A Smart Card-based Authentication Scheme Using User Identify Cryptography

Chin-Chen Chang[1,2] and Chia-Yin Lee[3]
(Corresponding author: Chin-Chen Chang)

Department of Information Engineering and Computer Science, Feng Chia University[1]
No. 100, Wenhwa Rd., Seatwen, Taichung 407, Taiwan
Department of Computer Science and Information Engineering, Asia University[2]
No. 500, Lioufeng Rd., Wufeng, Taichung 413, Taiwan
Information & Communication Technology Laboratories, National Chiao Tung University[3]
No. 1001, Tahsueh Rd., Hsinchu 300, Taiwan
(Email: ccc@cs.ccu.edu.tw)
(Received Nov. 12, 2012; revised and accepted Feb. 20, 2013)

Abstract

The user authentication scheme is a useful mechanism for verifying the legitimacy of a remote user over insecure network environments. Recently, smart card-based user authentication schemes have been used in a wide range of applications, such as Internet commerce, electronic mail system, and voice over Internet protocol. However, most existing authentication schemes cannot protect the privacy of the user's identity. Therefore, the dynamic ID-based user authentication scheme is proposed to overcome this drawback. In this article, we analyze some security properties for recent dynamic ID-based user authentications. In addition, we propose an enhanced authentication scheme that can withstand the possible attacks and reduce the overhead of the system implementation.

Keywords: Authentication, dynamic identity, one-way hash function, smart card

1 Introduction

With the rapid growth of computer networks, the user client can access services or download data from remote servers. The user authentication scheme has become a simple and useful mechanism for verifying the legitimacy of the user's login request. In the general solution, such as Lamport's scheme [23], users must register with the server and keep identity/password pairs for login into the server; at the same time, the server must maintain a registration table to record the password for each registered user. However, when the server must keep so much secret information, security problems can occur and increase the overhead for verifying legal users. To overcome this drawback, Hwang and Li [14] proposed a new user authentication scheme using smart cards. Due to the fact that the smart card can store the verifier securely, there is no need for the remote server to maintain the password table for registered users. Subsequent to Hwang and Li's scheme, many user authentication schemes based on smart cards have been proposed in the literature [3, 4, 5, 8, 10, 11, 13, 15, 17, 19, 20, 21, 22, 24, 25, 26, 28, 34, 36, 38, 40].

In a unidirectional authentication scheme, an entity can authenticate the other one by challenging some secret information. In addition, a mutual authentication protocol can allow two communicating parties to verify each other. As we know, there are four important security problems that an ideal user authentication scheme must solve, i.e., 1) it must determine whether users are legitimate or not; 2) the server must be authenticated; 3) a common session key can be established; and 4) the privacy of legal users must be ensured. To protect users' privacy, Das et al. [6] were the first to propose a dynamic, ID-based user authentication scheme. This scheme uses dynamic identity for each login session, thus, this scheme can reduce the threat of exposing a user's real identity. However, some researchers [1, 9, 18, 27, 29, 30, 33] have pointed out that Das et al.'s scheme might suffer from possible attacks. In 2009, Wang et al. [39] argued that Das et al.'s scheme does not provide mutual authentication and does not protect the user's password. By this security flaw, an adversary can use a random password to login into the server. To overcome this weakness, Wang et al. also proposed an improvement based on Das et al.'s scheme. Recently, Khan et al. [16] pointed out that Wang et al.'s scheme cannot protect the privacy of the user's identity and cannot construct a common session key between the user and the server. Khan et al. also proposed an enhanced version to overcome these drawbacks. In this article, we demonstrate that Wang et al.'s scheme suffers from the impersonation attack. In addition, both Wang et al.'s and Khan et al.'s schemes use the timestamp to prevent the replay attacks [37]. Actually, it is difficult to verify the timestamp when the user and the server are located in different time zones or when there is a congested network environment that has unstable latency. Therefore, additional time-synchronized mechanisms [31, 32] are needed to adjust the clock between these two parties.

Moreover, Khan et al.'s scheme uses a registration table to record the status of each registered user. This method not only resists the objective of using the smart card, but it also increases the overhead of the server to maintain the registration table. To overcome the above drawbacks, we propose a novel, user authentication scheme using a smart card. In addition, we proved the correctness of our scheme by using logical rules, and we demonstrated that our scheme can withstand possible attacks.

The rest of this article is organized as follows. In Section 2, we review Wang et al.'s scheme briefly. In Section 3, we demonstrate that Wang et al.'s scheme suffers from impersonation attacks. In addition, we discuss some drawbacks of related works. In Section 4, we propose an enhanced, dynamic ID-based user authentication scheme based on random nonces and one-way hash functions [35]. We present our analysis of the proposed scheme and compare the security properties with related works in Section 5. Some conclusions are summarized in Section 6.

2 Review of Wang et al.'s Scheme

In this section, we review Wang et al.'s scheme briefly. Their scheme is composed of four phases, i.e., the registration phase, the login phase, the verification phase, and the password change phase. The detailed processes of each phase are described below.

Registration phase

When the user U_i wants to register with the remote server *S*, U_i must choose an identity id_i and send the identity to *S* in a secure channel. After receiving the registration request, the server *S* performs the following processes.

