HOTP-Based User Authentication Scheme in Home Networks

Binod Vaidya[1], Jong Hyuk Park[2], and Joel J.P.C. Rodrigues[3]

[1] Instituto de Telecomunicações, Covilhã, Portugal
bnvaidya@gmail.com
[2] Dept. of Computer Eng., Kyungnam Univ., Korea
parkjonghyuk1@hotmail.com
[3] Instituto de Telecomunicações,
University of Beira Interior, Covilhã, Portugal
joeljr@ieee.org

Abstract. Home networks are one of the focused areas of research these days. One of the important services that home networks provide is to remotely control home appliances in home network. However, the remote control service causes home networks to have various security threats. Hence, home networks should provide strong security services, especially remote user authentication. In this paper, we provide an efficient solution for authentication scheme to provide secure remote access in home network environments. Our proposed scheme uses HMAC-based one-time password algorithm for the user authentication in home networks. The proposed scheme is not only has several advantage features but also is quite satisfactory in terms of the security requirements of home networks.

1 Introduction

Home networks are one of the focused areas of research these days as they provide remote access control over the connection between information home appliances and information devices on Internet [1,2,3]. This service enables residential users to remotely access and control home appliances such as TVs, lights, washing machines, and refrigerators using their handheld devices. For example, from their office, they can turn on or turn off their gas range using their cellular phone. Figure 1 shows the general architecture for the home networks.

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. In home control protocols, authentication and encryption should be considered as security functions [4].

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

J.H. Park et al. (Eds.): ISA 2009, LNCS 5576, pp. 672–681, 2009.

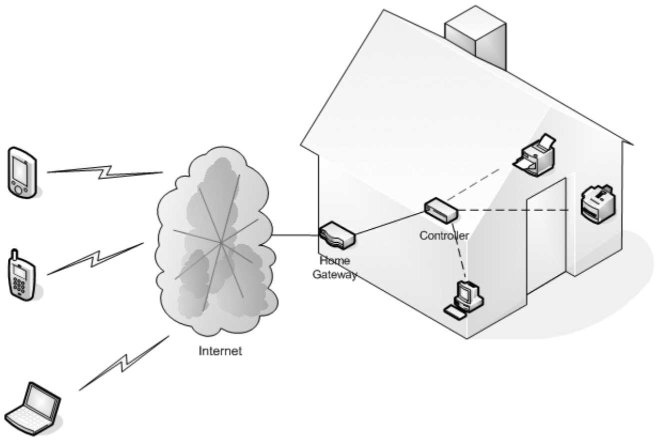

Fig. 1. Home Network Architecture

violate person's privacy and ultimately threaten the life of home users, so appropriate security measures must be considered carefully. Hence, home networks should provide strong security services, especially remote user authentication.

User authentication is a ubiquitous process in the modern Internet era. Password authentication is the simple and convenient remote user authentication mechanism. To prevent direct wiretapping attacks in open network environments, many modern password authentication schemes use one-time passwords.

Thus One-Time Password (OTP) is certainly one of the simplest and most popular forms of two-factor authentication for securing network access.

In this paper, we propose an authentication protocol based on HMAC-Based OTP (HOTP) algorithm, which is suitable for home network environments.

The rest of this paper is organized as follows: Section 2 presents related work, while Section 3 briefly describes HMAC-Based OTP (HOTP) algorithm. Section 4 presents a proposed HOTP-based User Authentication Scheme for home networks and Section 5 gives an analysis of the proposed scheme. Finally, Section 6 concludes the paper and provides future works.

2 Related Work

Password-based authentication scheme that was first introduced in [5] is the most widely used method for remote User Authentication (UA). Existing schemes could be categorized into two types [6]. One uses weak-password approach, while the other uses strong-password one.

Up to now, many one-time password-based authentication schemes have been proposed [7,8,9,10,11]. The purpose of a one-time password (OTP) is to make it more difficult to gain unauthorized access to restricted resources.

In [11], a new user authentication (UA) scheme based on OTP protocol using smart cards for home networks was proposed, which not only can protect against illegal access for home services but also does not allow unnecessary service access by legitimate users.

