12

Designs of a Secure Wireless LAN Access Technique and an Intrusion Detection System for Home Network

Taesub Kim[1], Yikang Kim[1], Byungbog Lee[3],
Seungwan Ryu[2] and Choongho Cho[1]
[1]*Department of Computer and Information Science, Korea University,*
[2]*Department of Information Systems, Chung-Ang University,*
[3]*Electronics and Telecommunications Research Institute*
Korea

1. Introduction

Home network service has been integrated with various communication technologies to help people have a more convenient life. It is expected that wireless LAN (WLAN), Bluetooth, ultra wide band (UWB), and Zigbee will be used in home networks 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 in that access points (APs) cannot control the transmission range. This property allows the neighbor or person in the next house to receive the traffic and a malicious intruder to subvert the privacy. Therefore, authentication mechanisms have to be considered so that only an eligible user is authenticated to use the resources of a home network.

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

In this research, we propose access control mechanism considering the convenience of users, secure authentication protocol, and the intrusion detection system to support access control mechanism. Section II presents related literatures. In Section III, we propose authentication mechanism and the intrusion detection system for home network. The performance analysis of the proposed security mechanisms is presented in Section IV. Finally Section V concludes the research.

2. Related literatures

2.1 EAP (Extensible Authentication Protocol)

Extensible Authentication Protocol (EAP) is a mechanism that defines a standard message exchange between devices using an agreed upon authentication protocol. EAP is used as one of the base technologies to allow both wired and wireless clients to authentication to network devices. Because the EAP protocol does not require the IP protocol to communicate (it uses the link layer), it can transport messages between devices without the EAP clients requiring an IP Address. EAP is effective in networks that rely on DHCP for their IP addresses - as the client will not be able to retrieve an IP address from the DHCP server until they are authenticated to the network and given a network connection.

EAP by itself cannot be used as an authentication protocol - as it is merely a standard by which to exchange authentication messages between a client and an authentication server. EAP supports a number of authentication protocols to provide security during the authentication process. The security features and encryption strength vary with each EAP authentication protocol allowing companies to choose which EAP authentication protocol makes the most sense for their 802.1X application.

EAP is a method of conducting an authentication conversation between a Client/supplicant, Authenticator and an authentication server.

* Client/Supplicant: The client, or supplicant, is the device that needs to be authenticated. The client supplies the authentication credentials (such as certificate or username and password information) to the authenticator and requests access to the network. The client uses EAP Over LAN (EAPOL) to talk to the authenticator. Examples of clients include workstations (both wired and wireless), PDA's, and wireless Voice Over IP phones.

* Authenticator: The authenticator is the device performing the 802.1X port-level security and it controls access to the network. The authenticator receives the user credentials from the client, passes it onto the authentication server, and performs the necessary block or permit action based on the results from the authentication server. Depending on the EAP authentication protocol negotiated between the client and authentication server, the authenticator relays the necessary messages between the client and authentication server to facilitate the authentication request.

The authenticator can operate in two different modes: it can perform the EAP messaging functions locally and communicate with the authentication server using the RADIUS protocol or it can operate as an EAP pass-through device to allow the authentication server to perform the necessary EAP protocol messaging functions. Examples of authenticators include network switches and routers (wired network application) and wireless access points or wireless gateway switches.

Authentication Server: The authentication server validates the user's credential information from the client and specifies whether or not access is granted. The authentication server also specifies the EAP authentication protocol to be used between the client and itself and may specify optional parameters once access is granted. Optional parameters may be used to authorize access to specific areas of the network using dynamic VLAN or user policies. Examples of authentication servers include RADIUS and Active Directory servers.

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.

