Improvements of a Remote User Password Authentication Scheme using Smart Card

Kwang Cheul Shin and Won Whoi Huh

Division of Industrial Management Engineering, Sungkyul University,
#147-2, Anyang 8 dong, Manan-gu, Anyang-si,
Gyeonggi-do 430-742, Korea

skcskc12@sungkyul.edu, wonwhoi@hanmail.net

Abstract

In 2009, Hsiang et al.'s proposed a secure, improved remote user authentication scheme using smart card against the parallel session attack, masquerading attack, and password guess attack. Hsiang et al.'s scheme, however, is still vulnerable to off-line password guess attack if the attacker steals or temporarily accesses the smart card to extract the information stored in it, and does not satisfy the security requirement against the adversary that have to be considered in remote user authentication scheme using password-based smart cards. In this paper, I proposed an efficient mutual authentication scheme that based on the hash function and random number. Accordingly, an improved remote user authentication scheme is proposed that is secure against password guess attack.

Keywords: *Remote Authentication, Smart Card, Password Guess*

1. Introduction

With the large scale proliferation of internet and network technologies, smart card based authentication schemes have been widely deployed to verify the legitimacy of remote user's login request.

In remote authentication process, a remote server authenticates a registered user based on his secret credentials.

In traditional authentication schemes, the server or system has to store a password table to save passwords of all the registered user of the system.

In 1981, Lamport [1] proposed a password based authentication scheme using password table to authenticate remote users insecure network.

Since then, many password based authentication schemes were proposed to improve the security, efficiency or cost [2-8].

2008 Hsiang *et al.*, [9] proposed an improved efficient scheme to solve the problems of Yoon et al.'s [10] scheme of 2004, that is vulnerable to parallel session attack and seems to be vulnerable to masquerading attack and password guess attack. The present paper suggests Hsiang *et al.'s* proposed scheme is still vulnerable to password guess attack. An attacker can be disguised as a legitimate system user and guess password by extracting the information stored on a smart card that is lost or stolen, or illegally accessed on by the attacker [11-12].

Therefore, Hsiang *et al.'s* scheme does not meet safety requirements of a smart card based authentication system [13]. The present paper proposes an improved smart card based authentication system that solved such problems while maintaining the scheme proposed by Hsiang *et al.'s*.

2. Review of Hsiang *et al.*'s Scheme

In this section, the authentication techniques of Hsiang *et al.'s* scheme are analyzed, followed by the derivation and discussion of its vulnerability.

In this section, I briefly review Hsiang *et al.'s* scheme which consists of four parts namely, registration phase, login phase, verification phase and password change.

2.1. Notations

The notations used throughout this paper can be summarized as follows:

U : the user.
ID : the identity of U.
pw : the password of U.
S : the remote server.
x : the permanent secret key of S.
h() : a hash function.
⇒ : a secure channel.
↛ : a common channel.

2.2. Registration Phase

In this phase, the user U initially registers with the server S.

(1) U chooses his ID, pw and a random number b, then computes h(pw) and h(b⊕pw). At last, U sends ID, h(pw) and h(b⊕pw) and over a secure communication channel to S.

(2) Upon receiving ID, h(pw) and h(b⊕pw), S checks if it is U's first registration. If it is, creates an entry for in the account database and store n=0 in the entry. Otherwise, S sets n=n+1 in the existing entry for U. Next, S computes EIDu=h(ID || n), P=h(EIDu⊕x), R=P⊕h(b⊕pw), and V=h(P⊕h(pw)). At last, S stores the secure information V, R and h() into U's smart card CARD and gives the smart card to U.

(3) Upon receiving CARD, U enters b into his smart card.

2.3. Login Phase

In this phase, the user U sends a login request message to the server S whenever U wants to access some resources upon S.

(1) U inserts his smart card, CARD, into a smart card reader and then inputs his ID and pw.

