A Secure Wireless LAN Access Technique for Home Network

*Ju-A Lee, *Jae-Hyun Kim, **Jun-Hee Park, and **Kyung-Duk Moon
*School of Electrical and Computer Engineering
Ajou University, Suwon, Korea
{gaia, jkim}@ajou.ac.kr
**Home Network Device Research Team
ETRI, Daejeon, Korea
{juni, kdmoon}@etri.re.kr

Abstract—IEEE 802.11i standard supports a secure access control for wireless LAN and IEEE 802.1X standard includes various authentication method protocols. It is expected that next-generation wireless LAN security techniques will be based on IEEE 802.1X and IEEE 802.11i standards. However, at present users who are not familiar with a computer and an authentication details have difficulty to setup the network security based on IEEE 802.11i. Accordingly, this paper proposes authentication scenarios to minimize the process by users, a password method which is changed randomly and periodically, and authentication protocols. The proposed protocols provide convenience for nonprofessional computer users as well as secure home network environment against the unwanted attacks such as a brute force attack or a replay attack.

I. INTRODUCTION

Home network service has been integrated with various communication technologies for the convenient life. It is expected that wireless LAN (WLAN), Bluetooth, ultra wide band (UWB), and Zigbee are used in home network as wireless access technologies to provide various home network services. WLAN study among them is actively making progress. But WLAN communication technologies have a problem that access points (APs) can not control the transmission range. This property offers the chance that the neighbor or man beside the house can receive the traffic and the malicious intruder makes bad use of privacy. Therefore, authentication mechanisms have to be considered as a mechanism that only an eligible user is authenticated to use resources of home network.

IEEE 802.11 working group (WG) specifies an authentication procedure but it provide the only basic mechanism which can not protect the WLAN communications from the ineligible approach. IEEE 802.11i standardization group is working on the access control based on IEEE 802.1X and air traffic encryption to strengthen WLAN security techniques. In conventional method, nonprofessional user is very difficult to setup security information inside WLAN stations and APs. However there are the various user levels of computer knowledge in home network. Because of this reason the way to setup authentication information should be prepared easily for users who are not computer professionals.

In this paper, we propose access control scenarios considering the convenience of users and the secure authentication protocol to support access control scenarios.

Section II presents related works. In Section III, we propose authentication scenarios and the security mechanisms for home network. The performance analysis of the proposed security mechanisms is presented in Section IV. Finally Section V concludes the paper.

II. RELATED WORKS

A. IEEE 802.11i

IEEE 802.11i provides enhanced security in the medium access control (MAC) layer for IEEE 802.11 networks [1], [2]. One of the major missions of IEEE 802.11i is to define a robust security network (RSN). The definition of an RSN according to IEEE 802.11i specification is a security network that only allows the creation of robust security network associations. To provide associations in an RSN, IEEE 802.11i defines authentication, encryption improvements, key management, and key establishment.

As shown in Fig. 1, in the first stage, IEEE 802.11i starts with Open System Authentication defined IEEE 802.11. And the WLAN station is authenticated and associated with an AP. At the end of this stage, IEEE 802.1X port remains blocked and no data packets can be exchanged. The second stage consists of IEEE 802.1X authentication which employs extensible authentication protocol (EAP) to authenticate users. A user can surf the Internet after the completion of 4-Way Handshake execution in the third stage.

B. IEEE 802.1X

IEEE 802.1X standard specifies how to implement port-based access control for IEEE 802 LANs, including wireless LAN [3]. In IEEE 802.1X, the port represents the association between a WLAN station and an AP. Basically IEEE 802.1X has three entities which are a supplicant, an authenticator, and a backend authentication server. In the context of a wireless LAN, the supplicant is a wireless LAN station, the authenticator is an AP, and the authentication server can be a centralized remote access dial-in user service (RADIUS) server.
The authenticator controls the authorized state of its controlled port depending on the outcome of the authentication processes. Before the supplicant is authenticated, the authenticator uses an uncontrolled port to communicate with the supplicant. The authenticator blocks all traffic except the EAP messages before the supplicant is authenticated.

