Integrated OTP-based User Authentication Scheme Using Smart Cards in Home Networks

Jongpil Jeong*, Min Young Chung* and Hyunseung Choo*
*Intelligent HCI Convergence Research Center
Sungkyunkwan University, Suwon, Korea 440-746, +82-31-290-7145
Email: {jpjeong, mychung, choo}@ece.skku.ac.kr

***Abstract*—In this paper, we propose a new user authentication (UA) scheme based on one-time password (OTP) protocol using smart cards for home networks. The proposed scheme is to authenticate home users who uses home devices. Several techniques using technology based on biometrics, passwords, certificates, and smart cards can be used for user authentication in the similar environments. However, such user authentication techniques must be examined before being employed in an environment where home devices have low efficiency and performance. Here, we present the important security functions of home networks. The proposed authentication protocol is designed to accept the existing home networks based on the one-time password protocol. Also, it is a well suited solution and is quite satisfactory in terms of the security requirements of home networks, because of requiring low computation by performing simple operations using one-way hash functions. Our proposed scheme can protect against illegal access for home services and devices and does not allow unnecessary service access by legitimate users. Therefore, it allows the user to provide real-time privilege control and good implementation in secure home networks.**

I. Introduction

Home networks provide remote access control over the connection between information home appliances and information devices on the Internet [1], [2], [3], [4]. And, it is possible to operate bi-directional communication services that use contents such as music, video and data. Therefore, it provides convenient, secure, healthy, pleasant and efficient living for home users through the future-focused home environments that make it possible to use several services regardless of device, time and place. This can be realized using integrated IT technologies.

Home networks consist of several wired/wireless mediums and protocols, so it also has the existing security vulnerabilities. And it has the problem that it can be adapted to current network-based cyber attacks. Home networks information appliances have relatively low computing capabilities, and they are difficult to build with security functions, so they can be used in cyber attacks and have the possibility of being targeted by several attacks. Home networks services contain private information, and will provide direct-life services such as health-care service. Therefore, attacks on home networks can violate person's privacy and ultimately threaten the life of home users, so appropriate security measures must be considered carefully. Integrated OTP-based user authentication scheme using smart cards proposed for home networks, so that legitimate users only can access home services.

There are two types of password-based authentication and public key based authentication schemes for home users to provide security in wired/wireless networks. These authentication schemes are vulnerable for several attacks and have the critical problem of large processing overhead for home networks appliances. In this paper, the proposed scheme based on strong-password approach uses one-way hash functions to perform simple authentication operations, so it requires low computational load. Also, it enhances the security level by using OTP technology.

The proposed scheme protects from replay attack of ID/PW very well, and uses the OTP technique and one-way hash functions to reduce the processing overhead. The OTP technique is based on mathematical cryptography for generating regular patterns, and it is the best technology for authentication problems because its safety is ensured theoretically. The OTP transmits an input password that is different each time. So it is impossible to reuse the revealed value although messages captured by attackers. In this paper, we propose a secure user authentication protocol based on OTP schemes such as S/Key [8], Lamport [7], Revised SAS [6] and SAS-2 [5]. It employs a three-way challenge-response handshake technique to provide mutual authentication. The computation in the user device is reduced, resulting in less power consumption in the mobile devices.

The rest part of the paper is organized as follows. In Section 2, related works are presented. An authentication protocol suitable for home network environments is proposed in Section 3. Finally, this paper is concluded, and future directions are noted in Section 5.

II. Related Works

Password-based authentication schemes are the most widely used methods for remote UA. Existing schemes could be categorized into two types [9]. One uses a weak-password approach, while the other uses a strong-password one. The weak-password authentication approach is based on the El Gamal cryptosystem. The advantage of this scheme is that the remote system does not need to keep the userID-password table to verify the user. However, such a weak-password authentication approach leads to heavy computational load on the entire system. Thus, it cannot be applied to home network environments, as home appliances cannot afford this heavy

1530-1605/08 $25.00 © 2008 IEEE

computation. Unlike the weak-password approach, strong-password authentication is mostly based on the one-way hash function [13] and exclusive-OR operations (XOR). It requires much less computation and needs only simple operations. With this in mind, this scheme may have advantages when applied to home network environments.

