Secure key exchange scheme for WPA/WPA2-PSK using public key cryptography

Jaewon Noh, Jeehyeong Kim, Giwon Kwon, Sunghyun Cho
Hanyang University, Korea
wodnjs1451@hanyang.ac.kr, manje111@gmail.com, giwonkwon@hanyang.ac.kr, chopro@hanyang.ac.kr

Abstract

This paper proposes authentication and key exchange scheme to communicate between users securely in small scale Wi-Fi networks. Depend on the Wi-Fi options, there can be various vulnerabilities in the network. Especially, most of small scale Wi-Fi networks have used the options which can cause several vulnerabilities. These Wi-Fi networks use passphrase for access authentication. However, these passphrases are known by the small network owner. In such circumstances, the network cannot assure security between users in the same network. In the existing Wi-Fi network, attackers in the same network can acquire pairwise keys by eavesdropping messages. Thus, this paper proposes the secure key exchange scheme to apply a public key cryptography. Using public key system, a station and an access point exchange a secondary key which user selects. This key is used for pairwise key generation. Through the proposed scheme, the network can protect users from several attacks in the same Wi-Fi network.

Keywords: Wi-Fi, WPA, WPA2, PSK, Authentication, Public key, Security, Key exchange.

1. Introduction

Wi-Fi is wireless LAN access technology based on the IEEE 802.11 standard. Currently, Wi-Fi is used in many places such as office, university, cafe, home, etc. Depending on applications of Wi-Fi, authentication and encryption methods can be different. Unfortunately, most of small Wi-Fi networks have poor security level. Wi-Fi in the public places uses no password or open password for access. In this paper, a key exchange scheme is proposed to assure security of individual communication in the open Wi-Fi network. Most of existing small scale Wi-Fi networks use WPA (Wi-Fi Protected Access) or WPA2 (Wi-Fi Protected Access II) authentication method which uses a pre-shared key (PSK). In this paper, we assume that the Wi-Fi networks use WPA2-PSK because of higher security level compared to WPA-PSK. In addition, CBC-MAC protocol (CCMP) based on AES algorithm is used for encryption.

2. Related work

Up to now, many researches related to Wi-Fi security have been done. The only possible attack to find a PSK in WPA2-PSK Wi-Fi network is brute force attack. To protect a PSK from this attack, a defense scheme was proposed [1]. In [2], the authors compared security protocols in Wi-Fi such as WEP, WPA and WPA2, and proposed secure protocol for public Wi-Fi hotspot. In the other research, 11 issues and problems that exist in Wi-Fi are classified [3]. Also possible attacks such as traffic analysis, Address Resolution Protocol (ARP) spoofing, fake authentication and key cracking were analyzed in the research.

Wi-Fi security issues described above can be occurred frequently because many people use same Wi-Fi network easily in public places. WPA2-PSK has been known as a safe protocol because it is difficult to find a WPA2-PSK passphrase. However, the attackers can be in the same network that uses an open password. In this paper, we propose a secure scheme to provide higher security level in case that attackers are in the same network.

3. Wi-Fi network architecture

Wi-Fi network can be divided into two types according to the existence of authentication authorization accounting (AAA) server. AAA server is in charge of authentication to access Wi-Fi network. Thus AAA server is usually used in enterprise and internet service provider (ISP). In the Wi-Fi network with AAA server, users authenticate with an AAA server. However, in the small public Wi-Fi network that does not have AAA server, users authenticate with access point (AP).

In the network that has AAA server, several authentication methods are used such as EAP-AKA, EAP-TLS and EAP-SIM. On the contrary to this case, Wi-Fi network without AAA server uses the PSK authentication method using a passphrase. There are multiple options to encrypt information using key. WEP

978-1-5090-2743-9/16/$31.00 ©2016 IEEE

and temporal key integrity protocol (TKIP) encryption is not recommended currently. CCMP based on AES algorithm is widely used in WPA2-PSK Wi-Fi.

3.1 Access procedure

Figure 1 shows an access procedure of Wi-Fi system. An AP frequently broadcasts beacon message that includes Wi-Fi information. And user device (station) sends Probe Request message and receives Probe Response message. Through these messages, station and AP exchange authentication and encryption information of that Wi-Fi network.

