International Journal of Innovative Computing, Information and Control
Volume **8**, Number **5(B)**, May **2012**

 ISSN 1349-4198
pp. 3661–3675

A SECURITY ENHANCED REMOTE USER AUTHENTICATION SCHEME USING SMART CARDS

Eun-Jun Yoon[1], Sung-Ho Kim[2] and Kee-Young Yoo[2,*]

[1]Department of Cyber Security
Kyungil University
33 Buho-Ri, Hayang-Ub, Kyungsan-Si, Kyungsangpuk-Do 712-701, Republic of Korea
ejyoon@kiu.ac.kr

[2]School of Computer Science and Engineering
Kyungpook National University
1370 Sankyuk-dong, Buk-gu Daegu 702-701, Republic of Korea
shkim@knu.ac.kr; *Corresponding author: yook@knu.ac.kr

Received November 2010; revised March 2011

Abstract. *A remote user authentication system has become an important part of security, along with confidentiality and integrity, for systems such as the Internet that offer remote access over untrustworthy networks. In 2006, Liaw et al. proposed an efficient and complete remote user authentication scheme using smart cards that includes a session key being agreed and an updated password phase. However, the current paper demonstrates that Liaw et al.'s scheme is vulnerable to some attacks and then presents an improved scheme in order to isolate such security problems.*
Keywords: Security, Authentication, Smart card, Diffie-Hellman key agreement, Cryptography, Cryptanalysis

1. Introduction.

Recently, a remote user authentication system has become an important part of security, along with confidentiality and integrity, for systems such as the Internet that offer remote access over untrustworthy networks [1-22]. In a remote password authentication scheme, based on knowledge of the password, a user can use it to create and send a valid login message to a remote system to gain the right to access. The remote system also uses the shared password to check the validity of the login message and authenticate the user. However, these remote password authentication schemes are vulnerable to password guessing attacks since most users usually choose easy-to-remember passwords. In 1981, a remote password authentication scheme was first proposed by Lamport [23] over an insecure channel. Since then, several schemes [24-43] have been proposed for improving security and achieving greater functionality.

In 2006, Liaw et al. [34] proposed an efficient and complete remote password authentication scheme using smart cards including an agreed session key and updated password phase. Their scheme had several merits: (1) the remote system does not need a dictionary of verification tables to authenticate users; (2) users can choose their passwords freely; (3) mutual authentication was achieved, between the user and the remote system; (4) the communication and computational costs are very low; (5) users can update their passwords after the registration phase; (6) a session key agreed by the user and the remote system can be generated in every session; and (7) the timestamp is discarded in order to avoid the serious time synchronization problem.

However, we found out that Liaw et al.'s scheme does not secure against some attacks [44-46]. It means that the scheme cannot practically be used for smart card-based authentication applications. Based on these motivations, the current paper demonstrates that Liaw et al.'s scheme is vulnerable to some attacks. That is, their session phase is vulnerable to a forgery attack, their registration phase is vulnerable to an insider attack and their updated password phase is vulnerable to a denial of service attack, where an unauthorized user can easily change the smart card password. Furthermore, we present an improved scheme in order to isolate and solve such security problems. Compared with Liaw et al.'s scheme, the proposed scheme can provide strong key agreement function with the property of perfect forward secrecy to reduce the computation loads for smart cards. As a result, compared with related authentication schemes, the proposed scheme has strong security and enhanced computational efficiency. Thus, the proposed scheme is extremely suitable for use in smart card-based authentication applications.

The remainder of this paper is organized as follows. Section 2 briefly reviews Liaw et al.'s remote user authentication scheme using smart cards. Section 3 demonstrates the security weaknesses of Liaw et al.'s scheme. The proposed authentication scheme is presented in Section 4, while Sections 5 and 6 discuss the security and efficiency of the proposed scheme. The conclusion is provided in Section 7.

2. Review of Liaw et al.'s Scheme.

This section briefly reviews Liaw et al.'s remote user authentication scheme using smart cards [34]. The security of Liaw et al.'s scheme depends on the secure one-way hash function. Liaw et al.'s scheme consists of five phases: registration, login, verification, session and updated password phases.

2.1. Registration phase.

Let x be a secret key maintained by the remote system, $h(\cdot)$ be a secure one-way hash function [47, 48] with fixed-length output such as SHA-2 while U_i denotes the ith user who submits his/her identity ID_i and password PW_i to the remote system for registration purpose. For U_i's registration request, the remote system then performs the following operations:

1. Compute U_i's secret information $v_i = h(ID_i, x)$.
2. Compute $e_i = v_i \oplus PW_i$, where $\oplus$ is a bit-wise exclusive-OR operation.
3. Write $h(\cdot)$ and e_i into the memory of a smart card.
4. Issue the smart card to U_i.

Figure 1 shows Liaw et al.'s registration phase.

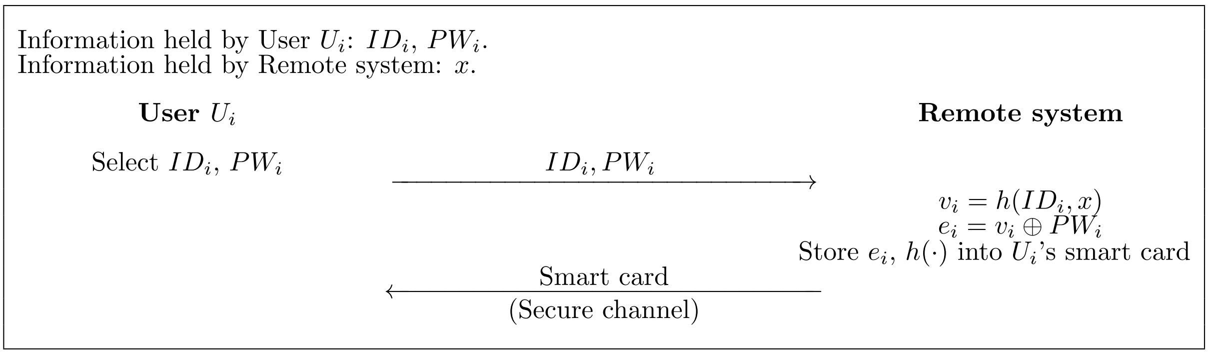

FIGURE 1. Liaw et al.'s registration phase

Shared Information: $h(\cdot)$, $E(\cdot)$, $D(\cdot)$.
Information held by User U_i: ID_i, PW_i, smart card$(e_i, h(\cdot))$.
Information held by Remote system: x.