Das *et al.* proposed a dynamic ID-based scheme [9], which is based on the strong-password authentication approach. The scheme allows the users to choose and change their userIDs and passwords freely. The system has no need to assign a password to a particular userID. This feature will be incorporated into our proposed UA scheme for Home Networks as well. The algorithms in [9] are claimed to be secure against IDtheft; and able to resist the replay and forgery attacks, as well as insider attacks. However, some of the algorithms were proved by Awasthi [10] to have loopholes in the process of password verification. These loopholes are already enough to make the whole system insecure, as an intruder is able to use any random password to get into the system.

Most of the existing UA schemes require high computation cost caused by exponentiation operations; and are not suitable for mobile devices (e.g. PDAs, mobile phones, sensor nodes etc.). Lee *et al.* [11] also proposed an improved UA scheme with low computation cost by using smart cards and one-way hash functions. Only three phases are used here, namely, Registration Phase, Login Phase, and Authentication Phase. This scheme can resolve the attacks of forgery, replay, and modified login message. Our proposed solution in Section 3 makes use of the framework having the three phases above; but adapts it to the home network environments. Jeong *et al.* [19] proposed a mutual authentication scheme between 3-parties (user, authentication server, and home gateway server) for home networks, which uses a pre-shared symmetric key based on two nonces between two servers and verifies the session key calculated by using the two nonces. However, authors do not consider the critical problem in home services in the case of leaking a user password to attackers. In this paper, we make up the weak points of [19], fulfilling the low computation load and security requirements for home networks. Here we employ the OTP protocol to use the password between home appliances (mobile devices) and authentication server.

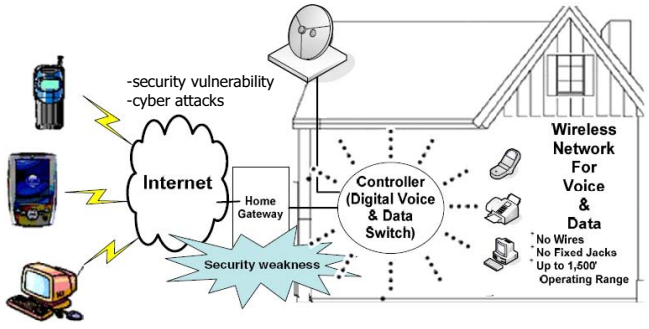

Fig. 1. Home Network architecture and Various attacks.

One form of attack on network computing systems is eavesdropping on network connections to obtain authentication information such as the login IDs and passwords of legitimate users. Once this information is captured, it can be used in a later time to gain access to the system. The OTP system [14] is designed to counter this type of attack, called a replay attack. A sequence of OTP is produced by applying multiple times a secure hash function to the output of the initial step (called S). That is, the first OTP to be used is produced by passing S through the secure hash function a number of times (N) specified by the user. The next OTP to be used is generated by passing S through the secure hash function $N-1$ times. An eavesdropper who has monitored the transmission of OTP would not be able to generate the next required password because doing so would mean inverting the hash function. The OTP improves security by limiting the danger of eavesdropping and replay attacks that have been used against the simple password system. The use of the OTP system only provides protection against passive eavesdropping and replay attacks. It does not provide for privacy of transmitted data, and it does not provide protection against active attacks. The success of the OTP system to protect host system is dependent on the non-invert (one-way) of the secure hash functions used.

