and digital symbol; four is the standard reference in the information security protection, improve equipment safety protection level of commercial WiFi.

Summary

In security, The current standard of wireless protocol is up to the standard, and it is relatively safe. The probability of successful WiFi crack is still very low, the attack hackers succeeded, mostly because of lack of user security awareness, equipment configuration, improper password strength and security assistance is not in place and other factors. This paper lists the attack form of household and commercial WiFi network and means, put forward security defense strategies and methods under the current situation of the WiFi network, to prevent in advance in the use or management of WiFi network, so as to guarantee the security of wireless network user information.

Reference

[1] Feng Yang and Haojun Zhang: Research and implementation of wireless LAN security protocol(Beijing University of Posts and Telecommunications Press, China 2005).

[2] Xuechen He: Information confrontation and network security(Tsinghua university press, China 2010).

[3] Erli Hao and Qing Yang: Wireless Network Security (Science Press, China 2009).

[4] Anderw S.Tanenbaum and Aimin Pan:Fifth edition of computer network(Tsinghua university press,China 2012).

[5] Information on http://mi.techweb.com.cn

[6] Huaifeng WANG and Guangyao Gao: China Computer & Communication, (2011) NO.10 P.131

[7] Jinlong Wang : Cognitive wireless network(Machinery Industry Press,China 2010)

[8] Zhe Yang: Wireless network security attack and defense actual combat(Electronic Industry Press,China 2008).

[9] Xu Chen: Youth Science (2014) NO.11 P414

[10] Zhiyong Lu: Wireless LAN and Its Countermeasures(National Defense Industry Press China 2006)