International Journal of Security and Its Applications
Vol.7, No.5 (2013), pp.343-354
http://dx.doi.org/10.14257/ijsia.2013.7.5.31

A Study on Differential User Authentication Scheme based on Client in Home Network

Changhoon Lee, Woongryul Jeon, Dongho Won*

Information Security Group, Sungkyunkwan University
clee@security.re.kr, wrjeon@security.re.kr, dhwon@security.re.kr

Abstract

Home network service is recently installed in each home with the popularity of ubiquitous environment. There are being developed systems that efficiently controlled and handling home entry, electricity product, lamp and boiler at the remote environment as well as at home. The home network has the convenience, but because of there may be the danger to be divested of the authority handling the home network. Therefore, it is ensured the authority handling the home network. This paper proposes the scheme for differential user authentication based on client in home network at a remote place. The scheme supports the convenience and strengthens the security by using the unique value of the registered client. In case of using the unregistered client, it protects the authority accessing the home network via the method strengthening the user authentication by using the security card.

Keywords: *Home Network, User Authentication, Security Card*

1. Introduction

Nowadays, as ubiquitous environment is spreading, Home network installed in houses. There are developing systems that efficiently controlled and handling home entry, electricity product, lamp and boiler at the remote environment as well as at home. The home network systems assure the serviceability, availability and effectiveness in living, but we can use stable convenience systems when threat factors of the systems are removed. If the member of the family uses the home network system, the member handles efficiently the home appliances. However because it is danger to be divested of the authority handling them, we must protect preferentially the authority handling the home appliances from attacker. The research about the method protecting systems from the threat getting the authority at the remote place is necessary than protecting the threat handling them at home.

Home network service must strictly limit that other people are not members of home access to it and offer the convenience to users are members of home. When users use their clients, they could access to service in the best convenient way. On the other hand, when they use other's clients, it is necessary to authenticate in more secure way. However, in prior research, it is only possible to authenticate to access to service when using clients registered with home network and it is impossible to access to service when using clients unregistered with it. To access home network whenever and wherever users are, it should be possible to use home network service with unregistered clients.

Therefore, in this paper, it is proposed the scheme for differential user authentication based on client in home network to reinforce the security as well as to offer convenience to users using the service. Users register their clients with home network and registered clients could

* The corresponding author

ISSN: 1738-9976 IJSIA

easily access to home network with ID and Password. On the other hand, we propose the way that could ensure security by using a potable security card as well as ID and password when using unregistered clients. As registered clients have a secret key, it can access to service without a security card. However, unregistered clients could temporarily communicate with home network by using a one-time session key users generated with a security card.

The rest part of the paper is organized as follows. In Section 2, we discuss related works. In Section 3, we propose user authentication scheme based on client in home network. In Section 4, we present security analysis on our scheme. In Section 5, we present our conclusion.

2. Related Work

It has been studied to improve the security of the ubiquitous environment. It has been proposed the efficient schemes on user authentication and access control for the home network. In the case using the authentication and access control protocol based on PKI proposed in [1], home network can authenticate users because of transmitting private certificates after encryption with symmetric key. Also, it has the advantage improving the security by using other encryption key whenever users connect the network.

However, the weakness of this protocol is that the user is only available to connect the home network with client stored certificate after he register the DID (Device ID) on home server. Therefore for the convenience of the user it need the method to connect the home network over ensuring the security with client device unregistered on home server as well as prequalified.

The user authentication scheme based the OTP proposed in [3] offer more secure communication service by using the OTP based on hash function than scheme using the general password. However, this scheme also is only available to connect the home network with client device registered on home server in advance. In case of losing a client, others can access to home network if user's password is cracked by their password attack.

Device authentication/authorization protocol proposed in [8] offer roaming service that make clients to able to access external home network as well as inter home net-work by using synchronization value and public key encryption method made with secret key and device ID. However, it is no way to change a public key and private key made device ID. When losing clients, others can access to home network if PIN number is exposed by attacker's password guessing attack and it have much more risk because of roaming service. Also, this protocol can only access to home network by using registered client.

