PLOS ONE

RESEARCH ARTICLE

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

Yanrong Lu[1,2], Lixiang Li[1,2]*, Xing Yang[1,2], Yixian Yang[1,2]

1 Information Security Center, State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China, **2** National Engineering Laboratory for Disaster Backup and Recovery, Beijing University of Posts and Telecommunications, Beijing 100876, China

* li_lixiang2006@163.com

Citation: Lu Y, Li L, Yang X, Yang Y (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

Academic Editor: Wen-Bo Du, Beihang University, CHINA

Received: September 17, 2014

Accepted: March 30, 2015

Published: May 15, 2015

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

Funding: This work was supported by National Natural Science Foundation of China (grant no. 61121061), the Beijing Natural Science Foundation (grant no. 4142016), and the Asia Foresight Program under NSFC Grant (grant no. 61411146001). 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.

Abstract

Biometrics authenticated schemes using smart cards have attracted much attention in multi-server environments. Several schemes of this type where proposed in the past. However, many of them were found to have some design flaws. This paper concentrates on the security weaknesses of the three-factor authentication scheme by Mishra et al. After careful analysis, we find their scheme does not really resist replay attack while failing to provide an efficient password change phase. We further propose an improvement of Mishra et al.'s scheme with the purpose of preventing the security threats of their scheme. We demonstrate the proposed scheme is given to strong authentication against several attacks including attacks shown in the original scheme. In addition, we compare the performance and functionality with other multi-server authenticated key schemes.

Introduction

With the swift development of wireless communications and network technologies, more and more people use wireless handheld devices (e.g.PDA, notebook and mobile phone, etc) to enjoy mobile services almost anytime and anywhere. However, open nature of networks demands for security concern of paid and protected resources available over the network [1–5]. Authentication mechanism becomes an essential need before a remote user can access the services. Since then Lamport [6] proposed the first authentication scheme, a number of authentication schemes have been put forward for different applications [7–13].

However, most of the existing password authentication schemes are based on a single-server environment which are unfit for the multi-server environments. Recently, a large number of smart cards based remote user authentication schemes for multi-server environments have been proposed. In addition, compared with other authentication schemes, schemes that only use random numbers and a hash function were getting much more attention because of their low computation costs. In 2008, Tsai [14] proposed an efficient multi-server authentication scheme using the random number and one-way hash function. After that, numerous

authenticated key agreement schemes were presented for multi-server environments one after another [15–17]. In 2012, Li et al. [18] proposed a novel authenticated key exchange scheme for multi-server environments. Unfortunately, Xue et al.[19] showed that Li et al.'s scheme did not resist some types of known attacks, such as vulnerability to verifier stolen, off-line password guess, replay, denial of service and forgery attacks. Then, Xue et al. proposed an improved scheme to remedy the weaknesses of Li et al.'s scheme. Nevertheless, Lu et al.[20] observed that Xue et al.'s scheme was not only really insecure against masquerade and insider attacks but also was vulnerable to off-line password guessing attack. To improve the shortcomings of Xue et al.'s scheme, Lu et al. proposed a slight modified authentication scheme for multi-server environments.

All above mentioned authentication schemes are based on password and smart cards. Note that the password cannot be considered as a unique identity identifier and it's needed to be remembered. Moreover, possibility of password guessing attack is also a concern. Compared with cryptographic keys and passwords, biometric keys (e.g.fingerprint, face, iris, hand geometry and palm-print, etc.) have many advantages [21], for example, they are difficult to lose or forget; they are difficult to copy or share; they are difficult to forge or distribute biometrics; they are difficult to guess; they are more difficult to break biometric keys. Recently, Chuang et al.[22] presented an efficient biometrics based authentication scheme using smart cards for multi-server environments, which was previously considered to be have more security properties. However, Mishra et al. [23] showed that Chuang et al.'s scheme was vulnerable to stolen smart card attack, server spoofing attack and impersonation attack. In addition, they proposed an improved biometrics-based multi-server authenticated key agreement scheme using smart cards and they claimed that their scheme satisfied all desirable security requirements. Unfortunately, this paper will demonstrate that the scheme cannot really resist replay attack and cannot provide an efficient password change phase.

In this paper, we concentrate on the security weaknesses of the three-factor authentication scheme by Mishra et al. After carefully analysis, we find their scheme does not really resist replay attack while fails to provide an efficient password change phase. We further propose an improvement of Mishra et al.'s scheme with the purpose of preventing the security threats of their scheme. We demonstrate the proposed scheme is given to strong authentication against several attacks including attacks showed in the original scheme. In addition, we compare the performance and functionality with other related schemes.

The rest of paper is organized as follows: In Section 2 and Section 3, we review and analyze the Mishra et al.'s scheme. In Section 4, we propose an enhancement authentication scheme for multi-sever environments. In Section 5, we present a security analysis of our scheme. Section 6 shows security and performance analyses by comparing our scheme with previous schemes. We conclude in Section 7.

Review of Mishra et al.'s scheme

There are three phases relating to Mishra et al.'s scheme which consists of the registration, login and authentication and password updating. Table 1 lists the notations used in this paper.

Registration

Suppose RC is the trusted third party responsible for registration of U_i and S_j.

Server registration.

1. S_j sends the registration request to RC;
2. After receiving the request, RC sends the key PSK to S_j through a secure channel;

Table 1. Notations.

