RESEARCH ARTICLE

An Improvement of Robust Biometrics-Based Authentication and Key Agreement Scheme for Multi-Server Environments Using Smart Cards

Jongho Moon, Younsung Choi, Jaewook Jung, Dongho Won*

Department of Computer Engineering, Sungkyunkwan University, Suwon, Gyeonggido 16419, Korea

* dhwon@security.re.kr

Abstract

In multi-server environments, user authentication is a very important issue because it provides the authorization that enables users to access their data and services; furthermore, remote user authentication schemes for multi-server environments have solved the problem that has arisen from user's management of different identities and passwords. For this reason, numerous user authentication schemes that are designed for multi-server environments have been proposed over recent years. In 2015, Lu et al. improved upon Mishra et al.'s scheme, claiming that their remote user authentication scheme is more secure and practical; however, we found that Lu et al.'s scheme is still insecure and incorrect. In this paper, we demonstrate that Lu et al.'s scheme is vulnerable to outsider attack and user impersonation attack, and we propose a new biometrics-based scheme for authentication and key agreement that can be used in multi-server environments; then, we show that our proposed scheme is more secure and supports the required security properties.

Citation: Moon J, Choi Y, Jung J, Won D (2015) An Improvement of Robust Biometrics-Based Authentication and Key Agreement Scheme for Multi-Server Environments Using Smart Cards. PLoS ONE 10(12): e0145263. doi:10.1371/journal.pone.0145263

Editor: Yongtang Shi, Nankai University, CHINA

Received: June 2, 2015

Accepted: November 30, 2015

Published: December 28, 2015

Data Availability Statement: All relevant data are within the paper.

Funding: 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) (http://www.nrf.re.kr/nrf_eng_cms/). The funders had no role in study design, data collection and analysis, decision to publish, or preparation of the manuscript.

Competing Interests: The authors have declared that no competing interests exist.

Introduction

Since Lamport [1] proposed the first password-based authentication scheme for insecure communications in 1981, password-based authentication schemes [2–6] have been extensively investigated. The remote user authentication scheme is one of the most convenient authentication schemes for dealing with the transmission of secret data over insecure communication channels, and during the last two decades, many researchers have proposed different remote user authentication schemes.

A problem that occurs with respect to password-based authentication schemes, however, is that a server must maintain a password table for the verification of the legitimacy of a login user; therefore, the server requires additional memory space to store the password table. For this reason, many researchers have proposed a new type of remote user authentication scheme whereby the biological characteristics of persons such as a fingerprint or an iris are used. The main advantageous property of biometrics is uniqueness, leading to the proposal of numerous remote user authentication schemes [7–13] that use biological characteristics. In 2008, Tsai [14] proposed an efficient multi-server authentication scheme using a random number and the one-way hash function; after that, a considerable succession of authenticated key agreement schemes was presented for multi-server environments [15–17]. In 2012, Li et al. [18] proposed a novel authenticated key exchange scheme for multi-server environments; unfortunately, however, Xue et al. [19] found that Li et al.'s scheme did not resist some types of known attacks such as replay, denial of service, forgery, and off-line password guessing. Xue et al. therefore proposed an improved scheme to remedy the weaknesses of Li et al.'s scheme; nevertheless, Lu et al. [20] showed that Xue et al.'s scheme is not only very insecure against impersonation and insider attacks, but that it is also vulnerable to off-line password guessing attack. To overcome the vulnerability of Xue et al.'s scheme, Lu et al. then proposed a slightly modified authentication scheme for multi-server environments. Recently, Chuang et al. [21] presented an efficient, biometrics-based, smart card authentication scheme for a multi-server environment that was previously considered as one that comprises more security properties; however, Mishra et al. [22] found that Chuang et al.'s scheme is vulnerable to a stolen smart card, server spoofing, and impersonation attacks. Mishra et al. also proposed an improved biometrics-based, multi-server authenticated key agreement scheme for which smart cards are used, and they claimed that their scheme satisfied all of the desirable security requirements; unfortunately, Lu et al. [23] showed that Mishra et al.'s scheme did not satisfy key security attributes including replay attack and the incorrect password change phase. Lu et al. then proposed a biometrics-based smart card scheme for authentication and key agreement that can be used in multi-server environments, claiming that their scheme is secure against a variety of known attacks; however, we found that Lu et al.'s scheme is still insecure and is incorrect regarding the login and authentication phase.

In this paper, we concentrate on the security weaknesses of Lu et al.'s biometrics-based authentication scheme. After a careful analysis, we found that their scheme does not effectively resist outsider and impersonation attacks; to resolve 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, Lu 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 security and performance analyses whereby our scheme is compared with previous schemes; and, our conclusion is presented in section 7.

Review of Lu et al.'s scheme

In this section, we will review Lu et al.'s biometrics-based scheme for authentication and key agreement that can be used in a multi-server environment. The following three participants are involved: the user U_i, the server S_j, and the registration center RC. The RC chooses a secret key PSK and a secret number x and shares them with S_j over a secure channel. The scheme consists of the registration, login and authentication, and password updating. For convenience, some of the notations that are used in Lu et al.'s scheme are described in Table 1.

Registration

1. U_i enters his/her biometrics BIO_i, identity ID_i and password PW_i; then, U_i sends $\{ID_i, h(PW_i \| H(BIO_i))\}$ to the RC.

Table 1. Notations used in Lu et al.'s scheme.

U_i, S_j	User and a server
RC	The registration center
ID_i, SID_j	Identity of U_i and S_j
PW_i, BIO_i	Password and a biometrics of U_i
x, y	Secret number selected by the RC and U_i
PSK	Secure key shared by the RC and S_j
T	Timestamp
$h(\cdot)$	One-way hash function
$H(\cdot)$	Biohash function
$\oplus$, $\|$	Exclusive-or operation and concatenation operation

doi:10.1371/journal.pone.0145263.t001

2. After receiving the message from U_i, the RC computes $X_i = h(ID_i \| x)$, $V_i = h(ID_i \| h(PW_i \| H(BIO_i)))$; then, the RC stores $\{X_i, V_i, h(PSK)\}$ onto a smart card and submits them to U_i.
3. U_i computes $Y_i = h(PSK) \oplus y$, and replaces $h(PSK)$ with Y_i, lastly, the smart card stores the values of $\{X_i, Y_i, V_i, h(\cdot)\}$.

