Smart-card-loss-attack and Improvement of Hsiang et al.'s Authentication Scheme

Y. C. Lee

Department of Security Technology and Management
WuFeng University, Chiayi, 62153, Taiwan
yclee@wfu.edu.tw

ABSTRACT
Due to the open environment, all network systems suffer from various security threats. The remote user authentication scheme is a secure mechanism to allow users obtaining a variety of information services through insecure channels. For efficiency and security, many remote user authentication schemes identify users with smart cards. However, many smart card based schemes are vulnerable to lots of attacks. Recently, Hsiang *et al.* proposed a smart card based remote authentication scheme. In this article, we show that their scheme is vulnerable to the smart-card-loss-attack. That is, if an unauthorized person obtains the smart card, he/she can guess the correct password to masquerade as a legitimate user to login the system. The attack is caused by the smart card outputs fixed message for the same inputs. We propose an improved scheme to fix the flaw. The improved scheme withstands the off-line password guessing attack, parallel session attack and smart-card-loss-attack. Moreover, it also has the merits of providing mutual authentication, no verification table and users can freely update their passwords.

Keywords: Smart-card-loss-attack, off-line guessing attack, authentication scheme.

1. Introduction

Nowadays, people obtain a variety of information or services through networks. However, due to the open nature, all network systems always suffer various security threats. The remote user authentication scheme is a secure mechanism to allow users obtaining services through insecure channels [1-4], and it is the most common method used to check the validity of the login message and to authenticate the servers or users. A lot of authentication schemes also provide mutual authentication, key agreement and freely updating password.

A remote user authentication scheme includes two main entities: servers and remote users. The communications between the servers and users are through insecure open channels. Thus, the security vulnerabilities of the remote user authentication scheme may occur due to the remote users, servers and insecure channels [5]. Many remote user authentication schemes identify users by using smart cards. However, many smart card based schemes are vulnerable to various attacks. Moreover, lots of schemes suffer the smart-card-loss-attack. The smart-card-loss-attack means an adversary can launch various attacks such as off-line guessing attack when he/she obtains a legitimate user's smart card.

In 1981, Lamport [6] proposed the first well-known remote password authentication scheme by using smart cards. However, Lamport's scheme has the drawbacks such as high hash overhead and requiring a password table at the server end. Until now, there are many smart card based password authentication schemes have been proposed [1, 5, 7-9] to improve security, efficiency or to reduce costs. However, most schemes still cannot solve all possible problems and withstand all kinds of attacks [10-12].

Hwang *et al.* [7] proposed a smart card based remote password user authentication scheme to overcome the weakness in security. However, their scheme does not allow users to freely update passwords and it cannot withstand the masquerade attack either. In 2002, Chien *et al.* [13] developed a remote user password authentication scheme to provide mutual authentication and freely updating password. But Ku *et al.* [14] showed that Chien *et al.*'s scheme is vulnerable to the reflection attack and the insider attack. Ku *et al.* also proposed an improved scheme to fix the flaws. However, Yoon *et al.* [15] indicated that the improved scheme was also susceptible to the parallel session attack, and then presented an improved scheme to enhance the security.

In 2009, Hsiang *et al.* [16] showed that Yoon *et al.*'s scheme is vulnerable to the parallel session attack, masquerading attack and password guessing attack. They also proposed an improved scheme to remedy the drawbacks. In this paper, we will show that Hsiang *et al.*'s scheme is vulnerable to the smart-card-loss-attack. If the smart card is lost, an unauthorized person can correctly guess the password and masquerade as the legitimate user to login the system. We also propose an improved scheme to fix the flaw. The improved scheme has the merits of mutual authentication, no verification table, and users can freely update their passwords. Moreover, the improved scheme withstands the off-line password guessing attack, parallel session attack and smart-card-loss-attack.

The remainder of this article is organized as follows. The notations used throughout this paper are listed in the next Section. In Section 3, we briefly describe Hsiang *et al.*'s remote user authentication scheme. Next, we show the smart-card-loss-attack on their scheme in Section 4. The improvement scheme and its security analysis are presented in Sections 5. Finally, we make brief conclusions in Section 6.