User U_i		**Remote system**
Login phase:		
Input ID_i and PW_i		
Generate N_i		
$v_i = e_i \oplus PW_i$		
$C = h(v_i, N_i)$	$\xrightarrow{(ID_i, C, N_i)}$	
Verification phase:		
		Check ID_i
		$v_i' = h(ID_i, x)$
		Check $C \stackrel{?}{=} h(v_i', N_i)$
		Generate N_s
$(N_i', N_s') = D_{v_i}(M)$	$\xleftarrow{M}$	$M = E_{v_i'}(N_i, N_s)$
Check $N_i' \stackrel{?}{=} N_i$	$\xrightarrow{N_s'}$	Check $N_s' \stackrel{?}{=} N_s$

Figure 2. Liaw et al.'s login and verification phases

2.2. **Login phase.** When U_i wishes to log into the remote system, he/she inserts the smart card into the terminal and types his/her identity ID_i and password PW_i. The smart card then performs the following operations:

1. Generate a random nonce N_i.
2. Compute $v_i = e_i \oplus PW_i$.
3. Compute $C = h(v_i, N_i)$.
4. Send an authentication request message (ID_i, C, N_i) to the remote system.

2.3. **Verification phase.** After receiving the authentication request message (ID_i,C,N_i), the remote system and smart card execute the following steps to facilitate a mutual authentication process between the user and the remote system. The remote system first performs the following operations:

1. Verify whether ID_i is a valid user identity: If not, the login request is rejected.
2. Compute $v_i' = h(ID_i, x)$ and then check whether $C \stackrel{?}{=} h(v_i', N_i)$. If not, the request is rejected; otherwise, it proceeds to Step 3.
3. Generate a random nonce N_s.
4. Create the encrypted message $M = E_{v_i'}(N_i, N_s)$ by using v_i'.
5. Send $M = E_{v_i'}(N_i, N_s)$ to the smart card.

After receiving the message M, the smart card then performs the following operations:

1. Compute $v_i = e_i \oplus PW_i$.
2. Decrypt M by computing $D_{v_i}(M)$ to derive (N_i', N_s').
3. Verify whether $N_i' \stackrel{?}{=} N_i$. If yes, N_s' is sent to the remote system. If no, the connection is disconnected.

After receiving the message N_s', the remote system verifies whether $N_s' \stackrel{?}{=} N_s$ regarding the smart card. If yes, the mutual authentication process is complete. Figure 2 shows Liaw et al.'s login and verification phases.

2.4. **Session phase.** The security of a session phase is based on the Diffie-Hellman key exchange protocol [49]. In the session phase, a common session key is generated in order to encrypt an individual conversation between the user and the remote system within a session. The session phase involves two public parameters p and α, where p is a large

Shared Information: $h(\cdot)$, $E(\cdot)$, $D(\cdot)$.
Information held by User U_i: ID_i, PW_i, smart card$(e_i, h(\cdot))$, v_i, N_i.
Information held by Remote system: x, v_i', N_s.

User U_i		**Remote system**
$W_i = \alpha^{N_i} \bmod p$		$S_i = \alpha^{N_s} \bmod p$
	$\xrightarrow{W_i}$	
	$\xleftarrow{S_i}$	
$K_u = (S_i)^{N_i} \bmod p$		$K_s = (W_i)^{N_s} \bmod p$
	$\xrightarrow{K_u}$	
	$\xleftarrow{K_s}$	
Check $K_u \stackrel{?}{=} K_s$		Check $K_s \stackrel{?}{=} K_u$
Select a message M_u		Select a message M_s
	$\xrightarrow{E_{v_i}(M_u \oplus K_u)}$	
	$\xleftarrow{E_{v_i'}(M_s \oplus K_s)}$	
$M_s = D_{v_i}(E_{v_i'}(M_s \oplus K_s)) \oplus K_u$		$M_u = D_{v_i'}(E_{v_i}(M_u \oplus K_u)) \oplus K_s$

FIGURE 3. Liaw et al.'s session phase

prime number and α is a primitive element $\bmod p$. In order to agree a secure session key, the remote system and smart card perform the following operations:

1. The remote system computes $S_i = \alpha^{N_s} \bmod p$ and sends S_i to the smart card.
2. The smart card computes $W_i = \alpha^{N_i} \bmod p$ and sends W_i to the remote system.
3. The remote system computes $K_s = (W_i)^{N_s} \bmod p$ and the smart card computes $K_u = (S_i)^{N_i} \bmod p$. Then both determine whether $K_s = K_u$. If yes, a new session is created. That is because

$$\begin{aligned} K &= (S_i)^{N_i} \bmod p \\ &= (\alpha^{N_s} \bmod p)^{N_i} \bmod p \\ &= (\alpha^{N_s N_i} \bmod p) \bmod p \\ &= (\alpha^{N_i} \bmod q)^{N_s} \bmod p \\ &= (W_i)^{N_s} \bmod p. \end{aligned}$$

4. If the remote system wants to send private data or message M_s to U_i, it encrypts message $E_{v_i'}(M_s \oplus K_s)$ with v_i' and sends it to U_i. After U_i receives the message, the smart card decrypts the message and makes an exclusive operation to derive M_s.
5. If U_i wants to send private data or message M_u to the remote system, it encrypts message $E_{v_i}(M_u \oplus K_u)$ and sends it to the remote system. After the remote system receives the message, it decrypts the message and makes an exclusive operation to derive M_u.

Figure 3 shows Liaw et al.'s session phase.

2.5. **Updated password phase.** If U_i wants to change his/her password from PW_i into PW_i' after registration, the following procedure is performed.