(2) Using pw, the smart card computes C1=R⊕h(b⊕pw) and C2=h(C1⊕Tu), where Tu is the current timestamp.

(3) U↛ S {ID, Tu, C2}

2.4. Authentication Phase

In this phase, the server S verifies the authenticity of the login message requested by the user U.

(1) Upon receiving the message ID, Tu, C2, S checks ID and Tu. If either ID or Ts-Tu ≤ 0. S rejects U's login request. Otherwise, S computes h(h(EIDu⊕x)⊕Tu). If the computed result

equals the received C2, S accepts U's login request and computes C3=h(h(EIDu⊕x)⊕Ts), where Ts is S's current timestamp. Otherwise, S rejects U's login request.

(2) S → U: {Ts, C3}

(3) Upon receiving the message {Ts, C3}, U checks Ts. If Ts is invalid or equals Tu, U terminates this session. Otherwise, U computes h(C1⊕Ts), then compares the result to the received C3. If equal, U successfully authenticates S.

2.5. Password Change Phase

In this phase, the user U changes his password any time he wants.

(1) U inserts his smart card into a smart card reader and then types in his ID and pw.

(2) The smart card computes P*=R⊕h(b⊕pw) and V*=h(P*⊕h(pw)).

(3) The smart card compares V* with the stored V in smart card. If they are not equal, the smart card rejects the password change request. Otherwise, U chooses a new password pw'.

(4) The smart card then computes R'=P*⊕h(b⊕pw') and V. It now replaces R and V with newly updated R' and V', respectively.

2.6. Scheme Analysis

In this section, it will be pointed out that Hsiang *et al.'s* proposed authentication scheme is vulnerable to password guess attack.

Kocher and Messerges claimed in their paper [7], [8] that the information stored in the smart card can be extracted using power consumption attack, etc. Based on these facts, a password guess attack can be performed to figure out the user's password when: ① the user lost or was stolen the smart card [14]; ② the attacker temporarily makes access to the smart card and extracts the information in it.

In order to analyze the stability of Hsiang *et al.'s* scheme, it is assumed that the attacker has the following attack abilities.

The attacker can control all the process of communication between the server and the user, and tap, delete, modify and add the contents of the message being delivered.

The attacker is able to extract the information that is stored in user's smart card.

The case ①, if an attacker steals the smart card from a legal user, the attacker could guess password effectively. I will show how the attacker gets the user's password in their authentication scheme.

Note that the value R, V, h() and b are stored in the card. They are enough which gives necessary information to guess correct password pw to the attacker.

First of all, the attacker chooses a candidate password from the dictionary, and performs hash function h() with the result of the exclusive OR operation using the random number b and the guessed password. By using the guessed password pw', the attacker computes:

P'=R⊕h(b⊕pw')
V'=h(P'⊕h(pw'))

The attacker verifies V' with the stored V. If they are not equal, the attacker tries another guess for password and repeat the operations again. If the attacker passes the verification, it means that the guessed password is the correct password.

The case ② is the method the attacker intercepts the login message when the user U

transfers a login message {ID, Tu, C2} to S, and figuring out U's password by off-line password guess attack .

The user U's password pw' is guessed and the following computation is performed.

C1'=R⊕h(b⊕pw')
C2'=h(C1'⊕Tu)
C1'and C2' are checked if they have the same value.

The attacker repeats the process with his/her guess pw until C1' and C2 'are the same. Hsiang *et al.'s* authentication scheme is vulnerable to safety because the attacker can figure out the user's password using the off-line password guess attack like this.

3. Propose Scheme

The problem of Hsiang *et al.'s* authentication scheme lies in the value of V and b stored on a smart card for checking the guessed password. In this section, therefore, b is created by server S and distributed differently for each user (not stored in the smart card); and V is not generated.

The proposed scheme is composed of the registration phase, login phase, authentication phase, and password change phase.

3.1. Registration Phase

This phase is invoked whenever user U initially registers or re-registers to the authentication server S.

