Security Analysis and Enhancements of A Remote User Authentication Scheme

Shou-Qi Cao, Qing Sun, and Li-Ling Cao
(Corresponding author: Li-Ling Cao)

College of Engineering Science and Technology, Shanghai Ocean University
Shanghai 201306, China
(Email: llcao@shou.edu.cn)

(Received June 6, 2018; Revised and Accepted Sept. 22, 2018; First Online Jan. 23, 2019)

Abstract

Many remote user authentication schemes have been designed and developed to establish secure and authorized communication between the users and the sever over an insecure channel. By employing a secure remote user authentication scheme, the users and the server can authenticate each other and utilize advanced services. In 2012, Hsieh and Leu proposed a remote user authentication scheme. However, we review and analyze Hsieh and Leu's scheme and find that their scheme can't provide user anonymity and is vulnerable to slow wrong password detection, masquerading attack and password guessing attack. In order to solve these drawbacks, we propose a security-improved authentication scheme which can resist all attacks above. Finally, security formal analysis of the proposed scheme using Burrows-Abadi-Needham logic (BAN-logic) is given, which indicates that the proposed scheme can protect against several possible types of attacks with only a slightly high computational cost.

Keywords: Authentication; Hash Function; Masquerading Attack; User Anonymity

1 Introduction

With the rapid development of the internet, computer applications have penetrated into all areas of society, which provide us a lot of services and bring conveniences to our life and work. However, it also brings many negative effects such as the fortified ability of attackers via the internet. At the same time, information security has become an important issue. In order to protect the security of information, many scholars have proposed some authentication schemes to establish secure and authorized communication between the users and the server. After Lamport [13] first proposed a password-based user authentication scheme, many researchers proposed password-based user authentication schemes with key agreement [7,16,20]. However, Lennon et al. [15] and Yen and Liao [25] demonstrated that Lamport's scheme was vulnerable to stolen verifier attacks. Typically, in one-factor authentication schemes, the server maintains a table containing the verifiers of the users [8]. Therefore, the servers tend to be easy objects of attack, because if an adversary achieves the verifier of a user that is stored in the verification table, then he/she can masquerade as the victim user [2, 6, 11].

In order to overcome these problems, some schemes based on smart card which also called two-factor authentication schemes have emerged. In 1991, Chang and Wu [4] developed the first smart-card-based password authentication scheme. Then, many improvements were made to enhance its security and efficiency [12,14,17,24]. In 2004, Yoon et al. [26] proposed a scheme which enabled users to change passwords freely and securely without the help of a remote server, while also providing secure mutual authentication. However, Hsiang and Shih [9] found that it can't resist parallel session attack and masquerading attack and password guessing attack. Therefore, Hsiang and Shih proposed their own scheme, but He et al. [5] pointed out that it was still vulnerable to password guessing attack, masquerading attack. Besides, Hsieh and Leu [10] found that an insider can carry out an infringed account attack and a resembling account attack on Hsiang et al.'s solution. However, Wang et al. [22] showed that, under their non-tamper- resistance assumption of the smart cards, Hsieh and Leu's scheme was still prone to offline dictionary attack, in which an attacker could obtain the victim's password when getting temporary access to the victim's smart cards. Wang et al. didn't put forward improved scheme. In this paper, we find that Hsieh and Leu's scheme is still exposed to masquerading attack, password guessing attack and can't provide user anonymity, mutual authentication, fast password detection. Therefore, we propose our improved scheme that can fight against all aforementioned attacks.

The rest of the paper is organized as follows. The review and the analysis of Hsieh and Leu's scheme are presented in Section 2 and 3. In Section 4, we propose a scheme that can resist all attacks mentioned in related researches. Section 5 devotes to making security formal

analysis based on Burrows-Abadi-Needham logic (BAN-logic) and comparing the proposed scheme with some existing ones. The result indicates that our modified scheme has a slightly high computational cost and can protect against some possible attacks. Finally, we conclude this paper in Section 6.

2 Review of Hsieh and Leu's Scheme

Hsieh and Leu's scheme is a remote user authentication scheme which uses hash functions. It contains four phases: registration, login, authentication and password change.

2.1 Registration Phase

In this phase, the initial registration is different from the re-registration. The process of the initial registration is depicted as follows.

R1. User U chooses a random number b and computes $h(b \oplus PW_u)$.

R2. U sends the message ID_u, $h(PW_u)$ and $h(b \oplus PW_u)$ to S.

R3. In the account database, the server S creates an entry for U and stores $n = 0$ in this entry.

R4. S performs the following computations: $P = h(EID \oplus x)$, $EID = h(h(ID_u)||n)$, $R = P \oplus h(b \oplus PW_u)$, $V = h(h(PW_u) \oplus h(x))$ which is stored in the entry of U.

R5. S gives a smart card to U containing R and $h(\cdot)$.

