Enhancement of Timestamp-based User Authentication Scheme with Smart Card

Hui-Feng Huang, Hong-Wei Chang, and Po-Kai Yu
(Corresponding author: Hui-Feng Huang)

Department of Computer Science and Information Engineering
National Taichung University of Science and Technology, Taichung 404, Taiwan
(Email: *phoenix@nutc.edu.tw*)

(Received Apr. 12, 2013; revised and accepted May 16, 2013)

Abstract

User authentication is an important technology to guarantee that only the legal users can access resources from the remote server. The advantages of smart cards are storage and computation abilities. Recently, there are many remote user authentication protocols with smart card have been proposed to improve security, efficiency, and functionality extensively by many scholars. This article finds that Awasthi *et al.'s* scheme may suffer impersonate attack, and do not allow changing password freely for the user. Finally, we proposed an improved timestamp-based user authentication scheme. The modified method is more efficient and secure than Awasthi *et al.'s* scheme.

Keywords: Authentication, password, security, smart card

1 Introduction

With rapid development of the network technology, we could access any service from any place and at any time. Password based authentication has been the essential security mechanism for the remote access control systems. In 1981, Lamport [6] proposed a password authentication scheme using a one-way hash function and a password table to achieve remote user authentication for insecure communication. Lamport's scheme is simple and efficient, but it suffers from the replay attack and the impersonation attacks caused by modifying or stealing the hashed password table maintained by the servers.

The advantages of smart cards are storage and computation abilities. There are many remote user authentication protocols with smart card have been proposed to improve security, efficiency, and functionality extensively by many scholars in recent years [2,3,4,5,7,9,10]. However, those previous schemes are still vulnerable for some offline password guessing attack, replay attack and forgery attack [1]. Moreover, some scholars' schemes have to maintain a verified table of password and do not allow changing passwords freely [3,5,7,9,10]. In 2003, Shen *et al.* [9] proposed a timestamp-based password authentication scheme with smart card in which the remote server does not need to store the passwords or verification table for user authentication. Unfortunately, Awasthi *et al.* [1] showed that Shen *et al.*'s scheme is vulnerable to forged login attack, and presented an improved remote authentication scheme which still keeps the feature of the non-storage of data at server side. However, this paper finds that Awasthi *et al.*'s scheme may suffer impersonate attack, and do not allow changing password freely for the user.

To overcome Awasthi *et al.*'s weaknesses, we present an improved password authentication scheme. In the proposed scheme, the remote server does not require any verification information for the users.

The remainder of this paper is organized as follows. We give a brief review of Awasthi *et al.*'s scheme in the next section. In Section 3, the security weakness of Awasthi *et al.*'s given. In Section 4, we present the improved scheme and analyze its security. At last, some conclusions will be made in the last section.

2 Review of Awasthi *et al.'s* Scheme

In this section, we will review Awasthi *et al.*'s scheme [1]. In their scheme, first, the KIC (Key Information Center) is responsible for generating some related parameters. There are four phases in Awasthi *et al.*'s scheme: initialization, registration, login, and authentication phases.

2.1 Initialization Phase

The KIC performs the following steps.

Step 1: Generate two large primes p and q and compute $n = p \times q$.

Step 2: Choose two integers e and d such that $ed = 1 \bmod \phi(n)$, where $\phi(n) = (p-1)(q-1)$ and e and d are the system's public key and private key, respectively.

Step 3: Find an integer g which is a primitive element of modulo n.

2.2 Registration Phase

A new user U_i performs the following steps for the registration phase.

Step 1: U_i sends his/her identifier ID_i and password PW_i to KIC over a secure channel.

Step 2: KIC computes $CID_i = f(ID_i \oplus d)$, $h_i = g^{pw_i \times d} \bmod n$, and $S_i = CID_i^d \bmod n$, where f( ) is a one way function.

Step 3: KIC stores $\{n, e, g, ID_i, S_i, h_i\}$ into a smart card and then sends this smart card to user U_i through a secure channel.

2.3 Login Phase

In this phase, the smart card will execute the following steps.