1. Calculate $e_i' = e_i \oplus PW_i \oplus PW_i' = v_i \oplus PW_i'$.

2. Update e_i on the memory of smart card to set e'_i. That is done because

$$\begin{aligned} e'_i &= e_i \oplus PW_i \oplus PW'_i \\ &= v_i \oplus PW_i \oplus PW_i \oplus PW'_i \\ &= v_i \oplus PW'_i \\ &= h(ID_i, x) \oplus PW'_i. \end{aligned}$$

Figure 4 shows Liaw et al.'s updated password phase.

Information held by User U_i: ID_i, PW_i
Information held by Smart card: e_i, $h(\cdot)$

User U_i **Smart card**

Input PW_i and PW'_i $\xrightarrow{(PW_i, PW'_i)}$

$e'_i = e_i \oplus PW_i \oplus PW'_i$
Update e_i with e'_i

Figure 4. Liaw et al.'s updated password phase

3. **Cryptanalysis of Liaw et al.'s Scheme.** This section shows that Liaw et al.'s scheme has the following security flaws.

3.1. **Integrity violence of the session key due to illegal modification at the session phase.** Liaw et al.'s session phase is vulnerable to session key integrity violence due to illegal modification. In Steps 4 and 5 of the session phase, since U_i's smart card and the remote system do not check the integrity of the derived private data or message M_s and M_u, respectively, an attacker can easily conduct an illegal modification attack as follows. When the remote system sends encrypted message $E_{v'_i}(M_s \oplus K_s)$ to U_i, the attacker intercepts and replaces it with a random nonce X. After U_i receives the forged message X, the smart card will decrypt X and make an exclusive operation to derive private data or message M_s. Since the derived M_s is a random value, U_i cannot receive the correct M_s. In addition, when U_i's smart card sends an encrypt message $E_{v_i}(M_u \oplus K_u)$ to the remote system, the attacker intercepts and replaces it with a random nonce X. Upon receiving the forged message X, the remote system will decrypt X and make an exclusive operation to derive private data or message M_u. Since the derived M_u is also a random value, the remote system cannot receive the correct M_u. In fact, an illegal modification attack is not a serious attack, since it cannot prevent the two communication parties from reaching a common secret key, even though this key is not the correct one. Most important, the attacker cannot access the agreed common key as a result of this illegal modification attack. However, since the Diffie-Hellman session key $\alpha^{N_i N_s} \bmod p$ is invalid, it cannot guarantee the integrity of the session key. As a result, Liaw et al.'s session phase is vulnerable to session key integrity violence due to illegal modification procedures.

3.2. **Insider attack on the registration phase.** Liaw et al.'s registration phase is vulnerable to an insider attack. In practice, it is likely that user U_i uses the same password PW_i to access several servers for his/her convenience. If the intruder of the remote system has obtained the user's password PW_i, he/she can impersonate the user U_i to access other remote systems [29]. In the registration phase of Liaw et al.'s scheme, the user U_i sends his/her password PW_i to the remote system with plain-text. It is very easy to mount an insider attack because the system recognizes U_i's password PW_i and an insider attacker may get it to login to other remote systems for the purpose of accessing data. Furthermore, if a user loses his/her smart card and it is located by the insider, or if the insider stole the user U_i's smart card, then the insider can easily impersonate the legitimate user U_i by using the password PW_i as well as the smart card at the login phase. In addition, if some users use the same password for multiple accounts, those will be compromised as well. Although it is also possible that all the privileged insiders of the remote system are trusted and U_i does not use the same password to access several servers, the implementers and users of the system should be aware of this potential weakness. As a result, Liaw et al.'s scheme is vulnerable to an insider attack.

3.3. **Denial of service attack on the update password phase.** When a smart card is stolen, an unauthorized user can easily create a new password for the smart card at Liaw et al.'s password change phase [30-32]. The attack can be performed as follows. First, an unauthorized user inserts U_i's smart card into the smart card reader of a terminal, enters the ID_i and PW_a, where PW_a is the unauthorized user's arbitrary password, and request a password change. Next, the unauthorized user enters an arbitrary new password PW'_a and then the smart card will compute $e'_i = e_i \oplus PW_a \oplus PW'_a$, which yields $v_i \oplus PW_i \oplus PW_a \oplus PW'_a$. Finally, the smart card will replace e_i with e'_i without any confirmation. Procedures being followed. If a malicious user stole user U_i's smart card for a short period of time and changed to an arbitrary new password as above described, then the legal user U_i's succeeding login requests will be denied unless he/she re-registers with the remote server again due to $C \neq h(v'_i, N_i)$ in regards to Step 2 of the verification phase. In addition, if user U_i types an incorrect password PW_{wrong} by mistake at the update password phase, then U_i's smart card will compute meaningless $e'_i = e_i \oplus PW_{wrong} \oplus PW'_i$, which yields $v_i \oplus PW_i \oplus PW_{wrong} \oplus PW'_i$ and replaces it with existing e_i. As a result, the user U_i cannot login to the remote system anymore by using the new password PW'_i because the remote system always rejects U_i's login request. As outlined, Liaw et al.'s password change phase is vulnerable to a denial of service attack.

3.4. **Inefficiency for error password login.** Even if U_i inputs an error password in the login phase, the smart card will still send U_i's login request unconditionally to the remote system. This error is not detected until the remote system checks $C \stackrel{?}{=} h(v'_i, N_i)$ at the authentication phase. Therefore, the password authentication procedure is delayed and inefficient.

4. **Proposed Scheme.** In this section, we propose improvements to Liaw et al.'s remote user authentication scheme using smart cards. The security of the proposed scheme also depends on a secure one-way hash function and its nonce-based scheme. The proposed scheme consists of five phases: registration, login, verification, session and updated password phases.

4.1. **Registration phase.** When a new user U_i wants to access resources from the remote system, he/she must register in the remote system over a secure channel and perform the following operations:

1. Chooses his/her identity ID_i, password PW_i and a random number R, then computes password verifier $vpw = PW_i \oplus R$.
2. Sends his/her identity ID_i and password verifier vpw to the remote system.

The remote system then performs the following operations:

1. Compute U_i's secret information $v_i = h(ID_i, x)$.
2. Compute $e_i = v_i \oplus vpw$ and $vk_i = h(v_i, e_i)$.
3. Write $h(\cdot)$, e_i and vk_i into the memory of a smart card.

