computers

MDPI

Article

An Improvement on Remote User Authentication Schemes Using Smart Cards

Chin-Ling Chen [1,2,*], Yong-Yuan Deng [1], Yung-Wen Tang [3], Jung-Hsuan Chen [4] and Yu-Fan Lin [1]

1 Department of Computer Science and Information Engineering, Chaoyang University of Technology, Taichung 41349, Taiwan; allen.nubi@gmail.com (Y.-Y.D.); s9827623@cyut.edu.tw(Y.-F.L)
2 School of Information Engineering, Changchun Sci-Tech University, Changchun 130600, China
3 School of Physical Therapy, Chun Shan Medical University, Taichung 40201, Taiwan; tangyw@csmu.edu.tw
4 Department of Industrial Education, National Taiwan Normal University, Taipei 10610, Taiwan; jhchen@ntnu.edu.tw
* Correspondence: clc@mail.cyut.edu.tw; Tel.: +886-4-2332-3000 (ext. 4761)

Received: 4 December 2017; Accepted: 12 January 2018; Published: 15 January 2018

Abstract: In 2010, Yeh et al. proposed two robust remote user authentication schemes using smart cards; their claims were such that their schemes defended against ID-theft attacks, reply attacks, undetectable on-line password guessing attacks, off-line password guessing attacks, user impersonation attack, server counterfeit attack and man-in-the-middle attack. In this paper, we show that Yeh et al.'s schemes are still vulnerable to ID-theft attack, off-line password guessing attacks, undetectable on-line password guessing attacks and user impersonation attack. Notably, problems remain in situations where the user lost a smart card or the malicious legal user. To remedy these flaws, this paper proposes an improvement on Yeh et al.'s remote user authentication schemes using smart cards.

Keywords: authentication; cryptanalysis; security; smart card

1. Introduction

With the rapid growth of network technologies, it is extremely important to pay close attention to any developing security concerns. As such, password-based authentication has become one of the best practically applied techniques used to problem-solve regarding various applications in wireless environments and other remote authentication systems. In 1981, Lamport [1] proposed the first password-based remote authentication scheme for identifying a legal user using a hash-chain technique through insecure communication. In our scheme, all secret passwords are stored in a verifier's table that is maintained by the remote server; in a situation such as this, there exists a potential threat such that all maintained records might be modified by attackers. In order to solve these problems, numerous undertakings in research [2–29] have been executed during recent years.

In 1990, Hwang et al. [12] proposed a non-interactive password authentication scheme without password tables using smart cards. Follow up research [3,6,16,18,23,24,30–39] has also been proposed. Because these schemes suffered from a susceptibility to ID-theft attack, an attacker could forge a legal user using an eavesdropped users' identity documentation. Das et al. [6] proposed a dynamic ID-based remote user authentication scheme that has significant advantages; most notably, the remote server does not need to maintain a verifier's table. However, in 2009, Wang et al. [25] pointed out that Das et al.'s scheme still exhibited several weaknesses. For example, it is susceptible to server counterfeit attack and provides poor password authentication. In the same year, Hsiang and Shih [11] proposed a remote user authentication scheme using smart cards claiming that their scheme provided many security features, such as: mutual authentication, the ability to freely change passwords and protection from masquerade attack.

Next, Yeh et al. [27] proposed two robust remote user authentication schemes using smart cards. Their schemes illustrated how Wang et al.'s scheme and Hsiang and Shih's scheme were still susceptible to masquerade attack, off-line password guessing attacks and undetectable on-line password guessing attacks. Thus, Yeh et al. proposed two schemes to remedy these weaknesses that were more efficient than both Wang et al.'s scheme and Hsiang and Shih's scheme. Nevertheless, according to our cryptanalysis, Yeh et al.'s schemes still have notable weaknesses to ID-theft attack, off-line password guessing attacks, undetectable on-line password guessing attacks and user impersonation attack. Moreover, the smart-card-based schemes [6,9,11,19,25,28] suffered in contexts involving a lost smart card. In fact, some researches [15,21] reveal the stored parameters of smart card. Therefore, we propose an improved scheme to overcome all of the security weaknesses mentioned above.

The security requirements of a remote user authentication scheme based on smart cards are listed as follows:

- Mutual authentication

In the information transmission process, the message receiver must be able to verify the identity legitimacy of the sender. Thus, each party must be able to verify the identity legitimacy of the other parties in a remote user authentication environment. If the two parties have confirmed each other's identities, then mutual authentication is achieved.

- Lost smart card

If the user's smart card is stolen by an attacker, the attacker may use the smart card for future malicious communications, or use it to obtain previous messages. A secure remote user authentication environment should avoid these situations, when the smart card is stolen by an attacker.

- ID-theft attack

Malicious attacks may also attempt to get a person's identification by tracing their transmitted messages. Thus, a secure remote user authentication scheme must prevent such ID-theft attack.

- Server counterfeit attack and user impersonation attack

Any information transferred in an unencrypted network environment is vulnerable to malicious attack in the form of modification, where the message delivered to the receiver is not the original message transmitted by the sender. The attacker may pretend a legal server or a legal user. The legality of the transmitted parties must therefore be ensured and protected against tampering in transit.

- Replay attacks

Malicious attacks may also intercept the transmitted message between the user and the server and then impersonate a legitimate transmitter in order to send the same message to the intended receiver. This constitutes a serious breach of personal data security and must be prevented by a secure remote user authentication environment.

The rest of this paper is organized as follows. Section 2 provides a brief review of the weakness of Yeh et al.'s schemes. Section 3 provides details of the proposed scheme. Section 4 provides a security analysis of our scheme. Section 5 shows a security and performance comparison with related research. We provide conclusions in the last section.

2. Cryptanalysis of Yeh et al.'s Schemes

2.1. Review of Yeh et al.'s Timestamp Based Scheme

In this subsection, we briefly describe Yeh et al.'s timestamp based scheme [27], which consists of four phases: the registration phase, the login phase, the authentication phase and the password-change phase. The overview is described in Figure 1 and the notation of this scheme is listed as follows:

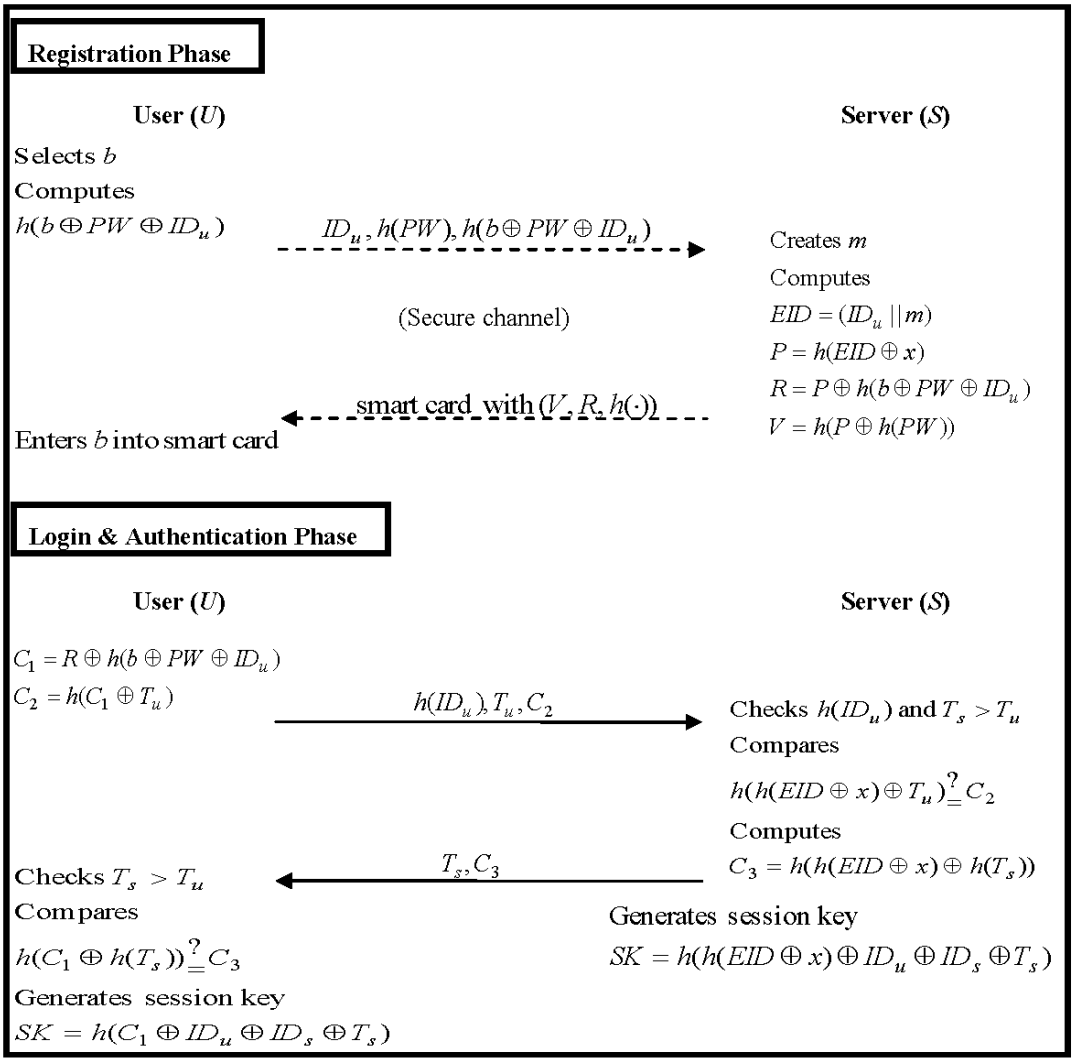

Figure 1. Overview of Yeh et al.'s first scheme. U: the user; S: the remote server; T_u, T_s: the timestamps generated by user and remote server respectively; ID_X: the identity of X; PW: the user's password; x: the permanent secret key of remote server; m: the times of registration; the initial value is $m = 0$; b, r: random numbers; n, N_u, N_s: nonces; $h(\cdot)$: a one-way hash function; $\oplus$: bitwise exclusion operation; $||$: concatenation operation; $A \stackrel{?}{=} B$: determine whether A is equal to B.

2.1.1. Registration Phase

In this phase, U initially registers, or re-registers, to S and the steps are described as follows:

1. U selects a random number b and computes $h(b \oplus PW \oplus ID_u)$. He or she then securely send ID_u, $h(PW)$ and $h(b \oplus PW \oplus ID_u)$ to S.
2. S creates a new entry with a value $m = 0$ for U in the database or sets $m = m + 1$ in the existing entry. Here, m denotes the number of times of re-registering to S for each user U. Next, S computes EID, P, R and V:

$$EID = (ID_u||m) \tag{1}$$

$$P = h(EID \oplus x) \tag{2}$$

$$R = P \oplus h(b \oplus PW \oplus ID_u) \tag{3}$$

$$V = h(P \oplus h(PW)) \tag{4}$$

Then, S securely issues a smart card containing V, R, $h(\cdot)$ to U.

3. Finally, U enters a random number b into his or her smart card.

2.1.2. Login Phase

When U wants to login S, the following steps will be performed:

1. U inserts his or her smart card into the card reader and then enters the ID_u and PW.
2. U's smart card computes C_1, C_2 and sends the authentication request messages ($h(ID_u)$, T_u, C_2) to S:

$$C_1 = R \oplus h(b \oplus PW \oplus ID_u) \tag{5}$$

$$C_2 = h(C_1 \oplus T_u) \tag{6}$$

2.1.3. Authentication Phase

Upon receiving the request messages ($h(ID_u)$, T_u, C_2), the remote server S and the smart card perform the following steps:

1. S first checks the validity of $h(ID_u)$ and $T_s > T_u$. If it does not hold, S rejects U's login request; otherwise, S computes $h(h(EID \oplus x) \oplus T_u)$ and compares it with C_2:

$$h(h(EID \oplus x) \oplus T_u) \stackrel{?}{=} C_2 \tag{7}$$

If the Equation (7) holds, S accepts U's login request and computes C_3:

$$C_3 = h(h(EID \oplus x) \oplus h(T_s)) \tag{8}$$

otherwise, S rejects it. Continuously, S sends the response messages (T_s, C_3) to U and generates a session key SK for later secure communication:

$$SK = h(h(EID \oplus x) \oplus ID_u \oplus ID_s \oplus T_s) \tag{9}$$

2. According the received messages (T_s, C_3), U's smart card checks the validity of $T_s > T_u$. If it does not hold, U terminates the session; otherwise, U computes $h(C_1 \oplus h(T_s))$ and compares it with C_3:

$$h(C_1 \oplus h(T_s)) \stackrel{?}{=} C_3 \tag{10}$$

If the Equation (10) holds, U successfully authenticates S. Finally, U computes the same session key SK:

$$SK = h(C_1 \oplus ID_u \oplus ID_s \oplus T_s) \tag{11}$$

and then, U and S can use the session key SK to securely communicate with each other.

2.1.4. Password Change Phase

In this phase, U intends to exchange his or her password PW with a new one PW_{new}. The steps are described as follows:

1. U inserts his or her smart card into the card reader, enters ID_u and PW and then requests a password change.
2. U's smart card computes P^*, V^* and compares V^* with the stored V:

$$P^* = R \oplus h(b \oplus PW \oplus ID_u) \tag{12}$$

$$V^* = h(P^* \oplus h(PW)) \tag{13}$$

$$V^* \stackrel{?}{=} V \tag{14}$$

If Equation (14) does not hold, the smart card rejects the request; if the number of login failures exceeds a predefined value, the smart card is locked immediately to prevent exhaustive password guessing attacks; otherwise, U inputs the new password PW_{new}. Afterward, U's smart card computes R_{new} and V_{new} as follows:

$$R_{new} = P * \oplus h(b \oplus PW_{new} \oplus ID_u) \tag{15}$$

$$V_{new} = h(P * \oplus h(PW)) \tag{16}$$

then, replaces R, V with R_{new}, V_{new}, respectively.

2.2. Weakness of Yeh et al.'s Timestamp Based Scheme

Although Yeh et al.'s timestamp based scheme was an improved version of Hsiang-Shih's scheme [11], several security weaknesses still exist. These susceptibilities include: ID-theft attack, off-line password guessing attacks and undetectable on-line password guessing. We describe these attacks as follows.

2.2.1. ID-Theft Attack

In the login phase, an attacker A can intercept the login messages ($h(ID_u)$, T_u, C_2) to compute the user's identity ID_u as follows:

1. A guesses an identity ID_A, computes a hashed value $h(ID_A)$ and compares it with the intercepted $h(ID_u)$.
2. If the guessed hashed value is equal to $h(ID_u)$, this indicates that A guessed the correct identity (i.e., $h(ID_A) = h(ID_u)$); otherwise, A retries Steps 1 and 2.

