SECURITY ENHANCEMENT FOR A LOW COMPUTATION COST USER AUTHENTICATION SCHEME

Behnam Sattarzadeh, Mahdi Asadpour and Rasool Jalili
Computer Engineering Department, Sharif University of Technology, Azadi ave, Tehran, Iran.

Keywords: Forgery attack, Authentication, Smart card.

Abstract: In 2003, Wu and Chieu proposed a user friendly remote authentication scheme using smart cards. Later, Yang and Wang pointed out that Wu and Chieu's scheme is vulnerable to the password guessing and forgery attacks. Recently, Lee et al. proposed an improved authentication scheme and claimed that their scheme is secure against forgery attack. However, in this paper, we illustrate that Lee et al.'s scheme is still vulnerable to the forgery attack. We also propose an enhancement of the scheme to resist such that attack.

1 INTRODUCTION

User authentication is an important security topic for remote login systems and there are many schemes existed for this purpose. Among them, the password scheme is the most convenient and widely adopted one (Lin and Hwang, 2003).

In 1981, Lamport proposed a remote authentication scheme for insecure communication (Lamport, 1981). The scheme could resist against replay attack, however it needed a password table for the user's authentication and that may cause problem if intruders can modify the passwords stored in the password table (Hwang and Li, 2000).

Sun, 2000, proposed an efficient remote user authentication scheme using smart card (Sun, 2000). In his scheme, no password table is required to keep in, but the password of the user is generated by the system and the lengthy assigned password does not provide adequate satisfaction for the user.

Next in 2003, Wu and Chieu proposed a user friendly remote authentication scheme to improve the disadvantage of Sun's scheme (Wu and Chieu, 2003). Their scheme allows the user to choose or change his password freely but it requires costly exponential computation. Since the computation capabilities of smart cards are limited, time-consuming operations are not suitable in such environments (Fan et al., 2005).

Later Yang and Wang in (Yang and Wang, 2004), independently Min–Shiang Hwang et al. in (Hwang et al., 2005) and Kuo–Feng Hwang et al. in (Hwang and Liao, 2005), have pointed out the scheme suffers from the password guessing and forgery attacks.

Recently Lee et al. proposed an improved low computation cost user authentication scheme, which uses one-way hash functions instead of exponential operations to be suitable for smart card applications and mobile devices (Lee et al., 2005). By the way, they claimed that their scheme not only is secure against forgery attack, but also can be used for mobile communications.

In this paper, we show that Lee et al.'s authentication scheme still suffers from the forgery attack. Then we present an enhancement of the scheme to resolve that problem.

The rest of this paper is organized as follows. In the following section, we review the Lee et al.'s scheme. In section 3, we illustrate that their scheme is insecure against forgery attack. In section 4, an improved scheme is proposed to overcome this attack, followed by its security and computation cost analyses. Finally, a concluding remark is given in section 6.

2 REVIEW OF LEE ET AL.'S SCHEME

There are three phases in the scheme: *registration*, *login* and *authentication* phases. We recall the three phases in the following (Figure 1).

Sattarzadeh B., Asadpour M. and Jalili R. (2006).
SECURITY ENHANCEMENT FOR A LOW COMPUTATION COST USER AUTHENTICATION SCHEME.
In *Proceedings of the International Conference on Security and Cryptography*, pages 5-8
DOI: 10.5220/0002099900050008

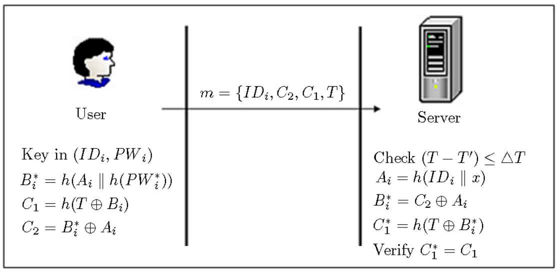
User
Server
$m = \{ID_i, C_2, C_1, T\}$
Key in (ID_i, PW_i)
$B_i^* = h(A_i \parallel h(PW_i^*))$
$C_1 = h(T \oplus B_i)$
$C_2 = B_i^* \oplus A_i$
Check $(T - T') \leq \triangle T$
$A_i = h(ID_i \parallel x)$
$B_i^* = C_2 \oplus A_i$
$C_1^* = h(T \oplus B_i^*)$
Verify $C_1^* = C_1$

Figure 1: Login and authentication phases in Lee et al.'s scheme.