1) Compute $N_i = h(pw_i) \oplus h(x) \oplus id_i$, where *x* is the secret key of S, and pw_i is the password of U_i, assigned by S.
2) S issues a smart card and then stores the parameters $h(\cdot)$, N_i, and *y* into the smart card. Note that the parameter *y* is the secret code of *S*, shared with each registered user.
3) Deliver the smart card with corresponding password pw_i to U_i through a secure channel.

Login phase

When the user U_i wants to login into the server *S*, U_i inserts the smart card to the terminal device and keys in the identity id_i and the corresponding password pw_i. Afterward, the smart card performs the following processes.

1) Computes the dynamic identity CID_i as $CID_i = h(pw_i) \oplus h(N_i \oplus y \oplus T) \oplus id_i$, where T is the current timestamp.
2) U_i sends the login message $m_1 = \{id_i,\ CID_i,\ N_i,\ T\}$ to the remote server *S* for verification.

Verification phase

Upon receiving the message $m_1 = \{id_i,\ CID_i,\ N_i,\ T\}$, the server *S* performs the following processes.

1) Verify the timestamp by checking whether $T' - T \overset{?}{\leq} \Delta T$, where T' is current timestamp. If the result holds, *S* accepts the login request of U_i; otherwise, the login request will be terminated.
2) Compute $h(pw_i)^* = CID_i \oplus h(N_i \oplus y \oplus T) \oplus id_i$.
3) Compute id_i^* as $id_i^* = N_i \oplus h(x) \oplus h(pw_i)^*$ and verify whether it is equal to the received id_i. If the result is correct, *S* accepts the login request; otherwise, the login request is refused.
4) Compute $a' = h(h(pw_i)^* \oplus y \oplus T')$ and then send the message $m_2 = \{a',\ T'\}$ to the user U_i.

Upon receiving the response message $m_2 = \{a',\ T'\}$ from S at time T'', U_i checks the validity of timestamp $T'' - T' \overset{?}{\leq} \Delta T$; if the timestamp is valid, U_i computes $a = h(h(pw_i) \oplus y \oplus T')$ and then compares it with the received a'. If the result is equivalent, it means that the server *S* is authenticated.

Password change phase

When the user U_i wants to change the current password, U_i inserts the smart card to the terminal device and keys in the current password pw_i; next, U_i requests to change the password to a new one, i.e., pw_i'. The smart card computes $N_i' = N_i \oplus h(pw_i) \oplus h(pw_i')$ and replaces the original parameter N_i stored in the smart card with the new parameter N_i'.

3 Comments on Related Works

First of all, we point out that Wang et al.'s scheme might suffer from the impersonation attack. Then, we discuss some drawbacks of related works.

3.1 Weaknesses of Wang et al.'s Scheme

We consider a scenario when an attacker U_A wants to use an intended identity id_A to login into the server *S*. Suppose that U_A has collected previous login messages transmitted between a legal user U_i and the server *S*. Therefore, U_A can obtain the login parameters id_i, CID_i, and N_i and the past timestamp T. Afterward, the attacker can masquerade as a legal user to cheat the server as shown below:

1) U_A forges the login parameters id_A, CID_A, and N_A such as $id_A = id_i \oplus T \oplus T_A$, $CID_A = CID_i \oplus T \oplus T_A$, and $N_A = N_i \oplus T \oplus T_A$, where T_A is the current timestamp.
2) U_A sends the login message $\{id_A, CID_A, N_A, T_A\}$ to S for verification.

Upon receiving the message $\{id_A, CID_A, N_A, T_A\}$ at time T^*, the server S verifies the user by the following processes:

1) Check whether $T^* - T_A \overset{?}{\le} \Delta T$; actually, the result holds since the timestamp T_A is correct.
2) S computes the term $h(pw_A)^*$ as $h(pw_A)^* = CID_A \oplus h(N_A \oplus y \oplus T_A) \oplus id_A$. Note that $h(pw_A)^*$ can be written as:

$$h(pw_A)^* = CID_i \oplus T \oplus T_A \oplus h(N_i \oplus T \oplus T_A \oplus y \oplus T_A) \oplus id_i \oplus T \oplus T_A = CID_i \oplus h(N_i \oplus y \oplus T) \oplus id_i.$$

3) S computes id_A^* as $id_A^* = N_A \oplus h(x) \oplus h(pw_A)^*$ and verifies whether id_A^* is equal to the received id_A. If $id_A^* = id_A$, the server S will validate that U_A is a legal user.

We show that the term id_A^* in 3) is equal to id_A as follows:

$$\begin{aligned} id_A^* &= N_i \oplus T \oplus T_A \oplus h(x) \oplus CID_i \oplus h(N_i \oplus y \oplus T) \oplus id_i \\ &= h(pw_i) \oplus h(x) \oplus id_i \oplus T \oplus T_A \oplus h(x) \oplus h(pw_i) \oplus h(N_i \oplus y \oplus T) \oplus id_i \oplus \\ &\quad h(N_i \oplus y \oplus T) \oplus id_i \\ &= id_i \oplus T \oplus T_A \\ &= id_A. \end{aligned}$$

From the above derivative result, we demonstrate that Wang et al.'s scheme suffers from the impersonation attack. On the other hand, Wang et al.'s scheme does not preserve the feature of anonymity for users, since the users must send their real identities to the server for authentication. Therefore, this scheme loses the property of dynamic identity.