Therefore, in this paper, we propose a scheme that can be efficiently and securely connect to your home network with unregistered client device as well as pre-authentication client device on the home server.

3. The Differential Authentication Scheme based on Client

3.1. The Authentication Scheme for Registered Client

3.1.1. Client Registration: In ubiquitous environment, users get the authority to control the home network by connecting the home network remotely with the mobile client or the computer outside. However, an attacker with malicious intent and purpose can also try to have the home network control authority to penetrate at someone's home or to undermine the members and components.

In this paper, in order to ensure the safety on authority acquisition and protect the rights of the remote control for the home network, we propose the scheme of authority acquisition differentiated client device to connect the home network.

A home network is made up of the clients, home network provider, home server, home devices. The authentication of the client is carried out at the home network authentication server (HNAS) of the home network provider, and authenticated clients are able to handle home devices through the home server (HS).

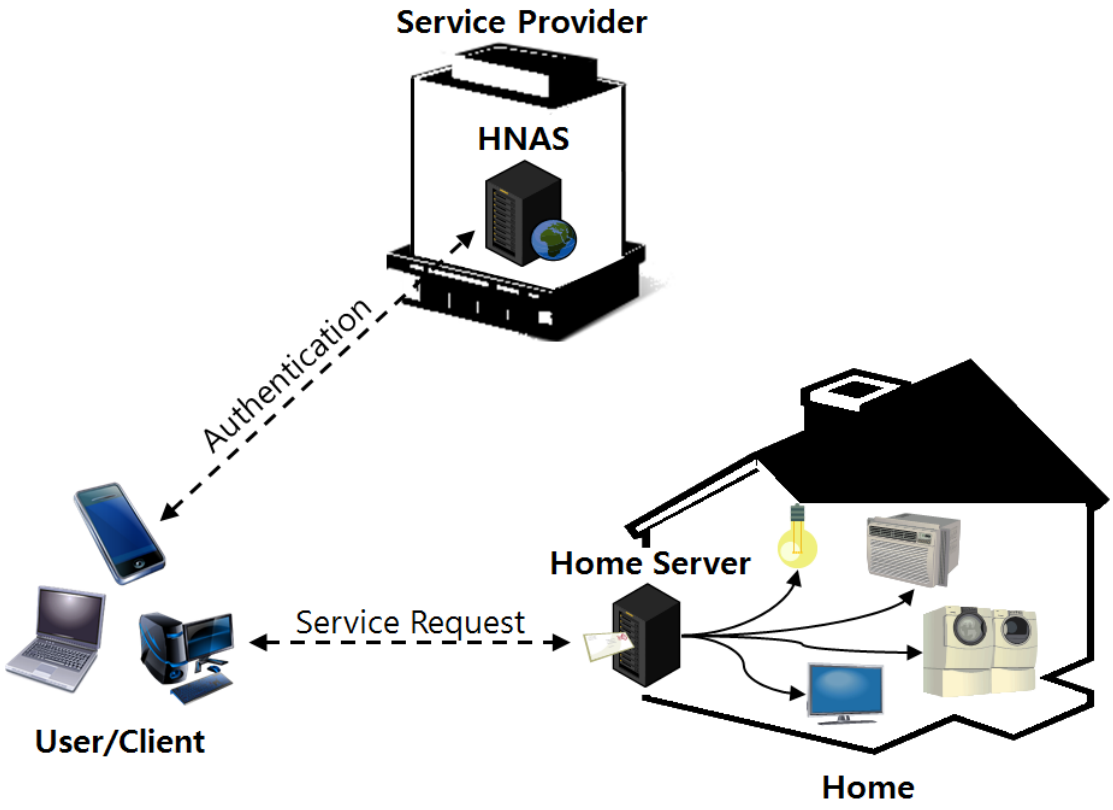

Figure 1. Home Network Architecture

Clients are distinguished depending on whether clients are registered and authenticate on the home network system or not. If user use a client registered and authenticated on the home network system, access authority acquisition procedure is relatively simple. ID, PW(Pass Word), SN(Serial Number) and AD(MAC Address) of client are used to register the client on home network. HNAS stores the user and client information. A user can have a unique account and it can be a number of client information in an account for user having the many clients.