In HMAC-Based One-Time Password Algorithm (HOTP) [12] based on the HMAC-SHA-1 algorithm [13], it uses an increasing counter value representing the message in the HMAC computation.

In this paper, we have proposed a new user authentication based on HMAC-based OTP algorithm for home network environment which has better security features.

3 HOTP: HMAC-Based One-Time Password Algorithm

On both the client and the server, the choice of algorithm for passcode generation is essentially arbitrary, so long as it provides adequate security and can be used in a user friendly manner (this is particularly relevant for the client).

In this scheme, we chose a counter-based algorithm called HMAC-Based One-Time Password (HOTP) Algorithm that is relatively easy to implement and met the necessary usability requirements. The algorithm is described in detail in [12].

The HOTP algorithm is based on a monotonically increasing counter value and a static symmetric key known only to the client and the server. In order to create the HOTP value, the HMAC-SHA-1 algorithm is used. Each client has a unique shared secret, typically 128 bits or 160 bits in length. The shared secret is combined with an increasing counter, also shared between the client and the server, to generate the current passcode. The obtained HOTP is as follows:

$$\begin{array}{rcl} \text{HOTP}(K,C) & = & \text{Truncate(HMAC-SHA-1}(K,C)) \\ & \text{where} & \text{Truncate represents the function that converts} \\ & & \text{an HMAC-SHA-1 value into an HOTP value; and} \\ & & \text{the key } (K)\text{, the counter } (C)\text{, and Data values} \\ & & \text{are hashed high-order byte first.} \end{array}$$

The actual HOTP algorithm is relatively simple to understand. First, a SHA-1 HMAC generator is initialized using the shared secret. Then the HMAC of the current counter, or moving factor, is computed. Next, through a process called dynamic truncation, certain bytes are extracted from the HMAC. Finally, these bytes are taken modulo 10^n, where n is the number of digits desired in the passcode, to produce the current passcode.

In order for a client to authenticate to a server, both must generate the same passcode. Specifically, assuming that the server has already distributed the shared secret to the client, the client counter and the server counter must be synchronized. When the counters are not synchronized, a process called resynchronization must occur. The HOTP algorithm has two basic mechanisms to resynchronize the server with the client. The most straightforward method is for the client to simply send the counter value over to the server. The server would merely need to verify that the new counter is greater than the current counter. The second method is for the server to maintain a look-ahead window of future passcodes. If the client provides a passcode that lies within this window, the server will ask the user to generate the next passcode and send it to the server.

If two consecutive passcodes match, then the server will resynchronize. While the first of these two resynchronization methods is easier to implement, this project chose to use a look-ahead window to follow industry convention.

4 HOTP-Based User Authentication Scheme

In this section, we propose an efficient remote password authentication scheme based on HOTP algorithm and using smart cards. The security of our scheme depends on the secure HMAC function and encryptions. The nonce or random number is also used to avoid replay attack and the serious time synchronization problem. Table 1 shows the notations used for this scheme.

The proposed scheme consists of registration phase, login/authentication phase and service request phase. The proposed scheme has light-weighted overhead for home networks.

The user transmits information required for HOTP operation in login and authentication phases to Integrated Authentication Server (IAS) through the secure channel, while the IAS writes all the needed information in smart card and issued to the user.

The user can select their own PIN in the registration phase and the IAS doesn't store a password table for each user, but one-way collision-resistant hash functions of the user's identifications.

Service subscribers require mutual authentication between IAS and home gateway server (HG), 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. Figure 2 illustrates the proposed user authentication scheme.

Table 1. Notation used for the proposed scheme

Notation used	Description
ID_C	User's Identifier
ID_{IAS}	IAS's identifier
PIN	User's pin identification number
x	Secret key maintained by the remote system
$h(.)$	One-way hash function
$\oplus$	XOR operation
$\|\|$	Concentration
$H_i(K, C)$	ith HMAC-Based One-Time Password
C_X	8-byte counter value, the moving factor (C - client, S - server, M - Max allowed)
K	shared secret between client and server
S_K	Session key
K_{IAS-HG}	Symmetric key between IAS and HG
T	Timestamp
$E_{K_X}(M)$	Encryption of message M with K_X