3.2 Some Drawbacks of Related Works

In order to provide the feature of anonymity and provide session key establishment, Khan et al. proposed an improved version of Wang et al.'s scheme. Khan et al.'s scheme has many attractive features, such as user anonymity, session key establishment, and lost smart card revocation. However, the remote server must maintain a registration table to record the status of each registered user. This table may increase the system overhead on the server side. In other words, it will spend much time to recognize the legal user when the table stores tens of thousands of records. On the other hand, both Wang et al.'s and Khan et al.'s schemes use the timestamp to withstand the replay attacks. As we know, it is difficult to verify the timestamp when participants are located in different time zones or when there is a congested network environment that has variant delay time. Thus, additional time-synchronized mechanisms are needed to adjust the clock between the client and the server.

In this article, we propose an improvement to enhance the security and performance of Wang et al.'s and Khan et al.'s schemes. Our scheme not only can achieve all security requirements presented in related works, but it can do so without using any time-synchronized mechanism. The detailed processes of our scheme are described in the next section.

4 Proposed Scheme

In this section, we propose an enhanced, dynamic ID-based user authentication scheme without timestamps. Our scheme consists of four phases, i.e., the registration phase, the authentication phase, the password change phase, and the lost card revocation phase.

Registration phase

First of all, the user U_i selects a fixed length id_i and corresponding pw_i to be her/his identity and password, respectively. Next, U_i submits id_i and pw_i to the server S for registration. Suppose that x and y are two secret keys of S; then, S executes the following steps:

1) Select a 128-bit sized integer r_i randomly.
2) Compute $R_1 = h(id_i \| x \| r_i)$, where $h(\cdot)$ is a collision-resistant, one-way hash function, such as SHA [42].
3) Compute $R_2 = g^{xy} \bmod p$, where g is a primitive element in Z_p^*, and p is a large prime number.
4) Compute $R_3 = h(id_i \| R_2) \oplus h(pw_i)$.
5) Issue a smart card with a 32-bit sized serial number sn_i, where sn_i has a specific format.
6) Combine the identity of the user U_i with the serial number of the smart card as $SID_i = (id_i \| sn_i)$, where the symbol $\|$ denotes the concatenation operation.
7) Finally, store R_1, R_2, R_3, SID_i and $h(\cdot)$ on the smart card and, then, deliver the smart card to the user U_i.

All processes of the registration phase must be conducted in a secure manner. The registration phase is illustrated in Figure 1.

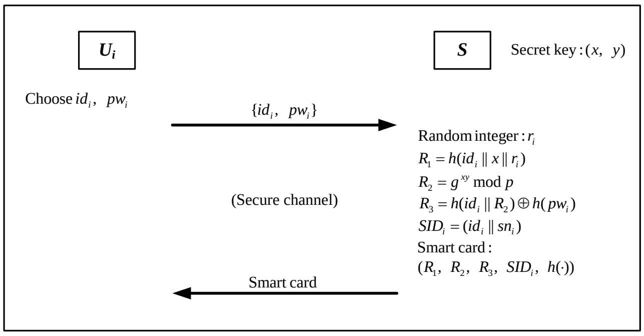

Figure 1: The registration phase of the proposed scheme

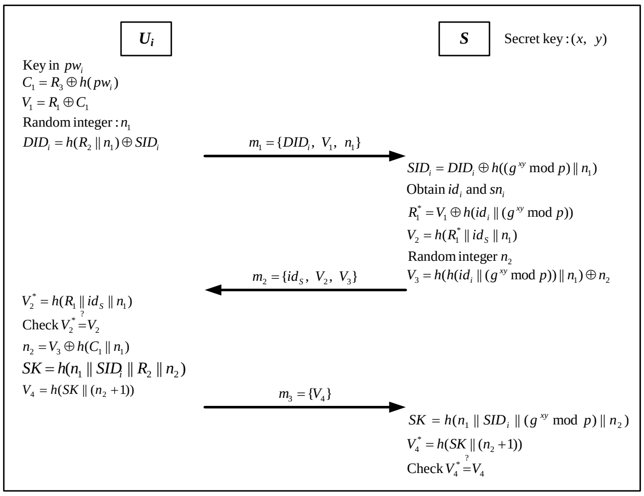

Figure 2: The authentication phase of the proposed scheme

Authentication phase

We assume that a mobile user U_i requests to access the server *S*. Before providing services, *S* must authenticate the legitimacy of U_i. For authentication, U_i inserts the smart card to the terminal device and then inputs her/his password pw_i. Afterward, the smart card performs the following steps:

1) Compute $C_1 = R_3 \oplus h(pw_i)$.

2) Compute $V_1 = R_1 \oplus C_1$.

3) Generate a 160-bit sized integer n_1 randomly.

4) Generate a dynamic identity DID_i by computing $DID_i = h(R_2 \| n_1) \oplus SID_i$.

5) Finally, send the message $m_1 = \{DID_i,\ V_1,\ n_1\}$ to *S* for authentication.

Upon receiving the authentication request message m_1, the server *S* performs the following steps:

1) Obtain the term SID_i by computing $SID_i = DID_i \oplus h((g^{xy} \bmod p) \| n_1)$.

2) Retrieve the identity id_i and the serial number sn_i from the term SID_i and then check the format of id_i and sn_i.

Note that the server *S* can use the serial number sn_i to determine whether the smart card is revoked.