2. Preliminaries and notations

Generally, a smart card based remote user authentication scheme comprises the following four phases: registration phase, login phase, authentication phase and password changing phase. In the registration phase, the user sends a registration request along with related information to the server via a secure channel. The server identifies the user and generates related messages to store in the smart card, and then delivers the card to the user. In the login phase, the user attaches his/her smart card into a card reader and keys in password to login the system. In the authentication phase, the server checks the validity of the login request. If the user is authenticated, the server allows the user to access the system. In the password changing phase, the remote users freely update their passwords. Some schemes allow the server and users to obtain mutual authentication and establish a common session key.

All the notations used throughout this paper are listed as follows:

(1) U: A remote user.

(2) ID_U: The identity of the remote user U.

(3) PW_U: The password corresponding to the user U.

(4) S: The server of the system.

(5) x: The secret key of the server S.

(6) $h(\ )$: A cryptographic secure one-way-hash function.

(7) $\oplus$: The bitwise exclusive-OR (XOR) operation.

(8) b, r: Random numbers.

(9) $\|$: The concatenation operation.

(10) $A \Rightarrow B : \{M\}$: The entity A sends a message M to B through a secure channel.

(11) $A \rightarrow B : \{M\}$: The entity A sends a message M to B through an open insecure channel.

(12) T_A: A timestamp of the entity A.

3. Hsiang *et al.*'s remote user authentication scheme

In 2009, Hsiang *et al.* [16] pointed that Yoon *et al.*'s scheme [15] is vulnerable to the parallel session attack, masquerading attack, and password guessing attack. They proposed an improved scheme to fix the drawbacks. Hsiang *et al.*'s scheme comprises registration phase, login phase, authentication phase and password updating phase as follows.

3.1 Registration phase

In the registration phase, the user U registers with the server S by the following steps.

Step R-1. Firstly, U chooses an identity ID_U and password PW_U. Then he/she computes $h(PW_U)$ and $h(b \oplus PW_U)$ after generating a random number b. Next, U sends $\{ID_U, h(PW_U), h(b \oplus PW_U)\}$ to S via a secure channel.

Step R-2. Upon receiving ID_U, $h(PW_U)$, and $h(b \oplus PW_U)$, S creates an entry for U in the account database and stores $n = 0$ in the entry for the first registration. Otherwise, S sets $n = n + 1$ in the existing entry for U. Next, S computes EID_U, P, R and V as follows.

$$EID_U = h(ID_U \| n) \quad (1)$$

$$P = h(EID_U \oplus x) \quad (2)$$

$$R = P \oplus h(b \oplus PW_U) \quad (3)$$

$$V = h(P \oplus h(PW_U)) \quad (4)$$

At last, S stores V, R, and hash function $h(\ )$ into the smart card and sends it to U.

Step R-3. Upon receiving the smart card, U keys in the random number b into the card.

3.2 Login phase

If the user U wants to log into the system, the steps of the login phase are as follows.

Step L-1. The user U inserts his/her smart card into a card reader and keys in ID_U and PW_U.

Step L-2. The smart card computes C_1 and C_2 as follows, where T_U is the user's current timestamp.

$$C_1 = R \oplus h(b \oplus PW_U) \quad (5)$$

$$C_2 = h(C_1 \oplus T_U) \quad (6)$$

Step L-3. $U \rightarrow S$: $\{ID_U, T_U, C_2\}$. The user sends $\{ID_U, T_U, C_2\}$ to the server. Note that $C_2 = h(h(EID_U \oplus x) \oplus T_U)$.

3.3 Authentication phase

Upon receiving $\{ID_U, T_U, C_2\}$, the server S verifies the login message to authenticate the user by the following steps.