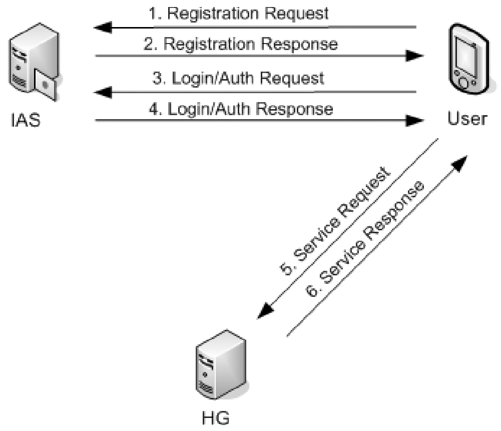

Fig. 2. Proposed User Authentication Scheme

It is assumed that IAS is located on the outside of the home network environment, manages the home gateway, and performs authentication, authorization, and accounting (AAA) functions.

A user authentication protocol is proposed for home network environments, focusing on user authentication for receiving the home service and controlling the service privilege. For the proposed scheme, the following assumptions have been considered:

- The algorithm is counter-based, that means the HOTP algorithm embedded in smart cards.
- The algorithm uses a strong shared secret. The length of the shared secret must be at least 128 bits and preferably of 160 bits.
- The 8-byte counter must be synchronized between the HOTP generator (client) and the HOTP validator (server).
- Each HOTP generator has a different and unique secret K shared between client and server.
- The IAS has established the security association with home gateway server (HG) using symmetric key K_{IAS-HG}

4.1 Registration Phase

The user submits its identity and PIN to the remote system for registration.

1. User sends ID_C, PIN to IAS.

After receiving the registration request, the remote integrated authentication server (IAS) will perform as follows:

1. Compute $v_T = h(ID_C \oplus x)$
2. Compute $e_T = v_T \oplus h(ID_C \| PIN)$
3. Save $ID_C, h(ID_C \| PIN)$
4. Write $h(.), e_T, K, C_M$ to a smart card and
5. Issue securely the card to User

4.2 Login/ Authentication Phase

When the user wants to log into the remote system, he must insert his smart card into the terminal and input the ID_C and $h(ID_C\|PIN)$. The smart card will then perform the following operations:

1. Generate current HOTP
   $H^i_{(K,C_C)} = HOTP(K, C_C, h(ID_C\|PIN))$
2. Increase to C_C to $C_C + 1$
3. Compute $G = h(e_T \oplus H^i_{(K,C_C)})$

The user will send ID^*_C, G to the IAS server.

After receiving the authentication request, the IAS will perform the following operations:

1. Check ID^*_C
2. Compute $H^i_{(K,C_S)} = HOTP(K, C_S, h(ID_C\|PIN))$ with C_S
3. Compute $v'_T = h(ID^*_C \oplus x)$ with the received ID^*_C
4. Compute $G' = h(v'_T \oplus h(ID_C\|PIN) \oplus H^i_{(K,C_S)})$
5. Check if $H^i_{(K,C_C)} = H^i_{(K,C_S)}$ and $G' = G$
6. If the both equations are true, then increase C_S to $C_S + 1$
7. Then compute $K_1 = h(H^i_{(K,CS)}\|K)$ and
8. generate random number K_2 as shared secret
9. Compute $S_K = h(K_1\|K_2\|T)$ and $A_S = h(S_K\|ID_C)$
10. Compute $E_{K_1}(ID_C, ID_{IAS}, K_2, A_S, T)$ and
    $E_{K_{IAS-HG}}(ID_C, ID_{IAS}, K_2, K_1, T)$
11. Send Authentication Response $E_{K_1}(ID_C, ID_{IAS}, K_2, A_S, T)$ along with authentication ticket $E_{K_{IAS-HG}}(ID_C, ID_{IAS}, K_2, K_1, T)$ to the user

The user will perform the following steps:

1. Compute $K_1 = h(H^i_{(K,C_C)}\|K)$
2. Then decrypt $E_{K_1}(ID_C, ID_{IAS}, K_2, A_S, T)$ with K_1 and get K_2
3. Compute $S'_K = h(K'_1\|K_2\|T)$ and $A'_S = h(S_K\|ID_C)$
4. Check if $A'_S = A_S$ to verify the authentication response

