A Survey WLAN Security Defenses Based on the Link Layer

Bo Huang

***Abstract*—These instructions give you guidelines for preparing papers for the International Journal of Information and Education Technology (IJIET). Use this document as a template if you are using Microsoft Word 6.0 or later. Otherwise, use this document as an instruction set. The electronic file of your paper will be formatted further at International Journal of Information and Education Technology. Define all symbols used in the abstract. Do not cite references in the abstract. Do not delete the blank line immediately above the abstract; it sets the footnote at the bottom of this column.**

***Index Terms*—WLAN, link encryption, link security, WEP, WPA, WPA2**

I. Introduction

As the network technology and communication technology are increasingly developing and maturing, Internet users have been gradually freed from the bondage of "line"; that means, the user can get access to the Internet network with the help of any point of its coverage or using the diversity of terminal equipment in the process of moving. Wireless network breaks out of cable ties and brings free mobile space. Compared with the traditional cable network, the superiority of the wireless network is obvious: it has mobility, high flexibility, convenient installation, and strong expansion ability; since the wireless network is free from the geographical space constraints, the network planning and adjustment can be carried out easily. Therefore, Wireless network, owing to its unique convenience, has been widely used. As a result, with the lower cost and better technology, more and more customers can, with low budget, enjoy high speed of surfing and stable wireless access service, which, in turn, engenders the popularity of wireless networks. There is no wonder that man can take advantage of wireless network almost everywhere in China, ranging from the prosperous commercial street, high and new technology industry development zone, the university campus, scientific research units, the government and police and troops subordinate organizations, to ordinary families.

Despite its prosperity, we must realize that while wireless network does bring its users convenience, it generates some defects, which calls for our concern over its safety. First of all, since wireless network depends on the radio waves to transmit signals, the transmission can be hindered by buildings, vehicles, trees and other obstacles; consequently, the performance of the network will be influenced. Secondly, the transmission rate and cable channels of wireless network transmission are relatively low, so it is only suitable for personal terminal and small-scale network application. Thirdly, wireless signals are discrete, and easy to be monitored; as a result, information leakage will happen now and then. For all these reasons, the security problem related to wireless network cannot be neglected. The following is the explanation and analysis of encryption and authentication security based on the wireless network link layer.

Manuscript received May 9, 2012; revised June 15, 2012.

Bo Huang is with the Liaoning Police Academy, Dalian, China (e-mail: hb730@yahoo.cn).

II. The Link Layer Safety and Link Encryption

The link layer is on the first floor of the OSI reference model. The link layer provides service for the network layer on the basis of the physical service; its most basic service is to transmit the data from the source machine network layer to the adjacent target machine network layer. The function of link layer is the realization of the correct transmission between binary data units within system entities by a series of synchronous control and error control, flow control; to be exact, the whole process contains: how to combine the data into the data block – the teleport units frame of the link layer ; how to control the transmission of frame in physical channel, including how to deal with transmission error; how to adjust the send rate to correspond with the receive party; and how to set up, maintain and release data link pathway between two network entities

As far as the safety of link layer connection is concerned, it is relatively weak. In cable network the encryption based on the link layer is seldom used. In the wireless network, by contrast, encryption and authentication is an essential technical scheme, mainly because there are tangible transmission media in the cable network transmission, and the closed transmission channel forms natural physical barriers for the security of the information transmission, especially the characteristics of different transmission media guarantee the security of the information transmission. On the contrary, without tangible physical transmission media in WLAN network, the link layer is exposed to the public space in the atmosphere, so the security of the link layer in the course of WLAN transmission does arouse more concerns.

Link encryption is encryption of transferred data conducted only in the physical link layer. For some communication link between two network nodes, link encryption can ensure the security of the data transmitted online. As to link encryption, it means that all data are encrypted before transmission, and then each node of the network decrypts the data received; after that, the data are encrypted using the key of the next link before they are sent. Before reaching the destination, a data may pass through

many a communication link. Because in each transmitting node the data is first decrypted and then encrypted, and all data on the link, including routing information, are in the form of the cipher text, link encryption can cover up the point of origin and the end point of the transmitted data. At the same time, owing to the use of the filling technology and the fact that a fill character can be encrypted without being transmitted, the characteristics of frequency and length of the transmitted data can be covered, which can prevent the analysis of communication services and ensure the security of network communication.