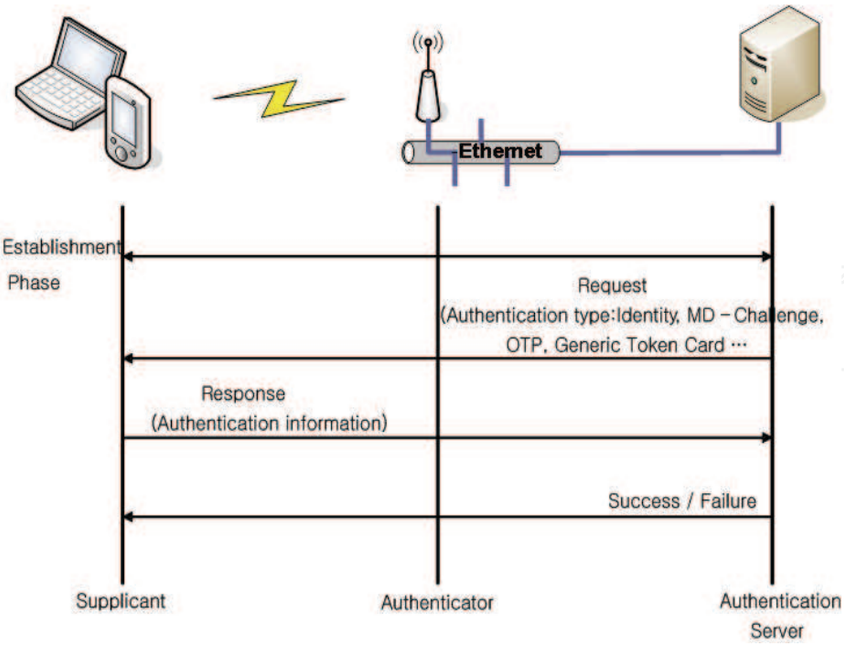


Fig. 1. EAP-based authentication procedure flow

* EAP-MD5: EAP-MD5 is the base security requirement in the EAP standard and uses username and passwords as the authentication credentials. EAP-MD5 protects the message exchange by creating a unique "fingerprint" to digitally sign each packet to ensure that the EAP messages are authentic. EAP-MD5 is very "light weight" and performs its operations very quickly, making it easy to implement and configure. EAP-MD5 does not use any PKI certificates to validate the client or provide strong encryption to protect the authentication messages between the client and the authentication server. This makes the EAP-MD5 authentication protocol susceptible to session hijacking and man-in-the-middle attacks. EAP-MD5 is best suited for EAP message exchanges in wired networks where the EAP client is directly connected to the authenticator and the chances of eavesdropping or message interception is very low. For wireless 802.1X authentication, stronger EAP authentication protocols are used.
* EAP-TLS: EAP-TLS (Transport Level Security) provides strong security by requiring both client and authentication server to be identified and validated through the use of PKI certificates. EAP-TLS provides mutual authentication between the client and the authentication server and is very secure. EAP messages are protected from eavesdropping by a TLS tunnel between the client and the authentication server. The major drawback of EAP-TLS is requirement for PKI certificates on both the clients and the authentication servers - making roll out and maintenance much more complex. EAP-TLS is best suited for installations with existing PKI certificate infrastructures. Wireless 802.1X authentication schemes will typically support EAP-TLS to protect the EAP message exchange. Unlike wired networks, wireless networks send their packets over open air making it much easier to capture and intercept unprotected packets.
* EAP-TTLS: Proposed by Funk and Certicom, EAP-TTLS (Tunneled TLS) is an extension of EAP-TLS and provides the benefits of strong encryption without the complexity of mutual certificates on both the client and authentication server. Like TLS, EAP-TTLS supports mutual authentication but only requires the authentication server to be validated to the

client through a certificate exchange. EAP-TTLS allows the client to authenticate to the authentication server using usernames and passwords and only requires a certificate for the authentication servers. EAP-TTLS simplifies roll out and maintenance and retains strong security and authentication. A TLS tunnel can be used to protect EAP messages and existing user credential services such as Active Directory, RADIUS, and LDAP can be reused for 802.1X authentication. Backward compatibility for other authentication protocols such as PAP, CHAP, MS-CHAP, and MS-CHAP-V2 are also provided by EAP-TTLS. EAP-TTLS is not considered full proof and can be fooled into sending identity credentials if TLS tunnels are not used. EAP-TTLS is best suited for installations that require strong authentication without the use of mutual certificates. Wireless 802.1X authentication schemes will typically support EAP-TTLS.

* PEAP: Protected EAP Protocol (PEAP) is an Internet-Draft that is similar to EAP-TTLS in terms of mutual authentication functionality and is currently being proposed by RSA Security, Cisco and Microsoft as an alternative to EAP-TTLS. PEAP addresses the weaknesses of EAP by:

- protecting user credentials
- securing EAP negotiation
- standardizing key exchanges
- supporting fragmentation and reassembly
- supporting fast reconnects

PEAP allows other EAP authentication protocols to be used and secures the transmission with a TLS encrypted tunnel. It relies on the mature TLS keying method for it's key creation and exchange. The PEAP client authenticates directly with the backend authentication server and the authenticator acts as a pass-through device, which doesn't need to understand the specific EAP authentication protocols. Unlike EAP-TTLS, PEAP doesn't natively support username and password authentication against an existing user database such as LDAP. Vendors are answering this need by creating features to allow this. PEAP is best suited for installations that require strong authentication without the use of mutual certificates. Wireless 802.1X authentication schemes will typically support PEAP.

* Cisco LEAP: Cisco's Lightweight EAP Protocol (LEAP) was developed in November 2000 to address the security issues of wireless networks. LEAP is a form of EAP that requires mutual authentication between the client and the authenticator. The client first authenticates itself to the authenticator and then the authenticator authenticates itself to the client. If both authenticate successfully, a network connection is granted. Unlike EAP-TLS, LEAP is based on username and password schemes and not PKI certificates, simplifying roll out and maintenance. The drawback is that it is proprietary to Cisco and has not been widely adopted by other networking vendors. LEAP is best suited for wireless implementations that support Cisco AP's and LEAP compliant wireless NIC cards.

EAP was originally developed for use with PPP in RFC 2284 and has since been widely deployed with IEEE 802 on both wired and wireless networks. With the growing popularity of wireless networks, securing the authentication process between the client, authenticator, and authentication server have become a high priority. Security concerns that were once benign on wired networks have become challenges and open security holes on wireless networks.