Therefore, A can easily obtain U's identity; the relevant details will be discussed in the next subsection.

2.2.2. Off-Line Password Guessing Attacks

This involves a situation where a user's smart card was stolen by an attacker A and where A uses the stolen smart card to extract the secret parameters b and R [15,21]. Continuously, A can use the previously eavesdropped messages ($h(ID_u)$, T_u, C_2) or (T_s, C_3) to obtain U's password PW according to the following steps:

1. Following Section 2.2.1, the attacker A can obtain the real identity of U. Afterward, A guesses a password PW_A.
2. A computes counterfeit messages C_{A1} and C_{A2} for comparison with the intercepted messages C_2 or C_3, as follows:

$$C_{A1} = h(R \oplus (b \oplus PW_A \oplus ID_u) \oplus T_u) \tag{17}$$

$$C_{A1} \stackrel{?}{=} C_2 \tag{18}$$

or

$$C_{A2} = h(R \oplus (b \oplus PW_A \oplus ID_u) \oplus h(T_s)) \tag{19}$$

$$C_{A2} \stackrel{?}{=} C_3 \tag{20}$$

3. Since ID_u is revealed following Section 2.2.1, A can guess the correct ID_u and PW to change the user's password. Refer to the password change phase of Section 2.1.4.

2.2.3. On-line Password Guessing Attacks

This refers to Section 2.2.2, where an attacker A is able to extract the secret parameters b and R through the stolen smart card. As with the previously eavesdropped messages ($h(ID_u)$, T_u, C_2), A can guess the U's password as follows:

1. A guesses a possible password PW_A and computes a value following Equation (17) C_{A1} with a timestamp T_A. A then computes counterfeit messages ($h(ID_A)$, T_A, C_{A1}) to send to the server S.
2. After receiving the messages, S first checks the timestamp $T_s > T_u$. Continuously, S computes $h(h(EID \oplus x) \oplus T_A)$ to compare the received value C_{A1}. If both of them are equal, then PW_A is U's correct password.
3. Then, S accepts this login request and sends the messages (T_s, C_3) to A.
4. According to the received messages, A can recognize that the correct password has been guessed; otherwise, A retries the above attack procedures until obtaining the correct password.

2.3. Review of Yeh et al.'s Nonce Based Scheme

Yeh et al.'s nonce based scheme [27] consists of four phases: the registration phase, the login phase, the authentication phase and the password change phase. The overview is described in Figure 2.

2.3.1. Registration Phase

When a user U wants to register to the remote server S, he or she has to perform the following steps:

1. The user U first selects a password PW and a random number r. Then, U submits ID_u, $h(PW)$ to the remote server S through a secure channel.
2. When receiving the registration request messages from U, S first computes a hash value $h(r||x)$. With $h(r||x)$, ID_u and $h(PW)$, S computes N and Y:

$$N = h(r||x) \oplus h(PW) \tag{21}$$

$$Y = h(ID||h(r||x)) \tag{22}$$

Next, S initializes the smart card with r, N, Y, $h(\cdot)$ and sends it to U via a secure channel.

2.3.2. Login Phase

When U intends to login S, he or she first insert his or her own smart card into a card reader or the terminal. Next, U enters his or her identity ID_u and password PW. The smart card then performs the following steps:

1. First, the smart card uses PW and N to derive the value $h(r||x)$. Next, the smart card computes Y':

$$h(r||x)' = N \oplus h(PW) \tag{23}$$

$$Y' = h(ID_u||h(r||x)') \tag{24}$$

and compares Y' with the stored Y; otherwise, the login request is rejected.
2. Second, the smart card generates a nonce n and computes K, L and CID:

$$K = h(r||x)' \oplus n \tag{25}$$

$$L = ID_u \oplus h(h(r||x)'||n) \tag{26}$$

$$CID = h(ID_u||n) \tag{27}$$

3. Third, the smart card sends login request messages (r, K, L, CID) to S.

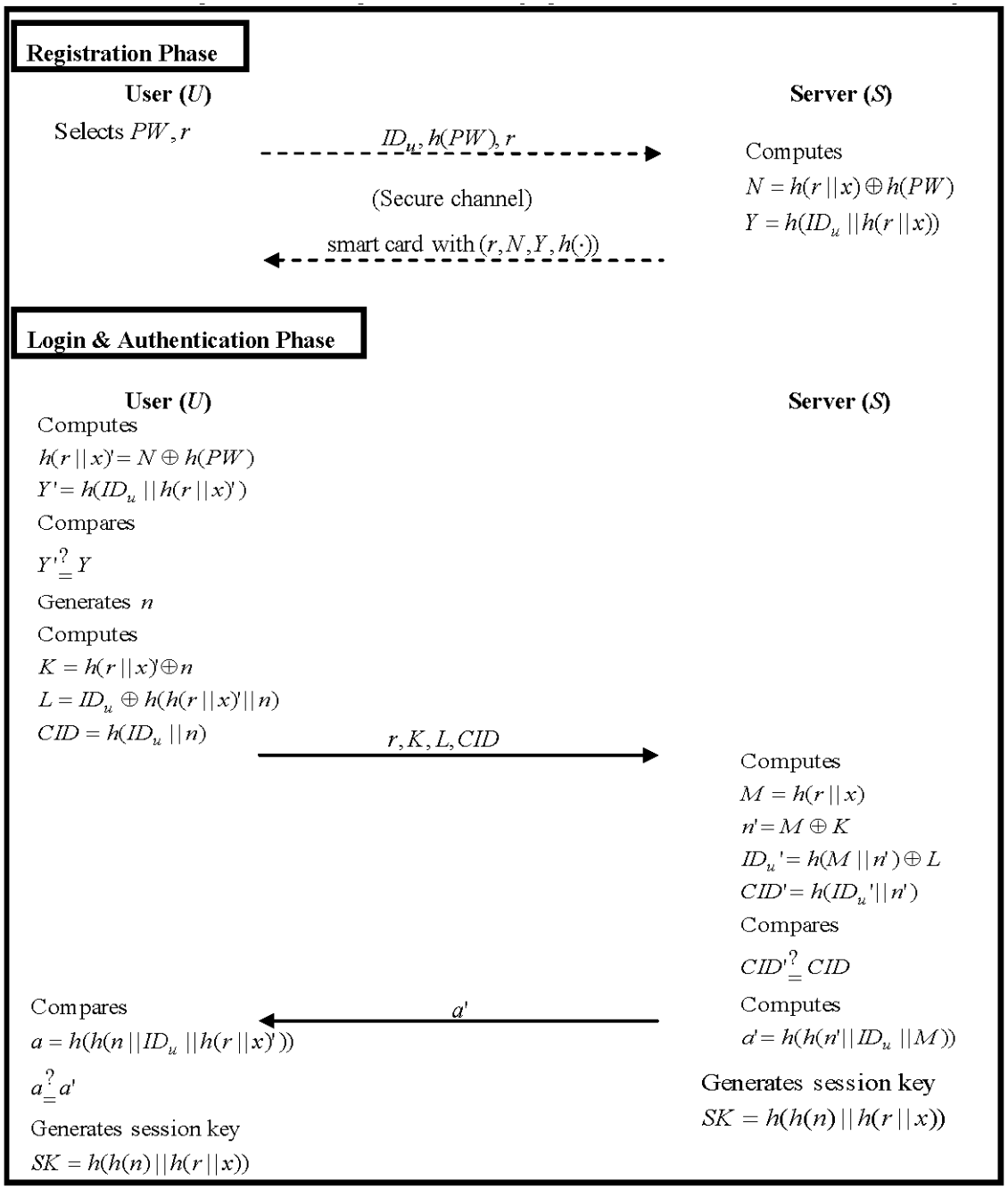

Figure 2. Overview of Yeh et al.'s second scheme.

