Security Enhancements of a Mutual Authentication Scheme Using Smart Cards

Younghwa An and Youngdo Joo

Abstract Password-based authentication schemes have been widely adopted to protect resources from unauthorized access. In 2008, Liu et al. proposed a new mutual authentication scheme using smart cards which can withstand the forgery attack. In this paper, we analyze the security of Liu et al.'s scheme, and we show that Liu et al.'s scheme is still vulnerable to the various attacks. Also, we propose the enhanced scheme to overcome these security weaknesses and provide mutual authentication between the user and the server, even if the secret information stored in the smart card is revealed by an attacker. As a result of security analysis, the enhanced scheme is more secure than Liu et al.'s scheme.

Keywords Mutual authentication · Smart card · User impersonation attack · Password guessing attack

1 Introduction

With the rapid development of network technology, the user authentication scheme using smart card has been becoming one of important security issues. Due to the careless password management and the sophisticated attack techniques,

Y. An (✉) · Y. Joo
Computer and Media Information Engineering, Kangnam University,
111, Gugal-dong, Giheung-ku, Yongin-si, Gyeonggi-do 446-702, Korea
e-mail: yhan@kangnam.ac.kr

Y. Joo
e-mail: ydjoo@kangnam.ac.kr

Y.-H. Han et al. (eds.), *Ubiquitous Information Technologies and Applications*,
Lecture Notes in Electrical Engineering 214, DOI: 10.1007/978-94-007-5857-5_77,

the remote user authentication scheme has been exposed seriously to the menace of an attacker. Several enhanced authentication schemes using smart card have been proposed [1–10].

Yang et al. [1], in 1999, proposed a timestamp-based password authentication scheme using smart card which does not need to store the passwords or verification tables for user's authentication. In 2003, Shen et al. [2] pointed out that Yang et al.'s scheme does not resist the forgery attack, and proposed an improved scheme providing mutual authentication. But, in 2005, Yoon et al. [6] pointed out that the improved Shen et al.'s scheme was vulnerable to the forgery attack. In 2008, Liu et al. [10] also pointed out that Shen et al.'s scheme allowed an attacker to perform the forgery attack, and proposed a new nonce-based mutual authentication scheme which can withstand the forgery attack.

In this paper, we analyze the security of Liu et al.'s scheme and we show that Liu et al.'s scheme is still vulnerable to the forgery attack, the password guessing attack and the insider attack. To analyze the security of Liu et al.'s scheme, we assume that an attacker can extract the values stored in the smart card by monitoring the power consumption or analyzing the leaked information [11–13] and intercept messages communicating between the user and the server. Also, we propose the enhanced scheme to overcome these security weaknesses, even if the secret information stored in the smart card is revealed.

This paper is organized as follows. In Sect. 2, we briefly review Liu et al.'s scheme. In Sect. 3, we describe the attacks against Liu et al.'s scheme. The enhanced mutual authentication scheme is presented in Sect. 4, and its security analysis is given in Sect. 5. Finally, conclusions are made in Sect. 6.

2 Reviews of Liu et al.'s Scheme

Liu et al. proposed a nonce-based mutual authentication scheme using smart cards, in 2008. This scheme is composed of four phases: initialization, registration, login and authentication phase. The notations used in this paper are as shown in Table 1.

Table 1 Notation and definition

Notation	Description
KIC	Key information centre
U_i	User i
S	Remote server
PW_i	Password of the user i
ID_i	Identifier of the user i
CID_i	Identifier of the smart card for user i
h()	A one-way hash function
$x \oplus y$	Exclusive-OR of x and y

2.1 Initialization Phase

The KIC, which is responsible for generating parameters and providing a smart card to a new user, performs the following steps.

I1. The KIC generates two large primes p and q, and computes $n = p \cdot q$.
I2. The KIC chooses a prime e and an integer d such as $e \cdot d = 1 \bmod (p - 1)(q - 1)$, where e is the system's public key and d is the system's private key. The cryptographic parameters should be provided to the server through a secure channel.
I3. The KIC finds an integer g, which is a primitive element in both GF (p) and GF (q) and the public information in the system.

