ISSN 1975-8359(Print) / ISSN 2287-4364(Online)
The Transactions of the Korean Institute of Electrical Engineers Vol. 65, No. 12, pp. 2167∼2176, 2016
http://dx.doi.org/10.5370/KIEE.2016.65.12.2167

멀티서버 환경을 위한 생체정보 기반 삼중 요소 사용자 인증 기법의 안전성 개선

Security Improvement on Biometric-based Three Factors User Authentication Scheme for Multi-Server Environments

문 종 호* · 원 동 호†
(Jongho Moon · Dongho Won)

Abstract - In the multi-server environment, remote user authentication has a very critical issue because it provides the authorization that enables users to access their resource or services. For this reason, numerous remote user authentication schemes have been proposed over recent years. Recently, Lin et al. have shown that the weaknesses of Baruah et al.'s three factors user authentication scheme for multi-server environment, and proposed an enhanced biometric-based remote user authentication scheme. They claimed that their scheme has many security features and can resist various well-known attacks; however, we found that Lin et al.'s scheme is still insecure. In this paper, we demonstrate that Lin et al.'s scheme is vulnerable against the outsider attack and user impersonation attack, and propose a new biometric-based scheme for authentication and key agreement that can be used in the multi-server environment. Lastly, we show that the proposed scheme is more secure and can support the security properties.

Key Words : User authentication, Multi-server environment, Biometric-based, Smart card

1. Introduction

Since Lamport [1] proposed the first password-based authentication scheme over insecure communications in 1981, password-based authentication schemes [2-5] have been extensively investigated. Remote user authentication scheme is one of the most convenient authentication schemes for dealing with the transmission of secret data through insecure communication channels. During the last two decades, many researchers have proposed the remote user authentication schemes.

A problem that occurs with respect to password-based authentication schemes, however, is that a server must maintain a verification table of the legitimacy of a remote user; therefore, the server requires additional storage to store the verification table. For this reason, many researchers have proposed a new types of remote user authentication schemes whereby the biological characteristics such as a fingerprint are used. The main advantageous property of the biometrics is uniqueness, leading to the proposal of numerous. In the view of fact that several biometric-based remote user authenticati on schemes using smart card [6-8] have been proposed.

In 2010, Li and Hwang [9] proposed a remote user authentication scheme which was based on biometric verification, smart card, one-way hash function and nonce for the authentication. However, in 2011, Li et al. [10] have shown that Li and Hwang's scheme does not provide proper authentication and cannot resist man-in-the-middle attack. In 2014, Chuang and Chen [11] proposed a multi-server authenticated key agreement scheme using smart card and biometrics with user anonymity. However, Mishra et al. [12] found that their scheme cannot resist the stolen smart card attack and impersonation attack, and proposed an improved remote user authentication scheme. Unfortunately, Baruah et al. [13] found that Mishra et al.'s scheme also cannot withstand the stolen smart card attack and impersonation attack.

Recently, Lin et al. [14] found that Baruah et al.'s scheme cannot resist the stolen smart card attack, and proposed an enhanced user authentication scheme. In order to overcome these weaknesses, they used the fuzzy extractor technology [15]. However, Lin et al.'s user authentication scheme is still insecure.

In this paper, we demonstrate the security weaknesses of

† Corresponding Author : Dept. of Computer Engineering, Sungkyunkwan University, Korea.
E-mail: dhwon@security.re.kr
* Dept. of Electrical and Computer Engineering, Sungkyunkwan University, Korea.
Received : October 18, 2016; Accepted : November 21, 2016

Lin et al.'s biometrics-based three factors user authentication scheme. Their scheme does not effectively resist the outsider and impersonation attacks; to overcome these security vulnerabilities, we propose a new biometrics-based scheme for authentication and key agreement that can be used in a multi-server environment. In addition, we demonstrate that the proposed scheme provides a strong authentication defense against a number of attacks including the attacks of the original scheme. Lastly, we compare the performance and functionality of the proposed scheme with other related schemes.

The rest of the paper is organized as follows: In section 2 and section 3, we review and analyze, respectively, Lin et al.'s scheme; in Section 4, we propose an improved authentication scheme for multi-server environments; in section 5, we present a security analysis of our scheme; section 6 shows the functional and performance analyses whereby the proposed scheme is compared with previous schemes; and, our conclusion is presented in section 7.