R6. When receiving the smart card issued by the server S, U inputs b into his smart card. Finally, the smart card contains b, R and $h(\cdot)$. After this phase, U does not need to remember b.

If U misses her/his smart card and wants to re-register to S, the process of the re-registration is as the follows.

RR1. User U chooses a new random number b' and computes $h(b' \oplus PW_u)$.

RR2. U sends the message ID_u, $h(PW_u)$, $h(b' \oplus PW_u)$ to S.

RR3. S computes $V' = h(h(PW_u) \oplus h(x))$ and compares V with V'.

RR4. If V' is equal to V, S sets $n = n+1$ in the existing entry. Then S performs the following computations: $P_{new} = h(EID \oplus x)$, $EID = h(h(ID_u)||n)$, $R_{new} = P \oplus h(b' \oplus PW_u)$.

RR5. Finally, S performs Steps R5 and R6 shown in the initial registration process.

2.2 Login Phase

When U wants to login to the remote server S, the following operations will be performed.

L1. U inserts his smart card into the smart card reader and enters his ID_u and PW_u.

L2. The following computations are performed by U's smart card: $C_1 = R \oplus h(b \oplus PW_u)$, $C_2 = h(C_1 \oplus T_u)$, where T_u denotes U's current timestamp .

L3. U sends $C = \{ID_u, T_u, C_2\}$ to S.

2.3 Authentication Phase

After receiving the login request message $C = \{ID_u, T_u, C_2\}$, the remote server S and U's smart card perform the following operations.

A1. If either ID_u or T_u is invalid or $T_s - T_u \leq 0$, S rejects U's login request. Otherwise, S computes $C_2' = h(h(EID \oplus x) \oplus T_u)$ and compares C_2' with the received C_2. If $C_2' = C_2$, S accepts U's login request and computes $C_3 = h(h(EID \oplus x) \oplus h(T_s))$, where T_s is S's current timestamp. Otherwise, S rejects U's login request.

A2. S sends T_s and C_3 to U.

A3. If either T_s is invalid or $T_s = T_u$, this session will be terminated by U. Otherwise, U computes C_3' and compares C_3' with the received C_3, $C_3' = h(C_1 \oplus h(T_s))$. If C_3' is equal to C_3, U authenticates S successfully.

2.4 Password Change Phase

When U wants to change his password, the following process will be performed.

P1. U inserts his smart card into the smart card reader and enters ID_u, PW_u and new password PW_{new}.

P2. U sends the message ID_u, $h(PW_u)$, $h(PW_u) \oplus h(PW_{new})$, $h(b \oplus PW_{new})$ to S.

P3. S computes $V' = h(h(PW_u) \oplus h(x))$ and compares V' with V in the account database.

P4. If V' is equal to V, then S computes $h(PW_u) \oplus h(PW_{new}) \oplus h(PW_u)$ to get $h(PW_{new})$. Next, S performs the following computations.

$$\begin{aligned} P &= h(EID \oplus x) \\ EID &= h(h(ID_u)||n) \\ R_{new} &= P \oplus h(b \oplus PW_{new}) \\ V_{new} &= h(h(PW_{new}) \oplus h(x)) \end{aligned}$$

which is stored in U's entry.

P5. S sends R to U.

P6. Finally, U's smart card replaces R with R_{new}.

3 Cryptanalysis of Hsieh and Leu's Scheme

In this section, we analyze the security of Hsieh and Leu's scheme on the basis of the following assumptions:

1) An attacker can eavesdrop, intercept, and modify any message in the channel.

2) An attacker may either (1) obtain a user's password or (2) extract the secret information of the smart card, but can't achieve both (1) and (2) at the same time.

3.1 User Anonymity

Whenever a legal user U sends a login request message, the login request message contains the identity ID_u of the user. Therefore, Hsieh and Leu's scheme can't protect the anonymity of the user.

3.2 Slow Wrong Password Detection

Slow wrong password detection refers to instances in which the user can't know of a mistake immediately when inputs the wrong password, and the user can know when server S notifies there is a wrong user password. In Hsieh and Leu's authentication scheme, the user's smart card can't verify the accuracy of the user password during the login phase. Only S verifies a legal user by comparing the similarities between C_2' and C_2 during authentication phase. Concretely, U inputs ID_u and PW_u, then if U selects a wrong password PW_u^*, the smart card is unaware that the password is incorrect. The smart card does not check the PW_u^* and it computes various values $\{C_1^*, C_2^*\}$ using PW_u^* for login and authentication. The smart card then sends $\{ID_u, T_u, C_2^*\}$.