2.2 Registration Phase

A new user U_i submits his identifier ID_i and password PW_i to the KIC through a secure channel. Then, the KIC performs the following steps.

R1. The KIC computes the user's secret information $S_i = ID_i^d \bmod n$.
R2. The KIC computes $CID_i = h(ID_i \oplus d)$ and $h_i = g^{PWi \cdot d} \bmod n$.
R3. The KIC issues the smart card to the user through a secure channel, where the smart card contains the secret values such as n, e, g, ID_i, CID_i, S_i and h_i.

2.3 Login Phase

The user U_i inserts his smart card into a card reader and keys in his ID_i and PW_i when he wants to login to the remote server S. Then, the smart card performs the following steps.

L1. The smart card computes $SID_i = h(CID_i)$, and sends a message $M_1 = \{ID_i, SID_i\}$ to the remote server.
L2. Upon receiving the message M_1, the remote server computes $CID_i = h(ID_i \oplus d)$. If the computed value $h(CID_i)$ equals SID_i, the login request is accepted.
L3. The remote server generates a random session nonce N_s as a challenge to the user and computes $S_n = N_s \oplus CID_i$. Then the remote server sends it back to the smart card.
L4. Upon receiving S_n, the smart card gets the session nonce N_s by computing $(S_n \oplus CID_i)$ and generates a random number r_c as a challenge to the server.
L5. The smart card computes the message $M_2 = \{X_i, Y_i\}$ where $X_i = g^{rc \cdot PWi} \bmod n$ and $Y_i = S_i \cdot h_i^{rc \cdot Ns} \bmod n$, and then sends it to the remote server S.

2.4 Authentication Phase

After receiving the message M_2, the remote server S performs the following steps.

A1. The remote server checks whether $Y_i^e = ID_i \cdot X_i^{Ns} \bmod n$ or not. If it holds, the smart card is authenticated to the remote server.
A2. To perform mutual authentication, the remote server computes $M_3 = (h(CID_i, X_i))^d \bmod n$ and sends M_3 to the smart card.
A3. Upon receiving the message M_3, the smart card checks whether $M_3^e = h(CID_i, X_i) \bmod n$ or not. If it holds, the remote server is authenticated to the smart card.

3 Attacks Against Liu et al.'s Scheme

To analyze the security of Liu et al.'s scheme, we assume that an attacker can extract the secret values (CID_i, S_i, h_i) stored in the legal smart card by monitoring the power consumption or analyzing the leaked information [11–13].

3.1 User Impersonation Attack

With the extracted secret values, an attacker can perform the user impersonation attack in the following steps. The procedure of the user impersonation attack is illustrated in Fig. 1.

UA1. An attacker computes $SID_{ia} = h(CID_i)$ and sends the forged message $M_{1a} = \{ID_i, SID_{ia}\}$ to the remote server S.

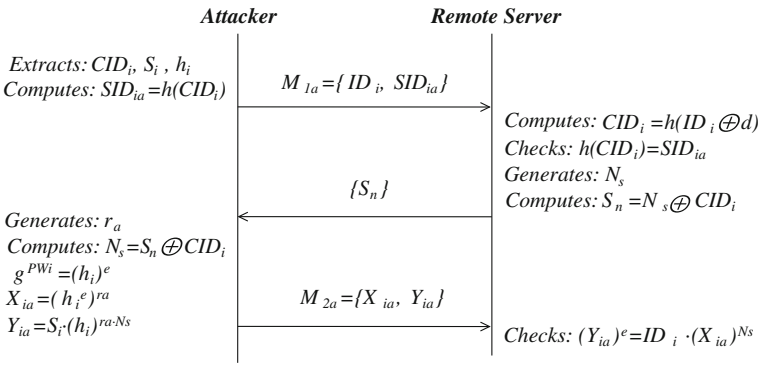

Fig. 1 User impersonation attack

UA2. Upon receiving the message M_{1a}, the remote server computes $CID_i = h(ID_i \oplus d)$. If the computed value $h(CID_i)$ equals SID_{ia}, the remote server accepts the login request. Then, the remote server computes $S_n = N_s \oplus CID_i$ and sends it back to the attacker, where N_s is a random session nonce.