Login and authentication

1. U_i inserts his/her smart card into the device and enters his/her identity ID_i, password PW_i and biometrics BIO_i; then, the smart card validates whether $V_i' = h(ID_i \| h(PW_i \| H(BIO_i)))$ is equal to the stored V_i; if validation occurs, the smart card generates a random number n_1 and computes $K = h((Y_i \oplus y) \| SID_j)$, $M_1 = K \oplus ID_i$, $M_2 = n_1 \oplus K$, $M_3 = h(PW_i \| H(BIO_i)) \oplus K$, and $Z_i = h(X_i \| n_1 \| h(PW_i \| H(BIO_i)) \| T_1)$. Lastly, U_i sends $\{Z_i, M_1, M_2, M_3, T_1\}$ to S_j over a public channel, where T_1 is the current timestamp.
2. After receiving the message from U_i, S_j first checks whether $T_c - T_1 \leq \triangle T$ and then computes $K = h(SID_j \| h(PSK))$ by using a secure pre-shared key PSK; then S_j retrieves $ID_i = M_1 \oplus K$, $n_1 = M_2 \oplus K$, $h(PW_i \| H(BIO_i)) = M_3 \oplus K$. S_j subsequently computes $X_i = h(ID_i \| x)$ and verifies whether $h(X_i \| n_1 \| h(PW_i \| H(BIO_i)) \| T_1) \overset{?}{=} Z_i$; if it holds, S_j generates a random number n_2 and computes $SK_{ji} = h(n_1 \| n_2 \| K \| X_i)$, $M_4 = n_2 \oplus h(n_1 \| h(PW_i \| H(BIO_i)) \| X_i)$, and $M_5 = h(ID_i \| n_1 \| n_2 \| K \| T_2)$. Then, S_j sends back the authentication message $\{M_4, M_5, T_2\}$ to U_i, where T_2 is the current timestamp.
3. Upon checking the freshness of T_2, U_i first computes $n_2 = M_4 \oplus h(n_1 \| h(PW_i \| H(BIO_i)) \| X_i)$ and then verifies whether $h(ID_i \| n_1 \| n_2 \| K \| T_2)$ is equal to the received M_5; if they are equal, U_i computes the common session key $SK_{ij} = h(n_1 \| n_2 \| K \| X_i)$ and sends $\{M_6 = h(SK_{ij} \| ID_i \| n_2 \| T_3), T_3\}$ to S_j, where T_3 is the current timestamp.
4. S_j verifies the freshness of T_3 and the correctness of M_6 by using SK_{ji}, and if they do not hold, S_j stops the execution; otherwise, S_j confirms the common session key SK_{ji} with U_i.

Password updating

U_i first inputs his/her smart card into the device and provides his/her identity ID_i, password PW_i and biometrics BIO_i. The smart card then validates whether $V_i' = h(ID_i \| h(PW_i \| H(BIO_i)))$ is equal to the stored V_i; if they are equal, U_i keys in the new password $PW_{i(new)}$, but otherwise the smart card refuses the request. Lastly, the smart card computes $V_{i(new)} = h(ID_i \| h(PW_{i(new)} \| H(BIO_i)))$ and replaces V_i by $V_{i(new)}$.

Security analysis of Lu et al.'s scheme

According to [24, 25], in the basic adversary model, a probabilistic polynomial-time (PPT) adversary $\mathcal{A}$ can have a full control over all communication messages. The adversary $\mathcal{A}$ then can read, modify or delete all communication messages transmitted between a user and the server. Furthermore, power analysis attacks [26] can extract all of the information from the smart card by using the side channel attack. Lu et al. claimed that their scheme could resist a session-key attack; however, we demonstrated that their scheme is still insecure against a session key attack. We also found that their scheme is unable to provide protection against outsider and user impersonation attacks, and it cannot support user anonymity; furthermore, a number of the phases of Lu et al.'s scheme are not correct and we point out the details of these problems in the following subsections.

Incorrect login phase

During the login phase, the user U_i inserts his/her smart card into the card reader, inputs his/her identity ID_i, password PW_i, and then imprints his/her biometrics BIO_i at the sensor. The smart card then validates whether $V_i' = h(ID_i \| h(PW_i \| H(BIO_i)))$ is equal to the stored V_i; if it holds, the smart card should compute $K = h((Y_i \oplus y) \| SID_j)$, but this is actually impossible because the secret key y does not exist in the smart card. Lu et al. claimed that even if an adversary $\mathcal{A}$ has gathered the information $\{X_i,Y_i,V_i,h(\cdot)\}$ that is stored in U_i's smart card, $\mathcal{A}$ cannot figure out the login request message $\{Z_i,M_1,M_2,M_3,T_1\}$ without the secret key y; therefore, we assumed that the secret key y is entered by user U_i during the login process.

Incorrect authentication phase

During the authentication phase, the server S_j computes $K = h(SID_j \| h(PSK))$ by using a secure pre-shared key PSK; however, the value $K = h(SID_j \| h(PSK))$ cannot be made equal to $K = h((Y_i \oplus y) \| SID_j) = h(h(PSK) \| SID_j)$ by computing U_i. We therefore assumed that server S_j computes $K = h(h(PSK) \| SID_j))$.

Outsider Attack

During the registration phase, the RC stores $\{X_i,V_i,h(PSK)\}$ onto a smart card and submits them to U_i. After receiving the smart card, U_i computes $Y_i = h(PSK) \oplus y$, and replaces $h(PSK)$ with Y_i. Let $\mathcal{A}$ who is in possession of the smart card extracted information $\{X_{\mathcal{A}}, V_{\mathcal{A}}, h(PSK)\}$, be an active adversary of the legal user; then, $\mathcal{A}$ can easily compute $K = h(h(PSK) \| SID_j)$ that is the same for each legal user that belongs in the server S_j. Furthermore, if $\mathcal{A}$ intercepts his/her own login request message $\{Z_{\mathcal{A}}, M_1, M_2, M_3, T_1\}$, then $\mathcal{A}$ can also compute $K = M_3 \oplus h(PW_{\mathcal{A}} \| H(BIO_{\mathcal{A}}))$.

Violation of the Session Key Security

Suppose an outsider adversary $\mathcal{A}$ intercepts the communication between U_i and S_j and steals the smart card of U_i; then, he/she can obtain all of the messages $\{Z_i,M_1,M_2,M_3,M_4,M_5,M_6,T_1,T_2,T_3\}$ and extract the information $\{X_i,Y_i,V_i,h(\cdot)\}$, thereby easily obtaining the session key that is transmitted between U_i and S_j. The details are described as follows.

1. $\mathcal{A}$ computes $n_1 = M_2 \oplus K$, $ID_i = K \oplus M_1$, and $h(PW_i \| H(BIO_i)) = M_3 \oplus K$.

2. Then, $\mathcal{A}$ can compute $n_2 = M_4 \oplus h(n_1 \| h(PW_i \| H(BIO_i)) \| X_i)$; therefore, $\mathcal{A}$ can obtain the session key $SK_{ij} = h(n_1 \| n_2 \| K \| X_i)$.

User Impersonation Attack

As described in this subsection, $\mathcal{A}$ can also impersonate as a legal user to cheat S_j when he/she knows the value of K. The details are described as follows.