3) Compute $R_1^* = V_1 \oplus h(id_i \| (g^{xy} \bmod p))$.

4) Generate a 160-bit sized integer n_2 randomly.

5) Compute $V_2 = h(R_1^* \| id_s \| n_1)$ and $V_3 = h(h(id_i \| (g^{xy} \bmod p)) \| n_1) \oplus n_2$, and then send the message $m_2 = \{id_S,\ V_2,\ V_3\}$ to the user U_i.

Upon receiving the message m_2, the user U_i executes the following steps:

1) Compute $V_2^* = h(R_1 \| id_S \| n_1)$.

2) Check whether $V_2^* \overset{?}{=} V_2$. If the result holds, the server *S* is authenticated; otherwise, the connection with the server is terminated.

3) Obtain the random nonce n_2 by computing $n_2 = V_3 \oplus h(C_1 \| n_1)$.

4) Generate the session key *SK* shared with *S* by computing $SK = h(n_1 \| SID_i \| R_2 \| n_2)$.

5) Compute $V_4 = h(SK \| (n_2 + 1))$ and send the message $m_3 = \{V_4\}$ to *S*.

After receiving the message m_3, the server *S* performs the following processes:

1) Generate the session key *SK* shared with the user U_i by computing $SK = h(n_1 \| SID_i \| (g^{xy} \bmod p) \| n_2)$.

2) Compute V_4^* as $V_4^* = h(SK \| (n_2 + 1))$ and check whether $V_4^* \overset{?}{=} V_4$. If they are equivalent, the user U_i is authenticated, and the session key *SK* shared with U_i is authenticated. After that, the server *S* can provide service or send messages securely by using the session key *SK* to encrypt the content.

The authentication processes between the user U_i and the server *S* are illustrated in Figure 2.

Note: To prevent on-line password guessing attacks, if the verifying result of the equation $V_4^* \overset{?}{=} V_4$ is invalid more than three times continuously for the same id_i, the server *S* will revoke the smart card with the serial number sn_i.

Password change phase

When the user U_i wants to change the current password pw_i to a new password pw_i', U_i must insert the smart card to the terminal device and key in the identity id_i with corresponding password pw_i. Then, the smart card will perform the following processes without interacting with the server *S*.

1) Compute $Q_1 = h(id_i \| R_2)$ and $Q_1^* = R_3 \oplus h(pw_i)$.

2) Compare Q_1 with Q_1^*; if $Q_1 = Q_1^*$, U_i is allowed to change the password. Otherwise, the password change procedure is terminated.

3) Compute the new term R_3' as $R_3' = h(id_i \| R_2) \oplus h(pw_i) \oplus h(pw_i) \oplus h(pw_i')$ and replace the original R_3 with the new R_3'.

Lost card revocation phase

When the user U_i loses her/his smart card, U_i must notify the server S to revoke the smart card. When receiving the revocation request, S first validates the U_i by checking her/his secret personal information. All procedures in this phase are executed through a secure channel. After validating the revocation request, S records the serial number sn_i of the revoked smart card in the database and issues a new smart card with new serial number sn_i' for U_i. Afterward, U_i can choose a new password for the new smart card by executing the procedure similar to the registration phase.

5 Security Analysis

In 1990, Burrows et al. [2] proposed useful logical rules to prove the validity of authentication protocols. We used the BAN logic proposed by Burrows et al. to analyze the authentication procedures of the proposed scheme. Then, we show that our scheme can withstand some possible attacks.

5.1 Authentication Proof based on BAN Logic

We used BAN logic to verify that our user identification protocol can achieve mutual authentication. The main goal of our protocol is to establish a common session key *SK* between the user U_i and the remote server *S*. We used the following logical postulates to show that U_i and S can mutually authenticate and share a session key *SK*.

U_i **believes** id_S,

S **believes** id_i,

U_i **believes** S **believes** $U_i \overset{SK}{\leftrightarrow} S$,

U_i **believes** $U_i \overset{SK}{\leftrightarrow} S$,

S **believes** U_i **believes** $U_i \overset{SK}{\leftrightarrow} S$, and

S **believes** $U \overset{SK}{\leftrightarrow} S$.

According to the analytical procedures of BAN logic, each round of the protocol must be transformed into an idealized form. First, we illustrate some notations of BAN logic as follows.

(X, Y): formula X or formula Y is one part of formula (X, Y).

$< X >_S$: formula *X* combined with a secret parameter *S*.

$\{X\}_K$: formula *X* encrypted by the secret key *K*.

$P \overset{K}{\leftrightarrow} Q$: *P* and *Q* may use the shared key *K* to communicate. Note that *K* will never be discovered by anyone except P and *Q*.

$P \overset{S}{\Leftrightarrow} Q$: The secret formula *S* is known only to *P* and *Q*. Only *P* and *Q* can use *S* to prove their identities to each other.

We use BAN logic to transform our protocol, illustrated in Figure 2, into the idealized form. We show the messages in idealized form as follows:

m_1. $U_i \rightarrow S: \{SID_i, n_1\}_{R_2}$.

m_2. $S \rightarrow U_i$:

$< id_S, n_1 >_{R_1}, \{S \overset{n_2}{\Leftrightarrow} U_i, n_1\}_{h(id_i \| R_2)}, \{S \overset{SK}{\leftrightarrow} U_i, n_1\}_{n_2}$.

m_3. $U_i \rightarrow S: \{U_i \overset{SID_i}{\leftrightarrow} S, n_2\}_{R_2}, \{S \overset{SK}{\leftrightarrow} U_i, n_2\}_{SID_i}$.