III. WLAN Safety Standard 802.11i

Wireless network security standard 802.11i contains WPA and WPA2 subset, which, in order to enhance the performance of WLAN data encryption and authentication, defines RSN, and improves the WEP encryption. IEEE 802.11i requires the use of 802.1 x authentication and Key management and, in data encryption, defines three types of encryption: the TKIP (Temporal Key Integrity Protocol), CCMP (Counter-Mode/CBC-MAC Protocol) and WRAP (Wireless Robust Authenticated Protocol). TKIP uses RC4 of WEP mechanism as the core encryption algorithm to reach the goal of the safety of WLAN by upgrading the firmware and driver of existing equipment; CCMP, which is based on AES (Advanced Encryption Standard) Encryption algorithm and CCM (Counter-Mode/CBC-MAC) the authentication style, enhances the safety degree of WLAN greatly and, therefore, is a must to realize RSN. Since AES has a high demand for hardware, the upgrading of CCMP cannot be fulfilled on the basis of the existing equipment; therefore, it is an optional encryption mechanism to combine WRAP mechanism with AES encryption algorithm and OCB (Offset Codebook).

IV. WLAN Encryption and Authentication of the Link Layer

The purpose of applying WLAN encryption and authentication is to make wireless business achieve the same level of security as that of cable business. The process of encryption and authentication is realized in the link layer of the wireless LAN. Considering the fact that encryption and authentication technology includes SSID, MAC, WEP, WPA, and WPA2, etc, they all belong to the encryption and authentication methods of integrated network card.

A. SSID Broadcasting Technology

SSID is Service Set Identifier of wireless local area network, which is a password between wireless client and wireless router. A wireless card can be connected with a wireless router only when SSID is exactly the same. At present SSID technology has two concepts: one is BSSID (Basic SSID, Basic service set marks), the other is ESSID (Extended SSID, Extended service set mark). BSS is used to mark a smaller BSS region, and each host communicates in small region; ESSID, by contrast, is to make the various BSS expand to ESS, and many BSSID constitute an ESS area.

In the wireless local area network, Service Set Identifier, namely, SSID broadcasting is one of the important functions of routing equipment. Open the wireless local area network of SSID broadcasting, and then the router will automatically broadcast SSID to the wireless network client within the effective scope and the client can receive the SSID by scanning, and immediately get access to wireless LAN. At present, a user usually owns his or her own client system. Since a lot of people know SSID, it is easy to be shared by illegal users. Meanwhile, many public wireless routers or AP set the same SSID, and the SSID is set to broadcast externally when the router is restarted. Of course, this kind of practice brings users much convenience, but it also opens the door for invaders.

With respect to the security problem of the SSID broadcasting technology we can take some measures such as modifying the SSID Settings of the wireless router, closing SSID broadcasting or presetting for all the legal wireless client. Thus, illegal users will not be able to connect with this wireless router or AP whose SSID broadcasting has been closed.

B. MAC Address Filtering and Static IP Binding

Wireless LAN can also use MAC address filtering in cable network, so as to allow or prohibit the part of the MAC address hosts to get access to the corresponding wireless LAN according to need. At present, MAC address filtering can be realized in the wireless router or AP supported by IEEE 802.11g standard or above. Such equipment can allow or prohibit the MAC address users in the list of the MAC address to get access to the wireless local area network.

When a wireless router or AP configures IP addresses, DHCP, which means Dynamic Host Configuration Protocol, is usually defaulted, and this, to the wireless local area network, generates potential safety hazard: as long as the invaders find the wireless local area network, it is easy for them to get a legitimate IP address through DHCP and enter the local area network. So close DHCP service, configure a fixed static IP address for each personal computer, and then bind the IP address with the MAC address for a computer network card. In this way the security of wireless local area network can be greatly improved.

C. WEP Encryption

WEP (Wired Equivalent Privacy, cable equivalence secret) protocol is the security technology used for encryption and authentication of link layer frame data flow, especially for WLAN network with IEEE802.11 x series standard. WEP adopts symmetrical encryption mechanism and RC4 encryption algorithm, and the same key and encryption algorithm are used for data encryption and decryption. WEP uses encryption key to encrypt data of each data packet exchanged on 802.11 x Internet. The whole process is like this: a key is configured in the wireless router or in the AP, which will encrypt this key, and users must enter the same key to online when they connect to a wireless router or AP.

However, people have found out the predictability of the method of using WEP to generate a key; that means, it is easy for the potential intruders to intercept and crack the key. The current plan of WEP has transformed the original 40-bit key to a 104-bit key, making it impossible to crack the key in a high performance using "exhaustively method"; but when a

single key solution is adopted, it still has the chance to crack a WEP key. Therefore, WEP designers embed "initial vector (IV)" in a WEP key; 24-bit IV changes with each transmitted information packet, and is attached behind the original sharing key in order to minimize the probability of the same key. But the general WEP IV strategy allows IV to be used repeatedly and IV value can be transmitted openly with packets, which enables the attacker to threat the safe WLAN transmission by analyzing the same cipher text emerged frequently.

D. WPA Encryption

In view of WEP weaknesses, Wi-Fi Alliance (The Wi-Fi Alliance) has established WPA (Wi-Fi Protected Access, Wi-Fi protect Access), which can be defined as WPA = 802.1 x + EAP + TKIP + MIC. Among them 802.1 x refers the identity authentication standard of IEEE 802.1 x; EAP (Extensible Authentication Protocol) is a kind of expansion identity authentication protocol; TKIP (Temporal Key Integrity Protocol) is a key management agreement and MIC (Message Integrity Code) checks the integrity of information.