Step A-1. The server S checks ID_U and T_U. If ID_U is correct and T_U is in a valid time interval, S computes $C_2' = h(h(EID_U \oplus x) \oplus T_U)$; otherwise, S will reject the user's login request. If the computed result C_2' equals to the received message C_2, S accepts the login request and then computes C_3 as follows.

$$C_3 = h(h(EID_U \oplus x) \oplus h(T_S)) \quad (7)$$

Where T_S is the server's current timestamp.

Step A-2. $S \rightarrow U$: $\{T_S, C_3\}$. The server sends $\{T_S, C_3\}$ to the user.

Step A-3. Upon receiving the message $\{T_S, C_3\}$, U checks the timestamp T_S. If T_S is in a valid time interval, U computes $C_3' = h(C_1 \oplus h(T_S))$ and compares C_3' with the received C_3. The user U will authenticate the server S only if $C_3' = C_3$ holds.

3.4 Password changing phase

If the user U wants to change his/her password, the steps of password changing phase are as follows.

Step C-1. U inserts his smart card into the card reader and keys in his/her ID_U and PW_U.

Step C-2. The smart card computes $P' = R \oplus h(b \oplus PW_U)$ and $V' = h(P' \oplus h(PW_U))$.

Step C-3. The smart card compares V' with the stored V. If they are not equal, the smart card rejects the request. Otherwise, U chooses a new password PW_{U_new} and proceeds to the next step.

Step C-4. With the password PW_{U_new}, the smart card computes $R' = P' \oplus h(b \oplus PW_{U\_new})$ and $V' = h(P' \oplus h(PW_{U\_new}))$. Next, the smart card replaces R and V with R' and V', respectively.

4. Smart-card-loss-attack on Hsiang *et al.*'s remote user authentication scheme

Though Hsiang *et al.* declared that their scheme withstands the guessing attack, but recently He *et al.*, by using differential power analysis (DPA), has shown that Hsiang *et al.*'s scheme is vulnerable to the guessing attack and the masquerading attack [17]. The DPA attack is a method based on an analysis of the correlation between the electricity usage of a chip in a smart card and the encryption key it contains [18].

In this section, we will show the smart-card-loss-attack on Hsiang *et al.*'s scheme. The smart-card-loss-attack is more practical and more easily to be realized than DPA attack. We start to describe the attack by the following theorem.

Theorem 1. For Hsiang *et al.*'s remote user authentication scheme, the smart card will output fixed C_2 if the same timestamp T_U and correct password PW_U are keyed into the card.

Proof. Suppose that an adversary E wants to launch the smart-card-loss-attack on a user's smart card. E monitors the communications between the server and user. Suppose that the adversary intercepts message C_2 on a login session, where $C_2 = h(C_1 \oplus T_U) = (h(EID \oplus x) \oplus T_U)$. Next, the adversary obtains the smart card and starts a new session of login. E keys in the guessing password PW_U', and the smart card computes $C_1' = R \oplus h(b \oplus PW_U')$, where R and b are the secret information stored in the card and $R = h(EID \oplus x) \oplus h(b \oplus PW_U)$. Note that PW_U is the correct password used in the last login session. Hence the smart card will output C_2', where

$$\begin{aligned} C_2' &= h(C_1' \oplus T_U) \\ &= h(R \oplus h(b \oplus PW_U') \oplus T_U) \\ &= h((h(EID \oplus x) \oplus h(b \oplus PW_U)) \oplus h(b \oplus PW_U') \oplus T_U). \end{aligned}$$

If $PW_U' = PW_U$, then

$$\begin{aligned} C_2' &= h(h(EID \oplus x) \oplus T_U) \\ &= C_2 \end{aligned}$$

That is, the smart card will output a fixed C_2 if the adversary keys in the correct password and the same timestamp. The adversary can verify his/her guess of password by checking whether $C_2' = C_2$ holds. Q.E.D.

The attack is based on the assumption that the adversary obtains the legitimate user's smart card. The assumption is reasonable in the real world, especially for some VIPs, any adversary always wants to get the cards to obtain benefits or to hurt someone though it is illegal.