Since the server S shares secrets, such as $R_1 = h(id_i \| x \| r_i)$, $R_2 = g^{xy} \bmod p$, and $h(id_i \| R_2)$, with the user U_i via the smart card, we can make some assumptions without loss of generality as follows:

*A*1. U_i **believes fresh** n_1.

*A*2. *S* **believes fresh** n_2.

*A*3. U_i **believes** $U_i \overset{R_1}{\Leftrightarrow} S$.

*A*4. U_i **believes** $U_i \overset{h(id_i \| R_2)}{\leftrightarrow} S$.

*A*5. *S* **believes** $U_i \overset{R_2}{\leftrightarrow} S$.

*A*6. *S* **believes** $U_i \overset{h(id_i \| R_2)}{\leftrightarrow} S$.

*A*7. U_i **believes** (*S* **controls** id_S).

*A*8. U_i **believes** (*S* **controls** $U_i \overset{n_2}{\leftrightarrow} S$).

*A*9. U_i **believes** (*S* **controls** $U_i \overset{SK}{\leftrightarrow} S$).

*A*10. *S* **believes** (U_i **controls** $U_i \overset{SID_i}{\leftrightarrow} S$).

A11. S **believes** *(*U_i **controls** $U_i \overset{SK}{\leftrightarrow} S$*).*

Actually, assumptions *A*1 and *A*2 are basic assumptions of BAN logic. We analyzed the idealized form of the proposed authentication protocol using the assumptions above and the rules of BAN logic. We show the main steps of the proof as follows:

By m_1 and $A5$, we apply the message-meaning rule to derive

S **believes** U_i **said** $(SID_i,\ n_1)$. (Statement 1)

By m_2, we break conjunctions and produce the following:

U_i **sees** $< id_S,\ n_1 >_{R_1}$, (Statement 2)

U_i **sees** $\{S \overset{n_2}{\Leftrightarrow} U_i,\ n_1\}_{h(id_i || R_2)}$, (Statement 3)

and

U_i **sees** $\{S \overset{SK}{\leftrightarrow} U_i,\ n_1\}_{n_2}$. (Statement 4)

By $A3$ and Statement 2, we apply the message-meaning rule to derive

U_i **believes** S **said** $(id_S,\ n_1)$. (Statement 5)

By $A1$ and Statement 5, we apply the nonce-verification rule to deduce

U_i **believes** S **believes** $(id_S,\ n_1)$. (Statement 6)

By Statement 5, we break the conjunction to obtain

U_i **believes** S **believes** id_S. (Statement 7)

By $A7$ and Statement 7, we apply the jurisdiction rule to obtain

U_i **believes** id_S. (Statement 8)

By $A4$ and Statement 3, we apply the message-meaning rule to derive

U_i **believes** S **said** $(S \overset{n_2}{\Leftrightarrow} U_i,\ n_1)$. (Statement 9)

By $A1$ and Statement 9, we apply the nonce-verification rule to deduce

U_i **believes** S **believes** $(S \overset{n_2}{\Leftrightarrow} U_i,\ n_1)$. (Statement 10)

By Statement 10, we break the conjunction to derive

U_i **believes** S **believes** $S \overset{n_2}{\Leftrightarrow} U_i$. (Statement 11)

By $A8$ and Statement 11, we apply the *jurisdiction* rule to obtain

U_i **believes** $S \overset{n_2}{\Leftrightarrow} U_i$. (Statement 12)

By Statement 4 and Statement 12, we apply the *message-meaning* rule to derive

U_i **believes** S **said** $(U_i \overset{SK}{\leftrightarrow} S,\ n_1)$. (Statement 13)

By $A1$ and Statement 13, we apply the *nonce-verification* rule to deduce

U_i **believes** S **believes** $(U_i \overset{SK}{\leftrightarrow} S,\ n_1)$. (Statement 14)

By Statement 14, we break the conjunction to derive

U_i **believes** S **believes** $(U_i \overset{SK}{\leftrightarrow} S)$. (Statement 15)

By $A9$ and Statement 15, we apply the *jurisdiction* rule to obtain

U_i **believes** $S \overset{SK}{\leftrightarrow} U_i$. (Statement 16)

By m_3, we break conjunctions and produce the following:

S **sees** $\{U_i \overset{SID_i}{\leftrightarrow} S,\ n_2\}_{R_2}$, (Statement 17)

and

S **sees** $\{S \overset{SK}{\leftrightarrow} U_i,\ n_2\}_{SID_i}$. (Statement 18)

By $A5$ and Statement 17, we apply the *message-meaning* rule to derive

S **believes** U_i **said** $(U_i \overset{SID_i}{\leftrightarrow} S,\ n_2)$. (Statement 19)

By $A2$ and Statement 19, we apply *nonce-verification* rule to deduce

S **believes** U_i **believes** $(U_i \overset{SID_i}{\leftrightarrow} S,\ n_2)$. (Statement 20)

By Statement 20, we break the conjunction to obtain

S **believes** U_i **believes** $U_i \overset{SID_i}{\leftrightarrow} S$. (Statement 21)