U_i, S_j	User, server
RC	The registration center
ID_i, SID_j	Identity of U_i, S_j
PW_i, BIO_i	Password and biometrics of U_i
x, y	Master secret key of U_i and RC
PSK	Secure key shared by RC and S_j
$h(\cdot)$	Hash function
$H(\cdot)$	Biohash function
$\oplus$, $\|\|$	Exclusive-or operation and concatenation operation

doi:10.1371/journal.pone.0126323.t001

3. Upon receiving the secret key PSK, S_j stores it with aim to authorize a legitimate user.

User registration.

1. U_i selects his identity ID_i, password PW_i and keys his biometrics BIO_i. Then, U_i generates a random number N_i, computes $W_1 = h(PW_i||N_i)$, $W_2 = h(ID_i \oplus N_i)$ and sends the registration message $\{ID_i, W_1, W_2\}$ to RC via a secure channel.
2. RC computes $A_i = h(ID_i||x||T_r)$, $B_i = h(A_i)$, $X_i = W_i \oplus B_i$, $Y_i = h(PSK) \oplus W_2$ and $Z_i = PSK \oplus A_i$, where T_r is the registration time. Then, RC issues the smart card SC_i to U_i which contains $\{X_i, Y_i, Z_i, h(\cdot)\}$ over a secure channel.
3. Upon receiving SC_i, U_i enters his personal biometric BIO_i at the sensor and computes $N = N_i \oplus H(BIO_i)$, $V = h(ID_i||N_i||PW_i)$. Finally, U_i stores $\{X_i, Y_i, Z_i, N, V, h(\cdot)\}$ into SC_i.

Login and authentication

1. U_i inserts SC_i into the terminal and inputs his identity ID_i, password PW_i and imprints his biometrics BIO_i at the sensor.
2. SC_i computes $N_i = N \oplus h(BIO_i)$ and checks $h(ID_i \,||\, N_i \,||\, PW_i) \stackrel{?}{=} V$. If it holds, SC_i continues to compute $W_1 = h(PW_i||N_i)$, $W_2 = h(ID_i \oplus N_i)$, $B_i = X_i \oplus W_i$ and $h(PSK) = Y_i \oplus W_2$. Then, SC_i generates a random number n_1 and computes $M_1 = h(PSK) \oplus n_1$, $M_2 = ID_i \oplus h(n_1||B_i)$ and $M_3 = h(ID_i||n_1||B_i)$. Finally, U_i sends $\{Z_i, M_1, M_2, M_3\}$ to S_j.
3. When receiving the message from SC_i, S_j immediately computes $A_i = Z_i \oplus PSK$, $n_1 = M_1 \oplus h(PSK)$, $ID_i = M_2 \oplus h(n_1||h(A_i))$ and checks whether $h(n_1 \,||\, B_i \,||\, ID_i) \stackrel{?}{=} M_3$. If it is equal, S_j generates a random number n_2 and computes $SK_{ji} = h(ID_i||SID_j||B_i||n_1||n_2)$, $M_4 = n_2 \oplus h(ID_i||n_1)$, $M_5 = h(SK_{ji}||n_1||n_2)$. Then, S_j sends $\{SID_j, M_4, M_5\}$ to SC_i.
4. SC_i first computes $n_2 = M_4 \oplus h(ID_i||n_1)$, $SK_{ij} = h(ID_i||SID_j||B_i||n_1||n_2)$ and then checks whether $h(SK_{ij}||n_1||n_2)$ is consistent with M_5. If it is true, SC_i computes $M_6 = h(SK_{ij}||n_1||n_2)$ and delivers it to S_j.
5. S_j verifies the verification condition $M_6 \stackrel{?}{=} h(SK_{ji} \,||\, n_1 \,||\, n_2)$. If this verification holds, S_j can now use the keys SK_{ji} to communicate with U_i securely.

Password updating

U_i inputs his ID_i, PW_i and imprints his biometrics BIO_i at the sensor. SC_i computes $N_i = N \oplus h(BIO_i)$ and checks $h(ID_i \,||\, N_i \,||\, PW_i) \stackrel{?}{=} V$. If SC_i determines that they are equal, then U_i can key the new password PW_i^{new}. Subsequently, SC_i computes $W_1^{new} = h(PW_i^{new} \,||\, N_i)$, $X_i^{new} = X_i \oplus W_1 \oplus W_1^{new}$, $V_i^{new} = h(ID_i \,||\, N_i \,||\, PW_i^{new})$ and replaces X_i and V_i with X_i^{new} and V_i^{new}, respectively.

Security analysis of Mishra et al.'s scheme

This section presents a cryptanalysis of a recently scheme proposed by Mishra et al. We show their scheme does not satisfy the key security attribute such as vulnerability to replay attack and incorrect password change phase. We assume that a malicious adversary $\mathcal{A}$ has totally supervised the communication channel in login and session key establishment phases. In other words, $\mathcal{A}$ has the capacity to intercept, insert, delete, refresh or update any information delivered between U_i and S_j [6].