4. Issue the smart card to U_i.

After receiving the smart card, U_i stores the random number R in his/her smart card. Figure 5 shows the proposed registration phase.

Information held by User U_i: ID_i, PW_i.
Information held by Remote system: x.

User U_i		**Remote system**
Select ID_i, PW_i, R $vpw = PW_i \oplus R$	$\xrightarrow{ID_i, vpw}$	
		$v_i = h(ID_i, x)$ $e_i = v_i \oplus vpw$ $vk_i = h(v_i, e_i)$ Store $e_i, vk_i, h(\cdot)$ into U_i's smart card
Input R into smart card	$\xleftarrow[\text{(Secure Channel)}]{\text{Smart card}}$	

Figure 5. Proposed registration phase

4.2. **Login phase.** When U_i wishes to log into the remote system, he/she inserts the smart card into the terminal and types his/her identity ID_i and password PW_i. The smart card then performs the following operations:

1. Generate a random nonce N_i.
2. Compute $vpw' = PW_i \oplus R$ and $h(e_i \oplus vpw', e_i)$ and verify whether it is equal to the stored vk_i.
3. If it holds, compute $C = h(e_i \oplus vpw', N_i) = h(v_i, N_i)$.
4. Send an authentication request message (ID_i, C, N_i) to the remote system.

4.3. **Verification phase.** After receiving the authentication request message (ID_i,C,N_i), the remote system and smart card will execute the following steps to facilitate mutual authentication between the user and the remote system. The remote system first performs the following operations:

1. Verify that ID_i is a valid user identity. If not, the login request is rejected.
2. Compute $v_i' = h(ID_i, x)$ and then confirm whether $C \stackrel{?}{=} h(v_i', N_i)$. If not, the request is rejected; otherwise, it proceeds to Step 3.
3. Generate a random nonce N_s.
4. Computes $h(v_i', N_i, N_s)$ and sends it back with N_s to the smart card.

After receiving the message $h(v_i', N_i, N_s)$ and N_s, the smart card then performs the following operations:

1. Computes $h(v_i, N_i, N_s)$ and then verifies whether $h(v_i, N_i, N_s) \stackrel{?}{=} h(v_i', N_i, N_s)$.
2. If yes, computes $h(v_i, N_s, N_i)$ which is sent to the remote system for mutual authentication. If no, the connection is disconnected.

After receiving the message $h(v_i, N_s, N_i)$, the remote system verifies whether $h(v_i', N_s, N_i) \stackrel{?}{=} h(v_i, N_s, N_i)$. If yes, the mutual authentication is complete. If no, the connection is terminated. Figure 6 illustrates the proposed login and verification phases.

Shared Information: $h(\cdot)$, $E(\cdot)$, $D(\cdot)$.
Information held by User U_i: ID_i, PW_i, Smart card$(e_i, vk_i, R, h(\cdot))$.
Information held by Remote system: x.

User U_i		**Remote system**
Login phase:		
Input ID_i and PW_i		
$vpw' = PW_i \oplus R$		
Check $vk_i \stackrel{?}{=} h(e_i \oplus vpw', e_i)$		
Generate N_i		
$C = h(e_i \oplus vpw', N_i)$	$\xrightarrow{(ID_i, C, N_i)}$	
Verification phase:		
		Check ID_i
		$v_i' = h(ID_i, x)$
		Check $C \stackrel{?}{=} h(v_i', N_i)$
		Generate N_s
	$\xleftarrow{N_s, h(v_i', N_i, N_s)}$	Compute $h(v_i', N_i, N_s)$
Check $h(v_i, N_i, N_s) \stackrel{?}{=} h(v_i', N_i, N_s)$		
Compute $h(v_i, N_s, N_i)$		
	$\xrightarrow{h(v_i, N_s, N_i)}$	
		Check $h(v_i', N_s, N_i) \stackrel{?}{=} h(v_i, N_s, N_i)$

FIGURE 6. Proposed login and verification phases

4.4. **Session phase.** This subsection describes how to confirm the shared session key K is correctly computed by the remote system and U_i's smart card unlike Liaw et al.'s session phase. The proposed session phase involves two public parameters p and α, where p is a large prime number and α is a primitive element mod p. In order to agree a secure session key, the remote system and smart card perform the following operations:

1. The remote system computes $S_i = \alpha^{N_s} \bmod p$ and sends S_i to the smart card.
2. The smart card computes $W_i = \alpha^{N_i} \bmod p$ and sends W_i to the remote system.
3. The remote system computes $K_s = (W_i)^{N_s} \bmod p$ and the smart card computes $K_u = (S_i)^{N_i} \bmod p$. Then both the remote system and U_i's smart card check whether $K_s = K_u$ by sending $h(v_i', W_i, K_s)$ and $h(v_i, S_i, K_u)$, respectively. If yes, a new session is created due to the following:
$$\begin{aligned} K &= (S_i)^{N_i} \bmod p \\ &= (W_i)^{N_s} \bmod p \\ &= \alpha^{N_s N_i} \bmod p. \end{aligned}$$
4. If the remote system wants to send private data or a message M_s to U_i, it encrypts message $E_{v_i'}(M_s \oplus K_s)$ with v_i' and sends it and $h(M_s)$ to U_i. After U_i receives the message, the smart card decrypts the message and makes an exclusive operation to derive M_s'. Finally, U_i checks that hashed M_s' is equal to the received $h(M_s)$. If yes, U_i confirms the integrity of M_s' and accepts it.
5. If U_i wants to send private data or a message M_u to the remote system, it encrypts message $E_{v_i}(M_u \oplus K_u)$ and sends it and $h(M_u)$ to the remote system. After the remote system receives the message, it decrypts the message and makes an exclusive operation to derive M_u'. Finally, the remote system checks whether the hashed M_u' is equal to the received $h(M_u)$. If yes, the remote system confirms the integrity of M_u' and accepts it.

Figure 7 shows the proposed session phase.

Shared Information: $h(\cdot)$, $E(\cdot)$, $D(\cdot)$.
Information held by User U_i: ID_i, PW_i, smart card$(e_i, vk_i, R, h(\cdot))$, v_i, N_i.
Information held by Remote system: x, v_i', N_s.