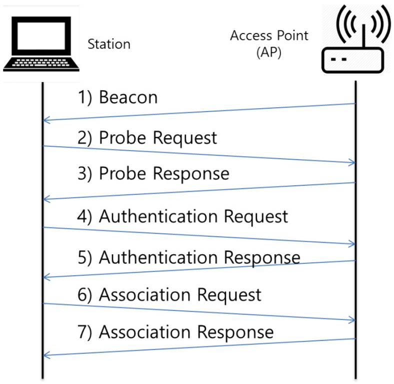

Figure 1. Wi-Fi access procedure

Authentication is processed using passphrase. After the authentication, association procedure is performed and a station is connected with network if the whole processes are successful. In the case of Wi-Fi network that has AAA server, null authentication is performed in 4, 5 steps. Instead, AAA server performs authentication procedure based on 802.1x standard after the association. In other words, PSK authentication performs authentication using passphrase. And EAP authentication that is used in enterprises performs authentication using user information in AAA server after the association. [4]

3.2 4-way handshake

After Wi-Fi access procedure, next procedure is to generate secret keys for communication is performed. This procedure consists of 4-way handshake. Figure 2 shows the whole process from making a PSK and a Master Key (MK) to generate a Pairwise Transient Key (PTK) and a Group Temporal Key (GTK).

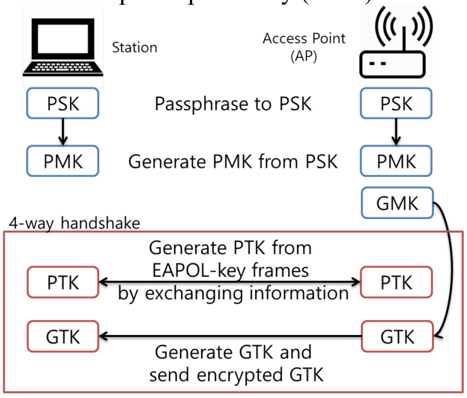

Figure 2. 4-way handshake

Passphrase and Service Set Identification (SSID) is used to generate a PSK. In 802.11i standard, PSK is generated using Password Based Key Derivation Function 2 (PBKDF2) [5]. The function is defined as

$$PSK = \mathrm{PBKDF2}(PassPhrase,\ ssid,\ ssidLength, 4096, 256).$$

In WPA2-PSK, a PSK is same as a Pairwise Master Key (PMK). Based on the PMK, 4-way handshake is performed. 4-way handshake is composed of 4 EAPOL-key type messages defined in 802.1x standard. From these messages, a PTK and a GTK are generated. First of all, an AP generates an ANonce and sends to a station. Then, the station that received an ANonce also generates the other nonce value called an SNonce. Also the station makes a PTK using a PMK, ANonce, SNonce and MAC addresses. In second EAPOL message, the station sends an SNonce and calculated Message Integrity Check (MIC) to the AP. When the AP receives this second message, it also makes a PTK, generates a GTK, and checks a MIC compared to the received MIC. Thirdly, the AP sends message including the ANonce, MIC, and encrypted GTK by the PTK. Finally, the station checks this MIC and sends an ack message. [5, 6, 7]

3.3 Vulnerabilities

Authentication and 4-way handshake operations have been defined to support secure communication in Wi-Fi network. Even though these efforts, there are several vulnerabilities. By using WPA2 protocol, the network can be safe from external access. However, the vulnerabilities can exist in the case that attackers are in the same network. Following sections describe the attack types using vulnerabilities in the current Wi-Fi system.

3.3.1 Traffic analysis

Traffics in the air between a station and an AP can be eavesdropped by sniffing tools like wireshark. By using sniffing tools, attackers can capture data packets and get information from the packets. If an attacker analyzes packets that are not encrypted, it would be critical threat to users. Based on traffic analysis, other attacks can be tried such as Denial of Services (DoS), key recovery, fake authentication and Man in the Middle attack [8]. Thus, this is one of the important vulnerabilities to be solved surely.

3.3.2 Key recovery

Assume an attacker eavesdrops on the progress 4-way handshake of a target station. The attacker already knows a passphrase and a SSID. It means attacker also knows a PSK and a PMK. So, if the attacker can get an ANonce and an SNonce from the EAPOL messages, a PTK could be derived in the attacker side. First and second EAPOL messages are encrypted using PMK. From the third and fourth EAPOL messages, a GTK also could be derived by the attacker. Consequently, the attacker can capture all encrypted packets of the target using the same PTK and GTK. This problem is very critical in Wi-Fi systems because the target doesn't know the problem that all packets are exposed to the attacker. Thus, it is important to keep keys securely.

3.3.3 Denial of Service attack

DoS attack includes all types of attack that interrupt normal communication in the network. It can cause large communication delay because users have to send same messages continuously [9]. For example, in association procedure of Wi-Fi network, an attacker changes the authentication request message on purpose. It makes the failure of authentication. In 4-way handshake, an AP and a station must share the same security information. So the attacker can interrupt to exchange information in the same manner with the prior example. These problems are hard to be solved. Thus, just reducing the possibility of the attacks has meaning for more secure system.

4. Proposed scheme

The proposed scheme applies the public key cryptography to Wi-Fi network. An AP has a public key and a private key. We assume that the passphrase is encrypted using the public key of the AP. In the original public key cryptography system, both sides should have public and private keys [10]. However, a station doesn't have two keys in the proposed scheme. Also the secondary key between a station and an AP is generated during the Wi-Fi access procedure.