Depending on the EAP authentication protocol used, 802.1X authentication can help solve the following security issues:

- Dictionary Attack: Attacker obtains the challenge and response message exchange from a password authentication session and uses a brute force method to crack the password. 802.1X solves this type of attack with the use of TLS tunnels to protect the username and password exchanges between the client and the authenticator.
- Session Hijack Attack: Attacker obtains the packets passed between the client and the authenticator and recovers the identity information of the client. It forces the "real" client off the network through a form of DoS attack and impersonates the client to continue the conversation with the authenticator. 802.1X's authentication abilities with dynamic session-based keys (with user configurable re-keying) can help encrypt the conversation between the client and authenticator to thwart Hijacking attacks.
- Man-in-the-Middle Attack: Attacker obtains the necessary information from the client and the authenticator and inserts their host between the two. The attacker's host becomes the "middle man" and has access to the packets that are passed between the client and the authenticator. Through 802.1X's authentication and dynamic session-based keys (with user configurable re-keying), the data stream between the client and authenticator is encrypted to prevent Man-in-the-Middle attacks.

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 research, 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.

2.2 IEEE 802.1x

IEEE 802.Ix standard specifies how to implement port based access control for IEEE 802 LANs, including wireless LAN. In IEEE 802.1x, the port represents the association between a WLAN station and an AP. Basically IEEE 802.Ix 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.

802.1X port authentication can be coupled with MAC port security for tighter access control (see Figure 2). With MAC port security enabled, the network port can control access through enforcement of the client's MAC address as well as the user's 802.1X credentials.

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 traffics except the EAP messages before the supplicant is authenticated. IEEE 802.Ix 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.Ix standard. Instead, IEEE 802.1x provides RADIUS usage guidelines in the Annex.

The advantages of using 802.1X port-based network authentication include:

- Multi-vendor standard framework for securing the network.
- Improves security through session based dynamic keying of encryption keys.
- Standards based message exchange based on EAP.
- Uses open security architecture allowing the addition of newer authentication methods without replacing network equipment.

- Uses industry standard authentication servers (example: RADIUS).
- Centralizes management for network access.
- Uses existing user security information, if necessary.
- Supports both wired and wireless networks.

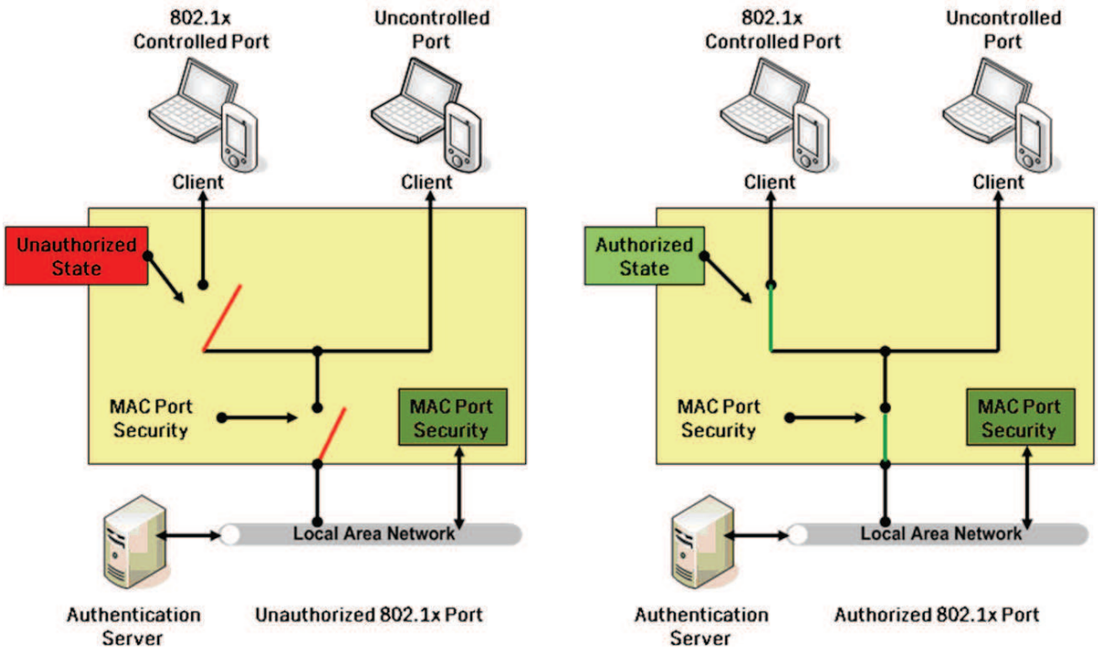


Fig. 2. 802.1x port authentication

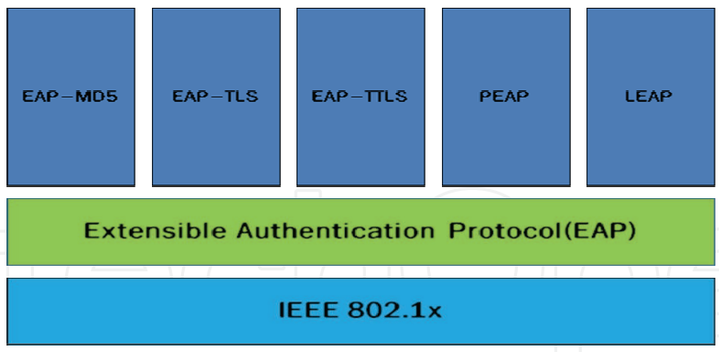


Fig. 3. 802.1x authentication components

2.3 IEEE 802.11i

IEEE 802.11i provides enhanced security in the medium access control (MAC) layer for IEEE 802.11 networks. 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 Figure. 4, 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.