Not withstanding the replay attack

Suppose an adversary $\mathcal{A}$ has intercepted a past login message $\{Z_i, M_1, M_2, M_3\}$. He is able to launch a replay attack and login to the server by resending the eavesdropped message $\{Z_i, M_1, M_2, M_3\}$ to S_j. In other words, the adversary without running the "Login phase", sends the eavesdropped message $\{Z_i, M_1, M_2, M_3\}$ to S_j. In the "Login and authentication", upon receiving the message $\{Z_i, M_1, M_2, M_3\}$, S_j computes $A_i = Z_i \oplus PSK$, $n_1 = M_1 \oplus h(PSK)$, $ID_i = M_2 \oplus h(n_1 || h(A_i))$, $M_3' = h(n_1 \,||\, B_i \,||\, ID_i)$ and checks whether M_3' is equal to the received M_3 or not. Since M_3 and M_3' are equal, S_j will authenticate $\mathcal{A}$ and $\mathcal{A}$ will be able to login to S_j. Thus, $\mathcal{A}$ can easily login to S_j by re-sending an old login message. Since S_j does not check the freshness of the received login message $\{Z_i, M_1, M_2, M_3\}$ and authenticate U_i in (3) of the "Login and authentication", S_j will not be able to discover replay attack.

Incorrect password change phase

The user U_i inserts his smart card into a card reader and enters his identity ID_i, password PW_i and imprints his personal biometric BIO_i at the sensor corresponding to his smart card. Then smart card computes $N_i = N \oplus h(BIO_i)$, $V_i' = h(ID_i \,||\, N_i \,||\, PW_i)$ and compares V_i' with the stored value of V in its memory to verify the legitimacy of U_i. Once the authenticity of cardholder is verified then U_i can instruct smart card to change his password. Afterwards, smart card asks the cardholder to resubmit a new password PW_i^{new}, then $X_i = B_i \oplus h(PW_i || N_i)$ and $V = h(ID_i || N_i || PW_i)$ stored in the smart card can be updated with $X_i^{new} = X_i \oplus W_1 \oplus W_1^{new}$ and $V_i^{new} = h(ID_i \,||\, N_i \,||\, PW_i^{new})$, where $W_1^{new} = h(PW_i^{new} \,||\, N_i)$. The X_i^{new} value contains older password PW_i in $h(PW_i||N_i)$. Therefore, the modified X_i^{new} is not correct.

The proposed scheme

In this section, we will present our robust biometrics based authentication scheme using smart cards for multi-sever environments. In our scheme, there are also three participants, the user U_i, the server S_j and the registration center RC. RC chooses the secret key PSK and a secret number x and shares them with S_j via a secure channel. We will describe all the phases relating to our scheme in the subsections, i.e. registration, login and authentication, and password update, where registration and login and authentication phases are shown in Fig 1.