Step 4: First, U_i inputs his password PW_i and chooses a random number r_i and the current timestamp T_C, then computes X_i and Y_i as follows: $X_i = g^{r_i \cdot pw_i} \bmod n$ and $Y_i = S_i \cdot h_i^{r_i \cdot f(ID_i \cdot T_C)} \bmod n$.

Step 5: U_i sends the login request messages $M = \{ID_i, X_i, Y_i, n, e, g, T_C\}$ to the server S.

2.4 Authentication Phase

After receiving the login request message M at time T_S, S performs the following steps:

Step 1: Verify whether the ID_i is a legitimate user or not.

Step 2: Check timestamp T_s. If $(T_s - T_c) < \Delta T$ holds, S accepts the login request of U_i; otherwise, rejects this request.

Step 3: S computes $CID_i = f(ID_i \oplus d)$.

Step 4: S checks the equation $Y_i^e = CID_i \cdot X_i^{f(CID_i \cdot T_c)} \bmod n$. If the equation is holds, then S accept the login request; otherwise, rejects it.

Step 5: Then S computes $R = (f(ID_i, T_s'))^d \bmod n$, and sends $M' = \{R, T_s'\}$ to U_i, where T_s' is the current timestamp on the server.

After receiving the reply message M' at time T_c', U_i performs the following steps:

Step 1: Check timestamp T_s'. If $(T_c' - T_s') < \Delta T$ holds, U_i accepts the login respond of S; otherwise, stops this procedure.

Step 2: U_i computes $R' = R^e \bmod n$, and then checks If the equation $R' = f(ID_i, T_s')$ holds. If it holds, U_i accepts the S; otherwise, rejects S.

3 Security Analysis Of Awasthi *et al.'s* Scheme

In this section, we will point out that Awashi *et al.*'s scheme may suffer impersonate attack. Moreover, in their scheme, user cannon easily change his/her password without the remote server joining this phase. The detail of the impersonation attack is given below:

1. Assume that an adversary U_A obtains U_i's smart card, and logins request at time T_A.
2. U_A selects a random number $r_A = 0$, then computes $X_i = g^{r_A \cdot pw_A} = 1$ and $Y_i = S_i \cdot h_i^{r_A f(ID_i, T_A)} = S_i \bmod n$, where pw_A is randomly selected by adversary U_A.
3. U_A sends the login request messages $M_A = \{ID_i, X_i, Y_i, n, e, g, T_A\}$ to server S.
4. S verifies whether the ID_i is a legitimate user or not.
5. S checks timestamp T_A. If $(T_s - T_A) < \Delta T$ holds, S accepts the login request of U_i, where T_s is the current timestamp on the server.
6. S computes $CID_i' = f(ID_i \oplus d)$.
7. S checks the equation $Y_i^e = CID_i' \cdot X_i^{f(ID_i \cdot T_A)} \bmod n$, where $X_i = 1$ and $Y_i = S_i = (f(ID_i \oplus d))^d$. In Step 7, it is obvious that $Y_i^e = S_i^e = CID_i' \times 1 = CID_i'$.

After executing above steps, the adversary U_A can pretend as the legitimate user U_i and be successfully authenticated by the server S.

Moreover, in the registration phase, the KIC computer $h_i = g^{PW_i \times d} \bmod n$ and stores it in U_i's smart card. If U_i wants to update his/her password, he/she should be to derive the new $h_i^* = (h_i)^{PW^{-1} PW_i^*} = h_i^{PW_i^* \times d} \bmod n$, where PW_i^* is a new password. However, without knowing the $\phi(n)$ of the server, it is very hard for U_i to obtain $PW_i^{-1} \bmod \phi(n)$. Therefore, in Awasthi *et al.*'s scheme, the user cannot freely change his/ her password without the server S.

4 The Improved Scheme And Security Analysis

In this section, we improve the Awasthi *et al.*'s scheme to remedy their weaknesses and enhance the security. To illustrate the protocol clearly, the notations used in the proposed protocol are the same as Awasthi *et al.*'s scheme. There are four phases in our scheme: initialization, registration, login and authentication, updated password phases. The details steps of the proposed protocol are described as follows:

4.1 Initialization Phase

First, the KIC performs the following steps:

Step 1: Generate two large primes p and q and compute $n = p \times q$.