If the adversary E wants to adopt the smart-card-loss-attack on Hsiang *et al.*'s scheme, the steps of the attack are described in details as follows.

Step D-1. Firstly, E intercepts $\{ID, T_U, C_2\}$ on a login session.

Step D-2. E steals the smart card or gets the card by any means.

Step D-3. E inserts the card into a card reader and keys in T_U. Next, she inputs the guessed password PW_U'.

Step D-4. The smart card computes and outputs C_2'.

Step D-5. E checks whether $C_2' = C_2$ holds. The guessed password is correct if $C_2' = C_2$; otherwise, E repeats the Step D-3 to D-5 until the exact password is found.

Usually, for ease of memory, the bit-length of the password is quite short. Thus it is very quickly to correctly guess the password. For illustration, the smart-card-loss-attack is shown in Figure 1.

5. The improved scheme

The smart-card-loss-attack on Hsiang *et al.*'s scheme is caused by the smart card outputs fixed C_2 when the user inputs the same timestamp and password. If the output C_2 is varied on each login session for the same inputs, the attack will be avoided. The improved scheme is described as follows. Note that the registration phase and the password changing phase of the improved scheme are the same as Hsiang *et al.*'s scheme.

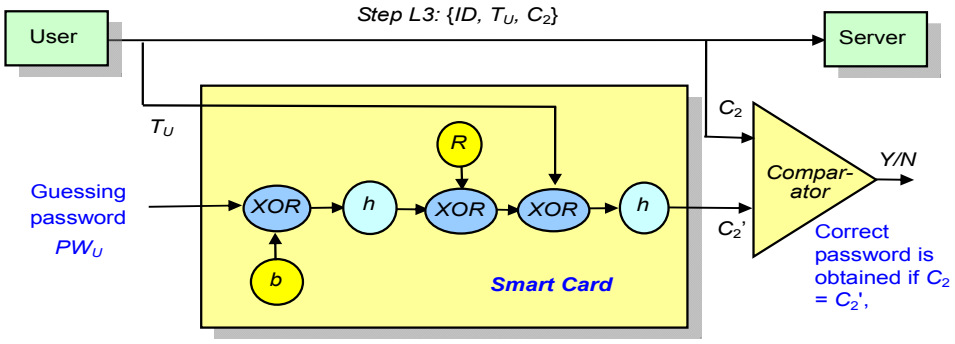

Figure 1. The Smart-card-loss-attack on Hsiang *et al.*'s scheme.

5.1 Login phase

The steps of the login phase are modified as follows.

Step L-1*. The user U inserts his/her smart card into a card reader and keys in ID_U and PW_U.

Step L-2*. The smart card computes C_1, C_2 and C_3 as follows, where T_U is the user's current timestamp and r is a random number.

$$C_1 = R \oplus h(b \oplus PW_U) \quad (8)$$

$$C_2 = h(C_1 \oplus r \oplus T_U) \quad (9)$$

$$C_3 = h(C_1) \oplus r \quad (10)$$

Step L-3*. $U \rightarrow S$: $\{ID_U, T_U, C_2, C_3\}$. The user sends the login information $\{ID_U, T_U, C_2, C_3\}$ to the server.

5.2 Authentication phase

The steps of the authentication phase are as follows.

Step A-1*. After receiving $\{ID_U, T_U, C_2, C_3\}$, the server checks ID_U and T_U. If ID_U is incorrect or T_U is not in a valid time interval, the server terminates the login steps. Otherwise, the server computes C_1, r' and C_2' by

$$C_1 = h(EID \oplus x) \quad (11)$$

$$r' = C_3 \oplus h(C_1) \quad (12)$$

$$C_2' = h(C_1 \oplus r' \oplus T_U) \quad (13)$$

Then the server compares C_2' with the received C_2. If $C_2' = C_2$, the server accepts the user's login request and computes C_4 by

$$C_4 = h(C_1 \oplus r \oplus h(T_S)) \quad (14)$$

Where T_S is the server's current timestamp.