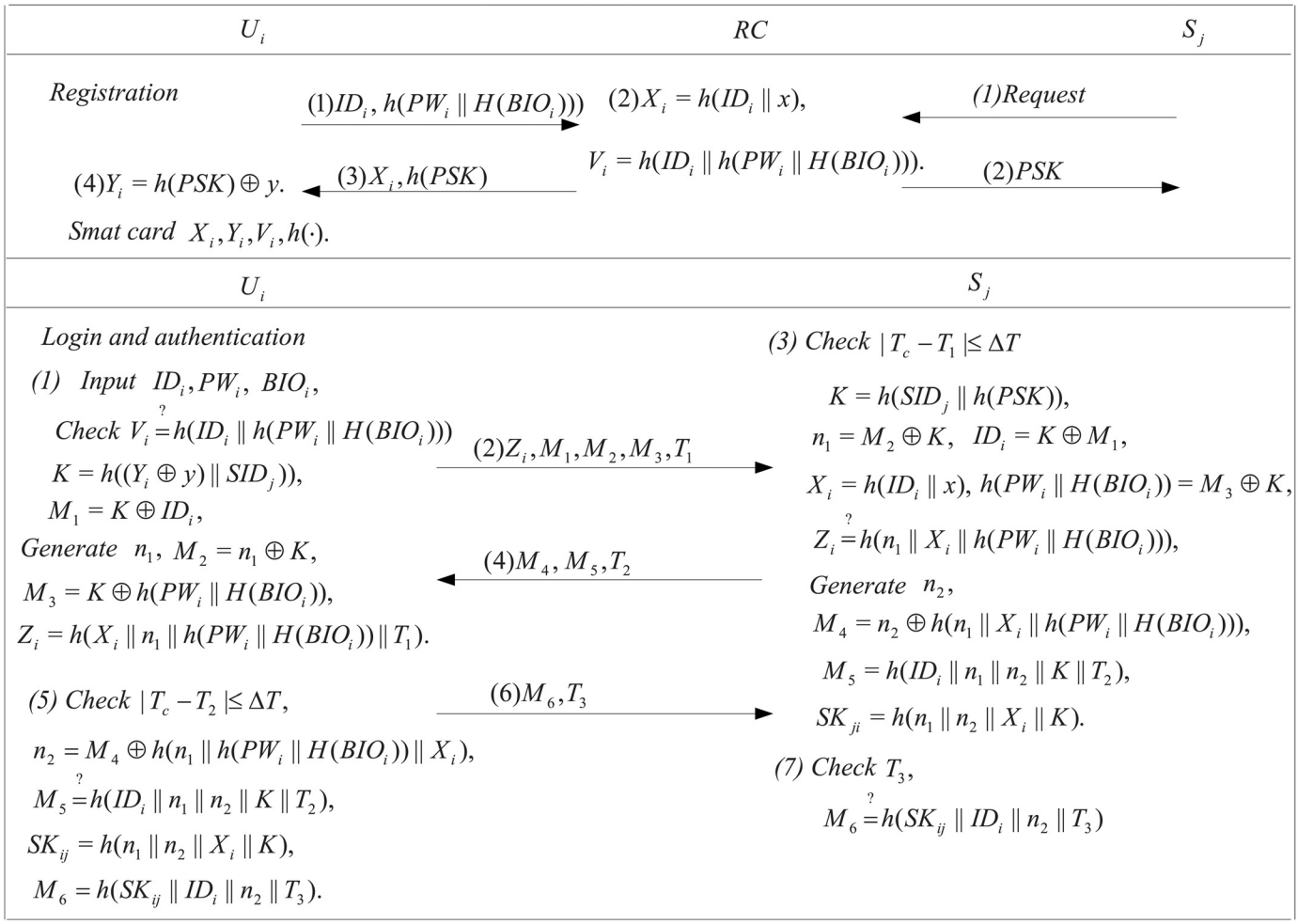

Fig 1. Registration and authentication phases.

doi:10.1371/journal.pone.0126323.g001

Registration

1. U_i keys his biometrics BIO_i, identity ID_i and password PW_i. Then, U_i sends $\{ID_i, h(PW_i||H(BIO_i))\}$ to RC.
2. Upon receiving the message from U_i, RC computes $X_i = h(ID_i||x)$, $V = h(ID_i||h(PW_i||H(BIO_i)))$. Then, RC stores $\{X_i, V_i, h(PSK)\}$ into 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. Finally, the smart card stores the values of $\{X_i, Y_i, V_i, h(\cdot)\}$.

Login and authentication

1. U_i inserts his smart card into device and enters his 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. If it holds, the smart card generates a random number n_1 and computes $K = h((y \oplus Y_i)||SID_j)$, $M_1 = K \oplus ID_i$, $M_2 = n_1 \oplus K$, $M_3 = h(PW_i||H(BIO_i)) \oplus K$, $Z_i = h(B_i||n_1||h$

$(PW_i||H(BIO_i))||T_1)$. Finally, U_i submits $\{Z_i, M_1, M_2, M_3, T_1\}$ to S_j, where T_1 is the current timestamp.

2. Upon receiving the message from U_i, S_j first checks whether $T_c - T_1 \leq \Delta T$ and then computes $K = h(SID_j||h(PSK))$ by using a secure pre-shared key PSK. Then, S_j retrieves $ID_i = M_1 \oplus K$, $n_1 = M_2 \oplus K$, $h(PW_i||BIO_i) = M_3 \oplus K$. Now, S_j computes $X_i = h(ID_i||x)$ and verifies whether $h(X_i \,||\, n_1 \,||\, h(PW_i \,||\, H(BIO_i))) \stackrel{?}{=} Z_i$. If it holds, S_j generates a random number n_2 and computes $SK_{ji} = h(n_1||n_2||K||X_i)$, $M_4 = n_2 \oplus h(n_1||h(PW_i||H(BIO_i))||X_i)$, $M_5 = h(ID_i||n_1||n_2||K||T_2)$. Then, S_j sends back authentication message $\{M_4, M_5, T_2\}$ to U_i, where T_2 is the current timestamp.

3. After 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 $h(ID_i||n_1||n_2||K)$ 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 T_3 and the correctness of M_6 by using SK_{ji}. 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 smart card into the device and provides his 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 they are not equal, the smart card refuses the request; Otherwise, U_i keys in the new password PW_i^{new}. Finally, 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 the proposed scheme

In this section, we first adopt Burrows-Abadi-Needham (BAN)Logic [24] to demonstrate the completeness of the proposed scheme. Then, we conduct discussion and a cryptanalysis of the proposed scheme through both the informal and formal analyses.

Verifying the proposed scheme with BAN logic

BAN logic [24] is a set of rules for defining and analyzing information exchange schemes. It helps its users determine whether exchanged information is trustworthy, secured against eavesdropping, or both. It has been highly successful in analyzing the security of authentication schemes. First, we introduce some notations and logical postulates of BAN logic in Table 2.

1. BAN logical postulates

   a. Message-meaning rule: $\frac{A|\equiv A \stackrel{K}{\leftrightarrow} B, A \triangleleft <X>_K}{A|\equiv |B \sim X}$: if A believes that the key K is shared by A and B, and sees X encrypted with K, then A believes that B once said X.

   b. Fresh conjuncatenation rule: $\frac{A|\equiv \#(X)}{A|\equiv \#(X,Y)}$: if A believes freshness of X, then A believes freshness of the (X, Y).

   c. Belief rule: $\frac{A|\equiv X,\ A|\equiv Y}{A|\equiv (X,Y)}$: if A believes X and Y, then A believes (X, Y).

Table 2. BAN logic notations.

