International Journal of Security and Its Applications
Vol. 10, No. 1 (2016), pp.315-328
http://dx.doi.org/10.14257/ijsia.2016.10.1.29

An Enhanced Biometric-Based Three Factors User Authentication Scheme for Multi-server Environments

Youping Lin[1, *], Kaihui Wang[2], Baocan Zhang[1], Yuzhen Liu[2], Xiong Li[2]

[1]*Chengyi University College, Jimei University, Xiamen 361021, China*
[2]*School of Computer Science and Engineering, Hunan University of Science and Technology, Xiangtan 411201, China*
[*] *youpinglin@126.com*

Abstract

Authentication is an important and basic security service for many network based applications, which allows the registered user access remote services after the validity of his/her identity is verified by the remote server. Password, smart card and biometric are three frequently used factors in authentication, and some remote user authentication schemes for different environments had been presented based on these factors by researchers. Recently, Baruah et al. pointed out the weaknesses of Mishra et al.'s three factors user authentication scheme for multi-server environments, and they proposed an enhanced scheme. They claimed that their scheme has many security features and can resist some common attacks. However, based on our analysis, Baruah et al.'s scheme cannot resist stolen smart card attack, cannot protect user's anonymity, and it is also vulnerable to Denial of Service attack. In this paper, an enhanced three factors user authentication scheme for multi-server environments based on fuzzy extractor technology is proposed, and the analysis show that the proposed scheme is more security and efficient than other related schemes.

Keywords*: user authentication, biometric, fuzzy extractor, smart card, multi-server environment*

1. Introduction

In today's information society, the network is everywhere and people can access a variety of services via network only by clicking the mouse in front of the screen. Although the network brings us convenient for our life, the network and information security problems go along with it bring people great troubles. So, how to ensure user securely accesses the remote network services becomes an important thing. There are some techniques to protect the information and network security, such as user authentication, access control, intrusion detection technology, *etc*. These techniques resolve the information and network security problems from different perspectives, and among these techniques, the user authentication is a basis and efficient mechanism.

In order to real the user authentication, the user first registers to remote server, and the server stores some personal secret information of the user. At the time of authentication, the user presents the personal secret information to the server, and the server compares it with the information stored in the database to verify the validity of the user. Generally, there are three types of factors can be used to the authentication system: (1) what the user know, such as the password; (2) what the user have, such as the smart card, and (3) what the user is, such as the biometric. Due to its convenient, easy to deploy and use, password

ISSN: 1738-9976 IJSIA

mechanism is widely used in network based applications such as forum, html email, *etc*. However, it is also the most vulnerable method. [1]

A smart card, contains an embedded integrated circuit, is also widely used in some applications such as bank due to it has storage, calculation, data encryption and other functions. Compared with the password and smart card, the biometric characteristics such as fingerprints and faces, are usually universal, unique and cannot be duplicated, lost or forgotten, can be used as an excellent method for user authentication. The researcher can design a user authentication scheme for different levels of security requirements by adopting these three factors.

Since Lamport [1] proposed the first password user authentication scheme for insecure networks, many remote user authentication schemes for different environments were proposed, such as user authentication schemes for single server environments, multi-server environments, *etc*. In these schemes, biometric based user authentication scheme is an important type. In 2002, Lee et al. [2] first proposed a fingerprint-based remote user authentication scheme using smart cards, where the user can access the remote servers if the identity, password and fingerprint are pass the verification. However, their scheme was found vulnerable to masquerade attack [3] and conspiring attack [4]. In 2003, a password authentication scheme based on smart cards and fingerprints was proposed by Kim et al. [5], however, there scheme was found insecure [6]. Khan and Zhang [7] pointed out Lin and Lai's biometrics-based authentication scheme [3] is susceptible to the server spoofing attack. In 2010, Li and Hwang [8] proposed a biometric based three factors remote user authentication scheme, their scheme is very efficient due to it just needs one-way hash function operations. However, Li and Hwang's scheme was found vulnerable to man-in-the-middle attack and denial of service attack [9]. Besides, their scheme was found existed some other security weaknesses [10]. Recently, An [11] proposed an improved three-factors user authentication scheme to overcome the security weaknesses of Das's scheme [10]. However, Li et al. [12] found An's scheme is also exist some flaws, *i.e*. it cannot resist denial-of-service (DoS) attack caused by the hash function problem in biometric authentication, cannot resist forgery attack, cannot quickly detect unauthorized login, and does not provide session key agreement. In 2014, Chuang and Chen [13] proposed a multi-server authenticated key agreement scheme using smart card and biometrics with anonymity property. However, it was found cannot resist stolen smart card attack and impersonation attacks, and an enhanced scheme was proposed by Mishra et al [14]. Recently, Baruah et al. [15] found Mishra et al.'s scheme [14] also cannot withstand stolen smart card attack and impersonation attacks, and they presented an improved scheme. Unfortunately, based on our analysis, Baruah et al.'s scheme [15] cannot resist stolen smart card attack, cannot protect user anonymity, and it is also vulnerable to Denial of Service attack. In order to overcome the aforementioned weaknesses, an enhanced three factors user authentication scheme for multi-server environments based on fuzzy extractor technology [16] is proposed in this paper, and the analysis show that the proposed scheme is more secure and efficient than other related schemes.