User U_i		**Remote system**
$W_i = \alpha^{N_i} \bmod p$		$S_i = \alpha^{N_s} \bmod p$
	$\xrightarrow{W_i}$	
	$\xleftarrow{S_i}$	
$K_u = (S_i)^{N_i} \bmod p$		$K_s = (W_i)^{N_s} \bmod p$
	$\xrightarrow{h(v_i, S_i, K_u)}$	
	$\xleftarrow{h(v_i', W_i, K_s)}$	
Check $h(v_i, W_i, K_u) \stackrel{?}{=} h(v_i', W_i, K_s)$		Check $h(v_i', S_i, K_s) \stackrel{?}{=} h(v_i, S_i, K_u)$
Select a message M_u		Select a message M_s
	$\xrightarrow{E_{v_i}(M_u \oplus K_u), h(M_u)}$	
	$\xleftarrow{E_{v_i'}(M_s \oplus K_s), h(M_s)}$	
$M_s' = D_{v_i}(E_{v_i'}(M_s \oplus K_s)) \oplus K_u$		$M_u' = D_{v_i'}(E_{v_i}(M_u \oplus K_u)) \oplus K_s$
Check $h(M_s') \stackrel{?}{=} h(M_s)$		Check $h(M_u') \stackrel{?}{=} h(M_u)$

FIGURE 7. Proposed session phase

Information held by User U_i: ID_i, PW_i
Information held by Smart card: e_i, vk_i, R, $h(\cdot)$

User U_i		**Smart card**
Input PW_i and PW_i'	$\xrightarrow{(PW_i, PW_i')}$	
		Check $h(e_i \oplus PW_i \oplus R, e_i) \stackrel{?}{=} h(vk_i)$
		$e_i' = e_i \oplus PW_i \oplus PW_i'$
		Update e_i with e_i'

FIGURE 8. Proposed updated password phase

4.5. **Updated password phase.** If U_i wants to change his/her password from PW_i into PW_i' after registration, the following procedure is performed.

1. Calculate $h(e_i \oplus PW_i \oplus R, e_i)$ and verify whether it is equal to the stored vk_i.
2. If it holds, the smart card calculates $e_i' = e_i \oplus PW_i \oplus PW_i' = v_i \oplus R \oplus PW_i'$.
3. Update e_i on the memory of smart card to set e_i'. That is done because

$$\begin{aligned} e_i' &= e_i \oplus PW_i \oplus PW_i' \\ &= v_i \oplus vpw \oplus PW_i \oplus PW_i' \\ &= v_i \oplus PW_i \oplus R \oplus PW_i \oplus PW_i' \\ &= v_i \oplus R \oplus PW_i \\ &= h(ID_i, x) \oplus R \oplus PW_i. \end{aligned}$$

Figure 8 shows the proposed updated password phase.

5. **Security Analysis.** This section analyzes the security of the proposed remote user authentication scheme using smart cards. We only illustrate and discuss the enhanced security features. The remaining features are the same as the original Liaw et al.'s scheme

as described in the research literature [34]. Readers are referred to [34] for more comprehensive references. First, we define the security terms [49-52] needed to conduct an analysis of the proposed scheme. They are as follows:

Definition 5.1. *A weak secret key* (*user's password* PW_i) *is the value of low entropy* $W(k)$, *which can be guessed in polynomial time.*

Definition 5.2. *A strong secret key* (*server's secret key* x) *is the value of high entropy* $S(k)$, *which cannot be guessed in polynomial time.*

Definition 5.3. *The discrete logarithm problem* (*DLP*) *is explained by the following: Given a prime* p, *a generator* α *of* ${}_RZ_p^*$, *and an element* $R \in {}_RZ_p^*$, *find the integer* a, $0 \le a \le p-2$, *such that* $\alpha^a \equiv R \bmod p$.

Definition 5.4. *The Diffie-Hellman problem* (*DHP*) *is explained by the following: Given a prime* p, *a generator* α *of* ${}_RZ_p^*$, *and elements* $\alpha^a \bmod p$ *and* $\alpha^b \bmod p$, *find* $\alpha^{ab} \bmod p$.

Definition 5.5. *A secure one-way hash function* $y = h(x)$ *is one where given* x *to compute* y *is easy and given* y *to compute* x *is difficult.*

The following four security properties must be considered for the proposed protocol; an illegal modification attack at the session phase, an insider attack at the registration phase, a secure password change, and incorrect password detection. Regarding the above mentioned definitions, the following theories are used to analyze the eight security properties of the proposed scheme.

Theorem 5.1. *In the proposed session phase, an attacker cannot successfully initiate the forgery attack, which is described Subsection 3.1.*

Proof: After decrypting the received $E_{v_i'}(M_s \oplus K_s)$ from the remote system and $E_{v_i}(M_u \oplus K_u)$ from the U_i's smart card in Steps 4 and 5 of the proposed session phase, U_i's smart card and the remote system always check that the hashed M_s' and M_u' are equal to the received $h(M_s)$ and $h(M_u)$, respectively; no one can forge the private data or messages M_s and M_u. Therefore, the proposed session phase is secure from the forgery attack, which is described in Subsection 3.1.

Theorem 5.2. *In the proposed registration phase, an insider attacker cannot successfully initiate an insider attack, which is described in Subsection 3.2.*

Proof: Since U_i registers to the remote system by presenting ID_i and $PW_i \oplus R$ instead of ID_i and PW_i unlike Liaw et al.'s registration phase, the insider attacker of the remote system cannot directly obtain or guess the password PW_i without knowing the random number R. Therefore, the proposed registration phase is secure from an insider attack, which is described in Subsection 3.2.

Theorem 5.3. *In the proposed updated password phase, an unauthorized user cannot successfully initiate the denial of service attack, which is described in Subsection 3.3.*

Proof: Because the smart card can verify $h(e_i \oplus PW_i \oplus R, e_i)$ using the stored vk_i in Step 1 of the proposed updated password phase, when the smart card has been stolen or lost, an unauthorized user cannot change the password because the card always verifies $h(e_i \oplus PW_i^* \oplus R, e_i)$ using the stored vk_i, where PW_i^* is an unauthorized user's guessed random password. Thus, no one can initiate a denial of service attack using the stolen or lost smart card. Therefore, the proposed updated password phase is secure from the denial of service attack, which is described in Subsection 3.3.