$A\mid\equiv X$	A believes a statement X
$A \overset{K}{\leftrightarrows} B$	Share a key K between A and B
$\#X$	X is fresh
$A \lhd X$	A sees X
$A \Rightarrow X$	A controls X
$A\mid\sim X$	A said X
$(X)_K$	The formula X is hashed by K
$< X, Y > K$	X and Y are encrypted with the key K
(X, Y)	The formula X or Y is one part of the formula (X, Y)

doi:10.1371/journal.pone.0126323.t002

d. Nonce-verification rule: $\frac{A\mid\equiv\#(X), A\mid\equiv B\mid\sim X}{A\mid\equiv B\mid\equiv X}$: if A believes that X could have been uttered only recently and that B once said X, then A believes that B believes X.

e. Jurisdiction rule: $\frac{A\mid\equiv B\Rightarrow X, A\mid\equiv B\mid\sim X}{A\mid\equiv X}$: if A believes that B has jurisdiction over X and A trusts B on the truth of X, then A believes X.

2. Establishment of security goals

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

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

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

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

3. Idealized scheme

$U_i :< n_1, ID_i, h(PW_i \| H(BIO_i))>_K, (n_1, X_i, T_1)_{h(PW_i \| H(BIO_i))}, (n_2, U_i \overset{SK_{ij}}{\longleftrightarrow} S_j, T_3)_{ID_i}$

$S_j: < n_1, X_i, h(PW_i \| H(BIO_i)) > n_2, (ID_i, n_1, n_2, T_2)_K$

4. Initiative premises

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

$p_5.S_j \mid\equiv U_i \overset{K}{\leftrightarrows} S_j p_6.U_i \mid\equiv U_i \overset{K}{\leftrightarrows} S_j$

$p_7.\ U_i\mid\equiv ID_i\ p_8.\ S_j\mid\equiv U_i \Rightarrow h(PW_i \| BIO_i)$

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

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

5. Scheme analysis

a_1. By p_5 and $S_j \lhd < n_1, ID_i, h(PW_i \| BIO_i) > K$, we apply the message-meaning rule to derive: $S_j\mid\equiv U_i\mid\sim (n_1, ID_i, h(PW_i \| H(BIO_i)))$

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

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 $S_j \lhd (n_2, U_i \overset{SK_{ij}}{\longleftrightarrow} S_j, T_3)_{ID_i}$, we apply the message-meaning rule to derive: $S_j \mid\equiv U_i \mid\sim (n_2, U_i \overset{SK_{ij}}{\longleftrightarrow} S_j, T_3)$

a_5. By p_4 and a_4, we apply the fresh conjuncatennation rule and the nonce-verification rule

to derive: $S_j \mid\equiv U_i \mid\equiv (n_2, U_i \overset{SK_{ij}}{\longleftrightarrow} S_j, T_3)$

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

g_2. By g_1 and p_{11}, we apply the jurisdiction rule to derive: $S_j \mid\equiv U_i \overset{SK_{ij}}{\longleftrightarrow} S_j$

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_9, 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 $U_i \triangleleft < n_1, X_i, h(PW_i||BIO_i) > n_2$, we apply the message-meaning rule to derive: $U_i \mid\equiv S_j \mid\sim (n_1, X_i, h(PW_i||BIO_i))$

a_{11}. By a_{10} and p_1, we apply the fresh conjuncatennation rule and the nonce-verification rule to derive: $U_i \mid\equiv S_j \mid\equiv (n_1, X_i, h(PW_i||BIO_i))$

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

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

Informal security analysis

This subsection verifies whether the proposed scheme is secure against various kinds of known attacks. We assume that a malicious adversary $\mathcal{A}$ has totally supervised the communication channel in login and session key establishment phases. In other words, $\mathcal{A}$ has the capacity to intercept, insert, delete, refresh or update any information delivered between U_i and S_j [6].

Anonymity. U_i's identity ID_i is well protected by the shared secret parameter K as a substitute for real ones, $\mathcal{A}$ can not get users' real identities. In addition, the unauthorized server cannot get ID_i without knowing K since K is protected by the secret key PSK only known by the authorized server and is not exposed in the open channel. Thus, our scheme provides user anonymity, which can prevent the leakage of private user identities to malicious attackers.

Mutual authentication. In order to authenticate U_i, S_j has to verify validity of the evidence $Z_i = h(X_i||n_1||h(PW_i||H(BIO_i)))$. The evidence is computed with the common secret parameter K only known U_i and S_j. In other words, $(n_1, ID_i, h(PW_i||H(BIO_i)))$ are derived from the valid login message $\{Z_i, M_1, M_2, M_3, T_1\}$ through K, no one can counterfeit the evidence. In addition, to compute X_i, secret key x is needed but only known by S_j. Moreover, checking $h(SK_{ij}||ID_i||n_2)$ to further assist S_j in authenticating U_i because the session key is only known by U_i and S_j. To authenticate S_j, U_i needs to verify whether $M_5 \overset{?}{=} h(ID_i \mid\mid n_1 \mid\mid n_2 \mid\mid K)$. Because ID_i and K are only known by U_i and S_j, no one can forge a valid $\{M_4, M_5, T_2\}$ without them. Hence, mutual authentication between U_i and S_j is achieved.

Resist stolen smart card attack. Even if $\mathcal{A}$ has gathered [25] the information $\{X_i, Y_i, V_i, h(\cdot)\}$ stored in the 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. Moreover, $\mathcal{A}$ cannot get the identity ID_i and PW_i since they are protected by hash functions with the U_i's biometrics BIO_i. Hence, $\mathcal{A}$ still cannot succeed if he steals the smart card.