2. Review of Lin et al.'s scheme

In this section, we review the biometric-based three factors user authentication scheme for multi-server environments by Lin et al. [14] in 2016. As previous researches, Lin et al. demonstrated the security weaknesses of Baruah et al.'s scheme [13], and proposed an enhanced biometric-based three factor user authentication scheme for multi-server environments using smart card. Lin et al.'s scheme used the fuzzy extractor technique [15] and it consists of four phases: registration, login, authentication, and password change phase which as follows. The notations used in this paper are summarized as Table 1.

Table 1 Notations used in this paper

Term	Description
U_i	The i^{th} user
ID_i	Identity of the i^{th} user
SID_j	Identity of the j^{th} server
RC	Registration center
PW_i	Password of the i^{th} user
BIO_i	Biometrics of the i^{th} user
PSK	Pre-shared key of the servers
y_i	Random number unique to user selected by RC
x	Master secret key maintained by the RC
$h(\cdot)$	A one way hash function
$\oplus$	Exclusive-OR operation
$\Vert$	Massage concatenation operation

2.1 Fuzzy extractor

The fuzzy extractor [15, 16] recovers the original biometric key data for a noisy biometric using public information and τ. Let $M=\{0,1\}^u$ be a finite u -dimensional metric space of biometric data points, $d: M\times M \rightarrow Z^+$ a distance function useful for computing the distance between any two points based on the chosen metric, the l bit-length of the output string, and the τ error tolerance parameter, where Z^+ is the set of all positive integers.

Definition 1. The fuzzy extractor is a tuple $\{M,\ l,\ \tau\}$, which is composed of the following two algorithms, called Gen and Rep.

Gen. This probabilistic algorithm takes a biometric information $B_i \in M$ as input and then outputs a secret key data $\sigma_i \in \{0,1\}^l$ and a public reproduction parameter σ_i, where $Gen(B_i) = \{\sigma_i,\ \tau_i\}$.

Rep. This deterministic algorithm takes a noisy biometric information $B_i' \in M$ and a public parameter σ_i and τ_i related to B_i, and then it reproduces (recovers) the biometric key data σ_i. In other words, we have $Rep(B_i, \tau_i) = \sigma_i$ provided that the condition $d(B_i,\ B_i') \le \tau$ is satisfied.

2.2 Registration phase

In Lin et al.'s scheme, the registration phase consists of two sub-phases, i.e. the user registration phase and the server registration phase. In this phase, the user and the server should register themselves to the registration center RC and obtains the secret information to initial the system.

User registration phase. The user must first register to the registration center RC if they want to access any services provided by the registered servers. Therefore, the user U_i first chooses an identity ID_i and a password PW_i, and imprints his/her biometric information BIO_i at the sensor device to obtains $Gen(BIO_i) = (R_i, P_i)$. Then, the user U_i sends the registration request message $\{ID_i, A_i = h(PW_i \| R_i), P_i\}$ to the registration center RC over a secure channel. The registration center RC hence computes:

$$B_i = h(ID_i \| A_i)$$
$$C_i = h(ID_i \| x)$$
$$D_i = h(PSK \| x) \oplus C_i$$
$$E_i = h(A_i \| ID_i) \oplus h(C_i)$$
$$F_i = h(PSK) \oplus A_i$$

The registration center RC stores the information $\{B_i, D_i, E_i, F_i, h(\cdot), P_i\}$ into the smart card and sends the smart card to the user U_i via a secure channel.

Server registration phase. When a server wants to provide some service to the public, then it has to first register itself to the registration center RC. The server sends a registration request along with its identity SID_j to the registration center RC. In return, the registration center RC replies with $h(SID_i \| h(PSK))$ and $h(PSK \| x)$ through the Internet Key Exchange Protocol version 2 (IKEv2) [17]. The server uses these secrets to authenticate any registered user.

2.3 Login phase

The user U_i must first login to a specific terminal using smart card SC_i. The user inserts his/her smart card into the card-reader and inputs his/her identity ID_i, password PW_i, and imprints the biometric information BIO_i' at the sensor with fuzzy extractor, and obtains $R_i' = Rep(BIO_i', P_i)$. The smart card SC_i then executes the following sequence of operations.

(1) The smart card SC_i computes $A_i' = h(PW_i \| R_i)$, $B_i' = h(ID_i \| A_i')$, and verifies whether B_i' is equal to B_i or not. If failure occurs, the login phase is immediately aborted. Otherwise, the following steps are executed.

