Singapore Management University

Institutional Knowledge at Singapore Management University

Research Collection School Of Computing and Information Systems | School of Computing and Information Systems

2-2015

Analysis and improvement on a biometric-based remote user authentication scheme using smart cards

Fengtong WEN

Willy SUSILO

Guomin YANG
Singapore Management University, gmyang@smu.edu.sg

Follow this and additional works at: https://ink.library.smu.edu.sg/sis_research

 Part of the Information Security Commons

Citation

WEN, Fengtong; SUSILO, Willy; and YANG, Guomin. Analysis and improvement on a biometric-based remote user authentication scheme using smart cards. (2015). *Wireless Personal Communications*. 80, (4), 1747-1760.
Available at: https://ink.library.smu.edu.sg/sis_research/7341

This Journal Article is brought to you for free and open access by the School of Computing and Information Systems at Institutional Knowledge at Singapore Management University. It has been accepted for inclusion in Research Collection School Of Computing and Information Systems by an authorized administrator of Institutional Knowledge at Singapore Management University. For more information, please email cherylds@smu.edu.sg.

Wireless Pers Commun (2015) 80:1747–1760
DOI 10.1007/s11277-014-2111-6

Analysis and Improvement on a Biometric-Based Remote User Authentication Scheme Using Smart Cards

Fengtong Wen · Willy Susilo · Guomin Yang

Published online: 14 October 2014
© Springer Science+Business Media New York 2014

Abstract In a recent paper (BioMed Research International, 2013/491289), Khan et al. proposed an improved biometrics-based remote user authentication scheme with user anonymity. The scheme is believed to be secure against password guessing attack, user impersonation attack, server masquerading attack, and provide user anonymity, even if the secret information stored in the smart card is compromised. In this paper, we analyze the security of Khan et al.'s scheme, and demonstrate that their scheme doesn't provide user anonymity. This also renders that their scheme is insecure against other attacks, such as off-line password guessing attack, user impersonation attacks. Subsequently, we propose a robust biometric-based remote user authentication scheme. Besides, we simulate our scheme for the formal security verification using the wide-accepted BAN logic to ensure our scheme is working correctly by achieving the mutual authentication goals.

Keywords Roaming · Authentication · Biometrics · Security · Smart card · BAN logic

1 Introduction

In recent years, with the fast development of network technologies, wired and wireless networks have become widely available and interconnected. Remote user authentication is a fundamental research problem in network security.

F. Wen (✉)
School of Mathematical Sciences, University of Jinan, Jinan 250022, China
e-mail: wftwq@163.com

F. Wen · W. Susilo · G. Yang
School of Computer Science and Software Engineering, University of Wollongong, Wollongong, NSW 2522, Australia

Present Address:
F. Wen
University of Wollongong, Wollongong, NSW 2522, Australia

The security of traditional remote user authentication is based on passwords [1], and hence, it is susceptible to simple dictionary attacks. In order to improve security, smart card based remote user authentication scheme has been proposed [2–10]. Henceforth, the security is based on the password and the smart card. However, the security of these smart card based password authentication schemes will be largely downgraded if the smart card is compromised, for example, an attacker can extract all the secret information stored in a smart card by monitoring the power consumption or by analyzing the leaked information [11,12].

To resolve the security weaknesses in smart card based password authentication schemes, biometrics have been introduced as another authentication factor in designing authentication schemes. Biometric data provide a source of high-entropy information and have the following advantages: (i) they will not be lost or forgotten; (ii) they are very difficult to copy or share; (iii) they are extremely hard to forge; and (iv) they cannot be guessed easily. Hence, they are believed to be a reliable authentication factor. Recently, several biometrics-based remote user authentication schemes [13–18] have been proposed. However, it is unfortunate that most of the existing protocols have been broken shortly after they were proposed.

In 2012, An [19] proposed an enhancements of an efficient biometrics-based remote user authentication scheme using smart cards, and claimed that the scheme is secure against user impersonation attack, server masquerading attack, and so on. However, Khan et al. [20] analyzed the security of An's authentication scheme, and showed that the scheme is in fast vulnerable to several attacks and cannot provide mutual authentication between the user and the server. In order to fix the flaws, Khan et al. proposed an scheme and claimed that the new scheme is secure even if the secret information stored in the smart card is revealed to an attacker. Therefore, Khan et al.'s scheme is very attractive and it is promising for adoption in practice.

1.1 Our Contributions

The contributions of this paper are twofold. First, we analyze Khan's scheme and point out that the scheme cannot provide user anonymity and is also vulnerable to several attacks, such as off-line password guessing attack and server masquerading attack. Secondly, we propose a new biometrics-based remote user authentication protocol. Finally, we demonstrate the validity of the proposed scheme through the BAN logic.

1.2 Paper Organization

In Sect. 2, we briefly review Khan et al.'s scheme. Then we show its weaknesses in Sect. 3. We then propose our new protocol in Sect. 4 and analyze its security in Sect. 5. We compare the performance of our new protocol with the previous schemes in Sect. 6. The paper is concluded in Sect. 7.

2 Review of Khan et al.'s Scheme

Khan et al.'s scheme [20] is divided into four phases: registration phase, login phase, authentication phase and password change phase. We only review three phase. In this scheme, there are three participants, the trusted registration center R, the server S_i, and the user U_i. The sever maintains two secret keys x_s, y_s.