Suppose x, b are secret key and secret random number, b is used to provide during the authentication phase, when card holder is losted parameter b.

(1) U chooses his ID and pw, then computes h(pw).

(2) U ⇒ S: ID, h(pw)

(3) Upon receiving ID and h(pw). S checks if it is U's first registration. If it is, creates an entry for in the account database and store n=0, In addition, S selects U's random number b and computes b ⊕ x with his private key, and computes ID⊕h(x) with U's ID and stores the resulting value in the database. Otherwise, S sets n=n+1 in the existing entry for U. Next, S computes EIDu=h(ID ‖ n), P=h(EIDu⊕x) and R=P⊕h(b⊕h(pw)), At last, S stores the secure information ID, R and h() into U's smart card and gives the b to U.

3.2. Login Phase

In this phase, the user U sends a login request message to the server S whenever U wants to access some resources upon S.

(1) U inserts his smart card, into a smart card reader and then inputs his pw and b.

(2) Using pw and b, the smart card computes C1=R⊕h(b⊕h(pw)) and C2=h(C1⊕Tu), where Tu is the current timestamp.

At the end of login phase, User U sends login message m={ID, Tu, C2} to S for the authentication process.

(3) U↣ S {ID, Tu, C2}

User U **Server S**

registration phase
ID, h(pw)
----------> DB entry n=0 or n=n+1,
b⊕x, ID⊕h(x)
EIDu=h(ID||n)
P=h(EIDu⊕x)
R=P⊕h(b⊕h(pw))
<---------- in store smart card[ID, R, h()] and b

login phase
input pw, b
C1=R⊕h(b⊕h(pw))
C2=h(C1⊕Tu)
ID, Tu, C2 ----------> **authentication phase**
ID, Tu check (accept or reject)
C2'=H(h(EIDu⊕x) ⊕Tu)
C2'=?C2 (accept or reject)
C3=h(h(EIDu⊕x) ⊕b⊕Ts)
<---------- C3, Ts

authentication phase
Ts check (accept or reject)
C3'=h(C1⊕b⊕Ts)
C3'=?C3 (accept or reject)

password change phase
P'=R⊕h(b⊕h(pw)).
Input new password pw' and b
R'=P*⊕h(b⊕h(pw'))

Figure 1. The Improved Propose Scheme

3.3. Authentication Phase

In this phase, upon receiving the login request message m={ID, Tu, C2}, the server S verifies the authenticity of the login message requested by the user U.

(1) Upon receiving the message ID, Tu, C2, S checks ID and Tu. If either ID or Ts-Tu ≤ 0. S rejects U's login request. Otherwise, S computes h(h(EIDu⊕x)⊕Tu). If the computed result equals the received C2, S accepts U's login request and computes ID⊕h(x) using U's own private key and ID from the database, and find b from b⊕x in the same entry as the computation result.

It continues to compute C3=h(h(EIDu⊕x)⊕b⊕Ts), where Ts is S's current timestamp. Otherwise, S rejects U's login request.

For mutual authentication, S acquires current timestamp Ts and then sends the authentication message {Ts, C3} to U.

(2) S → U : {Ts, C3}

(3) Upon receiving the message {Ts, C3}, U checks Ts. If Ts is invalid or equals Tu, U terminates this session. Otherwise, U computes h(C1⊕b⊕Ts), then compares the result to the received C3. If equal, U successfully authenticates S.

3.4. Password Change Phase

In this phase, the user U changes his password any time he wants.

(1) First of all U performs login and authentication phases. Only if U finishes the phase successfully, U's smart card computes P'=R⊕h(b⊕h(pw)).

(2) U selects a new password pw' and input b.

(3) The smart card then computes R'=P*⊕h(b⊕h(pw')), which yield h(EIDu⊕x)⊕h(b⊕h(pw')).