1. $\mathcal{A}$ generates a random number n'_1 and computes $M_1 = K \oplus ID_i$, $M_2 = n'_1 \oplus K$, $M_3 = K \oplus h(PW_i \| H(BIO_i))$ and $Z_i = h(X_i \| n'_1 \| h(PW_i \| H(BIO_i)) \| T'_1)$; then, $\mathcal{A}$ sends the login request message $\{Z_i, M_1, M_2, M_3, T'_1\}$ to server S_j, where T'_1 is the current timestamp.
2. After receiving the login request message from $\mathcal{A}$ who pretends to be U_i, the message can successfully pass S_j's verification and S_j performs the subsequent scheme normally. Lastly, S_j sends the authenticated message $\{M_4, M_5, T'_2\}$ to $\mathcal{A}$, where n'_2 and T'_2 are the random number and the current timestamp on the server side, respectively.
3. Upon receiving the login response message from S_j, $\mathcal{A}$ computes $n'_2 = M_4 \oplus h(n'_1 || h(PW_i || H(BIO_i)) || X_i)$, $SK_{ij} = h(n'_1 \| n'_2 \| K \| X_i)$, and $M_6 = h(SK_{ij} \| ID_i \| n'_2 \| T'_3)$, and sends the message $\{M_6, T'_3\}$ to S_j, where T'_3 is the current timestamp.
4. Upon receiving the message from $\mathcal{A}$, S_j continues to proceed with the scheme without detection. Lastly, $\mathcal{A}$ and S_j "successfully" agree on the session key SK_{ij}, but unfortunately S_j mistakenly believes that he/she is communicating with the legitimate, genuine U_i.

User is not anonymous

Lu et al. claimed that U_i's identity ID_i is well protected by the shared parameter K that is used as a substitute for the actual parameters. Additionally, an unauthorized server cannot obtain ID_i without knowing K, since K is protected by a secret key PSK that is only known by the authorized server and is not exposed on the open channel. We found, however, that if the outsider adversary $\mathcal{A}$ can obtain $h(PSK)$, then he/she can compute $K = h(h(PSK) \| SID_j)$; furthermore, $\mathcal{A}$ can also compute $K = M_3 \oplus h(PW_{\mathcal{A}} \| H(BIO_{\mathcal{A}}))$ without $h(PSK)$, meaning that $\mathcal{A}$ can compute $ID_i = M_1 \oplus K$. We therefore concluded that Lu et al.'s scheme cannot provide user anonymity.

Our proposed scheme

In this section, we will propose a new biometrics-based password authentication scheme for multi-server environments. In our scheme, there are also three participants, as follows: the user U_i, the server S_j, and the registration center RC. The RC chooses a secret key PSK and a secret number x, and then shares them with S_j over a secure channel. Our proposed scheme consists of the following four phases as shown in Fig 1: registration, login, authentication, and password changing. For convenience, some of the notations that are used in our proposed scheme are described in Table 2.

Registration phase

1. U_i inputs his/her biometrics BIO_i and selects an identity ID_i and a password PW_i. Then, U_i computes $PWD_i = h(PW_i \| H(BIO_i))$ and sends $\{ID_i, PWD_i\}$ to the RC.

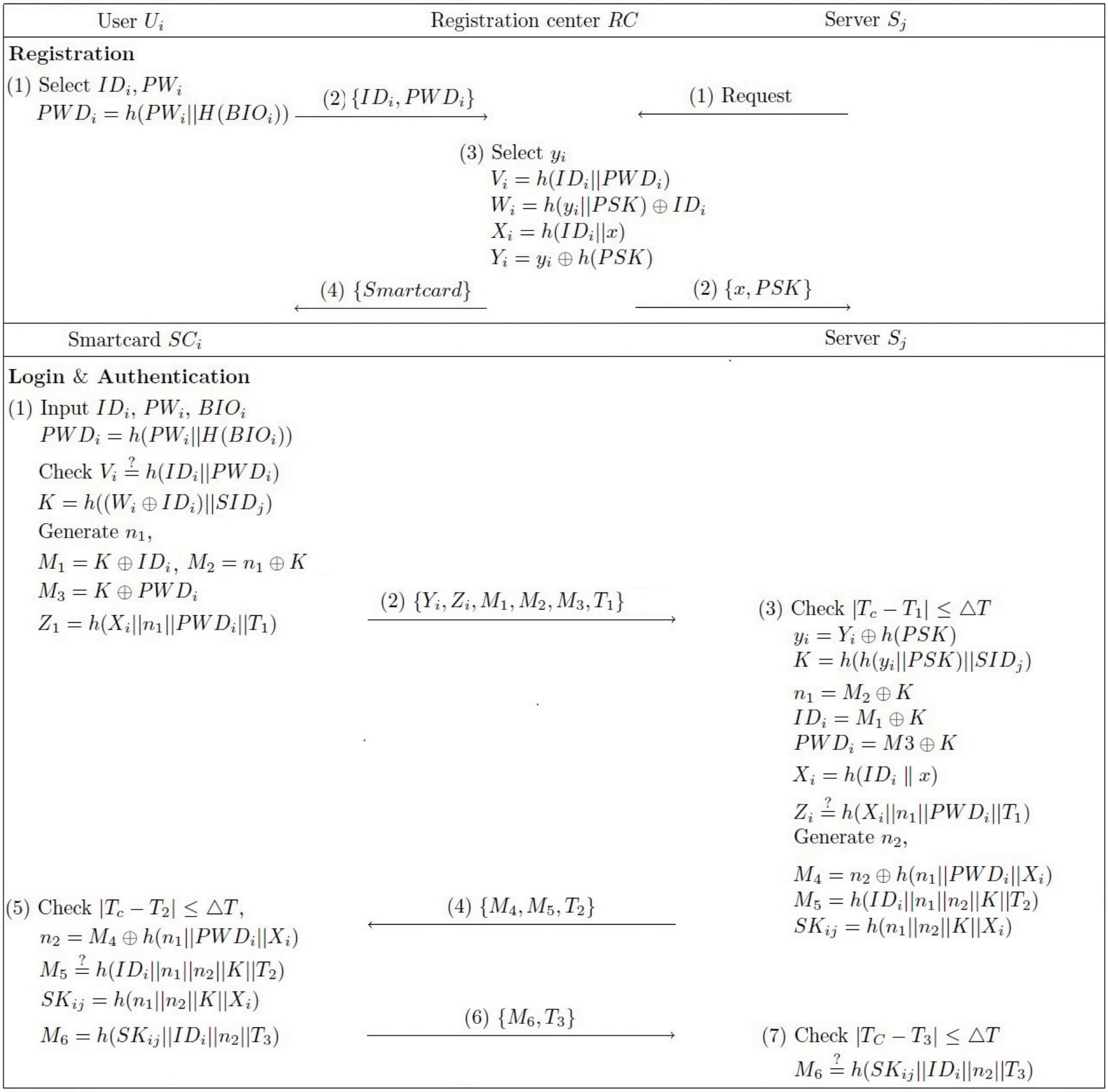

Fig 1. Our proposed authentication and key agreement protocol for multi-server environments.

doi:10.1371/journal.pone.0145263.g001

2. After receiving the registration request message from U_i, the RC generates a random number y_i that is unique to U_i. Then, the RC computes $V_i = h(ID_i \parallel PWD_i)$, $W_i = h(y_i \parallel PSK) \oplus ID_i$, $X_i = h(ID_i \parallel x)$, and $Y_i = y_i \oplus h(PSK)$, followed by the storage of $\{V_i, W_i, X_i, Y_i, h(\cdot), H(\cdot)\}$ by the RC onto a smart card and the submission of them to U_i.