4.3 Service Request Phase

In order to use the available services, the authenticated users can request home services to the HG. The user performs the followings:

1. Send $E_{K_{IAS-HG}}(ID_C, ID_{IAS}, K_2, K_1, T)$,
   $E_{S_K}(ID_C, service\_req)$ to the HG.

After receiving the service request, the HG will perform the followings:

1. Decrypt $E_{K_{IAS-HG}}(ID_C, ID_{IAS}, K_2, K_1, T)$ using K_{IAS-HG} and get K_2, K_1, T
2. Compute $S_K = h(K_1\|K_2\|T)$

3. Decrypt $E_{S_K}(ID_C, service\_req)$ with session key S_K
4. Verify ID_C in authentication ticket and service request
5. Send $E_{S_K}(K_1\|T)$ to the user

The user will also authenticate HG by following process:

1. Decrypt $E_{S_K}(K_1\|T)$ with session key S_K
2. Verify K_1, T

5 Analysis of Proposed Scheme

5.1 Features of the Proposed Scheme

In this sub-section, we present some of the following essential criteria for authentication schemes:

A. Freely chosen PIN by the users: In our scheme, each user can choose his own PIN, not decided by the system.

B. No time synchronization: In time stamp-based authentication scheme [14], the clocks of the system and all users' computers must be synchronized with one another and the transmission delay time of the login message also has to be limited. To eliminate the requirement of clock synchronization and the limitation of transmission delay time, our scheme is based on counter and nonce instead of timestamps.

C. Server authentication: Any illegal server cannot cheat a user to log into its system without (K, C) in the proposed scheme. Since it cannot obtain the correct HOTP for that particular user, the login process will be terminated by the user by verifying $AS' = AS$. Also the user will authenticate HG by verifying K_1.

D. Session key agreement: A session key agreed by the user and the remote system generated in every session.

E. Low communication cost: Due to usage of HOTP algorithm, the communication cost is relatively low.

Table 2. Comparison between the proposed scheme with Jeong *et at.*'s scheme in terms of functionalities

Features	Jeong *et at.*'s scheme [11]	Proposed scheme
Freely chosen PIN by the users	Yes	Yes
No time synchronization	Yes	Yes
Server authentication	Yes	Yes
Session key agreement	Yes	Yes
Low communication cost	Yes	Yes
Resynchronization of OTP	No	Yes

Besides, our proposed scheme can provide resynchronization of OTP. Assuming that the server has already distributed the shared secret to the client, the counters in client and server must be synchronized. In the proposed scheme, when the client counter and server counter are not synchronized, HOTP algorithm use two mechanisms as mentioned in Section 3 to resynchronize them.

We compare the proposed scheme with Jeong *et at.*'s scheme [11] as per the above-mentioned features. Table 2 shows the comparison between two schemes.

5.2 Security Analysis of Proposed Scheme

In the proposed scheme, it assumed that there is a symmetric key is shared between IAS and HG. In addition, it is assumed that trusted IAS exists outside the home network, which manages the home gateway, authenticates users, grants privileges, and controls accounting as the home gateway operator.

Authentication between HG and users is achived with the authentication ticket granted by the IAS, and users can request and receive services with a valid authentication ticket until authentication ticket's validity does not expire so there is no requirement to login each time when the users request services.

A. Eavesdropping 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 and Wireless LAN are especially vulnerable to this type of attack. Our scheme can resist eavesdropping attack as all the important messages such as the authentication response, authentication ticket, service request and service response are encrypted with the K_1, symmetric key and session keys respectively.

B. 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. HOTP that is sent to the IAS is computed using counter-based HMAC-SHA1 so attackers cannot replay the password to the authentication server after intercepting user's password.

C. Man-in-the-middle attack: An attacker intercepts and modifies the messages between two parties with a malicious intent without either party knowing that the link between them has been compromised. The proposed scheme is based on HMAC one-time password protocol is that attackers cannot reuse the user's passcode because the passcode is changed each time during login and authentication request to the authentication server. And also the messages are encrypted so the adversaries cannot modify the message.