Step 2: Choose two integers e and d such that $ed = 1 \bmod \phi(n)$, where $\phi(n) = (p-1)(q-1)$ and e and d are the system's public key and private key, respectively.

4.2 Registration Phase

A new user U_i carries out the following steps for the registration phase.

Step 1: U_i sends his/her identifier ID_i and password PW_i to KIC over a secure channel.

Step 2: KIC computes $CID_i = f(ID_i \oplus d)$, and $S_i = (CID_i^d \bmod n) \oplus f(PW_i)$, where f( ) is a one way function.

Step 3: KIC stores $\{n, e, S_i, ID_i\}$ into a smart card and then sends this smart card to user U_i through a secure channel.

4.3 Login And Authentication Phase

In this phase, the smart card will execute the following steps.

Step 1: First, U_i inputs his password PW_i and computes X_i and Y_i as follows:

$X_i = S_i \oplus f(PW_i)$ and $Y_i = X_i^{f(ID_i, T_c)} \bmod n$, where T_c is the current timestamp on the user U_i.

Step 2: U_i sends the login request messages $M = \{ID_i, n, e, T_c, Y_i\}$ to the server S.

Step 3: After receiving the login request message M at time T_s, S verifies whether the ID_i is a legitimate user or not. Next, S checks the current timestamp T_s. If $(T_s - T_c) < \Delta T$ holds, the login request is proceed; otherwise, rejects this request.

Step 4: S computes $CID_i = f(ID_i \oplus d)$ and checks the equation $Y_i^e = f(ID_i \oplus d)^{f(ID_i, T_c)} \bmod n$. If the equation is holds, S accepts the login request; otherwise, rejects it.

Step 5: Then S computes $R = (f(ID_i, T_s'))^d \bmod n$, and sends $M' = \{R, T_s'\}$ to U_i, where T_s' is the current timestamp on the server.

Step 6: After receiving the reply message M' at time T_c', U_i checks the timestamp T_s'. If $(T_c' - T_s') < \Delta T$ holds, U_i accepts the login respond of S; otherwise, stops this procedure.

Step 7: U_i computes $R' = R^e \bmod n$, and then checks if the equation $R' = f(ID_i, T_s')$ holds. If it holds, U_i accepts the server S; otherwise, rejects S.

The above login and authentication process are briefly illustrated in Figure 1.

4.4 Updated Password Phase

In our method, if a user wants to arbitrarily update his password PW_i, he does not need to register with the remote server. It is very convenient for the user to change his password. Now, suppose user U_i would like to change his password, he is only required to perform the following steps.

1. Choose a new password PW_i'.
2. Compute $S_i' = S_i \oplus f(PW_i) \oplus f(PW_i')$, and PW_i is an old password of user U_i.
3. Replace S_i with S_i' on the memory of the smart card. It is accepted because
$$S_i' = S_i \oplus f(PW_i) \oplus f(PW_i') = CID_i^d \oplus f(PW_i'),$$
where $S_i = CID_i^d \oplus f(PW_i)$.

The improvement protocol is based on the RSA cryptosystem [8]. That is $n = p \cdot q$, it is computationally intractable to factorize n when p and q are large enough. Given n, then determining $\phi(n) = (p-1)(q-1)$ is equivalent to factoring n. It lies on the difficulty of the integer factoring problem. Moreover, giving n, e, C, and M, it is intractable to find d such that such that $C = M^d \bmod n$, where $e \times d = 1 \bmod (p-1)(q-1)$. It is also equivalent to factoring n such that such that $e \times d = 1 \bmod (p-1)(q-1)$ and $C = M^d \bmod n$.