When the client is registered on the HNAS, they share the secret key (k_c). Key generator in HNAS generates the secret key. This secret key k_c is used to communicate securely by encrypting the mutual transmission data when the session connects between the user and the home network. We use PKI (Public Key Infrastructure) to distribute the generated secret key safely [6]. In case of changing a secret key, we can safely distribute it by using PKI.

3.1.2. The Authentication Scheme for the Registered Client: In order to ensure the convenience of the ubiquitous environment, the method accessing the home network should be simple if the secure communication is possible. As the purpose conveniently controls the user's home at remote place, the complex procedures for the control may undermine the convenience. Most of client registered to the HNAS are owned by the members of home. Therefore, it is possible to communicate securely by using encryption because the client and HNAS can share the secret key when the users register their account and store the client's information on the HNAS.

Table 1. Terminology and Notations

Article	Description
Client	User's computing device
HNAS	The authentication server of the home network provider
HS	Home server in the home network
ID	User Identifier
HID	Hash value of the ID
PW	User password
SN	Client's serial number
AD	Client's MAC address
CN	Client's registration number
UN	Unregistered client's number
TN	Client's temporary identification number
k_c	The secret key sharing HNAS and registered client
k_s	The session key sharing HS and unregistered client
k_t	The session key sharing HS and client
k_h	The secret key sharing HNAS and HS
$E_k()$	Algorithm encrypting with secret key *k*
AP	Authentication parameter
TS	Time stamp
TC	Time parameter
Ticket	The ticket used for user to access HS
Flag	Flag confirming client registration

Ticket Request Phase: As users implement the application accessing the home network with the remote client outside, clients generate HID and HNAS confirms the client that was registered at the home network before the current access by transmitting the message (1).

$$CN||E_{k_c}(HID||AP_1||TS_1) \quad (1)$$

After the HNAS confirm the message (1), if client is authenticated, the HNAS transmits the message (2) to the client.

$$E_{k_c}(Flag||TC||TS_2) \quad (2)$$

As TC is the constant changing via time, it makes the security increases because it used to change the value continuously when generating the session key or the ticket for user to access HS. Flag is used to confirm that the client was registered on the home network, and the flag value of the registered client is 1, it of the unregistered client is 0. In this case, flag value is 1 due to the state using registered client.

