A New Strong-Password Authentication Scheme Using One-way Hash Functions

Chwei-Shyong Tsai,[1,*] Chih-Wei Lin,[2,**] and Min-Shiang Hwang[1,***]

[1]*Department of Management Information System, National Chung Hsing University*

[2]*Department of Information Management, Chaoyang University of Technology*

Recently, Sandirigama et al. have proposed an authentication scheme by the name of SAS and claimed that it has lowest storage, processing, and transmission overhead. In 2001, Lin et al. showed that the protocol is insecure and proposed an optimal strong-password authentication protocol called the OSPA protocol. However, Chen and Ku pointed out that both SAS and OSPA are vulnerable to the stolen-veri»er attack in 2002. Later, Lin, Shen and Hwang proposed a modi»ed OSPA protocol to repair the security Aaw of OSPA protocol. In this paper, we shall propose a new strong-password authentication protocol that not only can withstand many possible attacks including the stolen-veri»er attack, but also eБcient than the modi»ed OSPA protocol.

1. INTRODUCTION

In public network systems, user authentication is the most important part as far as security is concerned. The identities of the communication parties must be veri»ed before they start a new connection to make sure that no harm is done. A variety of password-based authentication schemes have been proposed so far [1ч10]. Existing password authentication schemes can provide a legitimate user with the power to login a remote server and access the resources.

In 2000, Sandirigama et al. [11] proposed a simple strong-password authentication scheme called SAS, and the authors claimed that it can resist the "Man in the middle" attack

* Electronic address: tsaics@nchu.edu.tw

** Electronic address: chihwei@ms70.url.com.tw

*** Electronic address: mshwang@nchu.edu.tw

Table 1. The abbreviations and notations used in this article

U_i	User i
S	Authentication server
A	Attacker
ID_i	Identity of the entity i
P_i	Strong password of the entity i
N_i, N_i'	Random numbers of the entity i
$h(\cdot)$	Strong one-way hash function
$\|\|$	Concatenation
$\oplus$	Exclusive operation
$A \rightarrow B : X$	X is transmitted from A to B

and that it has the lowest storage, processing, and transmission overhead. However, the SAS protocol su«ers from the replay attack and the denial of service attack by Lin et al. [12]. Lin et al. also proposed a new scheme called the OSPA (Optimal Strong-Password Authentication) protocol and claimed that this protocol can withstand the stolen-veri»er attack, replay attack and denial of service attack. Nevertheless, Chen and Ku [13] showed that neither the SAS protocol nor the OSPA protocol could withstand the stolen-veri»er attack. Recently, Lin, Shen and Hwang [14] proposed a modi»ed OSPA protocol to repair the security Aaw of OSPA protocol.

In this article, we shall propose a new strong-password authentication protocol that can withstand the stolen-veri»er attack and other possible attacks. In addition, our new protocol is eБcient than the previous protocol [14]. This article is organized as follows: In Section 2, we shall review the modi»ed OSPA protocol. Then, we shall propose a new protocol in Section 3. In Section 4, we shall analyze the security and eБciency of our protocol. Finally, our brief conclusion will be in Section 5. In Table 1 below, we list the abbreviations and notations used in this article.

2. REVIEW OF LIN-SHEN-HWANG'S PROTOCOL

Let's brieAy review the security enhancement for the OSPA protocol proposed by Lin, Shen and Hwang [14]. The OSPA protocol is composed of two phases, which are the registration and authentication phases. The detailed procedures are described as follows.

Registration phase: Suppose a new user U_i wants to register with the server S for accessing services. The user sends a message $(ID_i, h^2(P_i \oplus N_i))$ to the server S for registration. The server stores the registration message $(ID_i, h^2(P_i \oplus N_i))$ and $K = h^2(P_i \oplus N_i) \oplus h(x||ID_i)$ into the database and U_i's smart card after identifying the identity of the user, respectively. Then, the server issues the smart card to U_i through a secure channel.

Authentication phase: The authentication phase will perform the operations as follows when U_i wants to login via his/her smart card and password.

1. $U_i \rightarrow S : (ID_i, c_2, c_3)$
   Here, c_2 and c_3 are calculated as follows:

$$\begin{aligned} c_1 &= K \oplus h^2(P_i \oplus N_i), \\ c_2 &= c_1 \oplus h(P_i \oplus N_i), \\ c_3 &= h(c_1) \oplus h^2(P_i \oplus N_i'). \end{aligned}$$

2. Upon receiving the login request (ID_i, c_2, c_3) from U_i, the server checks if $h^2(P_i \oplus N_i) = h(c_2')$ holds, where $c_2' = h(x||ID_i) \oplus c_2$. If it holds, the server derives the $h^2(P_i \oplus N_i')$ via $h^2(x||ID_i) \oplus c_3$. The server updates $h^2(P_i \oplus N_i)$ with $h^2(P_i \oplus N_i')$ in the database for next authentication.

