Security Analysis and Improvements of a Password-Based Mutual Authentication Scheme with Session Key Agreement

Younghwa An and Youngdo Joo

Division of Computer and Media Information Engineering, Kangnam University
111, Gugal-dong, Giheung-gu, Yongin-si, Gyounggi-do, 446-702, Korea
{yhan, ydjoo}@kangnam.ac.kr

Abstract

Password-based authentication schemes have been widely adopted to protect resources from unauthorized access. In 2008, Chang-Lee proposed a friendly password-based mutual authentication scheme to avoid the security weaknesses of Wu-Chieu's scheme. In this paper, we demonstrate that Chang-Lee's scheme is vulnerable to user impersonation attack, server masquerading attack, password guessing attack, and insider attack. Also, we propose an improved scheme to overcome the security weaknesses of Chang-Lee's scheme, even if secret information stored in the smart card is revealed. As a result of security analysis, we prove that the proposed scheme is secure for the various attacks and provides session key agreement.

Keywords: *User Impersonation Attack, Server Masquerading Attack, Password Guessing Attack, Session Key Agreement*

1. Introduction

With the rapid development of network technology, user authentication scheme in e-commerce and m-commerce has been becoming one of important security issues. However, the security weaknesses in the remote user authentication scheme have been exposed seriously due to the careless password management and the sophisticated attack techniques. Several researches [1-10] have been proposed to improve security, reliability, and efficiency in the user authentication scheme.

In 2000, Sun [1] proposed an elaborate remote user authentication scheme using a smart card with the advantages of a no password table. But the scheme also has the disadvantage in that the password of the user is assigned by the remote server. Wu-Chieu [2], in 2003, proposed a user friendly remote user authentication scheme with smart cards to improve the drawback of Sun's scheme which required the assignment of un-human lengthy passwords. However, in 2004, Yang-Wang [4] pointed out that Wu-Chieu's scheme is vulnerable to password guessing attack and forgery attack. In 2008, Chang-Lee [7] proposed a friendly password-based mutual authentication scheme to avoid security weaknesses of Wu-Chieu's scheme. They claimed that their scheme was secure against the forgery attack, the password guessing attack, and the replay attack, as well as provided mutual authentication between the user and the remote server.

In this paper, we analyze the security of Chang-Lee's scheme and we show that Chang-Lee's scheme is still insecure against the various attacks. To analyze the Chang-Lee's scheme, we assume that an attacker can access a user's smart card and extract the secret information stored in the smart card by monitoring the power consumption [11-12] and intercept the

messages communicating between the user and the server. Also, we propose an improved scheme to overcome the security weaknesses of Chang-Lee's scheme, even if the secret information stored in the smart card is revealed. And, we assume that an attacker may possess the following capabilities to thwart the security schemes.

• An attacker has total control over the communication channel between the user and the server in the login and authentication phase. That is, the attacker may intercept, insert, delete, or modify any message across the communication procedures.

• An attacker may (i) either steal a user's smart card and then extract the secret values stored in the smart card, (ii) or steal a user's password, but cannot commit both of (i) and (ii) at a time.

If both of the user's smart card and password were stolen at the same time, then there is no way to prevent an attacker from impersonating as the legal user. Therefore, a remote user authentication scheme should be secure if only one case out of (i) and (ii) is happening.

This paper is organized as follows. In section 2, we review Chang-Lee's scheme. In section 3, we describe security weaknesses of Chang-Lee's scheme. The proposed scheme is presented in section 4, and its security analysis is given in section 5. Finally, brief conclusions are drawn in section 6.

2. Reviews of Chang-Lee's Scheme

In 2008, Chang-Lee [7] proposed a friendly password mutual authentication scheme for remote login network systems. The scheme is divided into three phases: registration phase, login phase, and authentication phase. The notations used throughout this paper are shown in Table 1.

Table 1. Notations and Descriptions

Notation	Description
U_i	User i
S	Remote server
PW_i	Password of the user i
ID_i	Identity of the user i
h()	A secure hash function
x	A secret information maintained by server
$x \| y$	Concatenation operation of x and y
$x \oplus y$	Exclusive-OR operation of x and y

2.1. Registration Phase

This phase works whenever a user U_i wants to register initially or re-register to the remote server S.