2.1 Registration Phase

The user submits her/his identity ID_i and a chosen password PW_i to the server. Upon receiving the registration request, the server performs the following steps:

1. Compute $A_i = h(ID_i \parallel x)$, where x is the server's private key and $h(.)$ is a one-way hash function.
2. Compute $B_i = h(A_i \parallel h(PW_i))$.
3. The server issues a smart card with the secure information $\{ID_i, A_i, B_i, h(.)\}$, and delivers it to the user through a secure channel.

2.2 Login Phase

When the user wants to login, she/he inserts her/his smart card into the card reader and keys in the identity ID_i and password PW_i^*, then the smart card performs the following operations:

1. Compute
$$\begin{aligned} B_i^* &= h(A_i \parallel h(PW_i^*)), \\ C_1 &= h(T \oplus B_i) \quad \text{and} \\ C_2 &= B_i^* \oplus A_i, \end{aligned}$$
where A_i and B_i are stored in the smart card and T is the current date and time.
2. Send the login message $m = \{ID_i, C_2, C_1, T\}$ to the server.

2.3 Authentication Phase

After receiving the message m at the time T', the server first checks the format of ID_i to make sure whether it is valid. Then, the server authenticates the user with the following steps:

1. Verify whether the $(T' - T)$ is in the valid time interval $\triangle T$. If it is not, the system rejects the login request.
2. Compute $A_i = h(ID_i \parallel x)$, and obtain B_i^* by computing $B_i^* = C_2 \oplus A_i$.

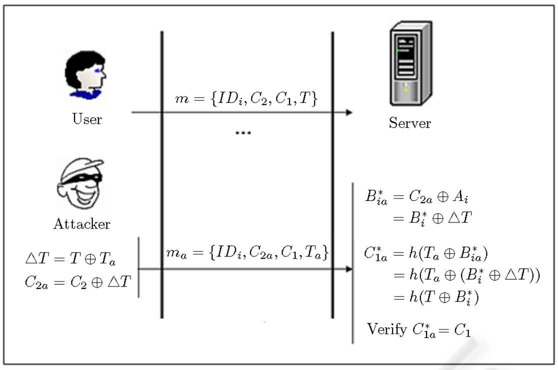
User
Server
$m = \{ID_i, C_2, C_1, T\}$
...
Attacker
$\triangle T = T \oplus T_a$
$C_{2a} = C_2 \oplus \triangle T$
$m_a = \{ID_i, C_{2a}, C_1, T_a\}$
$B_{ia}^* = C_{2a} \oplus A_i$
$= B_i^* \oplus \triangle T$
$C_{1a}^* = h(T_a \oplus B_{ia}^*)$
$= h(T_a \oplus (B_i^* \oplus \triangle T))$
$= h(T \oplus B_i^*)$
Verify $C_{1a}^* = C_1$

Figure 2: A forgery attack on Lee et al.'s scheme.

3. Compute $C_1^* = h(T \oplus B_i^*)$. If C_1^* matches with C_1, the system will accept the login request. Otherwise, it rejects the login request.

3 FORGERY ATTACK ON LEE ET AL.'S SCHEME

In this section, we present a forgery attack against Lee et al.'s scheme, as summarized in Figure 2. Forgery attack occurs when an attacker pretends to be a legal user and is successfully authenticated by the server.

Suppose the user identifier is ID_i. An adversary can forge a valid login request for ID_i using the following steps:

1. Intercept one of user's login messages, say $\{ID_i, C_2, C_1, T\}$.
2. Compute
$$\begin{aligned} \triangle T &= T \oplus T_a \quad \text{and} \\ C_{2a} &= C_2 \oplus \triangle T, \end{aligned}$$
where T_a denotes the login date and time of the attacker.
3. Send $m_a = \{ID_i, C_{2a}, C_1, T_a\}$ to the server.