TABLE 1. Security properties of the proposed scheme and other related schemes

	Liaw et al.'s scheme [34]	Cheng et al.'s scheme [35]	Wang et al.'s scheme [36]	Yang et al.'s scheme [40]	Xu et al.'s scheme [42]	Proposed scheme
No verification table	Yes	No	Yes	Yes	Yes	Yes
Freely chosen password	Yes	Yes	Yes	Yes	Yes	Yes
Mutual authentication	Yes	Yes	Yes	Yes	Yes	Yes
Lower communication and computation cost	Low	Low	Low	Medium	Medium	Low
Updated password	Yes	Yes	Yes	Yes	No	Yes
Session key agreement	Yes	Yes	Yes	Yes	Yes	Yes
Perfect forward secrecy	Yes	No	No	Yes	Yes	Yes
Time synchronization	Yes	No	No	Yes	No	Yes
Replay attack	Secure	Secure	Secure	Secure	Secure	Secure
Guessing attack	Secure	Insecure	Insecure	Secure	Secure	Secure
Impersonation attack	Secure	Secure	Secure	Secure	Secure	Secure
Server spoofing attack	Secure	Secure	Secure	Secure	Secure	Secure
Illegal modification attack on the session phase	Insecure	No support	No support	No support	No support	Secure
Insider attack on the registration phase	Insecure	Insecure	Secure	Secure	Insecure	Secure
Denial of service attack on the updated password phase	Insecure	Secure	Secure	Insecure	No support	Secure
Wrong password detection	Slow	Fast	Fast	Slow	Slow	Fast

Theorem 5.4. *In the proposed login phase, the incorrect input password can easily detected by the smart card without being revealed it to the remote system.*

Proof: In Liaw et al.'s remote user authentication scheme, if user U_i inputs an incorrect password by mistake, this wrong password will be detected by the remote system at the authentication phase. Therefore, Liaw et al.'s scheme is slow to detect the user's incorrect password. In contrast to Liaw et al.'s scheme, at the proposed login phase, if user U_i inputs the incorrect password by mistake, this incorrect password will be quickly detected by a smart card since the smart card can verify $vk_i \stackrel{?}{=} h(e_i \oplus vpw', e_i)$ using the stored e_i and vk_i in Step 2 of the login phase. Therefore, the proposed login phase quickly detects that an incorrect input password has been entered by the user.

We compared the proposed scheme with other related schemes [35, 36, 40, 42] as well as Liaw et al.'s scheme [34]. Table 1 shows the comparison results of the security properties of the proposed scheme and various other remote authentication schemes based on smart cards.

6. **Efficiency Analysis.** This section analyzes efficiency of the proposed scheme. Table 2 provides computational costs of the proposed scheme with various other related schemes [35, 36, 40, 42] as well as Liaw et al.'s scheme [34] in regards to the registration, login, verification, session and updated password phases.

Table 2. Computational costs of the proposed scheme and other related scheme

	Registration	Login	Verification	Session	Updated password
Proposed scheme	$2T(f)$ $2T(\oplus)$	$2T(f)$ $2T(\oplus)$	$6T(f)$	$4T(ME)$ $4T(S)$ $2T(f)$ $4T(\oplus)$	$1T(f)$ $3T(\oplus)$
Liaw et al.'s scheme [34]	$1T(f)$ $1T(\oplus)$	$1T(f)$ $1T(\oplus)$	$2T(f)$ $2T(S)$	$4T(ME)$ $4T(S)$ $2T(\oplus)$	$2T(\oplus)$
Cheng et al.'s scheme [35]	$2T(f)$ $1T(\oplus)$	$(n+1)T(f)$ $2T(\oplus)$	$(n+3)T(f)$ $3T(\oplus)$	No support	$3T(f)$ $5T(\oplus)$
Wang et al.'s scheme [36]	$3T(f)$ $3T(\oplus)$	$4T(f)$ $5T(\oplus)$	$4T(f)$ $5T(\oplus)$	No support	$4T(f)$ $4T(\oplus)$
Yang et al.'s scheme [40]	$5T(f)$ $3T(\oplus)$	$1T(f)$ $1T(\oplus)$ $1T(ME)$	$3T(ME)$ $4T(A)$	No support	$2T(f)$ $2T(\oplus)$
Xu et al.'s scheme [42]	$1T(ME)$ $2T(f)$ $1T(\oplus)$	$3T(f)$ $1T(\oplus)$ $2T(ME)$	$6T(f)$ $4T(ME)$	No support	No support

$T(f)$: computation cost of one-way function; $T(\oplus)$: computation cost of exclusive-OR operation or addition operation; $T(S)$: computation cost of symmetric encryption; $T(A)$: computation cost of asymmetric encryption; $T(ME)$: computation cost of modular exponentiation.

In the registration phase, Liaw et al.'s scheme requires 1 time one-way function operation and 1 time exclusive-OR operation. However, Liaw et al.'s registration phase is insecure to an insider attack. In the proposed registration phase, 1 time one-way function operation and 1 time exclusive-OR operation are additionally required to resist an insider attack compared with Liaw et al.'s scheme. In the verification phase, Liaw et al.'s scheme requires 2 times one-way function operations and 2 times symmetric encryption operations. However, in the proposed verification phase, it does not require any computation costs of symmetric encryption unlike Liaw et al.'s scheme. The proposed verification phase requires only 6 times one-way function operations. In the session phase, Liaw et al.'s scheme requires 4 times modular exponentiations, 4 times symmetric encryption operations, and 2 times one-way function operations. However, Liaw et al.'s session phase is insecure to forgery attacks. In the proposed session phase, 2 times one-way function operations and 2 times exclusive-OR operations are additionally required to resist the forgery attacks compared with Liaw et al.'s scheme. In the updated password phase, Liaw et al.'s scheme requires 2 times one-way function operations. However, Liaw et al.'s updated password phase is insecure to DoS attacks. In the proposed updated password phase, 1 time one-way function operation and 1 time exclusive-OR operation are additionally required to resist a stolen or lost smart card attack compared with Liaw et al.'s scheme.