The rest of this paper is organized as follows: a briefly review of Baruah et al.'s scheme [15] is given in section 2. Some security weaknesses of Baruah et al.'s scheme [15] are pointed out in section 3. The enhanced three factors user authentication scheme for multi-server environments and the corresponding security analysis are given in section 4 and section 5, respectively. At last, section 6 concludes the full paper.

2. Review of Baruah et al.'s Scheme

Baruah et al. [15] pointed out the security weaknesses of Mishara et al.'s scheme [14], and proposed an improved biometric-based multi-server authentication scheme using

Youping Lin is the corresponding author.

smart card. In this section, we briefly review Baruah et al.'s scheme. There are three parties in Baruah et al.'s scheme, *i.e*. user U_i, server SID_j and registration center *RC*. Where the registration center *RC* is responsible for the registration of the user and the server. Their scheme contains four phases, *i.e*. the registration phase, login phase, authentication phase and password change phase. We list the notations used in this paper in table 1, and the detailed description of their scheme is as follow.

Table 1. Notations Used in This Paper

Notation	Description
ID_i	Identity of the *i*th user
SID_j	Identity of the *j*th sever
RC	Registration center
PW_i	Password of the *i*th user
BIO_i	Biometric of the *i*th user
PSK	Pre-shared key of the servers
x	Master secret key maintained by the registration center
$h(\cdot)$	A one way hash function
$\oplus$	Exclusive-OR operation
$\|\|$	Message concatenation operation

2.1. Registration Phase

In Baruah et al.'s scheme [15], the registration phase contains two sub-phases, *i.e*. the server registration phase and the user registration phase. In this phase, the user and the server should register themselves to the registration center and gets secret information to initial the system.

Server Registration Phase: Before becoming a service provider, the server has to register itself to the registration center *RC*. The server sends its identity SID_j as the registration request to the registration center *RC*. In response, *RC* submits the secret information $h(SID_j||h(PSK))$ and $h(PSK||x)$ to server SID_j through the Internet Key Exchange Protocol version 2 (IKEv2) [17].

User Registration Phase: When a user wants to access the services provided by the registered servers, he/she has to register to the registration center *RC*. The user U_i chooses an identity ID_i and a password PW_i, and presents his/her biometric information BIO_i at the sensor terminal. Then, U_i submits the identity ID_i and $R_1 = h(PW_i||BIO_i)$ to the registration center through a secure channel. The registration center then computes:

$A_i = h(ID_i||x)$;

$B_i = h(PSK||x) \oplus A_i$;

$C_i = h(R_1||ID_i) \oplus h(A_i)$;

$D_i = h(PSK) \oplus h(ID_i)$;

$E_i = R_1 \oplus ID_i$.

The registration center chooses a smart card SC_i for U_i, and stores the information $\{B_i, C_i, D_i, E_i, h(\cdot)\}$ into the smart card. Then the smart card is provided to the user via a secure channel.

2.2. Login Phase

In order to access the registered server S_j, the user U_i first logins to the server using the smart card SC_i. U_i inserts the smart card into the card reader and enters the identity ID_i, password PW_i, and then imprints the biometric information BIO_i at the sensor. SC_i executes the following steps to generate a login request:

(1) SC_i computes $R_1 = h(PW_i||BIO_i)$, $ID_i' = R_1 \oplus E_i$, and checks whether the entered identity ID_i equals to ID_i'. If they are not equal, the session is immediately terminated. Otherwise, the following steps are executed.
(2) SC_i computes $h(PSK) = h(ID_i) \oplus D_i$, $h(A_i) = C_i \oplus h(R_1||ID_i)$ using the smart card data.
(3) SC_i generates a nonce N_i and computes:

$M_1 = h(SID_j||h(PSK)) \oplus h(ID_i||N_i)$;

$M_2 = N_i \oplus h(A_i)$;

$V_1 = h(N_i \oplus B_i)$.

(4) The smart card transmits the login request message $\{B_i, M_1, M_2, V_1\}$ to the server SID_j via a public channel.

