A Security Framework for Archiving the Permission of Mobile Terminal in Wireless Environment

Byung-Kil Byun, Ki-Young Lee, *Member, KIMICS*

***Abstract*— Traditional voice traffic over mobile communication has been changed into data and media contents traffic, which makes traffic amount increases and speedy data transfer required. In the near future ubiquitous mobile terminal environment will be common so that security issues will arise due to many heterogeneous equipments and connections. In this paper, many previous methods used for terminal authentication are examined. And we propose new system model which uses our novel user authentication protocol based on strong one-time password (OTP) and short message service (SMS). We verify our system model and protocol by implementation.**

***Index Terms*— Wireless network security, OTP, SMS, Authentication server algorithm**

I. INTRODUCTION

SINCE DynaTAC (the cellular phone) was introduced over the wireless environment by the Motorola, Inc. in 1983, the mobile users have increased rapidly now more than 4.1 billion users in 26 years, which tells 68% of the whole population in the world. The rapid increase of the mobile users, who experienced the IP and WWW, can develop also the technology of the wireless LAN and 3G in order to meet the requirements of the users who want to use the web service without wire anywhere and anytime.

Due to this technological development of the wireless network environment, there has been explosive demand of the wireless notebook and smart phone. It is evolved that information is transferred by communication between cellular phones and notebooks. For example, while a person is working on PC at home, he/she can receive a call through the Internet. Also while a person left home, he/she can receive a call through his/her smart phone. Even in the time of driving to the office, a person can arrange the meeting by calling to the office. During the teleconference call he/she can make other members to join the conference. The technological development and products enable the above scenarios, not in the future but in nowadays.

Manuscript received January 31, 2011; revised March 16, 2011; accepted March 30, 2011.

Byung-Kil Byun is with the Dept. of Info & Telecomm Eng., Univ. of Incheon, Incheon, 406-772, Korea (Email: bgbyun@stu.ac.kr), Ki Young Lee (corresponding author) is with the Dept. of Info & Telecomm Eng, Univ. of Incheon, Incheon 406-772, Korea (Email: kylee@incheon.ac.kr)

However, to meet such expectations there must be some unified standard for authentication, authorization, charging and roaming services, which is not limited by the individual ways of the different business entities. Moreover, it is essential that not only voice, data and multimedia services should not be interrupted but also quality assurance by satisfying the QoS should be kept.

All the mobile terminals which implement such high quality services are communicated through data, and media access through this inter communication has become an issue. Each terminal has its own hardware, and in it software and data are operated to provide required services, which exposes fundamental instability. Therefore the need of research arises that not only it should satisfy the user's usability but also apply the security in order to overcome the fundamental instability.

The Public Key Infrastructure (PKI) standard, which has become the de facto standard in the wired environment, has been attempted over the wireless environment for the last two years, but a new standard is required due to the rapid technological development of wireless terminals. In terms of policy and management, a new security technology system is required to interoperate with WI-FI, 3G, and 4G over the network, which exceeds the existing security level. To realize such a high level security, the new system should overcome the weakness caused by many separated heterogeneous security systems, vulnerability of not working well due to interoperation between terminals and different security standards [1] [2]. In a real life, the security measures are ignored to increase usability of mobile terminals. For example, in case of smart phone, from April 2009 DRM which is the multimedia security protocol is not applied and the users are not observing the regulation of privacy protection effected from 2007 due to the distrust of the effect of vaccine software, even though the regulation said that users can be termed in less than three years jail if not properly observed. This means that the security measures should also reflect the user's desire for use of convenience.

Received from the wired network solutions for the safe has been studied several security. And in addition, real-time wireless network security, many studies are underway to strengthen [3]. Therefore in this thesis I would like to study about improvement of the security application which can be used in real life.

