Enhanced Biometrics-based Remote User Authentication Scheme Using Smart Cards

Il-Soo Jeon[1], Hyun-Sung Kim[2], Myung-Sik Kim[3]

Abstract

Secure and efficient authentication scheme has been a very important issue with the development of networking technologies. Li and Hwang proposed an efficient biometrics-based remote user authentication scheme using smart cards. However, recently, Li et al. pointed out that their scheme is vulnerable to the man-in-the-middle attack, and does not provide proper authentications, and Li et al. proposed an improved biometrics-based authentication scheme. These schemes are vulnerable to various attacks even if the schemes are based on tamper-resistant technologies. Tamper-resistant technologies have been developed with the various applications of smart cards. Therefore, we will assume that the user could use the tamper-resistant smart card in this paper. First of all, this paper shows that Li et al.'s scheme is vulnerable to the replay attack and has a weakness to the password changing scheme even if it is assumed that the scheme could use the tamper-resistant smart cards. Furthermore, we propose an enhanced authentication scheme to solve the security flaws in the two schemes.

Keywords : Authentication protocol, Biometrics, Smart cards, Information security

1. Introduction

Remote user authentication is a method to authenticate remote users to a server over insecure networks. To authenticate remote users, the password-based authentication method has been widely used. Lamport in [1] proposed an authentication scheme based on passwords, in which a password verification table was used in the server. However, since the scheme needs to maintain a verification table in the server, it is very vulnerable to the server compromise attack or the verification table modification attack.

Received(January 03, 2011), Review request(January 04, 2011), Review Result(1st:January 18, 2011, 2nd:January 30, 2011)
Accepted(April 30, 2011)

[1]Professor at School of Electronic Engineering, Kumoh National Institute of Technology, Sanhoro 77, Kumi, Kyungbuk 730-701
email: isjeon@kumoh.ac.kr

[2]Professor at School of Computer Engineering, Kyungil University, Kyungsan, Kyungbuk 702-701
email: kim@kiu.ac.kr

[3](Corresponding Author) Professor at School of Electronic Engineering, Kumoh National Institute of Technology, Sanhoro 77, Kumi, Kyungbuk 730-701
email: kimms@kumoh.ac.kr

* 본 연구는 금오공과대학교 학술연구비에 의하여 연구된 논문

In order to overcome those problems, Hwang and Li in [2] proposed a remote user authentication scheme using smart cards based on ElGamal's public key cryptosystem, which does not use a verification table. Since then, many password-based authentication schemes using smart cards have been proposed [3-10]. Even if a scheme uses smart cards for the user authentication, it is not easy to make a secure scheme resist various attacks, because humans cannot remember lengthy password. Therefore, lots of user authentication schemes using smart cards suffer from the password guessing attack.

To enhance the security of the password-based remote user authentication scheme, some research results using biometric information with smart cards were published [11-16]. Biometric information cannot be lost or stolen, and can provide a strong authentication of the owner. Lee et al. in [11] proposed a fingerprint-based remote user authentication scheme using smart cards. But Lin and Lai in [13] pointed out that the scheme of Lee et al. is vulnerable to the masquerade attack, and proposed a flexible biometrics-based remote user authentication scheme. However, Khan and Zhang in [14] showed that the scheme of Lin and Lai is vulnerable to the server spoofing attack, and proposed an improved scheme of theirs. And Kim et al. in [12] proposed an ID-based password authentication scheme using smart cards and fingerprints, but Scott in [17] presented cryptanalysis of Kim et al.'s scheme.

Recently, Li and Hwang in [16] proposed an efficient biometrics-based remote user authentication scheme using smart cards. The security of their scheme is based on hash function, biometrics verification, and smart cards. The computation cost of their scheme is relatively low compared to other related schemes [6-7, 13-14, 18]. However, quite recently, Li et al. in [19] showed that Li and Hwang's scheme does not provide proper authentication, thus it cannot resist the man-in-the-middle attack, and has a problem in biometrics authentication method. And Li et al. proposed an improved biometrics-based remote user authentication scheme in order to remove the weaknesses existing in Li and Hwang's scheme. However, we have found that Li et al.'s scheme cannot resist the replay attack and has a weakness to the password changing scheme.

In this paper, we show the security flaws in Li et al.'s scheme and propose an improved biometrics-based remote user authentication scheme using tamper-resistant smart cards to effectively resolve the security flaws that exist in Li et al.'s scheme and Li and Hwang's scheme. Most authentication schemes using smart cards including Li and Hwang's scheme and Li et al.'s scheme are susceptible to stolen smart card attacks, not assuming that the smart cards have a tamper-resistant feature. Tamper-resistant technologies have been developed with the various applications of smart cards [20-24].

The rest of this paper is organized as follows. In the following section, we review the schemes of Li et al. and Li and Hwang, and show a cryptanalysis of their schemes. Next, we present an improved authentication scheme in Section 3. The security and performance analysis of the proposed scheme are discussed in Section 4. Finally, the conclusion is given in Section 5.

2. Review of Related Schemes

In this section, we briefly discuss the attributes of smart cards that qualify them for remote user authentication schemes and review Li and Hwang's scheme in [16] and Li et al.'s scheme in [19] with the cryptanalysis of their schemes.

2.1. Attributes of Smart Cards

These days, smart cards play an important role in our everyday life. We utilize them as credit cards, electronic purses, health cards, and secure tokens for authentication of individual identity. But, since smart cards have low computing capability, lots of authentication schemes using smart cards have been designed without public key cryptosystem technology for computation efficiency. Under the circumstances, if a smart card is lost or stolen, those schemes are usually weak from the offline password guessing attack, because human-memorable passwords are not long enough to resist the attack.