Session key agreement. We provide the session key $SK = h(n_1||n_2||K||X_i)$ to protect the message communication between U_i and S_j, where (n_1, n_2, K, X_i) are known to anybody but U_i and S_j. In addition, SK is different in each session, $\mathcal{A}$ has obtained a known session key cannot be used to calculate the value of the next session key.

Resist replay attack. Assume $\mathcal{A}$ has intercepted all the communication message $\{Z_i, M_1, M_2, M_3, T_1, M_4, M_5, T_2, M_6, T_3,\}$ and tried to replay them to U_i or S_j to obtain authentication. However, it is impossible to come true since all the authenticated messages imply the timesstamp which is also exposed in public channel. If $\mathcal{A}$ resends the transmitted messages, the receiver will immediately detect the attack through the authenticated message. Hence, our scheme can withstand replay attack.

Resist stolen verifier and insider attacks. In the registration phase, *RC* does not directly get the U_i's password PW_i and biometrics information BIO_i. Hence, $\mathcal{A}$ performs a stolen verifier attack or insider attack will be hard.

Resist off-line guessing attack. In our proposed scheme, trying to launch an off-line passsword guessing attack with the information stored in the smart card and the eavesdropped messages is trying to solve the input from the given hash value. Since the identity ID_i and the random number N_i are required with the purposed of knowing PW_i, both the secrets are protected by the hash function and known by the user himself.

Formal security analysis of the proposed scheme

This subsection presents the formal security analysis of our scheme and shows that it is secure. For this, we first define the following hash function [26].

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 $h(x) \in \{0,1\}^n$ and 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 scheme is provably secure against an attacker $\mathcal{A}$ for protecting user's personal information including identity ID_i, password PW_i and biometrics BIO_i, sever's private key x and PSK.

Proof. The formal security proof of our scheme is similar to that as in [27–28]. Using the following oracle to construct $\mathcal{A}$ who will have the ability to derive the user's ID_i, password PW_i, biometrics BIO_i, sever's private key x and PSK.

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

$\mathcal{A}$ runs the experimental algorithm showed in Table 3, $EXP^{BAKASSCMSE}_{HASH,\mathcal{A}}$ for our biometrics based authentication and key agreement scheme using smart cards for multi-server environments, say BAKASSCMSE.

Define the success probability for $EXP^{BAKASSCMSE}_{HASH,\mathcal{A}}$ is $Succ^{BAKASSCMSE}_{HASH,\mathcal{A}} = \mid Pr[EXP^{BAKASSCMSE}_{HASH,\mathcal{A}} = 1] - 1 \mid$ and the advantage function for this experiment then becomes $Adv^{BAKASSCMSE}_{HASH,\mathcal{A}}(t, q_R) = max_{\mathcal{A}}\ Succ^{BAKASSCMSE}_{HASH,\mathcal{A}}$, where the maximum is taken over all $\mathcal{A}$ with execution time t and the number of queries q_R made to the Reveal oracle. Consider the experiment showed in Table 3 for $\mathcal{A}$. If $\mathcal{A}$ has the ability to solve the hash function problem provided in Definition 1, then he can directly derive U_i's identity ID_i, password PW_i, biometrics BIO_i, and S_j's private key x and PSK. 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., $Adv^{BAKASSCMSE}_{HASH,\mathcal{A}}(t) \leq \epsilon, \forall \epsilon > 0$. Hence, we have $Adv^{BAKASSCMSE}_{HASH,\mathcal{A}}(t, q_R) \leq \epsilon$, since $Adv^{BAKASSCMSE}_{HASH,\mathcal{A}}(t, q_R)$ depends on $Adv^{BAKASSCMSE}_{HASH,\mathcal{A}}(t)$. As a result, there is no way for $\mathcal{A}$ to discover the complete connections between U_i and S_j and our scheme is provably secure against an adversary for deriving (ID_i, PW_i, BIO_i, x, PSK).

Table 3. Algorithm $EXP^{BAKASSCMSE}_{HASH,A}$.

1.	Eavesdrop login message $\{Z_i, M_1, M_2, M_3, T_1\}$
2.	Call the Reveal oracle. Let $(X_i', n_1', p') \leftarrow Reveal(Z_i)$
3.	Eavesdrop authentication message $\{M_4, M_5, T_2\}$
4.	Call the Reveal oracle. Let $(ID_i', n_1'', n_2', K', T_2) \leftarrow Reveal(M_5)$
5.	**if** $(n_1' = n_1'')$ **then**
6.	Call the Reveal oracle. Let $(PW_i', BIO_i') \leftarrow Reveal(p')$
7.	Call the Reveal oracle. Let $(ID_i', x') \leftarrow Reveal(X_i')$
8.	Compute $K'' = M_2 \oplus n_1'$
9.	**if** $(K' = K'')$ **then**
10.	Call the Reveal oracle. Let $(q', SID_j) \leftarrow Reveal(K)$
11.	Compute $n_2'' = M_4 \oplus h(n_1' \| X_i \| h'(PW_i \| BIO_i))$
12.	**if** $(n_2' = n_2'')$ **then**
13.	Call the Reveal oracle. Let $(PSK') \leftarrow Reveal(q')$
14.	Accept ID_i', PW_i', BIO_i' as the correct ID_i, PW_i and BIO_i of U_i x' and PSK' as the correct private key of S_j
15.	**return** 1
16.	**else**
17.	**return** 0
18.	**end if**
19.	**else**
20.	**return** 0
21.	**end if**
22.	**else**
23.	**return** 0
24.	**end if**

doi:10.1371/journal.pone.0126323.t003

Performance and functionality analysis

In this section, we compare our scheme with other existing multi-server authenticated schemes ([18–20], [22–23]) regarding security and performance. Table 4 lists the functionality comparisons of our proposed scheme with other related schemes. It can be seen that the proposed scheme achieves all security and functionality requirements and is more secure than other related schemes.