II. RELATED WORKS

Before we explain the wireless LAN password and authentication, we would like to explain first the Public Key Infrastructure (PKI) which has widely used in wired banks and governmental offices. The PKI is a standard of security in wired network. The PKI provides its framework and service in order to create, distribute, manage and identify a public key certificate. The PKI provide data integrity, denial blocking, safe encoding, and authentication of network transaction with applications using the PKI. The PKI can apply the robust security measures and can be used in the area of application level such as not only strong authentication through user's certificate but also signature and encoding. But wireless has not standard of overall representation yet. Since 1999 it was approved as the IEEE 802.11b standard in 1999. The wireless LAN has been used widely in the area of network environment where the wired network cannot be easily installed anything.

In comparison with the relatively simple wired Ethernet protocol, the wireless LAN needs security mechanism to protect the process of authentication of access control.

2.1. Authentication (User authentication, Access Control, Authority verification)

EAP(Extensible Authentication Protocol) used in 802.1x includes EAP-MD5, EAP-TLS(Transaction-Level Security), EAP-TTLS(Tunneled Transport Layer Security), LEAP(Lightweight-EAP),PEAP(Protected-EAP). The EAP-TTLS is used many times due to it providing strong security and net required a certificate from terminal side.[4]

In this chapter, the EAP-TTLS (Extensible Authentication Protocol-Tunneled Transport Layer Security) which is used without a certificate over wireless environment is briefly explained. Brief explanation about One-Time Password (OTP) is presented too.

In case of TTLS, the requester does not request a certificate. Here, two phases are separated and used.

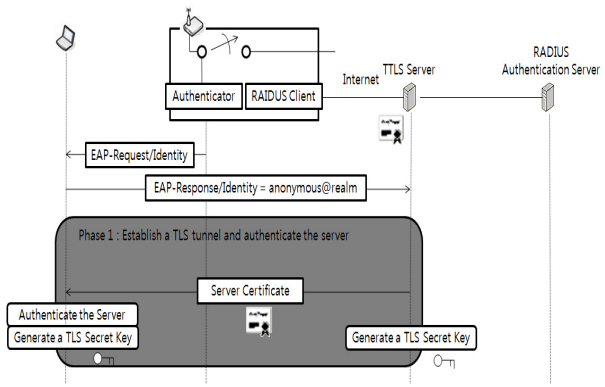

Fig. 1. Diagram of TLS tunnel & server.

1) During Phase 1, the TTLS server sends a certificate to the requester, and requester authenticates the server.

2) Both parties generate the encryption key for TLS using the Key material.

3) During Phase 2, user authentication is performed in the secured TLS tunnel. The authentication server authenticates users by using a variety of EAP authentication methods and existing PAP, CHAP and MS-CHAP-V2 etc in the TLS tunnel.

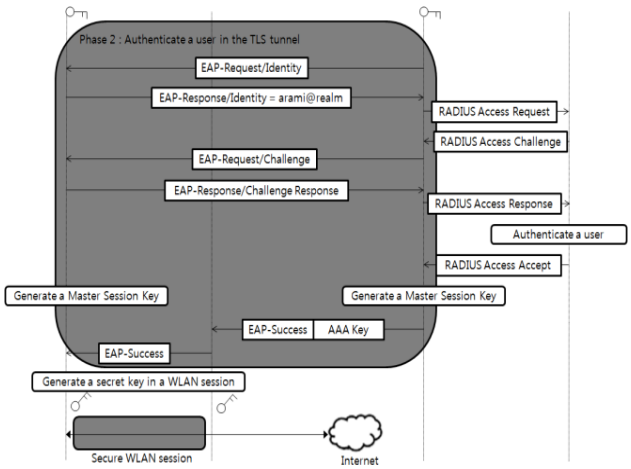

Fig. 2. Diagram of user in TLS tunnel.

4) Upon user authentication completion, the authentication server generates the Master Session Key which will be used as the wireless protection key between requester (terminal) and authenticator (wireless AP), and forward this key to the authenticator.

5) Using the master session key, a user can access the Internet wirelessly.

