Efficient Biometrics Remote User Authentication Scheme

Ming-Jheng Li
Department of Computer Science and
Information Engineering
National Chi Nan University
Puli, Nantou 54561 Taiwan

Justie Su-Tzu Juan
Department of Computer Science and
Information Engineering
National Chi Nan University
Puli, Nantou 54561 Taiwan

Abstract Recently, bio-information has been playing an important role in modern user authentication schemes. In 2004, Lin and Lai proposed a flexible biometrics remote user authentication scheme. However, their scheme is vulnerable and cannot provide mutual authentication between user and remote system. Hence, Khan and Zhang improved the security of a flexible biometrics remote user authentication scheme in 2007. This paper shows that Khan et al.'s scheme is still vulnerable to both the impersonation attack and the man-in-the-middle attack. Moreover, an efficient and flexible biometries user authentication scheme is proposed to enhance the performance and correct the security problems.

Keywords: cryptanalysis, user authentication, fingerprint verification, smart card, biometrics.

I. INTRODUCTION

Remote user authentication has become an important technique in modern computer network systems in which it is used to validate the legitimacy of a remote login user. In 1981, Lamport [6] first proposed a remote password-based authentication scheme that could authenticate remote users over an insecure channel. In Lamport’s scheme, a remote host system was able to authenticate the remote login users based on identity and password. However, their scheme requires a password table for authenticating the legitimacy of the user. In 1984, Shamir [11] first proposed ID-based cryptosystems. In [11], the public key directory table is not needed, and the assistance of a trusted third party is not required.

More recently, bio-information has been playing an important role in modern user authentication schemes, such as fingerprint, iris, voice, face etc. In 2002, Lee, Ryu and Yoo [7] first proposed a fingerprint-based remote user authentication scheme by using a smart card. Their fingerprint verification method is based on minutiae extraction and matching [1]. However, their scheme is still not safe to against impersonation attack [9]. In 2003, Kim, Lee and Yoo [4] proposed two ID-based password authentication scheme by using smart cards and fingerprints based on [7]. Li and Juan [8] pointed out that Kim et al.’s scheme is still insecure. In 2004, Lin and Lai [9] proposed a flexible biometrics remote user authentication scheme. Their scheme is proposed to enhance the security of [7]. Moreover, in their scheme users can conveniently choose and change their passwords. In 2007, Khan and Zhang [3] pointed out that [9] is vulnerable to attack, and there is no mutual authentication between user and remote system. For this reason, Khan et al. improved the security of [9], and provided security patch establishes trust between client and remote system by using mutual authentication. Unfortunately, [3] is still insecure. In this paper, we point out that [3] is vulnerable to both the impersonation attack and man-in-the-middle attack. Moreover, we propose a new flexible biometrics remote user authentication scheme to improve the security of [3] and [9]. In addition, the proposed scheme is more efficient than both of theirs by using low computation cost.

This paper is organized as follows. In Section II, we briefly review Khan et al.’s scheme (called Khan-Zhang scheme in this paper). In Section III, we present a cryptanalysis of Khan-Zhang scheme by showing that their scheme is still vulnerable to both the impersonation attack and man-in-the-middle attack. In Section IV, the new efficient and flexible biometrics remote user authentication scheme is proposed. In Section V, the security analysis and the time complexity performance of the proposed scheme are given. Finally, the conclusions of this work are drawn in Section VI.

II. BRIEFLY REVIEW OF KHAN-ZHANG SCHEME

Khan-Zhang’s scheme [3] is composed of five phases: registration, login, authentication, change password, and mutual authentication. Now, we briefly review their scheme as follows.

A. Registration phase

In this phase, a new user \( U_i \) chooses his \( ID_i \) and password \( PW_i \) to the system in order to register. In addition, \( U_i \) personally imprints his fingerprint on the input device to produce his fingerprint template \( S_i \) and offer his \( ID_i \) and \( PW_i \) in the registration center. The system of the registration center performs the following steps:

1) Compute \( PW'_i = h(PW_i \oplus S_i) \), where \( h(.) : \{0, 1\}^* \rightarrow \mathbb{Z}_p \) denotes a one-way hash function, \( S_i \) denotes the fingerprint template of \( U_i \), and \( \oplus \) denotes a symbol of exclusive or.

