A Friendly Password Mutual Authentication Scheme for Remote-Login Network Systems

Chin-Chen Chang[1, 2] and Chia-Yin Lee[2]
[1] *Department of Information Engineering and Computer Science, Feng Chia University, Taichung 407, Taiwan*
[2] *Department of Computer Science and Information Engineering National Chung Cheng University, Chiayi 621, Taiwan*

Abstract

In 2000, Sun proposed a user authentication scheme without using a password table but the user's password is assigned by the server. Due to this reason, Wu and Chieu proposed an improved scheme to overcome the drawback in 2003. Their scheme provides users to choose and change passwords freely. However, Yang and Wang has presented the possible attacks on Wu-Chieu scheme in 2004. In this article, we proposed an efficient scheme to avoid the weakness of Wu-Chieu scheme. Besides, our scheme provides the feature of mutual authentication between the user and the server.

Keywords: *Remote-login, smart card, one-way hash function, forgery attack, mutual authentication*

1. Introduction

Recently, many user authentication schemes have been purposed [1]-[4]. Without using a password table, Sun [5] proposed a user authentication scheme based on one-way hash functions in 2000. One of the characteristics that passwords are assigned to the registered users by the server is a drawback in Sun's schemes. In 2003, Wu and Chieu [6] proposed a user authentication scheme with smart cards to overcome the drawback. Their scheme provides that users be able to choose and change their passwords freely. However, Yang and Wang [7] have presented two possible attacks on their scheme in 2004. In this article, we propose an efficient protocol with mutual authentication. Without using modular exponential computation operator, our scheme not only solves the problems but also reduces the computational cost.

The remainder of this article is organized as follows. Section 2 gives the review of Wu-Chies's scheme and its weakness. In Section 3, an efficient protocol with mutual authentication is proposed. We analyze the secure characteristics of our scheme in Section 4 and compare it with Wu-Chieu's in Section 5.Finally, we give some conclusions in Section 6.

2. A review of Wu-Chieu scheme and its weakness

Wu and Chieu's scheme consists of three phases: the registration phase, the login phase and the authentication phase. At first, the user U_i submits his (or her) identity ID_i and a chosen password PW_i to the server for registration. Let p be a large prime. On receiving the request, the server does the following.

Step 1: Compute $A_i = h(ID_i \| x)$, where x is the server's secret key and $h(\cdot)$ is a secure

one-way hash function.
Step 2: Compute $B_i = g^{A_i \cdot h(PW_i)} \bmod p$, where g is a public primitive element in $GF(p)$.
Step 3: The server issues a smart card, which contains secret information $\{ID_i,\ A_i,\ B_i,\ h(\cdot),\ p,\ g\}$.

In the login phase, the user U_i first inserts his (or her) smart card into the device and keys in the identity ID_i with the corresponding password PW_i^*, and then the smart card performs the following operations:
Step 1: Compute $B_i^* = g^{A_i \cdot h(PW_i^*)} \bmod p$, and $C_1 = h(T \oplus B_i)$ (T denotes the current date and time).
Step 2: Send the message $m = \{ID_i,\ B_i^*,\ C_1,\ T\}$ to the server.

In the authentication phase, the server authenticates the user with the following steps:
Step 1: Test the validity of ID_i, if the format of ID_i is incorrect, the server rejects the login request.
Step 2: Test the timestamp T with T' (current date and time). If the time interval $(T' - T) \geq \Delta T$, where ΔT denotes the expected valid time interval for transmission delay, then the server rejects the login request.
Step 3: Compute $C_1^* = h(T \oplus B_i^*)$ and check whether $C_1^* \stackrel{?}{=} C_1$ or not. If they are equal, it means that PW_i^* is equal to PW_i. Then the system accepts the login request. Otherwise, it rejects the request.

In 2004, Yang and Wang have presented how the possible attacks by an intruder can be succeeded.

2.1 Password guessing attack

An intruder can collect the login message $m = \{ID_i,\ B_i^*,\ C_1,\ T\}$, from that he (or she) can obtain the correct value of B_i since $B_i^* = B_i$ for a legal user in the login phase. Due to the smart card stores some secure parameters, if an intruder obtains a legal user's smart card, he (or she) can guess the password to generate the parameter $B_i^* = g^{A_i \cdot h(PW_i^*)} \bmod p$. If the computed value is the same as B_i, the intruder can get the correct password of a legal user.

2.2 The forgery attack

After collecting a legal login message $m = \{ID_i,\ B_i^*,\ C_1,\ T\}$, the intruder can forge the verifiable value C_{1e} by computing $C_{1e} = h(T' \oplus B_i)$, where T' is the update timestamp. Therefore, the intruder can send the message $m_e = \{ID_i,\ B_i^*,\ C_{1e},\ T'\}$ to the server. We can see that, with this m_e, he (or she) will pass through the verification phase and then masquerade successfully the legal user U_i.

From the above analysis, we know that Wu-Chieu scheme is insecure.