III. Integrated OTP-based UA Scheme Using Smart Cards

Currently, the home network is exposed to various cyber attacks through the Internet, and has security vulnerabilities such as hacking, malignancy code, worm and virus, DoS (Denial of Service) attack, and communication network tapping as shown in Fig. 1. As a result, the technical development of the home network with respect to security mostly focuses on putting security functions on the home gateway to cope with cyber attacks. Home gateway needs countermeasures against the attacks on main resources through illegal device connection or possibility of leakage of main data. Especially, in the premise of the home network, vulnerability of component and data security exists in the wireless part needing authentication for accessing the component and data.

Security function is preferred to be loaded into a home gateway that provides a primary defense against the external illegal attacks as an entrance guard that connects the public network out of the house to the home network. The representative security functions loaded in the home gateway are firewall, VPN (Virtual Private Network), etc. However, they are not suitable to the HN because the firewall allows data to enter the premise network if the destination is correct, and VPN is more suitable to a large network of high traffic.

The main features needed to be considered in the design of an authentication protocol are for coping with attacks like the following [15], [16]:

Eavesdropping attack: This is the simplest type of attack. A host is configured to ”listen” to and capture data not belonging to it. Carefully written eavesdropping programs can take usernames and passwords when users first login to the network. Broadcast networks like Ethernet are especially vulnerable to this type of attack.

Replay attack: An attack in which a valid data transmission is maliciously or fraudulently repeated either by the originator or by an adversary who intercepts the data and retransmits it, possibly as part of a masquerade attack.
Man-in-the-middle attack: An attack in which an attacker is able to read and modify the messages between two parties with a malicious intent without either party knowing that the link between them has been compromised. The attacker must be able to observe and intercept messages transferred between the two victims.
Stolen-verifier attack: In most applications the server stores hashed passwords instead of clear text passwords. The stolen-verifier attack means that an adversary who steals the password-verifier from the server can use it directly to masquerade as a legitimate user during the user authentication phase.

A. Preliminary and Notation

The user (Mobile device) transmits information for OTP operation in login and verification phases to authentication server (IAS: Integrated Authentication Server) through the secure channel. The user can select their own password in the registration phase by separating the registration phase and login/verification phases. [19] is based on public key infrastructure (PKI), so it causes the processing overhead for authentication messages between authentication servers and mobile devices. But, the proposed scheme has light-weighted overhead for home networks. Also it doesn't use a password table for each user, but one-way collision-resistent hash functions as the OTP mechanism.

Service subscribers require mutual authentication between IAS and home gateway server (HGW), in order to access home network services. In addition, they must be able to operate service access control when privileged services are granted. Users are authenticated through single-sign-on (SSO) and then, they can access other home services without additional authentication procedures. Fig. 2 illustrates the user authentication mechanism.

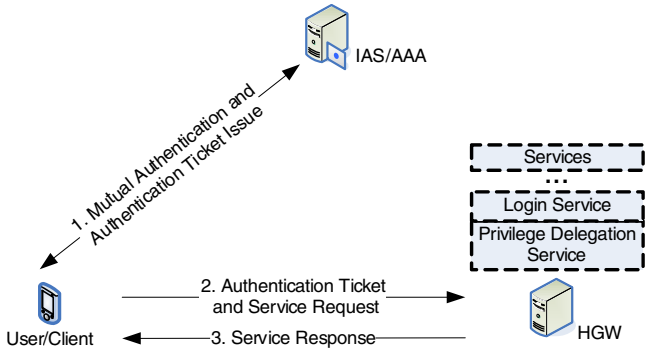

Fig. 2. User authentication mechanism.

In this section, it is assumed that IAS is located on the outside of the home network environment, manages the home gateway, and performs AAA functions of authentication, authorization, and accounting. A suitable user authentication protocol is proposed for home network environments, focusing on authentication for users receiving the home service and controlling the service privilege.

TABLE I
NOTATION.