2) Compute \( Y_i = (ID_i^{X_s} \mod p) \oplus PW'_i \), where \( p \) is a large prime number and \( X_s \) denotes the secret key of the system.

Finally, the registration center issues a smart card to the user \( U_i \). In the smart card, \( h(.) \), \( p \), \( Y_i \), \( S_i \) and \( ID_i \) are stored.
B. Login phase

When $U_i$ wants to login, $U_i$ has to insert his own smart card into the card reader and imprint the fingerprint, then type his password $PW_i$. If $U_i$ passes the fingerprint verification ($S_i$ is correct), the smart card will perform the following steps:

1) Generate a random number $r$ by using the coordinate of minutenia of input fingerprint. Whenever a fingerprint is input, a different map of minutenia is made. Therefore, the input map could be used as an one-time random number.

2) Compute $PW''_i = h(PW_i \oplus S_i)$, where $S_i$ is the user's fingerprint template stored on the smart card.

3) Compute $Y'_i = Y_i \oplus PW''_i$.

4) Compute $C_1 = (ID_i)^r \mod p$.

5) Compute $M = h(Y'_i \oplus T_0)$, where $T_0$ is the current timestamp of the login device.

6) Compute $C_2 = (Y'_i)^r \cdot M \mod p$.

7) $U_i$ sends a login message $C = (ID_i, C_1, C_2, T_0)$ to the remote system.

C. Authentication phase

When the remote system receives the login request $C = (ID_i, C_1, C_2, T_0)$ at time $T_1$, where $T_1$ is the current timestamp of the system. The remote system then performs the following steps to authenticate the valid remote login user.

1) The system checks the $ID_i$. If it does not hold, the login request is rejected.

2) Check the validity of the timestamp $T_1$. If $(T_1 - T_0) \geq T$, then the system rejects the login request. Where $T$ denotes the expected valid time interval for transmission delay.

3) The system verifies whether $C_2(C_1^{-1}X_i)^{-1} \equiv h((ID_i)^{X_i} \mod p) \oplus T_0)$ (mod $p$) or not. If it holds, the system accepts the login request. Otherwise, the system rejects the login request.

D. Change password

Whenever $U_i$ wants to change the old password $PW_i$ to the new password $PW''_i$, $U_i$ has to imprint his fingerprint then smart card compares it with the template stored on the smart card. If $U_i$ passes the fingerprint verification, $U_i$ inputs old password $PW_i$ and the new password $PW''_i$. The client device performs the following steps:

1) Compute $PW''_i = h(PW_i \oplus S_i)$, where $S_i$ is $U_i$'s minutiae template stored on the smart card.

2) Compute $Y'_i = Y_i \oplus PW''_i = ID_i^{X_i}$ (mod $p$).

3) Compute new $Y''_i = Y'_i \oplus h(PW''_i \oplus S_i)$.

4) Replace the old $Y_i$ with the new $Y''_i$ on the smart card.

E. Mutual authentication phase

When $U_i$ passed the authentication phase, the remote system has to send a message to $U_i$ for mutual authentication. The remote system performs the following steps:

1) If $U_i$ has passed the authentication phase, the remote system obtains its current timestamp $T_2$ and computes $C_3 = h(ID_i^{X_i} \mod p \oplus T_2)$. Then remote system sends mutual authentication message $(C_3, T_2)$ to the $U_i$.

2) When $U_i$ receives the $(C_3, T_2)$ at time $T_3$, $U_i$ checks whether $(T_3 - T_2) \geq T$ or not. If it does not hold, the message is rejected.

3) $U_i$ computes $ID_i^{X_i} \mod p = Y_i \oplus PW''_i$, where $Y_i$ is stored in the user’s smart card and $PW''_i = h(PW_i \oplus S_i)$ can be calculated by the password of the user $U_i$.

4) Finally, $U_i$ computes $C_3^* = h(ID_i^{X_i} \mod p \oplus T_2)$ and checks whether $C_3^* = C_3$ or not. If it holds true, the mutual authentication between $U_i$ and remote system is completed, otherwise $U_i$ terminates the connection.