IEEE 802.1X employs EAP as an authentication framework that can carry many authentication protocols, between the supplicant and the authenticator. The protocol between the authenticator and the authentication server is not specified in the IEEE 802.1X standard. Instead, IEEE 802.1X provides RADIUS usage guidelines in the Annex.

Fig. 2 shows the protocol stack for the authentication in IEEE 802.1X. The EAP messages in EAP over LAN or wireless LAN (EAPoL) transmit the authentication information to the authenticator from the supplicant. And the RADIUS protocol is used to carry EAP messages to the authentication server from the authenticator.

C. EAP

EAP is a method of conducting an authentication conversation between a supplicant and an authentication server. It is also an authentication protocol for general purpose. The authentication methods in EAP include message digest 5 (MD5), transport layer security (TLS), tunneled TLS (TTLS) and so on. These method protocols have features as follows.

- EAP-MD5 [6]: EAP-MD5 uses challenge handshake authentication protocol (CHAP [7]) which is a challenge-response process for the user authentication portion. It is one of the most popular EAP types because it is easy to use. The authentication server asks for the password by sending RADIUS-Access-Challenge. The password hash is then sent by using EAP-Response, which is further encapsulated by RADIUS-Access-Request.

- EAP-TLS [8]: EAP-TLS provides a way to use certificates for both the supplicant and the server to authenticate each other. Therefore, the forged APs can be detected. Both the supplicant and the authentication server need to have valid certificates when using EAP-TLS.

- EAP-TTLS [9]: EAP-TTLS extends EAP-TLS to exchange additional information between the supplicant and the authentication server by using the secure tunnel established by TLS negotiation. An EAP-TTLS negotiation comprises two phases: the TLS handshake phase and the TLS tunnel phase. During phase one, the TLS process is used for the supplicant to authenticate the authentication server by using certificates. In phase two, the authentication of the supplicant can use any non-EAP protocols [10].

To apply these protocols mentioned above to the user's device, the user has to know how to setup these authentication protocols. Accordingly, it needs a simple and easy way to authenticate the home network users. In this paper, we consider the home network user who is not familiar with the authentication method. We also discuss how to provide automatic authentication mechanism for the users.

III. SECURITY MECHANISMS FOR HOME NETWORK

A. Access control scenarios

It is required to consider computer knowledge as well as various ages of users in home network environment. However, the current implementation of WLAN security mechanisms is very difficult to use for common users because users have to access to the parameter setting window of WLAN stations and APs, and edit authentication parameters which are not familiar words.

To solve this problem, we suggest several access control scenarios. These scenarios give secure network environment to the home network users.

- Scenario 1: the use of a password
We assume that WLAN stations and APs have the interface to input the password. The password is changed periodically by software without user's participation.
• Scenario 2: the use of a storage device
The home network service provider gives a user a storage device such as a USB memory stick which contains an authentication installation file. When the user plugs it directly into the WLAN stations, an authentication setup file is installed automatically. If the installed authentication file uses password method, it will be also changed periodically without user’s participation.

• Scenario 3: the use of a MAC address
We assume that a WLAN station seller registers a MAC address of the purchased device at the service provider’s MAC address server. Then authentication procedure is executed automatically between the WLAN station and the authentication server in home. But a hacker can steal services by using an eligible user’s MAC address because the MAC address can be known by sniffing the air traffic. Therefore we use the MAC address method at the first time and then change the password method in which password is changed periodically.

• Scenario 4: the use of a certificate
A WLAN station seller downloads a certificate for authentication to the WLAN station from a certification authority (CA). After this procedure, it is authenticated by the certificate in the home network environment.

• Scenario 5: the use of both the password and the certificate
This scenario combines the password method and the certificate method. A user’s WLAN station uses only the password and an authentication server uses the certificate to be authenticated. The user enters the password at the first time to access the home network and the mutual authentication is operated by using the password and the certificate. After that, the password is changed periodically and automatically.