Next, we analyze the security of the improvement method as follows. Based on Awasthi *et al.'s* scheme [1], our scheme can overcome the weaknesses indicated above of Section 3. In our improved method, in Steps 1 and 5, an adversary could use the eavesdropped the messages $M = \{ID_i, n, e, T_C, Y_i\}$ and $R = (f(ID_i, T_S'))^d \bmod n$ from the communication network, where $Y_i = X_i^{f(ID_i, T_c)} = (f(ID_i \oplus d)^d)^{f(ID_i, T)_c} \bmod n$. Even if an adversary knows the messages n, R, and Y_i, it is exceedingly difficult for him to derive d, p, and q for $n = p \cdot q$. Since d, p, and q are based on the difficulty of the integer factoring problem. Without having the value of p and q, it is not easy to guess the secret d of the server S. The probability of obtaining the exactly R and Y_i is equivalent to performing an exhaustive search on p and q. Hence, the off-line guessing attack is thwarted by the improved protocol. Moreover, without any password PW_i of the U_i in the transmitted messages R and Y_i, it is very hard for the adversary to derive the password of U_i from the network.

With regard to efficiency and communications, for convenience, we define related notations to analyze the computational complexity. The notation Te means the time for one modular exponentiation, T_m denotes the time for one modular multiplication computation, and T_h denotes

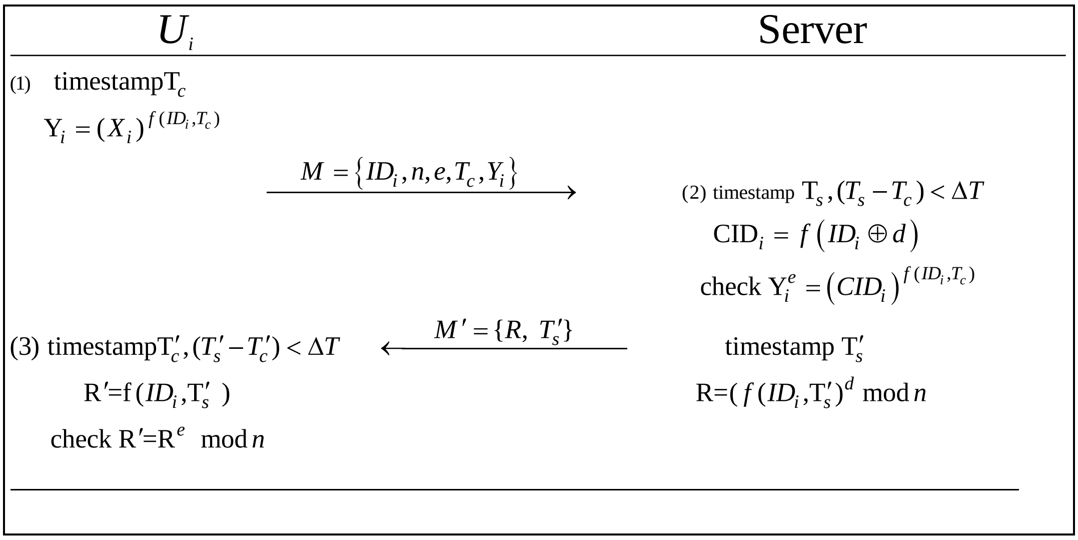

Figure 1: The proposed of login and authentication phase

Table 1: Comparisons of computation and transmission for two schemes

Schemes	Awasthi *et al.'s*	The improved scheme
Computations for user to achieve authentication	$3Te + 3T_m + 2T_h$	$2Te + 2T_h$
Computations for server to achieve authentication	$3Te + 1T_m + 3T_h$	$3Te + 2T_h$

the time for executing the adopted one-way hash function in one's scheme. Note that the times for computing modular addition is ignored, since they are much smaller than Te, T_m, and T_h.

We summarize the comparisons of the proposed scheme with Awasthi *et al.'s* in Table 1. As shown in Table 1, in Awasthi *et al.'s* scheme [8], each user needs to perform two hash function computation ($2T_h$), three modular multiplication computation ($3T_m$), and three modular exponentiations ($3Te$) for authentication. And it is required three hash function computation ($3T_h$), one modular multiplication computation ($1T_m$), and three modular exponentiations ($3Te$) for the server in Awasthi *et al.'s* authentication phase.