1) A user submits his identity ID_i and password PW_i to the server through a secure channel.

2) The server computes $A_i=h(ID_i \| x)$ and $B_i=h(A_i \| h(PW_i))$, where x is a secret key of server.

3) The server issues the smart card to the user through a secure channel, where the smart card contains $\{ID_i, A_i, B_i, h()\}$.

2.2. Login Phase

This phase works whenever the user U_i wants to login to the remote server S. The login and authentication phase are illustrated in Figure 1.

1) The user inserts his smart card into a card reader, and enters his identity ID_i and password PW_i^*.

2) The smart card computes $B_i^*=h(A_i \| h(PW_i^*))$, $C_1=h(B_i \oplus T_1)$ and $C_2= B_i^* \oplus h(A_i \oplus T_1)$, where T_1 is the current time stamp.

3) The user sends a message $m_1=\{ID_i, C_1, C_2, T_1\}$ to the server.

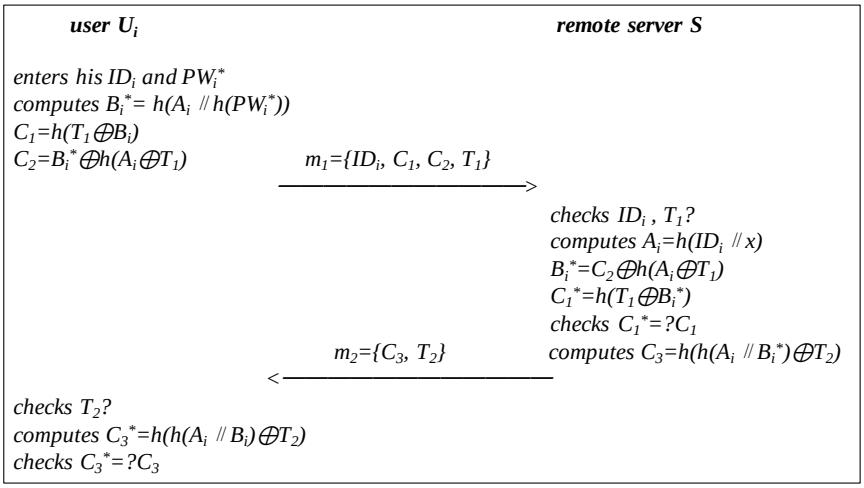


Figure 1. Login and Authentication Phase of the Chang-Lee's Scheme

2.3. Authentication Phase

This phase works whenever the remote server S receives the user's login request message.

1) The server checks the validity of the user's identity ID_i, and then verifies the validity of the time interval between T' and T_1, where T' is the time of receiving m_1 at the remote server.

2) The server computes $A_i=h(ID_i \| x)$, $B_i^*=C_2 \oplus h(A_i \oplus T_1)$ and $C_1^*=h(B_i^* \oplus T_1)$.

3) The server checks whether $C_1^*=C_1$ or not. If they are equal, the user's login request is accepted.

4) The server sends a message $m_2=\{C_3, T_2\}$, where $C_3=h(h(A_i \| B_i^*) \oplus T_2)$ and T_2 is the current time stamp.

5) Upon receiving the message, the smart card verifies the validity of the time interval between T" and T_2, where T" is the time of receiving m_2 at the user.

6) The smart card computes $C_3^*=h(h(A_i \| B_i) \oplus T_2)$, and then checks whether $C_3^*= C_3$ or not. If they are equal, the server is authenticated to the user.

3. Security Weaknesses of Chang-Lee's Scheme

In this section, we analyze the security of Chang-Lee's scheme. To analyze the security weaknesses, we assume that an attacker can access a user's smart card and extract the secret information stored in the smart card by monitoring the power consumption [11-12] and intercept the messages communicating between the user and the server.

3.1. User Impersonation Attack

As described above, the attacker can extract the secret values (A_i, B_i) from the user's smart card illegally by some means and intercept the message $m_1=\{ID_i, C_1, C_2, T_1\}$ communicating between the user and the server. The procedure for user impersonation attack occurs in the following steps. The user impersonation attack is illustrated in Figure 2.

1) In the login phase, the attacker computes easily $C_{1a}=h(B_i \oplus T_{1a})$ and $C_{2a}=B_i \oplus h(A_i \oplus T_{1a})$ by extracting the secret values (A_i, B_i), where T_{1a} is the current timestamp.