Even if a smart card is lost or stolen, to protect important data in the smart card such as password and secret key information, proper tamper-resistant technologies in both hardware and software have been developed to counteract various attacks [20-24]. According to smart card alliance, today's smart card technology is extremely difficult to duplicate or forge and has built-in tamper-resistance. Smart card chips include a variety of hardware and software capabilities that detect and react to tampering attempts and help counter possible attacks. For example, the chips are manufactured with features such as extra metal layers, sensors to detect thermal and UV light attacks, and additional software and hardware circuitry to thwart differential power analysis [25].

It is important to develop authentication schemes using general smart cards, but they are usually insecure for the stolen smart card attack. Considering the poor computing capability of smart cards, authentication schemes using smart cards are required to have low computation cost by performing of hash functions or symmetric key cryptosystems as their main operations. Therefore, to develop an efficient and secure authentication scheme which can resist the smart card stolen attack, temper-resistant smart cards can be used.

2.2. Related Schemes and Cryptanalysis of Them

In this section, we briefly review Li and Hwang's scheme and Li et al.'s scheme, and show the cryptanalysis of them.

2.2.1. Li and Hwang's Scheme

To clearly describe Li and Hwang's Scheme in [16], some notations were used and summarized in Table 1.

These notations will be used in other authentication schemes throughout this paper.

Li and Hwang's scheme uses smart cards, biometrics verification, and hash functions as its main operation. There are three participants, the trusted registration center, R, the server, S_i ,and the client (user), C_i. Li and Hwang's scheme contains a registration phase, a login phase, an authentication phase, and a password change phase. In this paper, the login phase and authentication phases were integrated into one phase to provide a brief description. We review each phase of their scheme in the following subsections.

A. Registration Phase

We briefly describe the registration process of their scheme in the following steps.

Step 1: The user presents his/her identification, ID_i personal biometrics, B_i, and the password, PW_i, to the trusted registration center, R_i, via a secure channel.

Step 2: R_i computes $f_i=h(B_i)$ and $e_i=h(ID_i \| x_S) \oplus h(PW_i \| f_i)$, where x_S is secret information which will be maintained by the server, S_i. Lastly, R_i stores (ID_i, $h(\ )$, f_i, e_i) into the user's smart card and sends it to the user via a secure channel.

[Table 1] Notations

Symbol	Description
C_i	Client (User)
S_i	Server
R_i	Trust registration center
ID_i	Identity of user i
SID_i	Identity of S_i
PW_i	Password of the C_i
B_i	Biometric template of the C_i
$h(\ )$	One-way hash function
x_S	Secret information of the server
R_C	Random number chosen by the client
R_S	Random umber chosen by the server
$\|$	Concatenation operator
$\oplus$	XOR operator

B. Login and Authentication Phase

Whenever the remote user, C_i, wants to login to the server, S_i, in order to authenticate S_i and be authenticated by S_i, he/she has to perform the following steps.

Step 1: C_i inserts his/her smart card into the card reader and inputs the personal biometrics, B_i, on the biometrics input device. Then, the smart card computes $h(B_i)$ and checks if $h(B_i)=f_i$ holds or not. If

it does not hold, C_i fails the biometrics verification and the login process is terminated. Otherwise, C_i passes the biometrics verification and then C_i inputs the password, PW_i.

Step 2: Upon receiving PW_i, C_i's smart card computes $M_1=e_i \oplus h(PW_i \| f_i)=h(ID_i \| x_S)$ and $M_2=M_1 \oplus R_C$, where R_C is a random number generated by C_i.

And then, C_i sends the message, (ID_i, M_2), to S_i.

Step 3: After receiving (ID_i, M_2), S_i checks whether the format of ID_i is valid or not. If it is not valid, S_i rejects the login request. Otherwise, S_i computes the following messages:

$M_3=h(ID_i \| x_S)$, $M_4=M_2 \oplus M_3=R_C$, $M_5=M_3 \oplus R_S$, where R_S is a random number generated by S_i.

$M_6=h(M_2 \| M_4)$

And then, S_i sends the message, (M_5, M_6) to C_i.

Step 4: C_i, checks if $M_6=h(M_2 \| R_C)$ is hold or not. If it does not hold, C_i cannot authenticate S_i and terminates the login request. Otherwise, if it holds, C_i believes that S_i is authenticated and then computes the following messages:

$M_7=M_5 \oplus M_1=R_S$, $M_8=h(M_5 \| M_7)$

And then, C_i sends the message, M_8 to S_i.

Step 5: S_i checks if $M_8=h(M_5 \| R_S)$ is hold or not. If it does not hold, S_i cannot authenticate C_i and rejects the login request. Otherwise, S_i can authenticate C_i and accepts C_i's login request.

C. Password Change Phase

A remote user, C_i, can freely change the current password, PW_i, to a new password, PW_i' without the server S_i's help. To change the password, C_i inserts the smart card and inputs his/her biometric template, B_i to verify his/her biometrics. If $h(B_i)=f_i$ holds, C_i passes the biometric verification, then he/she inputs the original password, PW_i and the new password, PW_i'. Then, the smart card performs $e_i'=e_i \oplus h(PW_i \| f_i) \oplus h(PW_i' \| f_i)=h(ID_i \| x_S) \oplus h(PW_i' \| f_i)$. Finally, the user's password will be changed to the new password by replacing of e_i with e_i' on the smart card.