(2) SC_i generates a nonce N_i and computes:

$$h(C_i) = E_i \oplus h(A_i \| ID_i)$$
$$C_i = h(ID_i \| x)$$
$$D_i = h(PSK \| x) \oplus C_i$$
$$E_i = h(A_i \| ID_i) \oplus h(C_i)$$
$$F_i = h(PSK) \oplus A_i$$

(3) Lastly, the smart card SC_i sends the login request message $\{M_1, M_2, M_3\}$ to the server SID_j over a public channel.

2.4 Authentication phase

After receiving the login request message, the server SID_j and the user U_i performs the following steps to authenticate each other and agree on a session key.

(1) SID_j computes:

$$N_i' = M_1 \oplus h(SID_j \| h(PSK))$$
$$C_i' = M_2 \oplus h(PSK \| x) \oplus N_i'$$
$$M_3' = h(h(C_i') \| N_i)$$

and whether M_3' is equal to M_3. If they are not equal, the session is terminated by the SID_j. Otherwise, the validity of U_i is authenticated by the server, and SID_j performs the following steps.

(2) SID_j generates a nonce N_j and computes:

$$SK_{ji} = h(h(C_i') \| SID_j \| N_i \| N_j)$$
$$M_4 = N_i \oplus N_j$$
$$M_5 = h(SK_{ji} \| N_j)$$

and sends the response message $\{M_4, M_5\}$ to the user U_i.

(3) When receiving the response message $\{M_4, M_5\}$, the U_i computes:

$$N_j' = M_4 \oplus N_i$$
$$SK_{ij} = h(h(C_i) \| SID_j \| N_i \| N_j')$$
$$M_5' = h(SK_{ji} \| N_j')$$

and checks whether M_5' is equal to received M_5. If they are not equal, the session is rejected. Otherwise, the U_i is authenticated by the server

SID_j, and they are share a common session key $SK_{ji}(=SK_{ij})$ at last.

2.5 Password change phase

If the user wants to change his/her password, it can be done without informing the registration center. After checking the entered information such as the identity ID_i, password PW_i and imprints the biometric BIO_i at the sensor with fuzzy extractor and obtains R_i from the $Rep(BIO_i', P_i)$. The smart card SC_i hence computes $A_i' = h(PW_i \| R_i)$, $B_i' = h(ID_i \| A_i')$, and verifies whether B_i' is equal to B_i or not. If failure occurs, the password change phase is immediately terminated. Otherwise, the user U_i can enter a new password PW_i^*, and then SC_i computes:

$$A_i^* = h(PW_i^* \| R_i)$$
$$B_i^* = h(ID_i \| A_i^*)$$
$$E_i = E_i \oplus h(A_i' \| ID_i) \oplus h(A_i^* \| ID_i)$$
$$F_i = F_i \oplus A_i' \oplus A_i^*$$

Lastly, SC_i replaces B_i, E_i, and F_i with B_i^*, E_i^*, and F_i^*, respectively, to finish the password change phase. Now, the smart card contains the information $\{B_i^*,\ D_i,\ E_i^*,\ F_i^*,\ h(\cdot),\ P_i\}$.

3. Security analysis of Lin et al.'s scheme

In this section, we demonstrate the vulnerability of Lin et al.'s scheme in various communication scenarios. The security analysis of Lin et al.'s scheme was conducted under the following four assumptions.

(1) An adversary A can be either a user or server. A registered user can act as an adversary.

(2) An adversary A can eavesdrop on every communication across public channels. He/she can capture any message that is exchanged between a user and a server.

(3) An adversary A has the ability to alter, delete, or reroute a captured message.

(4) Any information can be extracted from the smart card by examining the power consumption of the card.

3.1 Outsider attack

Any adversary U_a who is the legal user and owns a smart card obtain information $\{B_a,\ D_a,\ E_a,\ F_a,\ h(\cdot),\ P_a\}$, and then he/she can compute $h(PSK) = F_a \oplus A_a$. Thus, an adversary U_a can get $h(PSK)$ which same for each legal user and is the hash value of pre-shared key of the servers.

3.2 Stolen smart card and off-line identity guessing attack

If an outsider adversary U_a steals the smart card of legitimate user U_i and obtains the parameters $\{B_i,\ D_i,\ E_i,\ F_i,\ h(\cdot),\ P_i\}$, then he/she can perform an off-line identity guessing to get the current identity of the user U_i.