Table 4. Functionality comparison.

	Ours	Mishra et al. [23]	Chuang et al. [22]	Lu et al. [20]	Xue et al. [19]	Li et al. [18]
Provide mutual authentication	Yes	Yes	No	Yes	Yes	Yes
User anonymity	Yes	Yes	Yes	Yes	Yes	Yes
Resist insider attack	Yes	Yes	Yes	Yes	No	Yes
Resist off-line guessing attack	Yes	Yes	Yes	Yes	No	No
Resist stolen smart card attack	Yes	Yes	No	-	Yes	Yes
Resist replay attack	Yes	No	No	No	No	No
Resist verifier attack	Yes	Yes	Yes	-	No	Yes
Session key agreement	Yes	Yes	Yes	Yes	Yes	Yes
Efficient password change phase	Yes	No	No	Yes	No	No

doi:10.1371/journal.pone.0126323.t004

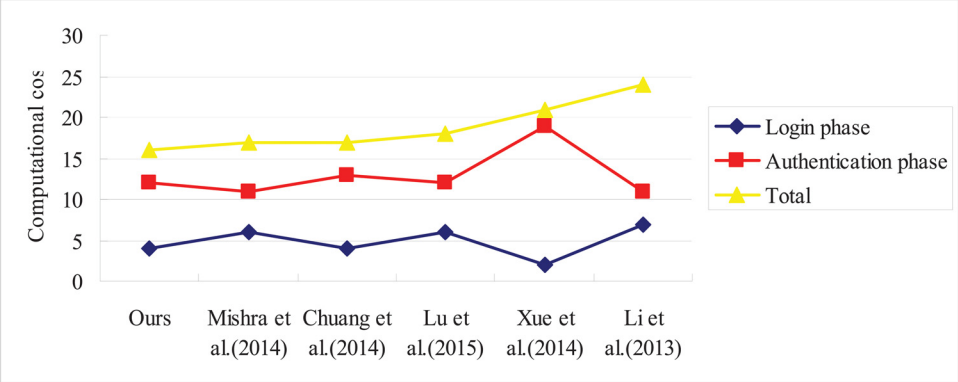

Fig 2. Performance comparison.

doi:10.1371/journal.pone.0126323.g002

For performance analysis, we compare the computational primitives involved in login and authentication phases of our scheme and other related schemes. To analyze the computational complexity of the schemes, we use hashing operation as the time complexity since XOR operations require very little computations. Fig 2 shows comparison regarding the performance. From this comparison, we can see that our proposed scheme has better efficiency in comparison with other schemes.

Conclusion and future work

In this paper, we presented a cryptanalysis of a recently proposed Mishra et al.'scheme and showed that their scheme was susceptible to replay attack while failed to provide an efficient password change phase. An improved scheme is proposed that inherits the merits of Mishra et al.'s scheme and resists different possible attacks. The proposed scheme is practical and efficient compared with other related schemes. Comprehensive security analysis proves that the robustness of our scheme is more secure than other related schemes. Among the open problems to be faced in the near future we can mention the study of specific applications and practical limitations of our scheme for mutual authentication using smart cards based on biometrics and their large-scale implementation in real multi-sever environments.

Author Contributions

Conceived and designed the experiments: YRL LXL XY YXY. Performed the experiments: YRL LXL XY YXY. Analyzed the data: YRL LXL XY YXY. Contributed reagents/materials/analysis tools: YRL LXL XY YXY. Wrote the paper: YRL LXL XY YXY.

References

1. Liu C, Du WB, Wang WX. Particle Swarm Optimization with Scale-Free Interactions. PLoS One 9(5). 2014.
2. Du WB, Wu ZX, Cai KQ. Effective usage of shortest paths promotes transportation efficiency on scale-free networks. Physica A. 2013; 392(17): 3505–3512. doi: 10.1016/j.physa.2013.03.032
3. Wang Z, Perc M. Aspiring to the fittest and promotion of cooperation in the prisoner's dilemma game. Physical Review E. 2010; 82(2), 021115. doi: 10.1103/PhysRevE.82.021115