Table 2. Notations used in our proposed scheme.

U_i	The i^{th} user
S_j	The j^{th} server
SC_i	The smart card of the i^{th} user
RC	The registration center
ID_i	Identity of the i^{th} user
SID_j	Identity of the j^{th} server
PW_i	Password of the i^{th} user
BIO_i	Biometrics of the i^{th} user
x	A secret number selected by RC
y_i	A random number unique to user selected by RC
PSK	Secure key pre-shared by RC and S_j
T	A timestamp
$h(\cdot)$	A one-way hash function
$H(\cdot)$	Biohash function
$\oplus$, $\|$	Exclusive-or operation and concatenation operation

doi:10.1371/journal.pone.0145263.t002

3. The RC sends the smart card SC_i to U_i over a secure channel and the registration phase is therefore complete.

Login phase

1. U_i inserts his/her smart card into the card reader and enters identity ID_i, password PW_i and imprints biometrics BIO_i; then, the smart card SC_i computes $PWD_i = h(PW_i \| H(BIO_i))$ to validate whether $V_i' = h(ID_i \| PWD_i)$ is equal to the stored V_i. If it holds, the smart card generates a random number n_1 and computes $K = h((W_i \oplus ID_i) \| SID_j)$, $M_1 = K \oplus ID_i$, $M_2 = n_1 \oplus K$, $M_3 = PWD_i \oplus K$, and $Z_i = h(X_i \| n_1 \| PWD_i \| T_1)$.
2. U_i then sends $\{Y_i, Z_i, M_1, M_2, M_3, T_1\}$ to S_j over a public channel, where T_1 is the current timestamp.

Authentication phase

1. After receiving the login request message from U_i, S_j first checks whether $T_c - T_1 \leq \triangle T$ so that it can then compute $y_i = Y_i \oplus h(PSK)$ by using a secure pre-shared key PSK; then, S_j computes $K = h(h(y_i \| PSK) \| SID_j)$, $ID_i = M_1 \oplus K$, $n_1 = M_2 \oplus K$, and $PWD_i = M_3 \oplus K$.

   Next, S_j computes $X_i = h(ID_i \| x)$ and verifies whether $h(X_i \| n_1 \| PWD_i \| T_1) \overset{?}{=} Z_i$. If it holds, S_j generates a random number n_2 and computes $SK_{ji} = h(n_1 \| n_2 \| K \| X_i)$, $M_4 = n_2 \oplus h(n_1 \| PWD_i \| X_i)$, and $M_5 = h(ID_i \| n_1 \| n_2 \| K \| T_2)$. Then, S_j sends the login response message $\{M_4, M_5, T_2\}$ to U_i where T_2 is the current timestamp.
2. Upon checking the freshness of T_2, U_i first computes $n_2 = M_4 \oplus h(n_1 \| PWD_i \| X_i)$ and then verifies whether $h(ID_i \| n_1 \| n_2 \| K \| T_2)$ is equal to the received M_5. If they are equal, U_i computes the common session key $SK_{ij} = h(n_1 \| n_2 \| K \| X_i)$ and sends $\{M_6 = h(SK_{ij} \| ID_i \| n_2 \| T_3), T_3\}$ to S_j, where T_3 is the current timestamp.
3. S_j verifies the freshness T_3 and the correctness of M_6 by using SK_{ji}; if they hold, S_j confirms the common session key SK_{ji} with U_i, but otherwise, S_j terminates this session.

Password updating

The password change is done locally without the involvement of the RC. If U_i wants to change his/her password, he/she first inserts his/her smart card into a card reader and provides his/her identity ID_i, password PW_i and biometrics BIO_i. The smart card SC_i then computes $PWD_i = h(PW_i \| H(BIO_i))$ to validate whether $V_i' = h(ID_i \| PWD_i)$ is equal to the stored V_i. If they are equal, SC_i accepts U_i to enter a new password $PW_{i(new)}$, but otherwise, the smart card rejects the password changing request. Lastly, SC_i computes $PWD_{i(new)} = h(PW_{i(new)} \| H(BIO_i))$, and $V_{i(new)} = h(ID_i \| PWD_{i(new)})$, and replaces V_i with $V_{i(new)}$.

Security analysis of our proposed scheme

In this section, we demonstrate that our scheme, which retains the merits of Lu 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 our proposed scheme was conducted under the following four assumptions:

1. An adversary $\mathcal{A}$ can be either a user or a server. A registered user as well as a registered server can act as an adversary.
2. An adversary $\mathcal{A}$ 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 $\mathcal{A}$ has the ability to alter, delete, or reroute a captured message.
4. Information can be extracted from the a smart card by examining the power consumption of the card.

Verifying the authentication scheme with BAN logic

Burrows-Abadi-Needham(BAN) logic [27] is a set of rules for the definition and analysis of information exchange protocols. Concretely, BAN logic helps its users to decide whether exchanged information is trustworthy, whether it is secured against eavesdropping, or both. In this subsection, we use BAN logic to prove that a shared session key between a user and a server can be correctly generated during the authentication process. Some of the notations and logical postulates [28] that are used in the BAN logic are described in Table 3.

Table 3. Notations used in BAN Logic.

$\mathcal{P} \| \equiv \mathcal{X}$	The principal $\mathcal{P}$ believes the statement $\mathcal{X}$.
$\#(\mathcal{X})$	The formula $\mathcal{X}$ is fresh.
$\mathcal{P} \Rightarrow \mathcal{X}$	The principal $\mathcal{P}$ has jurisdiction over the statement $\mathcal{X}$.
$\mathcal{P} \overset{K}{\leftrightarrow} \mathcal{Q}$	The principals $\mathcal{P}$ and $\mathcal{Q}$ may use the shared key $\mathcal{K}$.
$\mathcal{P} \triangleleft \mathcal{X}$	The principal $\mathcal{P}$ sees the statement $\mathcal{X}$.
$\mathcal{P} \| \sim \mathcal{X}$	The principal $\mathcal{P}$ once said the statement $\mathcal{X}$.
$\{\mathcal{X}\}_{\mathcal{K}}$	The formula $\mathcal{X}$ encrypted under the key $\mathcal{K}$.
$(\mathcal{X})_{\mathcal{K}}$	The formula $\mathcal{X}$ hashed under the key $\mathcal{K}$.
$\langle\mathcal{X}\rangle_{\mathcal{Y}}$	The formula $\mathcal{X}$ combined with the key $\mathcal{Y}$.
$\mathcal{P} \overset{\mathcal{X}}{\Leftrightarrow} \mathcal{Q}$	The formula $\mathcal{X}$ is a secret known only to P and Q.