UA3. Upon receiving S_n, the attacker computes the following forged login request message $M_{2a} = \{X_{ia}, Y_{ia}\}$ without the legal user's password and sends it to the remote server, where r_a is a random number generating by the attacker.

$$N_s = S_n \oplus CID_i$$
$$g^{PWi} = (h_i)^e \bmod n$$
$$X_{ia} = \left(h_i^e\right)^{ra} \bmod n$$
$$Y_{ia} = S_i \cdot h_i^{ra \cdot Ns} \bmod n$$

UA4. Upon receiving the message M_{2a}, the attacker is authenticated as the legal user by the remote server if the equation $(Y_{ia})^e = ID_i \cdot (X_{ia})^{Ns} \bmod n$ holds.

3.2 Password Guessing Attack

Generally, most of users tend to select a password that is easily remembered for his convenience. Hence, these passwords are potentially vulnerable to password guessing attack.

With the extracted secret values, an attacker can perform the password guessing attack in the following steps.

PA1. The attacker computes $(g^{PWi*} \bmod n) = (h_i)^e$ from the registration phase as the following equation, where PW_i^* is a guessed password.

PA2. The attacker verifies a correctness of user's password PW_i^*.

PA3. The attacker repeats the above steps by replacing a guessed password PW_i^* until the correct password PW_i is found.

3.3 Insider Attack

The user who wants to be authenticated from the remote server has to submit his password to the KIC in the registration phase. If the user's password PW_i is revealed to the server, the insider of the server may directly obtain the user's password PW_i. With the obtained password, the attacker as an insider can impersonate as the legal user to access the user's other accounts in other server if the user uses same password for the other accounts.

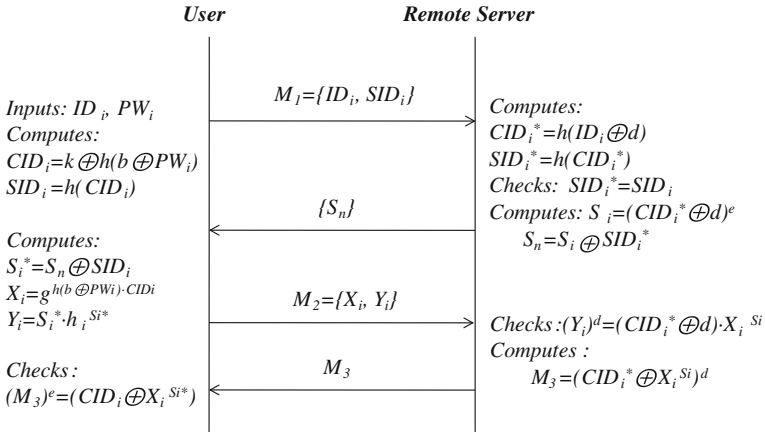

Fig. 2 Login and authentication phase

4 The Enhanced Mutual Authentication Scheme

In this section, we propose an enhanced authentication scheme which not only can provide mutual authentication between the user and the server, but also withstand the various attacks. The enhanced scheme is divided into four phases: initialization phase, registration phase, login phase and authentication phase. In this section, these remarks regarding the initialization phase are omitted as they are described in Sect. 2.1. The login and authentication phase are illustrated in Fig. 2.

4.1 Registration Phase

This phase works whenever the user U_i initially registers to the KIC. A user submits his identifier ID_i and password information $h(b \oplus PW_i)$ to the KIC through a secure channel, where a random number b is chosen by the user. The KIC performs the following steps.