2.2.2. Cryptanalysis of Li and Hwang's Scheme

In this section, we briefly review the cryptanalysis of Li and Hwang's scheme presented by Li et al. in [19].

A. Li and Hwang's Scheme Fails to Provide Proper Authentication

Case1: an attacker, E, intercepts the login message, (ID_i, M_2), when C_i sends it to S_i. E chooses a random number R_E and computes $M_2'=M_2 \oplus R_E$, then E sends the fabricated message, (ID_i, M_2'), to the server S_i. After receiving (ID_i, M_2'), S_i checks whether the format of ID_i is valid or not. Obviously it is valid, then S_i

computes $M_3=h(ID_i \| x_S)$, $M_4=M_2' \oplus M_3=R_C \oplus R_E$, $M_5=M_3 \oplus R_S$, and $M_6=h(M_2' \| M_4)=h(M_2 \oplus R_E \| R_C \oplus R_E)$. S_i sends the message, (M_5, M_6), to C_i. Upon receiving (M_5, M_6), C_i computes $h(M_2 \| R_C)$ and compares it with M_6. It is obvious that $h(M_2 \| R_C) \neq M_6=h(M_2 \oplus R_E \| R_C \oplus R_E)$, so C_i terminates the session. C_i thinks S_i is a cheater, but S_i is actually the honest server.

Case2: an attacker, E, intercepts the authentication message, (M_5, M_6), when S_i sends it to C_i. E chooses a random number, R_S', and computes $M_5'=M_5 \oplus R_S'$, then E sends the fabricated message, (M_5', M_6), to C_i. After receiving (M_5', M_6), C_i checks whether the equation, $M_6=h(M_2 \| R_C)$, holds or not. Since E does not change the message, M_6, the equation holds. Then, C_i computes $M_7=M_5' \oplus M_1=R_S \oplus R_S'$, and $M_8=h(M_5' \| M_7)=h(M_5 \oplus R_S' \| R_S \oplus R_S')$. Finally, C_i sends the message M_8 to S_i. After receiving M_8, S_i computes $h(M_5 \| R_S)$ and compares it with M_8. It is obvious that $h(M_5 \| R_S) \neq M_8=h(M_5 \oplus R_S' \| R_S \oplus R_S')$, so S_i terminates the session. S_i thinks C_i is a cheater, but C_i is actually the honest user.

B. Man-in-the-middle Attack

When C_i sends the login message, (ID_i, M_2), to S_i, the attacker, E, eavesdrops the message, (ID_i, M_2), then he also starts a session with S_i and sends the message, (ID_i, M_{E2}) = (ID_i, M_2), to S_i. After receiving (ID_i, M_2) and (ID_i, M_{E2}), S_i chooses two random numbers R_S and R_{ES} for the two sessions respectively. Then S_i computes $M_3=h(ID_i \| x_S)$, $M_4=M_2 \oplus M_3$, $M_5=M_3 \oplus R_S$, $M_6=h(M_2 \| M_4)$, and $M_{E3}=h(ID_i \| x_S)$, $M_{E4}=M_{E2} \oplus M_{E3}$, $M_{E5}=M_{E3} \oplus R_{ES}$, $M_{E6}=h(M_{E2} \| M_{E4})$, then S_i sends the messages, (M_5, M_6) and (M_{E5}, M_{E6}), for the two sessions respectively. Here, we need to note that: $M_{E3}=M_3$, $M_{E4}=M_4$, $M_{E5}=M_3 \oplus R_{ES}$, $M_{E2}=h(M_2 \| M_4)=h(M_{E2} \| M_{E4})$. E intercepts (M_5, M_6) and (M_{E5}, M_{E6}) and sends the fabricated message, (M_5', M_6') = (M_{E5}, M_{E6}), to C_i. After receiving (M_5', M_6'), C_i first verifies whether $M_6'=h(M_2 \| R_C)$ holds or not. It is obvious that $M_6'=M_{E6}=h(M_2 \| M_4)=h(M_2 \| R_C)$. So S_i is authenticated by C_i. Then, C_i computes $M_7=M_5' \oplus M_1=R_{ES}$, $M_8=h(M_5' \| M_7)=h(M_{E2} \| R_{ES})$. C_i sends the message, M_8, to S_i. E intercepts M_8 and sends the message, $M_{E8}=M_8$, to S_i. After receiving M_{E8}, S_i verifies the equation $h(M_{E5} \| R_{ES})=M_8$. Therefore, *E's* masquerading as C_i is authenticated by S_i.

C. Hash Function Problem

One of the fundamental properties of hash functions is that the outputs are very sensitive to small perturbations in their inputs. Generally speaking, those cryptographic hash functions cannot be applied straight forwardly when the input data contains noises within biometrics. In Li and Hwang's scheme, the biometric authentication relies on the verifying of $h(B_i)=f_i$. But, there may be few differences between the input biometrics each time and this situation will make the legal user unable to pass biometric authentication.

2.3. Li et al.'s scheme

In this section, we review Li et al.'s scheme in [19]. They also assume three participants, the trusted registration center, R, and the server, S_i, and the client (user), C_i. R chooses a master key, x_s, a secret random number, y, and distributes x_s and y to the server via a secure channel. The master secret key, x_s, is shared between R and S_i, and y is shared between S_i and C_i's smart card. Their biometrics verification method is different from that of Li and Hwang's scheme. To overcome the biometrics authentication method in Li and Hwang's scheme, Li et al. use the biometric template matching method. The general matching system decides match or no-match by the degree of similarity between the inputted biometric information and the stored biometric template. If the similarity is larger than the predefined thresholds, it will be declared as match, otherwise it is determined no-match. Additionally, their scheme is able to provide a session key agreement after the authentication process.