Step A-2*. $S \rightarrow U$: $\{T_S, C_4\}$. The server forwards $\{T_S, C_4\}$ to the user.

Step A-3*. Upon receiving the message $\{T_S, C_4\}$, U checks the timestamp T_S. If T_S is in a valid time interval, U computes $C_4' = h(C_1 \oplus r \oplus h(T_S))$ and thereby compares C_4' with the received C_4. The user and the server obtain mutual authentication if $C_4' = C_4$.

5.3 Discussions and security analysis

The improved scheme has the merits of providing mutual authentication, no verification table, and freely updating password. Due to only exclusive-OR and hash function operations are adopted in the smart card, the computation cost of the proposed scheme is quite low. The pseudo random number generator is built in the computer of the user end. Thus the proposed scheme is easy and practical for implementation. A simple comparison on security among our scheme and other smart card based authentication schemes are listed in Table 1. Note

that we assume that the DPA method is not adopted on all attacks, the secret information $\{V, R, b\}$ in the smart card is unknown by any adversary or any malicious insiders.

Schemes	Guessing attack	Insider attack	Reflection attack	Smart-card-loss-attack
Ku *et al.*'s [14]	✓	✓	✓	✓
Chien *et al.*'s [13]	×	✓	✓	✓
Yoon *et al.*'s [15]	×	×	✓	✓
Hsiang *et al.*'s [16]	×	×	✓	✓
Ours scheme	×	×	×	×

Table1. Comparison of the smart card based authentication schemes.

The scheme withstands the smart-card-loss-attack, off-line password guessing attack, and parallel session attack. The security analysis is described as follows.

(1) It can resist the smart-card-loss-attack.

In the Step L-3* of the login phase, the user sends $\{ID_U, T_U, C_2, C_3\}$ to the server, where $C_2 = h(C_1 \oplus r \oplus T_U)$, $C_3 = h(C_1) \oplus r$ and $C_1 = R \oplus h(b \oplus PW_U)$. The server authenticates the user by verifying C_2. Because the random number r is included in C_2, thereby C_2 value varied on each login session. The ever changed C_2 to result in the adversary cannot verify her guessing. Thus the improved scheme resists the smart-card-loss-attack.

(2) It can withstand the off-line password guessing attack.

Suppose the adversary E wants to adopt off-line guessing attack on the improved scheme. E intercepts $\{ID_U, T_U, C_2, C_3\}$ from Step L-3*. Since $C_2 = h(C_1 \oplus r \oplus T_U)$ and $C_3 = h(C_1) \oplus r$, it is infeasible for the adversary E to obtain C_1 or r from C_2 and C_3. Similarly, if E intercepts $\{T_S, C_4\}$ from Step A-2*, it is also difficult to recover C_1 or r due to $C_4 = h(C_1 \oplus r \oplus h(T_S))$. Even if C_1 or r are known by the adversary, due to $C_1 = R \oplus h(b \oplus PW_U)$, it is also difficult for the adversary to guess password since R and b are unknown. Thus the improved scheme withstands the off-line password guessing attack.

(3) It can avoid the parallel session attack.

Parallel session attack is resulted from symmetric computations of response messages on both the server and smart card ends. In the improved scheme, suppose that the adversary E wants to mount the parallel session attack by initiating a parallel session. When a legitimate user U sends the login request $\{ID_U, T_U, C_2, C_3\}$ to the server, E also sends $\{ID_U, T_U', C_2, C_3\}$ to the server. However, the server will check C_2 to authenticate the user. Note that $C_2 = h(C_1 \oplus r \oplus T_U)$, thus the parallel session attack will be detected by the server with the following two cases: (1) If $T_U' = T_U$ the replay request is detected by S due to the presence of the same timestamp; (2) If $T_U' \neq T_U$ the parallel session attack will be detected by checking C_2. Thus the improved scheme withstands the parallel session attack.