R1. The KIC computes the smart card's identifier CID_i and the secret values k, h_i.

$$\begin{aligned} CID_i &= h(ID_i \oplus d) \\ k &= CID_i \oplus h(b \oplus PW_i) \\ h_i &= g^{h(b \oplus PWi) \cdot CIDi \cdot e} \bmod n \end{aligned}$$

R2. The KIC issues the smart card to the user through a secure channel, where the smart card contains the secret values such as n, e, g, k and h_i.

R3. The user U_i stores b into his new smart card so that the user does not need to remember b.

4.2 Login Phase

This phase works whenever the user U_i wants to login to the remote server S. The user U_i inserts his smart card into a card reader and inputs in his identifier ID_i and password PW_i. The smart card performs the following steps.

L1. The smart card computes $CID_i = k \oplus h(b \oplus PW_i)$ and $SID_i = h(CID_i)$. And the smart card sends a message $M_1 = \{ID_i, SID_i\}$ to the remote server.
L2. Upon receiving the message M_1, the remote server computes $CID_i^* = h(ID_i \oplus d)$ and $SID_i^* = h(CID_i^*)$. If the SID_i^* equals SID_i, the login request is accepted.
L3. The remote server computes $S_i = (CID_i^* \oplus d)^e \bmod n$ as a challenge to the user and $S_n = S_i \oplus SID_i^*$. Then the remote server sends $\{S_n\}$ back to the smart card.
L4. Upon receiving $\{S_n\}$, the smart card computes the message $M_2 = \{X_i, Y_i\}$ and sends it to the remote server.

$$S_i^* = S_n \oplus SID_i$$
$$X_i = g^{h(b \oplus PWi) \cdot CIDi} \bmod n$$
$$Y_i = S_i^* \cdot h_i^{Si*} \bmod n$$

4.3 Authentication Phase

This phase works whenever the remote server S received the user U_i's login request. After receiving the message M_2, the remote server performs the following steps.

A1. The remote server checks whether $(Y_i)^d = (CID_i^* \oplus d) \cdot X_i^{Si} \bmod n$ or not. If it holds, the smart card is authenticated to the remote server.
A2. To perform mutual authentication, the remote server computes $M_3 = (CID_i^* \oplus X_i^{Si})^d \bmod n$ and sends M_3 to the smart card.
A3. Upon receiving the message M_3, the smart card checks whether $(M_3)^e = (CID_i^* \oplus X_i^{Si*}) \bmod n$ or not. If it holds, the remote server is authenticated to the smart card.

5 Security Analysis of the Enhanced Mutual Authentication Scheme

In this section, we have the security analysis of the enhanced mutual authentication scheme based on the difficulty of factoring a large number and the discrete logarithm problem.

5.1 Security Analysis

To analyze the security of the enhanced scheme, we assume that an attacker can extract the values (k, h_i) stored in the smart card by monitoring the power consumption or analyzing the leaked information [11–13] and intercept the messages (M_1, M_2, S_n) communicating between the user and the remote server.

User impersonation attack: To impersonate as the legal user, an attacker attempts to make a forged login request message which can be authenticated to the server. However, the attacker cannot make the forged login request message even if the attacker can extract the secret values (k, h_i) stored in the user's smart card and intercept the messages (M_1, M_2, S_n) communicating between the user and the server, because the attacker cannot compute the forged messages (M_{1a}, M_{2a}) sending to the server without knowing the secret key d kept by the server.

Password Guessing Attack: With the extracted secret values (k, h_i) stored in the user's smart card illegally, the attacker attempts to guess the user's password PW_i computing $k = CID_i \oplus h(b \oplus PW_i)$ repeatedly in the registration phase. However, the attacker cannot guess the user's password PW_i, because the attacker does not know the secret key d kept by the server.

Insider Attack: If the user's password PW_i is revealed to the server in the registration phase, the insider of the server may directly obtain the user's password and try to access the user's accounts in other server using the same password. In the enhanced scheme, the attacker as an insider cannot obtain the user's password PW_i directly, because the user submits the user's password information $h(b \oplus PW_i)$ instead of the user's password PW_i to the server.