2.3. Authentication Phase

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

(1) Using the secret information $h(SID_j||h(PSK))$, $h(PSK||x)$ and the login request message, SID_j computes $A_i = B_i \oplus h(PSK||x)$, $h(ID_i||N_i) = M_1 \oplus h(SID_j||h(PSK))$ and $N_i = M_2 \oplus h(A_i)$.
(2) SID_j computes $V_1' = h(N_i \oplus B_i)$, and checks whether it equal to V_1 or not. If they are not equal, the session is aborted. Otherwise, SID_j generates a random nonce N_j.
(3) SID_j generates a session key $SK_{ji} = h(h(ID_i||N_i)||SID_j||B_i||N_j)$ using the user's information and its nonce N_j and identity SID_j.
(4) SID_j computes $M_3 = N_j \oplus h(ID_i||N_i)$, $V_2 = N_i \oplus h(SK_{ji}||N_j)$, and submits $\{M_3, V_2\}$ to U_i via a public channel.
(5) When receiving the message $\{M_3, V_2\}$, U_i computes $N_j = M_3 \oplus h(ID_i||N_i)$ and $SK_{ij} = h(h(ID_i||N_i)||SID_j||B_i||N_j)$.
(6) U_i computes $N_i' = V_2 \oplus h(SK_{ij}||N_j)$, and checks whether it equals to N_i. If they are equal, the validity of the server SID_j is verified by U_i, and U_i shares a session key SK_{ij} (=SK_{ij}) with SID_j.

2.4. Password Change Phase

In this phase, the user can change his/her password without communicate with the registration center. U_i inserts the smart card SC_i into the card reader and enters the identity ID_i, password PW_i, and imprints the biometric BIO_i at the sensor. SC_i computes $R_1 = h(PW_i||BIO_i)$, $ID_i' = R_1 \oplus E_i$, and checks whether the entered identity ID_i equals to ID_i'. If so, the user can input a new password PW_i^*, and then SC_i computes:

$R_1^* = h(PWi^*||BIO_i)$

$E_i^* = E_i \oplus R_1 \oplus R_1^*$

$C_i^* = h(R_1^*||ID_i) \oplus h(R_1||ID_i) \oplus C_i$

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

3. Cryptanalysis of Baruah et al.'s Scheme

Although Baruah et al. [15] shown their scheme can resist types of attacks, some weaknesses are also found by us. In this section, a cryptanalysis of Baruah et al.'s scheme [15] is pointed out, and their scheme is found cannot resist stolen smart card attack, denial of service attack, and cannot protect user's anonymity.

3.1. Stolen Smart Card Attack

The stolen smart card attack is that if the user's smart card was stolen by an adversary, he/she can extract the information stored in the smart card by using the methods mentioned in references [18, 19], and then guess corresponding password or impersonate the user to login to the system by generating a valid login request message. In Baruah et al.'s scheme [15], they claimed their scheme can resist stolen smart card attack even if the adversary is a user or a server. However, the truth is not the case, and we find a user or a server can use a stolen smart card to generate a valid login request message.

In this section, we suppose user U_i's smart card is stolen by a malicious user U_k. U_k has his/her own smart card SC_k, and can extract the information $\{B_k, C_k, D_k, E_k, h(\cdot)\}$ from the smart card by using the methods mentioned in references [18, 19]. Then, using the smart card information and his/her own identity ID_k, U_k can get $h(PSK) = D_k \oplus h(ID_k)$. U_k extracts U_i's smart card information $\{B_i, C_i, D_i, E_i, h(\cdot)\}$, and computes $h(ID_i) = h(PSK) \oplus D_i$. Then U_k can guess the identity ID_i by using the dictionary attack, *i.e*. U_k chooses an identity ID_i', and compares whether $h(ID_i') = h(ID_i)$, and this operation is repeated until the right identity ID_i is found. Next, U_k computes $R_1 = E_i \oplus ID_i$, $h(A_i) = h(R_1||ID_i) \oplus C_i$. When gets the information $\{B_i, ID_i, h(PSK), h(A_i)\}$, U_k can impersonate as user U_i to login in the server SID_j by generating a valid login request message. U_k generates a nonce N_i and computes $M_1 = h(SID_j||h(PSK)) \oplus h(ID_i||N_i)$, $M_2 = N_i \oplus h(A_i)$, $V_1 = h(N_i \oplus B_i)$. This login request message will be accepted by the server due to the login request will be verified successfully, and at last U_k shares a session key SK_{ij} with the server SID_j. Besides, if U_i's smart card is stolen by a valid but malicious server, since he/she has the secret information $h(PSK)$, he/she also can masquerade as user U_i to generate a valid login request message by using the method mentioned above. Therefore, Baruah et al.'s scheme is vulnerable to stolen smart card attack.

3.2. No Provision of User Anonymity

With the rapid development and wide application of network technology, the protection of user's privacy in network based applications such as in online shopping, online game, have received more and more attentions. In privacy protection of network based applications, the location and the identity information are two important aspects, and user anonymity is a desirable property for remote user authentication. The user authentication scheme with user anonymity can protect the user's sensitive information such as personal preference, social circle, shopping patterns, from being revealed by adversary thorough the analysis of the login information.

Generally, the scheme with user anonymity contains two aspects of content, one is the user's real identity cannot be revealed by an adversary, and another is that the user cannot be traced by an adversary by using the login request. Dynamic ID technique is the most used method in user authentication scheme to provide the property of user anonymity, where the user's identity is dynamic change for each session and makes the adversary cannot get the real identity of the user or trace a special user.