Therefore, as in Table 2, we can see that the proposed scheme has the lowest computational costs and is well suited to the smart card's applications.

7. **Conclusion.** In 2006, Liaw et al. proposed an efficient and complete remote password authentication scheme. Their scheme has several merits. However, the current paper demonstrated that Liaw et al.'s scheme is vulnerable to some attacks. We proved that their session phase is vulnerable to a forgery attack, that their registration phase is vulnerable to

an insider attack and that their updated password phase is vulnerable to a denial service attack, where an unauthorized user can easily exchange a new password for the smart card. Furthermore, we presented an improved scheme in order to isolate such security problems. As a result, the proposed scheme is more secure than Liaw et al.'s scheme and provides similar computational efficiency.

Acknowledgment. We would like to thank the anonymous reviewers for their helpful comments in improving our manuscript. This research (Grants Nos. 00047239 and 00047610) was supported by Business for Cooperative R&D between Industry, Academy, and Research Institute funded Korea Small and Medium Business Administration in 2011 and was also partially supported by the MKE (The Ministry of Knowledge Economy), Korea, under the ITRC (Information Technology Research Center) support program (NIPA-2012- H0301-12-2004) supervised by the NIPA (National IT Industry Promotion Agency).

REFERENCES

[1] Z. Zhang, B. Fang, M. Hu and H. Zhang, Security analysis of session initiation protocol, *International Journal of Innovative Computing, Information and Control*, vol.3, no.2, pp.457-469, 2007.

[2] Y.-F. Chang, A practical three-party key exchange protocol with round efficiency, *International Journal of Innovative Computing, Information and Control*, vol.4, no.4, pp.953-960, 2008.

[3] C.-Y. Chen, H.-F. Lin and C.-C. Chang, An efficient generalized group-oriented signature scheme, *International Journal of Innovative Computing, Information and Control*, vol.4, no.6, pp.1335-1345, 2008.

[4] J.-S. Lee, Y.-F. Chang and C.-C. Chang, Secure authentication protocols for mobile commerce transactions, *International Journal of Innovative Computing, Information and Control*, vol.4, no.9, pp.2305-2314, 2008.

[5] H.-F. Huang and W.-C. Wei, A new efficient and complete remote user authentication protocol with smart cards, *International Journal of Innovative Computing, Information and Control*, vol.4, no.11, pp.2803-2808, 2008.

[6] C.-L. Chen, Y.-Y. Chen and Y.-H. Chen, Group-based authentication to protect digital content for business applications, *International Journal of Innovative Computing, Information and Control*, vol.5, no.5, pp.1243-1251, 2009.

[7] R.-C. Wang, W.-S. Juang and C.-L. Lei, A robust authentication scheme with user anonymity for wireless environments, *International Journal of Innovative Computing, Information and Control*, vol.5, no.4, pp.1069-1080, 2009.

[8] T.-H. Chen, An authentication protocol with billing non-repudiation to personal communication systems, *International Journal of Innovative Computing, Information and Control*, vol.5, no.9, pp.2657-2664, 2009.

[9] C.-T. Li, C.-H. Wei and Y.-H. Chin, A secure event update protocol for peer-to-peer massively multiplayer online games against masquerade attacks, *International Journal of Innovative Computing, Information and Control*, vol.5, no.12(A), pp.4715-4723, 2009.

[10] W.-S. Juang, C.-L. Lei, H.-T. Liaw and W.-K. Nien, Robust and efficient three-party user authentication and key agreement using bilinear pairings, *International Journal of Innovative Computing, Information and Control*, vol.6, no.2, pp.763-772, 2010.

[11] J.-H. Yang and C.-C. Chang, An efficient payment scheme by using electronic bill of lading, *International Journal of Innovative Computing, Information and Control*, vol.6, no.4, pp.1773-1780, 2010.

[12] J.-Y. Huang, Y.-F. Chung, T.-S. Chen and I-E. Liao, A secure time-bound hierarchical key management scheme based on ECC for mobile agents, *International Journal of Innovative Computing, Information and Control*, vol.6, no.5, pp.2159-2170, 2010.

[13] C.-T. Li and M.-S. Hwang, An online biometrics-based secret sharing scheme for multiparty cryptosystem using smart cards, *International Journal of Innovative Computing, Information and Control*, vol.6, no.5, pp.2181-2188, 2010.

[14] I.-C. Lin, C.-W. Yang and S.-C. Tsaur, Nonidentifiable RFID privacy protection with ownership transfer, *International Journal of Innovative Computing, Information and Control*, vol.6, no.5, pp.2341-2352, 2010.