doi:10.1371/journal.pone.0145263.t003

1. BAN logical postulates

    a. Message-meaning rule: $\frac{\mathcal{P}|\equiv\mathcal{P}\overset{\mathcal{K}}{\leftrightarrow}\mathcal{Q},\mathcal{P}\lhd\{\mathcal{X}\}_{\mathcal{K}}}{\mathcal{P}|\equiv\mathcal{Q}|\sim\mathcal{X}}$: If principal $\mathcal{P}$ believes that he/she shares the secret key $\mathcal{K}$ with $\mathcal{Q}$, and $\mathcal{P}$ sees the statement $\mathcal{X}$ encrypted under $\mathcal{K}$. Then $\mathcal{P}$ believes that $\mathcal{Q}$ once said $\mathcal{X}$.

    b. Nonce-verification rule: $\frac{\mathcal{P}|\equiv\#(\mathcal{X}),\mathcal{P}|\equiv\mathcal{Q}|\sim\mathcal{X}}{\mathcal{P}|\equiv\mathcal{Q}|\equiv\mathcal{X}}$: If principal $\mathcal{P}$ believes that $\mathcal{X}$ is fresh and $\mathcal{P}$ believes that $\mathcal{Q}$ once said $\mathcal{X}$, then $\mathcal{P}$ believes that $\mathcal{Q}$ believes $\mathcal{X}$.

    c. The belief rule: $\frac{\mathcal{P}|\equiv\mathcal{X},\mathcal{P}|\equiv\mathcal{Y}}{\mathcal{P}|\equiv(\mathcal{X},\mathcal{Y})}$: If principle $\mathcal{P}$ believes $\mathcal{X}$ and $\mathcal{Y}$, then $\mathcal{P}$ believes $(\mathcal{X},\mathcal{Y})$.

    d. Freshness-conjuncatenation rule: $\frac{\mathcal{P}|\equiv(\mathcal{X})}{\mathcal{P}|\equiv(\mathcal{X},\mathcal{Y})}$: If principle $\mathcal{P}$ believes that $\mathcal{X}$ is fresh, then $\mathcal{P}$ believes $(\mathcal{X},\mathcal{Y})$ is fresh.

    e. Jurisdiction rule: $\frac{\mathcal{P}|\equiv\mathcal{Q}|\Rightarrow\mathcal{X},\mathcal{P}|\equiv\mathcal{Q}|\equiv\mathcal{X}}{\mathcal{P}|\equiv\mathcal{X}}$: If principle $\mathcal{P}$ believes that $\mathcal{Q}$ has jurisdiction over $\mathcal{X}$ and $\mathcal{P}$ believes that $\mathcal{Q}$ believes $\mathcal{X}$, then $\mathcal{P}$ believes $\mathcal{X}$.

2. Idealized scheme

    U_i: $\langle y_i\rangle_{h(PSK)}$, $\langle n_1,ID_i,PWD_i\rangle_K$, $(n_1,X_i,T_1)_{PWD_i}$, $(n_2, U_i \overset{SK_{ij}}{\longleftrightarrow} S_j, T_3)_{ID_i}$

    S_j: $\langle n_1,X_i,PWD_i\rangle_{n_2}$, $(ID_i,n_1,n_2,T_2)_K$

3. Establishment of security goals

    g_1. $S_j| \equiv U_i| \equiv U_i \overset{SK_{ij}}{\longleftrightarrow} S_j$

    g_2. $S_j| \equiv U_i \overset{SK_{ij}}{\longleftrightarrow} S_j$

    g_3. $U_i| \equiv S_j| \equiv U_i \overset{SK_{ij}}{\longleftrightarrow} S_j$

    g_4. $U_i| \equiv U_i| \overset{SK_{ij}}{\longleftrightarrow} S_j$

4. Initiative premises

    p_1. $U_i \mid \equiv \#n_1$, p_2. $U_i \mid \equiv S_j \Rightarrow \#n_2$, p_3. $S_j \mid \equiv \#n_1$, p_4. $S_j \mid \equiv \#n_2$,

    p_5. $S_j \mid \equiv U_i \overset{K}{\leftrightarrow} S_j$, p_6. $U_i \mid \equiv U_i \overset{K}{\leftrightarrow} S_j$, p_7. $U_i \mid \equiv ID_i$,

    p_8. $S_j \mid \equiv U_i \Rightarrow PWD_i$, p_9. $S_j \mid \equiv U_i \Rightarrow ID_i$, p_{10}. $U_i \mid \equiv S_j \Rightarrow X_i$,

    p_{11}. $S_j \mid \equiv U_i \Rightarrow U_i \overset{SK_{ij}}{\longleftrightarrow} S_j$, p_{12}. $U_i \mid \equiv S_j \Rightarrow U_i \overset{SK_{ij}}{\longleftrightarrow} S_j$

5. Our proposed scheme analysis

    a_1. By p_5, $S_j \lhd \langle y_i\rangle_{h(PSK)}$, and $S_j \lhd \langle n_i,ID_i,PWD_i\rangle_K$, we apply the message-meaning rule to drive: $S_j \mid \equiv U_i| \sim (n_1,ID_i,PWD_i)$

    a_2. By a_1 and p_3, we apply the fresh conjuncatenation rule and the nonce-verification rule to derive: $S_j \mid \equiv U_i \mid \equiv (n_1,ID_i,PWD_i)$

    a_3. By a_2, p_3 and p_8, we apply the belief rule and the jurisdiction rule to derive: $S_j \mid \equiv ID_i$

a_4. By a_3 and $S_j \triangleleft (n_2, U_i \xleftrightarrow{SK_{ij}} S_j, T_3)_{ID_i}$, we apply the message-meaning rule to derive: $S_j \mid\equiv U_i \mid\sim (n_2, U_i \xleftrightarrow{SK_{ij}} S_j, T_3)$

a_5. By p_4 and a_4, we apply the fresh conjuncatenation rule and the nonce-verification rule to drive: $S_j \mid\equiv U_i \mid\equiv (n_2, U_i \xleftrightarrow{SK_{ij}} S_j, T_3)$

g_1. By a_5, we apply the belief rule to derive: $S_j \mid\equiv U_i \mid\equiv U_i \xleftrightarrow{SK_{ij}} S_j$

g_2. By g_1 and p_1, we apply the jurisdiction rule to derive: $S_j \mid\equiv U_i \xleftrightarrow{SK_{ij}} S_j$

a_6. By p_6 and $U_i \triangleleft (ID_i, n_1, n_2, T_2)_K$, we apply the message-meaning rule to derive: $U_i \mid\equiv S_j \mid\sim (ID_i, n_1, n_2, T_2)$