Li et al.'s scheme also contains a registration phase, a login phase, an authentication phase, and a password change phase like Li and Hwang's scheme. To provide a brief description, login phase and authentication phase were integrated into one phase. We review each phase of their scheme in the following subsections.

2.3.1 Registration Phase

We briefly describe the registration process of their scheme in the following steps.

Step 1: The user, C_i, chooses a random number, N, and computes $RPW_i=h(N \| PW_i)$, then C_i inputs his/her personal biometrics, B_i, on the specific device and provides RPW_i, his/her identity, ID_i, and personal biometrics, B_i, to the trusted registration center, R, via a secure channel.

Step 2: R computes $h(B_i)=f_i$ and $e_i=h(ID_i \| x_S) \oplus h(RPW_i \| f_i)$, stores $(ID_i, h(\ ), f_i, e_i)$ into C_i's smart card, and sends it to the user via a secure channel.

Step 3: C_i enters N into his/her smart card.

2.3.2. Login and Authentication Phase

Whenever the remote user, C_i, wants to login to the server, S_i, he/she has to perform the following steps.

Step 1: C_i inserts his/her smart card into the card reader and inputs the personal biometrics, B_i, on the biometrics input device. If the biometric information does not match the template which stored in the system, the login process is terminated. Otherwise, C_i passes the biometrics verification, then C_i inputs his/her ID_i and the password, PW_i.

Step 2: Upon receiving ID_i and PW_i, C_i's smart card computes $RPW_i=h(N \| PW_i)$, $M_1=e_i \oplus h(RPW_i \| f_i)=h(ID_i \| x_S)$, $M_2=M_1 \oplus R_C$, $M_3=h(y \| R_C)$, $M_4=RPW_i \oplus M_3$, and $M_5=h(M_2 \| M_3 \| M_4)$, where R_C is a random number chosen by C_i. Finally, C_i sends the message, (ID_i, M_2, M_4, M_5), to S_i.

Step 3: After receiving (ID_i, M_2, M_4, M_5), S_i checks whether the ID_i is valid or not. If it is not valid, S_i

rejects the login request. Otherwise, S_i computes $M_6=h(ID_i \| x_S)$, $M_7=M_2 \oplus M_6=R_C$, $M_8=h(y \| M_7)$, and verifies the equation, $M_5=h(M_2 \| M_8 \| M_4)$. If they are equal and the computed M_7 does not equal the M_7' stored in the database at the most recent session, S_i accepts the login request and stores M_7 in the database to replace M_7'. And S_i computes $M_9=M_4 \oplus M_8$, $M_{10}=h(M_9 \| SID_i \| y) \oplus M_8 \oplus R_S$, and $M_{11}=h(M_6 \| M_9 \| y \| R_S)$, where R_S is a random number chosen by S_i. Finally, S_i sends the message, (M_{10}, M_{11}), to C_i. Otherwise, S_i reject the login request and terminates the process, because S_i considers it as a replay attack or man-in-the-middle attack.

Step 4: After receiving (M_{10}, M_{11}), C_i computes $M_{12}=h(RPW_i \| SID_i \| y) \oplus M_3 \oplus M_{10}$ and checks if $M_{11}=h(M_1 \| RPW_i \| y \| M_{12})$ holds or not. If it does not hold, C_i cannot authenticate S_i and terminates the process. Otherwise, S_i is authenticated by C_i.

After the mutual authentication phase, C_i and S_i compute $h(RPW_i \| M_3 \| M_{12} \| SID_i)$ and $h(M_9 \| M_8 \| R_S \| SID_i)$ which are taken as their session key respectively.

2.3.3. Password Change Phase

A remote user, C_i, can freely change the current password, PW_i, to a new password, PW_i', without the help of the registration center, R. To change the password, C_i inserts the smart card into the card reader and inputs his/her biometric template, B_i, on the specific device to verify his/her biometrics. If C_i passes the biometric verification, then he/she inputs the current password, PW_i, and the new password, PW_i'. Then, the smart card computes $RPW_i=h(N \| PW_i)$, $RPW_i'=h(N \| PW_i')$, and $e_i'=e_i \oplus h(RPW_i \| f_i) \oplus h(RPW_i' \| f_i)=h(ID_i \| x_S) \oplus h(RPW_i' \| f_i)$. Finally, the user's password will be changed to the new password by replacing e_i with e_i' on the smart card.

2.4. Cryptanalysis of Li et al.'s Scheme

Li et al. claimed that their scheme resists various attacks, but we have found that their scheme is vulnerable to the replay attack and has a weakness to the password changing scheme even if their scheme uses tamper-resistant smart cards. We show the security flaws that exist in Chen et al.'s scheme in the following subsections.