2) Then, the attacker sends the forged message $m_{1a}=\{ID_i, C_{1a}, C_{2a}, T_{1a}\}$ to the remote server.

3) Upon receiving the message, the remote server checks the validity of ID_i and verifies the validity of the time interval. If it holds, the remote server will be convinced the message m_{1a} sent from the user by verifying whether $C_1^*=C_{1a}$ or not. And then the remote server makes the reply massage $m_2=\{C_3, T_2\}$ by computing $C_3=h(h(A_i \| B_i^*) \oplus T_2)$ in the authentication phase.

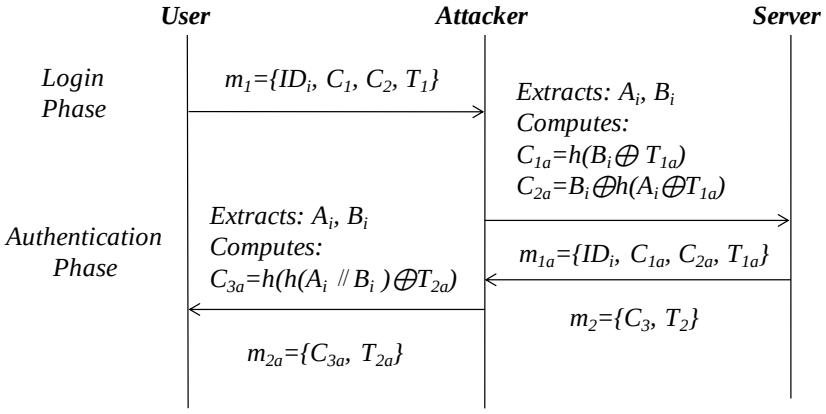


Figure 2. User Impersonation Attack and Server Masquerading Attack

3.2. Server Masquerading Attack

In the same manner, the attacker can extract the secret values (A_i, B_i) from the user's smart card illegally by some means and intercepts the message $m_2=\{C_3, T_2\}$ communicating between the user and the server. The procedure for server masquerading attack occurs in the following steps. The server masquerading attack is illustrated in Figure 2.

1) In the authentication phase, the attacker computes easily $C_{3a}=h(h(A_i \| B_i) \oplus T_{2a})$ extracting the secret values (A_i, B_i), where T_{2a} is the current timestamp.

2) Then, the attacker sends the forged message $m_{2a}=\{C_{3a}, T_{2a}\}$ to the user.

3) Upon receiving the message, the user verifies the validity of the time interval. If it holds, the user will be convinced the message m_{2a} sent from the remote server by verifying whether $C_3^*=C_{3a}$ or not.

3.3. Password Guessing Attack

As mentioned earlier, the attacker can extract the secret values (A_i, B_i) from the user's smart card illegally by some means. Now, the attacker can easily find out the user's password PW_i by employing the password guessing attack, in which each guess of PW_i^* for PW_i can be verified by the following steps.

1) The attacker computes the parameter $B_i^*=h(A_i \| h(PW_i^*))$ from the registration phase.

2) The attacker verifies the correctness of PW_i^* by checking $B_i^*= B_i$.

3) The attacker repeats the above steps until a correct password PW_i^* is found. Finally, the attacker can derive the correct user's password PW_i.

Thus, the attacker can perform the password guessing attack, and can successfully impersonate the legal user with the guessed user password.

3.4. Insider Attack

In the registration phase, if the user's password PW_i is revealed to the server, the insider of the server may directly obtain PW_i. Thus the insider as an attacker can impersonate as the legal user to access the user's other accounts in other server if the user uses the same password for the other accounts. Therefore, Chang-Lee's scheme is not secure for the insider attack.

3.5. Mutual Authentication

As you notice in the attacks such as the user impersonation attack and the server masquerading attack, Chang-Lee's scheme fails to provide the mutual authentication between the user and the remote server. Namely, if the attacker can extract the secret values (A_i, B_i) from the legal user's smart card illegally by some means and intercept the messages communicating between the user and the server, the attacker can impersonate the legal user easily by computing the equations $C_{1a}=h(B_i \oplus T_{1a})$ and $C_{2a}=B_i \oplus h(A_i \oplus T_{1a})$. Also, the attacker can masquerade the legal remote server easily by computing the equation $C_{3a}=h(h(A_i \| B_i) \oplus T_{2a})$.