In each login phase of Baruah *et al*.'s scheme [15], user U_i submits the login request message $\{B_i, M_1, M_2, V_1\}$ to the server SID_j. In this message, B_i ($A_i = h(PSK||x) \oplus h(ID_i||x)$) is fixed and unique for each user when he/she had registered, and it can be seen as user U_i's identification. Although the adversary cannot reveal user U_i's real identity from the login request message, he/she can distinguish whether two sessions are launched by the same user. Therefore, the adversary can trace a special user by using B_i as the identification, and Baruah *et al*.'s scheme fails to preserve user anonymity.

3.3. Denial of Service

As shown in [9], in a typical biometric authentication system, the user's biometric feature information is extracted by the biometric process equipment as the biometric

template in the registration phase. In the authentication phase, the user's biometric information is scanned by the sensor terminal, and the scanned biometric information is compared with the biometric template to verify whether the user is a valid one. Generally, there are some noises during the extraction of the biometric, and this feature makes the biometric information extracted in different time are not totally the same. Therefore, most of biometric authentication methods are rely on the similarity comparison between the scanned biometric information with the biometric template. There is a pre-defined threshold for the similarity comparison, if the similarity between the scanned biometric information with the template is higher than the threshold, the biometric is claimed to be match, and otherwise the biometric authentication is failed. On the other side, hash functions have a fundamental property that its outputs are very sensitive to small perturbations in the inputs. Therefore, hash functions cannot be directly applied to biometric authentication due to the inputted biometric information will not be exactly the same for each time. However, in login phase of Baruah *et al*.'s scheme [15], U_i inserts the smart card into the card reader and enters the identity ID_i, password PW_i, and then imprints the biometric information BIO_i' (which would not equal to BIO_i) at the sensor. SC_i computes $R_1' = h(PW_i||BIO_i')$ ($\neq R_1$), and gets $ID_i' = R_1' \oplus E_i \neq ID_i$. Therefore, the noise property of biometric would cause the legal user unable to pass the biometric authentication, and Baruah *et al*.'s scheme [15] is vulnerable to denial of service attack.

4. The Proposed Scheme

In order to remove the security weaknesses of Baruah *et al*.'s scheme [15], an enhanced three factors user authentication scheme for multi-server environments is proposed based on the so called fuzzy extractor technique [16].

4.1. Basis of Biometric Authentication-Fuzzy Extractor

In this subsection, we introduce a basis of biometric authentication-fuzzy extractor, which converts biometric data into random strings, and makes it possible to apply cryptographic techniques for biometric security. Based on the reference [16], for the inputted biometrics B_i, the fuzzy extractor can reliably extract a uniform randomness pair (R_i, P_i), and the extraction is error tolerant that R_i will be the same under the help of auxiliary information P_i even if the inputted biometric has some little difference, as long as it remains reasonably close to the original. Generally, a fuzzy extractor is given by two procedures (*Gen*, *Rep*).

(1) $Gen(B_i) = (R_i, P_i)$

Gen is a probabilistic generation procedure, which on biometric input B_i outputs an "extracted" string R_i and an auxiliary string P_i.

(2) $Rep(B_i, P_i) = R_i$ if B_i' is reasonably close to B_i

Rep is a deterministic reproduction procedure, which allows to recover R_i from the corresponding auxiliary string P_i and any vector B_i' close to B_i.

The detailed information about fuzzy extractor can be founded in literature [16].

4.2. Registration Phase

In our scheme, the registration phase also contains two sub-phases, *i.e*. the server registration phase and the user registration phase. In this phase, the user and the server should register themselves to the registration center and gets secret information to initial the system.

Server Registration Phase: Before becoming a service provider, the server has to register itself to the registration center *RC*. The server sends its identity SID_j as the

registration request to the registration center. In response, *RC* submits the secret information $h(SID_j||h(PSK))$ and $h(PSK||x)$ to server SID_j through the Internet Key Exchange Protocol version 2 (IKEv2) [17].

User Registration Phase: When a user wants to access the services provided by the registered servers, he/she has to register to the registration center *RC*. The user U_i first chooses an identity ID_i and a password PW_i, and presents his/her biometric information BIO_i at the sensor terminal to gets $Gen(BIO_i) = (R_i, P_i)$. Then, U_i submits $\{ID_i, A_i = h(PW_i||R_i), P_i\}$ to the registration center through a secure channel. The registration center then computes:

$B_i = h(ID_i||A_i)$;

$C_i = h(ID_i||x)$;

$D_i = h(PSK||x) \oplus C_i$;

$E_i = h(A_i||ID_i) \oplus h(C_i)$;

$F_i = h(PSK) \oplus A_i$.