a_7. By p_2 and a_6, we apply the fresh conjuncatenation rule and the nonce-verification rule to derive: $U_i \mid\equiv S_j \mid\equiv (ID_i, n_1, n_2, T_2)$

a_8. By a_7, we apply the belief rule to derive: $U_i \mid\equiv S_j \mid\equiv n_2$

a_9. By p_2 and a_8, we apply the jurisdiction rule to derive: $U_i \mid\equiv n_2$

a_{10}. By a_9 and $U_i \triangleleft \langle n_1, X_i, PWD_i \rangle_{n_2}$, we apply the message-meaning rule to derive: $U_i \mid\equiv S_j \mid\sim (n_1, X_i, PWD_i)$

a_{11}. By a_{10} and p_1, we apply the fresh conjuncatenation rule and the nonce-verification rule to derive: $U_i \mid\equiv S_j \mid\equiv (n_1, X_1, PWD_i)$

g_3. By p_1, p_3, p_4, p_6, a_{11} and $SK_{ij} = h(n_1 \| n_2 \| K \| X_i)$, we apply the fresh conjuncatenation rule and the nonce-verification rule to derive: $U_i \mid\equiv S_j \mid\equiv U_i \xleftrightarrow{SK_{ij}} S_j$

g_4. By g_3 and p_{12}, we apply the jurisdiction rule to derive: $U_i \mid\equiv U_i \xleftrightarrow{SK_{ij}} S_j$

Informal security analysis

In this subsection, we verify whether our proposed scheme is secure against a variety of known attacks.

Anonymity. Our proposed scheme can preserve the identity anonymity since ID_i cannot be derived from M_1 without the knowledge of K; furthermore, K cannot be derived from Y_i without the random number y_i and the pre-shared secret key PSK. Also, owing to the one-way hash function, ID_i cannot be derived from M_5. Our proposed scheme therefore provides user anonymity.

Resisting outsider attack. Suppose that an adversary $\mathcal{A}$ extracts all of the information $\{V_{\mathcal{A}}, W_{\mathcal{A}}, X_{\mathcal{A}}, Y_{\mathcal{A}}\}$ from a smart card by using side channel attack; however, he/she cannot obtain any of the secret information of S_j. $\mathcal{A}$ can compute $h(y_{\mathcal{A}} \| PSK) = W_{\mathcal{A}} \oplus ID_{\mathcal{A}}$, but the value $y_{\mathcal{A}}$ 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 S_j; therefore, $\mathcal{A}$ does not know and our proposed scheme can resist an outsider attack.

Resisting impersonation attack. Suppose that an adversary $\mathcal{A}$ intercepts all of message $\{Y_i, Z_i, M_1, M_2, M_3, M_4, M_5, M_6, T_1, T_2, T_3\}$ that are transmitted over a public channel between U_i and S_j; however, $\mathcal{A}$ cannot generate the legal login request message $\{Y_i, Z_i, M_1, M_2, M_3, T_1\}$, where $Y_i = y_i \oplus h(PSK)$, $Z_i = h(X_i \| n_1 \| PWD_i \| T_1)$, $M_1 = K \oplus ID_i$, $M_2 = n_1 \oplus K$ and $M_3 = PWD_i \oplus K$, because the value y_i is a random number that is unique to the user that is selected by the RC and n_1 is a random number that is generated by U_i; furthermore, $\mathcal{A}$ cannot generate the login response message $\{M_4,M_5,T_2\}$ without the random number n_2. Our proposed scheme can therefore resist an impersonation attack.

Session key agreement. Suppose that an adversary $\mathcal{A}$ intercepts all of the message $\{Y_i,Z_i,M_1,M_2,M_3,M_4,M_5,M_6,T_1,T_2,T_3\}$ that are transmitted over a public channel between U_i and S_j, steals the smart card of U_i, and then extracts the all information $\{V_i,W_i,X_i,Y_i,h(\cdot),H(\cdot)\}$; however, $\mathcal{A}$ cannot compute the session key $SK_{ij} = h(n_1 \parallel n_2 \parallel K \parallel X_i)$. To compute K from W_i, the U_i's identity ID_i is needed. To retrieve ID_i from V_i, $\mathcal{A}$ needs to know PW_i and $H(BIO_i)$. Since only U_i can imprint the biometrics BIO_i at the sensor, an adversary $\mathcal{A}$ cannot attain the U_i's identity ID_i and PW_i. Our proposed scheme can therefore provide session key security.

Formal security analysis

In this subsection, we demonstrate the formal security analysis of our proposed scheme and show that it is secure. First, we define the following hash function [29].

Definition 1. A secure one-way hash function h: $\{0, 1\}^* \rightarrow \{0, 1\}^n$, which takes an input as an arbitrary length binary string $x \in \{0, 1\}^*$ and outputs a binary string $h(x) \in \{0, 1\}^n$, satisfies the following requirements: a. Given $y \in Y$, it is computationally infeasible to find an $x \in X$ such that $y = h(x)$:b. Given $x \in X$, it is computationally infeasible to find another $x' \neq x \in X$, such that $h(x') = h(x)$:c. It is computationally infeasible to find a pair $(x',x) \in X' \times X$, with $x' \neq x$, such that $h(x') = h(x)$.

Theorem 1. Under the assumption that the one-way hash function $h(\cdot)$ closely behaves like an oracle, then our proposed scheme is provably secure against an adversary $\mathcal{A}$ for the protection of a user's personal information including the identity ID_i, password PW_i and biometrics BIO_i, a server's secret number x that is selected by the RC and a pre-shared secret key PSK that is between the RC and S_j.

Proof. The formal security proof of our proposed scheme is similar to those in [23, 29, 30]. Using the following oracle to construct $\mathcal{A}$ who will have the ability to derive the user U_i's identity ID_i, password PW_i, biometrics BIO_i, the server's secret number x that is selected by the RC, and a pre-shared secret key PSK between the RC and S_j.

Reveal: This random oracle will unconditionally output the input x from the given hash result $y = h(x)$.

Now, $\mathcal{A}$ runs the experimental algorithm that is shown in Table 4, $EXP^{JKMSE}_{HASH,A}$ for our proposed scheme JKMSE.