III. CRYPTANALYSIS OF KHAN-ZHANG SCHEME

In this section, we show that Khan-Zhang scheme is insecure against two attack mechanisms. One is impersonation attack, and the other is man-in-the-middle attack.

A. Impersonation attack

In this subsection, we shall present an impersonation attack on Khan-Zhang scheme off-line. Off-line means that the user can pass login phase without inserting his smart card into the card reader. In addition, the impersonation attack means that several users try to forge another valid ID and PW without having the other user’s ID and password PW. Suppose an adversary $U_a$ wants to impersonate another valid user $U_i$ on off-line without knowing the PW of $U_i$. Next, we describe the way of this attack as follows.

1) An adversary $U_a$ obtains the $ID_i$ of $U_i$ by eavesdropping on the login request message.

2) $U_a$ picks two integers $k$ and $k'$, where $k \cdot k' = 1$ (mod $p - 1$), then $U_a$ computes his identity $ID_a = ID_i^k$ (mod $p$). Note that, $ID_i = ID_a^k$ (mod $p$).

3) $U_a$ registers his $ID_a$ to the remote system ($PW_a$ without concern). Therefore, $U_a$ will receive his smart card, and he can obtain $Y_a$ from his smart card. And then, $U_a$ can easily compute $ID_i^{X_{a}} = (ID_a^{X_{a}})^k = (Y_a \oplus PW''_a)^k$ (mod $p$).

4) $U_a$ determines $C'_1 = ID_i = ID_a^k$ and computes $C'_2 = h((ID_a^{X_{a}})^k \cdot p) \oplus T'_0 = (ID_a^{X_{a}})^k \cdot p$ (mod $p$).

5) $U_a$ sends the forged login request $C'_1 = (ID_i, C'_1, C'_2, T'_0)$ to the remote system, where $U_a$ can successfully pass the verification equation as follows:

$C'_2 = h(C'_1)^{-1} \equiv h((ID_a^{X_{a}})^k \cdot p) \oplus T'_0 \cdot (ID_a^{X_{a}})^k \cdot ID_a \cdot T'_0$ (mod $p$).

As a result, $U_a$ can easily impersonate any valid user $U_i$ without their password $PW_i$. Because our impersonation attack is off-line, $U_a$ can therefore successfully pass the verification equation without inserting any valid smart card into the card reader and imprinting the fingerprint in the login phase. Hence, this scheme cannot withstand the impersonation attack.

B. Man-in-the-middle attack

When $U_a$ intercepts the login request $C = (ID_i, C_1, C_2, T_0)$ delivering from a valid user $U_i$. First, $U_a$
can easily compute $ID_{i}^{X_{i}} \equiv (ID_{a}^{X_{i}})^{k} \equiv (Y_{a} \oplus PW_{i}^{T})^{k}$ (mod $p$) by our impersonation attack scenario, and then computes $h(ID_{i}^{X_{i}} \mod p \oplus T_{0})$. After that, $U_{a}$ impersonations the valid remote system, and sends $h(ID_{i}^{X_{i}} \mod p \oplus T_{0})$ to $U_{i}$ immediately in mutual authentication phase. Then, $U_{i}$ will undetectable pass the verify equation $C_{3}^{*} = h(ID_{i}^{X_{i}} \mod p \oplus T_{0})$ and trust the $U_{a}$ as the valid remote system. Hence, the mutual authentication is vulnerable to man-in-the-middle attack. In other words, Khan-Zhang scheme is useless for mutual authentication between user and remote system.

IV. THE PROPOSED SCHEME

Some modifications are provided to improve the security of Khan-Zhang scheme. The security of the proposed scheme is based on the one-way hash function, fingerprint verification and smart cards. The notations of the proposed scheme are similar to Khan-Zhang scheme. Now, we describe the five phases of the scheme separately as follows.

A. Registration phase

The registration phase of the proposed scheme is based on Khan-Zhang scheme. The system of the registration center performs the following steps:

1) Compute $PW_{i}^{T} = h(PW_{i} \oplus S_{i})$.
2) Use a secret number $x$, and compute $Y_{i} = h(ID_{i} \oplus x) \oplus PW_{i}^{T}$.

