Cryptanalysis and Improvement on Robust Three-Factor Remote User Authentication Scheme with Key Agreement for Multimedia System

Younsung Choi and Dongho Won*
Affiliation College of Information and Communication Engineering, Sungkyunkwan University, Suwon-si, Gyeonggi-do, Republic of Korea

{yschoi, dhwon}@security.re.kr

ABSTRACT

A three-factor authentication combines biometrics information with user password and smart card to provide security-enhanced user authentication. An proposed user authentication scheme improved Das’s scheme. But An’s scheme is not secure against denial of service attack in login phase, forgery attack. Li et al. pointed out them and proposed three-factor remote user authentication scheme with key agreement. However, Li et al.’s scheme still has some security problem. In this paper, we present a cryptanalysis and improvement of Li et al.’s remote user authentication scheme.

KEYWORDS

Three-factor authentication, Key agreement scheme, Cryptanalysis, Smart card, Biometrics information

1 INTRODUCTION

Recently, internet technology is growing up. The system providing various multimedia service consists of many different servers around the world. Since various servers providing access for the user are usually greater than one, authentication schemes for multiple server environments are required for the high level of security. And the protection of digital data becomes a significant issue in network-based remote application systems [1, 2]. Lamport [3] firstly proposed a password-based authentication scheme for communication via insecure channels but the server has to store a password table. Lamport’s scheme has critical vulnerability on stolen-verifier attack. So, some researchers proposed the security enhanced password authentication schemes but those are easily broken by dictionary attacks. Thus, a lot of research have combined a user’s biometrics with a password and a smart card to design the remote user authentication scheme for multi-server [4, 5]. Hwang et al. proposed ElGamal-based remote user authentication scheme using smart card [6]. Kim et al. introduce an ID-based password authentication scheme using smart card and fingerprints, which is one of biometric information [7]. And Lin and Lai proposed a fingerprint-based user authentication scheme for multimedia systems [8]. Yang and Yang and Yoon and Yoo proposed biometric-based multi-server authentication schemes. Yang and Yang’s scheme needs to perform exponential operations that have high computational cost. And He and Diabao was demonstrated that Yoon and Yoo’s scheme is vulnerable to privileged insider attack, masquerade attack and stolen smart card attack. To solve these problems, Chuang and Chen proposed an anonymous multi-server authenticated key agreement scheme using smart card, password and biometrics [9-12]. Li et al. and Das indicated design flaws and security problem of Li and Hwang’s scheme [13, 14]. In 2012, An pointed out the security problems of Das’s scheme and proposed security enhanced user authentication scheme [15]. But Li et al. analyzed the security of An’s authentication scheme and figure out that An’s scheme is not secure against various attack and proposed robust three-factor remote user authentication scheme with key agreement for multimedia system[1]. But Li et al.’s scheme still has
various security problems. So we analyze the Li et al.’s scheme and point out the vulnerability of this scheme.

The remainder of this paper is organized as follows. Section 2 provides some related work for understanding this paper. And section 3 describes the Li et al.’s authentication scheme. In section 4, we performs cryptanalysis on Li et al.’s authentication scheme. And section 5 proposes the requirement for enhancing the security of authentication scheme. Section 6 concludes the paper.

2 RELATED WORKS

In this section, we introduce the related works to understand this paper.

2.1 Three-factor authentication

The three classes of human authentication factors are as follows, something you know (as secret password), something you have (as a secure device with a secret key, smartcard), and something you are (as a biometric). Two-factor authentication scheme requires the combination of two authentication factors (as password and smartcard). But it has various vulnerability like offline password attack and stolen smart card attack. To enhance security of authentication scheme, the three-factor authentication is introduced. In client-server system, it uses three-factor as user password, smartcard, and biometrics. Biometrics information are difficult to forge or distribute. And it cannot be lost or forgotten. Recently, various researchers study the efficiency and security of three-factor authentication schemes [16, 17].

2.2 Fuzzy extraction

Fuzzy extractor converts biometric information into random strings. So it makes it possible to apply cryptographic techniques for biometric security. It consist of a pair of efficient randomized procedures, Gen and Rep. They mean “generate” and “reproduce”. In Li et al’s scheme, Gen(B) = (R, P) and R = Rep(B’, P) are used. Fuzzy extractor Gen generates R and P using user’s biometric in registration phase. R is uniform and random string. P is helper string, so R can be same under the assistance of auxiliary information P even if inputted the biometric information is changed, so long as it maintain reasonably similar status with original biometric information. So fuzzy extraction is error-tolerant. Fuzzy extractor Rep reproduces the R using new inputted biometric information B’ and P in login phase. To reproduce the same R, the metric space distances between B and B’ have to meet the verification threshold [18, 19].

2.3 Elliptic curve cryptography

ECC is one of public-key cryptography and based on the algebraic structure of elliptic curves over finite fields. Also, elliptic curves are used in several integer factorization algorithms. The important benefit of ECC is a smaller key size, So ECC can maintains the same degree of security with the smaller key size than other public-key cryptography such as RSA, DH and DSA. Therefore, ECC is especially useful for wireless devices which are typically limited in terms of their CPU, power and network connectivity. Table 1 shows NIST guidelines on choosing the computationally equivalent symmetric and public key size [20].