WPA uses In IEEE802.1 x and EAP as foundation of its users' authentication. Before they login the wireless local area network, users need to provide the corresponding identification, which will be checked against corresponding legal user database to confirm whether they have the authority to join. Whoever logins the wireless local area network must through such an authentication process. TKIP is the authentication depending on groups of keys distributed by the authentication server. The formation of the key is dynamic. TKIP distributes a group of dynamic keys to its wireless client, wireless router or AP, and then key levels and management system are established. The only data encryption key will be produced by using its matching key, and the only data key will be encrypted to realize the data packets. MIC is used to prevent the attacker from intercepting, tampering and even redelivering data packets.

WPA is a kind of interoperable WLAN safety enhancement solution based on the standard, which can significantly improve the data protection and access control level of wireless local area network. WPA can protect of the data of WLAN users, for only the authorized users who have been through the identity authentication and integrity examination can login the network WLAN network.

E. WPA2 Encryption

WPA2 is the second version of the WPA, the upgraded version concerning safety. It mainly transforms WPA TKIP/MIC to AES-CCMP. WPA2 may be defined as WPA2 = IEE802.11 I = 802.1 x/EAP + AES + CCMP.

The 802.1x and EAP in WPA2 have the same authentication standard and protocol role as in WPA. 802.1x is a terminal access agreement by authentication to protect network, while EAP is used to transmit validation information between the client and the server user. In WPA2 an encryption technology AES-CCMP (Advanced Encryption Standard-Counter mode Cipher-block chaining Message authentication code Protocol) with better performance and higher safety is used, which provides more security than TKIP.

AES used in WPA2 is a kind of advanced encryption algorithm. In WPA2 AES is not directly used for encryption, but AES-CCMP uses AES block encryption algorithm, and limit of the key's length is 128 digits. The combination of two complex encryption technologies (Counter mode and CBC-MAC) provides a secure encryption and authentication protocol between the wireless client and wireless router or AP and it is also applied in the etheric frame. In short, AES-CCMP is the highest level of public wireless security protocol, in which CCMP provides encryption, authentication, completeness checks and replay protection, etc.

In respect of WLAN encryption and authentication technology, SSID broadcasting technology and MAC address filtering and static IP binding are two basic methods, which are easy to be conducted and applied in daily life. Because of that, common WLAN clients can arrange them at home. In comparison, WEP, WPA and WPA2 are the progressive technologies in the field of encryption, among which, WPA2 is, theoretically, the best. When both the cost of encryption and that of the security of WLAN network are concerned, WPA2 should be the best choice, since the current wireless routers or AP have no problem with all the encryption technologies mentioned above.

V. Conclusion

The wireless local area network has such advantages as good transmission performance, wide cover range, easy expansion and flexible networking, so there is no wonder that it is widely used in many fields and received by more and more users. In this case, the network security problem must be given more concern, since it has close connection with our work as well as our daily life. Aiming at its potential security threats, corresponding technology should be used to achieve the security of wireless local area network and to effectively control the invasion of the invaders. Security technology must be constantly developed and bettered and security strategy must be continuously improved in order to guarantee the safety of the wireless local area network. With the constant growth of wireless applications, in the near future, a set of united, sound and popular security system will be set up.

References

[1] W. Da, "Network Engineer -Network Security System Design," *Publishing House of Electronics Industry*, 2009. vol. 8, pp. 81－128

[2] W. Jiang, "Wireless Network Security Technology Comparison," *Computer Knowledge and Technology*, 2009. vol. 10, pp. 8426-8427

[3] B. C. Young, J. Muller, C.r V. Kopek, and J. M. Makarsky, "Corporate wireless LAN security: threats and an effective security assessment framework for wireless information assurance," *International Journal of Mobile Communications*, vol. 4, no. 3, pp. 266-290, 2006.

[4] Y. Li, "Wireless LAN—Security and Protection," *Technological Development of Enterprise*, 2009, vol. 28, no. 8.

[5] T. Hassinen, "Overview of WLAN Security," *Seminar on Network Security* 2006. vol. 11, no. 12.

[6] Wireless LAN: Security Issuesand Solutions. [Online]. Available: http://www.san.org/reading_room/whitepapers/wireless/wireless-lan-security-issues-solutions_1009

[7] J. Vollbrecht and Founder. 802.11b Wireless Networking and Why It Needs Authentication. [Online]. Available: http://www.interlinknetworks.com/whitepapers/WLAN_Access_Control.pdf

[8] S. Gayal and S. A. VethaManickam. [Online]. Available: "WirelessLANSecurity",http://www.itsec.gov.cn/docs/20090507163620550203.pdf