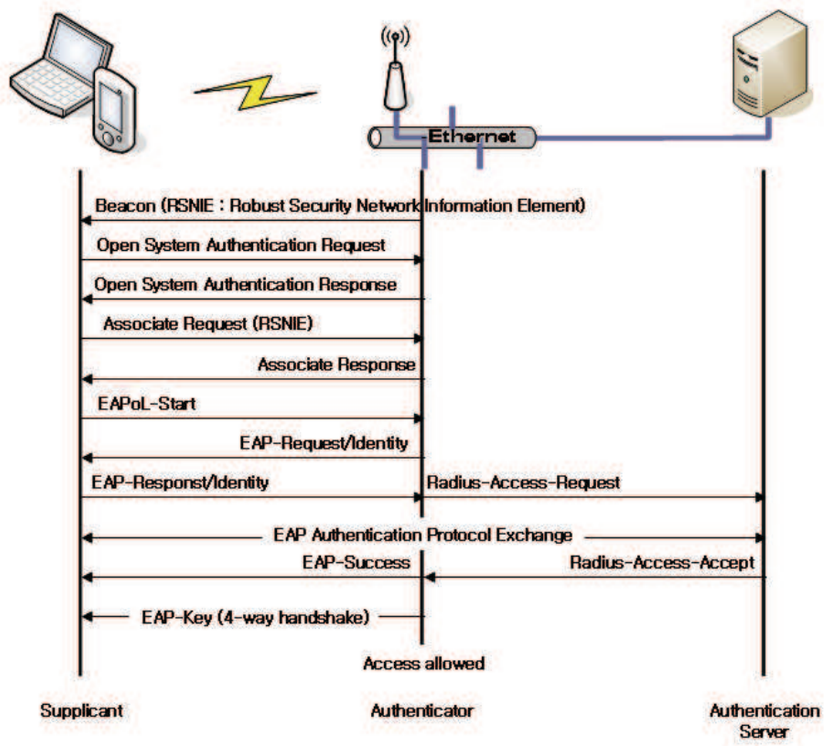


Fig. 4. IEEE 802.11i-based authentication procedure flow

2.4 SNMP (Simple Network Management Protocol)

The SNMP is a management protocol used to manage TCP/IP networks. Nowadays, it is widely used in several commercial networks, since it is a relatively simple protocol, but powerful enough to be used in the management of heterogeneous networks. The SNMP management comprises an agent, a manager and a MIB (Management Information Base), as shown in Figure. 5 The MIB is a database composed of objects that will be managed and/or monitored through the SNMP protocol. A manageable object represents a real resource in the network, such as a rotator, a switch and also the final system resources, like, for example, CPU, memory, etc. Each manageable object has a set of variables of which values can be read or altered by the agents.

The management agent is a software resident in a final system or in some network device about to be managed that collects information from the MIB and send it to the managing process. The latter (NMS - Network Management System) resides in a management station (by acting remotely), or in a local station (by acting in the site) and sends messages to the agent processes in order to read or alter the value of a manageable object. The agents use SNMP primitives to read or change the values of the MIB objects. These are some examples of primitives: get-request, get-response, getnext, set-request and trap.