Notation	Meaning
R_{Ui}	Number calculated by IAS using U_{ID} and Password
R_{Si}	Random Number generated by IAS
$F(), h()$	collision-resistant hash function
N	permitted number of login times
S_{key}	Shared Session Key between Client and HGW
U_{ID}	User's Identifier
IAS_{ID}	IAS's Identifier
$E_{IAS-HGW}(-)$	Encryption using Symmetric key between IAS and HGW
$E_K(-)$	Encryption using K
T	Timestamp to decide Session key's validation

In this section, we propose an efficient and complete remote password authentication scheme using smart cards. The security of our scheme depends on the secure one-way hash function and is nonce-based. The nonce is a random number that is generated and has a value that has not been used before, to avoid replay attack and the serious time synchronization problem. Our proposed scheme consists of registration, login, and authentication/service request phases. Login and Authentication phases for the proposed authentication scenario is described in Fig. 3.

B. Registration Phase

Let *x* be a secret key maintained by the remote system, *h()* be a secure one-way hash function with fixed-length output and U_{ID} denote the user who submits their identity and password to the remote system for registration. The remote authentication system (IAS/AAA server) then performs the following operations:

1) Compute U_{ID}'s secret information $v_i = h(U_{ID}, x)$ and $e_i = v_i \bigoplus F_N(password)$.
2) Write $h()$ and e_i into the memory of a smart card and issue the card to U_{ID}. $F_N(.)$ represents the total number of hashing that accepted for home users.
3) Authentication server stores U_{ID} and password value calculated by F hash function.

C. Login and Authentication Phases

When U_{ID} wishes to log into the remote system, they must insert the smart card into the terminal and type their identity U_{ID} and password $F_N(password)$. The smart card then performs the following operations:

1) Generate the result of i-times hashing, $F_N^i(password)$ for i-th authentications.
2) Compute $C = h(e_i \bigoplus F_N^i(password))$.
3) Send the message (U_{ID}, C) to the remote authentication system (IAS/AAA server).