S is unable to immediately confirm the wrong password after receiving the message $\{ID_u, T_u, C_2^*\}$. First, S checks the validity of ID_u and T_u, then computes $C_2' = h(h(EID \oplus x) \oplus T_u)$. Then, because C_2^* is not the same as C_2', S eventually confirms that the received messages are not normal, and maybe U could have input the wrong password. Finally, S sends the wrong password notification to U. Hsieh and Leu's authentication scheme requires a lengthy phase that includes value computation and message transmission before confirming that the user input the wrong password. Therefore, a smart card needs a fast wrong password detection technique during login. When U inputs the wrong password during the login phase, the smart card needs to quickly identify the incorrect password and should immediately notify U of the mistake.

3.3 User Masquerading Attack & Replay Attack

When an attacker steals the smart card and intercepts the login request message $\{ID_u, T_u, C_2\}$ from U, he may send the replaying message $\{ID_u, T_u, C_2\}$ to S in a new session during authentication phase. Then S will compute C_2' and find C_2' is the same as C_2. Then S regards the attacker as legal user and accepts the login request.

3.4 Password Guessing Attack

Hsieh and Leu pointed out that Hsiang and Shih's scheme could not resist offline password attack. However, we find that Hsieh and Leu's scheme also fails to solve the problem. Then the attacker can guess the password in the following two conditions.

1) An attacker can know the information $\{R, h(\cdot), b\}$ stored in a smart card.

2) An attacker can intercept the login request message $\{ID_u, T_u, C_2\}$ over the communication channel.

The specific steps are as follows:

1) An attacker selects a password PW_u^*.

2) Computes $C_1^* = R \oplus h(b \oplus PW_u^*)$ and $C_2^* = h(C_1^* \oplus T_u)$.

3) Verifies the correctness of PW_u^* by checking if the computed C_2^* is equal to the intercepted C_2.

4) Repeats 1) $\sim$ 3) of this procedure until the correct value of PW_u is found.

Once the smart card is stolen or picked up, the corresponding password factor can be guessed. So Hsieh and Leu's scheme is not a two-factor scheme and is insecure.

3.5 Mutual Authentication

Generally, if authentication scheme is secure, it can resist user impersonation attack and server masquerading attack. However, the authentication scheme can't resist user impersonation attack as described in Section 4.3. Therefore, Hsieh and Leu's scheme fails to provide mutual authentication.

4 Proposed Scheme

In this section, we propose an enhanced scheme based on Hsieh and Leu's scheme which can resist all the attacks mentioned in Section 3. The enhanced scheme contains four phases: registration, login, authentication, password change phase.

4.1 Registration Phase

The registration phase of the proposed scheme is shown in Figure 1.

1) Initial registration.

R1, R2, R3. The same as Hsieh and Leu's scheme.

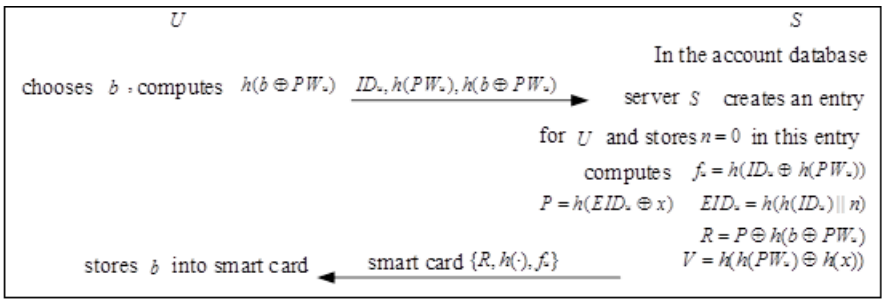

Figure 1: Registration phase

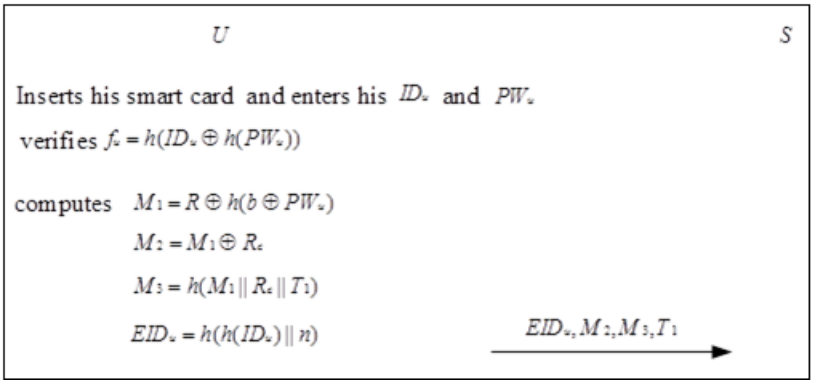

Figure 2: Login phase

R4. S computes f_u, P, R, V as follows.

$$\begin{aligned} f_u &= h(ID_u \oplus h(PW_u)) \\ P &= h(EID_u \oplus x) \\ EID_u &= h(h(ID_u)||n) \\ R &= P \oplus h(b \oplus PW_u) \\ V &= h(h(PW_u) \oplus h(x)). \end{aligned}$$

R5. S sends U a smart card containing f_u, R, $h(\cdot)$. Then U stores b in the smart card.