2.4.1. Replay Attack

Assume an attacker, E, has eavesdropped C_i's a login message, (ID_i, M_2, M_4, M_5), from one of the previous sessions which is not the most recent session. Then, E requests to login to the server, S_i, by sending the eavesdropped message, (ID_i, M_2, M_4, M_5). On receiving the message, S_i checks validity of ID_i. Obviously ID_i is valid, so S_i computes $M_6=h(ID_i \| X_S)$, $M_7=M_2 \oplus M_6=R_C$, and $M_8=h(y \| M_7)$. Then, S_i verifies the equation, $M_5=h(M_2 \| M_8 \| M_2)$, and compares M_7 to M_7' stored in the database at the most recent session. Since the login

message used by E is not from the most recent session, the M_7 of current session is different from the M_7' stored in the database. Therefore, S_i considers the login request as a legal one and stores current session's M_7 to the database. Finally, S_i authenticates E, computes $M_{10}=h(M_9 \| SID_i \| y) \oplus M_8 \oplus R_S$, $M_{11}=h(M_6 \| M_9 \| y \| R_S)$, and sends ($M_{10}$, M_{11}) to E. Therefore, E can masquerade as C_i through the replay attack.

2.4.2. Weakness to the Password Changing Scheme

To change C_i's password, C_i inserts the smart card into the card reader and inputs his/her biometrics on the biometrics input device. After passing the biometric verification, C_i inputs the current password, PW_i, and the new password, PW_i'. Then, the smart card will change password. Even if C_i inputs the current password or a new password incorrectly by mistake, the system will perform the process with the wrong information. If the user is unaware of this mistake, the smart card may have reached unrecoverable state.

3. Proposed Authentication Scheme

In this section, we propose an enhanced biometrics-based remote user authentication scheme to overcome the security flaws which exist in both Li and Hwang's scheme and Li et al.'s scheme. In Li and Hwang's scheme, even if the attacker, E, does not know the secret value, $h(ID_i \| x_S)$, enclosed in e_i on C_i's smart card, he/she can send a login message. But S_i does not know if E knows the secret value or not. Likewise, when an authentication message is sent from S_i to C_i, C_i does not know if the other party knows the secret value, $h(ID_i \| x_S)$, or not. This enables E to successfully complete the attacks described in Section 2. Therefore, in the proposed scheme, we use symmetric key cryptosystem to prevent E from modification or extraction of important information in the login and authentication messages.

To overcome the problem of password changing in Li et al.'s scheme, our scheme only performs the password changing process after login and authentication process to avoid an unintentional input mistake of the current password and double-checks for a new password. In addition, in order to resist the stolen smart card, we assume that our scheme uses tamper-resistant smart cards. To perform the biometrics authentication in the proposed scheme, since the outputs of hash functions are very sensitive to small perturbations in their inputs in [19], we use the biometric template matching method used by Li et al. Additionally, our scheme also provides a session key agreement after the authentication process.

The proposed scheme contains a registration phase, a login and authentication phase, and a password change phase. These phases are described in the following subsections and illustrated briefly in Fig. 1.

3.1. Registration Phase

We briefly describe the registration process of our scheme in the following steps.

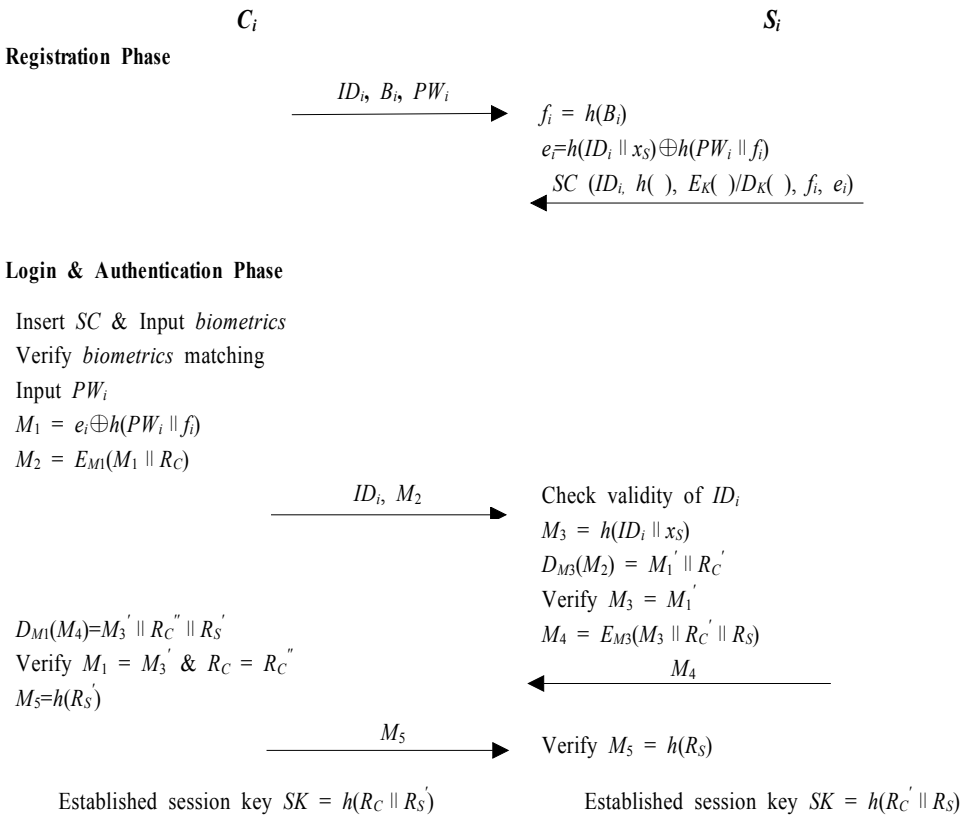
Step 1: The user, C_i, presents his/her identification, ID_i personal biometrics, B_i, and the password, PW_i, to the trusted registration center, R_i, via a secure channel.