3. THE PROPOSED SCHEME

In this section, we shall propose a new strong-password authentication protocol which not only can withstand the stolen-veri»er attack and some attacks, but also eБcient than the previous protocol. Our scheme is composed of two phases: the registration phase and authentication phase.

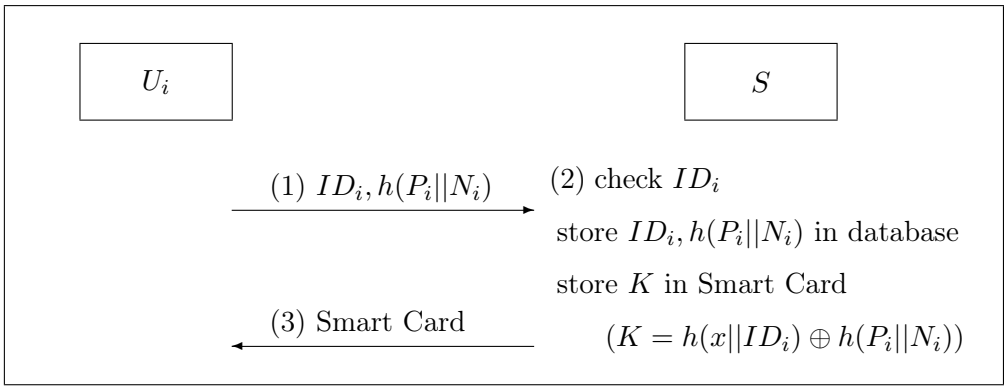

Figure 1. The registration phase of the proposed scheme

Registration phase: Suppose a new user U_i wants to register with the server S for accessing services.

1. $U_i \rightarrow S$: $ID_i, h(P_i||N_i)$
   The user U_i calculates a veri»er $h(P_i||N_i)$ and sends it along with his/her identity ID_i to the server S for registration through a secure channel. Here, P_i and N_i are the strong password nonce of U_i, respectively.

2. $S \rightarrow U_i$: smart card
   The server stores $h(P_i||N_i)$ into the database after the identity of the user is identi»ed. Then, S calculates and writes K into a smart card as well as issues it to U_i,

$$K = h(x||ID_i) \oplus h(P_i||N_i)$$

   where x is a secret key and is maintained by the server.

The registration phase of the proposed scheme is illustrated in Figure 1.

Authentication phase: To access a server, U_i inserts his/her smart card into a login device and keys in the password P_i. Afterwards, the smart card performs the following operations:

1. Calculate $c_1(= K \oplus h(P_i||N_i) = h(x||ID_i))$, where K is stored the smart card.

2. Calculate c_2 as follows:

$$\begin{aligned} c_2 &= h(K) \oplus h(P_i||N_i') \\ &= h(h(x||ID_i) \oplus h(P_i||N_i)) \oplus h(P_i||N_i') \end{aligned}$$

   where N_i' is a new random nonce used against a replay attack.

3. Calculate c_3 to hide the next veri»er for the next login.

$$\begin{aligned} c_3 &= h(c_1 \oplus h(P_i||N_i')) \\ &= h(h(x||ID_i) \oplus h(P_i||N_i')) \end{aligned}$$

4. $U_i \rightarrow S$: (ID_i, c_2, c_3)
   Send a login request (ID_i, c_2, c_3) to the server.

Upon receiving the login request (ID_i, c_2, c_3) from U_i, the server performs the following operations to identify the login user:

1. First, check the format of ID_i. If it does not pass the test, then disconnect this connection.
2. Check the identity of the login user by verifying c_2. The server can derive $h(P_i||N_i')$ by XORing $h(h(x||ID_i) \oplus h(P_i||N_i))$ with c_2, where $h(P_i||N_i)$ is stored in the database of the server. Then, calculate $c_3' = h(h(x||ID_i) \oplus h(P_i||N_i'))$ by using the previously derived $h(P_i||N_i')$. Then, check the equality: $c_3 = c_3'$. If it holds, U_i is authenticated and allowed to access the server. Finally, update the stored veri»er $h(P_i||N_i)$ with $h(P_i||N_i')$ for the next login.

The authentication phase of the proposed scheme is illustrated in Figure 2.

4. ANALYSIS

The security and eБciency of the proposed protocol will be discussed in this section.

4.1. Security Analysis

We show that the proposed scheme can withstand the well-known attacks as follows.