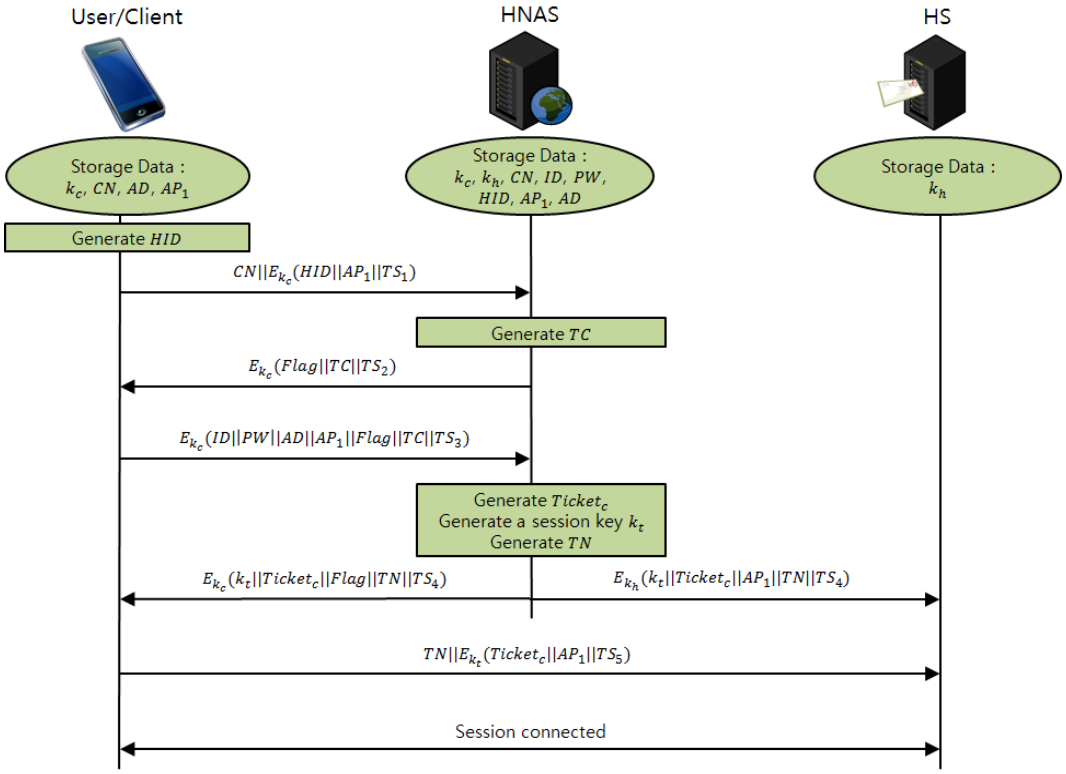

Figure 2. Authentication Protocol of Registered Client

As the client receive the message (2) to notice that the HNAS confirmed what the client had been registered on the home network, the client send the HNAS the message (3) to gain the authority to access the home network.

$$E_{k_c}(ID||PW||AD||AP_1||Flag||TC||TS_3) \quad (3)$$

The HNAS decrypts message (3) with the sharing secret key and give the access authority to the client by verifying ID, PW, and AP_1. AP_1 is a value calculating the user and client information via hash algorithm. Equation (4) descripts to make the AP.

$$AP_1 = H(ID||PW||SN||AD) \quad (4)$$

The HNAS have to store all the AP_1 value of the members. It has to be possible to authenticate the user and client by AP_1 at the same time. Although the attacker gets AP_1, he has to be impossible to recover the original data by using the one-way hash function. It set the clipping level in case losing the client because of being exposed the secret key and AP_1. When ID and PW entered wrong a certain number of times, the user using the client can't access to the home network a certain amount of time. If it is repeated, the HNAS blocks that the client access to it.

HNAS receives the message (3), and it compares ID, PW, and AP_1 in the message (3) to them in the table of HNAS. The user and client are authenticated if the values in message (3) and them in table is same. Then, HNAS generate the ticket that a client can use to access to HS. Equation (5) descripts to generate the ticket.

$$Ticket_c = H(ID||PW||AD||AP_1||TC) \quad (5)$$

HNAS generates randomly a temporary session key k_t and temporary identification number TN, and it sends the ticket and session key k_t to a client and HS after encrypting it. HNAS send the message (6) to the client, and send the message (7) to HS.

$$E_{k_c}(k_t||Ticket_c||Flag||TN||TS_4) \quad (6)$$

$$E_{k_h}(k_t||Ticket_c||AP_1||TN||TS_4) \quad (7)$$

HNAS makes client and HS to communicate securely by distributing equal ticket and session key k_t to them.

Service Request Phase: A client can request the service to HS with the ticket. It sends the message (8) encrypted with the session key k_t to request service to the HS.

$$TN||E_{k_t}(Ticket_c||AP_1||TS_5) \quad (8)$$

TN is a temporary identification number for HS identifies clients. First, HS identifies a client with TN. Then HS compares $Ticket_c$, AP_1 from the client to them from the HNAS. If the values from the client and them from the HNAS are same, HS allow the client to access it and it is built secure session between the client and HS. Figure 2 shows the authentication protocol of unregistered client.