In the improved scheme, the computation time for each user to achieve mutual authentication is two hash function computations ($2T_h$) and two modular exponentiations ($2Te$).Consequently, the improved method needs two hash function computations ($2T_h$) and three modular exponentiations ($3Te$) to achieve mutual authentication for the server. Therefore, the improved method is more efficient than Awasthi *et al.'s* scheme.

5 Conclusions

In this paper, we have proposed an improvement to overcome the weaknesses of Awasthi *et al.'s*. The improved method can provide the following characters: (1) no password table is required for KIC and the designated servers; (2) users can freely choose their own passwords; (3) users may update their passwords after registration phase; (4) it supplies mutual authentication between the user and the designated server. In addition, the improved method is more efficient than Awasthi *et al.'s* scheme.

Acknowledgments

This research was partially supported by the National Science Council, Taiwan, under contract no: (101-2221-E-025-017).

References

[1] K. Awasthi, K. S. Srivastava, and R. C. Mittal, "An improved timestamp-based remote user authentication scheme," *Computers and Electrical Engineering*, vol. 37, pp. 869-874, 2011.

[2] C. C. Chang and C. Y. Lee, "A smart card-based authentication scheme using user identify cryptography," *International Journal of Network Security*, vol. 15, no. 2, pp. 139-147, 2013.

[3] H. Y. Chien, J. K. Jan, and Y. M. Tseng, "An efficient and practical solution to remote authentication: Smart card," *Computer & Security*, vol. 21, pp. 372-375, 2002.

[4] S. T. Hsu, C. C. Yang, and M. S. Hwang, "A study of public key encryption with keyword search", *International Journal of Network Security*, vol. 15, no. 2, pp. 71-79, 2013.

[5] M. S. Hwang and L. H. Li, "A new remote user authentication scheme using smart cards," I*EEE Transactions on Consumer Electronics*, vol. 46, pp. 28-30, 2000.

[6] L. Lamport, "Password authentication with insecure communication," *Communication of ACM*, vol. 24, pp. 770-772, 1981.

[7] J. Y. Liu, A. M. Zhou, and M. X. Gao, "A new mutual authentication scheme based on nonce and smart cards," *Computer Communications,* vol. 31, pp. 2205–2209, June 2008.

[8] R. L. Rivest, A. Shamir, and L.M. Adleman, "A method for obtaining digital signatures and public key cryptosystems," *Communications of the ACM*, vol. 21, pp. 120-126, Feb. 1978.

[9] J. J. Shen, C. W. Lin, and M. S. Hwang, "A modified remote user authentication scheme using smart cards," *IEEE Transactions on Consumer Electronics*, vol. 49, pp. 414-416, 2003.

[10] H. M. Sun, "An efficient remote user authentication scheme using smart cards," *IEEE Transactions on Consumer Electronics,* vol. 46, pp. 958-961, 2000.

Hui-Feng Huang received her M. S. and Ph.D. degrees in Mathematics from National Taiwan University and Computer Science and Information Engineering from National Chung Cheng University, respectively. Currently, she is a professor at the Department of Computer Science and Information Engineering in National Taichung University of Science and Technology. Her research interests focus on the areas of cryptography and information security, network security, algorithm, and electronic commerce etc.

Hong-Wei Chang received the B.C.S. degrees from Department of Computer Science and Information Engineering in National Taichung University of Science and Technology, Taiwan, ROC in 2011. Currently, he is a master of Computer Science and Information Engineering student in National Taichung University of Science and Technology, Taiwan, ROC. His current research interests focus on the cryptography, information security, network security and electronic commerce etc.

Po-Kai Yu received he B.C.S. degree and M.S. student in Computer Science and Information Engineering from Southern Taiwan University of Science and Technology and National Taichung University of Science and Technology, respectively. Currently, he is a student at the Department of Computer Science and Information Engineering in National Taichung University of Science and Technology. He research interests focus on the areas of Cryptography and information security, network security, and electronic commerce etc.