4. The Proposed Scheme

In this section, we propose an improvement on Chang-Lee's scheme with mutual authentication and session key agreement. The proposed scheme is divided into three phases: registration phase, login phase and authentication phase. The login and authentication phase are illustrated in Figure 3.

4.1. Registration Phase

Before performing the registration phase, the remote server S has to generate a large prime p and finds an integer g which is a primitive element in GF(p). Then, a user U_i registers to S in the following steps.

1) A user submits his identity ID_i and $h(b \oplus PW_i)$ to the server through a secure channel, where a random number b is generated by U_i.

2) The server computes $A_i=h(ID_i \oplus x)$ and $B_i=A_i \oplus h(b \oplus PW_i))$, where x is a secret key of server.

3) The server issues the smart card to the user through a secure channel, where the smart card contains $\{ID_i, B_i, h()\}$.

4) The user 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.

1) The user inserts his smart card into a card reader, and enters his identity ID_i and password PW_i.

2) The smart card generates a random number r_c and computes $R_c=g^{rc} \bmod p$.

3) The smart card computes the following equations.

$$A_i=B_i \oplus h(b \oplus PW_i)$$
$$C_1=h(A_i \oplus R_c)$$
$$C_2= R_c \oplus h(A_i \oplus T_1)$$

4) The user sends a message $\{ID_i, C_1, C_2, T_1\}$ to the server, where T_1 is the current timestamp.

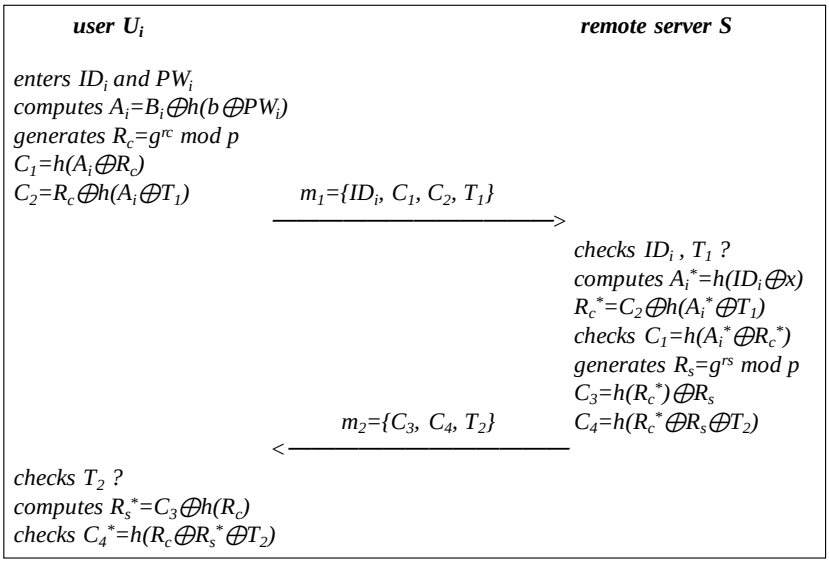


Figure 3. Login and Authentication Phase of the Proposed Scheme

4.3. Authentication Phase

This phase works whenever the remote server S receives the user's login request. Upon receiving the message from the user, the server performs the following steps.

1) The server checks the validity of ID_i, and then verifies the time stamp T_1 with the current time T'. If $(T'-T_1) \leq \Delta T$, the server accepts the login request, where ΔT denotes the expected valid time interval for transmission delay.

2) The server computes the following equations.

$$A_i^* = h(ID_i \oplus x)$$

$$R_c^* = C_2 \oplus h(A_i^* \oplus T_1)$$

$$C_1^* = h(A_i^* \oplus R_c^*)$$

3) The server checks whether $C_1^* = C_1$ or not. If they are equal, the user's login request is accepted.

4) The server generates a random number r_s and computes $R_s = g^{rs} \bmod p$.

5) The server computes $C_3 = h(R_c^*) \oplus R_s$ and $C_4 = h(R_c^* \oplus R_s \oplus T_2)$, where T_2 is the current timestamp, and then sends a message $\{C_3, C_4, T_2\}$ to the user.