2.1 Registration Phase

User U_i first generates a random number K_i and submits his/her registration information $\{ID_i, PW_i \oplus K_i, B_i \oplus K_i\}$ to R via a secure channel. After receiving the request, R personalizes a smart card SC_i with parameters $(c_i, h(\cdot), e_i)$, and sends SC_i, f_i to the user via a secure channel, where $h(\cdot)$ denotes a cryptographic hash function, $f_i = h(B_i \oplus K_i), r_i = h(PW_i \oplus K_i) \oplus f_i$ and $c_i = h(x_s \| y_s) \oplus f_i$, $e_i = h(ID_i \| x_s) \oplus r_i$. On receiving SC_i, f_i, U_i computes $g_i = (ID_i \| PW_i) \oplus f_i$, $j_i = (ID_i \| PW_i) \oplus K_i$ and stores g_i, j_i into the smart card.So that now $SC_i = \{c_i, e_i, g_i, j_i, h()\}$

2.2 Login Phase

When the user U_i wants to login the remote server S_i, the user performs the following steps:

(1) U_i inserts his/her smart card into a card reader and inputs his/her ID_i, PW_i and the biometrics information B_i.

(2) SC_i retrieves $f_i = (ID_i \| PW_i) \oplus g_i$ and $K_i = (ID_i \| PW_i) \oplus j_i$. The system authenticates U_i's personal biometrics B_i by matching the biometric template $f_i = h(B_i \oplus K_i)$, and generates a request $\{M_3, M_4, M_5\}$ to S_i, where $r_i = h(PW_i \oplus K_i) \oplus f_i, M_1 = c_i \oplus f_i$, $M_2 = e_i \oplus r_i, M_3 = M_1 \oplus R_c$, $M_4 = h(M_1 \| R_c) \oplus ID_i, M_5 = h(M_2 \| R_c)$ and R_c is a random number generated by U_i.

2.3 Authentication Phase

After receiving the request login message, the remote server S_i performs the following steps with the user U_i for mutual authentication.

Step 1. S_i computes $M_6 = h(x_s \| y_s)$ and $M_7 = M_3 \oplus M_6$, $ID_i = M_4 \oplus (M_6 \| M_7)$.

Step 2. S_i checks the format of ID_i. If it is valid, S_i computes $M_8 = h(ID_i \| x_s)$. It then checks if $M_5 = h(M_8 \| M_7)$. If both are equal, S_i generates a random number R_s and computes $M_9 = M_8 \oplus R_s$ and $M_{10} = h(M_8 \| R_s)$.

Step 3. S_i sends the message $\{M_9, M_{10}\}$ to U_i, U_i computes $M_{11} = M_9 \oplus M_2$ and verifies whether $M_{10} = h(M_2 \| M_{11})$ or not. If the verification is successful, U_i computes $M_{12} = h(M_2 \| R_c \| M_{11})$ and sends the message M_{12} to S_i.

Step 4. After receiving the message, S_i verifies whether $M_{12} = h(M_8 \| M_7 \| R_s)$ or not. If the equation holds, S_i accepts the user's login request.

3 Security Analysis of Khan et al.'s Scheme

In [20], Khan et al. claimed that the scheme can provide user anonymity and resist off-line password guessing attacks even if the secret information in a user's smart card is known by an adversary. Unfortunately, below we demonstrate that this claim is false.

3.1 Failure of Protecting User Anonymity

In Khan et al.'s scheme, their scheme is believed to provide user anonymity as well as user un-traceability. However, we find that it is not true due to the following analysis:

Any legal but malicious user A of the server can get the secret value $h(x_s \| y_s)$ using his/her own information $\{c_a, B_a, K_a, j_a, ID_a, PW_a\}$ by computing $h(x_s \| y_s) = c_a \oplus f_a = c_a \oplus h(B_a \oplus K_a) = c_a \oplus h(B_a \oplus j_a \oplus (ID_a \| PW_a))$. Consider that A has recorded U_i's previous

login request message $\{M_3, M_4, M_5\}$. Then, with the secret information $h(x_s \| y_s)$, he/she can easily compute $R_c = M_3 \oplus h(x_s \| y_s)$, $ID_i = M_4 \oplus (M_1 \| R_c) = M_4 \oplus (h(x_s \| y_s) \| R_c)$. So he/she gets the U_i's ID_i.

When the adversary get the user's ID_i, he/she can perform the following attacks.

3.2 Off-line Password Guessing Attack

If the malicious user A can extract the secret values $\{c_i, e_i, g_i, j_i, h()\}$ from the user U_i's smart card, he/she can perform the off-line password guessing attack with the computed secret value $h(x_s \| y_s)$:

Step 1. A computes $c_i \oplus h(x_s \| y_s) = f_i$, $g_i \oplus (ID_i \| PW_i^*) = f_i^*$, where PW_i^* is a guessed password.
Step 2. A verifies whether $f_i = f_i^*$ or not, if it is true, A obtains the correct password PW_i of legal user U_i.
Step 3. Otherwise, A repeats the above steps until the correct password is found.

Thus, by launching the above off-line password guessing attack, the adversary can successfully recover the user's password.