2.3.3. Authentication Phase

After receiving the messages (r, K, L, CID), S performs the following steps to authenticate U:

1. S uses the received value r and its secret x to compute the hashed value M:

$$M = h(r||x) \tag{28}$$

Next, S computes n', ID_u' and CID':

$$n' = M \oplus K \tag{29}$$

$$ID_u' = h(M||n') \oplus L \tag{30}$$

$$CID' = h(ID_u||n') \tag{31}$$

After that, S checks whether CID' is equal to CID or not. If it holds, S confirms that U is valid and replies a message a' to U:

$$a' = h(h(n||ID_u||M)) \tag{32}$$

otherwise, S rejects the login request.

2. Upon receiving message a', U first calculates value a:

$$a = h(h(n||ID_u||h(r||x)') \tag{33}$$

and compares it with the received value a'. If both of these two values are identical, U confirms that S is valid. Since they already possess the current secret values $h(r||x)$ and n, the session key SK will be securely agreed upon by S and U:

$$SK = h(h(n)||h(r||x)) \tag{34}$$

2.3.4. Password Change Phase

If U wants to change his or her password, the procedures are as follows:

1. U first inserts his or her smart card into a card reader or the terminal and keys in the identity ID_u and the original password PW.
2. Next, according to Equations (23) and (24), the smart card examines the validity of ID_u and PW and checks to see if $Y' = Y$. If the verification holds, U is allowed to enter a new password PW_{new}; otherwise, the smart card rejects the password change request.
3. Finally, the smart card calculates N':

$$N' = N \oplus h(PW) \oplus h(PW_{new}) = h(r||x) \oplus h(PW_{new}) \tag{35}$$

and replaces the old value N with the new one N'. Now, the password has been successfully changed without the participation of S.

2.4. Weakness of Yeh et al.'s Nonce Based Scheme

Within Yeh et al.'s nonce based scheme, a security flaw has presented. We will now describe the details of the weakness.

User Impersonation Attack

In this subsection, we assume that an attacker A, who is a malicious legal user, can use his or her smart card to extract their own secret parameters r, N and Y. A uses those parameters to impersonate the other user as follows:

1. A uses his or her own PW and N to compute the hashed value $h(r||x)'$ (see Equation (23)).

   Continuously, A selects a nonce n and the same format of identity ID_i to compute the authentication message K, L and CID:

$$K = h(r||x)' \oplus n \tag{36}$$

$$L = ID_i \oplus h(h(r||x)'||n) \tag{37}$$

$$CID = h(ID_i||n) \tag{38}$$

   and then A sends (r, K, L, CID) to S.

2. S uses the received value r and its secret x to compute the hashed value M (Refer to Equation (28)):

   Next, S computes n' (Refer to Equation (29), $ID_i{}'$ and CID':

$$ID_i' = h(M||n') \oplus L \tag{39}$$

$$CID' = h(ID_i||n') \tag{40}$$

   After that, S checks whether CID' is equal to CID or not. If it holds, S confirms that A is valid and replies a message a' to A:

$$a' = h(h(n||ID_i||M)) \tag{41}$$

3. After receiving message a', A can confirm that he or she pass the authentication to impersonate the User i.

For this reason, if A is a malicious legal user, he or she can impersonate any legal user to communicate with remote user. Yeh et al.'s nonce based scheme is similar to a no identity authentication.

3. The Improved Scheme

In the context of Yeh et al.'s two user authentication schemes, there are some security flaws remaining. Therefore, we have designed a scheme with two unknown factors to protect each parameter in the smart card. Our remediable scheme consists of four phases: the registration phase, the login phase, the authentication phase and the password change phase. We describe these phases in the following subsection and an overview of our improved scheme is presented in Figure 3.

3.1. Registration Phase

1. The user U chooses a password and selects a random number r, then submits the registration messages (ID_u, $h(PW)$, r) to the remote server S via a secure channel.
2. When S receives the registration messages from U, S first generates a nonce N_s and uses ID_u and $h(PW)$ to compute three values P, R and V:

$$P = h(x) \oplus (ID_u||N_s) \tag{42}$$

$$R = h(x||N_s) \oplus h(h(PW) \oplus r) \tag{43}$$

$$V = h(ID_u||h(x||N_s) \oplus r) \tag{44}$$

   Afterward, S issues the smart card with parameters P, R, V and $h(\cdot)$ to U through a secure channel.

3.2. Login Phase

If U wants to login S, he or she first insert his or her own smart card into a card reader or the terminal. Then, U enters his or her ID_u and PW. The smart card performs the following steps:

1. The smart card uses random number r, PW and R to compute a value $h(x||N_s)'$ and calculate V' to compare with V:

$$h(x||N_s)' = R \oplus h(h(PW) \oplus r) \tag{45}$$

$$V' = h(ID_u||h(x||N_s)' \oplus r) \tag{46}$$

$$V' \stackrel{?}{=} V \tag{47}$$

If Equation (47) holds, the smart card generates a nonce N_u and computes messages C_1, SK and C_2; otherwise, the login request is rejected:

$$C_1 = R \oplus h(h(PW) \oplus r) \oplus N_u \tag{48}$$

$$SK = h(h(x||N_s)||N_u) \tag{49}$$

$$C_2 = h(h(ID_u)||N_u||SK) \tag{50}$$

2. Finally, the smart card sends login request messages (P, C_1, C_2) to S.

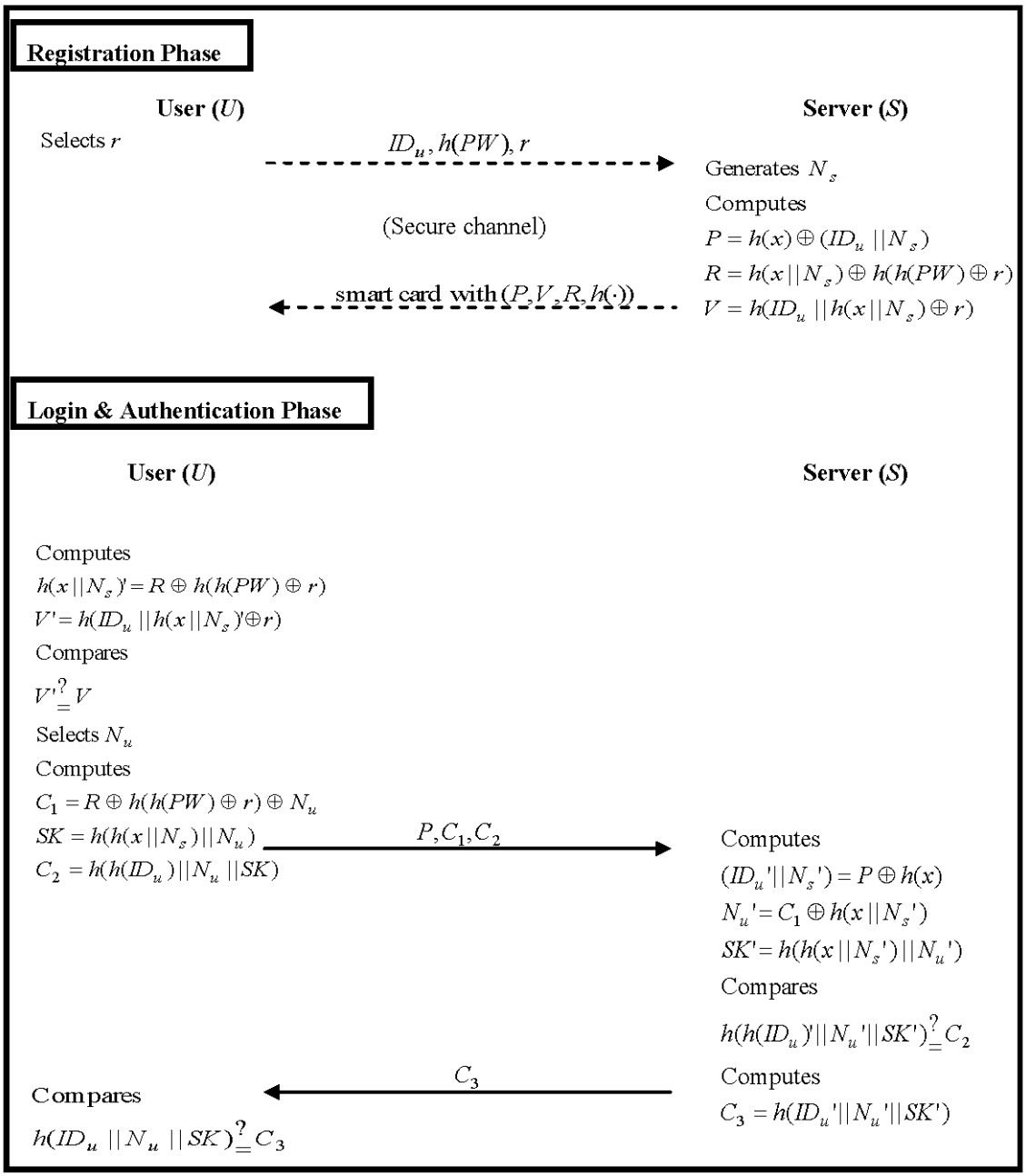

Figure 3. Overview of our improved scheme.

3.3. Authentication Phase

Upon receiving the login request (P, C_1, C_2), S has to perform the following steps to authenticate U:

1. S uses the received value P and its secret key x to obtain ($ID_u{}'$ and $N_s{}'$):

$$(ID_u'||N_s') = P \oplus h(x) \tag{51}$$

Afterward, S computes $N_u{}'$ and SK' to check if the authentication message C_2 is valid or not:

$$N_u' = C_1 \oplus h(x||N_s') \tag{52}$$

$$SK' = h(h(x||N_s')||N_u') \tag{53}$$

$$h\left(h(ID_u')||N_u'||SK'\right) \stackrel{?}{=} C_2 \tag{54}$$

If Equation (54) holds, S confirms that U is a legal user and responds a message C_3 to U:

$$C_3 = h(ID_u'||N_u'||SK') \tag{55}$$

Otherwise, S rejects the login request.

2. When receiving the response C_3, U first verifies whether the message is valid or not:

$$h\left(ID_u||N_u||SK'\right) \stackrel{?}{=} C_3 \tag{56}$$

If the Equation (56) holds, U confirms that S is valid. Afterward, U and S can use the same session key SK to securely communicate with each other.

3.4. Password Change Phase

In this phase, if a U wants to change his or her password, he or she will perform the following steps:

1. First, U inserts his or her smart card into a card reader or the terminal and enters the ID_u and the original PW.
2. Second, according to Equations (46) and (47), the smart card examines the validity of ID_u and PW and compares V' with the stored V. If this holds, U is allowed to key in a new password PW_{new}; otherwise, the smart card rejects the password change request.
3. Third, the smart card calculates R':

$$R' = R \oplus h(PW) \oplus h(PW_{new}) = h(x||N_s) \oplus h(PW_{new}) \tag{57}$$

and replaces the old value R with the new R'. Thus, the password has been successfully changed without the participation of remote server S.

4. Security Analysis

In this section, we will discuss the security of our improved scheme and demonstrate how it is more secure than previous schemes.

4.1. Mutual Authentication

In the proposed scheme, when the personal reader wants to communicate with the medical reader, they must authenticate each other. In this subsection, we use the Burrows–Abadi–Needham (BAN) logic model [40] to proof the correctness of our improved scheme. Recently, many authentication

schemes [41–43] have applied BAN logic to proof the correctness of an authentication and key establishment. The symbols N_s and N_u are nonces; $h(x)$, $h(x||N_s)$ and SK denotes the secret keys; the notation of Ban logic is described as follows:

$P\|\equiv X$	P believes X, or P would be entitled to believe X.
$P \lhd X$	P sees X. Someone has sent a message containing X to P, who can read and repeat X.
$P\| \sim X$	P once said X. P at some time sent a message including X.
$P\|\Rightarrow X$	P has jurisdiction over X. P is an authority on X and should be trusted on this matter.
$< X >_Y$	This represents X combined with Y.
$\#(X)$	The formula X is fresh, that is, X has not been sent in a message at any time before the current run of the protocol.
$P \overset{K}{\leftrightarrow} Q$	P and Q may use the shared key K to communicate.
$P \overset{S}{\Leftrightarrow} Q$	The formula S is a secret known only to P and Q and possibly to principals trusted by them.

The main goal of our scheme is to authenticate the session key establishment between a user U and the remote server S.

$G1$	$U\| \equiv U \overset{SK}{\leftrightarrow} S$
$G2$	$U\| \equiv S\| \equiv U \overset{SK}{\leftrightarrow} S$
$G3$	$S\| \equiv U \overset{SK}{\leftrightarrow} S$
$G4$	$S\| \equiv U\| \equiv U \overset{SK}{\leftrightarrow} S$
$G5$	$S\| \equiv ID_u$
$G6$	$S\| \equiv U\| \equiv ID_u$

According to our authentication phase, we use BAN logic to produce an idealized form as follows:

$M1$	$(< ID_u\|\|N_s >_{h(x)}, < N_u >_{h(x\|\|N_s)}, < U \overset{SK}{\leftrightarrow} S >_{h(h(ID_u)\|\|N_u)})$
$M2$	$(< U \overset{SK}{\leftrightarrow} S >_{h(ID_u\|\|N_u)})$

To analyze our improved scheme, we make the following assumptions:

$A1$	$U\| \equiv \#(N_u)$
$A2$	$S\| \equiv \#(N_u)$
$A3$	$U\| \equiv U \overset{h(x\|\|N_s)}{\Leftrightarrow} S$
$A4$	$S\| \equiv U \overset{h(x\|\|N_s)}{\Leftrightarrow} S$
$A5$	$U\| \equiv S\| \Rightarrow U \overset{SK}{\leftrightarrow} S$
$A6$	$S\| \equiv U\| \Rightarrow U \overset{SK}{\leftrightarrow} S$
$A7$	$S\| \equiv U\| \Rightarrow ID_u$