Mutual Authentication: To provide mutual authentication, the user and the server have to authenticate each other. In the enhanced scheme, the user can make the login request message (M_1, M_2) sending to the server and the reply message (M_3) sending to the user. But the attacker cannot make the forged login request message (M_{1a}, M_{2a}) and the forged reply message (M_{3a}) without knowing the secret key d kept by the server, even if the attacker can extract the secret values (k, h_i) stored in the user's smart card.

5.2 Security Comparison of the Enhanced Scheme and Liu et al.'s Scheme

In this section, the security analysis of Liu et al's scheme and the enhanced scheme are summarized in Table 2. As a result of comparison, the enhanced scheme is relatively more secure than Liu et al.'s scheme. In addition, the enhanced scheme provides secure mutual authentication between the user and the server.

Table 2 Comparison of the enhanced scheme and Liu et al's scheme

Security feature	Liu et al's scheme	The enhanced scheme
Impersonation attack	Possible	Impossible
Password guessing attack	Possible	Impossible
Insider attack	Possible	Impossible
Mutual authentication	Not provided	Provided

6 Conclusions

In this paper, we discussed the security of Liu et al.'s scheme. Although Liu et al.'s scheme improved more secure than Shen et al.'s scheme, we showed that Liu et al.'s scheme is still vulnerable to the user impersonation attack, the password guessing attack and the insider attack. Also, we proposed the enhanced scheme to overcome these security weaknesses and provide mutual authentication between the user and the server while preserving all their merits, even if the secret information stored in the smart card is revealed. As a result of security analysis, the enhanced scheme is relatively more secure than Liu et al.'s scheme in terms of the security.

References

1. Yang, W.H., Shieh, S.P.: Password authentication with smart cards. Comput. Secur. **18**(8), 727–733 (1999)
2. Shen, J.J., Lin, C.W., Hwang, M.S.: Security enhancement for the timestamp-based password authentication scheme using smart cards. Comput. Secur. **22**(7), 591–595 (2003)
3. Wu, S.T., Chieu, B.C.: A user friendly remote authentication scheme with smart cards. Comput. Secur. **22**(6), 457–550 (2003)
4. Das, M.L., Sxena, A., Gulathi, V.P.: A dynamic ID-based remote user authentication scheme. IEEE Trans. Consum. Electron. **50**(2), 629–631 (2004)
5. Chien, H.Y., Chen, C.H.: A remote password authentication preserving user anonymity. In: Proceedings of the 19th International Conference on Advanced Information Networking and Applications, (AINA '05) (2005)
6. Yoon, E.J., Ryu, E.K., Yoo, K.Y.: Attack on the Shen et al.'s timestamp-based password authentication scheme using smart cards. IEICE Trans. Fundam. **E88-A**(1), 319–321 (2005)
7. Lin, C.W., Tsai, C.S., Hwang, M.S.: A new strong-password authentication scheme using one-way hash functions. J. Comput. Syst. Sci. Int. **45**(4), 623–626 (2006)
8. Bindu, C.S., Reddy, P.C.S., Satyanarayana, B.: Improved remote user authentication scheme preserving user anonymity. Int. J. Comput. Sci. Netw. Secur. **8**(3), 62–66 (2008)
9. Chang, C.C., Lee, C.Y.: A friendly password mutual authentication scheme for remote login network systems. Int. J. Multimedia Ubiquit. Eng. **3**(1), 59–63 (2008)
10. Liu, J.Y., Zhou, A.M., Gao, M.X.: A new mutual authentication scheme based on nonce and smart cards. Comput. Commun. **31**, 2205–2209 (2008)
11. Kocher, P., Jaffe, J., Jun, B.: Differential power analysis. In: Proceedings of Advances in Cryptology, pp. 388–397 (1999)
12. Messerges, T.S., Dabbish, E.A., Sloan, R.H.: Examining smart-card security under the threat of power analysis attacks. IEEE Trans. Comput. **51**(5), 541–552 (2002)
13. Brier, E., Clavier, C., Oliver, F.: Correlation power analysis with a leakage model. Lect. Notes Comput. Sci. **3156**, 135–152 (2004)