6) Upon receiving the message, the smart card verifies the time stamp T_2 with the current time T". If $(T"-T_2) \leq \Delta T$, and then the smart card computes $R_s^* = C_3 \oplus h(R_c)$ and $C_3^* = h(R_c \oplus R_s^* \oplus T_2)$.

7) The smart card checks whether $C_3^* = C_3$ or not. If they are equal, the server is authenticated to the user and allowed to access the smart card.

8) After achieving mutual authentication, the server and the user can generate the session key, $SK = (R_s')^{rc} = (R_c')^{rs} = g^{rs \cdot rc} \bmod p$ each other for secrecy communication.

5. Security Analysis of the Proposed Scheme

In this section, we analyze the security of the proposed scheme based on secure one-way hash function. To analyze the security of the proposed scheme, we assume that an attacker can access a user's smart card and extract the values stored in the smart card by some means [11-12], and eventually intercept the messages communicating between the user and the server.

5.1. User Impersonation Attack

To impersonate the legal user, an attacker attempts to make a forged login request message which can be authenticated to the server. However, the attacker cannot impersonate the user by forging the login request massage, because the attacker cannot compute the forged message C_{1a} and C_{2a} without knowing the remote server's secret value x and the random number r_c chosen by the user. Hence, the attacker has no chance to login by launching a user impersonation attack

5.2. Server Masquerading Attack

To masquerade as the legal server, an attacker attempts to make the forged reply massage which can be masqueraded to the user when receiving the user's login request message. However, the attacker cannot masquerade as the server by forging the reply massage, because the attacker does not compute C_{3a} and C_{4a} without knowing the remote server's secret value x and the random number r_s chosen by the server. Hence, the attacker cannot masquerade as the legal server to the user by launching a server masquerading attack.

5.3. Password Guessing Attack

The attacker can extract the secret values (B_i) from the legal user's smart card by some means. Then the attacker attempts to derive the user's password PW_i using $B_i=h(A_i \oplus h(PW_i))$ in the registration phase. However, the attacker cannot guess the user's password PW_i using the secret values extracted from the legal user's smart card, because the attacker does not know the remote server's secret value x. Therefore, the proposed scheme is secure for the password guessing attack.

5.4. Insider Attack

In the registration phase, if the user's password PW_i is revealed to the server, the insider of the server may directly obtain PW_i and impersonate as the user to access user's other accounts in other server if the user use the same password for the other accounts. Therefore, the proposed scheme is secure for the insider attack, because this scheme asks the user to submit $h(b \oplus PW_i)$ instead of a PW_i to the server.

5.5. Mutual Authentication

As previously described in the cases such as the user impersonation attack and the server masquerading attack, the proposed scheme provides mutual authentication between the user and the remote server. Namely, even if the attacker can extract the secret information in the user's smart card, the legal user can be authenticated to the server and the legal server can be authenticated to the user. Because the attacker cannot attempt to make the forged messages each phase without knowing the remote server's secret value x and the random number r_c and r_s chosen by the user and the server each other.

5.6. Session Key Agreement

With the extracted secret values in the legal user's smart card and the intercepted messages communicating between the user and the server, the attacker may attempt to compute the one-time session key SK. However, the attacker cannot generate the one-time session key, $SK(=g^{r_s \cdot r_c} \bmod p)$ without knowing the random number R_s and the R_c generated by the server and the user, respectively.

The security features of the related schemes and the proposed scheme resulted from the above analysis, are summarized in Table 2. The proposed scheme is relatively more secure than Chang-Lee's scheme.

Table 2. Comparison of the Related Schemes and the Proposed Scheme

security feature	Sun's scheme [1]	Wu-Chieu's scheme [2]	Chang-Lee's scheme [7]	The proposed scheme
user impersonation attack	possible	possible	possible	impossible
server masquerading attack	not provided*	not provided*	possible	impossible
password guessing attack	possible	possible	possible	impossible
insider attack	possible	possible	possible	impossible
session key agreement	not provided	not provided	not provided	provided

6. Conclusions

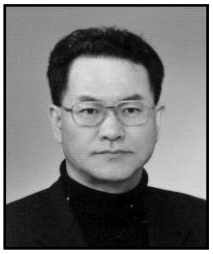
In this paper, we analyzed the security weaknesses of Chang-Lee's scheme. We showed that Chang-Lee's scheme is still insecure against the various attacks. Also, we proposed the improved scheme to overcome the security weaknesses of Chang-Lee's scheme, while preserving all their merits, even if the secret information stored in the smart card is revealed. As a result of security analysis, we proved that the proposed scheme is secure against the user impersonation attack, the server masquerading attack, the password guessing attack, and the insider attack, and provides the session key agreement.