If the success probability of $EXP^{JKMSE}_{HASH,A}$ is defined as $Success^{JKMSE}_{HASH,A} = |Pr[EXP^{JKMSE}_{HASH,A} = 1] - 1|$, the advantage function for this experiment then becomes $Adv^{JKMSE}_{HASH,A}(t, q_R) = max_A Success^{JKMSE}_{HASH,A}$, where the maximum is taken over all of $\mathcal{A}$ with the execution time t and the number of queries q_R that are made to the Reveal oracle. Consider the experiment that is shown in Table 4 for $\mathcal{A}$. If $\mathcal{A}$ has the ability to solve the hash function problem that is provided in Definition 1, then he/she can directly derive U_i's identity ID_i, password PW_i, biometrics BIO_i, the server's secret number x that is selected by the RC and the pre-shared secret key PSK that is between the RC and S_j. In this case, $\mathcal{A}$ will discover the complete connections between U_i and S_j; however, it is a computationally infeasible problem to invert the input from a given hash value, i.e., $Adv^{JKMSE}_{HASH,A}(t) \leq \epsilon, \forall \epsilon > 0$. Then, we have $Adv^{JKMSE}_{HASH,A}(t, q_R) \leq \epsilon$, since $Adv^{JKMSE}_{HASH,A}(t, q_R)$ depends on $Adv^{JKMSE}_{HASH,A}(t)$. As a result, there is no way for $\mathcal{A}$ to discover the complete connections between U_i and S_j, and, by deriving $(ID_i,PW_i,BIO_i,y_i,x,PSK)$, our proposed scheme is provably secure against an adversary.

Table 4. Algorithm $EXP^{JKMSE}_{HASH,A}$.

```
Eavesdrop login request message $\{Y_i, Z_i, M_1, M_2, M_3, T_1\}$
Call the Reveal oracle. Let $(n_1', X_i', PWD_i') \leftarrow Reveal(Z_i)$
Eavesdrop login response message $\{M_4, M_5, T_2\}$
Call the Reveal oracle. Let $(ID_i', n_1'', n_2', K', T_2) \leftarrow Reveal(M_5)$
if $(n_1' = n_1'')$ then
    Call the Reveal oracle. Let $(PW_i', BIO') \leftarrow Reveal(PWD_i')$
    Call the Reveal oracle. Let $(ID_i', x') \leftarrow Reveal(X_i')$
    Compute $K'' = M_2 \oplus n_1'$
    if $(K' = K'')$ then
        Call the Reveal oracle. Let $(h'(y_i' || PSK'), SID_j) \leftarrow Reveal(K)$
        Compute $n_2'' = M_4 \oplus h(n_1' \| X_i \| PWD_i')$
        if $(n_2' = n_2'')$ then
            Call the Reveal oracle. Let $(y_i' || PSK') \leftarrow Reveal(h'(y_i || PSK))$
            Accept $ID_i'$, $PW_i'$, $BIO_i'$, $y_i'$ as the correct $ID_i$, $PW_i$, $BIO_i$ and $y_i$ of $U_i$, $x'$ and $PSK'$ as the correct secret number of $S_j$ and pre-shared secret key between $RC$ and $S_j$
            return 1
        else
            return 0
        end if
    else
        return 0
    end if
else
    return 0
end if
```

doi:10.1371/journal.pone.0145263.t004

Functional and performance analysis

In this section, we evaluate the functionality the computational costs comparisons between our proposed scheme and the other related schemes [18–23].

Functional analysis

Table 5 lists the functionality comparisons of our 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.

Table 5. Functionality comparison.

	Ours	[23]	[22]	[21]	[20]	[19]	[18]
Provide mutual authentication	Yes	Yes	Yes	No	Yes	Yes	Yes
User anonymity	Yes	No	Yes	Yes	Yes	Yes	Yes
Resist insider attack	Yes	Yes	Yes	Yes	Yes	No	Yes
Resist off-line guessing attack	Yes	Yes	Yes	Yes	Yes	No	Yes
Resist stolen smart card attack	Yes	No	Yes	No	-	Yes	Yes
Resist replay attack	Yes	Yes	No	No	No	No	No
Resist verifier attack	Yes	Yes	Yes	Yes	-	No	Yes
Session key agreement	Yes	No	Yes	Yes	Yes	No	Yes
Efficient password change phase	Yes	Yes	No	No	Yes	No	No

doi:10.1371/journal.pone.0145263.t005

Table 6. Computational costs comparison.

Schemes	Registration	Login	Authentication	Total	Time(ms)
Li et al. [18]	$6T_H$	$6T_H$	$12T_H$	$24T_H$	4.8
Xue et al. [19]	$7T_H$	$6T_H$	$17T_H$	$30T_H$	6.0
Lu et al. [20]	$6T_H$	$5T_H$	$13T_H$	$24T_H$	4.8
Chuang et al. [21]	$3T_H$	$4T_H$	$13T_H$	$20T_H$	4.0
Mishra et al. [22]	$7T_H$	$4T_H$	$11T_H$	$22T_H$	4.4
Lu et al. [23]]	$5T_H$	$6T_H$	$12T_H$	$23T_H$	4.6
Our proposed	$5T_H$	$5T_H$	$13T_H$	$23T_H$	4.6

T_H: hash function evaluation

doi:10.1371/journal.pone.0145263.t006

Performance anaylsis

For the performance comparison, the definitions of T_E and T_H are the performance times of a symmetric encryption/decryption operation and a hash function, respectively. Recently, Xue and Hong [31] estimated the running time of different cryptographic operations whereby T_E is nearly 0.45 ms on average, and T_H is below 0.2 ms on average in the environment (CPU: 3.2 GHz, RAM: 3.0 G). Table 6 shows a comparison of the computational costs of the proposed scheme with the other related schemes. In the performance comparison, the proposed scheme requires a greater amount of computation to accomplish mutual authentication and the key agreement than Chuang et al.'s scheme as the proposed scheme performs four further hash operations; however, these operations consume a very small amount of time.

Conclusion

In this paper, we analyzed the security weaknesses of a biometrics-based authentication scheme for multi-server environments by Lu et al. Lu et al. claimed that their authentication scheme is secure and provides user anonymity; however, we found that Lu et al.'s scheme is still insecure against outsider attacks and impersonation attacks. To resolve these security vulnerabilities, we proposed an improved protocol for an authentication scheme that retains the merits of Lu et al.'s scheme and also achieves a comprehensive security. The security analysis of this paper explains that the proposed scheme rectifies the weaknesses of Lu et al.'s scheme.

Acknowledgments

All authors, especially the corresponding author Dongho Won, would like to thank the anonymous reviewers for their time and invaluable comments and suggestions on this paper.

Author Contributions

Conceived and designed the experiments: JM YC JJ DW. Performed the experiments: JM YC JJ. Analyzed the data: JM YC DW. Contributed reagents/materials/analysis tools: JM DW. Wrote the paper: JM YC JJ DW. Designed the scheme: JM YC DW. Proved the security of the scheme: JM YC.