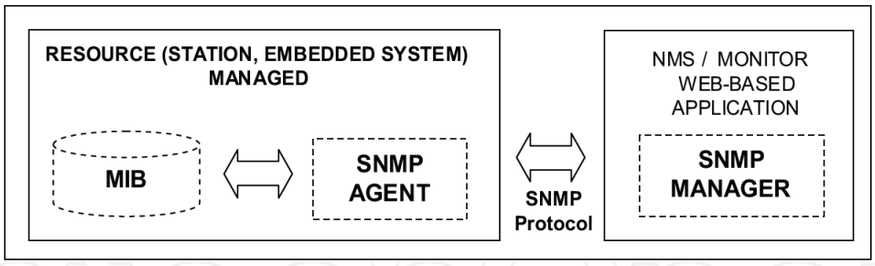


Fig. 5. Relation between components of the SNMP management

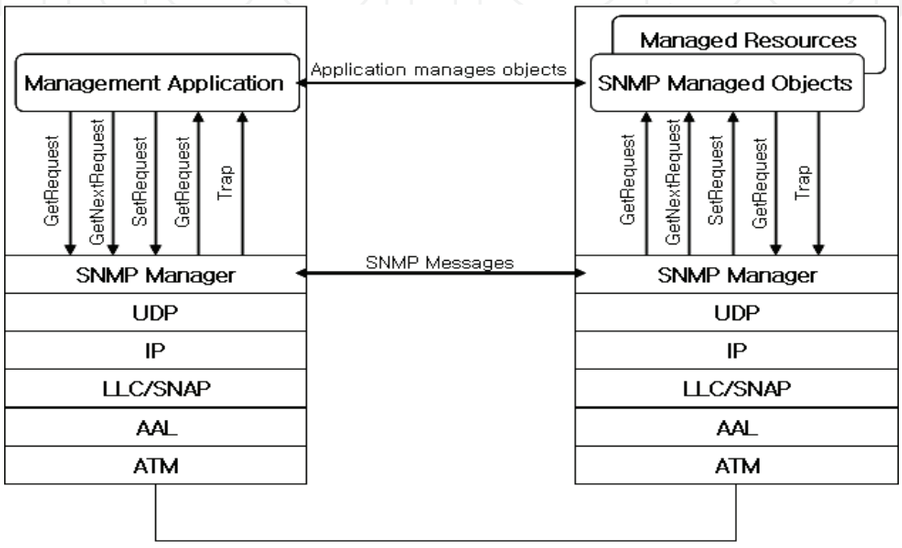


Fig. 6. SNMP management system architecture

3. Design of the security home gateway server

A security home gateway server is proposed to guard the access to the network. The security home gateway server collects and processes security related information from managed devices. It acts as the entry security provider for guarding the proper usage of upper layer application services, such as alarm reporting. Among these network management applications, both type of alarm reporting are of interest in this research. As shown in Figure. 7, this security home gateway server consists of five management units: traffic collection unit, traffic processing unit, authentication unit, policy management unit, and response unit. The gateway also cooperates with an authentication server to guarantee a secure link layer access control. Also to protect intrusion detection the AP must support SNMP agent functions and the security home gateway sever must support SNMP server functions.

Traffic Collection Unit: The unit collects traffic from routers, access points among other devices. The communication information can be obtained by log files, traffic mirror, or by polling SNMP agents on managed devices. The gathered information is passed to traffic processing unit for further classification and computation.

Traffic Processing Unit: This unit processes the data from the traffic collection unit. For example, Data packages are classified according to the type of ICMP, TCP, UDP, SNMP and

others. such as IP source and destination addresses. All data are stored in the database associated with timestamps.

Authentication Unit: This unit works together with APs. It is responsible for a port-base access control protocol, as specified in 802.1x. The authentication request, issued by a wireless client, is passed, by AP's forwarding feature, to the RADIUS server for verification. Using the information replied from the RADIUS server, access policy of the requesting client can be determined at AP. The authentication results are passed to behavior analysis unit for further processing.

Policy Management Unit: According to the vulnerabilities and threats we described in last section, there exist certain patterns for each potential security flaw. The characteristics of each attack or abnormal behavior are analyzed and predefined as security policies. Depending upon the management requirement, a policy could also be updated by security configuration management.

Response Unit: The response unit is responsible for notifying the network management server an abnormal behavior or for updating security configuration. Management applications of alarm reporting react upon receiving the messages from response unit correspondingly.

All five management units are integrated together to provide precaution security application services. Specifically, by cooperating with an authentication server, access control in the link layer is provided; by monitoring and analyzing data packages, the security threats prevention can be achieved in IP layer.

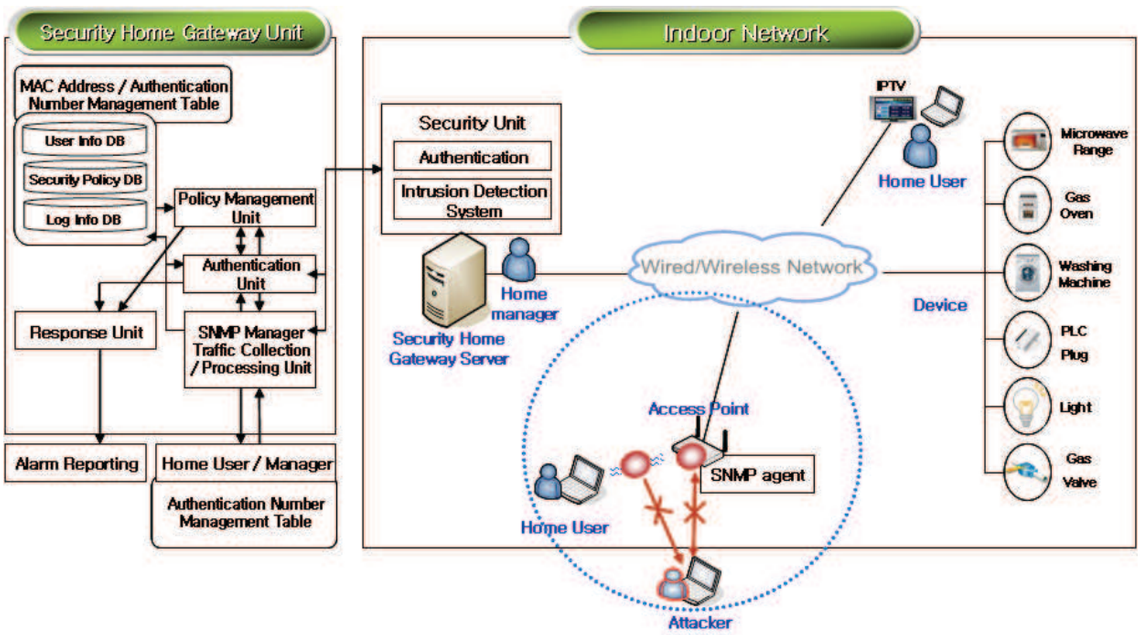


Fig. 7. Security home gateway system server architecture

3.1 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't 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.

MAC Address	Authentication number
00:00:F0:7A:B1:B7	1
00:00:F1:7A:B4:77	2
00:00:F1:8A:BB:A7	3
...	...

Table 1. The MAC address management table

Authentication Number	Password
1	1234
2	5678
3	9123
...	...