The user should input only user's ID and password which are the unique value of the account for the user and device authentication, but the client and HNAS are possible to communicate securely. Moreover, the client can obtain the authority to access to the home network through mutual authentication with the HNAS. Therefore, the user can conveniently take advantage of the home device by connecting to the home network.

3.2. The Authentication Scheme for Unregistered Client

3.2.1. Session Key Generation Mechanism: The member of home may not be able to use the client registered at the HNAS at the case may be. In this case, user should use the unregistered client. However, to use the unregistered client is more hazardous than to use the registered client, so it is relatively necessary complex procedure. To use unregistered client needs the security card. The security card, as an authentication tool to access the home network remotely, includes secret numbers to use unregistered client. The members of home have the same security cards and the secret numbers are equally stored the HNAS and security cards. Secret numbers of the security card are the medium to generate the secret key to communicate securely the unregistered client and the HNAS. It is possible to communicate securely by getting the access authority through the secret key generated. Therefore, as it is the serious threat for the home network security if the security card is exposed, the user doesn't have to lose or expose the security card. If a user loses the security card, all of the members must to change their security card.

The secret key generated by using the security card is the one-time key that can be used at the one session. To connect the other session has to use the other key generated again. The one-time key generated is the session key k_s.

The session key k_s is generated by using the two secret values from the security card. First of all, the HNAS send the plain numbers A and B to the client. The plain numbers A and B is the reference number used to find the secret numbers from the security card. The user check the reference numbers A, B and input the secret numbers in the client by finding them corresponding to reference numbers on the security card. The secret numbers are stored in the client. The HNAS have known the secret numbers corresponding to reference numbers it sends. Therefore, the HNAS and the client generate the same symmetric key by using the secret

numbers. When the secret numbers are X_A and X_B, the secret value v is generated by operating the Equation (9).

$$v = \alpha^{X_A \cdot X_B} \bmod \beta \quad (9)$$

In this equation, α and β are public global constant. α is the sufficiently large prime number, and β is a primitive roots of α. This equation is secure if X_A and X_B are sufficient long [5]. In addition, the session key is made by using a one-way hash function to enhance the security and to generate a key of a certain length. Therefore, session key k_s is generated by calculating the Equation (10).

$$k_s = H(v||TC) = H(\alpha^{X_A \cdot X_B} \bmod \beta||TC) \quad (10)$$

As this session key k_s is possible to be generated via the same operation in the HNAS, the HNAS and client mutually can do the secure encryption communication.

3.2.2. The Authentication Scheme for the Unregistered Client:

Ticket Request Phase: When the users run the application accessing the home network with unregistered clients, the application in the client transmits UN to HNAS because unregistered clients don't have the secret key k_c sharing with HNAS. A Client sends a message (11) to HNAS.

$$UN||HID \quad (11)$$

If the client transmits CN, HNAS decides the client error because there is no AP_1 to be able to authenticate whether the client is registered or not. In this case, if flag value continually is one, HNAS decide the flag attack and block the access from this client for a long time. HNAS received a message (11) decide that the unregistered client want to access to it. In order to request the secret value to the user, HNAS transmits a message (12) encrypted with secret value v to the client.

$$A||B||E_v(Flag||TC||TS_1) \quad (12)$$

The user generates secret value v with α, β and secret numbers mapped plain numbers A and B of the security card, and decrypts the message (12) with it. And the user generates the session key k_s with the secret value v and time parameter TC. There is possible the secure encryption communication with the session key.