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

4.3. Login Phase

In order to access the registered server SID_j, the user U_i first logins to the server using the smart card SC_i. U_i inserts the smart card into the card reader and enters the identity ID_i, password PW_i. Then U_i imprints the biometric information BIO_i' at the sensor with fuzzy extractor and gets $R_i' = Rep(BIO_i', P_i)$. SC_i executes the following steps to check the validity of user's identity, password and biometric, and generate a login request:

(1) SC_i computes $A_i' = h(PW_i||R_i')$, $B_i' = h(ID_i||A_i')$, and checks whether B_i' equals to B_i. If they are not equal, one of the factors is not valid and the session is immediately terminated. Otherwise, the following steps are executed.

(2) SC_i generates a nonce N_i and computes:

$h(C_i) = h(A_i'||ID_i) \oplus E_i$;

$h(PSK) = F_i \oplus A_i'$;

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

$M_2 = D_i \oplus N_i$;

$M_3 = h(h(C_i)||N_i)$.

(3) The smart card transmits the login request message $\{M_1, M_2, M_3\}$ to the server SID_j via a public channel.

4.4. Authentication Phase

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

(1) SID_j computes $N_i = M_1 \oplus h(SID_j||h(PSK))$, $C_i' = M_2 \oplus h(PSK||x) \oplus N_i$, $M_3' = h(h(C_i')||N_i)$, and checks whether M_3' equals to M_3. If they are not equal, the session is terminated by SID_j. Otherwise, the validity of U_i is authenticated by the server, and SID_j performs the following steps.

(2) SID_j generates a nonce N_j, and computes $SK_{ji} = h(h(C_i')||SID_j||N_i||N_j)$.

(3) SID_j computes $M_4 = N_i \oplus N_j$, $M_5 = h(SK_{ji}||N_j)$, and submits the response message $\{M_4, M_5\}$ to U_i.

(4) When receiving the message $\{M_4, M_5\}$, U_i computes $N_j = M_4 \oplus N_i$, $SK_{ij} = h(h(C_i)||SID_j||N_i||N_j)$.

(5) U_i computes $M_5' = h(SK_{ij}||N_j)$, and checks whether M_5' equals to M_5. If they are not equal, the session is rejected. Otherwise, SID_j is authenticated by the user U_i, and they are share a session key SK_{ij} (= SK_{ji}) at last.

4.5. Password Change Phase

In this phase, the user can change his/her password without communicate with the registration center. U_i inserts the smart card into the card reader and enters the identity ID_i, password PW_i. Then U_i imprints the biometric information BIO_i' at the sensor with fuzzy extractor and gets $R_i' = Rep(BIO_i', P_i)$. SC_i computes $A_i' = h(PW_i||R_i')$, $B_i' = h(ID_i||A_i')$, and checks whether B_i' equals to B_i. If they are not equal, the password change request is rejected. Otherwise, the user can input a new password PW_i^*, and then SC_i computes:

$A_i^* = h(PW_i^*||R_i')$;

$B_i^* = h(ID_i||A_i^*)$;

$E_i^* = E_i \oplus h(A_i'||ID_i) \oplus h(A_i^*||ID_i)$;

$F_i^* = F_i \oplus A_i' \oplus A_i^*$.

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

5. Security Analysis of the Proposed Scheme

In this section, we discuss the security of the proposed scheme, and compare our scheme with other related schemes in security and performance aspects.

5.1. Resist Impersonation Attack

In this attack, an adversary contains a malicious user or malicious server would like to masquerade as a legitimate user to login to servers.

We suppose U_x is a registered but malicious user, and he/she wants to impersonate as user U_i. In order to impersonate as U_i, U_x needs know $h(PSK)$, D_i and $h(C_i)$ to generate a valid login request message $\{M_1', M_2', M_3'\}$. Although U_x can obtain $h(PSK)$ from his/her own smart card, D_i and $h(C_i)$ are also unknown to U_x. Even if U_i's previous login request message $\{M_1, M_2, M_3\}$ was eavesdropped by U_x, and he/she may get D_i form D_i, but, he/she has no way to acquire $h(C_i)$. Therefore, the registered but malicious user cannot impersonate as another user.

Next, we consider the user impersonation attack launched by a valid but malicious server SID_j. From the description of the login phase, we can see SID_j has to get SID_k's secret information $h(SID_k||h(PSK))$ if he/she wants to impersonate as U_i to login to another server SID_k. However, $h(SID_k||h(PSK))$ is unknown to U_i, and the valid but malicious server has no way to impersonate as a user to login to another server.

From the above analysis, we can see that the proposed scheme is security against user impersonation attack.

5.2. Resist Server Spoofing Attack

In sever spoofing attack, a malicious user or malicious server would like to impersonate as a legitimate as a valid server.

When a malicious user U_i wants to masquerade as a server SID_k, he/she has to know SID_k's secret information $h(SID_k||h(PSK))$ and $h(PSK||x)$ to verify and response the user's login request message. Even though U_i can extract $h(PSK)$ from his/her own smart card, and then gets $h(SID_k||h(PSK))$, he/she remain has no way to obtain the required information $h(PSK||x)$ from the smart card information. Therefore, a registered but malicious user has no way to impersonate as a valid server to spoof users.