2.2. Encryption (Data Confidentiality, Data Integrity, Non-Repudiation)

The second method to ensure security over a wireless LAN is Encryption. It refers to data transfer which is securely received by the intending receiver.

Encryption + Authentication = Wireless Security

As above, a combination of encryption and authentication can be a completion of wireless security. The basic WEP authentication process is as follows: Using 24 bit initial vector and 40 bit (or 104 bit) key, a key stream which is obtained through the RC4 algorithm and plain text data are XORed to make and transfer the authenticated passage.

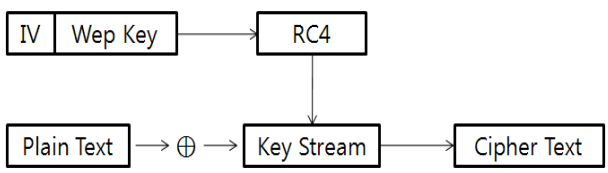

Fig. 3. RC4 stream encryption.

2.3. HOTP (One Time Password)

The one-time password is a password which is generated for one-time session or transaction. This method is easy to use and maintain strong security. Since this method uses a fresh password every time, it is much more difficult to attack by reuse of password compared to using a fixed password. Because passwords are generated by the prediction of traffic usage, it is almost impossible to find the next password generated.

Due to these characteristics, the OTP method has been considered as a secured authentication way. The OTP method can be categorized based on how to generate a password – Time-synchronization between authentication server and user, S/Key algorithm which generates a password based on the previous used password, Challenge – Response and Event Synchronization. The further explanations are described The S/key way is one of the traditional methods which prevent attacks by the reuse of packets which are sniffed in-between during remote log-in process through a public network. The method begins with an initial value which is shared with a user. The initial value is encoded by a hash function which is one of the password generation algorithms. Then this password is compared between a user and server. This way is easy to use and has been considered as a secured way of authentication since it has left no information except the initial value.

The strength of this way is that a hacker, who is successful to sniff a message, cannot find the original text or the hash function used even though he/she sniffs a hash value since a hacker cannot know the initial value. [5]

III. THE PROPOSED SYSTEM DESIGN

3.1. Improving the security performance in wireless

As described in Chap. 2, the well-known standard PKI in wired networks is to authenticate a desktop which is a terminal. In this paper, we focus on the application of security in a wireless network which needs to meet the requirements of mobility and portability.

The wireless environment has vulnerability to security threats such as interruption in AP or servers (DOS Interruption: make unavailable of system resources), Interception (without authorization access to the system assets) as well as interruption, interception, modification and fabrication of data over a communication network

Since the current IEEE 802.11 standard has no policy on data integrity and no strict rule applied, session hijacking and MIM attack are possible.

In the EAP-MD5 currently researched, only uni-directional authentication is provided and no data encryption is supported. The dynamic-WEP, EAP-TLS, EAP-TTLS generate traffic and all require certificate so that they are not applied to the real network environments. Therefore in order to overcome those limitations we propose our novel approach which strengthens security and is more convenient to use than other approaches. [6]

3.2. Improved security performance design techniques

3.2.1. Method to security execute

1) A user runs the client program and chooses a corresponding AP.

2) By entering ID and Password authentication is sent to the authentication server through AP.

3) The authentication server compares the received ID and password with the stored information in its database. If they are the same, OTP is generated and sends it to the user's mobile phone and sets its timer to run.(Fig.4)

4) The user entered the OTP received and sends it to the server to attempt the second authentication.

5) The server accepts or rejects the connection request based on the information received. At this time it might register the user in the connection block list of the Network Management System(NMS) if it does not receive the required information until the timer is expired.(Fig.5)

6) Upon authentication completed, the internet connection is done by applying the encryption method set between AP and client.

The NMS, which is a server for managing users, uses two lists for authenticated users and blocked users respectively.(Fig.6)

Authenticated users are added to the authenticated user list and the AP is checked so that users which are not connected to the AP are removed and the list is renewed on a regular basis.