It operates Equation (13) to make the authentication parameter AP_0 for the unregistered client.

$$AP_0 = H(ID||PW||X_A||X_B) \quad (13)$$

HNAS can make AP_0 because it knows secret values X_A and X_B, and decide to authenticate the client by comparing AP_0 from the client. The client transmits a message (14) to HNAS to obtain the access permission.

$$E_{k_s}(ID||PW||AD||AP_0||Flag||TC||TS_2) \quad (14)$$

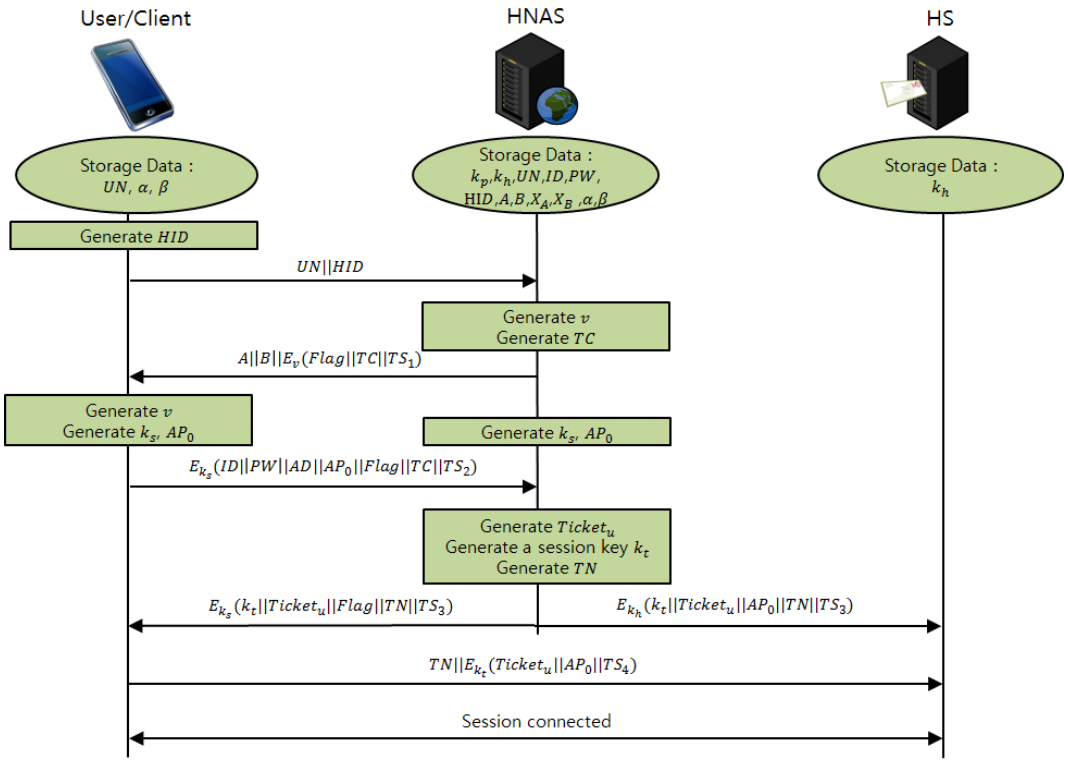

Figure 3. Authentication Protocol of Unregistered Client

The HNAS decrypts the message (14) by using the sharing session key k_s. It checks ID, PW and AP_0 and authorize to access the home network for the client. HNAS generates the ticket that a client can use to access to HS. Equation (15) descripts to generate the ticket.

$$\mathrm{Ticket_u} = \mathrm{H(ID||PW||AD||AP_0||TC)} \tag{15}$$

HNAS generates randomly a temporary session key k_t and temporary identification number TN, and it sends the ticket and session key k_t to a client and HS after encrypting it. HNAS send a message (16) to the client, and send a message (17) to HS.

$$\mathrm{E_{k_s}(k_t||Ticket_u||Flag||TN||TS_3)} \tag{16}$$

$$\mathrm{E_{k_h}(k_t||Ticket_u||AP_0||TN||TS_3)} \tag{17}$$

HNAS makes the client and HS to communicate securely by distributing equal ticket and session key k_t to them.