2) Re-registration.
This phase is the same as Hsieh and Leu's scheme.

4.2 Login Phase

The user U should execute the following steps when he logins to the remote server S (See Figure 2).

L1. The same as Hsieh and Leu's scheme.

L2. The smart card computes f_u and compares the computed f_u with the stored f_u.

L3. If they are the same, U generates the current timestamp T_1 and a random number R. Then U computes M_1, M_2, M_3, EID_u as follows:

$$\begin{aligned} M_1 &= R \oplus h(b \oplus PW_u) \\ M_2 &= M_1 \oplus R_c \\ M_3 &= h(M_1||R_c||T_1) \\ EID_u &= h(h(ID_u)||n). \end{aligned}$$

L4. U sends the login request message $\{EID_u, M_2, M_3, T_1\}$ to S.

4.3 Authentication Phase

After receiving the login request message $\{EID_u, M_2, M_3, T_1\}$, the remote server S and U's smart card perform the following operations and in Figure 3.

A1. S checks whether EID_u is the same as the EID_u stored in the database.

A2. If they are the same, S computes M_4 and M_5 as follows.

$$\begin{aligned} M_4 &= h(EID_u \oplus x) \\ M_5 &= M_2 \oplus M_4. \end{aligned}$$

A3. S compares the M_3 with $h(M_4||M_5||T_1)$. If they are equal, S computes M_6 and M_7.

$$\begin{aligned} M_6 &= M_4 \oplus R_5 \\ M_7 &= h(M_4||R_s||T_2), \end{aligned}$$

where T_2 and R_s respectively denotes S's current timestamp and random number. Then S sends $\{EID_u, M_6, M_7, T_2\}$ to U.

A4. U computes $M_8 = M_6 \oplus M_1$ and verifies whether $M_7 = h(M_1||M_8||T_2)$ or not. If they are the same, U

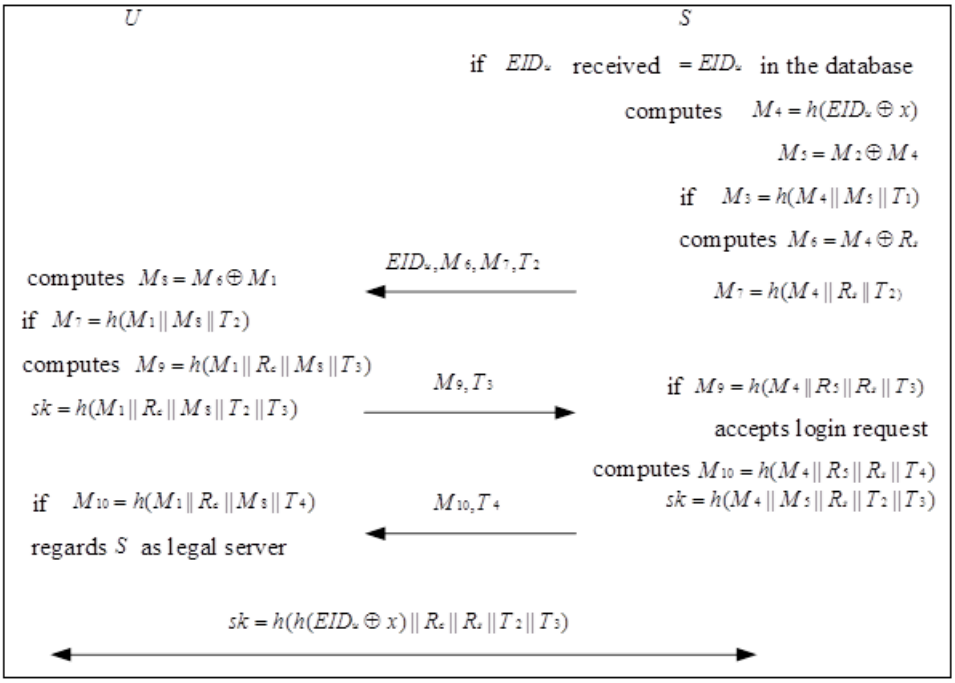

Figure 3: Authentication phase

computes M_9 and sk as follows.

$$\begin{aligned} M_9 &= h(M_1||R_c||M_8||T_3) \\ sk &= h(M_1||R_c||M_8||T_2||T_3) \end{aligned}$$

where T_3 is a timestamp.

A5. U sends $\{M_9, T_3\}$ to S.

A6. S receives the message and starts to verify whether the M_9 is equal to $h(M_4||M_5||R_s||T_3)$. If they are equal, S accepts the login request. Then S computes M_{10} and sk as follows.

$$\begin{aligned} M_{10} &= h(M_4||M_5||R_s||T_4) \\ sk &= h(M_4||M_5||R_s||T_2||T_3). \end{aligned}$$

A7. S sends $\{M_{10}, T_4\}$ to U.