Besides, in order to impersonate as server SID_j to spoof users, the server SID_k has to use SID_k's secret information $h(SID_k||h(PSK))$ to generate the response message, however, $h(SID_k||h(PSK))$ is unknown to any other servers except the server SID_k. Therefore, the proposed scheme is free from server spoofing attack launched by a malicious user.

5.3. User Anonymity

In the proposed scheme, when user U_i logins to the server SID_j, he/she submits the login request message $\{M_1, M_2, M_3\}$ to SID_j, where $M_1 = h(SID_j||h(PSK)) \oplus N_i$, $M_2 = D_i \oplus N_i = h(PSK||x) \oplus h(ID_i||x) \oplus N_i$, $M_3 = h(h(C_i)||N_i) = h(h(h(ID_i||x))||N_i)$, N_i is a nonce generated by U_i, and $h(C_i)$ is extracted from smart card information by using identity, password and biometric. From which, we can see M_1 has no relation with user's identity. Besides, since ID_i is protected by the hash function in M_2, M_3, and the adversary has to know N_i and x to guess the user's password. However, only SID_j can use $h(SID_j||h(PSK))$ to recover N_i, and x is hold only by the registration center RC. Therefore, the user's identity cannot be revealed by the adversary from the login request message. Besides, we can see that each part of the user's login request message is dynamically change with the nonce N_i in each session, and one of the login request message is different with those of other session. Therefore, the adversary has no way to trace a special user. From above analysis, we can see our scheme provides the property of user anonymity.

5.4. Resist Replay Attack

Replay attack is a common used attack in network security, which an adversary wants to impersonate as a user by replaying the user's previous submitted messages. Generally, there are two common used techniques to avoid this attack, *i.e*. timestamp based method and random number based method. Our scheme adopted the random number mechanism to resist replay attack. In each session of the proposed scheme, the user U_i and the server SID_j generates new random numbers N_i and N_j, respectively, and these random numbers are used to the computation of the login request message and response message. Therefore, the messages in one session are different with the messages in other session, and the proposed scheme can resist replay attack.

5.5. Resist Stolen Smart Card Attack

In the proposed scheme, if user U_i's smart card is stolen by an adversary, the adversary can extract the smart card information $\{B_i, D_i, E_i, F_i, P_i, h(\cdot)\}$, where $B_i = h(ID_i||A_i)$, $D_i = h(PSK||x) \oplus C_i$, $E_i = h(A_i||ID_i) \oplus h(C_i)$, $F_i = h(PSK) \oplus A_i$, $A_i = h(PW_i||R_i)$, $C_i = h(ID_i||x)$. If the adversary is a registered user U_x, he/she would extract $h(PSK)$ from his/her own smart card, then, he/she can compute A_i by using F_i. However, the adversary cannot guess the identity ID_i and password PW_i since they are protected by the one-way property of hash function. Therefore, if the lost smart card is obtained by a registered but malicious user, he/she cannot use the stolen smart card to do any forgery attack due to he/she cannot get enough useful information to change the password or to generate a valid login request message.

On the other side, if user U_i's smart card is stolen by a server SID_j, he/she can extract C_i from the smart card information by using D_i and $h(PSK||x)$. However, SID_j cannot

guess the user's identity ID_i without known the master secret key x. Also, SID_j cannot extract any useful information from the stolen smart card.

From the above analysis, the proposed scheme can resist stolen smart card attack.

5.6. Forward Secrecy and Known-key Security

Forward secrecy and known-key security are two important security properties should satisfied for user authentication scheme with session key, where forward secrecy is that the session key would not be compromised even if the master secret key or user's long term key is revealed, and known-key security means that the compromise of one session key would not lead to the compromise of other session keys.

In the proposed scheme, user U_i and server SID_j will share a session key $SK_{ij} = h(h(C_i)||SID_j||N_i||N_j) = SK_{ji}$ after they are authenticated each other, where $C_i = h(ID_i||x)$, N_i and N_j are two random numbers generated by U_i and SID_j, respectively. If master secret key x and user's password PW_i are both compromised for some reasons, and the messages $\{M_1, M_2, M_3\}$ and $\{M_4, M_5\}$ exchanged in previous session is obtained by an adversary, the adversary cannot compute the session key $SK_{ij} = h(h(C_i)||SID_j||N_i||N_j)$ due to he/she has no way to get ID_i, N_i and N_j. Therefore, the proposed scheme has the property of forward secrecy. Besides, the session key is related to two random numbers N_i and N_j which are generated by U_i and SID_j, respectively, for each session. Therefore, the compromise of one session key has no influence in the security of other session keys, and the proposed scheme can ensure known-key security.