<table>
<thead>
<tr>
<th>Symmetric</th>
<th>ECC</th>
<th>RSA/DH/DSA</th>
</tr>
</thead>
<tbody>
<tr>
<td>80</td>
<td>160</td>
<td>1024</td>
</tr>
<tr>
<td>112</td>
<td>224</td>
<td>2048</td>
</tr>
<tr>
<td>128</td>
<td>256</td>
<td>3072</td>
</tr>
<tr>
<td>192</td>
<td>384</td>
<td>7680</td>
</tr>
<tr>
<td>256</td>
<td>512</td>
<td>15360</td>
</tr>
</tbody>
</table>

In ECC, there are three mathematical problems. Elliptic Curve Discrete Logarithm Problem (ECDLP), Elliptic Curve Computational Diffie-Hellman Problem (ECCDH), Elliptic Curve Decisional Diffie-Hellman Problem (ECDDH).
There is no polynomial time algorithm to solve the ECDDHP, ECCDHP and ECDDLP with non-negligible probability. ECDDLP means that given a point element $Q$ in $G$, find an integer $x$, such that $Q = xP$, where $xP$ indicates that the point $P$ is added to itself for $x$ times by the elliptic curves operation. ECCDHP means that given two point elements $aP$, $bP$ in $G$, compute $abP$ in $G$. ECDDLP means given three point elements $aP$, $bP$ and $cP$ in $G$, decide whether $cP = abP$.

2.4 An’s authentication scheme

An’s authentication scheme improved Das’s scheme using security analysis. Das’s scheme is not secure against user impersonation attack, sever masquerading attack, password guessing attack, and insider attack. Also it does not provide mutual authentication between the user and the server. So An proposed the security enhanced effective biometric-based remote user authentication scheme. But Li et al point out the security problems of An’s authentication scheme. An’s scheme is not secure against denial of service attack in login phase, forgery attack. And in An’s scheme, wrong password cannot be quickly detected and it does not support session key agreement.

3. Review of Li et al.’s authentication scheme

To solve the security problems of An’s scheme, Li et al proposes robust three-factor remote user authentication scheme with key agreement using ECC. It uses the fuzzy extractor method for biometric authentication in order to solve the hash function problem of An’s scheme. Table 2 shows the notations used throughout this paper.

3.1 Registration phase

Before the legitimacy user ($C_i$) starts login and authentication phase, $C_i$ and $R$ should perform the registration phase as follows. Fig 1 describes the detailed steps of registration phase.

<table>
<thead>
<tr>
<th>Table 2 Notation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Symbol</td>
</tr>
<tr>
<td>$R$</td>
</tr>
<tr>
<td>$S_i$</td>
</tr>
<tr>
<td>$C_i$</td>
</tr>
<tr>
<td>$A_i$</td>
</tr>
<tr>
<td>$ID_i$</td>
</tr>
<tr>
<td>$PW_i$</td>
</tr>
<tr>
<td>$B_i$</td>
</tr>
<tr>
<td>$P$</td>
</tr>
<tr>
<td>$E_p(a, b)$</td>
</tr>
<tr>
<td>$h()$</td>
</tr>
<tr>
<td>$X_i$</td>
</tr>
<tr>
<td>$R_c$</td>
</tr>
<tr>
<td>$R_s$</td>
</tr>
<tr>
<td>$</td>
</tr>
<tr>
<td>$\oplus$</td>
</tr>
</tbody>
</table>

(1) $C_i$ chooses user’s $ID_i$, $PW_i$ and generates random number $K$. Then, $C_i$ inputs the user’s personal biometric information $B_i$ to the fuzzy extractor. $C_i$ sends the user’s $ID_i$, $B_i$, and $RPW_i = h(PW_i||K)$ to registration center $R$ through secure communication channel.

$$[C_i, PW_i]$$

chooses $ID_i, PW_i$

inputs $B_i$

generates a random number $K$

computes $RPW_i = h(PW_i||K)$

$$<ID_i, B_i, RPW_i>$$

computes $Gen(B_i) = (R_i, R_i)$

$e_i = h(ID_i||X_i) \oplus h(f_i||RPW_i)$

$r_i = h(ID_i||RPW_i)$

smart card $<e_i, f_i, r_i, P_i, h()>$

stores $K$ into the smart card

Fig. 1 Registration phase of Li et al.’s scheme
(2) R computes $Gen(B_i)$, $f_i$, $e_i$, and $r_i$ using user’s message and secret key $X$.

$$Gen(B_i) = (R_i, P_i)$$
$$f_i = h(ID||R_i)$$
$$e_i = h(ID||X_i) \oplus h(f_i||RPW_i)$$
$$r_i = h(ID||RPW_i)$$

(3) R stores $<e_i, f_i, r_i, P_i, h(\cdot)>$ on smart card and send it to $C_i$ through secure communication channel.