3.3 Impersonation Attack

After getting the correct value $\{PW_i, ID_i\}$ of U_i, the malicious user A can further impersonate the user U_i to make fool of the server with the compromised values $\{c_i, e_i, g_i, j_i\}$ stored in the smart card.

Step 1. A computes $K_i = j_i \oplus (ID_i \| PW_i)$, $f_i = g_i \oplus (ID_i \| PW_i), r_i = h(PW_i \oplus K_i) \oplus f_i$, $h(ID_i \| x_s) = e_i \oplus r_i$.
Step 2. A chooses a random number R_a and computes $M_3' = h(x_s \| y_s) \oplus R_a$, $M_4' = (h(x_s \| y_s) \| R_a) \oplus ID_i$, $M_5' = h(h(ID_i \| x_s) \| R_a)$.
Step 3. A sends the message $\{M_3', M_4', M_5'\}$ to S_i. It is easy to see that S_i can accept this message. Then, S_i sends message $\{M_9', M_{10}'\}$ to U_i, where $M_9' = h(ID_i \| x_s) \oplus R_s'$, $M_{10}' = h(h(ID_i \| x_s) \| R_s')$, R_s' is a random number chosen by S_i.
Step 4. A computes $R_s' = M_9' \oplus h(ID_i \| x_s)$ and sends $M_{12}' = h(h(ID_i \| x_s) \| R_a \| R_s')$ to S_i.

The adversary A can be accepted by S_i as the user U_i.

3.4 Server Masquerading Attack

If an attacker A is able to obtain the secret values $\{c_i, e_i, g_i, j_i\}$ and $\{PW_i, ID_i\}$ of user U_i, then she can compute $h(ID_i \| X_s)$ just like in Sect. 3.3 and $M_9' = h(ID_i \| X_s) \oplus R_a$, $M_{10}' = h(h(ID_i \| X_s) \| R_a)$, where R_a is a random number generated by the attacker. A sends $\{M_9', M_{10}'\}$ to the user U_i. It is easy to see that the verification will be successful. Hence, the attacker can masquerade as a legitimate sever.

3.5 Mutual Authentication

According to the above analysis, if the smart card of a user is compromised, then the attacker A can successfully recover the user's password and identity. Moreover, he/she can perform user impersonation attack and server masquerading attack. Therefore, Khan et al.'s scheme fails to provide remote mutual authentication.

Table 1 Notations

U_i	The user
ID_i	Identity of U_i
PW_i	Password of U_i
R	Registration center
ID_R	Identity of R
T	The timestamp
S_i	The sever
SID_i	Identity of S_i
x_s, y_s	Secret keys of the sever
$h(\cdot)$	A secure collision-free one-way hash function

4 The Proposed Protocol

We propose a new biometric-based remote user authentication scheme using smart card. The new protocol has four phases: registration, login, authentication and password change. The notations that will be used in the proposed protocol are listed in Table 1. Our scheme comprises three participants: the trusted registration center R, the server S_i, and the user U_i. R selects the master secret key x and distributes $K_{RS} = h(SID_i \| x)$ to S_i via a secure channel, where SID_i is S_i's identity. Let $E_k(\cdot)/D_k(\cdot)$ denote the encryption and decryption algorithms of a symmetric-key encryption scheme (e.g. AES).

4.1 Registration Phase

The user U_i generates a random number K and submits his/her registration information $\{ID_i, PW_i \oplus K, B_i \oplus K\}$ to R through a secure channel. After receiving the request, R personalizes a smart card with parameters $(ID_i, h(\cdot), e_i, f_i)$, and sends the smart card to the user via a secure channel, where $f_i = h((B_i \oplus K) \| (PW_i \oplus K))$, $r_i = h(PW_i \oplus K \oplus B_i \oplus K) \oplus f_i = h(PW_i \oplus B_i) \oplus f_i$ and $e_i = h(ID_i \| x) \oplus r_i$. Finally, U_i stores the random number K into the smart card.

4.2 Login Phase

When the user U_i wants to login a remote server S_i, the user U_i inserts his/her smart card into a card reader and inputs ID_i, PW_i and the biometrics information B_i. The system first authenticates U_i's personal biometrics B_i and password PW_i by matching f_i, and then generates a request (ID_i, ID_R, M_2, M_3) to S_i. Here $r_i = h(PW_i \oplus B_i) \oplus f_i$, $M_1 = r_i \oplus e_i$, $M_2 = E_{M_1}(R_1, T_i)$, $M_3 = h(M_1 \| R_1 \| SID_i \| T_i)$, where T_i is timestamp and R_1 is a random number generated by U_i.

4.3 Authentication Phase

After receiving the login request, the remote server S_i performs the following steps with the user U_i and R.

Step 1. After receiving the login request message from U_i, S_i acquires the timestamp T_s and generates a nonce R_2. Then S_i computes $M_4 = h(K_{RS} \| ID_i \| SID_i \| M_2 \| M_3 \| T_s)$, $M_5 = E_{K_{RS}}(ID_i, M_2, M_3, M_4, R_2)$ and sends the message (M_5, SID_i, T_s) to R.