According to those assumptions and the rules of BAN logic, we show the main proof of our authentication phase as follows:

1. Server S authenticates user U.

   By $M1$ and the *seeing rule*, we can derive:

$$S \lhd (< ID_u || N_s >_{h(x)}, < N_u >_{h(x||N_s)}, < U \overset{SK}{\leftrightarrow} S >_{h(h(ID_u)||N_u)}) \quad \text{(Statement 1)}$$

   By $A2$ and the *freshness rule*, we can derive:

$$S| \equiv \#(< ID_u || N_s >_{h(x)}, < N_u >_{h(x||N_s)}, < U \overset{SK}{\leftrightarrow} S >_{h(h(ID_u)||N_u)}) \quad \text{(Statement 2)}$$

   By (Statement 1), $A4$ and the *message meaning rule*, we can derive:

$$S| \equiv U| \sim (< ID_u || N_s >_{h(x)}, < N_u >_{h(x||N_s)}, < U \overset{SK}{\leftrightarrow} S >_{h(h(ID_u)||N_u)}) \quad \text{(Statement 3)}$$

   By (Statement 2), (Statement 3) and the *nonce verification rule*, we can derive:

$$S| \equiv U| \equiv (< ID_u || N_s >_{h(x)}, < N_u >_{h(x||N_s)}, < U \overset{SK}{\leftrightarrow} S >_{h(h(ID_u)||N_u)}) \quad \text{(Statement 4)}$$

   By (Statement 4) and the *belief rule*, we can derive:

$$S| \equiv U| \equiv U \overset{SK}{\leftrightarrow} S \quad \text{(Statement 5)}$$

   By (Statement 5), $A6$ and the *jurisdiction rule*, we can derive:

$$S| \equiv U \overset{SK}{\leftrightarrow} S \quad \text{(Statement 6)}$$

   By (Statement 6) and the *belief rule*, we can derive:

$$S| \equiv U| \equiv ID_u \quad \text{(Statement 7)}$$

   By (Statement 7), $A7$ and the *jurisdiction rule*, we can derive:

$$S| \equiv ID_u \quad \text{(Statement 8)}$$

2. User U authenticates server S.

   By $M2$ and the *seeing rule*, we can derive:

$$U \lhd (< U \overset{SK}{\leftrightarrow} S >_{h(ID_u||N_u)}) \quad \text{(Statement 9)}$$

   By $A1$ and the *freshness rule*, we can derive:

$$U| \equiv \#(< U \overset{SK}{\leftrightarrow} S >_{h(h(ID_u)||N_u)}) \quad \text{(Statement 10)}$$

   By (Statement 9), $A3$ and the *message meaning rule*, we can derive:

$$U| \equiv S| \sim (< U \overset{SK}{\leftrightarrow} S >_{h(h(ID_u)||N_u)}) \quad \text{(Statement 11)}$$

By (Statement 10), (Statement 11) and the *message meaning rule*, we can derive:

$$U| \equiv S| \equiv U \overset{SK}{\leftrightarrow} S \qquad \text{(Statement 12)}$$

By (Statement 12), *A5* and the *jurisdiction rule*, we can derive:

$$U| \equiv U \overset{SK}{\leftrightarrow} S \qquad \text{(Statement 13)}$$

By (Statement 5) to (Statement 8), (Statement 12) and (Statement 13), we can proof our improved scheme such that user U and the remote server S authenticate each other. Moreover, we are also able to prove that the improved scheme can establish a session key between the user U and the remote server S.

In our improved scheme, the server authenticates the user by checking the message C_2. If server's computed value $h(h(ID_u')||N_u'||SK')$ is equal to C_2, the server proves that the user is valid. Then, server sends message C_3 to the user. The user also compares C_3 with his or her computation value $h(ID_u||N_u||SK')$. If both of them are equal, the user confirms that the server is legitimate. Since the secret value $h(x||N_s)$ is shared between user and server, they can authenticate each other with the login messages (P, C_1, C_2) and the reply message C_3. Hence, mutual authentication obtains in our improved scheme.

Scenario: A malicious attacker uses an illegal server to authenticate a legal user.

Analysis: The attacker will not succeed because the legal user has not been registered to the illegal server and the illegal server cannot calculate the correct session key SK. Thus, it will fail when the legal user attempts to authenticate the illegal server. In the proposed scheme, the attacker cannot achieve their purpose using an illegal server. In the same scenario, the proposed scheme can also defend against a malicious attack using an illegal user to connect to a legal server. This is why the illegal user has not been registered to the legal server and the illegal user cannot calculate the correct session key SK. Thus, the attack will fail when the legal server attempts to authenticate the illegal user.

4.2. Lost Smart Card

According to our improved scheme, if an attacker A obtains a legal user U's smart card somehow, they cannot obtain any parameter without the user's password; even if A extracts the parameters P, R and V (see Equations (42)–(44)) from the smart card, they still cannot obtain any sensitive information (such as ID_u, PW, N_s or the server's secret key x) with those parameters. Notably, A does not know U's correct password and each parameter is always protected by two unknown factors of the smart card. Therefore, no one can use the stolen smart card to obtain authentication without U's correct password and identity.

4.3. ID-Theft Attack

As regards the login and authentication phases of our improved scheme, U's ID_u is always protected by P and C_2; it is impossible for an attacker A to acquire it from P and C_2. Notably, it is difficult to reveal ID_u from P without the server's secret key x and the nonce N_s. Additionally, A cannot obtain ID_u from C_2 without the nonce N_u. Therefore, ID_u cannot be known by the attacker.

4.4. Password Guessing Attacks

This situation involves an attacker A obtaining the U's smart card and intercepting previous messages. In this case, A intends to guess the U's PW from the stored parameter R of the smart card and must know the secret key x and the nonce N_s to compute similar parameters for comparison with parameter R. On the other hand, A can use R and the intercepted P to compute similar messages (P, C_1',

C_2') and send it to S in an attempt to guess U's PW. As A has two unknown values, ID_u and PW, it is difficult to successfully complete this password guessing attack.

4.5. Server Counterfeit Attack and User Impersonation Attack

Notably, Yeh et al.'s schemes will compromise the server's secret key x in the context of a malicious legal user, allowing forgery of another legal user and a remote server. Hence, in the registration phase of our improved scheme (see Equation (42)), the remote server S generates a nonce value N_s to compute parameter P with U's identity ID_u and its secret key x, where the nonce value N_s is different for each user. So, the malicious legal user cannot guess x with an unknown value N_s. As such, these two attacks will be prevented.

4.6. Replay Attack

In our improved scheme, we use a nonce mechanism to prevent the replay attack and to solve the synchronization problem. When an attacker intends to replay the previous messages (P, C_1, C_2) to achieve authentication, they cannot as the nonce value N_u is different in each session. For this reason, the attacker cannot achieve authentication using previous messages.

Scenario: A malicious attacker intercepts the transmitted message between the user and the server and sends the same message again to the user or the server.

Analysis: The attacker will not succeed because the legal user uses the nonce value N_u in each session. The attacker cannot get the correct nonce value N_u. Thus, the attack will fail when the legal server authenticates the received message. In the proposed scheme, the attackers cannot achieve their purpose by sending the same message again to the user or to the server. Therefore, attackers cannot achieve their purpose by replay attack.