A8. U receives the message and starts to verify whether the M_{10} is equal to $h(M_1||R_c||M_8||T_4)$. If they are equal, U regards S as legal server.

A9. Finally, they share a same session key $sk = h(h(EID_u \oplus x)||R_c||R_s||T_2||T_3)$.

4.4 Password Change Phase

For the proposed scheme, the password change phase is executed when U loses the smart card or wants to update the password.

P1. U selects and inputs ID_u, PW_u, $PW_{u_{new}}$ and generates a new random number b'. Then U submits ID_u, $h(PW_u)$, $h(b' \oplus PW_u)$, $h(PW_{u_{new}})$, $h(b \oplus PW_{u_{new}})$ to S through a secure channel.

P2. After S receives the message, S checks the database for the ID_u and computes $V' = h(h(PW_u) \oplus h(x))$ and compares it with V in the database.

P3. If V' is equal to V, then S carries out the computations as follows:

$$\begin{aligned} f_{u_{new}} &= h(ID_u \oplus h(PW_{u_{new}})) \\ P &= h(EID_u \oplus x) \\ EID_u &= h(h(ID_u)||n) \\ R_{new} &= P \oplus h(b' \oplus PW_{u_{new}}) \\ V_{new} &= h(h(PW_{u_{new}}) \oplus h(x)). \end{aligned}$$

P4. S sends a new smart card to U that contains $f_{u_{new}}$, R_{new}, $h(\cdot)$. Then U stores a new b' in the smart card.

5 Analysis of the Proposed Scheme

In this section, we first analyze the security of our proposed authentication scheme based on the assumptions stated in Section 3. Then, we show that the proposed scheme withstands all attacks mentioned in Hsieh and Leu's scheme.

5.1 Security Analysis Using BAN Logic

Burrows [3] proposed BAN logic in 1990. Although there are some controversial publications about BAN-logic [1, 18, 19, 23], it is the first formal analysis. As a method of analyzing authentication schemes, its simplicity and

intuitiveness have attracted the attention of scholars. The analysis of an authentication scheme using the BAN-logic tool consists of four steps [21] and the formal analysis of the security of the proposed scheme is described as follows.

Step 1. The goals of mutual authentication in the proposed scheme are shown as follows:

$$G1: U \models U \overset{sk}{\longleftrightarrow} S$$
$$G2: S \models U \overset{sk}{\longleftrightarrow} S$$
$$G3: U \models S \models U \overset{sk}{\longleftrightarrow} S$$
$$G4: S \models U \models U \overset{sk}{\longleftrightarrow} S.$$

Step 2. The idealization forms of the messages in the proposed scheme are shown as follows:

Message 1.

$$U \rightarrow S: \langle R_c \rangle_{h(EID_u \oplus x)}, (R_c, T_1)_{h(EID_u \oplus x)}, T_1.$$

Message 2.

$$S \rightarrow U: \langle R_s \rangle_{h(EID_u \oplus x)}, (R_s, T_2)_{h(EID_u \oplus x)}, T_2.$$

Message 3.

$$U \rightarrow S: (R_c, R_s, T_3)_{h(EID_u \oplus x)}, U \overset{sk}{\longleftrightarrow} S, T_3.$$

Message 4.

$$S \rightarrow U: (R_c, R_s, T_4)_{h(EID_u \oplus x)}, U \overset{sk}{\longleftrightarrow} S, T_4.$$

Step 3. The initial states of the proposed scheme can be assumed as follows:

$$P1: U \models \#(T_1)$$
$$P2: U \models \#(T_2)$$
$$P3: U \models \#(T_3)$$
$$P4: U \models \#(T_4)$$
$$P5: U \models U \overset{h(EID_u \oplus x)}{\longleftrightarrow} S$$
$$P6: S \models U \overset{h(EID_u \oplus x)}{\longleftrightarrow} S$$
$$P7: U \models S \Rightarrow U \overset{sk}{\longleftrightarrow} S$$
$$P8: S \models U \Rightarrow U \overset{sk}{\longleftrightarrow} S.$$

Step 4. According to the initial state assumptions and BAN-logic inference rules, the main analysis of the proposed scheme is stated as follows:

According to Message 3, we can get A1:

$$S \lhd \{(R_c, R_s, T_3)_{h(EID_u \oplus x)}, T_3, U \overset{sk}{\longleftrightarrow} S\}.$$

According to the assumption P6 and the message meaning rule, we can get A2:

$$S \models U \vdash \{(R_c, R_s, T_3)_{h(EID_u \oplus x)}, T_3, U \overset{sk}{\longleftrightarrow} S\}.$$

According to P3 and the freshness conjunction rule, we can get A3:

$$S \models \#\{(R_c, R_s, T_3)_{h(EID_u \oplus x)}, T_3, U \overset{sk}{\longleftrightarrow} S\}.$$