Step 2. Upon receiving (M_5, SID_i, T_s), R checks the validity of T_s. If it is invalid, R aborts the login request; else, R computes $K_{RS} = h(SID_i \| x)$ and $(ID_i, M_2, M_3, M_4, R_2)$

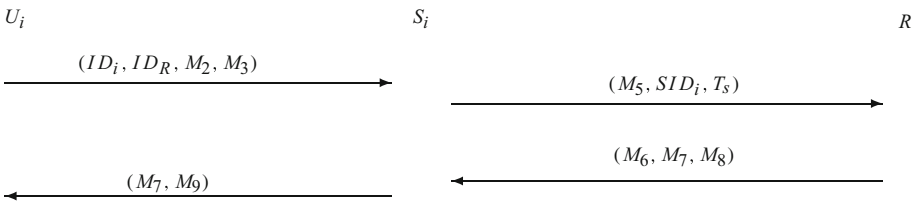


Fig. 1 Message flows in authentication phase

$= D_{K_{RS}}(M_5)$. Then R verifies the computed $h(K_{RS}\|ID_i\|SID_i\|M_2\|M_3\|T_s)$ with M_4 decrypted from M_5. If $M_4 = h(K_{RS}\|ID_i\|SID_i\|M_2\|M_3\|T_s)$, R continues to calculate $K_{RU} = h(ID_i\|x)$ and $(R_1, T_i) = D_{K_{RU}}(M_2)$. Subsequently, R checks the validity of T_i and verifies whether $M_3 = h(K_{RU}\|R_1\|SID_i\|T_i)$ or not. If either or both verifications fail, R terminates the session; otherwise, it acquires the timestamp T_r, generates a random number R_3 and computes $M_6 = E_{K_{RS}}(R_1, R_3, T_r)$, $M_7 = E_{K_{RU}}(R_1, R_2, R_3, T_r)$, $M_8 = h(K_{RS}\|ID_i\|SID_i\|M_6\|M_7)$, then sends (M_6, M_7, M_8) to the server S_i.

Step 3. S_i first verifies that $M_8 = h(K_{RS}\|ID_i\|SID_i\|M_6\|M_7)$ or not. If the verification is successful, S_i accepts the login request and computes $(R_1, R_3, T_r) = D_{K_{RS}}(M_6)$. Then, S_i verifies the validity of T_r, if it is invalid, S_i terminates this procedure immediately; on the contrary, S_i continues to calculate $M_9 = E_{R_3}(R_1, R_2, T_s', T_r)$ and the session key $SK = h(R_1\|R_2\|R_3)$, and then sends the message (M_7, M_9) to U_i, where T_s' is the timestamp.

Step 4. After receiving the message, U_i computes $(R_1, R_2, R_3, T_r) = D_{M_1}(M_7)$ and $(R_1, R_2, T_s', T_r) = D_{R_3}(M_9)$. Afterwards, U_i checks the validity of the timestamp T_s', T_r decrypted from M_9. If either or both have expired, the mutual authentication is given up by U_i himself/herself. Subsequently, U_i verifies whether T_r, R_1, R_2 decrypted from M_7 equals to the three decrypted from M_9, respectively. If the verifications fail, U_i terminates the session; otherwise, U_i sets $SK = h(R_1\|R_2\|R_3)$ as the session key shared with S_i (Fig. 1).

4.4 Password Change Phase

(1) U_i inserts his/her smart card into the device and enters his/her identity ID_i, old password PW_i^{old} and the biometrics information B_i.

(2) The smart card computes $f^* = H((B_i \oplus K)\|(PW_i^{old} \oplus K))$ and verifies if $f^* = f$ using the stored value f. If the equation does not hold, the smart card rejects the user. Otherwise, U_i enters his/her new password PW_i^{new} and the smart card computes $r_i^* = r_i \oplus h(PW_i^{old} \oplus B_i) \oplus h(PW_i^{new} \oplus B_i)$, $e_i^* = h(ID_i\|x) \oplus r_i^*$. The smart card then replaces the old values of (r_i, e_i) with (r_i^*, e_i^*) respectively.

5 Security Analysis of the Proposed Scheme

5.1 Authentication Proof Based on BAN Logic

In this section, we demonstrate that the proposed scheme is working correctly by achieving the authentication goals using BAN logic [21], which is vital to analyzing the correctness of

authentication protocols and uncovering protocol flaws in a logical manner. The notations used in BAN logic analysis are defined as follows:

- $\mathcal{P} \mid\equiv X$: The principal $\mathcal{P}$ believes a statement X or $\mathcal{P}$ would be entitled to believe X.
- $\sharp(X)$: The formula X is fresh.
- $\mathcal{P} \Rightarrow X$: The principal $\mathcal{P}$ has jurisdiction over the statement X.
- $\mathcal{P} \triangleleft X$: The principal $\mathcal{P}$ sees the statement X.
- $\mathcal{P} \mid\sim X$: The principal $\mathcal{P}$ once said the statement X.
- (X, Y): The formula X or Y is one part of the formula (X, Y).
- $\{X\}_Y$: The formula X is encrypted under the key Y.
- $\mathcal{P} \overset{K}{\longleftrightarrow} \mathcal{Q}$: The principals $\mathcal{P}$ and $\mathcal{Q}$ use the shared key K to communicate. Here, K will never be discovered by any principal except for $\mathcal{P}$ and $\mathcal{Q}$.
- SK: The session key used in the current session.