6. Conclusions

Smart card based password authentication scheme is a very widely used mechanism to allow users to access information or services through networks. However, many smart card based password authentication schemes are vulnerable to the smart-card-loss-attack. That is, an adversary can launch various attacks to get benefits or to hurt the cardholder when he/she obtains the smart card. The main contributions of this paper are:

(1) We have shown that Hsiang *et al.*'s remote user authentication scheme is vulnerable to smart-card-loss-attack. If an unauthorized person obtains the smart card, he can guess the password to masquerade as the legitimate user to login the system.

(2) We have proposed an improved scheme to fix the flaws. The improved scheme has the merits of providing mutual authentication, no verification table and users can freely update their passwords. The improved scheme can resist the smart-card-loss-attack, off-line password guessing attack and parallel session attack.

Acknowledgements

This work was partially supported by the National Science Council of the Republic of China under the contract number NSC 101-2632-E-274-001-MY3.

References

[1] C. C. Chang and T. C. Wu, "Remote password authentication with smart cards," IEE Proc E- Comput Digit Tech, vol.138, is. 3, pp. 65-168. 1993.

[2] Y. C. Lee and Y. C. Hsieh, "A password authentication scheme with forward secrecy," ICIC EL, vol. 5, no. 4 (A), pp. 1101-1105, 2011.

[3] I. E. Liao et al., "A password authentication scheme over insecure networks," J Comput Sys Sci, vol. 72, no. 4, pp. 727-740, 2006.

[4] C. S. Tsai et al., "Password authentication schemes: current status and key issues," Int J Net Sec, vol. 3, no. 2, pp. 101-115, 2006.

[5] M. Kumar, "A new secure remote user authentication scheme with smart cards," Int J Net Sec, vol. 11, no. 2, pp. 88-93, 2010.

[6] L. Lamport, "Password authentication with insecure communication," Commun ACM, vol. 24, no. 11, pp. 770-772, 1981.

[7] M. S. Hwang and L. H. Li, "A new remote user authentication scheme using smart cards," IEEE T Consum Electr, vol. 1, no. 46, pp. 28-30, 2000.

[8] H. M. Sun, "An efficient remote user authentication scheme using smart cards," IEEE T Consum Electr, vol. 4, no. 46, pp. 958-961, 2000.

[9] W. H. Yang and S. P. Shieh, "Password authentication schemes with smart card," COMPSEC, vol. 8, no. 18, pp. 727-733, 1999.

[10] C. M. Chen and W. C. Ku, "Stolen-verifier attack on two new strong-password authentication protocols," IEICE T Commun, vol. E85-B, pp. 2519-2521, 2002.

[11] B. T. Hsieh et al., "On the security of some password authentication protocols," Informatica, vol. 14, no. 2, pp. 195-204, 2003.

[12] S. M. Yen and K. H. Liao, "Shared authentication token secure against replay and weak key attacks," Inform Process Lett, vol. 62, no. 2, pp. 77-80, 1997.

[13] H. Y. Chien et al., "An efficient and practical solution to remote authentication: smart card," COMPSEC, vol. 4, no. 21, pp. 372-375, 2002.

[14] W. C. Ku and S. M. Chen, "Weaknesses and improvements of an efficient password based remote user authentication scheme using smart cards," IEEE T Consum Electr, vol. 50, no. 1, pp. 204-207, 2004.

[15] E. J. Yoon et al., "Further improvement of an efficient password based remote user authentication scheme using smart cards," IEEE T Consum Electr, vol. 50, no. 2, pp. 612-614, 2004.

[16] H. C. Hsiang and W. K. Shih, "Weaknesses and improvements of the Yoon-Ryu-Yoo remote user authentication scheme using smart cards," Comput Commun, vol. 32, pp. 649-652, 2009.

[17] D. He et al., "Weaknesses of a remote user password authentication scheme using smart card," Int J Net Sec, vol. 13, no. 1, pp. 58-60, 2011.

[18] P. Kocher et al., "Introduction to differential power analysis," J Crypto Eng, vol. 1, is. 1, pp. 5-27, 2011.