5.7. Avoid of Device of Service Attack

In biometric based authentication system, it is not suggested to directly use hash function to verify the validity of the biometric due to the noise property of the biometric. In the proposed scheme, in order to access the registered server SID_j, U_i inserts the smart card into the card reader and enters the identity ID_i, password PW_i. Then U_i imprints the biometric information BIO_i' at the sensor with fuzzy extractor and gets $R_i' = Rep(BIO_i', P_i)$. SC_i computes $A_i' = h(PW_i||R_i')$, $B_i' = h(ID_i||A_i')$, and checks whether B_i' equals to B_i. If they are equal, the user's identity, password and biometric are all passed the verification. In our scheme, we do not directly use hash function to verify the biometric information BIO_i, but we adopt the so called fuzzy extractor to process the biometric information. Although the user inputted biometric BIO_i' would not exactly the same as biometric template BIO_i, the fuzzy extractor will extract the same R_i with the help of auxiliary information P_i only if BIO_i' and BIO_i are reasonably close. Therefore, the proposed scheme is free from device of service attack.

5.8. Functionality and Performance Comparisons

In this section, we compare the proposed scheme with two previous related schemes in aspects of functionality and performance.

We list the results of functionality comparisons of our scheme and other related schemes [14, 15] in the table 2, and from which we can see that our scheme has more security properties. Both Mishra *et al*.'s scheme [14] and Baruah *et al*.'s scheme [15] cannot resist stolen smart card attack and denial of service attack, and they are both cannot protect user's anonymity due to an adversary can trace a special user using the static information in the login request message. Besides, Baruah *et al*.'s scheme [15] is vulnerable to impersonation attack and server spoofing attack. In the proposed scheme, we use the fuzzy extractor to resolve the denial of service problem. Besides, due to each part of the login request message of our scheme is different from those of other sessions, our scheme provides the untraceability property of the user. Therefore, the proposed scheme is more secure than other related schemes.

Table 2. Functionality Comparisons

	Mishra *et al*. [14]	Baruah *et al*. [15]	Our scheme
User anonymity	No	No	Yes
Resist insider attack	Yes	Yes	Yes
Resist server spoofing attack	No	Yes	Yes
Resist stolen smart card attack	No	No	Yes
Mutual authentication	Yes	Yes	Yes
Without clock synchronization	Yes	Yes	Yes
Resist impersonation attack	No	Yes	Yes
Resist password guess attack	Yes	Yes	Yes
Security of session key	Yes	Yes	Yes
Resist denial of service attack	No	No	Yes

Next, we compare the time complexity of the proposed scheme with other related schemes, due to the login phase and authentication phase are two frequently performed phases, we just consider these two phases. We list the performance comparisons in table 3, where T_h donates the time costs for executing a one-way hash function. From which, we can see that all the three schemes are efficient in computation costs due to they are all just using hash function operations. However, the proposed scheme is the most efficient due to it needs least hash function operations.

Table 3. Performance Comparisons

	Mishra et al. [14]	Baruah et al. [15]	Our scheme
Login phase	$6T_h$	$6T_h$	$5T_h$
Authentication phase	$12T_h$	$7T_h$	$6T_h$
Total	$18T_h$	$13T_h$	$11T_h$

6. Conclusions

In this article, the security weaknesses of Baruah et al.'s three factors user authentication scheme [15] for multi-server environments were pointed out. Their scheme was found vulnerable to stolen smart card attack and denial of service attack, and cannot provide the property of user's anonymity. In order to remedy the weaknesses of Baruah et al.'s scheme [15], an enhanced biometric-based three factors user authentication scheme for multi-server environments is proposed, where the proposed scheme adopts fuzzy extractor technique to process the biometric verification. Besides, the proposed scheme uses the random number mechanism to ensure the dynamic feature of the login request message, and then the user's anonymity property is ensured. The analysis shows that the proposed scheme is more security and efficient than other related schemes.

Acknowledgements

This work was supported by the Education and Scientific Research Project for Young and Middle-aged Teachers in Fujian Province under Grant no. 2014JA14368, the project of Education Department of Fujian Province under Grant no. JA15280, Li Shangda Discipline Construction Fund of Jimei University, the National Training Program of Innovation and Entrepreneurship for the Undergraduates of Local University with the no. 201410534003, and the Scientific Research Fund of Hunan Provincial Education Department under Grant no. 15C0545.