References

1. Lamport L. (1981) Password authentication with insecure communication. ACM Communication. 24 (11): 770–772. doi: 10.1145/358790.358797

2. Sun DZ, Huai JP, Sun JZ, Li JX, Zhang JW, Feng ZY. (2009) Improvements of Juang's password authenticated key agreement scheme using smart cards. IEEE Transactions on Industrial Electronics. 56(6): 2284–2291. doi: 10.1109/TIE.2009.2016508
3. Jeon W, Kim J, Nam J, Lee Y, Won D. (2012) An enhanced secure authentication scheme with anonymity for wireless environments. IEICE Transactions on Communications. 95(7):2505–2508. doi: 10.1587/transcom.E95.B.2505
4. Nam J, Choo K-KR, Kim J, Kang H, Kim J, Paik J, Won D. (2014) Password-only authenticated three-party key exchange with provable security in the standard model. The Scientific World Journal. Article ID 825072. doi: 10.1155/2014/825072
5. Kim J, Lee D, Jeon W, Lee Y, Won D. (2014) Security analysis and improvements of two-factor mutual authentication with key agreement in wireless sensor networks. Sensors. 14(4):6443–6462. doi: 10.3390/s140406443 PMID: 24721764
6. Nam J, Choo K-KR, Paik J, Won D. (2015) An offline dictionary attack against abdalla and pointcheval's key exchange in the password-only three-party setting. IEICE Transactions on Fundamentals of Electronics. 98(1):424–427. doi: 10.1587/transfun.E98.A.424
7. Son K, Han D, Won D. (2015) Simple and provably secure anonymous authenticated key exchange with a binding property. IEICE Transactions on Communications. 98(1):160–170. doi: 10.1587/transcom.E98.B.160
8. Nam J, Choo K-KR, Han S, Kim M, Paik J, Won D. (2015) Efficient and anonymous two-factor user authentication in wireless sensor networks: achieving user anonymity with lightweight sensor computation. PLoS One. 10(4):e0116709. doi: 10.1371/journal.pone.0116709 PMID: 25849359
9. Lu YR, Li LX, Yang YX. (2015) Robust and efficient authentication scheme for session initiation protocol. Mathematical Problems in Engineering. Article ID 894549, 9 pages.
10. Lu YR, Li LX, Peng HP, Yang YX. (2015) An enhanced biometric-based authentication scheme for telecare medicine information systems using elliptic curve cryptosystem. Journal of Medical Systems. 39 (3):1–8. doi: 10.1007/s10916-015-0221-7
11. Lu YR, Li LX, Peng HP, Yang YX. (2015) A biometrics and smart cards based authentication scheme for multi-server environments. Security and Communication Networks. doi: 10.1002/sec.1246
12. Lu YR, Li LX, Peng HP, Xie D, Yang YX. (2015) Robust and efficient biometrics based password authentication scheme for telecare medicine information systems using extended chaotic maps. Journal of Medical Systems. 39(6):1–10. doi: 10.1007/s10916-015-0229-z
13. Choi Y, Nam J, Lee D, Kim J, Jung J, Won D. (2015) Security enhanced anonymous multi-server authenticated key agreement scheme using smart cards and biometrics. The Scientific World Journal. Article ID 281305, 15 pages. doi: 10.1155/2014/281305
14. Tsai JL. (2008) Efficient multi-server authentication scheme based on one-way hash function without verification table. Computers & Security. 27(3–4):115–121. doi: 10.1016/j.cose.2008.04.001
15. Lu RX, Lin XD, Zhu HJ, Liang XH, Shen XM. (2012) BECAN: a bandwidth-efficient cooperative authentication scheme for filtering injected false data in wireless sensor networks. IEEE Transactions on Parallel and Distributed Systems. 23(1):32–43. doi: 10.1109/TPDS.2011.95
16. Liao YP, Wang SS. (2009) A secure dynamic ID based remote user authentication scheme for multi-server environment. Computer Standards & Interfaces. 31(1):24–29. doi: 10.1016/j.csi.2007.10.007
17. Lee CC, Lin TH, Chang RX. (2011) A secure dynamic ID based remote user authentication scheme for multiserver environment using smart cards. Expert Systems with Applications. 38(11):13863–13870.
18. Li X, Ma J, Wang WD, Liu CL. (2013) A novel smart card and dynamic ID based remote user authentication scheme for multi-server environments. Mathematical and Computer Modelling. 58:85–95. doi: 10.1016/j.mcm.2012.06.033
19. Xue KP, Hong PL, Ma CS. (2014) A lightweight dynamic pseudonym identity based authentication and key agreement protocol without verification tables for multi-server architecture. Journal of Computer and System Sciences. 80:195–206. doi: 10.1016/j.jcss.2013.07.004
20. Lu YR, Li LX, Peng HP, Yang X, Yang YX. (2015) A lightweight ID based authentication and key agreement protocol for multi-server architecture. International Journal of Distributed Sensor Network. Article ID 635890, 9 pages. doi: 10.1155/2015/635890
21. Chuang MC, Chen MC. (2014) An anonymous multi-server authenticated key agreement scheme based on trust computing using smart cards and biometrics. Expert Systems with Applications. 41:1411–1418. doi: 10.1016/j.eswa.2013.08.040
22. Mishra D, Das AK, Mukhopadhyay S. (2014) A secure user anonymity-preserving biometric-based multi-server authenticated key agreement scheme using smart cards. Expert Systems with Applications. 41(18):8129–8143. doi: 10.1016/j.eswa.2014.07.004

23. Lu YR, Li LX, Yang X, Yang YX. (2015) Robust biometrics based authentication and key agreement scheme for multi-server environments using smart cards. PLoS One. 10(5):e0126323. doi: 10.1371/journal.pone.0126323 PMID: 25978373
24. Canetti R, Krawczyk, H. (2001) Analysis of key-exchange protocols and their use for building secure channels. Proceedings of EUROCRYPT 2001, Heidelberg, Berlin. pp. 453–474.
25. Odelu V, Das AK, Goswami A. (2015) A secure biometrics-based multi-server authentication protocol using smart cards. IEEE Transactions on Information Forensics and Security. 10(9):1953–1966. doi: 10.1109/TIFS.2015.2439964
26. Messerges T, Dabbish E, Sloan R. (2002) Examining smartcard security under the threat of power analysis attacks. IEEE Transactions on Computers. 51(5):541–552. doi: 10.1109/TC.2002.1004593
27. Burrow M, Abadi M, Needham R. (1990) A logic of authentication. ACM Transactions on Computer System. 8(1):18–36. doi: 10.1145/77648.77649
28. Zhao DW, Peng HP, Li LX, Yang YX. (2013) A secure and effective anonymous authentication scheme for roaming service in global mobility networks. Wireless Personal Communication. 78(1):247–269. doi: 10.1007/s11277-014-1750-y
29. Das AK. (2013) A secure and effective user authentication and privacy preserving protocol with smart cards for wireless communications. Networking Science. 2(1–2):12–27. doi: 10.1007/s13119-012-0009-8
30. Das AK, Paul NR, Tripathy L. (2012) Cryptanalysis and improvement of an access control in user hierarchy based on elliptic curve cryptosystem. Information Sciences. 209:80–92. doi: 10.1016/j.ins.2012.04.036
31. Xue K, Hong P. (2012) Security improvement on an anonymous key agreement protocol based on chaotic maps. Communication Nonlinear Science Numererical Simulation. 17(7):2969–2977. doi: 10.1016/j.cnsns.2011.11.025