Some main logical postulates of BAN logic are described as follows:

- The message-meaning rule: $\frac{\mathcal{P}\mid\equiv\mathcal{Q}\overset{K}{\longleftrightarrow}\mathcal{P},\mathcal{P}\triangleleft\{X\}_K}{\mathcal{P}\mid\equiv\mathcal{Q}\mid\sim X}$.
- The freshness-conjuncatenation rule: $\frac{\mathcal{P}\mid\equiv\sharp(X)}{\mathcal{P}\mid\equiv\sharp(X,Y)}$.
- The nonce-verification rule: $\frac{\mathcal{P}\mid\equiv\sharp(X),\mathcal{P}\mid\equiv\mathcal{Q}\mid\sim X}{\mathcal{P}\mid\equiv\mathcal{Q}\mid\equiv X}$.
- The jurisdiction rule: $\frac{\mathcal{P}\mid\equiv\mathcal{Q}\Rightarrow X,\mathcal{P}\mid\equiv\mathcal{Q}\mid\equiv X}{\mathcal{P}\mid\equiv X}$, $\frac{\mathcal{P}\mid\equiv(X,Y)}{\mathcal{P}\mid\equiv X}$, $\frac{\mathcal{P}\mid\equiv\mathcal{Q}\overset{K}{\longleftrightarrow}\mathcal{P},\mathcal{P}\triangleleft\{X\}_K}{\mathcal{P}\triangleleft X}$, $\frac{\mathcal{P}\triangleleft(X,Y)}{\mathcal{P}\triangleleft X}$.

According to the analytic procedures of BAN logic, we list the verification goals of the proposed scheme in the following:

Goal.1: $U_i \mid\equiv (U_i \overset{SK}{\longleftrightarrow} S_i)$
Goal.2: $S_i \mid\equiv (U_i \overset{SK}{\longleftrightarrow} S_i)$
Goal.3: $R \mid\equiv (U_i \overset{SK}{\longleftrightarrow} S_i)$

Next, the proposed scheme is arranged from the generic type to the idealized form in the following:

Message 1: $U_i \rightarrow S_i$: $\{R_1, T_i\}_{K_{RU}}$
Message 2: $S_i \rightarrow R$: $\{\{R_1, T_i\}_{K_{RU}}, R_2, T_s\}_{K_{RS}}$
Message 3: $R \rightarrow S_i$: $(\{R_1, R_3, T_r\}_{K_{RS}}, \{R_1, R_2, R_3, T_r\}_{K_{RU}})$
Message 4: $S_i \rightarrow U_i$: $(\{R_1, R_2, R_3, T_r\}_{K_{RU}}, \{R_1, R_2, T_s', T_r\}_{R_3})$

We make the following assumptions about the initial state of the scheme to further analyze the proposed scheme:

A.1: $U_i \mid\equiv (U_i \overset{K_{RU}}{\longleftrightarrow} R)$
A.2: $S_i \mid\equiv (S_i \overset{K_{RS}}{\longleftrightarrow} R)$
A.3: $R \mid\equiv (U_i \overset{K_{RU}}{\longleftrightarrow} R)$
A.4: $R \mid\equiv (S_i \overset{K_{RS}}{\longleftrightarrow} R)$
A.5: $U_i \mid\equiv \sharp(T_r)$
A.6: $R \mid\equiv \sharp(T_s)$
A.7: $R \mid\equiv \sharp(T_i)$
A.8: $S_i \mid\equiv \sharp(T_r)$
A.9: $R \mid\equiv S_i \Rightarrow (\{R_1, T_i\}_{K_{RU}}, R_2, T_s)$
A.10: $S_i \mid\equiv R \Rightarrow (R_1, R_3, T_r)$

A.11: $U_i \mid\equiv R \Rightarrow (R_1, R_2, R_3, T_r)$
A.12: $R \mid\equiv U_i \Rightarrow (R_1, T_i)$

Based on the above-mentioned assumptions and rules of BAN logic, we analyze the idealized form of the proposed scheme and the main procedures of proof as follows:

According to the message 2, we obtain:

$$R \lhd \{\{R_1, T_i\}_{K_{RU}}, R_2, T_s\}_{K_{RS}}.$$

According to the assumption A.4 and the message-meaning rule, we obtain:

$$R \mid\equiv S_i \mid\sim (\{R_1, T_i\}_{K_{RU}}, R_2, T_s).$$

According to the assumption A.6 and the freshness-conjuncatenation rule, we obtain:

$$R \mid\equiv \sharp(\{R_1, T_i\}_{K_{RU}}, R_2, T_s).$$

According to $R \mid\equiv S_i \mid\sim (\{R_1, T_i\}_{K_{RU}}, R_2, T_s)$ and the nonce-verification rule, we obtain:

$$R \mid\equiv S_i \mid\equiv (\{R_1, T_i\}_{K_{RU}}, R_2, T_s).$$

According to the assumption A.9 and the jurisdiction rule, we obtain:

$$R \mid\equiv (\{R_1, T_i\}_{K_{RU}}, R_2, T_s).$$

According to the jurisdiction rule, we obtain:

$$R \mid\equiv R_2.$$

According to $R \lhd \{\{R_1, T_i\}_{K_{RU}}, R_2, T_s\}_{K_{RS}}$, the assumption A.4 and the jurisdiction rule, we obtain:

$$R \lhd (\{R_1, T_i\}_{K_{RU}}, R_2, T_s).$$

According to the jurisdiction rule, we obtain:

$$R \lhd \{R_1, T_i\}_{K_{RU}}.$$

According to the assumption A.3 and the message-meaning rule, we obtain:

$$R \mid\equiv U_i \mid\sim (R_1, T_i).$$

According to the assumption A.7 and the freshness-conjuncatenation rule, we obtain:

$$R \mid\equiv \sharp(R_1, T_i).$$

According to $R \mid\equiv U_i \mid\sim (R_1, T_i).$ and the nonce-verification rule, we obtain:

$$R \mid\equiv U_i \mid\equiv (R_1, T_i).$$

According to the assumption A.12 and the jurisdiction rule, we obtain:

$$R \mid\equiv (R_1, T_i).$$

According to the jurisdiction rule, we obtain:

$$R \mid\equiv R_1.$$

According to $SK = h(R_1 \| R_2 \| R_3)$, we obtain:

$$R \mid\equiv (U_i \overset{SK}{\longleftrightarrow} S_i)(\textbf{Goal 3}).$$

According to the message 3, we obtain:

$$S_i \lhd (\{R_1, R_3, T_r\}_{K_{RS}}, \{R_1, R_2, R_3, T_r\}_{K_{RU}}).$$

According to the jurisdiction rule, we obtain:

$$S_i \lhd \{R_1, R_3, T_r\}_{K_{RS}}.$$

According to the assumption A.2 and the message-meaning rule, we obtain:

$$S_i \mid\equiv R \mid\sim (R_1, R_3, T_r).$$

According to the assumption A.8 and the freshness-conjuncatenation rule, we obtain:

$$S_i \mid\equiv \sharp(R_1, R_3, T_r).$$

According to $S_i \mid\equiv R \mid\sim (R_1, R_3, T_r)$ and the nonce-verification rule, we obtain:

$$S_i \mid\equiv R \mid\equiv (R_1, R_3, T_r).$$

According to the assumption A.10 and the jurisdiction rule, we obtain:

$$S_i \mid\equiv (R_1, R_3, T_r).$$

According to the jurisdiction rule, we obtain:

$$S_i \mid\equiv R_1,$$
$$S_i \mid\equiv R_3.$$

According to $SK = h(R_1 \| R_2 \| R_3)$, we obtain:

$$S_i \mid\equiv (U_i \overset{SK}{\longleftrightarrow} S_i) (\textbf{Goal 2}).$$

According to the message 4, we obtain:

$$U_i \lhd (\{R_1, R_2, R_3, T_r\}_{K_{RU}}, \{R_1, R_2, T_s', T_r\}_{R_3}).$$

According to the jurisdiction rule, we obtain:

$$U_i \lhd \{R_1, R_2, R_3, T_r\}_{K_{RU}}.$$

According to the assumption A.1 and the message-meaning rule, we obtain:

$$U_i \mid\equiv R \mid\sim (R_1, R_2, R_3, T_r).$$

According to the assumption A.5 and the freshness-conjuncatenation rule, we obtain:

$$U_i \mid\equiv \sharp(R_1, R_2, R_3, T_r).$$

According to $U_i \mid\equiv R \mid\sim (R_1, R_2, R_3, T_r)$ and the nonce-verification rule, we obtain:

$$U_i \mid\equiv R \mid\equiv (R_1, R_2, R_3, T_r).$$

According to the assumption A.11 and the jurisdiction rule, we obtain:

$$U_i \mid\equiv (R_1, R_2, R_3, T_r).$$

According to the jurisdiction rule, we obtain:

$$U_i \mid\equiv R_2,$$
$$U_i \mid\equiv R_3.$$

According to $SK = h(R_1 \| R_2 \| R_3)$, we obtain:

$$U_i \mid\equiv (U_i \overset{SK}{\longleftrightarrow} S_i)(\textbf{Goal 1}).$$

5.2 Discussion on the Possible Attacks

In the following, we show that our proposed scheme can resist different types of attacks. We assume that the secret values stored in the smart card can be obtained by an attacker.

5.2.1 User Impersonation Attack

If an attacker wants to impersonate as a legitimate user to login the server, he/she must forge a correct login request message, which can be authenticated to the registration center R. However, the attacker cannot do this even if he/she can extract the secret values (f_i, e_i, K) stored in the user's smart card, because the attacker cannot compute the login request message (M_2, M_3) without knowing the value $h(ID_i \| x)$ which can only be computed based on the knowledge of PW_i and B_i. Hence, our proposed scheme can resist against the user impersonation attack.

5.2.2 Server Masquerading Attack

If an attacker wants to impersonate as the legitimate server S_i to fool the user, he/she must forge the correct message (M_7, M_9). However, since the attacker does not have the value $K_{RS} = h(SID_i \| x)$, she cannot obtain the value of R_1 or R_3, and therefore cannot compute the correct M_9. Hence, the attacker cannot perform server masquerading attacks to fool the user.