References

[1] L. Lamport. "Password authentication with insecure communication", Communications of the ACM, vol. 24, no. 11, **(1981)**, pp. 770-772.
[2] J. K. Lee, S. R. Ryu, K. Y. Yoo. "Fingerprint-based remote user authentication scheme using smart cards", Electronics Letters, vol. 38, no. 12, **(2002)**, pp. 554-555.
[3] C. H. Lin, Y. Y. Lai. "A flexible biometrics remote user authentication scheme", Computer Standards & Interfaces, vol. 27, no. 1, **(2004)**, pp. 19-23.
[4] C. C. Chang, I. C. Lin. "Remarks on fingerprint-based remote user authentication scheme using smart cards", ACMSIGOPS Operating Systems Review, vol. 38, no. 4, **(2004)**, pp. 91-96.
[5] H. S. Kim, S. W. Lee, K. Y. Yoo. "ID-based password authentication scheme using smart cards and fingerprints", ACM SIGOPS Operating Systems Review, vol. 37, no. 4, **(2003)**, pp. 32-41.
[6] M. Scott. "Cryptanalysis of an ID-based password authentication scheme using smart cards and fingerprints", ACM SIGOPS Operating Systems Review, vol. 38, no. 2, **(2004)**, pp. 73-75.
[7] M. K. Khan, J. S. Zhang. "Improving the security of 'a flexible biometrics remote user authentication scheme'", Computer Standards & Interfaces, vol. 29, no. 1, **(2007)**, pp. 82-85.
[8] C. T. Li, M. S. Hwang. "An efficient biometrics-based remote user authentication scheme using smart cards", Journal of Network and Computer Applications, vol. 33, no. 1, **(2010)**, pp. 1-5.
[9] X. Li, J. W. Niu, J. Ma, W. D. Wang, C. L. Liu. "Cryptanalysis and improvement of a biometrics-based remote user authentication scheme using smart cards", Journal of Network and Computer Applications, vol. 34, no. 1, **(2011)**, pp. 73-79.
[10] A. K. Das. "Analysis and improvement on an efficient biometric-based remote user authentication scheme using smart cards", IET Information Security, vol. 5, no. 3, **(2011)**, pp. 145-151.
[11] Y. H. An. "Security analysis and enhancements of an effective biometric-based remote user authentication scheme using smart cards", Journal of Biomedicine and Biotechnology, vol. **2012**, Article ID 519723, 6 pages, doi:10.1155/2012/519723.
[12] X. Li, J. W. Niu, M. K.Khan, J. G. Liao, X. K. Zhao. "Robust three-factor remote user authentication scheme with key agreement for multimedia systems", Security and Communication Networks, (**2014)**, online, doi: 10.1002/sec.961.
[13] M. C. Chuang and M. C. Chen, "An anonymous multi-server authenticated key agreement scheme based on trust computing using smart cards and biometrics", Experts Systems with Applications, vol. 41, no. 4, **(2014)**, pp. 1411-1418.
[14] D. Mishra, A.K. Das and S. Mukhopadhyay, "A secure user anonymity-preserving biometric-based multi-server authenticated key agreement scheme using smart cards", Expert Systems with Applications, vol. 41, no. 18, **(2014)**, pp. 8129-8143.
[15] K. C. Baruah, S. Banerjee, M. P. Dutta, C. T. Bhunia. "An improved biometric-based multi-server authentication scheme using smart card, International Journal of Security and Its Applications, vol. 9, no. 1, **(2015)**, pp. 397-408.
[16] Y. Dodis, L. Reyzin, A. Smith. "Fuzzy extractors: how to generate strong keys from biometrics and other noisy data", Advances in Cryptology, Eurocrypt 2004. LNCS. Springer Berlin Heidelberg: Interlaken, Switzerland, Vol. 3027, **(2004)**, pp. 523-540.
[17] C. Kaufman, P. Hoffman, Y. Nir, P. Eronen, T. Kivinen. Internet key exchange protocol version 2 (IKEv2), No. RFC 7296, **(2014)**.
[18] P. Kocher, J. Jaffe, B. Jun. "Differential power analysis", Advances in Cryptology-CRYPTO'99. Springer: Berlin Heidelberg, **(1999)**, pp. 388-97.
[19] T. S. Messerges, E. A. Dabbish, R. H. Sloan. "Examining smart-card security under the threat of power analysis attacks", IEEE Transactions on Computers, vol. 51, no. 5, **(2002)**, pp. 541-552.

Authors

Youping Lin received his master's degree in control engineering at Xiamen University in 2009. Now he is a lecture of Chengyi University College, Jimei University, and his research interests include information security and computer applications.

Kaihui Wang is a fourth year undergraduate at Hunan University of Science and Technology, and she majors in Information security.

Baocan Zhang received his master's degree in applied mathematics at Shantou University in 2009. Now he is a lecture of Chengyi University College, Jimei University, and his research interests include applied mathematics and cryptography.

Yuzhen Liu received his master's degree in computer science of Xiangtan University in 2004 and Ph.D. degree in computational mathematics from Xiangtan University in 2012. Dr. Liu now is a lecturer of Hunan University of Science and Technology. He has published about 10 papers His research interests include cryptography and information security, and intelligent computing.

Xiong Li received his master's degree in mathematics and cryptography from Shaanxi Normal University in 2009 and Ph.D. degree in computer science and technology from Beijing University of Posts and Telecommunications in 2012. Dr. Li now is a lecturer of Hunan University of Science and Technology. He has published more than 30 referred journal papers. His research interests include cryptography and information security.