Table 2. The authentication number management table

The proposed protocol solves the problem by adding the authentication number. The authentication number is an index number which corresponds to each password. It is numbered randomly whenever the password is changed. The security home gateway server manages two tables. One is the MAC address management table which records the MAC addresses of the authenticated devices and the authentication number. The other is the authentication number table. When the password is changed, the password and the authentication number are recorded in the authentication table. For example, there is a device which has the MAC address of 00:00:F0:7A:81:B7. After the device is authenticated when the password is 1234, the server records its MAC address with the current authentication number in the MAC address management table as shown in Table 1. Then the server transmits the current authentication number to the device. In this case, the current authentication number is 1. When the password is changed to 5678, as shown in Table 2, the authentication number is also changed to 2 and recorded in the authentication number table. Figure. 8 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 Figure. 8, the EAP-TTLS procedure by using the authentication 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 both the old authentication number and authentication status in the same EAP-Response message. After receiving it, the AP relays it to the server.
5. The server then verifies the old authentication number to determine whether the MAC address and the old authentication number of the WLAN station are the same as the stored data in the MAC address management table.
6. After the old authentication number is authenticated by the WLAN station, the server transmits the new authentication number to the WLAN station through the AP. The WLAN station which received the new authentication number information updates the authentication information for itself. The server will complete the course of authentication by using the password corresponding to the authentication number table. At this point, the authentication method is able to use many protocol. Here, we assume that CHAP is used.
7. The EAP-TTL procedure ends by sending the EAP success message to the WLAN station.

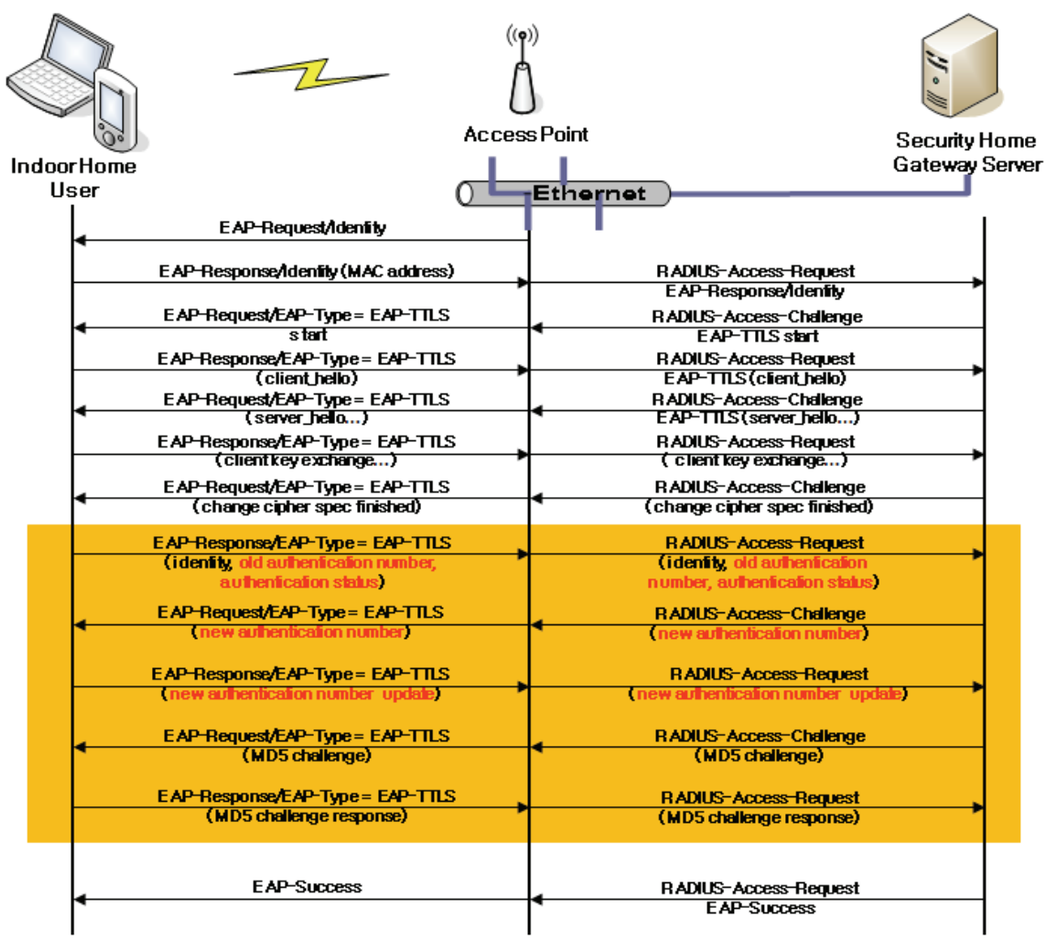
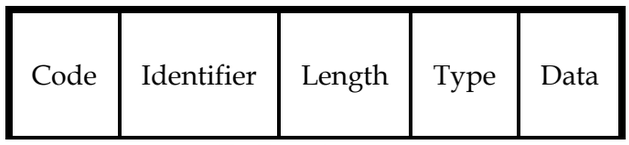