Step 2: R_i computes $f_i=h(B_i)$ and $e_i=h(ID_i \| x_S) \oplus h(PW_i \| f_i)$, where x_S is secret information which will be maintained by the server, S_i. Then, R_i stores (ID_i, $h(\ )$, $E_K(\ )/D_K(\ )$, f_i, e_i) into C_i's smart card, where $E_K(\ )/D_K(\ )$ is a symmetric key encryption/description system. Finally, R sends the smart card to C_i via a secure channel.

3.2. Login and Authentication Phase

Whenever the remote user, C_i, wants to login to the server, S_i, in order to authenticate S_i and be authenticated by S_i, he/she has to perform the following steps.

Step 1: C_i inserts his/her smart card into the card reader and inputs the personal biometrics, B_i, through the biometrics input device. If the biometric information does not match the template which stored in the system, the login process is terminated. Otherwise, C_i passes the biometrics verification, then C_i inputs his/her password, PW_i.



[Fig. 1] Proposed authentication scheme

Step 2: Upon receiving PW_i, C_i's smart card computes $M_1=e_i \oplus h(PW_i \| f_i)=h(ID_i \| x_S)$ and $M_2= E_{M1}(M_1 \| R_C)$, where R_C is a random number chosen by C_i. Then, C_i sends the message, (ID_i, M_2), to S_i.

Step 3: After receiving (ID_i, M_2), S_i checks whether the format of ID_i is valid or not. If ID_i is not valid, S_i rejects the login request. Otherwise, S_i computes $M_3=h(ID_i \| x_S)$ and $D_{M3}(M_2)=M_1' \| R_C'$. Then, S_i checks if $M_3 = M_1'$ holds or not. If it does not hold, S_i rejects the login request. Otherwise, S_i chooses a random number, R_S, and computes $M_4 = E_{M3}(M_3 \| R_C' \| R_S)$. Finally, S_i sends the message, M_4, to C_i.

Step 4: After receiving M_4, C_i computes $D_{M1}(M_4)=M_3' \| R_C'' \| R_S'$. Then, C_i checks if both $M_1 = M_3'$ and $R_C = R_C''$ hold or not. If they do not hold, C_i does not authenticate S_i and terminates the login request. Otherwise, C_i authenticates S_i, then computes $M_5=h(R_S')$. Finally, C_i sends the message, M_5, to S_i.

Step 5: After receiving M_5, S_i checks if $M_5 = h(R_S)$ holds or not. If it does not hold, S_i does not authenticate C_i, and rejects the login request. Otherwise, S_i authenticates C_i, and accepts C_i's login request.

After the mutual authentication phase, C_i and S_i compute $h(R_C \| R_S')$ and $h(R_C' \| R_S)$ which are taken as their session key respectively.

3.3. Password Change Phase

The proposed scheme requires the server's help to change the password of users. We briefly describe the password changing process in the following steps.

Step 1: C_i performs the login and authentication process as described in Section 3.2. The inputted current password, PW, for login is maintained in the smart card until the completion of password changing process.

Step 2: After completing the login and authentication process successfully, C_i inputs a new password, PW_n, two times. If both of the inputted new passwords are same, the smart card computes $e_i'=e_i \oplus h(PW_i \| f_i) \oplus h(PW_i' \| f_i)=h(ID_i \| x_S) \oplus h(PW_i' \| f_i)$. The C_i's password will be changed to the new password by replacing e_i with e_i' on the smart card.

4. Security and Performance Analysis

In this section, we analyze the security of our scheme by discussing its resistance to various attacks, and we discuss the performance of our scheme.

4.1 Security Analysis

In this section, we analyze the security of our scheme by showing its resistance to various attacks.

4.1.1. Impersonation Attack

It is difficult for an attacker, E, to successfully complete the impersonation attack on both the user side and the server side. For the user side, E cannot create a feasible $M_2=E_{M1}(M_1 \| R_C)$ without knowing the secret value, $M_1=h(ID_i \| x_s)$ which is used as the secret key of the encryption system. But it is enclosed in $e_i=h(ID_i \| x_s) \oplus h(PW_i \| f_i)$ on C_i's smart card. So, it cannot be extracted without the C_i's biometrics and password. Therefore, if E sends a fake login message, the login request will be rejected on S_i by the verification test of the secret value, $h(ID_i \| x_s)$, after the decryption of M_4. For the server side, E cannot create a feasible $M_4=E_{M3}(M_3 \| R_c' \| R_S)$ without knowing the secret value, $M_3=h(ID_i \| x_s)$. Therefore, if E sends a fake authentication message to C_i, C_i can detect the attack by the verification test of both the secret value, $h(ID_i \| x_s)$, and the random number, R_C, after the decryption of M_4. Thus, the proposed scheme is secure against the

impersonation attack.

4.1.2. Replay Attack

To perform a replay attack, E will use the eavesdropped message, M_2, from one of the C_i's previous sessions which is not the last session. If E sends the eavesdropped message, M_2, to S_i, S_i responds to E with $M_4'=E_{M3}(M_3 \| R_C' \| R_S')$. But, E cannot decrypt M_4' since he/she does not know $M_3=h(ID_i \| x_s)$ which is the secret key of the symmetric decryption system. And E cannot use the eavesdropped M_4 from one of the previous sessions to be authenticated by S_i, because the random number will be changed in every session. Therefore, since E cannot extract the correct R_S' from any communication messages nor create a correct message, $M_5=h(R_S')$. So, if E will send an incorrect message to S_i, then S_i will not authenticate E. Thus, the proposed scheme is secure against the replay attack.