(1) The adversary calculates $A_i = F_i \oplus h(PSK)$.

(2) The adversary then selects a random identity ID_i^*, computes $h(ID_i^* \| A_i)$ and compares it with B_i. If the result is equal to B_i, the adversary infers that ID_i^* is the identity of the user U_i. Otherwise, the adversary selects another identity nominee, and then performs the same processes, until he/she locates the valid identity.

(3) After guessing the identity of user U_i, the adversary can compute $h(C_i) = E_i \oplus h(A_i \| ID_i)$

3.3 User impersonation attack

An outsider and smart card stolen adversary U_a can obtain values D_i, $h(C_i)$ from the smart card of the legitimate user U_i. He/she can then easily impersonate as user U_i to login and access the remote server, because he/she can compute $\{M_1,\ M_2,\ M_3\}$.

(1) The adversary randomly generates a nonce N_i^*.

(2) The adversary then calculates:

$$M_1 = h(SID_j \| h(PSK)) \oplus N_i^*$$
$$M_2 = D_i \oplus N_i^*$$
$$M_3 = h(h(C_i) \| N_i^*)$$

(3) After computing parameters, an adversary U_a sends the login request message to the server SID_j over a public channel for authentication.

3.4 Violation of the session key security

If an outsider adversary U_a intercepts all of the communication message between user U_i and server SID_j, and steals the smart card of legitimate user U_i, he/she then obtains all of the messages $\{M_1, M_2, M_3, M_4, M_5\}$ and the parameters $\{B_i, D_i, E_i, F_i, h(\cdot), P_i\}$; furthermore, he/she can get the value $h(C_i)$, and also easily compute the session key between user U_i and server SID_j. The details are described as follows:

(1) The adversary U_a computes:

$$N_i = M_1 \oplus h(SID_j \| h(PSK))$$
$$N_j = M_4 \oplus N_i$$

(2) After computing the parameters, an adversary $U_a$can easily obtain the common session key $SK_{ji} = h(h(C_i) \| SID_j \| N_i \| N_j)$.

4. The proposed scheme

In this section, we propose a new biometric-based three factors user authentication scheme for multi-server environments. Lin et al. used the fuzzy-extractor technique [15]. We also adopted the same technique to protect user's biometrics, which can also counter a high number of false rejections that therefore decreases the probability that service access is denied [18]. The proposed scheme consists of the following four phases: registration, login, authentication, and password changing.

4.1 Registration phase

In our scheme, the registration phase consists of two sub-phases as same as Lin et al.'s scheme, i.e. the user registration phase and the server registration phase. In this phase, the user and the server should register themselves to the registration center RC and obtains secret information to initial the system.

User registration phase. The user must first register to the registration center RC if they want to access any services provided by the registered servers. Therefore, the user U_i first chooses an identity ID_i and a password PW_i, and imprints his/her biometric information BIO_i at the sensor device to obtains $Gen(BIO_i) = (R_i, P_i)$. Then, the user U_i sends the user registration request message $\{ID_i$, $A_i = h(PW_i \| R_i)$ $P_i\}$to the RC over a secure channel. The RC then computes,

$$B_i = h(ID_i \| A_i)$$
$$C_i = h(ID_i \| x)$$
$$D_i = h(y_i \| PSK) \oplus A_i$$
$$E_i = h(A_i \| ID_i) \oplus C_i$$
$$F_i = y_i \oplus h(PSK \| x)$$

The registration center RC stores the information $\{B_i$, D_i, E_i, F_i, $h(\cdot)$, $P_i\}$ into the smart card and sends the smart card to the user U_i via a secure channel.

Server registration phase. When a server wants to provide some service to the public, then it has to first register itself to the registration center RC. The server sends a registration request along with its identity SID_j to the registration center RC. In return, the registration center RC replies with PSK and $h(PSK \| x)$ through the Internet Key Exchange Protocol version 2 (IKEv2) [17]. The server uses these secrets to authenticate any registered user.

4.2 Login phase

The user U_i must first login to a specific terminal using smart card SC_i. The user inserts his/her smart card into the card-reader and enters his/her identity ID_i and password PW_i, imprints the biometrics BIO_i' at the sensor, and obtains $R_i' = Rep(BIO_i', P_i)$ using the fuzzy extractor. The smart card SC_i then performs the following sequence of operations.