In case that a user, who attempts to connect to the AP, cannot finish the authentication process before the timer expires, the user is added to the block list and the block list is initialized on a regular basis.

The flow charts for client, authentication server and NMS are as follows respectively:

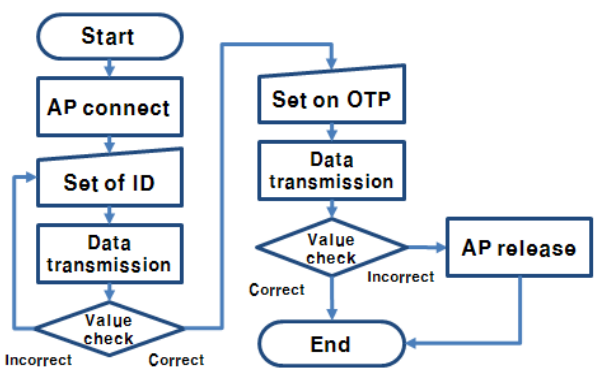

Fig. 4. Flow chart of client side.

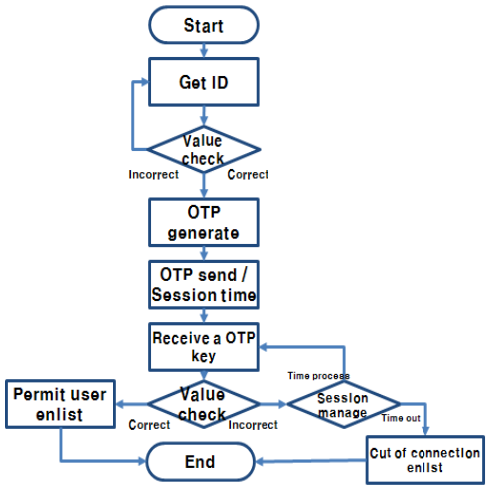

Fig. 5. Flow chart of server side.

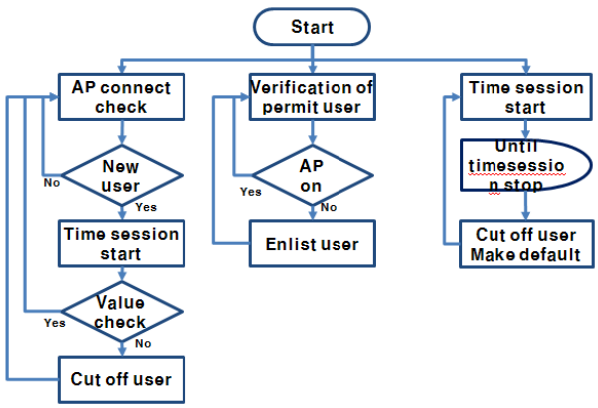

Fig. 6. Flow chart of NMS.

3.2.2. Proposed Method Analysis

The analysis of our proposed protocol on the requirements for the third party attack and its reliability as well as its efficiency is as follows:

Confidentiality: The key value during communication should not be known to the attacker. Since our protocol sends and receives encrypted values as well as using the one time password, the attacker cannot identify them.

Integrity: The authentication server transmits a OTP number using SMS A5/3 KASUMI encrypt algorithm to client and the authentication server authenticates to the client via the OTP number. Each telecommunications by secure connect (tunnel) that is authenticated to the OTP number.

User Authentication: After the authentication server authenticate to the client via ID and Password, the authentication server authenticate to the client via the OTP number again.

Non-Repudiation: The client is authenticated using generated OTP number by the authentication server and the authentication server generates the OTP number by client's id. Because the authentication server used the OTP number in permits client accessing to network, the authentication server cannot deny something.

Authority verify: After the authentication server verifies user's authority by searching for database system in first authentication step, determine processing second authentication step.