[15] H.-C. Hsiang, A novel dynamic ID-based remote mutual authentication scheme, *International Journal of Innovative Computing, Information and Control*, vol.6, no.6, pp.2407-2416, 2010.
[16] N. W. Lo and K.-H. Yeh, A practical three-party authenticated key exchange protocol, *International Journal of Innovative Computing, Information and Control*, vol.6, no.6, pp.2469-2484, 2010.
[17] K.-H. Yeh, N. W. Lo and E. Winata, Cryptanalysis of an efficient remote user authentication scheme with smart cards, *International Journal of Innovative Computing, Information and Control*, vol.6, no.6, pp.2595-2608, 2010.
[18] N. W. Lo and K.-H. Yeh, A novel authentication scheme for mobile commerce transactions, *International Journal of Innovative Computing, Information and Control*, vol.6, no.7, pp.3093-3104, 2010.
[19] C.-C. Chang and S.-C. Chang, An efficient Internet on-line transaction mechanism, *International Journal of Innovative Computing, Information and Control*, vol.6, no.7, pp.3239-3246, 2010.
[20] K.-H. Yeh and N. W. Lo, A novel remote user authentication scheme for multi-server environment without using smart cards, *International Journal of Innovative Computing, Information and Control*, vol.6, no.8, pp.3467-3478, 2010.
[21] J.-L. Tsai, T.-S. Wu, H.-Y. Lin and J.-E. Lee, Efficient convertible multi-authenticated encryption scheme without message redundancy or one-way hash function, *International Journal of Innovative Computing, Information and Control*, vol.6, no.9, pp.3843-3852, 2010.
[22] H.-L. Wang, T.-H. Chen, L.-S. Li, Y.-T. Wu and J. Chen, An authenticated key exchange protocol for mobile stations from two distinct home networks, *International Journal of Innovative Computing, Information and Control*, vol.6, no.9, pp.4125-4132, 2010.
[23] L. Lamport, Password authentication with insecure communication, *Communications of the ACM*, vol.24, pp.770-772, 1981.
[24] H. Y. Chien, J. K. Jan and Y. M. Tseng, An efficient and practical solution to remote authentication: Smart card, *Computers & Security*, vol.21, pp.372-375, 2002.
[25] C. L. Lin, H. M. Sun and T. Hwang, Attacks and solutions on strong-password authentication, *IEICE Trans. Commun.*, vol.E84-B, pp.2622-2627, 2001.
[26] M. Sandirigama, A. Shimizu and M. T. Noda, Simple and secure password authentication protocol (SAS), *IEICE Trans. Commun.*, vol.E83-B, pp.1363-1365, 2000.
[27] H. M. Sun, An efficient remote use authentication scheme using smart cards, *IEEE Trans. Consumer Electron.*, vol.46, no.4, pp.958-961, 2000.
[28] T. C. Yeh, H. Y. Shen and J. J. Hwang, A secure one-time password authentication scheme using smart cards, *IEICE Trans. Commun.*, vol.E85-B, pp.2515-2518, 2002.
[29] W. C. Ku and S. M. Chen, Weaknesses and improvements of an efficient password based remote user authentication scheme using smart cards, *IEEE Trans. on Consumer Electronics*, vol.50, no.1, pp.204-207, 2004.
[30] E. J. Yoon and K. Y. Yoo, New authentication scheme based on a one-way hash function and Diffie-Hellman key exchange, *CANS 2005, LNCS*, vol.3810, pp.147-160, 2005.
[31] E. J. Yoon and K. Y. Yoo, Robust secret key based authentication scheme using smart cards, *PCM 2005 Part II, LNCS*, vol.3768, pp.723-734, 2005.
[32] E. J. Yoon, E. K. Ryu and K. Y. Yoo, An improvement of Hwang-Lee-Tang's simple remote user authentication scheme, *Computers & Security*, vol.24, pp.50-56, 2005.
[33] W. G. Shieh and J. M. Wang, Efficient remote mutual authentication and key agreement, *Computers & Security*, vol.25, no.1, pp.72-77, 2006.
[34] H. T. Liaw, J. F. Lin and W. C. Wu, An efficient and complete remote user authentication scheme using smart cards, *Mathematical and Computer Modelling*, vol.44, pp.223-228, 2006.
[35] T. F. Cheng, J. S. Lee and C. C. Chang, Security enhancement of an IC-card-based remote login mechanism, *Computer Networks*, vol.51, no.9, pp.2280-2287, 2007.
[36] X. M. Wang, W. F. Zhang, J. S. Zhang and M. K. Khan, Cryptanalysis and improvement on two efficient remote user authentication scheme using smart cards, *Computer Standards & Interfaces*, vol.29, no.5, pp.507-512, 2007.
[37] L. L. Hu, X. X. Niu and Y. X. Yang, Weaknesses and improvements of a remote user authentication scheme using smart cards, *The Journal of China Universities of Posts and Telecommunications*, vol.14, no.3, pp.91-94, 2007.
[38] T. H. Chen and W. B. Lee, A new method for using hash functions to solve remote user authentication, *Computers & Electrical Engineering*, vol.34, no.1, pp.53-62, 2008.
[39] W. S. Juang and W. K. Nien, Efficient password authenticated key agreement using bilinear pairings, *Mathematical and Computer Modelling*, vol.47, no.11-12, pp.1238-1245, 2008.

[40] G. Yang, D. S. Wong, H. Wang and X. Deng, Two-factor mutual authentication based on smart cards and passwords, *Journal of Computer and System Sciences*, vol.74, no.7, pp.1160-1172, 2008.

[41] I. Liao, C. C. Lee and M. S. Hwang, A password authentication scheme over insecure networks, *J. Comput. System Sci.*, vol.72, no.4, pp.727-740, 2006.

[42] J. Xu, W. T. Zhu and D. G. Feng, An improved smart card based password authentication scheme with provable security, *Computer Standards & Interfaces*, vol.31, no.4, pp.723-728, 2008.

[43] Y. P. Liao and S. S. Wang, A secure dynamic ID based remote user authentication scheme for multi-server environment, *Computer Standards & Interfaces*, vol.31, no.1, pp.24-29, 2009.

[44] Z.-Y. Wu, Y. Chung, F. Lai, T.-S. Chen and H.-C. Lee, An enhanced password-based user authentication scheme for grid computing, *International Journal of Innovative Computing, Information and Control*, vol.7, no.7(A), pp.3751-3760, 2011.

[45] C.-T. Li, C.-C. Lee, L.-J. Wang and C.-J. Liu, A secure billing service with two-factor user authentication in wireless sensor networks, *International Journal of Innovative Computing, Information and Control*, vol.7, no.8, pp.4821-4832, 2011.

[46] E.-J. Yoon, M. K. Khan and K.-Y. Yoo, New robust protocols for remote user authentication and password change, *International Journal of Innovative Computing, Information and Control*, vol.7, no.9, pp.5583-5604, 2011.

[47] R. Rivest, The MD5 message digest algorithm, *Technical Report RFC 1321, IETF*, 1992.

[48] NIST, Secure hash standard, *Technical Report FIPS 180-1, NIST, US*, Department of Commerce, 1995.

[49] W. Diffie and M. E. Hellman, New directions in cryptography, *IEEE Trans. Inform. Theory*, vol.22, pp.644-654, 1976.

[50] A. J. Menezes, P. C. Oorschot and S. A. Vanstone, *Handbook of Applied Cryptograph*, CRC Press, New York, 1997.

[51] B. Schneier, *Applied Cryptography-Protocols. Algorithms and Source Code in C*, 2nd Edition, John Wiley & Sons, 1995.

[52] C. Boyd and A. Mathuria, *Protocols for Authentication and Key Establishment*, Springer-Verlag, 2003.