According to A2, A3 and the nonce verification, we can get A4:

$$S \models U \models \{(R_c, R_s, T_3)_{h(EID_u \oplus x)}, T_3, U \overset{sk}{\longleftrightarrow} S\}.$$

According to A4, we apply the belief rule, we can get A5:

$$G4: S \models U \models U \overset{sk}{\longleftrightarrow} S.$$

According to P8, A5 and the jurisdiction rule, we can get A6:

$$G2: S \models U \overset{sk}{\longleftrightarrow} S.$$

According to Message 3, we can get A7:

$$U \lhd \{(R_c, R_s, T_4)_{h(EID_u \oplus x)}, T_4, U \overset{sk}{\longleftrightarrow} S\}.$$

According to the assumption P5 and the message meaning rule, we can get A8:

$$U \lhd S \vdash \{(R_c, R_s, T_4)_{h(EID_u \oplus x)}, T_4, U \overset{sk}{\longleftrightarrow} S\}.$$

According to P4 and the freshness conjunction rule, we can get A9:

$$U \lhd \#\{(R_c, R_s, T_4)_{h(EID_u \oplus x)}, T_4, U \overset{sk}{\longleftrightarrow} S\}.$$

According to A8, A9 and the nonce verification, we can get A10:

$$U \models S \models \{(R_c, R_s, T_4)_{h(EID_u \oplus x)}, T_4, U \overset{sk}{\longleftrightarrow} S\}.$$

According to A10, we apply the belief rule, we can get A11:

$$G3: U \models S \models U \overset{sk}{\longleftrightarrow} S.$$

According to P7, A11 and the jurisdiction rule, we can get A12:

$$G1: U \models U \overset{sk}{\longleftrightarrow} S.$$

5.2 Comparison in Security Properties and Efficiency

The improved security properties of the proposed scheme, which is an extension of the Hsieh and Leu's scheme, are described as follows.

1) Identity preservation.
The adversary can easily intercept the user's login request $\{ID_u, T_u, C_2\}$ in Hsieh and Leu's scheme. In order to protect the identity of the legal user, we use the EID_u instead of the ID_u, what's more, the ID_u is encrypted by hash function. The content of M_2, M_3, M_6, M_7 are dynamic and different in each session by using R_c and R_s. Therefore, the proposed scheme can provide identity preservation.

Table 1: Security comparison of the proposed scheme with other related ones

Security features	Hsiang and Shih	Hsieh and Leu	Ours
Provide user anonymity	X	X	O
Mutual authentication	X	X	O
Resist user impersonation attack	X	X	O
Resist server masquerading attack	X	O	O
Resist slow wrong password detection	X	X	O
Resist offline password guessing attack	X	X	O

Table 2: Performance comparison of the proposed scheme with other related ones

Schemes	Login phase	Verification phase	Total
Hsiang and Shih's scheme	$2T_h$	$6T_h$	$8T_h$
Hsieh and Leu's scheme	$2T_h$	$6T_h$	$8T_h$
Proposed scheme	$5T_h$	$10T_h$	$15T_h$

2) Resist slow wrong password detection.
The proposed scheme can check the user's password during the login request. Therefore, it can quickly know whether the password is true or not. In the proposed scheme, when a user wants to login, he inputs his own ID_u, PW_u. On the basis of these, the smart card computes $f_u = h(ID_u \oplus h(PW_u))$ and compares it with the f_u stored in smart card. If the password is wrong, the computed f_u and stored f_u will be different, so the user can't login. At the same time, the user can quickly know he needs to input the correct password.

3) Resist user masquerading attack.
We suppose that an adversary can get the smart card and intercept the login request. If an adversary wants to masquerade as a legal user, he has to send the appropriate response to the server's request. When the adversary replays the login request $\{EID_u, M_2, M_3, T_1\}$ to the sever, the legal server responses $\{EID_u, M_6, M_7, T_2\}$ to the adversary, the adversary accepts it and must response the appropriate $\{M_9, T_3\}$ to the sever. However, he can't compute the correct $\{M_9, T_3\}$ without knowing ID_u, x and R_s, because the ID_u is encrypted by hash function and the x is only known by legal server and the R_s in the database.

4) Resist sever masquerading attack.
If an adversary wants to masquerade as a legal server, he has to send the appropriate response to the user's request. When the user sends $\{M_9, T_3\}$ to the adversary, he has to compute the appropriate $\{M_{10}, T_4\}$ to identify he is the legal server. However, he can't compute the correct $\{M_{10}, T_4\}$ without knowing ID_u, x and R_c, because the ID_u is encrypted by hash function and the x is only known by the legal server and the R_c in the database.