References

[1] H. M. Sun, "An Efficient Remote User Authentication Scheme Using Smart Cards", IEEE Transactions on Consumer Electronics, vol. 46, no. 4, **(2000)**, pp. 958-961.
[2] S. T. Wu, B. C. Chieu, "A User Friendly Remote Authentication Scheme with Smart Cards", Computers & Security, vol. 22, no. 6, **(2003)**, pp. 457-550.
[3] M. L. Das, A. Sxena and V. P. Gulathi, "A Dynamic ID-based Remote User Authentication Scheme", IEEE Transactions on Consumer Electronics, vol. 50, no. 2, **(2004)**, pp. 629-631.
[4] C. C. Yang and R. C. Wang, "Cryptanalysis of a User Friendly Remote Authentication Scheme with Smart Cards", Computers & Security, vol. 223, no. 5, **(2004)**, pp. 425-427.
[5] C. L. Lin and C. P. Hung, "Cryptanalysis and Improvement on Lee-Chen's One-Time Password Authentication Scheme", International Journal of Security and its Applications, vol. 2, no. 2, **(2008)**, pp. 1-8.
[6] J. Xu, W. T. Zhu and D. G. Feng, "Improvement of a Finger-Based User Authentication", International Journal of Security and its Applications, vol. 2, no. 3, **(2008)**, pp. 73-80.
[7] C. C. Chang and C. Y. Lee, "A Friendly Password Mutual Authentication Scheme for Remote Login Network Systems", International Journal of Multimedia and Ubiquitous Engineering, vol. 3, no. 1, **(2008)**, pp. 59-63.
[8] C. T. Li and M. S. Hwang, "An Efficient Biometrics-based Remote User Authentication Scheme Using Smart Cards", Journal of Network and Computer Applications, vol. 33, **(2010)**, pp. 1-5.
[9] C. C. Chang, S. C. Chang and Y. W. Lai, "An Improved Biometrics-based User Authentication Scheme without Concurrency System", International Journal of Intelligent Information Processing, vol. 1, no. 1, **(2010)**, pp. 41-49.
[10] C. C. Lee, Y. M. Lai and C. T. Li, "An improved Secure Dynamic ID Based Remote User Authentication Scheme for Multi-server Environment", International Journal of Security and its Applications, vol. 6, no. 2, **(2012)**, pp. 203-209.

[11] P. Kocher, J. Jaffe and B. Jun, "Differential Power Analysis. Proceedings of Advances in Cryptology", **(1999)**, pp. 388-397.
[12] T. S. Messerges, E. A. Dabbish and R.H. Sloan, "Examining Smart-Card Security under the Threat of Power Analysis Attacks", IEEE Transactions on Computers, vol. 51, no. 5, **(2002)**, pp. 541-552.

Authors



Younghwa An

He received his B.S. and M.S. degrees in electronic engineering from Sungkyunkwan University, Korea in 1975 and 1977, respectively. He obtained his Ph.D. in information security from same university, 1990. From 1983 to 1990, he served as an assistant professor with the department of electronic engineering at Republic of Korea Naval Academy. Since 1991, he has been a professor with department of computer and media information engineering at Kangnam University. During his tenure at Kangnam University, he served as the director of computer & information center and the director of central library. He performed research as a visiting professor at Florida State University from 2002 to 2003. His major research interests include information security and network security.

Youngdo Joo

He gained his M.S. degree in computer engineering form University of South Florida in 1988 and his Ph.D. in computer science from Florida State University in 1995. He is currently an associate professor in department of computer and media information engineering at Kangnam University. During 1995~2000, he worked as senior researcher for KT Network Research Lab. He led the research and technology business in ISP at Cisco Systems and Huawei Technology during 2000~2006. His research interests include future network, network security and network management.