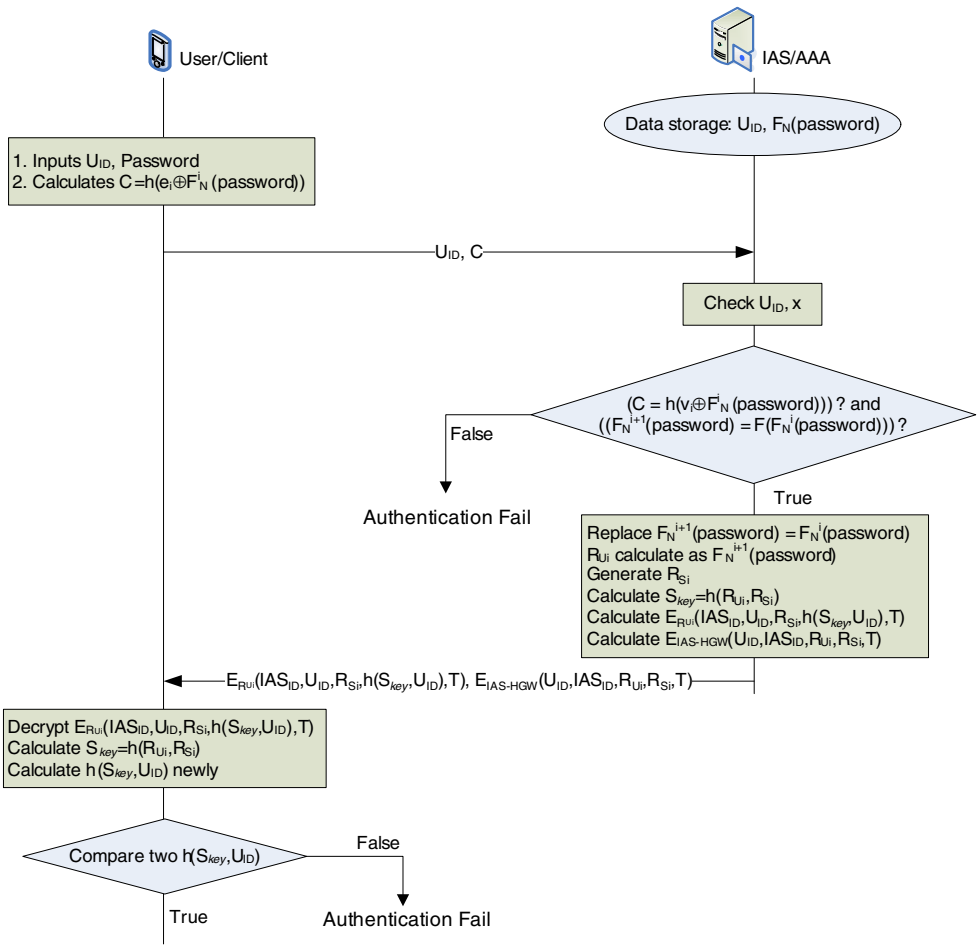

Fig. 3. ith Login and Authentication Phases.

After receiving the authentication request message, the remote system and smart card execute the following steps to facilitate a mutual authentication between the user and the remote system. The remote system performs the following operations:

4) IAS verifies U_{ID} and compute $v_i' = h(U_{ID}, x)$ and check whether $C = h(v_i', F_N^i(password))$. After then, it compare one more hashed value of $F_N^i(password)$ from client and one more hashed value, $F_N^{i+1}(password)$ of $F_N(password)$ on the server. If they are not equal, the client is rejected.
5) IAS generates nonce value, R_{Si} and takes R_{Ui} as $F_N^i(password)$, and then calculates $S_{key} = h(R_{Si}, R_{Ui})$.
6) We assumed that IAS established the security association with the home gateway server using symmetric key. IAS transmits the authentication ticket, $E_{IAS-HGW}(U_{ID}, IAS_{ID}, R_{Ui}, R_{Si}, T)$ encrypted with a symmetric key between the two authentication servers, and this also includes messages for mutual authentication between user and IAS, encrypted with R_{Ui}. Here, this message is $E_{R_{Ui}}(IAS_{ID}, U_{ID}, R_{Si}, h(S_{key}, U_{ID}), T)$.
7) Legitimate user only can verify the stored password from the previous registration phase and one more hashed value for verification, and then calculate S_{key} on the IAS server. Therefore, the legitimate user only can decrypt the $E_{R_{Ui}}(IAS_{ID}, U_{ID}, R_{Si}, h(S_{key}, U_{ID}), T)$ message using $R_{Ui} = F_N^i(password)$. The user decrypts the message, acquires the R_{Si}, calculates the S_{key} and then verifies the requested authentication by checking $h(S_{key}, U_{ID})$.

D. Service Request Phase

1) Authenticated users request home services to the home gateway server in home networks, according to the current available services. The user transmits two messages, $E_{IAS-HGW}(U_{ID}, IAS_{ID}, R_{Ui}, R_{Si}, T)$ authentication ticket and (U_{ID}, *Services*) encrypted with S_{key}, to the home gateway server, and requests home services for the home user.
2) The home gateway server verifies the two U_{ID}, one is to decrypt the authentication ticket using a symmetric key between IAS and home gateway server and the other is to decrypt the service request message, $E_{S_{key}}(U_{ID}, Services)$ using S_{key}, a hashed value of