Service request phase: The procedure of the service request phase is almost equal it of the registered client. A client sends the message (18) to HS to request the service.

$$\mathrm{TN||E_{k_t}(Ticket_u||AP_0||TS_4)} \tag{18}$$

First, HS identifies the client with TN. Then HS compares $\mathrm{Ticket_u}$, $\mathrm{AP_0}$ from the client to them from the HNAS. If the values from the client and them from the HNAS are same, HS allow the client to access it and it is built secure session between the client and HS. Figure 3 shows the authentication protocol of unregistered client.

The mechanism proposed this paper is the scheme to strength the authentication about the user with unregistered client by using the security card.

4. Security Analysis

In this section, we present the security analysis about our proposed authentication scheme.

4.1. Eavesdropping

In this scheme, an attacker can't confirm contents of messages because communication between a client and HNAS, HNAS and HS, a client and HS is encrypted by the secret key. A secret key k_c of a registered client is secure as it is distributed by using PKI. An attacker can't know information to make session key k_s of unregistered client because it is sent after encrypting with secret value v.

4.2. Replay Attack

There is a time stamp in the message to prevent replay attack. Although an attacker carry out replay attack, a receiver throw away the message from an attacker because time stamp value is wrong.

4.3. Client Loss

If a registered client is lost, a secret key and authentication parameter can be exposed to an attacker. Then an attacker can be certified for handling the home network if knowing the client user's password. In this case, we prevent the password crack because of clipping level.

4.4. Masquerading Attack

An attacker can request to authenticate to HNAS by capturing user's HID and masquerading unregistered client. In this case, HNAS send the message encrypted with a secret value v to him. He couldn't decrypt the message as he can't know the secret value. Moreover, he can't generate a session key k_s because he doesn't have the security card and can't find TC. Therefore, Masquerading attack is impossible.

4.5. Password Guessing Attack

An attacker is difficult to know user's password because clipping level is set to prevent password guessing attack in registered clients. Even though he can find the user's password with social engineering, he can't get the access authority if he don't have registered clients stored a secret key. Also, unregistered clients are secure because of having 2-factor authentication (Password, security card).

4.6. Mutual Authentication

It is needed the mutual authentication to connect securely a client and HS. HNAS make possible mutual authentication and encryption communication by issuing a temporary session key k_t when it connects a client and HS.

4.7. Security of Session Key

It is used a session key for secure communication between a unregistered client and HNAS. It is secure because an attacker can't find X_A and X_B, and generate the session key k_s

if he doesn't have a security card. If the X_A and X_B is large enough, we can ensure security. Also, we can make enough long key because of generating it by using hash function, and it changes continually because of including TC.

5. Conclusion

The home network system is the service to be able to increase the convenience and efficiency of the life in the home environment of the future. To manage the service safely and to maximize the benefits of this system priory need to protect the authority to control the system. If it especially lose the authority of the control to the other people, it can't ensure the own safety as well as the property of the member.

The differential authentication scheme based on client, proposed in this paper, increases the convenience and security about obtaining the access permission by using pre-authentication registration. Moreover, using the security card can strengthen the security on the unregistered client. Therefore, the authentication scheme proposed in this paper will contribute to build a more efficient and secure home network system.

Acknowledgements

This research was funded by the MSIP(Ministry of Science, ICT & Future Planning), Korea in the ICT R&D Program 2013.