(1) The smart card SC_i computes $A_i' = h(PW_i \| R_i)$, $B_i' = h(ID_i \| A_i')$, and checks whether B_i' is equal to B_i or not. If this does not hold, the SC_i immediately rejects the login request; otherwise, the following steps are executed.

User U_i		Server SID_j
$\langle ID_i, PW_i, BIO_i \rangle$		$\langle PSK, \text{h(PSK}\|\|\text{x)} \rangle$
Input ID_i, PW_i Imprint biometric impression BIO_i $Gen(BIO_i) = (R_i, P_i)$, $A_i = h(PW_i\|\|R_i)$, $h(ID_i\|\|A_i) \stackrel{?}{=} B_i$ Generate N_i $C_i = E_i \oplus h(A_i\|\|ID_i)$, $h(y_i\|\|PSK) = D_i \oplus A_i$, $M_1 = h(SID_j\|\|h(y_i\|\|PSK)) \oplus N_i$, $M_2 = C_i \oplus h(y_i\|\|PSK) \oplus N_i$, $M_3 = h(C_i\|\|N_i)$		
	$\langle M_1, M_2, M_3, F_i \rangle$ →	
		$y_i = F_i \oplus h(PSK\|\|x)$ $N_i = M_1 \oplus h(SID_j\|\|h(y_i\|\|PSK))$, $C_i = M_2 \oplus h(y_i\|\|PSK) \oplus N_i$, $h(C_i\|\|N_i) \stackrel{?}{=} M_3$ Generate N_j $SK_{ji} = h(C_i\|\|h(y_i\|\|PSK)\|\|SID_j\|\|N_i\|\|N_j)$, $M_4 = N_i \oplus N_j$, $M_5 = h(SK_{ji}\|\|N_j)$
	← $\langle M_4, M_5 \rangle$	
$N_j = M_4 \oplus N_i$, $SK_{ij} = h(C_i\|\|h(y_i\|\|PSK)\|\|SID_j\|\|N_i\|\|N_j)$, $h(SK_{ij}\|\|N_j) \stackrel{?}{=} M_5$,		

Fig. 1 Login and authentication phase of the proposed scheme

(2) SC_i generates a random nonce N_i and computes:

$$C_i = E_i \oplus h(A_i \| ID_i)$$
$$h(y_i \| PSK) = D_i \oplus A_i'$$
$$M_1 = h(SID_j \| h(y_i \| PSK)) \oplus N_i$$
$$M_2 = C_i \oplus h(y_i \| PSK) \oplus N_i$$
$$M_3 = h(C_i \| N_i)$$

(3) Lastly, the smart card SC_i sends the login request message $\{M_1, M_2, M_3, F_i\}$ to the server SID_j over a public channel.

4.3 Authentication phase

When receiving the login request message, the server SID_j and the user U_i performs the following steps to authenticate each other and agree on a common session key.

(1) SID_j first computes:

$$y_i = F_i \oplus h(PSK \| x)$$
$$N_i = M_1 \oplus h(SID_j \| h(y_i \| PSK))$$
$$C_i' = N_2 \oplus h(y_i \| PSK) \oplus N_i$$
$$M_3' = h(C_i' \| N_i)$$

and whether M_3' is equal to the received M_3. If this does not hold, the SID_j terminates this session; otherwise, the SID_j authenticates the user U_i, and performs the following steps.

(2) SID_j generates a nonce N_j and computes:

$$SK_{ji} = h(C_i' \| h(y_i \| PSK) \| SID_j \| N_i \| N_j)$$
$$M_4 = N_i \oplus N_j$$
$$M_5 = h(SK_{ji} \| N_j)$$

and sends the response message $\{M_4,\ M_5\}$ to user U_i.

(3) Upon receiving the response message $\{M_4,\ M_5\}$, the U_i computes:

$$N_j' = M_4 \oplus N_i$$
$$SK_{ij} = h(C_i \| h(y_i \| PSK) \| SID_j \| N_i \| N_j')$$
$$M_5' = h(SK_{ji} \| N_j')$$

and checks whether M_5' is equal to received M_5. If this does not hold, the U_i terminates this session; otherwise, the U_i is authenticates the server SID_j, and the U_i and SID_j are share a common session key $SK_{ji}(=SK_{ij})$ at last.