By $A10$ and Statement 21, we apply the jurisdiction rule to deduce

S **believes** $U_i \overset{SID_i}{\leftrightarrow} S$. (Statement 22)

According to the equation $SID_i = (id_i \parallel sn_i)$, we can derive

S **believes** id_i. (Statement 23)

By Statement 18 and Statement 22, we apply the *message-meaning* rule to obtain

S **believes** U_i **said** $(S \overset{SK}{\leftrightarrow} U_i,\ n_2)$. (Statement 24)

By $A2$ and Statement 24, we apply *nonce-verification* rule to deduce

S **believes** U_i **believes** $(S \overset{SK}{\leftrightarrow} U_i,\ n_2)$. (Statement 25)

By Statement 25, we break the conjunction to obtain

S **believes** U_i **believes** $U_i \overset{SK}{\leftrightarrow} S$. (Statement 26)

By $A11$ and Statement 26, we apply the jurisdiction rule to derive

S **believes** $U_i \overset{SK}{\leftrightarrow} S$. (Statement 27)

Based on Statement 15, Statement 16, Statement 26, and Statement 27, we prove that the proposed protocol establishes an authenticated session key SK between the user U_i and the server S. Due to the aforementioned results of Statement 8 and Statement 23, we also prove that U_i and S are able to authenticate each other using our protocol.

5.2 Withstand Possible Attacks

In order to prove that the proposed scheme can withstand possible attacks, some basic security assumptions are given as follows:

Table 1: Comparison of security properties among related works

Items	Das et al.'s [6]	Wang et al.'s [39]	Khan et al.'s [16]	Ours
Mutual authentication	No	Yes	Yes	Yes
Password chosen by users	Yes	No	Yes	Yes
User anonymity	Yes	No	Yes	Yes
Without registration table	Yes	Yes	No	Yes
Withstand impersonation attacks	No	No	Yes	Yes
Without time-synchronized mechanisms	No	No	No	Yes
Session key establishment	No	No	Yes	Yes
Perfect forward secrecy	No*	No*	Yes	Yes

* Since Das et al.'s and Wang et al.'s schemes do not provide session key establishment, these two schemes do not provide the property of perfect forward secrecy for transmitted messages.

• **Assumption 1** *Security characteristic of smart cards*

According to the smart card standard ISO/IEC 7816-4 [41], we assume that secret data, such as R_1, R_2, R_3, and SID_i, which are stored in the smart card cannot be retrieved by any outside entity.

• **Assumption 2** *One-way hash function assumption*

Let $h(\cdot)$ be a one-way hash function; then, 1) for any input x, it is easy to compute the hash value y, where $y = h(x)$; 2) given a hash value y, it is computationally intractable to recover x satisfying the equation $y = h(x)$; 3) it is difficult to find $x_1 \neq x_2$, such that $h(x_1) = h(x_2)$.

We show that the proposed scheme can resist certain possible attacks. Assume that communications are insecure and that there exists an adversary U_A. Therefore, U_A can intercept all messages communicated between U_i and *S*. In addition, we also assume that U_A can obtain or steal legal user U_i's smart card. We discuss some scenarios as follows.

Withstand replay attacks

The adversary U_A might replay an intercepted message $m_1 = \{DID_i,\ V_1,\ n_1\}$ to the server S for authentication. Later on, S responds by sending the message $m_2 = \{id_S,\ V_2,\ V_3\}$ to U_A. Thus, U_A tries to recover the nonce n_2 from the received V_3. First, U_A must obtain the secret parameter R_3 and the correct $h(pw_i)$. However, U_A cannot obtain the secret parameter R_3 from the stolen smart card (**Assumption 1**). In addition, U_A cannot compute the correct $h(pw_i)$ since the password pw_i is unknown. Therefore, U_A cannot compute a correct $V_4 = h(h(n_1 \| id_i \| R_2 \| n_2) \| (n_2 + 1))$ to pass the authentication procedure.

Withstand impersonation attacks

The adversary U_A might intercept the messages $m_1 = \{DID_i,\ V_1,\ n_1\}$ and $m_3 = \{V_4\}$ transmitted from legal user U_i in the previous sessions. U_A sends the authentication request m_1 to S and then tries to forge a message $m_3' = \{V_4'\}$ and sends m_3' to S for authentication. However, U_A has no capability to forge a valid V_4' as $V_4' = V_4^*$, since U_A cannot obtain the correct n_2. Thus, U_A cannot masquerade a legal user to cheat the server successfully.

Withstand identity disclosure attacks [12]

Assume that the adversary U_A is a legal user and that U_A wants to obtain the other legal user U_i's identity id_i from a intercepted DID_i. Due to $DID_i = h(R_2 \| n_1) \oplus (id_i \| sn_i)$, first, U_A must obtain the correct R_2. U_A might key in her/his correct password pw_A to obtain a correct DID_A from the smart card, and then U_A tries to retrieve the parameter R_2 from this DID_A. However, it will be difficult for U_A to derive R_2 as a result of the security characteristic of one-way hash functions (**Assumption 2**).