5.2.3 Password Guessing Attack

Suppose the attacker can extract the secret values (f_i, e_i, K) stored in the user's smart card, and try to derive the user's password PW_i based on some protocol transcripts. In our newly proposed protocol, we have $e_i = h(ID_i \| x) \oplus h(PW_i \oplus B_i) \oplus f_i$, and thus $h(ID_i \| x) = e_i \oplus f_i \oplus h(PW_i \oplus B_i)$ where $h(ID_i \| x)$ is used by the user in the login requests. However, different from the attack against An's protocol, now the attacker cannot derive the value of $h^* = e_i \oplus f_i \oplus h(PW_i^* \oplus B_i)$ based on a guessed password PW^* and then use the user's protocol transcripts to verify the correctness of the derived h^*, since the attacker does not know the user's biometrics information B_i.

5.2.4 Replay Attack

In a replay attack, the adversary first eavesdrops the communication flows of U_i, and later tries to imitate U_i to login S_i by replaying the eavesdropped messages. The proposed scheme is capable of detecting and resisting the replay attack since the random nonce and timestamp is contained in each session run. If an adversary eavesdrops and replays any login request message of U_i, the replayed message can be easily detected and dropped by R. Similarly, the adversary cannot replay the messages sent by R or S_i.

5.2.5 Insider Attack

In our new scheme, the user submits $(PW_i \oplus K, B_i \oplus K)$ instead of (PW_i, B_i) to the registration center R in the registration phase. Thus, the registration center cannot obtain PW_i or B_i which may also be used by the user in other applications. Hence, our proposed scheme is secure against the insider attack. However, we remark that for insider attack, we don't consider the situation that the registration server can obtain the value of K stored in the user's smart card.

5.2.6 Stolen Smart Cards Attacks

If an attacker stole the smart card of user U_i and wants to use the obtained smart card to login to the server, he/she has to input the correct information ID_i, PW_i, B_i of the user U_i. However, the attacker does not know U_i's PW_i, B_i, he/she can not successfully be authenticated by the server.

We further assume that the attacker can retrieve all the information $\{ID_i, f_i, e_i, K\}$ stored in the smart card by monitoring the power consumption [11,12]. Note that the user's biometric data B_i is not stored in the smart card, and the attacker knows neither B_i nor PW_i. Suppose the attacker wants to obtain x or PW_i from the retrieved message. From $f_i = h((B_i \oplus K)\|(PW_i \oplus K))$ the attacker has no feasible way to obtain PW_i, because he/she has to guess PW_i and B_i at the same time. Similarly, the attacker can not obtain PW_i, x from the information $e_i = h(ID_i\|x) \oplus h(PW_i \oplus B_i) \oplus f_i$, he/she has to guess PW_i,B_i and x at the same time.

5.2.7 Known Key Security

After the mutual authentication, an authentication scheme with key agreement allows the user and the server share an unique secret session key. The known key security means that even one session key is compromised, it should have no impact on other session keys. In the proposed scheme, with the compromised session key $SK = H(R_1\|R_2\|R_3)$, the adversary still cannot further compromise other secret keys or session keys due to the randomness of R_1, R_2 and R_3. Hence, the proposed scheme can achieve known key security.

6 Security Comparison

We compare our new scheme with two recently proposed biometric based remote user authentication schemes due to Khan [20] and An [19]. In Table 2, we provide the comparison based on the key security properties of these schemes. From the table, we can see that our proposed scheme provides better security than the other two schemes. Khan's scheme in [20] and An's scheme in [19] only satisfies two criterion listed in Table 2. Our proposed scheme satisfies all the criteria listed in Table 2. In particular, one special feature of our scheme is that we demonstrate the validity of the proposed scheme through the BAN logic.

7 Conclusion

In the paper, we analyzed the security of Khan et al.'s biometric-based remote user authentication scheme using smart cards. We showed that Khan et al.'s scheme is insecure against

Table 2 Security comparison

Feature	An [19]	Khan et al. [20]	Ours
Prevent user impersonation attack	×	×	✓
Prevent sever masquerading attack	×	×	✓
Prevent password guessing attack	×	×	✓
Prevent stolen smart cards attacks	×	×	✓
Mutual authentication	×	×	✓
Strong replay resistance	✓	✓	✓
Prevent insider attack	✓	✓	✓

the password guessing attack and fails to provide mutual authentication between the user and the server if the smart card has been compromised. Subsequently, we proposed a robust biometric-based remote user authentication protocol using smart cards which can overcome these security weaknesses. The security proof and analysis show that our proposed scheme is secure against various attacks. Also, only symmetric-key cryptographic techniques are used in our new scheme, which makes the scheme very practical.

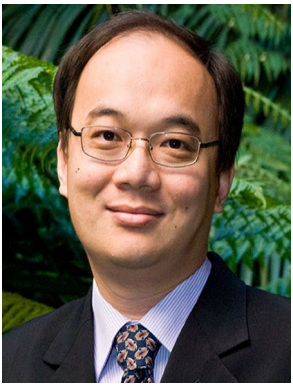
Acknowledgments The authors are grateful to the editor and anonymous reviewers for their valuable suggestions, which improved the paper. This work is supported by Natural Science Foundation of Shandong Province(Grant No. ZR2013FM009).