4.1 Access procedure

Figure 3 shows the proposed authentication procedure. The difference with the existing procedure is encrypting messages and exchanging the secondary key.

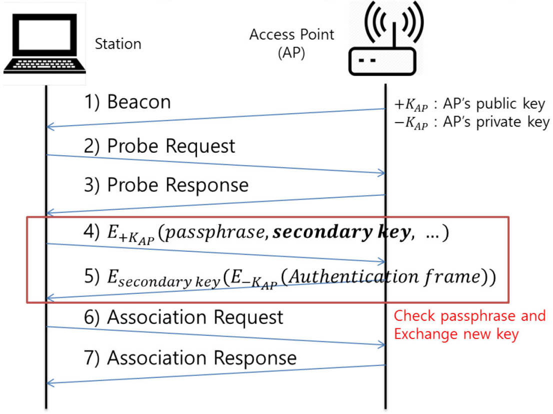
Station
Access Point (AP)
1) Beacon
$+K_{AP}$: AP's public key
$-K_{AP}$: AP's private key
2) Probe Request
3) Probe Response
4) $E_{+K_{AP}}(passphrase, \boldsymbol{secondary\ key}, \ldots)$
5) $E_{secondary\ key}(E_{-K_{AP}}(Authentication\ frame))$
6) Association Request
Check passphrase and Exchange new key
7) Association Response

Figure 3. Proposed access procedure

1) An AP broadcasts a beacon frame frequently that includes information about corresponding network.
2, 3) These steps are same as the original probe request and response messages.
4) When a station requests authentication, the station sends a secondary key as well as passphrase to the AP. This message is encrypted using the public key of AP. The secondary key will be used for only one user.
5) The AP decrypts the fourth message using its private key. The AP checks a passphrase. If it is correct, it sends a response message that is encrypted by private and secondary keys.

After the station receives the fifth message, it tries to decrypt the message using two keys. By decrypting the message, the station can know that the secondary key is exchanged successfully and this message is sent by the AP.
6, 7) After the authentication, the station and the AP perform association procedure in common with the existing procedure. And then, whole accessing procedure is finished.

We define the exchanged key to secondary key. This secondary key is used for generating a unique PSK. The proposed scheme can perform authentication and exchange a secondary key securely at the same time. It is the biggest difference compared to the existing scheme.

4.2 Key management

If the proposed access procedure is performed successfully, both of station and AP have a secondary key. This secondary key is a symmetric key. In key generation step, a PSK is generated using a secondary key, not a passphrase. Key generation procedure from a PSK to a PTK and a GTK is shown in figure 4. The PTK is a key for unicast, and the GTK is a key for multicast and broadcast.

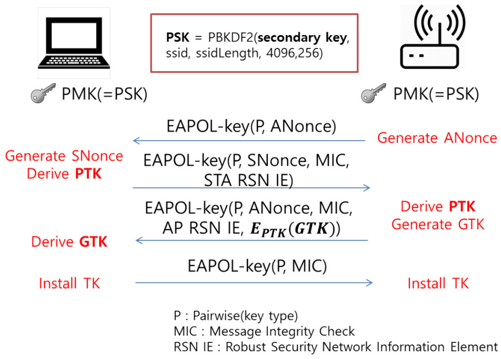
PSK = PBKDF2(secondary key, ssid, ssidLength, 4096,256)
PMK(=PSK)
PMK(=PSK)
EAPOL-key(P, ANonce)
Generate ANonce
Generate SNonce
Derive PTK
EAPOL-key(P, SNonce, MIC, STA RSN IE)
EAPOL-key(P, ANonce, MIC, AP RSN IE, $E_{PTK}(GTK)$)
Derive PTK
Generate GTK
Derive GTK
EAPOL-key(P, MIC)
Install TK
Install TK
P : Pairwise(key type)
MIC : Message Integrity Check
RSN IE : Robust Security Network Information Element

Figure 4. Proposed key management scheme

A PSK is derived by PBKDF2 which is a password based key derivation function using a secondary key, not the passphrase. A PMK is same as a PSK in WPA2-PSK Wi-Fi network. Station and AP perform 4-way handshake based on the PMK. First EAPOL-key message includes an ANonce that is generated by an AP. This message is encrypted using a PMK. A station can get an ANonce from this message. Then, the station also generates an SNonce, and derives a PTK using ANonce, SNonce, and PMK. Secondly, the station sends an SNonce and a MIC that can check message integrity with encryption. The AP derives a PTK using this information on the same way. After making a PTK, the AP generates a GTK. The GTK is encrypted with a PTK. The AP sends third EAPOL-key message that includes the encrypted GTK, ANonce, and MIC. Finally, the station gets a GTK by decrypting and sends an ack messages with a MIC. Consequently, both side install temporal key (TK) that is a part of a PTK.