Perfect forward secrecy [7]

In the proposed scheme, the common session key *SK* between the user U_i and the server *S* is established when each authentication session is completed successfully. Afterward, U_i and *S* can use *SK* to execute encryption and decryption of subsequent messages. Due to the reason that the session key is constructed by a one-way hash function with random nonces, such as n_1 and n_2, in each session, the subsequent messages transmitted between U_i and *S* are encrypted using this session key. Suppose that the adversary U_A has the ability to capture all encrypted messages from the network. Even if the server *S*'s long-term secret key $(x,\ y)$ is exposed to the attacker, it is computationally infeasible to derive the previous encryption messages without knowing the one-time session key *SK*.

We summarize some major security properties of authentication schemes and compare our scheme with related works in Table 1. The results show that our scheme is the only one that is capable of achieving all security requirements.

6 Conclusions

In this article, we discussed some drawbacks and weaknesses of existing dynamic ID-based user authentication schemes. We also proposed an enhanced scheme to withstand possible attacks and achieve the security properties presented in related works. In addition, our scheme uses random nonces to withstand replay attacks, so it can be implemented easily without additional, time-synchronized mechanisms.

References

[1] A. K. Awashti, "Comment on a dynamic ID-based remote user authentication scheme," *Transaction on Cryptology*, vol. 1, no. 2, pp. 15-16, 2004.

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

[3] C. C. Chang and K. F. Hwang, "Some forgery attacks on a remote user authentication scheme using smart cards," *Informatics*, vol. 14, no. 3, pp. 289-294, 2003.

[4] C. C. Chang, C. Y. Lee, and Y. W. Su, "A mutual authenticated key agreement scheme over insecure networks," *Journal of Discrete Mathematical Sciences & Cryptography*, vol. 10, no. 5, pp. 603-612, 2007.

[5] H. Y. Chien, J. K. Jan, and Y. M. Tseng, "An efficient and practical solution to remote authentication: smart card," *Computers & Security*, vol. 21, no. 4, pp. 372-375, 2002.

[6] M. L. Das, A. Saxena, and V. P. Gulati, "A dynamic ID-based remote user authentication scheme," IEEE Transactions on Consumer Electronics, vol. 50, no.2, pp. 629-631, 2004.

[7] W. Diffie, P. C. van Oorschot, and M.J. Wiener, "Authentication and authenticated key exchange," *Designs, Codes and Cryptography*, vol. 2, no. 2, pp. 107-125, 1992.

[8] C. I. Fan, Y. C. Chan, and Z. K. Zhang, "Robust remote authentication scheme with smart cards," *Computers & Security*, vol. 24, no.8, pp. 619-628, 2005.

[9] Z. Gao and Y. Tu, "An improvement of dynamic ID-based remote user authentication scheme with smart cards," in *Proceedings of the 7th World Congress in Intelligent Control and Automation*, pp. 4562-4567, Chongqing, China, 2008.

[10] 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, pp. 58-60, 2011.

[11] C. L. Hsu, "Security of Chien et al.'s remote user authentication scheme using smart cards," *Computer Standards & Interfaces*, vol. 26, no.3, pp. 167-169, 2004.

[12] C. L. Hsu and Y. H. Chuang, "A novel user identification scheme with key distribution preserving user anonymity for distributed computer networks," *Information Sciences*, vol. 179, no. 4, pp. 422-429, 2009.

[13] J. Hu, H. Xiong, and Z. Chen, "Further improvement of an authentication scheme with user anonymity for wireless communications," International Journal of Network Security, vol. 14, no. 5, pp. 297-300, 2012.

[14] 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.

[15] M. K. Khan, J. Zhang, "Improving the security of 'a flexible biometrics remote user authentication scheme'," *Computer Standards & Interfaces*, vol. 29, no. 1, pp. 82-85, 2007.

[16] M. K. Khan, S. K. Kim, and K. Alghathbar, "Cryptanalysis and security enhancement of a 'more efficient & secure dynamic ID-based remote user authentication scheme'," *Computer Communications*, vol. 34, no. 3, pp. 305-309, 2011.

[17] S. K. Kim and M. G. Chung, "More secure remote user authentication scheme," *Computer Communications*, vol. 32, no. 6, pp. 1018-1021, 2009.

[18] W. C. Ku and S. T. Chang, "Impersonation attack on a dynamic ID-based remote user authentication scheme using smart cards," *IEICE Transactions on Communications*, vol. E88-B, no. 5, pp. 2165-2167, 2005.

[19] W. C. Ku, S. T. Chang, and M. H. Chiang, "Further cryptanalysis of fingerprint-based remote user authentication scheme using smartcards," *Electronics Letters*, vol. 41, no. 5, pp. 240-241, 2005.

[20] M. Kumar, "New remote user authentication scheme using smart cards," *IEEE Transactions on Consumer Electronics*, vol. 50, no. 2, pp. 597-600, 2004.

[21] M. Kumar, "A new secure remote user authentication scheme with smart cards," *International Journal of Network Security*, vol. 11, no. 2, pp. 88-93, 2010.

[22] M. Kumar, "An enhanced remote user authentication scheme with smart card", *International Journal of Network Security*, vol. 10, no. 3, pp. 175-184, 2010.

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

[24] C. C. Lee, M. S. Hwang, and W. P. Yang, "A flexible remote user authentication scheme using smart cards," *ACM Operating Systems Review*, vol. 36, no. 3, pp. 46-52, 2002.