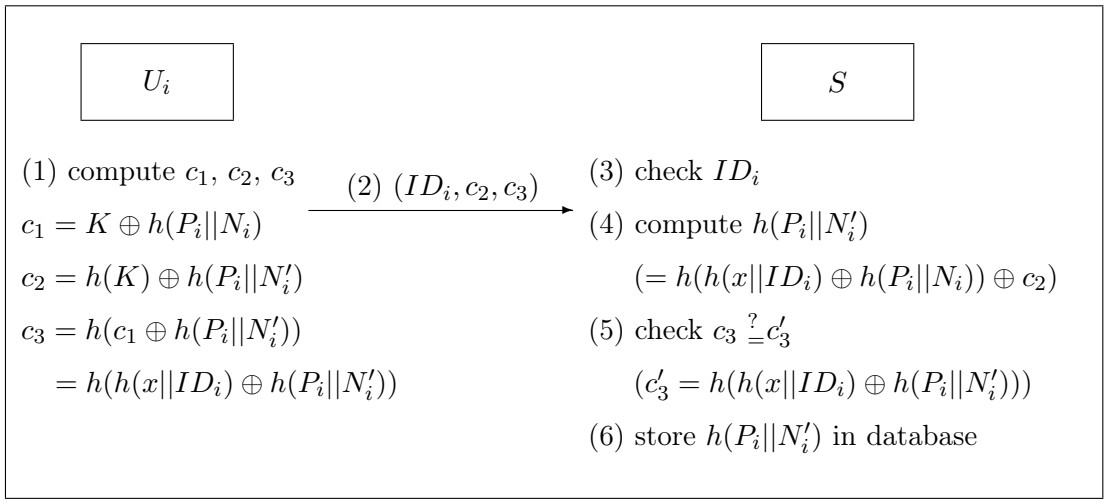

Figure 2. The authentication phase of the proposed scheme

Guessing attack: Assume that an attacker intercepts a login request (ID_i, c_2, c_3) over a public network. The attacker cannot derive the password P_i of the login user from c_2 and c_3. This is because the attacker does not know N_i, N_i' and x, where x is the secret key of the server.

Replaying attack: The user updates the veri»er $h(P||N_i)$ to resist the replay attack at each login. The next veri»er is hidden in the previous session such that c_3 is an implicit next veri»er $h(P||N_i')$. That is, an attacker cannot login the server by replaying the previous login request.

Impersonation attack: An attacker A may impersonate U_i by forging a login request (ID_i, c_{A_2}, c_{A_3}) and sending it to the server, where $c_{A_2} = h(h(x_A||ID_i) \oplus h(P_A||N_A)) \oplus h(P_A||N_A')$ and $c_{A_3} = h(h(x_A||ID_i) \oplus h(P_A||N_A')$. The server will execute the authentication phase for identifying the login user. However, the forged login request (ID_i, c_{A_2}, c_{A_3}) cannot pass because the verifying equation does not hold $(c_{A_3} \neq c'_{A_3})$.

$$\begin{aligned} c_{A_3} &\neq c'_{A_3} \\ &\neq h(h(x||ID_i) \oplus (c_{A_2} \oplus h(h(x||ID_i) \oplus h(P_i||N_i)))) \end{aligned}$$

Therefore, an attacker has no chance to login by launching the impersonation attack.

Stolen-veri»er attack: Assume that an attacker has stolen a veri»er $h(P_i||N_i)$ and intercepted U_i's $(N-1)$th login request (ID_i, c_2, c_3) from a remote server and over the

public network. Even so, he/she cannot derive $h(P_i||N_i')$ and $h(x||ID_i)$ from c_2 and c_3 by using the veri»er $h(P_i||N_i)$, respectively. Therefore, the proposed scheme can withstand the stolen-veri»er attack, since $h(\cdot)$ is a strong one-way hash function.

4.2. EБciency Analysis

Since Lin-Shen-Hwang scheme is only one in the literature can resist the stolen-veri»er attack, we only compare our scheme with Lin-Shen-Hwang scheme in the computational complexities. In Table 2, we see that the eБciency of the proposed scheme is eБcient than the modi»ed OSPA protocol. Here, $T(h)$ and $T(\oplus)$ denote the computation time of the strong one-way function and the exclusive operation, respectively.

In the registration phase of the proposed protocol, it requires two $T(h)$s and one $T(\oplus)$. These computation times include one $T(h)$ for user to generate a veri»er $h(P_i||N_i)$, one $T(h)$ and one $T(\oplus)$ for the server to generate K.