Fig. 8. The proposed protocol flow

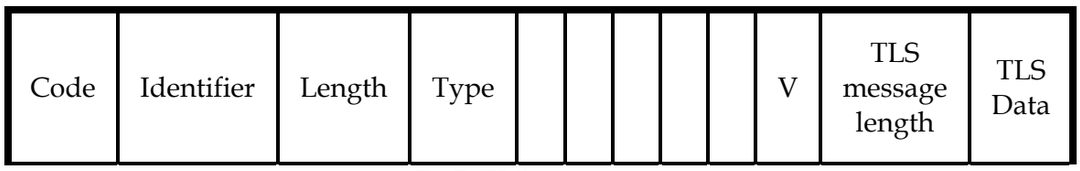
In this research, we use the EAP-TTLS protocol since the user name, password and authentication information are protected by the TLS connection. The proposed protocol also can be applied to EAP-MD5, EAP-TLS and other protocols. To inform the new authentication number from the server to the WLAN station,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

3.2 Packet format

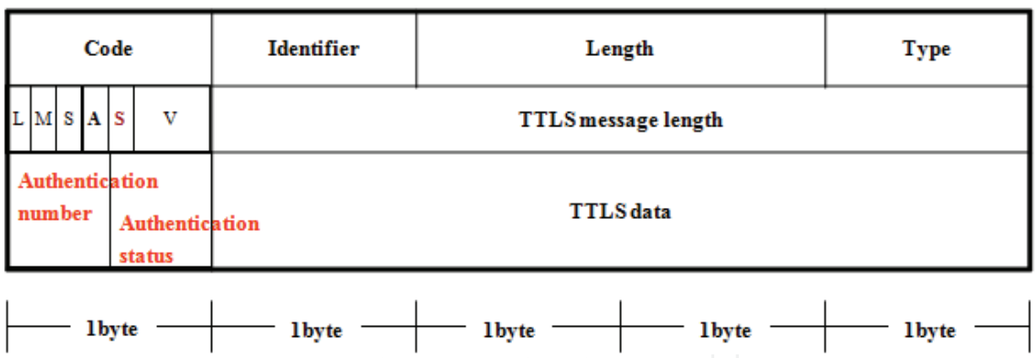
The format of EAP packet is shown in Figure. 9, (a) is the EAP packet format, (b) is the EAP-TLS packet format, and (c) is the proposed packet format



(a) EAP packet format



(b) EAP-TLS packet format



(c) The proposed packet format

Fig. 9. 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 Figure. 9 (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 number is included. If the C bit is set in the EAP message, it means that the message includes the authentication number or the authentication information. But when EAP-MD5 or EAP-TLS is used, the authentication number is added to identity message. The authentication server can't separate the authentication 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 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.

3.3 The proposed intrusion detection system

In the proposed intrusion-detection system, the secure home-gateway server (i.e., SNMP server) identifies whether or not the terminal node is an authenticated MAC address by polling (See Figure. 7). If this MAC address is violated, an alarm message notifies the response unit inside the home. This solves some leakage. Now the user should enroll the MAC address of the AP. Additionally, SNMP can obtain some traffic information (i.e., ICMP, TCP and UDP, etc.). If this traffic quantity is increased beyond a specific threshold, the user may consider it an intentional/unintentional leakage (i.e., an attack of intentional connection or DoS attack). Thus, the response unit warns of the leakage inside the home by giving an alarm message.

4. 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 number, a hacker can receive the challenge message and transmit the response message repeatedly. On the contrary, when the authentication 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 number because it is transmitted under encryption in the previous authentication procedure. Therefore, the server can detect a hacker who uses the authentication 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.

4.1 Password dictionary attack

A method used to break security systems, specifically password based security systems, in which the attacker systematically tests all possible passwords beginning with words that have a higher possibility of being used, such as names and places. The word dictionary refers to the attacker exhausting all of the words in a dictionary in an attempt to discover the password.

This research proposes authentication scenarios to minimize the process needed by users, a password method which is changed randomly and periodically, and authentication protocols. Also because it added a new parameter, being safe consequently, more it will be able to provide the home network environment which is convenient.

4.2 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 number, a hacker can receive the challenge message and transmit the response message repeatedly. On the contrary, when the authentication 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 number because it is transmitted under encryption in the previous authentication procedure. Therefore, the server can detect a hacker who uses the authentication number invalid. In our authentication protocol, additional parameters (i.e., old authentication number and authentication status) are padded into challenge response messages, thus protecting from replay attack

4.3 Denial of service and rogue attack

A DoS(Denial of Service) attack is a malicious attempt by a single person or a group of people to cause the victim, site, or node to deny service to its customers. When this attempt derives from a single host of the network, it constitutes a DoS attack. On the other hand, it is also possible that a lot of malicious hosts coordinate to flood the victim with an abundance of attack packets, so that the attack takes place simultaneously from multiple points. This type of attack is called a Distributed DoS, or DDoS attack, exactly an attacker overloads an AP in various ways so that the AP is unable to serve legitimate users. The attacker does not directly benefit but creates a nuisance, and rogue station attack is a rogue station affinitizing itself with an AP. The attacker benefits by becoming a participant in the wireless network and thus gaining the ability to send and receive data.

In our authentication protocol, additional parameters (i.e., old authentication number and authentication status) are padded into challenge response messages, thus protecting from denial of service attack and rogue station attack. Also, this proposed intrusion detection system, If this MAC address is violated, alarm message is notified to response unit inside home. This solves some leakage that user should enroll MAC address of AP. Additionally, SNMP can obtain some traffic information(i.e., ICMP, TCP and UDP etc). If this traffic quantity is increased more than specific threshold, user may consider an

intentional/unintentional leakage (i.e., an attack of intentional connection or DoS attack). Thus, response unit alarms the leakage inside home by alarm message.