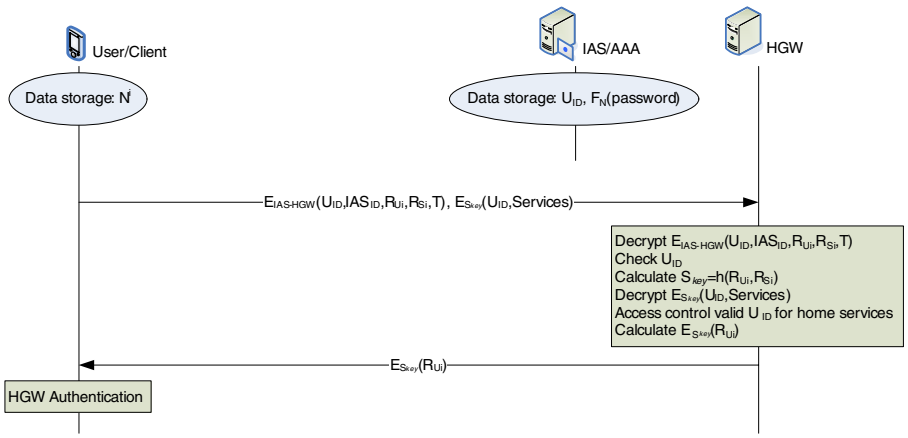

Fig. 4. Service Request Phase.

R_{Ui} and R_{Si} messages.

3) HGW transmits R_{Ui} encrypted using S_{key} to the client, and then authenticates HGW implicitly.

E. Updated password phase

If U_{ID} wants to change their password from $F_N^i(password)$ into $F_N^i(password')$ after registration, the following procedure is performed.

1) Calculate $e_i' = e_i \bigoplus F_N^i(password) \bigoplus F_N^i(password')$.
2) e_i on the memory of smart card to set e_i'. That is done because
$e_i' = v_i \bigoplus F_N^i(password)$
$= h(U_{ID}, x) \bigoplus F_N^i(password')$
$= e_i \bigoplus F_N^i(password) \bigoplus F_N^i(password')$.

IV. Analysis

The proposed protocol is designed under the assumption that a symmetric key is shared between IAS and HGW. In addition, it is assumed that IAS exists outside the home network, it manages the home gateway, authenticates users, grants privileges, and controls accounting as the home gateway operator. Another assumption is that service users trust IAS. Actually, the OSGi (Open Services Gateway Initiative) operator exists in the OSGi framework, it is outside the home network as the home gateway manager for managing the home gateway and authenticating users.

Authentication between HGW and users employ the authentication ticket granted from the authentication server, and users can request and receive services with a valid authentication ticket after authentication, there is no requirement to login each time when the users request services. Authentication ticket validation can verify its time-stamp, satisfied by authentication requirements. In addition, as U_{ID} is checked in authentication ticket after login, it can control whether having service privileges. ACL (Access Control List) is stored as table format for U_{ID} privileges list in HGW's policy file, and the purpose is to supply suitable services in response to user identification information.

Replay attack: One-time password that is sent to the authentication server is calculated by the one-way hash function($F()$), so attackers cannot replay the password to the authentication server after intercepting U_{ID}'s password.

Man-in-the-middle attack: The main benefit in the proposed scheme based on the one-time password protocol is that attackers cannot reuse the U_{ID}'s password because of the changing U_{ID}'s password each time during login and authentication request to the authentication server. Furthermore, authentication data are transferred between clients and two servers, so attacks should be detected if it changes.

Denial of Service attack: The proposed scheme changes the original password to a hashed-value ($F_N^i(password)$) and protects the user's authentication, and then the authentication server updates the hashed-value ($F_N^i(password)$) stored in the authentication server with one more hashed value ($F_N^{i+1}(password)$) when the authentication server authenticates successfully. Therefore, the proposed scheme prevents DoS attacks from the attackers.

Stolen-verifier attack: The user and authentication server shares the one-way hash functions for OTP operations through the secure channel, so the proposed scheme is secure. And it is very difficult for attackers to gain the values for OTP operations because authentication data are calculated by the one-way hash function.

Mutual Authentication: User authentication schemes satisfied the security requirements for home networks, but mutual authentication is necessary for critical applications in processing confidential data. The proposed scheme uses a 3-way challenge-response handshake protocol to provide the mutual authentication. Authentication server transmits the authentication data (Authentication Ticket) to user, user checks the timestamp T and authentication server authenticated successfully by user if T value is allowed.

V. Efficiency

In this section, we summarize the performances and criteria for authentication schemes. For a protection mechanism for user authentication, the following criteria are crucial.