B. The proposed protocol
To support the mentioned scenarios, the authentication protocol requires additional message exchanges including information which is not specified in Standards. Periodic changes may be problems from the viewpoint of users, when the password is changed while a user takes the WLAN station out of home. The WLAN station needs to be authenticated again when the user brings the WLAN station back to home. However the WLAN station can not obtain the authority without user’s assistance since the password is already changed. Other devices in home network also are needed to know the new password to keep the authority.

The proposed protocol solves the problem by adding the authentication count number. The authentication count number is an index number which corresponds to each password. It is numbered randomly whenever the password is changed. The authentication server manages two tables. One is the MAC address management table which records the MAC addresses of the authenticated devices and the authentication count number. The other is the authentication count number table. When the password is changed, the password and the authentication count number are recorded in the authentication table. For example, there is a device which has the MAC address of EACB. After the device is authenticated when the password is 56789, the server records its MAC address with the current authentication count number in the MAC address management table as shown in Table I. Then the server transmits the current authentication count number to the device. In this case, the current authentication count number is 1. When the password is changed to 12345, as shown in Table II, the authentication count number is also changed to 3 and recorded in the authentication count number table.

Fig. 3 presents the EAP-TTLS procedure to support the proposed authentication protocol. In this figure, the solid lines represent legitimate message exchanges and the dashed lines indicate supplementary message exchanges. As shown in Fig. 3, the EAP-TTLS procedure by using the authentication count number is as follows.

1. The user’s WLAN station associates with an AP using open authentication with wired equivalent privacy (WEP) turned off. Then the AP asks for the user’s identity.
2. The WLAN station transmits an EAP-request message encapsulated in an EAPoL-EAP frame to the AP, which contains the MAC address of the WLAN station.
3. The server is authenticated to the WLAN station using its security certificate and a TLS connection is established between them. The encryption key for the TLS connection will be used for air traffic encryption.
4. Inside the TLS connection (inside box), the exchanged messages are encapsulated into TLS records that are again encapsulated into EAP-request and EAP-response messages. In the existing protocol, the WLAN station informs the AP of a user name and a password. In addition, we propose that the WLAN station sends the authentication count number in the same EAP-Response message. After receiving it, the AP relays it to the server.
5. The server then verifies the authentication count number whether the MAC address and the authentication count number of the WLAN station same as the stored data in the MAC address management table. If the authentication count number is verified, the server will complete the course of authentication by using the password corresponding to the authentication count number table. At this point, the authentication method is

---

<table>
<thead>
<tr>
<th>Table I. The MAC Address Management Table</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC address</td>
</tr>
<tr>
<td>EACB</td>
</tr>
<tr>
<td>ABCD</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Table II. The Authentication Count Number Table</th>
</tr>
</thead>
<tbody>
<tr>
<td>authentication count number</td>
</tr>
<tr>
<td>-------------------------------</td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td>3</td>
</tr>
</tbody>
</table>
able to use many protocol. Here, we assume that CHAP is used.
6. After authenticating the WLAN station, the server transmits the current authentication count number and the password to the WLAN station through the AP. The WLAN station which received the current authentication information updates the authentication information for itself.
7. The server rewrites the authentication count number in the MAC address management table after receiving EAP-Response message.
8. The EAP-TTLS procedure ends by sending the EAP-Success message to the WLAN station.

In this paper, we use the EAP-TTLS protocol since the username, password and authentication information are protected by the TLS connection. The proposed protocol also can be applied to EAP-MD5, EAP-TLS and other protocols. To inform the authentication count number from the WLAN station to the server, the WLAN station sends its authentication count number and MAC address together with identity.

If the password used at the server is different from the password used at the WLAN station, before the success message transmission, the server sends the message that contains authentication information and updates the table. However there is a risk of man-in-the-middle attacks by which the current password and authentication information can be stolen. Hence we suggest that the transmitted information is encrypted by the password like TTLS protocol.

C. Packet format

The format of EAP packet is shown in Fig. 4, and (a) is the EAP packet format and (b) is the EAP-TLS packet format.