3. The proposed user authentication scheme

Our scheme is also divided into the registration phase, the login phase and the authentication phase. Besides, the notations of the scheme are exactly the same as those used in Wu-Chieu scheme.

First, U_i submits the ID_i and a chosen PW_i to the server. Then the server does the following.

Step 1: Use its private key x to obtain A_i by computing $A_i = h(ID_i \| x)$, where $h(\cdot)$ is a one-way hash function with an output value sized 512 bits, e.g. SHA-512 [8]. Then it computes $B_i = h(A_i \| h(PW_i))$.

Step 2: The server issues a smart card with $\{ID_i,\ A_i,\ B_i,\ h(\cdot)\}$ to the user through a secure channel.

In the login phase, a user U_i inserts his (or her) smart card into the card reader and keys in the identity ID_i with the corresponding password PW_i^*. The smart card will perform the following operations:

Step 1: Obtain B_i^* by computing $B_i^* = h(A_i \| h(PW_i^*))$, $C_1 = h(T_1 \oplus B_i)$ and $C_2 = B_i^* \oplus h(A_i \oplus T_1)$.

Step 2: Send a message $m_1 = \{ID_i,\ C_1,\ C_2,\ T_1\}$ to the server.

In the authentication phase, the server checks the validity of ID_i. Then, it does following.

Step 1: Verify the timestamp T_1 with the current date and time T'. If $(T' - T_1) \geq \Delta T$, where ΔT denotes the expected valid time interval for transmission delay, then the server rejects the login request.

Step 2: Compute $A_i = h(ID_i \| x)$ and obtain B_i^* by computing $B_i^* = C_2 \oplus h(A_i \oplus T_1)$.

Step 3: Compute $C_1^* = h(T_1 \oplus B_i^*)$ and check whether $C_1^* \stackrel{?}{=} C_1$ or not. If they are equal, it means that the user's password PW_i^* is correct (the user is authenticated). Otherwise, it rejects the login request.

Step 4: Send the $m_2 = \{C_3,\ T_2\}$ to the user, where $C_3 = h(h(A_i \| B_i^*) \oplus T_2)$ and T_2 is the current timestamp.

Step 5: After receiving the message $m_2 = \{C_3,\ T_2\}$, U_i checks if $T'' - T_2 \stackrel{?}{\leq} \Delta T$, where T'' is current date and time. If $T'' - T_2 \leq \Delta T$ holds, then the smart card computes $C_3^* = h(h(A_i \| B_i) \oplus T_2)$.

Step 6: Check whether $C_3^* \stackrel{?}{=} C_3$ or not. If the result is valid, U_i believes that the server is authenticated. We show the authentication protocol in Fig. 1.

4. Security analysis

Now, we analyze the security of our scheme as follows.

1) It is hard to derive the parameters A_i and B_i from a smart card directly.
2) Due to the parameter A_i is unknown and the one-way hash function (e.g. SHA-512) is used, it is difficult to guess PW_i from the equations $B_i^* = h(A_i \| h(PW_i^*))$ and $C_2 = B_i^* \oplus h(A_i \oplus T_1)$.
3) Replaying attacks (An intruder might replay an old login message $m_1 = \{ID_i,\ C_2,\ C_1,\ T_1\}$ to the server) cannot work because it will make Step 1 of the

authentication phase unsuccessful.

4) No one can compute a valid $C_1 = h(T_1 \oplus B_i)$, because it must be derived from PW_i and A_i. However, PW_i and A_i cannot be obtained if the server's secret key x is unknown.
5) An intruder might collect the legal login message $m_1 = \{ID_i,\ C_2,\ C_1,\ T_1\}$ and try to modify it into $m_e = \{ID_i,\ C_2,\ C_{1e},\ T_e\}$. Here T_e is the current date and time. He (or she) has to compute $C_{1e} = h(T_e \oplus B_i)$. However, the parameter $B_i = B_i^*$ cannot be obtained from C_2 without knowing A_i.
6) An intruder might forge the message $m_e = \{ID_i,\ C_{2e},\ C_{1e},\ T_e\}$, where $C_{2e} = 0$. In this case, due to the parameter $B_i^* = (C_{2e} \oplus A_i) = A_i$, he (or she) has to compute the verifiable value C_{1e} such that $C_{1e} = h(T_e \oplus B_i^*) = h(T_e \oplus A_i)$. Still, he (or she) cannot obtain the correct value of C_{1e}.
7) Since B_i^* and A_i are the message digests of SHA-512 (i.e. 512 bits in length), the probability of successfully guessing the correct values of B_i^* and A_i from C_2 is less than $(2^{512} \times 2^{512})^{-1}$. Obtaining B_i^* and A_i by just knowing C_2 is hard.
8) It is hard to obtain the correct C_3 such that $C_3 = C_3^* = h(h(A_i \| B_i) \oplus T_2)$ by knowing T_2 only.