4. Scheme Analysis

In this section, the security analysis is performed for the proposed scheme in the Table 1. What was focused on in this study is the password guess attack that can figure out user's password when: ① the user lost or was stolen the smart card; ② the attacker temporarily makes access to the smart card and extracts the information in it.

4.1. Resistance to Stolen Verifier Attack

In real environment, it is a common practice that many users use same passwords to access difference applications or servers for their convenience of remembering long password and use them easily.

The problem of Hsiang *et al.'s* authentication scheme is that the attacker can obtain b, R, V values stored in the smart card if the attacker gets the smart card.

The attacker selects pw' from the dictionary file, and computes P' = R⊕h(b⊕h(pw')); followed by V'=h(P'⊕h(pw')) is obtained using p'; and verifies if the guessed password is correct by comparing the V and V'.

In the proposed scheme, however, the value of b is not stored on the smart card.

The attacker is not able to compute the value of R(=P⊕h(b⊕h(pw))) even if he has acquired the smart card.

The attacker should attack the database of S in order to figure out the value of b; but the database does not have a clue about the value of b.

Without the private key x of S, U' ID (ID ⊕ h (x)) cannot figure out from the database. Without U's ID, the entry cannot be found. Even if U' ID is found, U's random number b cannot figure out without knowing S's private key x. The reason is that the random number b is the XOR operation value (b⊕x) with the private key x of S.

Therefore, the attacker cannot deduce pw without knowing b; and password guess attack is impossible.

4.2. Securely Chosen and Update Password

In the proposed scheme, the legitimate smart card holder can freely choose and change his password without any hassle of contacting the remote server S.

Any other adversary, even having stolen or lost smart card cannot change or update the password without knowing the corresponding valid pw and b of the smart card holder.

4.3. Mutual Authentication

In my scheme, mutual authentication of U and S is performed to keep trust of both communication parties. According to the requirements of authentication, U should also authenticate remote server.

In the presented scheme, S sends mutual authentication message {C3, Ts} to U to validate its authenticity.

The value of C3 is calculated by pw and b which is only known to U and this message is infeasible to forge by a fake server to impersonate the S.

Table 1. Security Analysis

Classified	Proposed scheme	Hsiang et al.'s scheme
Mutual Authentication	Yes	Yes
Password guess Attack	Yes	No
Forgery/Impersonation Attack	Yes	No
Secret key guess Attack	Yes	No
Stolen verifier Attack	Yes	No
Mutual Authentication	Yes	Yes

Yes: endure attacks, No: vulnerable to attacks

4.4. Forgery/Impersonation Attack

If an attacker wants to be disguised as a rightful user in the authentication scheme proposed in this paper, the attacker should have the user's ID, password, and the parameter b.

It is easy to get the user's ID because it is unveiled, but the guessing attacks on the user's password and the parameter b are impossible as mentioned previously. It is not possible to guess the password because the value of b is not saved in the smart card.

It means it is impossible for the attacker to conduct the disguised attack with forged information because C2 and C3 can't be created even if the attacker uses all of the available information.

As presented in Table 1, it is found that Hsiang *et al.'s* scheme is vulnerable to some attacks and the scheme proposed in this paper is an improved authentication scheme that solves the vulnerabilities of password guessing attack and disguised attack.

5. Conclusion

The user authentication scheme using smart card should be strong enough to prevent the extracted information, which the attacker extracted from the user's smart card, from use to figure out the user's password. In this paper, it was pointed out that Hsiang *et al.'s* scheme is vulnerable to offline password guess attack.

In other words, it is shown that the attacker can get the information saved in the user's smart card and then find out the user's password using the information.

In order to overcome the noted vulnerability, an improved user authentication scheme was proposed, based on random number b provided by hash function and server S to each user.
It is found that the proposed user authentication scheme makes password guessing attack, forgery and disguised attack impossible.

Thus, it is expected that the authentication scheme proposed in this paper efficiently solves the specified vulnerabilities while maintaining the advantages of the existing smart-card-based user authentication scheme.