5. Performance Analysis

In this section, we compare the security requirements and computation costs with other related proposals in the literature [9,11,27] in Tables 1 and 2, respectively. Recent research [6,9,11,19,25,27,28] has generally only considered one unknown factor for each parameter; this is why their schemes were compromised and have become susceptible to various attacks. However, our improved scheme always consists of two unknown factors within each communication to meet more stringent security requirements. It can be clearly observed that our scheme is more secure than those proposed by others. From Table 2, the proposed scheme's computation costs for our scheme and previous researchers' schemes in each phase are analyzed. For the highest computation cost in the login & authentication phase, Hsiang and Shih's scheme needs eight hash function operations and seven exclusive-or operations. Wang et al.'s scheme needs six hash function operations and thirteen exclusive-or operations. Yeh et al.'s timestamp-based scheme needs eleven hash function operations and fourteen exclusive-or operations. Yeh et al.'s nonce-based scheme needs fifteen hash function operations and five exclusive-or operations. Our scheme needs twelve hash function operations and four exclusive-or operations. Generally speaking, the computation cost of our scheme is comparable to Yeh et al.'s scheme and inferior to Hsiang and Shih's scheme. However, our scheme can defend against all of the attacks discussed herein more effectively than all previous attempts.

Table 1. Security comparison between other related researches and ours.

	Hsiang and Shih's Scheme (2009)	Wang et al.'s Scheme (2009)	Yeh et al.'s Timestamp-Based Scheme (2010)	Yeh et al.'s Nonce-Based Scheme (2010)	Ours
Mutual authentication	Yes	Yes	Yes	Yes	Yes
Freely change password	Yes	Yes	Yes	Yes	Yes
Solve clock synchronization problem	No	No	No	Yes	Yes
Lost smart card	No	No	No	Yes	Yes
Prevention of ID-theft attack	No	No	No	Yes	Yes
Prevention of undetectable on-line password guessing attacks	No	No	No	Yes	Yes
Prevention of off-line password guessing attacks	No	No	No	Yes	Yes
Prevention of user impersonation attack	No	No	Yes	No	Yes
Prevention of server counterfeit attack	No	No	Yes	Yes	Yes
Prevention of man-in-the-middle attack	No	No	Yes	Yes	Yes
Prevention of replay attack	No	No	Yes	Yes	Yes
Prevention of session parallel attack	Yes	Yes	Yes	Yes	Yes

Table 2. Performance comparison between other related researches and ours.

	Hsiang and Shih's Scheme (2009)	Wang et al.'s Scheme (2009)	Yeh et al.'s Timestamp-Based Scheme (2010)	Yeh et al.'s Nonce-Based Scheme (2010)	Ours
Registration phase	$4H + 4Xor$	$2H + 2Xor$	$4H + 5Xor$	$3H + 1Xor$	$4H + 2Xor$
Login & authentication phase	$8H + 7Xor$	$6H + 13Xor$	$11H + 14Xor$	$15H + 5Xor$	$12H + 4Xor$
Password change phase	$6H + 6Xor$	$2H + 2Xor$	$6H + 6Xor$	$3H + 2Xor$	$3H + 2Xor$
Total	$18H + 17Xor$	$10H + 17Xor$	$21H + 25Xor$	$21H + 8Xor$	$19H + 8Xor$

H denotes one way hash operation; *Xor* denotes bitwise exclusive operation.

6. Conclusions

In this paper, we first reviewed Yeh et al.'s two remote user authentication schemes using smart cards. They claimed that their schemes could defend against known attacks more effectively and more efficiently than previous related research. However, in our cryptanalysis, we find that Yeh et al.'s claims allow for further improvements and that their proposals exhibit serious security flaws, i.e., susceptibility to ID-theft attacks, off-line password guessing attacks, undetectable on-line password guessing attacks and user impersonation attacks. Moreover, based on other related researches [15,21], if an attacker can obtain a legal user's smart card, they can extract the secret parameters from the smart card to successfully complete password guessing attacks. Additionally, in cases where an attacker is a malicious legal user, the attacker can use their smart card to impersonate any legal user. This factor results in the security flaws we discussed above; hence, many schemes will be insecure.

To remedy the specific security problems detailed in this paper, we have proposed an improved scheme. The proposed scheme consistently protects each secret parameter with two unknown factors in the smart card; thus, an attacker cannot obtain any sensitive information, even if he or she is a malicious legal user. Most notably, our scheme not only addresses more stringent security requirements and protects against known types of attacks, it also reduces computation costs more effectively than Yeh et al.'s scheme. Therefore, our scheme holds substantial value in the context of numerous applications in various network environments.

Acknowledgments: This research was supported by the Ministry of Science and Technology, Taiwan, under contract numbers MOST 106-2221-E-324-013, MOST 106-2622-E-305-001-CC2 and MOST 103-2632-E-324-001-MY3.

Author Contributions: Chin-Ling Chen and Yu-Fan Lin conceived and designed the protocol; Yong-Yuan Deng, Yung-Wen Tang and Jung-Hsuan Chen analyzed the data All authors have read and approved the final manuscript.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Lamport, L. Password authentication with insecure communication. *ACM Commun.* **1981**, *24*, 770–772. [CrossRef]
2. Argyroudis, P.G.; Verma, R.; Tewari, H.; O'Mahony, D. Performance analysis of cryptographic protocols on handheld devices. In Proceedings of the 3rd International Symposium on Network Computing and Applications, Cambridge, MA, USA, 30 August–1 September 2004; pp. 169–174.
3. Awasthi, A.K.; Lal, S. A remote user authentication scheme using smart cards with forward secrecy. *IEEE Trans. Consum. Electron.* **2003**, *49*, 1246–1248. [CrossRef]
4. Bellare, M.; Rogaway, P. Entity authentication and key distribution. In *Advances in Cryptology—CRYPTO'93, LNCS*; Springer: Berlin, Germany, 1993; Volume 773, pp. 232–249.
5. Chien, H.Y.; Chen, C.H. A remote authentication scheme preserving user anonymity. In Proceedings of the 19th International Conference on Advanced Information Networking and Applications, Taipei, Taiwan, 28–30 March 2005; pp. 245–248.
6. Das, M.L.; Saxena, A.; Gulati, V.P. A dynamic ID-based remote user authentication scheme. *IEEE Trans. Consum. Electron.* **2004**, *50*, 629–631. [CrossRef]
7. Ding, Y.; Horster, P. Undetectable on-line password guessing attacks. *ACM SIGOPS Oper. Syst. Rev.* **1995**, *29*, 77–86. [CrossRef]
8. Duan, X.; Liu, J.W.; Zhang, Q. Security improvement on Chien et al.'s remote user authentication scheme using smart cards. In Proceedings of the IEEE International Conference on Computational Intelligence and Security, Guangzhou, China, 3–6 November 2006; pp. 1133–1135.
9. Gao, Z.X.; Tu, Y.Q. An improvement of dynamic ID-based remote user authentication scheme with smart cards. In Proceedings of the 7th World Congress on Intelligent Control and Automation, Chongqing, China, 25–27 June 2008; pp. 4562–4567.
10. Gong, L. A security risk of depending on synchronized clocks. *ACM Oper. Syst. Rev.* **1992**, *26*, 49–53. [CrossRef]