4.1.3. Parallel Attack

After C_i sends the login message, M_2, to S_i, assume that E immediately sends the same message to S_i. Then, E's message passes the verification test of the secret value on S_i. So, S_i responds to E with $M_4'=E_{M3}(M_3 \| R_C' \| R_S')$. This is the same situation explained in the replay attack. Therefore, E cannot be authenticated by S_i. Thus, the proposed scheme is secure against the parallel attack.

4.1.4. Man-in-the-middle Attack

In the proposed scheme, login and authentication messages encrypted with the secret key, $h(ID_i \| x_s)$, cannot be released to E. Therefore, E cannot fabricate feasible messages in the middle of S_i and C_i. If E sends a fake message for login or authentication, he/she will be detected by the secret value verification or random number verification on S_i or C_i. Thus, the proposed scheme is secure against the man-in-the-middle attack.

4.1.5. Password Guessing Attack

It is difficult for E to guess the C_i's password based on the communication messages between S_i and C_i since the password is not included in them. Also, E cannot guess the password from the password table in S_i since the password table does not exist in S_i. Even if E gets the C_i's smart card, it is difficult for E to guess the C_i's password, because the password exists in the form of $h(ID_i \| x_s) \oplus h(PW_i \| f_i)$ in the smart card. To find the correct password, E has to able to guess the secret value, $h(ID_i \| x_s)$, and C_i's biometrics. Since the smart card has a tamper-resistance feature, E cannot get the information from the smart card. So, E tries to guess $h(ID_i \| x_s)$ from the communication messages between S_i and C_i. But, $h(ID_i \| x_s)$ is always encrypted within the communication messages. Furthermore, E cannot create C_i's biometrics. Therefore, E cannot guess the password in our scheme. Thus, the proposed scheme is secure against the password guessing attack.

[Table 2] Computation and communication costs comparison

Comparison factors	Li and Hwang's scheme	Li et al.'s scheme	Our Scheme
No. of hash op. in registration phase	3	4	3
No. of hash op. in login & authentication phase	7	11	4
No. of total hash operations	10	15	7
No. of symmetric key encryption or decryption	0	0	4
No. of insecure communication	3	2	3

[Table 3] Security comparison

Comparison factors	Li and Hwang's scheme	Li et al.'s scheme	Our Scheme
Proper biometrics authentication	No	Yes	Yes
Man-in-the-middle attack resistance	No	Yes	Yes
Replay attack resistance	Yes	No	Yes
No use of DB for message storing	Yes	No	Yes
Session key agreement	No	Yes	Yes

4.2. Performance Analysis

In this section, we evaluate the performance of the proposed scheme in two aspects, security strength and the costs of computation and communication. To evaluate the performance, we compare our scheme to Li and Hwang's scheme in [16] and Li et al.'s scheme in [19]. We showed the results of computation and communication costs comparison in Table 2. We can say that all the schemes are efficient in computation because they do not use any modular exponentiations. Our scheme uses a symmetric key cryptosystem which is not used the others. It should be noted that the computational complexity of symmetric key encryption or decryption operation is similar to that of hash function operation. Feldhofer and Rechberger claimed that AES is even more efficient than SHA-256 in resource-constrained devices such as RFID tags [26]. Therefore, it will not a big problem even if we consider the symmetric key operation as the hash function operation to evaluate computation cost. Then, as shown in Table 2, the computation cost of our scheme is similar to that of Li and Hwang's scheme and less than Li et al.'s scheme. In communication cost, Li et al.'s scheme has 2 insecure communications, but the others have 3. Maybe the low number of communications caused their scheme to be vulnerable to the parallel attack. Therefore, although our scheme has one more communication than Li et al.'s scheme, it is valuable because it can resist the replay attack. In Table 3, we listed the comparison results about some security factors. As shown in Table 3, our scheme is the most secure among them. Our scheme is not

only secure against the man-in-the-middle attack and the replay attack but also does not use the database to store communication messages.

5. Conclusion

In this paper, we showed the vulnerability in Li et al.'s biometric-based remote user authentication scheme, and proposed an enhanced biometrics-based remote user authentication scheme based on tamper-resistant smart cards. We demonstrated that our scheme is efficient and secure against the various attacks through the analysis of security and computing efficiency. Therefore, considering the low computing capabilities of smart cards and the efficiency of our scheme, it will be suitable for practical uses.

References

[1] L. Lamport, "Password authentication with in secure communication," *Communications of the ACM*, Vol. 24, No. 11, pp. 770-772, 1981.

[2] M. S. Hwang and L. H. Li, "A new remote user authentication scheme using smart cards," *IEEE Transactions on Consumer Electronics*, Vol. 46, No. 1, pp. 28-30, 2000.

[3] H. M. Sun, "An efficient remote user authentication scheme using smart Cards," *IEEE Transactions on Consumer Electronics*, Vol. 46, No. 1, pp. 958-961, 2000.

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

[4] J. J. Shen, C. W. Lin, M. S. Hwang, "A modified remote user authentication scheme using smart cards," *IEEE Transactions on Consumer Electronics*, Vol. 49, No. 2, pp. 414-416, 2003.

[5] M. Kumar, "New remote user authentication scheme using smart cards," *IEEE Transactions on Consumer Electronics*, Vol. 50, No. 2, pp. 579-580, 2004.

[6] E. J. Yoon, E. K. Ryu, and K. Y. Yoo, "An improvement of Hwang–Lee–Tang's simple remote user authentication scheme," *Computers and Security*, Vol. 24, No. 1, pp. 50-56, 2005.