Finally, the registration center issues a smart card to the user $U_{i}$. In the smart card, $h(.)$, $p$, $Y_{i}$, $S_{i}$ and $ID_{i}$ are stored.

B. Login phase

In this phase, if $U_{i}$ passes the fingerprint verification, the smart card will perform the following steps:

1) Compute $PW_{i}^{T} = h(PW_{i} \oplus S_{i})$.
2) Compute $Y_{i} = Y_{i} \oplus PW_{i}^{T}$.
3) Compute $M = h(Y_{i} \oplus T_{0})$.
4) $U_{i}$ send $C = (ID_{i}, M, T_{0})$ to the remote system.

C. Authentication phase

When the remote system receives the login request $C = (ID_{i}, M, T_{0})$ at time $T_{1}$. The remote system then performs the following steps to authenticate the valid remote login user.

1) The system checks the $ID_{i}$. If it does not hold, the login request is rejected.
2) Check the validity of the timestamp $T_{1}$. If $(T_{1} - T_{0}) \geq \hat{T}$, the system rejects the login request.
3) System calculates $Y_{i} = h(ID_{i} \oplus x)$ and verifies whether $M = h(Y_{i} \oplus T_{0})$ or not. If it holds, the system accepts the login request. Otherwise, the system rejects the login request.

D. Change password

Assume $U_{i}$ wants to change the old password $PW_{i}$ to the new $PW_{i}^{T}$. The client device performs the following steps:

1) Compute $PW_{i}^{T} = h(PW_{i} \oplus S_{i})$, where $S_{i}$ is $U_{i}$’s minutiae template stored on the smart card.
2) Compute $Y_{i} = Y_{i} \oplus PW_{i}^{T} = h(ID_{i} \oplus x)$.

3) Compute new $Y_{i}^{*} = Y_{i} \oplus h(PW_{i}^{T} \oplus S_{i})$.
4) Replace the $Y_{i}$ with the $Y_{i}^{*}$ on the smart card.

E. Mutual authentication phase

1) If $U_{i}$ has passed the authentication phase, the remote system obtains its current timestamp $T_{2}$ and computes $C_{3} = h(Y_{i}^{*} \oplus T_{2})$, then sends mutual authentication message $(C_{3}, T_{2})$ to $U_{i}$

2) When $U_{i}$ receives the $(C_{3}, T_{2})$ at time $T_{3}, U_{i}$ checks whether $(T_{3} - T_{2}) \geq \hat{T}$ or not. If it does not hold, the message is rejected.

3) $U_{i}$ computes $C_{3}^{*} = h(Y_{i}^{*} \oplus T_{2})$ and checks whether $C_{3}^{*} = C_{3}$ or not. If it is true, the mutual authentication between $U_{i}$ and remote system is completed, otherwise $U_{i}$ terminates the connection.

V. Analysis

At first, the security analysis of the proposed scheme are shown in Subsection A. After that, the performance of the proposed scheme are shown in Subsection B.

A. Security Analysis

The scheme can be proved to be correct and secure due to one-way hash function. Here, we first give the following definitions.

Definition 1. (Primag resistant) [10] Consider the equation $H = h(m)$, where $h(.)$ is an one-way hash function and $m$ is an input value. Given $h(.)$ and $m$, it is a straightforward matter to calculate $H$. However, given $h(.)$ and $H$, it is very difficult to calculate $m$.

Definition 2. (Second primage resistant) [10] Given an input value $m_{1}$, it should be hard to find another input value $m_{2}$ (not equal to $m_{1}$), such that $h(m_{1}) = h(m_{2})$.

Definition 3. (Collision-resistant) [10] It should be hard to find two different messages $m_{1}$ and $m_{2}$, such that $h(m_{1}) = h(m_{2})$.

At the same time, considering the one-way property of hash function, the proposed scheme can withstand several attacks as follows.

Theorem 1. The proposed scheme can withstand to impersonation attack.