IV. IMPLEMANTATION

Radius authentication using complete and at the same time encrypted client information set by OTP server that sent to the client / response to 3G networks. Implemented as designed in the previous section3.2.1, when expressed in a scenario sequence diagram with shown Fig.7 below.

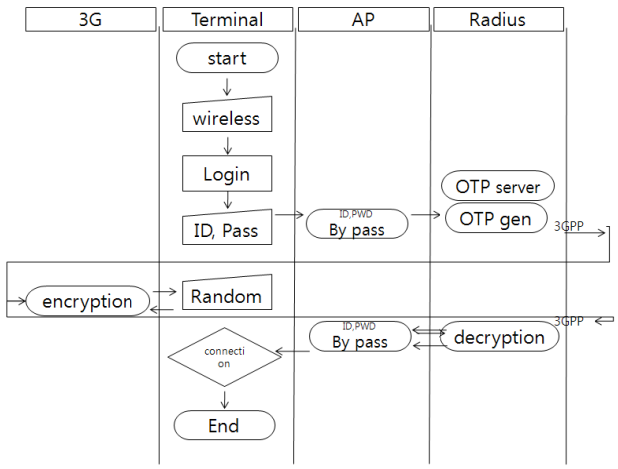

Fig. 7. Sequence diagram of scenario

From the terminal through the following screen, the authentication will start.

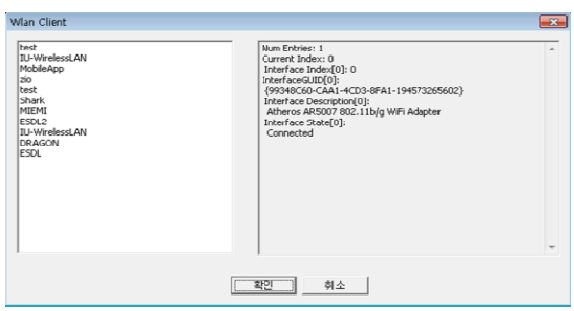

Fig. 8. Powered screen of WLAN Client.

At first, WLAN Client module will run the WLAN observer that watcher of WLAN Client and it's of mutual surveillance. List on the left is a list of the current detected wireless Internet. More information comes in, double-click.

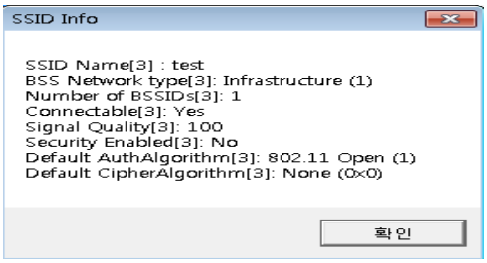

Fig. 9. Powered screen of SSID.

To access the wireless Internet, and then click the OK button The following confirmation window appears, ID, PASS and then click the OK button to enter.

1) ID & PASS

Database login using the member search and phone number to receive coming information

2) WLAN client module communicates with the Server verifies the user ID and password.

3) After DB confirmed then server generate the OTP.

4) At this point the information has AP.

5) The server will send SMS to GSM, random number.

6) Been sending SMS no input into the dialog box below.

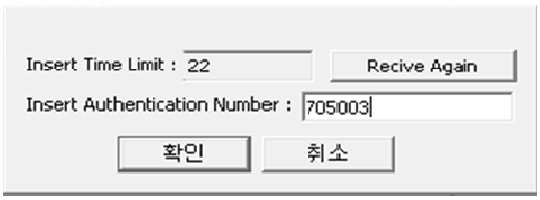

Fig. 10. Receive the certified value screen.

7) After checking this, enter the password and click the OK button. The window closes and returns to the background and all. Only this time the program is in progress in a compelling way to shut down when WLAN client

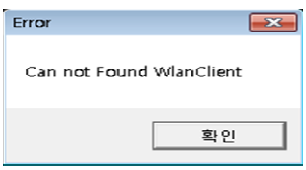

Fig. 11. Alert message.