4.4 Password change phase

If the user wants to change his/her password, it can be done without informing the registration center. After checking the entered information such as the identity ID_i, password PW_i and imprints the biometrics BIO_i at the sensor with fuzzy extractor and obtains R_i from the $Rep(BIO_i', P_i)$. The SC_i hence computes $A_i' = h(PW_i \| R_i)$, $B_i' = h(ID_i \| A_i')$, and checks whether B_i' is equal to the B_i or not. If this does not hold, the SC_i immediately terminates the password change phase; otherwise, the user U_i can enter a new password PW_i^*, and then SC_i computes:

$$A_i^* = h(PW_i^* \| R_i)$$
$$B_i^* = h(ID_i \| A_i^*)$$
$$D_i^* = D_i \oplus A_i' \oplus A_i^*$$
$$E_i^* = E_i \oplus h(A_i \| ID_i) \oplus h(A_i^* \| ID_i)$$

Lastly, SC_i replaces B_i, D_i, and E_i with B_i^*, D_i^*, and E_i^*, respectively, to finish the password change phase. Now, the smart card contains the information $\{B_i^*,\ D_i^*,\ E_i^*,\ F_i,\ h(\cdot),\ P_i\}$.

5. Security Analysis of the Proposed Scheme

In this section, we demonstrate that our scheme, which retains the merits of Lin et al.'s scheme, can withstand several types of possible attacks, and we also show that our scheme supports several security properties. The security analysis of the proposed scheme was conducted under the following four assumptions.

(1) An adversary A can be either a user or server. A registered user can act as an adversary.
(2) An adversary A can eavesdrop on every communication across public channels. He/she can capture any message that is exchanged between a user and a server.
(3) An adversary A has the ability to alter, delete, or reroute a captured message.
(4) Any information can be extracted from the smart card by examining the power consumption of the card.

5.1 Resisting the outsider attack

Suppose that an adversary U_a extracts all of the information $\{B_a,\ D_a,\ E_a,\ F_a,\ h(\cdot),\ P_a\}$ from a smart card by using side channel attack; however, he/she cannot obtain any of the secret information of SID_j. The U_a can compute $h(y_a \| PSK) = D_a \oplus A_a$, however the value y_a is a random number that is unique to the user that is selected by RC and PSK is the pre-shared secret key between the RC and SID_j; therefore, U_a does not know and the proposed scheme can resist an outsider attack.

5.2 Resisting the stolen smart card attack

Suppose that an adversary U_a steals the smart card of legitimate user U_i; then, he/she can extract all parameters $\{B_i,\ D_i,\ E_i,\ F_i,\ h(\cdot),\ P_i\}$ from the smart card by using the side channel attack [11], U_a, however, cannot obtain any of the secret information of U_i. The password PW_i is protected by the elements R_i that U_a does not know. The proposed scheme can therefore resist the smart card stolen attack.

5.3 Resisting the stolen smart card attack

Suppose that an adversary U_a can intercepts all of the messages $\{M_1,\ M_2,\ M_3,\ M_4,\ M_5\}$ that transmitted over a public channel between U_i and SID_j; however, U_a cannot generate the legal login request message $\{M_1, M_2, M_3, F_i\}$. This is because the value y_i is a random number that is selected by RC and is unique to user, and N_i is a random nonce that is generated by U_i. Furthermore, U_a cannot generate the login response message $\{M_4, M_5\}$ without the random nonce N_j. The proposed scheme can therefore resist the impersonation attack.

5.4 Session key agreement

Suppose that an adversary U_a intercepts all of the message $\{M_1, M_2, M_3, M_4, M_5\}$ that are transmitted over a public channel between U_i and SID_j, steals the smart card of U_i, and then extracts the all information $\{B_i, D_i, E_i, F_i, h(\cdot), P_i\}$; however, cannot compute the session key $SK_{ij} = h(C_i \| h(y_i \| PSK) \| SID_j \| N_i \| N_j')$. To compute N_i from the message M_1, the hash value $h(y_i \| PSK)$ is needed. To compute $h(y_i \| PSK)$ from D_i, the U_i's identity ID_i and biometric BIO_i are needed. To retrieve ID_i from B_i, needs to know PW_i and BIO_i. Since only U_i can imprint the biometrics BIO_i at the sensor, an adversary cannot attain the U_i's identity ID_i and PW_i. The proposed scheme can therefore provide session key security.