References

[1] L. Lamport, "Password authentication with insecure communication", communications of the ACM, vol. 24, no. 11, **(1981)**, pp. 770-772.
[2] M. S. Hwang and L. H. Li, "A new remote user authentication scheme using smart cards", IEEE Transactions on Consumer Electronics, vol. 46, no. 1, **(2000)**, pp. 28-30.
[3] Q. Xie, J.-K. Wang, D.-R. Chen and X.-Y. Wang, "A novel user authentication scheme using smart card", College of Computer Science, Zhejiang University, Hangzhou, 310027, P R China, and Graduate School, Hangzhou Normal University, **(2008)**.
[4] K.-C. Shin, "Analysis & Countermeasure for Authentication Scheme of Qi Xie's Based on Variable Authenticator", The Korean Institute of Information Technology, vol. 10, no. 1, **(2012)** January, pp. 139-146.
[5] H. Jiang, "Strong password authentication protocols", 2010 4th International Conference on Distance Learning and Education, **(2010)** October, pp. 50-52.
[6] R. Song, "Advance smart card based password authentication protocol", Computer Standards and Interface, vol. 32, **(2010)**, pp. 321-325.
[7] Kwang-Cheul Shin, "Vulnerability Analysis and Improvement in Man-in-the-Middle Attack for Remote User Authentication Scheme of Shieh & Wang et al.'s using Smart Card", Society e-Business Studies, vol. 17, no. 4, **(2012)** November, pp. 1-16. (dx.doi.org/10.7838 /jsebs.2012.17.4.001).
[8] K.-C. Shin, "Vulnerability Analysis and Improvement of a Remote User Authentication Scheme by Legitimate Members", Korea Knowledge Info. Tech. Society, vol. 7, no. 6, **(2012)** December, pp. 181-192.
[9] H. C. Hsiang and W. K. Shih, "Weakness and improvements of the Yoon-Ryu-Yoo remote user authentication scheme using smart cards", Computer Communications, vol. 32, **(2009)**, pp. 649-652.
[10] E. J. Yoon, E. K. Ryu and K. Y. Yoo, "Further improvements of an efficient password based remote user authentication scheme using smart cards", IEEE Trans. on Cons. Elect., vol. 50, no. 2, **(2004)**, pp. 612-614.
[11] P. Kocher, J. Jaffe and B. Jun, "Differential power analysis", Proceedings of Advances in Cryptology (CRYPTO 99), (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.
[13] D. He, J. Chen and J. Hu, "Weaknesses of a remote user password authentication scheme using smart card", International Journal of Network Security, vol. 13, no. 1, **(2011)** July, pp. 58-60.
[14] X. Y. Chen and H. S. Kim, "Enhancement of Hsiang and Shih's Remote User Authentication Scheme using Smart Card", Korean Institute of Information Scientists and Engineers, vol. 37, no. 2(B), **(2010)**, pp.52-55.

Authors

Kwang Cheul Shin

Division of Industrial Management Engineering, Sungkyul University, #147-2, Anyang 8 dong, Manan-gu, Anyang-si, Gyeonggi-do 430-742, Korea, skcskc12@sungkyul.edu

Education & Work experience: 2003, Ph.D. degree in Information and Communication Engineering, Sung kyunkwan University. Currently: Professor in Dept. of Industrial Management Engineering, Sungkyul University. Tel: 82-031-467-8916.

Won Whoi Huh

Division of Multimedia Engineering, Sungkyul University,#147-2, Anyang 8 dong, Manan-gu, Anyang-si, Gyeonggi-do 430-742, Korea, wonwhoi@hanmail.net

Education & Work experience: Graduate School of NID Fusion Technology, Digital Contents Design, 2012, Ph.D. Academic degree of Professional degree, IT & Design Fusion Program, Seoul national University of Science & Technology. Currently: Professor in Dept. of Multimedia Engineering, Sungkyul University. Tel: 82-031-467-8915.