5) Resist password guessing attack.
If an adversary gets the smart card, he can extract all information stored in smart card. If he wants to guess the password, he can guess it by $f_u = h(ID_u \oplus h(PW_u))$. Although the adversary knows f_u, the ID_u is encrypted by hash function, so he can't get the password.

6) Provide mutual authentication.
The proposed scheme can provide mutual authentication because it can resist the user masquerading attack and the server masquerading attack. The security comparison of the proposed scheme with other related ones is presented in Table 1. O denotes that scheme provides the property; X denotes that scheme fails to provide the property. The result obviously indicates that our scheme is more secure.

The computation costs of the proposed scheme and other related ones are calculated in Table 2. In Table 2, T_h presents the computation time for hash function and T_s stands for the computation time for symmetric encryption operation. The computation time for $\oplus$ and $||$ can be ignored because the time is very short.

The results in Table 1 and Table 2 indicate that our scheme provide all security properties with only a slightly high computational cost.

6 Conclusion

This article first reviews Hsieh and Leu's scheme and then analyses the security of Hsieh and Leu's scheme. Secondly, we point the shortcomings of the scheme. Finally, we propose a new scheme to protect against all attacks. The results show that the proposed scheme has more secure properties than some other related ones.

Acknowledgments

This study was supported by 2017 "innovative action plan" of Science and Technology Commission of Shanghai Municipality (17050502000), 2017 cooperative project on Industry-Academy-Research of Shanghai Lingang Administrative Committee (Key technology research and demonstration line construction of advanced laser intelligent manufacturing equipment), the Doctoral Scientific Research Foundation of Shanghai Ocean University (A2-0203-00-100361). The authors gratefully acknowledge the anonymous reviewers for their valuable comments.

References

[1] N. Agray, W. V. D. Hoek and E. D. Vink, " On BAN Logics for Industrial Security Protocols," *Lecture Notes in Computer Science*, vol. 2296, pp. 29-36, 2001.

[2] H. Arshad and M. Nikooghadam, "An efficient and secure authentication and key agreement scheme for session protocol using ECC," *Multimedial Tools Applications*, vol. 75, no. 1, pp. 181-197, 2016.

[3] M. Burrows, M. Abadi and R. Needham, "A logic of authentication," *ACM Transactions on Computer System*, vol. 8, no. 1, pp. 18-36, 1990.

[4] C. C. Chang and T. C. Wu, "Remote password authentication with smart cards," *IEE Proceedings - Computer Digital Technology*, vol. 138, no. 3, pp. 165-168, 1991.

[5] D. B. He, J. H. Chen and J. Hu, "Weaknesses of a remote user password authentication scheme using smart card," *International Journal of Network Security*, vol. 13, no. 1, pp. 58-60, 2011.

[6] D. B. He, N. Kumar and J. H. Lee, "Privacy- preserving data aggregation scheme against internal attackers in smart grids," *Wireless Networks*, vol. 22, no. 2, pp. 491-502, 2016.

[7] D. B. He, N. Kumar, H. Shen and J. H. Lee, "One-to-many authentication for access control in mobile pay-tv systems," *Science China-Information Sciences*, vol. 59, no. 5, pp. 1-14, 2016.

[8] D. B. He, H. Wang, L. Wang, J. Shen and X. Yang, "Efficient certificateless anonymous multi-receiver encryption scheme for mobile devices," *Soft Computing*, vol. 21, no. 22, pp. 6801-6810, 2016.

[9] H. C. Hsiang and W. K. Shih, "Weaknesses and improvements of the Yoon-Ryu-Yoo remote user authentication scheme using smart cards," *Computer Communications*, vol. 32, no. 4, pp. 649-652, 2009.

[10] W. B. Hsieh and J. S. Leu, "Exploiting hash functions to intensify the remote user authentication scheme," *Elsevier Advanced Technology Publications*, vol. 31, no. 6, pp. 791-798, 2012.

[11] J. J. Hwang and T. C. Yeh, " Improvement on Peyravian-Zunic's password authentication schemes," *IEICE Transactions on Communications*, vol. 85, no. 4, pp. 823-825, 2002.

[12] 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, pp. 28-30, 2000.

[13] L. Lamport, "Password authentication with insecure communication," *Communications of the ACM*, vol. 24, no. 11, pp. 770-772, 1981.

[14] C. C. Lee, L. H. Li and M. S. Hwang, "A remote user authentication scheme using hash functions," *IEEE Transactions on Consumer Electronics*, vol. 36, no. 4, pp. 23-29, 2002.

[15] R. Lennon, S. Matyas and C. Mayer, "Cryptographic authentication of time-invariant quantities," *IEEE Transactions on Communications*, vol. 29, no. 6, pp. 773-777, 1981.

[16] 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, no. 1, pp. 1-5, 2010.

[17] D. Mishra, "Efficient and secure two-factor dynamic ID-based password authentication scheme with provable security," *Cryptologia*, vol. 42, no. 2, pp. 146-175, 2018.