6. Functionality and performance analysis

In this section, we evaluate the functionality the computational costs comparisons between the proposed scheme and the other related schemes.

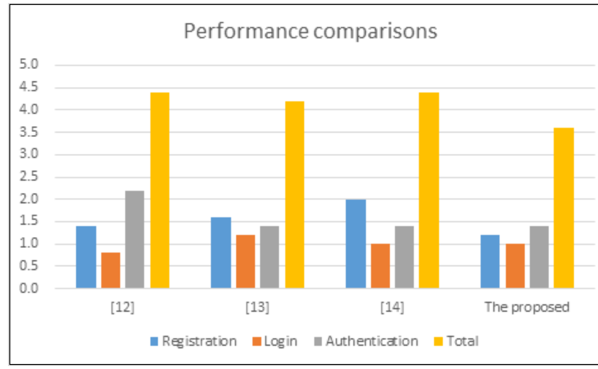

Fig. 2 Performance comparisons

6.1 Functionality analysis

Table 2 lists the functionality comparisons of the proposed scheme with the other related schemes. The table shows that the proposed scheme achieves all of the security and functionality requirements and is more secure than the other related schemes.

6.3 Performance analysis

For the performance comparison, the definition of T_H is the performance times of a hash function. Recently, Xue and Hong [19] estimated the running time of different cryptographic operations whereby T_H is below 0.2 ms on average in the environment (CPU: 3.2 GHz, Memory: 3.0 G). Fig. 2 shows a comparison of the computational costs of the proposed scheme with other related schemes. In the performance comparison, the proposed scheme requires a less amount of computation to accomplish mutual authentication and the key agreement than Lin et al.'s scheme as the proposed scheme performs four further hash

Table 2 Functionality comparisons

	Mishra et al. [12]	Baruah et al. [13]	Lin et al. [14]	The proposed
User anonymity	×	×	○	○
Mutual authentication	○	○	○	○
Without clock synchronization	○	○	○	○
Security of session key	○	×	×	○
Resist insider attack	○	○	○	○
Resist replay attack	×	×	×	○
Resist server spoofing attack	×	○	○	○
Resist stolen smart card attack	×	×	×	○
Resist user impersonation attack	×	×	×	○
Resist off-line password guessing attack	○	×	×	○
Resist denial of service attack	×	×	○	○

operations. Finally, our further research direction ought to propose a secure and efficient remote user authentication scheme.

7. Conclusion

In 2016, Lin et al. proposed a biometric-based three factors user authentication scheme based on Baruah et al.'s scheme and demonstrated its resistance to the typical attack types; however, we found that Lin et al.'s scheme is not secure against the outsider attack, the impersonation attack, and the stolen smart card attack, among others. In this paper, to solve these security vulnerabilities, we propose an improved authentication scheme for multi-server environments that maintains the merits of Lin et al.'s scheme and is more secure; furthermore, the computational cost of the proposed scheme is lower than that of Lin et al.'s scheme. The performed security analysis confirms that the proposed scheme rectifies the weaknesses of Lin et al.'s scheme.

감사의 글

This research was supported by the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Science, ICT, and Future Planning (2014R1A1A2002775)

References

[1] L. Lamport, "Password Authentication with Insecure Communication," Communication of the ACM, vol. 24, pp. 770-772, 1981.

[2] G. Conklin, G. Dietrich, and D. Walz, "Password-based Authentication:A System Perspective," System Sciences, vol. 50, pp. 629-631, 2004.

[3] M. Abdalla, P. Fouque, and D. Pointcheval, "Password-based Authenticated Key Exchange in the Three-Party Setting," On Public Key Gryptography-PKC 2005, vol. 3386, pp. 65-84, 2005.

[4] S. Jiang and G. Gong, "Password based Key Exchange with Mutual Authentication," Selected Areas in Cryptography, vol. 3357, pp. 267-279, 2005.

[5] R. Gennaro and Y. Lindell, "A framework for password-based authenticated key exchange," ACM Transactions on Information and System Security (TISSEC), vol. 9, pp. 181-234, 2006.

[6] J. Moon, Y. Choi, J. Jung, and D. Won, "An Improvement of Robust Biometrics-Based Authentication and Key Agreement Scheme for Multi-Server Environments Using Smart Cards," PLoS ONE, vol. 10, no. 12, pp. 1-15, 2015.