The following error window appears and all information will be deleted.

8) Server part

Server using the HOTP approach will generate the OTP. Server using the ID and time values to generate a hash value through HOTP generation module generates a list of individually OTP. Count value by using this list (Client's request) for the OTP is sent to your mobile phone. OTP value is entered to verify the server transmits the results WLAN client. Input received is equal to the value sent to transmit the complete frame. If not, re-transmissions HOTP and repeats the previous action.

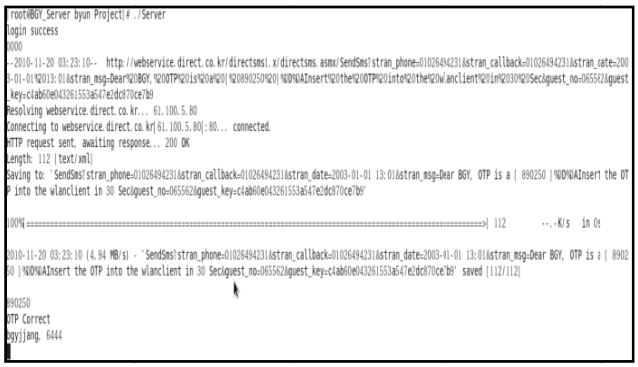

Fig.12. service messages used in.

V. CONCLUSIONS

In this paper, to enhance security when using wireless networks, as well as convenient SMS modules are designed and implemented an authentication server. The proposed method presented in the previous 18 steps of the algorithm in EAP-TLS Fewer than eight steps, reduced traffic load. It could have been able to use without a certificate and to improve the vulnerability

The simulation environment and the actual service configuration errors occur in the issue not be considered unexpected for this part of the supplement will be needed.

The proposed framework is applied to a separate certificate does not need to carry as well as Stability is proved and the general public people known SMS OTP encryption technology by applying it to the inside for security, to raise awareness about the invisible can do this.

The proposed network is relatively small in itself, was designed to be implemented between the standard and the bar operators in the future can be seen as challenges to be accomplished. Through this paper, similar as possible to hide radio service environment is expected to apply.

REFERENCES

[1] Kim, Lee , Han, Shin, "The trends of linked secirity technology of wireless network, pp100, vol.20 no1 February 2005 electronic telecommunication trends analysis.

[2] 3GPP TR 22.934 "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Feasibility Study on 3GPP System to Wireless Local Area Network(WLAN) Interworking(Release 6), " Sep. 2003.

[3] J.R. Walker, "Unsafe at any key size : An analysis of the WEP encapsulation." Tech.Rep. 03628, IEEE 802.11 committe, Mar, 2000.

[4] Sun Hee Lim , Okyeon yi , Sungik Jun , Jin-Hee Han ," The study of authentication scheme of Wibro applied EAP-AKA wireless networks " 442-443p, local journal of Korea.

[5] W.A. Arbauch, "Your 802.11 Wireless Network has no Clothes." University of Maryland, Mar 2001.

[6] RFC 3748 , 'Extensible Authentication Protocol(EAP)," June 2004.

Byung-Kil Byun He Received B.S. Degree in Industrial Chemistry from KonKuk University in 1993 and He Received M.S. Degree in Information and Telecommunication from University of Incheon in 2000. and He is finished a Ph.D course work in Information and Telecommunication from University of Incheon in 2006. He has been work a Head research of Main I.T center in Seoul T. Univ since 2007.

Ki Young Lee Received the B.S. and M.Eng. degrees in Electrical Engineering from Yonsei University, Seoul, Korea in 1982 and 1984, respectively. And he received M.S. (1987) from the University of Colorado, Boulder and the Ph.D. (1993) from the University of Alabama in Electrical & Computer Engineering. Since 1994, he has been a professor in the Department of Information and Telecommunication Engineering at the University of Incheon. His research interests include Internet traffic control and protocols, ubiquitous sensor networks and network security system.