References

1. Lamport (1981). Password authentication with insecure communication. *Communications of the ACM*, *24*(11), 770–772.
2. Zhu, J., & Ma, J. (2004). A new authentication scheme with anonymity for wireless environment. *IEEE Transactions on Consumer Electronics*, *50*(1), 230–234.
3. Chang, C. C., Lee, C. Y., & Chiu, Y. C. (2009). Enhanced authentication scheme with anonymity for roaming service in global mobility networks. *Computer Communications*, *32*(4), 611–618.
4. Das, A. K. (2013). A secure and effective user authentication and privacy preserving protocol with smart cards for wireless communications. *Networking Science*, 2(1-2), 12–27.
5. He, D., Ma, M., Zhang, Y., Chen, C., & Bu, J. (2011). A strong user authentication scheme with smart cards for wireless communications. *Computer Communications*, *34*(3), 367–374.
6. Wen, F. T., Susilo, W., & Yang, G. M. (2013). A secure and effective anonymous user authentication scheme for roaming service in global mobility networks. *Wireless Personal Communication*, *73*, 993–1004.
7. Lee, C. C., Hwang, M. S., & Liao, I. E. (2006). Security enhancement on a new authentication scheme with anonymity for wireless environments. *IEEE Transactions on Industrial Electronics*, *53*(5), 1683–1686.
8. Li, C. T., & Lee, C. C. (2012). A novel user authentication and privacy preserving scheme with smart cards for wireless communications. *Mathematical and Computer Modelling*, *55*(1–2), 35–44.
9. Wu, C. C., Lee, W. B., & Tsaur, W. J. (2008). A secure authentication scheme with anonymity for wireless communications. *IEEE Communications Letters*, *12*(10), 722–723.
10. Yang, G., Wong, D. S., Wang, H., & Deng, X. (2008). Two-factor mutual authentication based on smart cards and passwords. *Journal of Computer and System Sciences*, *74*(7), 1160–1172.
11. Kocher, P., Jaffe, J., & Jun, B. (1999). Differential power analysis. *Advances in Cryptology-CRYPTO, LNCS*, *1666*, 388–397.
12. Messerges, T. S., Dabbish, E. A., & Sloan, R. H. (2002). Examining smart-card security under the threat of power analysis attacks. *IEEE Transactions on Computers*, *51*(5), 541–552.
13. Ku, W. C., Chang, S. T., & Chiang, M. H. (2005). Further cryptanalysis of fingerprint-based remote user authentication scheme using smartcards. *Electronics Letters*, *41*(5), 240–241.
14. Khan, M. K., & Zhang, J. (2006). An efficient and practical fingerprint-based remote user authentication scheme with smart cards. *Lecture Notes in Computer Science*, *3903*, 260–268.

15. Baig, A., Bouridane, A., Kurugollu, F., & Qu, G. (2009). Fingerprint-Iris fusion based identification system using a single hamming distancematcher. *International Journal of Bio-Science and Bio-Technology*, *1*(1), 47–58.
16. Chang, C. C., Chang, S. C., & Lai, Y. W. (2010). An improved biometrics-based user authentication scheme without concurrency system. *International Journal of Intelligent Information Processing*, *1*(1), 41–49.
17. Li, C. T., & Hwang, M. S. (2010). An efficient biometrics-based remote user authentication scheme using smart cards. *Journal of Network and Computer Applications*, *33*(1), 1–5.
18. Das, A. K. (2011). Analysis and improvement on an efficient biometric-based remote user authentication scheme using smart cards. *IET Information Security*, *5*(3), 541–552.
19. An, Y. H. (2012). Security analysis and enhancements of an effective biometric-based remote user authentication scheme using smart cards. *Journal of Biomedicine and Biotechnology*, Article ID 519723, 2012. doi:10.1155//519723.
20. Khan, M. K., & Kumari, S. (2013). An improved biometrics-based remote user authentication scheme with user anonymity. *Journal of Biomedicine and Biotechnology*, Article ID 491289, 2013.
21. Burrows, M., Abadi, M., & Needham, R. (1990). A logic of authentication. *ACM Transactions on Computer Systems*, *8*(1), 18–36.

Fengtong Wen received his Ph.D. degree at Beijing University of Posts and Telecommunications. Now he is a professor of University of Jinan. His main research topics are Cryptography and information security. He has published more than 20 research paper.



Willy Susilo received a Ph.D. in Computer Science from University of Wollongong, Australia. He is a Professor at the School of Computer Science and Software Engineering and the director of Centre for Computer and Information Security Research (CCISR) at the University of Wollongong. He is currently holding the prestigious ARC Future Fellow awarded by the Australian Research Council (ARC). His main research interests include cryptography and information security. His main contribution is in the area of digital signature schemes. He has served as a program committee member in dozens of international conferences. He has published numerous publications in the area of digital signature schemes and encryption schemes.

Guomin Yang received his Ph.D. in Computer Science from the City University of Hong Kong in 2009. He worked as a Research Scientist in the Temasek Laboratories at the National University of Singapore from 2009 to 2012. He is now a Lecturer in the School of Computer Science and Software Engineering at the University of Wollongong. His main research interests include applied cryptography and network security.