Code is one byte indicating the type of packet: 1 indicates Request, 2 indicates Response, 3 indicates Success and 4 indicates Failure. Identifier is a value in the range 0-255 and it should be incremented for each message transmission. This helps to check which Response goes with which Request. Length is the total number of bytes in the EAP message. The Type field indicates the type of Request or Response. For example, 1 means the identity packet and 13 means the EAP-TLS packet. The Data field is the actual request or response data being sent. The format of the data field is determined by the Code field. If the Code field is 3 or 4 that is a success or a failure, these messages contain no data. In case of EAP-TLS, Data field is divided into more parts as shown in Fig. 4 (b). L, M, S, R, and V are flags which mean the length included, more fragments, start flag, Reserved, and Version number respectively.

For the backward compatibility, the proposed protocol uses the same packet format. In case of the EAP-TTLS protocol, we can use the existing packet format because the packet format for new messages and the additional information is able to use the same format as other messages. We change only the reserved bit with the C bit that means the authentication count number is included. If the C bit is set in the EAP message, it means that the message includes the authentication count number or the authentication information.

But when EAP-MD5 or EAP-TLS is used, the authentication count number is added to identity message. The authentication server can not separate the authentication count number from the user’s identity. Therefore, it needs a new type instead of 1 which means the identity. It can be other number for the Type field. In addition, the Data field can be divided into two parts: the former part is used for the authentication count number and the latter part is used for the identity. Additional messages that carry the authentication information are used in the same packet format as EAP-TTLS.

IV. PERFORMANCE EVALUATION

A. Security analysis

EAP-MD5 is more vulnerable to unwanted attacks than other authentication methods. One of such attacks is a brute force attack. A brute force attack is a method of defeating a cryptographic scheme by trying a large number of possibilities, for example, exhaustively working through all possible keys in order to decrypt a message. To protect the brute force attack, at least, the password should be changed by every month. The proposed protocol is robust to the brute force attack since it changes the password periodically.

It also helps to detect a replay attack. By using the replay attack, an attacker could pretend to be an authorized user to access a network. For example, an attacker could simply
intercept and replay a station's identity and password hash to be authenticated. When a user doesn’t use the authentication count number, a hacker can receive the challenge message and transmit the response message repeatedly. On the contrary, when the authentication count number is used, a hacker also should know it. It is easy to know user’s identity. But it is not easy to know the authentication count number because it is transmitted under encryption in the previous authentication procedure. Therefore, the server can detect a hacker who uses the authentication count number invalid.

In case of the mutual authentication, these security problems will be eliminated. Instead of security, the proposed protocol gives automatic re-authentication under the environment the password is changed.

B. Scalability

Since the server has to manage two tables, we need to calculate the required memory size for practical implementation. First of all, for the MAC address management table, the MAC address consists of 6 bytes and the authentication count number occupies 1 byte on the assumption whose range is from 0 to 255. The authentication number in the authentication count number table also occupies 1 byte like the MAC address management table. And if the password uses the WEP2 encryption, it will require the memory size of 16 bytes. If we assume that there are 30 WLAN stations and 100 records of the changed password, the total required memory capacity is 1.91 Mbytes. We calculate the total memory size by

\[
\text{total memory size} = (6+1) \text{bytes} \cdot N_p + (16+1) \text{bytes} \cdot N_c
\]

where \(N_p\) is the number of WLAN stations and \(N_c\) is the number of the used authentication count number.

V. Conclusion

We introduced secure and convenient mechanisms for home network WLAN access. We also proposed the authentication protocol to provide the automatic authentication when the password is changed. The automatic password change method enables users to use the home network without periodic password change. Under the threats we considered, the proposed protocol appeared to give a protection against a brute force attack and a replay attack. Although the password used before is changed for some reasons, the users do not need to enter the new password or other information again. From the viewpoint of users, the mechanisms applied in the proposed protocol are convenient since users do not need to know the authentication mechanism.

For the backward compatibility between the authentication methods, we modified the packet format using a reserved bit. The C bit is added for the authentication count number and the new type number which indicates not only the user’s identity but also the authentication count number should be used.

Compared with the current security set up procedure for WLAN, the proposed protocol can provide a simple procedure for WLAN users and protect them from unwanted attacks in home network environment.

REFERENCES