4. Boccaletti S, Bianconi G, Criado R, del Genio CI, Gómez-Gardeñes J, Romance M, et al. The structure and dynamics of multilayer networks. Physics Reports. 2014; 544(1): 1–122. doi: 10.1016/j.physrep.2014.07.001
5. Zhao DW, Peng HP, Li LX, Yang YX, Li SD. An efficient patch dissemination strategy for mobile networks. Mathematical Problems in Engineering. 2013; Article ID 896187, 13 pages., 2013.
6. Lamport L. Password authentication with insecure communication. ACM Communication. 1981; 24 (11): 770–772. doi: 10.1145/358790.358797
7. Sun DZ, Huai JP, Sun JZ, Li JX, Zhang JW, Feng ZY. Improvements of Juang's password authenticated key agreement scheme using smart cards. IEEE Transactions on Industrial Electronics. 2009; 56 (6): 2284–2291. doi: 10.1109/TIE.2009.2016508
8. Lu RX, Lin XD, Liang XH, Shen XM A dynamic privacy-preserving key management scheme for location-based services in vanets. IEEE Transactions on Intelligent Transportation Systems. 2012; 13(1): 127–139. doi: 10.1109/TITS.2011.2164068
9. Zhao DW, Peng HP, Li LX, Yang YX. A secure and effective anonymous authentication scheme for roaming service in global mobility networks. Wireless Personal Communications. 2013; 78: 247–269. doi: 10.1007/s11277-014-1750-y
10. Lu, YR, Li, LX, Yang, YX. Robust and efficient authentication scheme for session initiation protocol. Mathematical Problems in Engineering. 2015; 2015, Article ID 894549, 9 pages.
11. Lu YR, Li LX, Peng HP, Yang YX. An enhanced biometric-based authentication scheme for telecare medicine information systems using elliptic curve cryptosystem. Journal of Medical Systems. 2015; 39 (3): 1–8. doi: 10.1007/s10916-015-0221-7
12. Lu YR, Li LX, Peng HP, Yang YX. Robust and efficient biometrics based password authentication scheme for telecare medicine information systems using extended chaotic maps. Journal of Medical Systems. 2015. doi: 10.1007/s10916-015-0221-7
13. Lu, YR, Li, LX, Peng, HP, Yang, YX. A biometrics and smart cards based authentication scheme for multi-server environments. Security and Communication Networks. 2015;
14. Tsai JL. Efficient multi-server authentication scheme based on one-way hash function without verification table. Computers & Security. 2008; 27(3–4): 115–121. doi: 10.1016/j.cose.2008.04.001
15. Lu RX, Lin XD, Zhu HJ, Liang XH, Shen XM. BECAN: a bandwidth-efficient cooperative authentication scheme for filtering injected false data in wireless sensor networks. IEEE Transactions on Parallel and Distributed Systems. 2012; 23(1): 32–43. doi: 10.1109/TPDS.2011.95
16. Liao YP, Wang SS. A secure dynamic ID based remote user authentication scheme for multi-server environment. Computer Standards & Interfaces. 2009; 31(1): 24–29. doi: 10.1016/j.csi.2007.10.007
17. Lee CC, Lin TH, Chang RX. A secure dynamic ID based remote user authentication scheme for multi-server environment using smart cards. Expert Systems with Applications. 2011; 38(11): 13863–13870
18. Li X, Ma J, Wang WD, Liu CL. A novel smart card and dynamic ID based remote user authentication scheme for multi-server environments. Mathematical and Computer Modelling. 2013; 58: 85–95. doi: 10.1016/j.mcm.2012.06.033
19. Xue KP, Hong PL, Ma CS. A lightweight dynamic pseudonym identity based authentication and key agreement protocol without verification tables for multi-server architecture. Journal of Computer and System Sciences. 2014; 80: 195–206. doi: 10.1016/j.jcss.2013.07.004
20. Lu YR, Li LX, Peng HP, Yang X, Yang YX. A lightweight ID based authentication and key agreement protocol for multi-server architecture. International Journal of Distributed Sensor Network. 2015, Article ID 635890, 9 pages.
21. Li CT, Hwang MS. An efficient biometrics-based remote user authentication scheme using smart cards. Journal of Network and Computer Applications. 2010; 33(1): 1–5. doi: 10.1016/j.jnca.2009.08.001
22. Chuang MC, Chen MC. An anonymous multi-server authenticated key agreement scheme based on trust computing using smart cards and biometrics. Expert Systems with Applications. 2014; 41: 1411–1418. doi: 10.1016/j.eswa.2013.08.040
23. Mishra D, Das AK, Mukhopadhyay S. A secure user anonymity-preserving biometric-based multi-server authenticated key agreement scheme using smart cards. Expert Systems with Applications. 2014; 41(18): 8129–8143. doi: 10.1016/j.eswa.2014.07.004
24. Burrow M, Abadi M, Needham R. A logic of authentication, ACM Transactions on Computer System. 1990; 8(1): 18–36. doi: 10.1145/77648.77649
25. Messerges TS, Dabbish EA, Sloan RH. Examining smart-card security under the threat of power analysis attacks. IEEE Transactions on Computers. 2002; 51(5): 541–552. doi: 10.1109/TC.2002.1004593

26. Stallings W. Cryptography and Network Security: Principles and Practices, third ed. Prentice Hall. 2003.

27. Das AK. A secure and effective user authentication and privacy preserving protocol with smart cards for wireless communications. Networking Science. 2013; 2(1–2): 12–27. doi: 10.1007/s13119-012-0009-8

28. Das AK, Paul NR, Tripathy L. Cryptanalysis and improvement of an access control in user hierarchy based on elliptic curve cryptosystem. Information Sciences. 2012; 209: 80–92. doi: 10.1016/j.ins.2012.04.036