TABLE II
EFFECTIVENESS COMPARISONS AMONG THE PREVIOUS SCHEMES.

	C1	C2	C3	C4	C5	C6
Our scheme	Yes	Yes	Yes	Extremely low	Yes	Yes
Jeong et al. [19]	No	No	Yes	High	Yes	Yes
Wang and Chang [21]	Yes	Yes	No	Medium	No support	No
Yang and Shieh [20]	Yes	Yes	No	Medium	No support	Yes
Hwang and Li [23]	Yes	No	No	Medium	No support	No
Sun [22]	Yes	No	Yes	Extremely low	No support	No
Chien et al. [17]	Yes	Yes	Yes	Extremely low	No support	No
Hwang et al. [18]	Yes	Yes	No	Extremely low	No support	No

C1: *No verification table:* The remote system does not need the dictionary of verification tables to authenticate users.
C2: *Freely chosen password:* Users can choose their password freely.
C3: *Mutual authentication:* Whether the users and the remote system can authenticate each other.
C4: *Lower communication and computation cost:* Due to hardware constraints of home devices, it usually does not support power communication cost or higher bandwidth.
C5: *Session key agreement:* A session key agreed by the user and the remote system generated in every session.
C6: *No time synchronization:* Discard the timestamp to solve the serious time synchronization problem.

We made comparisons among the previous schemes and our proposed scheme. Table 2 shows that our scheme satisfies all criteria.

Without complicated cryptography algorithms, the proposed scheme has been successfully developed based on hash operations. In addition, the proposed scheme allows multiple-access requests with privacy protection. Furthermore, only a simple verification is required for a multiple-access request. We compare our proposed scheme with the previous schemes for six items in Table 2. It represents good performance for no verification table($C1$) and freely chosen password($C2$) items. Also, it shows significant benefits for communication and computation cost($C4$) by using one-way hash functions and the OTP mechanism, due to requiring low computation load by adopting the strong-password approach.

In addition to the efficiency of our scheme, some other practical merits are also obtained: (1) no user-sensitive data stored in the server; (2) user's freedom in choosing their passwords; (3) mutual authentication; (4) verifying multiple access requests in a single verification; (5) no plain transmission of user's passwords since an attacker can easily eavesdrop transmission data; (6) stateless server again network DoS (Denial of Service). In our scheme, the server can grant the user's access requests after validating the user's request, and does not need to keep the state. From the Table 2, our scheme achieves the best computational performance with the lowest implementation cost. In addition, it provides several practical merits - mutual authentication, no user-sensitive data on the server, verifying multiple access requests in a single verification, the freedom of choosing user's passwords, and the stateless server against network DoS.

VI. CONCLUSION

A home network is defined as an environment where users can receive home network services for anytime and anywhere access through any device, connected with a wired/wireless network to home information appliances including the PC. In this environment, there are many security threats that violate user's privacy and interfere with home services. In addition, the home network consists of several networks with each network being inter-connected, so network security for each network is required. This means that there are a number of security threats to other networks when a security threat occurs in any network. Also, users in the home network need a security mechanism, for receiving home services and sharing information between home information appliances securely.

In this paper, a user authentication mechanism between a home gateway and user is designed to accept existing home networks based on the OTP mechanism using low-cost smart cards. So, the proposed scheme requires low computation load and provides high security for secure home networks. In addition, it protects against illegal access from inside and outside home services and home devices. Therefore, our proposed scheme is possible to adopt for home networks, with real-time privilege control for legitimate users.

There is still progress in the standardization of home network architecture, which is should researched further in the future. In addition, research regarding the integration of authentication servers for 3G-WLAN and authentication servers in home networks needs to be conducted.

ACKNOWLEDGMENT

This research was supported by Ministry of Information and Communication, Korea under ITRC IITA-2006-(C1090-0603-0046) and grant No. R01-2006-000-10402-0 from the Basic Research Program Korea Science and Engineering Foundation of Ministry of Science & Technology.