In the authentication phase of the proposed protocol, it requires seven $T(h)$s and six $T(\oplus)$s. The user in this phase requires four $T(h)$s and three $T(\oplus)$s. These computation times include $1T(h) + 1T(\oplus)$, $2T(h) + 1T(\oplus)$, and $1T(h) + 1T(\oplus)$, for user to generate C_1, C_2, and C_3, respectively. The server in this phase requires three $T(h)$s and three $T(\oplus)$s. These computation times include $2T(h) + 2T(\oplus)$ and $1T(h) + 1T(\oplus)$ for server to generate $h(P_i||N_i')$ and check if $c_3 = c_3'$ holds, respectively.

In the registration phase of Lin-Shen-Hwang protocol, it requires three $T(h)$s and two $T(\oplus)$s. These computation times include two $T(h)$s and one $T(\oplus)$ for user to generate a veri»er $h^2(P_i||N_i)$, one $T(h)$ and one $T(\oplus)$ for the server to generate K.

In the authentication phase of Lin-Shen-Hwang protocol, it requires eight $T(h)$s and seven $T(\oplus)$s. The user in this phase requires »ve $T(h)$s and »ve $T(\oplus)$s. These computation times include $2T(h) + 2T(\oplus)$, $1T(\oplus)$, and $3T(h) + 2T(\oplus)$, for user to generate C_1, C_2, and C_3, respectively. The server in this phase requires three $T(h)$s and two $T(\oplus)$s. These computation times include $2T(h) + 1T(\oplus)$ and $1T(h) + 1T(\oplus)$ for server to check if $h^2(P_i \oplus N_i = h(h(x||ID_i) \oplus c_2)$ holds and generate $h^2(P_i||N_i')$, respectively.

Table 2. The computational complexity

Schemes	Registration Phase	Authentication Phase
Our Scheme	$2T(h) + 1T(\oplus)$	$7T(h) + 6T(\oplus)$
Lin-Shen-Hwang Scheme	$3T(h) + 2T(\oplus)$	$8T(h) + 7T(\oplus)$

5. CONCLUSIONS

In this article, we have proposed a new strong-password protocol that can resist the stolen-veri»er attack [13]. Our protocol not only can withstand many well-known attacks but also is eБcient than the previous protocol [14] which can resist the stolen-veri»er attacks.

6. REFERENCES

1. Chi-Kwong Chan, Cheng L. M. Cryptanlysis of timestamp-based password authentication scheme
   Computers and Security. 2002. V. 21. NO 1.
2. Hung-Yu Chien, Jinn-Ke Jan, Yuh-Min Tseng. A modi»ed remote login authentication scheme based on geometric approach
   Systems and Software. 2001. V. 55.
3. Min-Shiang Hwang. A remote password authentication scheme based on the digital signature method
   International Computer Mathematics. 1999. V. 70.
4. Min-Shiang Hwang, Cheng-Chi Lee, Yuan-Liang Tang. An improvement of SPLICE/AS in WIDE against guessing attack
   International Informatica. 2001. V. 12. NO 2.
5. Cheng-Chi Lee, Min-Shiang Hwang, Wei-Pang Yang. A Aexible remote user authentication scheme using smart cards
   ACM Operating Systems Review. 2002. V. 36. NO 3.

6. Cheng-Chi Lee, Li-Hua Li, Min-Shiang Hwang. A remote user authentication scheme using hash functions

   ACM Operating Systems Review. 2002. V. 36. NO 4.

7. Li-Hua Li, Iuon-Chung Lin, Min-Shiang Hwang. A remote password authentication scheme for multi-server architecture using neural networks

   IEEE Trans. Neural Networks. 2001. V. 12. NO 6.

8. Yuan-Liang Tang, Min-Shiang Hwang, Cheng-Chi Lee. A simple remote user authentication scheme

   Mathematical and Computer Modelling. 2002. V. 36.

9. Jau-Ji Shen, Chih-Wei Lin, Min-Shiang Hwang. A modi»ed remote user authentication scheme using smart cars

   accepted and to appear in *IEEE Trans. Consumer Electronics*. 2003.

10. Yang W. H., Shieh S. P. Password authentication schemes with smart cards

    Computers and Security. 1999. v. 18. NO 8.

11. Sandirigama M., Shimizu A., Noda M. T. Simple and secure password authentication protocol (sas)

    IEICE Trans. Communications. 2000. V. E83-B.

12. Lin C. L., Sun H. M., Hwang T. Attacks and solutions on strong-password authentication

    IEICE Trans. Communications. 2001. V. E84-B.

13. Chien-Ming Chen, Wei-Chi Ku. Stolen-veri»er attack on two new strong-password authentication protocols

    IEICE Trans. Communications. 2002 V. E85-B.

14. Chih-Wei Lin, Jau-Ji Shen, Min-Shiang Hwang. Security enhancement for optimal strong-password authentication protocol

    ACM Operating Systems Review. 2003. V. 37. NO 2.