[7] N. Y. Lee and Y. C. Chiu, "Improved remote authentication scheme with smart card," *Computer Standards and Interfaces*, Vol. 27, No. 2, pp. 177-180, 2005.

[8] S. K. Kim and M. G. Chung, "More secure remote user authentication Scheme," *Computer Communications*, Vol. 32, No. 6, pp. 1018-1021, 2009.

[9] 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, 2009.

[10] R. Song, "Advanced smart card based password authentication protocol," *Computer Standard & Interfaces*, Vol. 32, pp. 321-325, 2010.

[11] J. K. Lee, S. R. Ryu, and K. Y. Yoo, "Fingerprint-based remote user authentication scheme using smart cards," *IEE Electronics Letters*, Vol. 38, No. 12, pp. 554-555, 2002.

[12] H. S. Kim, S. W. Lee, and K. Y. Yoo, "ID-based Password Authentication Scheme using Smart Cards and Fingerprints," *ACM Operating Systems Review*, pp. 32-41, 2003.

[13] C. H. Lin and Y. Y. Lai, "A flexible biometrics remote user authentication scheme," *Computer Standard and Interfaces*, Vol. 27, No. 1, pp. 19-23, 2004.

[14] M. K. Khan, J. Zhang, and X. Wang, "Chaotic hash-based fingerprint biometric remote user authentication scheme on mobile devices," *Chaos Solutions & Fractals*, Vol. 35, No. 3, pp. 519-524, 2008.

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

[16] C. T. Li and M. S. Hwang, "An efficient biometrics-based remote user authentication scheme using smart

cards," *Journal of Network and Computer Applications*, Vol. 33, No. 1, pp. 1-5, 2010.

[17] M. Scott, "Cryptanalysis of an ID-based password authentication scheme using smart cards and fingerprints," *ACM SIGOPS Operating Systems Review*, Vol. 38, No. 2, pp. 73-75, 2004.

[18] Y. F. Chang, C. C. Chang, and Y. W. Su, "A secure improvement on the user-friendly remote authentication scheme with no time concurrency mechanism," *Proceedings of 20th international conference on advanced information networking and applications*, IEEECS, 2006.

[19] X. Li, J. W. Niu, J. Ma, W. D. Wang, "Cryptanalysis and improvement of a biometrics-based remote user authentication scheme using smart cards," *Journal of Network and Computer Applications*, 2010.

[20] O. Kommerling and M. G. Kuhn, "Design Principles for Tamper-Resistant Smartcard Processors," *Proceedings of the USENIX Workshop on Smartcard Technology*, pp. 9-20, 1999.

[21] S. Ravi, A. Raghunathan, and S. Chakradhar, "Tamper Resistance Mechanisms for Secure Embedded Systems," *IEEE Proceedings of the 17th International Conference on VLSI Design*, pp. 605-611, 2004.

[22] H. Jin, G. Myles, and J. Lotspiech, "Towards Better Software Tamper Resistance," *Lecture Notes in Computer Science*, Vol. 3650, pp. 417-430, 2005.

[23] P. Wang, S. K. Kang, and K. Kim, "Tamper Resistant Software Through Dynamic Integrity Checking," *The 2005 Symposium on Cryptography and Information Security*, 2005.

[24] X. Leng, "Smart card applications and security," *Information Security Technical Report*, Vol. 14, pp. 36-45, 2009.

[25] http://www.smartcardalliance.org/pages/smart-cards-faq#how-do-smart-cards-help-to- protect-privacy.

[26] M. Feldhofer and C. Rechberger, "A case against currently used hash functions in RFID protocols," *Lecture Notes in Computer Science*, Vol. 4277, pp. 372-381, 2006.

Authors

Il-Soo Jeon

Feb. 1984 : B. Sc. in Dept. of Electronic Engineering, Kyungpook Nat'l Univ.
Feb. 1988 : M. Sc. in Dept. of Electronic Engineering, Kyungpook Nat'l Univ.
Feb. 1995 : Ph. D. in Dept. of Electronic Engineering, Kyungpook Nat'l Univ.
March 1989 ~ Feb. 2004 : Ph. D. in Dept. of Computer Engineering, Kyungil Univ.
March 2004 ~ current : Professor at School of Electronic Engineering, Kumoh Nat'l Institute of Tech.
Research Interests : Network security, Cryptographic protocol, Information security

Hyun Sung Kim

Feb. 1996 : B. Sc. in Dept. of Computer Engineering, Kyungil University
Feb. 1998 : M. Sc. in Dept. of Computer Engineering, Kyungpook Nat'l Univ.
Feb. 2002 : Ph. D. in Dept. of Computer Engineering, Kyungpook Nat'l Univ.
March 2002 ~ current : Professor at Dept. of Computer Eng., Kyungil Univ.
March 2002 ~ current : Editorial board of KIISC journal
Jan. 2009 ~ Jan. 2010 : Visiting Professor at Dublin City University
Research Interests : Cognitive radio network security, Network security, Cryptographic protocol, Information security

Myung-Sik Kim

Feb. 1983 : B. Sc. in Dept. of Electronic Engineering, Kyungpook Nat'l Univ.
Feb. 1985 : M. Sc. in Dept. of Electric and Electronic Engineering, KAIST.
Feb. 1992 : Ph. D. in Dept. of Electric and Electronic Engineering, KAIST
March 1985 ~ July. 1992 : Senior Researcher in Applied Electronic Lab. KIST.
August 1992 ~ current : Professor at School of Electronic Engineering, Kumoh Nat'l Institute of Tech.
Research Interests : Semiconductor Circuit Design, Information Security