REFERENCES

[1] H. Sun, "Home Networking," Mitsubishi Electric Research Laboratories, http://www.merl.com/projects/hmnt/, 2004.
[2] K. Choi *et al*., "Trends of Home Networking Standardization in Korea," KETI Journal, 2003.
[3] Y. Park *et al*., "Home Station Architecture based on Digital Convergence toward U-Home age," ETRI Journal, 2003.
[4] S. Lim *et al*., "Home Network Protocol Architecture for Ubiquitous Communication," Journal of KIPS, vol.10, 2003.
[5] A. Shimizu, "A One-Time Password Authentication Method," Kochi University of Technology Masters thesis, January 2003.

[6] T. Tsuji and A. Shimizu, "Simple and secure password authentication protocol, ver.2 (SAS-2)," IEICE Technical Report, OIS2002-30, vol.102, no.314, September 2002.
[7] L. Lamport, "Password authentication with insecure communication," Communications of the ACM, vol.24, no.11, pp. 770-772, November 1981.
[8] N. Haller Bellcore, "The S/KEY One-Time Password System," Network Working Group, February 1995.
[9] M.L. Das, A. Saxena, and V.P. Gulati, "A Dynamic ID-based Remote User Authentication Scheme," IEEE Transactions on Consumer Electronics, vol.50, no.2, pp. 629-631, May 2004.
[10] A. Awasthi, "Comment on A dynamic ID-based Remote User Authentication Scheme," Transaction on Cryptology, vol. 01, issue 02, pp. 15-17, September 2004.
[11] C.Y. Lee, C.H. Lin, and C.C. Chang, "An Improved Low Communication Cost User Authentication Scheme for Mobile Communication," Proceedings of the IEEE 19th International Conference on Advanced Information Networking and Applications (AINA 2005), vol. 2, pp. 249-252, March 2005.
[12] N. El-Fishway, M. Nofal, and A. Tadros, "An Effective Approach for Authentication of Mobile Users," IEEE 55th Vehicular Technology Conference (VTC), vol. 2, pp. 598-601, May 2002.
[13] B. Schneier, "Applied cryptography," John Wiley and Sons Inc., New York, 2nd edition, 1996.
[14] N. Haller, C. Metz, P. Nesser, and M. Straw, "A One-Time Password System," IETF RFC 2289, February 1998.
[15] http://www.faqs.org/docs/linux_network/x-082-2-firewall.attacks.html.
[16] C. Lin and T. Hwang, "A Password Authentication Scheme With Secure Password Updating," Computers and Security, vol. 22(1), pp. 68-72(5), January 2003.
[17] H. Chien, J. Jan, and Y. Tseng, "An efficient and practical solution to remote authentication: smart cards," Computers and Security. vol. 21(4), pp. 372-375, August 2002.
[18] M. Hwang, C. Lee, and Y. Tang, "A simple remote user authentication scheme," Mathematical and Computer Modelling, vol. 36(1), pp. 103-107, July 2002.
[19] J. Jeong, M. Chung, and H. Choo, "Secure User Authentication Mechanism for Digital Home Networks," Lecture Note in Computer Science, vol. 4096, pp. 345-354, August 2006.
[20] W. Yang and S. Shieh, "Password authentication schemes with smart cards," Computers and Security, vol. 18(8), pp. 727-733, 1999.
[21] L. Ping, S. Young, E. Pol, W. Shiuh-Jeng, and C. Jin-Fu, "Smart card based secure password authentication scheme," Computers and Security, vol. 15(3), pp. 231-237, 1996.
[22] H. Sun, "Cryptanalysis of password authentication schemes with smart cards," Information Security Conference 2001, pp. 221-223, May 2001.
[23] M. Hwang and L. Li, "A new remote user authentication scheme using smart cards," IEEE Transactions on Consumer Electronics, vol. 46(1), pp. 28-30, February 2000.