Proof. Suppose $U_{a}$ wants to impersonate a valid user $U_{i}$ in the proposed scheme. He chooses two random numbers $k$ and $k'$ for computing his identity $ID_{a} = ID_{i}^{k}$ mod $p$, where $k \cdot k' \equiv 1$ (mod $p - 1$), and registers as our impersonation attack scenario. However, the proposed scheme is not based on ElGamal’s cryptosystem [2]. Thus, this impersonation attack scenario cannot work in the proposed scheme. Furthermore, even if adversary may try to use a random value $k'$ to compute the $ID_{a} = ID_{i}^{k'}$. However, it is very difficult...
to calculate the equation \( h(ID_a \oplus x) = h(ID_t \oplus x) \), if \( ID_a \neq ID_t \). According to Definition 3, the adversary must face the difficulty of reversing the one-way hash function, and has to know the secret value \( x \) of remote system by Definition 1. As a result, the proposed scheme can withstand to impersonation attack.

**Theorem 2.** The proposed scheme can withstand to man-in-the-middle attack.

**Proof.** Suppose an malicious user wants to make a valid response request message \( (C_3, T_2) \) to \( U_i \) from eavesdropping on the login request message \( C = (ID_t, M, T_0) \), where \( M = h(Y'_i \oplus T_0), Y'_i = h(ID_t \oplus x) \) in our mutual authentication phase. He can not succeed because \( h(ID_t \oplus x) \) cannot be obtained due to that \( h \) is a one-way function (see Definition 1). In addition, anyone should be hard to find a \( ID_a \), and let \( h(ID_a \oplus x) = h(ID_t \oplus x) \), if \( ID_a \neq ID_t \) (see Definition 2). Moreover, the secure value \( x \) cannot be obtained from \( h(ID_t \oplus x) \), hence adversary cannot also forge a remote system to compute the response message \( (C_3, T_2) \). Thus, man-in-the-middle attack cannot work in the proposed scheme.

**B. Performance**

Time complexity is used for comparison and estimate the cost of execution operations. The given symbols are defined in Table I. In the proposed scheme, the time complexity of exclusive-or operation is very low, so it is omitted in the calculation of the cost of computation. From Koblitz et al.’s paper [5], the computation load of the exponential and inverse operation are much heavier than those of the one-way hash function, exclusive-or and multiplication operations. The relationship among these operations are given as follows:

\[
T_{exp} \approx 240 \cdot T_{mul},
\]

\[
T_{hash} \approx 1.2 \cdot T_{mul}.
\]

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>( T_{exp} )</td>
<td>Time complexity of modulus exponentiation</td>
</tr>
<tr>
<td>( T_{mul} )</td>
<td>Time complexity of modulus multiplication</td>
</tr>
<tr>
<td>( T_{hash} )</td>
<td>Time complexity of one-way hash function</td>
</tr>
<tr>
<td>( T_{inv} )</td>
<td>Time complexity of modulus inverse element</td>
</tr>
</tbody>
</table>

Table II shows the comparisons between our scheme and other related works (Lin et al.'s scheme [9] and Khan et al.'s scheme [3]) in one time complete login phase (including authentication and mutual authentication phases). Obviously, it is easy to see that the proposed scheme is more secure and efficient than the other two schemes from Table II. In the proposed scheme, the smart card and remote server need only to perform three one-way function operations, separately. Hence, our scheme is efficient to be applied in practice.

<table>
<thead>
<tr>
<th>Types</th>
<th>[9]</th>
<th>[3]</th>
<th>Our scheme</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requirements</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Mutual authentication</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Computation cost of smart card</td>
<td>2</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>( T_{exp} )</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>( T_{mul} )</td>
<td>2</td>
<td>4</td>
<td>3</td>
</tr>
<tr>
<td>( T_{inv} )</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Computation cost of remote system</td>
<td>2</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>( T_{exp} )</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>( T_{mul} )</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>( T_{inv} )</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

**VI. Conclusions**

In this paper, we have demonstrated that Khan-Zhang scheme is vulnerable to both impersonation attack and man-in-the-middle attack. In order to amend above flaws, an efficient and flexible biometrics remote user authentication scheme is proposed. In addition, detailed security analysis of the proposed scheme are discussed. In the proposed scheme, it also reduces the computation cost by using few one-way hash function operation. Thus, the new scheme is suitable for both the modern computer network and applications with high security requirements.

**REFERENCES**