References

[1] Y. Lee, J. Kim, H. C. Kim and M. S. Jun, "A Study for PKI Based Home Network System Authentication and Access Control Protocol", Korea Information and Communications Society, vol. 35, no. 4, **(2010)**.
[2] H. Lee and M. Chung, "Context-Aware Security model for Social Network Service", International Conference on Broadband and Wireless Computing, Communication and Applications, **(2011)**.
[3] J. Jeong, M. Young Chung and H. Choo, "Integrated OTP-Based User Authentication Scheme Using Smart Cards in Home Networks", Hawaii International Conference on System Science, **(2008)**.
[4] J. Eom, S. Park and T. Chung, "A Study on Architecture of Access Control System with Enfored Security Control for Ubiquitous Computing Environment", Korea Institute of Information Security & Cryptology, vol. 18, no. 5, **(2008)**.
[5] W. Stallings, "Network Security Essential: Applications and Standards", Third Edition, **(2007)**.
[6] C. Adams and S. Lloyd, "Understanding PKI: Concepts, Standards, and Deployment Considerations, Second Edition, **(2002)**.
[7] Y. Lee, D. Lee, J. Han and T. Kim, "Home Network Device Authentication: Device Authentication Framework and Device Certificate Profile", The computer journal, vol. 52, no. 8, **(2009)**.
[8] J. Moon, D. Lee and I. Lee, "Device Authentication/Authorization Protocol for Home Network in Next Generation Security", Advances in Information Security and Assurance, LNCS 5576, **(2009)**.
[9] H. Kim and H. Jung, "Smartcard-Based User Authentication Protocol over Home Network", Future Information Technology, Application, and Service, LNEE 164, **(2012)**.
[10] B. Vaidya, J. Park, S. Yeo and J. J. P. C. Rodrigues, "Robust one-time password authentication scheme using smart card for home network environment", Computer communications, vol. 34, no. 3, **(2011)**.
[11] H. Jeong, D. Won and S. Kim, "Weaknesses and Improvement of Secure Hash-Based Strong Password Authentication Protocol", Journal of Information Science and Engineering, vol. 26, no. 5, **(2010)**.
[12] W. Jeon, J. Kim, J. Nam, Y. Lee and D. Won, "An Enhanced Secure Authentication Scheme with Anonymity for Wireless Environments", IEICE Transactions on Communications, vol. E95-B, no. 7, **(2012)**, pp. 2505-2508.
[13] K. Son, D. Han and D. Won, "A Privacy-Protecting Authentication Scheme for Roaming Services with Smart Cards", IEICE Transactions on Communications, vol. E95-B, no. 5, **(2012)**, pp. 1819-1821.
[14] M. Kim, N. Park and D. Won, "Security Improvement on a Dynamic ID-Based Remote User Authentication Scheme with Session Key Agreement for Multi-server Environment", SecTech/CA/CES3 2012, **(2012)**, pp. 122-127.
[15] M. Kim, N. Park and D. Won, "Security Weakness of a Dynamic ID-Based User Authentication Scheme with Key Agreement", CSA 2012, **(2012)**, pp. 687-692.

[16] W. Jeon, J. Kim, Y. Lee and D. Won, "Security Analysis of Authentication Scheme for Wireless Communications with User Anonymity", STA 2012, **(2012)**, pp. 225-231.

Authors

Changhoon Lee received the B.E. degrees in information and communication Engineering from Sungkyunkwan University, Korea, in 2009. He is now in the M.E. Course in Sungkyunkwan University. His research interests include information security, network security, and cryptography.

Woongryul Jeon received the B.E. and M.E. degrees in Computer Engineering from Sungkyunkwan University, Korea, in 2006 and 2008. He is now in the Ph.D. Course in Sungkyunkwan University. His research interests include electronic voting, network security, and security assurance.

Dongho Won received his B.E., M.E., and Ph.D. degrees from Sungkyunkwan University in 1976, 1978, and 1988, respectively. After working at ETRI (Electronics & Telecommunications Research Institute) from 1978 to 1980, he joined Sungkyunkwan University in 1982, where he is currently Professor of School of Information and Communication Engineering. In the year 2002, he served as the President of KIISC (Korea Institute of Information Security & Cryptology). He was the Program Committee Chairman of the 8th International Conference on Information Security and Cryptology (ICISC 2005). His research interests are on cryptology and information security.