5. 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 changes. Under the threats we considered, the proposed protocol appeared to give a protection against a dictionary attack, a replay attack, a denial of service attack and a rogue station 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. Also, it used the SNMP protocol so that the inside home user will be able to perceive an attack.

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 number and the new type number which indicates not only the user's identity but also the authentication 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.

6. Acknowledgement

This work was supported by National Research Foundation of Korea Grant funded by the Korean Government(KRF-2007-313-D00503)

7. References

B. Aboba et al. (2004). Extensible Authentication Protocol, *IETF RFC* 3748.

B. Aboba, D. Simon. (1999). PPP EAP TLS Authentication Protocol, *IETF RFC* 2716.

B. Aboba. (1999). PPP EAP TLS Authentication Protocol, *IETF RFC* 2716.

C. He and J. C. Mitchell. Security Analysis and Improvements for IEEE 802.1li, in proc. the *12th Annual Network and Distributed System Security*.

Chih-Mou Shih, Shang-Juh Kao. (2006). Security Gateway for Accessing IPv6 WLAN, *ICIS-COMSAR* 2006, pp83~88.

D. Potter et al. (2002). PPP EAP MS-CHAP-V2 Authentication Protocol, internet draft.

F. Baker. (1997). IP Forwarding Table MIB, RFC 2096.

H. Luo and P. Henry. (2003) A Secure Public Wireless LAN Access Technique That Supports Walk-Up Users, in *proc. GLOBECOM2003*, vol. 22, no. 1, pp. 1415-1419.

IEEE Std 802.11i. Medium Access Control(MAC) security Enhancements, 2004 edition.

IEEE Std 802.1x. Standard for port based Network Access Control, March 2001.

IEEE, LAN/MAN Specific Requirements - Part 11: Wireless Medium Access Control(MAC) and Physical Layer(PHY) Specification: Specification for Robust Security, *IEEE Std* 802.11i/D3.2, Apr. 2003.

J. C. Chen and Y. P. Wang. Extensible Authentication Protocol (EAP) and IEEE 802. lx: *Tutorial and Empirical Experience*, http://wire.cs.nthu.edu.tw/wirelx/.

J.D. Case, M. Fedor, M.L. Schoffstall, J. Davin. (1990). Simple Network Management Protocol(SNMP), RFC 1157.

Ju-A Lee, Jae-Hyun Kim, Jun-Hee Park, Kyung-Duk Moon. (2006). A Secure Wireless LAN Access Technique for Home Network, *VTC* 2006, pp818~822.

K. McCloghrie, Ed. (1996). SNMPv2 Management Information Base for the Internet Protocol using SMIv2, RFC 2011.

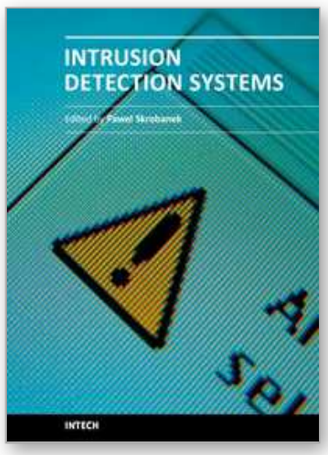
K. McCloghrie, Ed. (1996). SNMPv2 Management Information Base for the Transmission Control Protocol using SMIv2, RFC 2012.

K. McCloghrie, Ed. (1996). SNMPv2 Management Information Base for the User Datagram Protocol using SMIv2, RFC 2013.

L. Blunk, j. Vollbrecht. (1998). PPP Extensible Authentication Protocol(EAP), *IETF RFC* 2284.

P. Funk. (2004). EAP Tunneled TLS Authentication Protocol, internet draft.

W. Simpson. (1994). PPP Chanllenge Handshake Authentication Protocol (CHAP), *IETF RFC* 1994.



Intrusion Detection Systems

Edited by Dr. Pawel Skrobanek

ISBN 978-953-307-167-1

Hard cover, 324 pages

Publisher InTech

Published online 22, March, 2011

Published in print edition March, 2011

The current structure of the chapters reflects the key aspects discussed in the papers but the papers themselves contain more additional interesting information: examples of a practical application and results obtained for existing networks as well as results of experiments confirming efficacy of a synergistic analysis of anomaly detection and signature detection, and application of interesting solutions, such as an analysis of the anomalies of user behaviors and many others.

How to reference

In order to correctly reference this scholarly work, feel free to copy and paste the following:

Taesub Kim, Yikang Kim, Byungbog Lee, Seungwan Ryu and Choongho Cho (2011). Designs of a Secure Wireless LAN Access Technique and an Intrusion Detection System for Home Network, Intrusion Detection Systems, Dr. Pawel Skrobanek (Ed.), ISBN: 978-953-307-167-1, InTech, Available from: http://www.intechopen.com/books/intrusion-detection-systems/designs-of-a-secure-wireless-lan-access-technique-and-an-intrusion-detection-system-for-home-network

INTECH
open science | open minds

InTech Europe
University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

InTech China
Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821

IntechOpen