[25] S. Lee, H. Kim, and K. Yoo, "Improved efficient remote user authentication scheme using smart cards,"

IEEE Transactions on Consumer Electronics, vol. 50, no. 2, pp. 565-567, 2004.

[26] S. Lee, H. Kim, and K. Yoo, “Improvement of Chien et al.’s remote user authentication scheme using smart cards,” *Computer Standards & Interfaces*, vol. 27, no. 2, pp. 181-183, 2005.

[27] Y. C. Lee, G. K. Chang, W. C. Kuo, and J. L. Chu, “Improvement on the dynamic ID-based remote user authentication scheme,” in *Proceedings of the 7th International Conference on Machine Learning and Cybernetics*, pp. 3283-3287, Kunming, China, 2008.

[28] K. C. Leung, L. M. Cheng, A. S. Fong, and C. K. Chan, “Cryptanalysis of a modified remote user authentication scheme using smart cards,” *IEEE Transactions on Consumer Electronics*, vol. 49, no. 4, pp. 1243-1245, 2003.

[29] J. Li and L. L. Hu, “Improved dynamic ID-based remote user authentication scheme using smart cards,” in Proceedings of the 4th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM 2008), pp. 1-4, Dalian, China, 2008.

[30] I. E. Liao, C. C. Lee, and M. S. Hwang, “Security enhancement for a dynamic ID-based remote user authentication scheme,” in *Proceedings of the International Conference on Next Generation Web Services Practices* (NWeSP ’05), pp.437-440, Seoul, Korea, 2005.

[31] D. L. Mills, “Precision synchronization of computer network clocks,” *ACM SIGCOMM Computer Communication Review*, vol. 24, no.2, pp. 28-43, 1994.

[32] D. L. Mills, “Adaptive hybrid clock discipline algorithm for the network time protocol,” *IEEE/ACM Transactions on Networking*, vol. 6, no.5, pp. 505-514, 1998.

[33] M. Misbahuddin, M. A. Ahmed, A. A. Rao, C. S. Bindu, and M. A. M. Khan, “A novel dynamic ID-based remote user authentication scheme,” in *Proceedings of 2006 Annual IEEE India Conference*, pp. 1-5, New Delhi, India, 2006.

[34] J. J. Shen, C. W. Lin, and M.S. Hwang, “A modified remote user authentication scheme using smart cards,” *IEEE Transactions on Consumer Electronics*, vol. 49, no. 2, pp. 414-416, 2003.

[35] D. R. Stinson, *Cryptography*, 2nd ed., Boca Raton, Florida: CRC Press, 2002.

[36] H. M. Sun, “An efficient remote user authentication scheme using smart cards,” *IEEE Transactions on Consumer Electronics*, vol. 46, no. 4, pp. 958-961, 2000.

[37] P. Syverson, “A taxonomy of replay attacks,” in *Proceedings of the 7th IEEE Computer Security Foundations Workshop*, pp. 131-136, Franconia, New Hampshire, USA, 1994.

[38] H. Tang, X. Liu, and L. Jiang, “A robust and efficient timestamp-based remote user authentication scheme with smart card lost attack resistance,” International Journal of Network Security, vol. 15, no. 6, pp. 360-368, 2013.

[39] Y. Y. Wang, J. Y. Kiu, F. X. Xiao, and J. Dan, “A more efficient and secure dynamic ID-based remote user authentication scheme,” *Computer Communications*, vol. 32, no. 4, pp. 583-585, 2009.

[40] E. Yoon and K. Yoo, “More efficient and secure remote user authentication scheme using smart cards,” in *Proceedings of 11th International Conference on Parallel and Distributed Systems*, vol. 2, pp. 73-77, Fukuoka, Japan, 2005.

[41] *Identification Cards--Integrated Circuit(s) Cards With Contacts--Part 4: Organization, Security and Commands for Interchange*, ISO/IEC 7816-4.

[42] *Secure Hash Standard*, U.S. Federal Information Processing Standard Publication 180-2.

Chin-Chen Chang received the B.S. degree in applied mathematics and the M.S. degree in computer and decision sciences from National Tsing Hua University, Hsinchu, Taiwan, in 1977 and 1979, respectively. He received the Ph.D. degree in computer engineering from National Chiao Tung University, Hsinchu, Taiwan, in 1982. During the years 1980-1983, Dr. Chang was on the faculty of the Department of Computer Engineering, National Chiao Tung University. From 1983 to 1989, he was on the faculty of the Institute of Applied Mathematics, National Chung Hsing University, Taichung, Taiwan. From 1989 to 2002 he was a full professor of the Department of Computer Science and Information Engineering, National Chung Cheng University, Chiayi, Taiwan. From 2002 to 2005, he was a chair professor at the same University. Since February 2005, he has been a chair professor at Feng Chia Univeristy, Taichung, Taiwan. His current research interests include database design, computer cryptography, image compression, and data structures. Dr. Chang is a fellow of IEEE.

Chia-Yin Lee received his B.S. and M.S. degrees in computer science and information engineering from Tunghai University, Taichung, Taiwan, in 2001 and 2004, respectively. He received the Ph.D. degree in computer science and information engineering from National Chung Cheng University, Chiayi, Taiwan, in 2010. Since August 2011, Dr. Lee has been a postdoctoral research fellow at Information & Communication Technology Laboratories, National Chiao Tung University, Hsinchu, Taiwan. His research interests include information security and image processing.