This scheme is different from the original 4-way handshake scheme. In the proposed scheme, a station and an AP derive a PSK by using a secondary key instead of passphrase. Secondary key is unique from the others. The secondary key becomes a new passphrase for each user. From this approach, Wi-Fi network assures secure communication in the network.

5. Security analysis

5.1 Traffic analysis

Network traffic can be easily captured in the existing Wi-Fi network. In this case, one of the ways to increase security is reducing the exposure of information to attackers. The proposed scheme applies public key cryptography concept. According to this concept, authentication message is sent with encryption using AP's public key. Data packets encrypted with AP's public key can be decrypted only using AP's private key. Although an attacker captures packets during access procedure, the attacker has to solve AP's private key. Generally, a private key in public key cryptosystem is very hard to be solved. Thus, the attacker cannot get any information. In addition, the key exchanging scheme is progressed with encryption using a key that is difficult to be found. The proposed scheme protects the information in authentication and key generation messages. Even though attackers are in the same Wi-Fi network, the network provides an improved security level compared to the existing Wi-Fi network.

5.2 Key recovery

Attackers in the same network already know the passphrase for access. When an attacker tries to find communication key of a target user, the attacker can find this key by sniffing an ANonce and an SNonce in the existing Wi-Fi system. However, in the proposed scheme, a station and an AP exchange secondary key as well as a passphrase safely by public key encryption. Thus, each station can have different PSK. Even though the attacker finds two nonce values, the next key would be hard to be detected. Also an attacker cannot find PSK easily because both exchange secondary key securely. Furthermore, the attacker cannot easily get a PTK generated from PSK. Moreover, to find secondary key has the same difficulty with passphrase cracking in WPA2. Consequently, the proposed scheme provides the improved security for public small scale Wi-Fi network compared to the existing Wi-Fi network.

6. Conclusion

Wi-Fi is an access network that anyone can use, but it has several vulnerabilities of security. Especially, most of public Wi-Fi networks are using PSK authentication based on the shared passphrase. In these networks, data traffics can be sniffed by attackers who are in the same network. Thus, we proposed the authentication and key exchange scheme by applying public key cryptography concept. In the proposed scheme, a station and an AP exchange unique secondary key. Each user can use different keys in the same Wi-Fi network. From initial access procedure, attackers cannot get any information for other stations. By protecting traffic analysis, users are safe from additional attacks such as fake authentication, and key recovery attack. This paper contributes to improve the security level of WPA2-PSK and WPA in Wi-Fi networks.

Acknowledgement

This work was supported by the research fund of Signal Intelligence Research Center supervised by the Defense Acquisition Program Administration and Agency for Defense Development of Korea.

References

[1] Liu, Yonglei. "Defense of WPA/WPA2-PSK brute forcer." *Information Science and Control Engineering (ICISCE), 2015 2nd International Conference on*. IEEE, 2015.

[2] Raju, Laiju K., and Reena Nair. "Secure Hotspot a novel approach to secure public Wi-Fi hotspot." *2015 International Conference on Control Communication & Computing India (ICCC)*. IEEE, 2015.

[3] Waliullah, Md, et al. "An Experimental Study Analysis of Security Attacks at IEEE 802.11 Wireless Local Area Network." *International Journal of Future Generation Communication and Networking*, 9-18pp, 2015.

[4] Mitchell, C. H. J. C. "Security Analysis and Improvements for IEEE 802.11 i." *The 12th Annual Network and Distributed System Security Symposium (NDSS'05) Stanford University*, Stanford. 2005.

[5] IEEE 802.11i-2004: Amendment 6: Medium Access Control (MAC) Security Enhancements, IEEE Standards, July 2004.

[6] IEEE Std 802.11-2012: Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, IEEE Standards, March 2012.

[7] Ghanem, Mohamed Chahine, and Deepthi N. Ratnayake. "Enhancing WPA2-PSK four-way handshaking after re-authentication to deal with de-authentication followed by brute-force attack a novel re-authentication protocol." *2016 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (CyberSA)*. IEEE, 2016.

[8] Agarwal, et al. "Advanced stealth man-in-the-middle attack in wpa2 encrypted wi-fi networks." *IEEE Communications Letters,* pp. 581-584, 2015.

[9] Agarwal, et al. "Detection of De-Authentication DoS Attacks in Wi-Fi Networks: A Machine Learning Approach." *Systems, Man, and Cybernetics (SMC), 2015 IEEE International Conference on.* IEEE, 2015.

[10] Dolev, Danny, and Andrew Yao. "On the security of public key protocols." *IEEE Transactions on information theory*, pp. 198-208, 29.2, 1983.