After receiving the message m_a at time T', the server verifies ID_i and T_a. If they are valid, the server performs the following steps:

1. Compute $A_i = h(ID_i \parallel x)$, and B_{ia}^* as:
$$\begin{aligned} B_{ia}^* &= C_{2a} \oplus A_i \\ &= (C_2 \oplus \triangle T) \oplus A_i \\ &= ((B_i^* \oplus A_i) \oplus \triangle T) \oplus A_i \\ &= B_i^* \oplus \triangle T \oplus A_i \oplus A_i \\ &= B_i^* \oplus \triangle T \end{aligned}$$

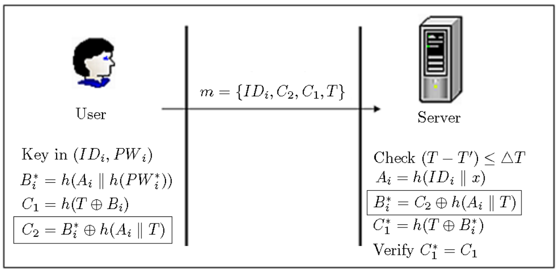
User
$m = \{ID_i, C_2, C_1, T\}$
Server
Key in (ID_i, PW_i)
$B_i^* = h(A_i \parallel h(PW_i^*))$
$C_1 = h(T \oplus B_i)$
$\boxed{C_2 = B_i^* \oplus h(A_i \parallel T)}$
Check $(T - T') \leq \triangle T$
$A_i = h(ID_i \parallel x)$
$\boxed{B_i^* = C_2 \oplus h(A_i \parallel T)}$
$C_1^* = h(T \oplus B_i^*)$
Verify $C_1^* = C_1$

Figure 3: Login and authentication phases of improved scheme.

2. Compute C_{1a}^* as:

$$\begin{aligned} C_{1a}^* &= h(T_a \oplus B_{ia}^*) \\ &= h(T_a \oplus (B_i^* \oplus \triangle T)) \\ &= h(T_a \oplus (B_i^* \oplus (T \oplus T_a))) \\ &= h(T \oplus B_i^* \oplus T_a \oplus T_a) \\ &= h(T \oplus B_i^*) \end{aligned}$$

As you find, the server can verify the equation $C_{1a}^* = C_1$, then it will accept this forged login request. By generalizing the above attack, an adversary can easily pretend to be any legal user and login to server at any time.

4 THE IMPROVED SCHEME

In this section, we propose an improvement on Lee et al.'s scheme to resist the attack, stated in previous section. As a summary, we only change the structure of message C_2 from $B_i^* \oplus A_i$ to $B_i^* \oplus h(A_i \parallel T)$. Now, C_2 depends on the time of the login message T through one additional one-way hash function. The proposed scheme is described as follows (Figure 3).

4.1 Registration Phase

The registration phase is the same as that of Lee et al.'s scheme.

4.2 Login Phase

The user inserts the smart card into the card reader and keys in identity ID_i and password PW_i^*, then the smart card performs the following operations:

1. Compute

$$\begin{aligned} B_i^* &= h(A_i \parallel h(PW_i^*)), \\ C_1 &= h(T \oplus B_i) \quad \text{and} \\ C_2 &= B_i^* \oplus h(A_i \parallel T), \end{aligned}$$

2. Send the login message $m = \{ID_i, C_2, C_1, T\}$ to the server.

4.3 Authentication Phase

Upon receiving the message m at the time T', first, server checks the format of ID_i. Then, the server authenticates the user with the following steps:

1. Verify whether the $(T' - T)$ is in the valid time interval $\triangle T$. If it is not, the system rejects the login request.
2. Compute

$$\begin{aligned} A_i &= h(ID_i \parallel x), \quad \text{and} \\ B_i^* &= C_2 \oplus h(A_i \parallel T). \end{aligned}$$

3. Compute $C_1^* = h(T \oplus B_i^*)$. If C_1^* matches with C_1, the system will accept the login request. Otherwise, it rejects the login request.

5 ANALYSIS

Since our scheme is a slight modification of the Lee et al.'s scheme and the security of their scheme have already been demonstrated in (Lee et al., 2005), so in the following subsection, we only discuss the difference between their scheme and ours in terms of security. Subsequently the computation cost analysis will be presented.

5.1 Security Analysis

We here demonstrate that the proposed scheme can withstand the forgery attack rather than other attacks described in Lee et al.'s scheme.

Assume that an attacker may impersonate ID_i by forging a login request $\{ID_i, C_2, C_1, T\}$ and sending it to the server with some modifications. But due to the below facts that:

1. It is extremely difficult to derive the server's secret key x from $A_i = h(ID_i \parallel x)$, because the one-way hash function is computationally difficult to invert.
2. No one can forge a valid parameter $C_1 = h(T \oplus B_i)$ or $C_2 = B_i^* \oplus h(A_i \parallel T)$, because these values are derived from B_i, B_i^* or A_i, which are unknown to everyone except legal user. By the way, the attacker can only generate them by acquiring the server's secret key x, which is infeasible.
3. On the other hand, since timestamp T in C_1 and C_2 is expired, the attacker must choose another valid timestamp, say T_a, and uses it in her/his login request. But she/he cannot generate $C_{1a} = h(T_a \oplus B_i)$ or $C_{2a} = B_i^* \oplus h(A_i \parallel T_a)$ with this new timestamp. The reason is the same as the above statement 2.