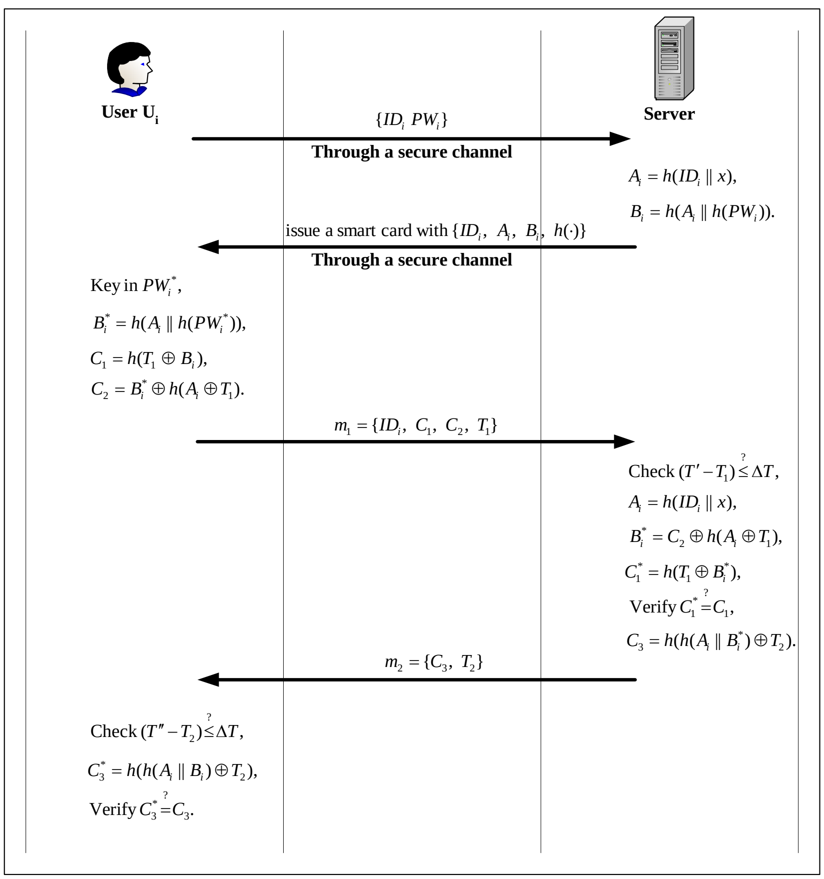

Fig. 1. The mutual authentication protocol

Table 1. The comparison of scheme and Wu-chiew's

Phases and Feature	Wu-Chieu scheme	Our scheme
Computation cost of registration phase	$1T_{EXP}+1T_{MUL}+2T_H$	$3T_H$
Computation cost of login phase	$1T_{EXP}+1T_{MUL}+2T_H+1T_{XOR}$	$3T_H+3T_{XOR}$
Computation cost of authentication phase	$1T_H+1T_{XOR}$	$6T_H+5T_{XOR}$
Mutual authentication	No	Yes

5. Comparisons

We define that T_{EXP} is the time needed by modular exponential computation; T_H is the time needed by one-way hash function $h(\cdot)$; T_{MUL} is the multiplication time; T_{XOR} is the time needed by exclusive-or $(\oplus)$.

We know that a modular exponential computation is much more time consuming than $h(\cdot)$. Besides, $\oplus$ can be performed efficiently. From Table 1, only one-way hash functions and exclusive-or operations are required in our scheme. So our scheme can be implemented efficiently and it provides the feature of mutual authentication.

6. Conclusions

In this article, we have shown the weakness of the Wu-Chieu scheme and then propose an improved scheme to solve these problems. The proposed scheme possesses all the merits of the existing methods and provides mutual authentication between the user and the server. We also analyze the security and computation cost required for the proposed scheme. Our scheme uses only low-cost functions and thus can be executed very efficiently. It could be easily to be implemented on a smart card with low computation capability.

7. References

[1] Lamport, L., "Password authentication with insecure communication," Communications of the ACM, Vol. 24, (1981) 770-772.

[2] Wu, T. C., "Remote login authentication scheme based on a geometric approach," Computer Communications, Vol. 18, No. 12, (1995) 959-963.

[3] Hwang, M. S., "A remote password authentication scheme based on the digital signature method," International Journal of Computer Mathematics, Vol. 70, (1999) 657-666.

[4] Hwang, M. S. and Li, L. H., "A new remote user authentication scheme using smart cards," IEEE Tr*ansactions on Consumer Electronics*, Vol. 46, No. 1, (2000) 28-30.

[5] Sun, H. M., "An efficient remote use authentication scheme using smart cards," *IEEE Transactions on Consumer Electronics*, Vol. 46, No. 4, (2000) 958-961.

[6] Wu, S. T. and Chieu, B. C., "A user friendly remote authentication scheme with smart cards," *Computers & Security*, Vol. 22, No. 6, (2003) 547-550.

[7] Yang, C. C. and Wang, R. C., "Cryptanalysis of a user friendly remote authentication scheme with smart cards," *Computers & Security*, Vol. 23, No. 5, (2004) 425-427.

[8] NIST, U.S. Department of Commerce, "Secure hash standard," *U.S. Federal Information Processing Standard (FIPS) 180-2*, (2002).