[7] Y.R. Lu, L.X. Li, H.P. Peng, and Y.X. Yang, "An Enhanced Biometric-Based Authentication Scheme for Telecare Medicine Information Systems using Elliptic Curve Cryptosystem," Journal of Medical Systems, vol. 39, no. 32, pp. 1-8, 2015.

[8] Y. Choi, Y. Lee, and D. Won, "Security Improvement on Biometric Based Authentication Scheme for Wireless Sensor Networks Using Fuzzy Extraction," International Journal of Distributed Sensor Networks, vol. 2016, pp. 1-16, 2016.

[9] C. Li and M. Hwang, "An Efficient Biometrics-based Remote User Authentication Scheme using Smart Card," Journal of Network and Computer Applications, vol. 33, pp. 1-5, 2010.

[10] X. Li, J. Niu, J. Ma, W. Wang, and C. Liu, "Cryptanalysis and Improvement of a Biometrics-based Remote User Authentication Scheme using Smart Cards," Journal of Network and Computer Applications, vol. 34, pp. 73-79, 2011.

[11] M.C. Chuang and M.C. Chen, "An Anonymous Multi-Server Authenticated Key Agreement Scheme based on Trust Computing using Smart Cards and Biometrics," Expert Systems with Applications, vol. 41, no. 4, pp. 1411-1418, 2014.

[12] D. Mishra, A.K. Das, and S. Mukhopadhyay, "A Secure User Anonymity-Preserving Biometric-based Multi-Server Authenticated Key Agreement Scheme using Smart Cards," Expert Systems with Applications, vol. 41, no. 18, pp. 8129-8143, 2014.

[13] K. C. Baruah, S. Banerjee, M. P. Dutta, and C. T. Bhunia, "An Improved Biometric-based Multi-Server Authentication Scheme using Smart Card," On Public Key Gryptography-PKC 2005, vol. 3386, pp. 65-84, 2005.

[14] Y. Lin, K. Wang, B. Zhang, Y. Liu, and X. Li, "An Enhanced Biometric-Based Three Factors User Authentication Scheme for Multi-server Environments," International Journal of Security and Its Applications, vol. 10, no. 1, pp. 315-328, 2016.

[15] Y. Dodis, L. Reyzin, and A. Smith, "Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data," Advances in Cryptology, vol. 3027, pp. 523-540, 2004.

[16] A.K. Das, "A Secure and Effective Biometric - based User Authentication Scheme for Wireless Sensor Networks

using Smart Card and Fuzzy Extractor," International Journal of Communication Systems, pp. 1-25, 2015.
[17] C. Kaufman, P. Hoffman, Y. Nir, P. Eronen, and T. Kivinen, "Internet key exchange protocol version 2 (IKEv2)" RFC 7236, 2014.
[18] A.K. Das and A. Goswami, "An Enhanced Biometric Authentication Scheme for Telecare Medicine Information Systems with Nonce using Chaotic Hash Function," Journal of Medical Systems, vol. 38, no. 6, pp. 1-19, 2014.
[19] K. Xue and P. Hong, "Security Improvement on an Anonymous Key Agreement Protocol based on Chaotic Maps," Communication Nonlinear Science Numerical Simulation, vol. 17, no. 7, pp. 2969-2977, 2012.

저 자 소 개

문 종 호(Jongho Moon)
2012년 2월 성균관대학교 전자전기컴퓨터공학과(공학사). 2014년 2월 성균관대학교 전자전기컴퓨터공학과(공학석사). 2014년 1월~2015년 2월 (주)시큐아이 보안서비스개발팀 연구원. 2015년 3월~현재 성균관대학교 전자전기컴퓨터공학과 박사과정. 관심분야는 정보보호, 사용자 인증, 악성코드 분석 등

원 동 호(Dongho Won)
1976년~1988년 성균관대학교 전자공학과(공학사, 공학석사, 공학박사). 1978년~1980년 한국전자통신연구원 전임연구원 1985년~1986년 일본 동경공업대학교 객원연구원. 1996년~1998년 국무총리실 정보화추진위원회 자문위원. 2002년~2003년 한국정보보호학회장. 1982년~현재 성균관대학교 컴퓨터공학과 교수. 現 성균관대학교 행단석좌교수, 한국정보보호학회 명예회장. 관심분야는 정보보호, 암호이론, 정보이론 등