Table 1: Comparison of computational cost.

Phase	Lee et al.'s scheme	Our scheme
Reg.	$3T_H$	$3T_H$
Login	$3T_H + 2T_{XOR}$	$4T_H + 2T_{XOR}$
Auth.	$2T_H + 2T_{XOR}$	$3T_H + 2T_{XOR}$

Hence, any forged login request will be rejected in steps 2 and 3 of authentication phase, where server tries to compute $B_i^* = C_2 \oplus h(A_i \parallel T_a)$ and $C_1^* = h(T_a \oplus B_i^*)$ and compare C_1^* with received C_1.

5.2 Computation Cost Analysis

We here evaluate the computation cost of the improved scheme and make comparison with the Lee et al.'s scheme.

All phases of proposed protocol only require limited number of hash computations, exclusive-or operations, and some other low-cost operations such as string concatenations. The hash operations can be performed efficiently and computation cost of other operations is extremely low, so the efficiency of user and server are guaranteed in the proposed protocol.

You can compare the computational cost of three phases of our scheme with Lee et al.'s scheme in Table 1, where T_H means execution time of one-way hash function $h(.)$, and T_{XOR} means execution time of exclusive-or operation $\oplus$. You can see that in both login and authentication phases, our scheme adds just one more T_H to their scheme, so it does not incur much more computational cost to provide protection against forgery attack. In other words, an additional hash computation may be the simplest way to prevent from forgery attack, as our scheme does.

6 CONCLUSION

In this paper, we showed that Lee et al.'s authentication scheme, which was proposed to solve the forgery attack of the Wu and Chieu's scheme, is still vulnerable to the forgery attack. So Lee et al.'s authentication scheme is insecure.

Finally, we proposed an improved scheme with very low additional computational cost that not only can achieve all the advantages of Lee et al.'s scheme but also can withstand against the forgery attack.

REFERENCES

Lin, C-L. and Hwang, T. (2003). A password authentication scheme with secure password updating. *Computers and Security*, Vol. 22, Issue 1, pp. 68–72.

Lamport, L. (1981). Password authentication with insecure communication. *Communications of ACM*, Vol. 24, pp. 770–772.

Hwang, M-S. and Li, L-H. (2000). A new remote user authentication scheme using smart cards. *IEEE Transactions on Consumer Electronics*, Vol. 46, Issue 1, pp. 28–30.

Sun, H-M. (2000). An efficient remote use authentication scheme using smart cards. *IEEE Transactions on Consumer Electronics*, Vol. 46, Issue 4, pp. 958–961.

Wu, S-T. and Chieu, B-C. (2003). A user friendly remote authentication scheme with smart cards. *Computers and Security*, Vol. 22, Issue 6, pp. 547–550.

Fan, C-I. and Chan, Y-C. and Zhang, Z-K. (2005). Robust remote authentication scheme with smart cards. *Computers and Security*, Vol. 24, Issue 8, pp. 619–628.

Yang, C-C. and Wang, R-C. (2004). Cryptanalysis of a user friendly remote authentication scheme with smart cards. *Computers and Security*, Vol. 23, Issue 5, pp. 425–427.

Hwang, M-S. and Lo, J-W. and Liu, C-Y. and Lin, S-C. (2005). Cryptanalysis of a user friendly remote authentication scheme with smart card. *Journal of Applied Sciences*, Vol. 5, Issue 1, pp. 99–100.

Hwang, K-F. and Liao, I-E. (2005). Two attacks on a user friendly remote authentication scheme with smart cards. *ACM SIGOPS Operating Systems Review*, Vol. 39, Issue 2, pp. 94–96.

Lee, C-Y. and Lin, C-H. and Chang, C-C. (2005). An improved low computation cost user authentication scheme for mobile communication. *Proceedings of 19th International Conference on Advanced Information Networking and Applications (AINA'05), IEEE Computer Society*, Vol. 2, pp. 249–252.