11. Hsiang, H.C.; Shih, W.K. Weaknesses and improvements of the Yoon-Ryu-Yoo remote user authentication scheme using smart cards. *Comput. Commun.* **2009**, *32*, 649–652. [CrossRef]
12. Hwang, T.; Chen, Y.; Laih, C.S. Non-interactive password authentication without password tables. In Proceedings of the IEEE Region 10 Conference on Computer and Communication Systems, Hong Kong, China, 24–27 September 1990; pp. 429–431.
13. Hwang, M.S.; Chong, S.K.; Chen, T.Y. DoS-resistant ID-based password authentication scheme using smart cards. *J. Syst. Softw.* **2010**, *83*, 163–172. [CrossRef]
14. Hwang, M.S.; Li, L.H. A new remote user authentication scheme using smart cards. *IEEE Trans. Consum. Electron.* **2000**, *46*, 28–30. [CrossRef]
15. Kocher, P.; Jaffe, J.; Jun, B. Differential power analysis. In *Advances in Cryptology: Proceedings of CRYPTO 99, LNCS*; Springer: Berlin, Germany, 1999; Volume 1666, pp. 388–397.
16. Ku, W.C.; Chang, S.T. Impersonation attack on a dynamic ID-based remote user authentication scheme using smart cards. *IEICE Trans. Commun.* **2005**, *E88-B*, 2165–2167. [CrossRef]
17. Lee, C.C.; Hwang, M.S.; Yang, W.P. A flexible remote user authentication scheme using smart cards. *ACM Oper. Syst. Rev.* **2002**, *36*, 46–52. [CrossRef]
18. Lee, C.C.; Li, L.H.; Hwang, M.S. A remote user authentication scheme using hash functions. *ACM Oper. Syst. Rev.* **2002**, *36*, 23–29. [CrossRef]
19. Liao, I.E.; Lee, C.C.; Hwang, M.S. Security enhancement for a dynamic ID-based remote user authentication scheme. In Proceedings of the IEEE International Conference on Next Generation Web Services Practices, Seoul, Korea, 22–26 August 2005; pp. 437–440.
20. Lo, N.W.; Yeh, K.H. Cryptanalysis of two three-party encrypted key exchange protocols. *Comput. Stand. Interfaces* **2009**, *31*, 1167–1174. [CrossRef]
21. Messerges, T.S.; Dabbish, E.A.; Sloan, R.H. Examining smart-card security under the threat of power analysis attacks. *IEEE Trans. Comput.* **2002**, *51*, 541–552. [CrossRef]
22. Misbahuddin, M.; Ahmed, M.A.; Shastri, M.H. A simple and efficient solution to remote user authentication using smart cards. In Proceedings of the Innovations in Information Technology, Dubai, UAE, 19–21 November 2006; pp. 1–5.
23. Sun, H.M. An efficient remote user authentication scheme using smart cards. *IEEE Trans. Consum. Electron.* **2000**, *46*, 958–961.
24. Shen, J.J.; Lin, C.W.; Hwang, M.S. A modified remote user authentication scheme using smart cards. *IEEE Trans. Consum. Electron.* **2003**, *49*, 414–416. [CrossRef]
25. Wang, Y.Y.; Liu, J.Y.; Xiao, F.X.; Dan, J. A more efficient and secure dynamic ID-based remote user authentication scheme. *Comput. Commun.* **2009**, *32*, 583–585. [CrossRef]
26. Xie, Q.; Wang, J.L.; Chen, D.R.; Yu, X.Y. A novel user authentication scheme using smart cards. In Proceedings of the 2008 International Conference on Computer Science and Software Engineering, Hubei, China, 12–14 December 2008; pp. 834–836.
27. Yeh, K.H.; Su, C.; Lo, N.W.; Li, Y.; Hung, Y.X. Two robust remote user authentication protocols using smart cards. *J. Syst. Softw.* **2010**, *83*, 2556–2565. [CrossRef]
28. Yoon, E.J.; Ryu, E.K.; Yoo, K.Y. Further improvement of an efficient password based remote user authentication scheme using smart cards. *IEEE Trans. Consum. Electron.* **2004**, *50*, 612–614. [CrossRef]
29. Zhang, X.; Feng, Q.Y.; Li, M. A modified dynamic ID-based remote user authentication scheme. In Proceedings of the International Conference on Communications, Circuits and Systems, Guilin, China, 25–28 June 2006; pp. 1602–1604.
30. Chang, C.; Hwang, K.F. Some forgery attacks on a remote user authentication scheme using smart cards. *Informatics* **2003**, *14*, 289–294.
31. Hwang, M.S.; Lee, C.C.; Tang, Y.L. A simple remote user authentication scheme. *Math. Comput. Model.* **2002**, *36*, 103–107. [CrossRef]
32. Hwang, T.; Ku, W.C. Reparable key distribution protocols for Internet environments. *IEEE Trans. Consum. Electron.* **1995**, *43*, 1947–1949.
33. Ku, W.C.; Chen, S.M. Weaknesses and improvements of an efficient password based remote user authentication scheme using smart cards. *IEEE Trans. Consum. Electron.* **2004**, *50*, 204–207.
34. Das, A.K.; Goswami, A. A robust anonymous biometric-based remote user authentication scheme using smart cards. *J. King Saud Univ. Comput. Inf. Sci.* **2015**, *27*, 193–210. [CrossRef]

35. Odelu, V.; Das, A.K.; Goswami, A. An efficient ECC-based privacy-preserving client authentication protocol with key agreement using smart card. *J. Inf. Secur. Appl.* **2015**, *21*, 1–19. [CrossRef]
36. Mishra, D.; Chaturvedi, A.; Mukhopadhyay, S. Design of a lightweight two-factor authentication scheme with smart card revocation. *J. Inf. Secur. Appl.* **2015**, *23*, 44–53. [CrossRef]
37. Chaturvedi, A.; Das, A.K.; Mishra, D.; Mukhopadhyay, S. Design of a secure smart card-based multi-server authentication scheme. *J. Inf. Secur. Appl.* **2016**, *30*, 64–80. [CrossRef]
38. Madhusudhan, R.; Hegde, M. Security bound enhancement of remote user authentication using smart card. *J. Inf. Secur. Appl.* **2017**, *36*, 59–68. [CrossRef]
39. Jeon, J.C.; Kang, B.H.; Kim, S.M.; Lee, W.S.; Yoo, K.Y. An improvement of remote user authentication scheme using smart cards. In Proceedings of the International Conference on Mobile Ad-Hoc and Sensor Networks, Vancouver, BC, Canada, 9–12 October 2006; pp. 416–423.
40. Burrows, M.; Abadi, M.; Needham, R. A logic of authentication. *ACM Trans. Comput. Syst.* **1990**, *8*, 18–36. [CrossRef]
41. Chang, C.C.; Lee, C.Y.; Chiu, Y.C. Enhanced authentication scheme with anonymity for roaming service in global mobility networks. *Comput. Commun.* **2009**, *32*, 611–618. [CrossRef]
42. Ren, K.; Lout, W.; Kim, K.; Deng, R. A novel privacy preserving authentication and access control scheme for pervasive computing environments. *IEEE Trans. Veh. Technol.* **2006**, *55*, 1373–1384. [CrossRef]
43. Yeh, L.Y.; Chen, Y.C.; Huang, J.L. PPACP: A portable privacy-preserving authentication and access control protocol in vehicular ad hoc networks. *Comput. Commun.* **2011**, *34*, 447–456. [CrossRef]