[18] W. Teepe, "BAN Logic is Not 'Sound', Constructing Epistemic Logics for Security is Difficult," in *Proceedings of Famas*, 2006. (`https://pdfs.semanticscholar.org/bf93/01895b281c2ce6645f260d211833e8dbff03.pdf`)

[19] W. Teepe, "On BAN logic and hash functions or: how an unjustified inference rule causes problems," *Autonomous Agents and Multi-Agent Systems*, vol. 19, no.1, pp. 76-88, 2009.

[20] C. S. Tsai, C. C. Lee and M. S. Hwang, " Password authentication schemes: Current status and key issues," *International Journal of Network Security*, vol. 3, no. 2, pp. 101-115, Sept. 2006.

[21] J. L. Tsai, T. C. Wu and K. Y. Tsai, "New dynamic ID authentication scheme using smart cards," *International Journal of Communication Systems*, vol. 23, no. 12, pp. 1449-1462, 2010.

[22] D. Wang and P. Wang, "Offline Dictionary Attack on Password Authentication Schemes Using Smart Cards," *Information Security*, vol. 52, pp. 1212-1217, 2015.

[23] G. Wedel and V. Kessler, "Formal semantics for authentication logics," in *European Symposium on Computer Security (ESORICS'96)*, vol. 1146, pp. 219-241, 1996.

[24] J. Wei, W. Liu and X. Hu, "Secure and efficient smart card based remote user password authentication scheme," *International Journal of Network Security*, vol. 18, no. 4, pp. 782-792, 2016,.

[25] S. Yen and K. Liao, "Shared authentication token secure against replay and weak key attack," *Information Process Letters*, vol. 62, no. 2, pp. 78-80, 1997.

[26] E. J. Yoon , E. K. Ryu and K. Y. Yoo , "Further improvement of an efficient password based remote user authentication scheme using smart cards," *IEEE*

Table 3: Main notations of BAN-logic

Notation	Meaning	Notation	Meaning
P, Q	Principals	X, Y	Message variable
K	Shared key	$\langle X \rangle_Y$	X combined with the formula Y
$P \models X$	P believes X	$\#(X)$	X is fresh
$P \lhd X$	P sees X	$P \overset{K}{\longleftrightarrow} Q$	P and Q may use the shared key K
$P \vdash X$	P once said X	(X, Y)	X or Y is one part of the formula (X, Y)
$P \Rightarrow X$	P has jurisdiction over X	$(X)_K$	X hashed under the key K

Transactions on Consumer Electronics, vol. 50, no. 2, pp. 612-614, 2004.

Appendix

In this section, we introduce the content of BAN-logic with symbols P and Q standing for principals and X and Y representing statements. The main notations of the logic are presented in Table 3.

To describe the logic postulates of BAN-logic, we present the following rules:

1) Message meaning rule.

$$\frac{P \models Q \overset{K}{\longleftrightarrow} P, P \lhd \{X\}_K}{P \models Q \vdash X}$$

P believes that Q once said X if P believes that K is the secret shared key with Q, and P sees X encrypted by K.

2) Nonce-verification.

$$\frac{P \models \#(X), P \models Q \vdash X}{P \models Q \vdash X}$$

P believes that Q believes X if P believes that X is fresh and Q has said X.

3) The belief rule.

$$\frac{P \models (X), P \models (Y)}{P \models (X, Y)}$$

P believes (X, Y) if P believes both X and Y.

4) Jurisdiction rule.

$$\frac{P \models Q \Rightarrow X, P \models Q \models X}{P \models X}$$

P believes Q on the validity of X if P believes that Q has jurisdiction over X.

5) Freshness conjunction rule.

$$\frac{P \models \#(X)}{P \models \#(X, Y)}$$

P believes that (X, Y) is fresh if P believes that X is fresh.

Biography

CAO Shouqi received his bachelor's degree in mechanical manufacturing technology and equipment from Sichuan University in 1996. He received his MS degree in mechanical manufacturing and automation from Sichuan University in 1999. He received his post doctoral degree in control science and Engineering in Shanghai University in 2009. Now he is a professor and doctoral supervisor at the College of Engineering Science and Technology, Shanghai Ocean University. His main research interest is marine Internet of things engineering, Fisheries Engineering and automation technology research.

SUN Qing received her bachelor's degree in electrical engineering and automation from Huaiyin Institute of Technology in 2016. Now, she is a student at the College of Engineering Science and Technology, Shanghai Ocean University. Her main research is communication security and Internet of things technology.

Cao Liling received a bachelor's degree in electronic information science and technology from Central South University in 2004. She received her MS degree in physics electronics in Central South University in 2007. She received a Ph.D. degree in testing technology and automation from Tongji University In 2017. Now she is an experimental teacher of College of Engineering Science and Technology, Shanghai Ocean University. Her main research is Network security, authentication protocol.