D. Denial of Service (DoS) attack: The proposed scheme uses HMAC-based OTP as a passcode and protects the user's authentication messages. And the HOTP is changed in each login and authentication phase. Therefore, the proposed scheme prevents DoS attacks from the attackers.

E. 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. The user and authentication server shares the shared secrets needed for HOTP operations during registration phase, so the proposed scheme is secure. And even if the adversary is successful to get $h(ID_C \| PIN)$ from the IAS server, it is very difficult for adversary to gain the HOTP values for HOTP operations because authentication data are calculated by HMAC function.

F. 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.

6 Conclusions and Future Work

In home networks major service is to provide remote control access to home appliances. However, the remote control service causes home networks to have major security threats. In order to provide secure remote access, we propose a simple solution for authentication scheme in home network environments. The proposed user authentication scheme is designed to accept existing home networks which are based on the HOTP algorithm using low-cost smart cards. So, the proposed scheme requires low communication cost and provides high security for secure home networks. Moreover, it protects against illegal access from inside as well as outside home networks.

In future, we will conduct detailed performance evaluation of the proposed scheme with existing representative schemes. Furthermore, we will conduct formal analysis of the proposed scheme as well.

Acknowledgment

Part of this work has been supported by *Instituto de Telecomunicações*, Next Generation Networks and Applications Group (NetGNA), Portugal.

References

1. Schulzrinne, H., Xiaotao, W., Sidiroglou, S., Berger, S.: Ubiquitous computing in home networks. IEEE Communications Magazine 41(11), 128–135 (2003)
2. Saito, T., Tomoda, I., Takabatake, Y., Arni, J., Teramoto, K.: Home gateway architecture and its implementation. IEEE Transactions on Consumer Electronics 46(4), 1161–1166 (2000)

3. Choi, K.S., Lim, S.O., Park, Y.C., Jung, K.M.: Home station, novel architecture of home gateway and its implementations. In: Proc. of the 4th WSEAS International Conference on Applied Informatics and Communications (AIC 2004) (2004)
4. Ise, M., Ogasahara, Y., Watanabe, K., Hatanaka, M., Onoye, T., Niwamoto, H., Keshi, I., Shirakawa, I.: Design and Implementation of Home Network Protocol for Appliance Control Based on IEEE 802.15.4. IJCSNS International Journal of Computer Science and Network Security 7(7), 20–30 (2007)
5. Lamport, L.: Password authentication with insecure communication. Communications of the ACM 24(11), 770–772 (1981)
6. Das, M.L., Saxena, A., Gulati, V.P.: A Dynamic ID-based Remote User Authentication Scheme. IEEE Transactions on Consumer Electronics 50(2), 629–631 (2004)
7. Haller, N., Metz, C., Nesser, P., Straw, M.: A One-Time Password System. IETF RFC 2289 (February 1998)
8. Yeh, T.C., Shen, H.Y., Hwang, J.J.: A Secure One-Time Password Authentication Scheme Using Smart Cards. IEICE Transaction on Communication E85-B(11), 2515–2518 (2002)
9. Tsuji, T., Shimizu, A.: One-time password authentication protocol against theft attacks. IEICE Transactions on Communications E87-B(3), 523–529 (2004)
10. Wang, N.W., Huang, Y.M.: User's Authentication in Media Services by using One-Time Password Authentication Scheme. In: Proc. of the 3rd International Conference on International Information Hiding and Multimedia Signal Processing (IIH-MSP 2007), vol. 01, pp. 623–626 (2007)
11. Jeong, J., Chung, M.Y., Choo, H.: Integrated OTP-Based User Authentication Scheme Using Smart Cards in Home Networks. In: Proc. of the 41st Annual Hawaii International Conference on System Sciences (HICSS 2008) (January 2008)
12. M'Raihi, D., Bellare, M., Hoornaert, F., Naccache, D., Ranen, O.: HOTP: An HMAC-Based One-Time Password Algorithm. IETF RFC 4226 (December 2005)
13. Krawczyk, H., Bellare, M., Canetti, R.: HMAC: Keyed-Hashing for Message Authentication. IETF RFC 2104 (February 1997)
14. Wu, S.T., Chieu, B.C.: A user friendly remote authentication scheme with smart cards. Computers and Security 22(6), 547–550 (2003)