(4) $C_i$ inputs $K$ to the smart card

### 3.2 Login phase

Before $C_i$ performs the authentication phase with $S_i$, $C_i$ need to execute the following steps to generate a legitimacy login request message. Fig 2 shows the detail steps of login phase.

(1) $C_i$ inserts $C_i$’s smart card into reader and inputs $ID_i$ and $PW_i$. And then, $C_i$ imprints $B_i$ at specific device with fuzzy extractor and computes $R_i = \text{Rep}(B_i', P_i)$.

(2) Next, the smart card computes $f_i' = h(ID||R)$ and compare it with $f_i$ which is stored in $C_i$’s smart card. If they are same, $C_i$ passes the biometric verification. And then, smart card executes next steps. If not, login phase is terminated.

(3) The smart card calculates $RPW_i = h(PW_i||K)$, $r_i' = h(ID||RPW_i)$ and verifies whether $r_i'$ is same to $r$ which is stored in smart card. If they are same, $C_i$ passes the $ID_i$ and $PW_i$ checking steps. And then, smart card executes the next steps. If not, the session is stopped.

(4) The smart card calculates $M_i = e_i \oplus h(f_i||RPW_i)$ and generates a random number $a \in Z_n^*$. Also, the smart card computes $M_3 = aP$, $M_3 = h(M_1||M_2)$. Next, $C_i$ sends login request message $<ID_i, M_2, M_3>$ to $S_i$.

### 3.3 Authentication phase

$S_i$ receives the $C_i$’s request message and then, $S_i$ and $C_i$ start to perform the steps to authenticate each other and establish session key using key agreement step. Fig 3 describes the detail steps of authentication phase.

(1) $S_i$ checks and verifies the format of $ID_i$.

(2) If the $ID_i$ is correct, $S_i$ computes $M_4 = h(ID_i||X_i)$ and verifies whether $M_3 = h(M_4||M_2)$. If they are same, $S_i$ accepts the $C_i$’s login message and confirms the validity of $C_i$. If not, the session is terminated.

(3) $S_i$ generates a random number $b \in Z_n^*$ and calculates $M_5 = bP$, $M_6 = h(M_4||M_2||M_3)$. And then, $S_i$ submits the message $<M_5, M_6>$ to $C_i$ for mutual authentication.

![Fig. 2 Login phase of Li et al.’s scheme](image1)

![Fig. 3 Authentication phase of Li et al.’s scheme](image2)
4 Cryptanalysis of Li et al.’s scheme

This section presents the cryptanalysis about offline password attack, authentication without biometrics, denial-of-service and Insider attack.

4.1 Offline password attack

Various studies pointed out that the confidential information stored in all existing smart cards could be extracted by physically monitoring its power consumption. Therefore, if the user lost his smart card, all information in the smart card could be revealed by attacker [21-23]. In Li et al.’s scheme, attacker can figure out the user’s password using revealed information. Fig 4 describes the detailed steps of off-line password attack on Li et al.’s scheme.

```
Attacker
gets(steals) user’s smart card
obtains information from smart card using SPA and DPA
→ gets $e_i, f_i, r_i, P, h(\cdot)$ and $K$
Attacker knows $r_i, h(\cdot), ID_i$ and $K$
→ $r_i = h(ID_i \parallel h(PW_i \parallel K))$
attacker don’t know only user’s password
attacker executes off-line password attack
→ figures out user’s password $PW_i$
```

**Fig. 4 Offline password attack**

In Li et al.’s scheme, the smart card includes various information for the login and authentication between $C_i$ and $S_i$. Firstly, the attacker monitors the communication between $C_i$ and $S_i$. And then, attacker obtains the user $ID_i$ and steal the user’s smart card. The smart card for $C_i$ stores $e_i$, $f_i$, $r_i$, $P$, $h(\cdot)$, and $K$. The attacker can obtain them using attacks such as simple power analysis (SPA), differential power analysis (DPA). After the attacker combines these information (especially $r_i$, $h(\cdot)$, $ID_i$, $K$), the attacker can make the following formula.
\[ r_i = h(ID_i \| h(PW_i \| K)) \]

In this formula, attack don’t know only user’s password \( PW_i \). So attacker can executes off-line password attack using dictionary attack, brute-force attack, rainbow table etc. If \( PW_i \) is not long enough, the attacker can figure out \( PW_i \). It is possible for the attacker to abuse the \( PW_i \) in a variety of ways because the user generally set up the similar password.

### 4.2 Authentication without biometrics

In Li et al.’s authentication scheme, legitimacy user needs to know user’s \( ID_i \) and password and to have the user’s biometric information and smart card. Therefore, when all of three-factor (\( ID_i / PW_i, B_i, \) smart card) are confirmed, user can authenticated with server. But Li et al.’s scheme has vulnerability. If an attacker get or steal user’s smart card, the attacker can be authenticated to server without the user’s biometrics information. Fig 5 describes the detailed steps of authentication without the biometrics on Li et al.’s scheme.

An attacker can get user \( ID_i \) in the public communication between \( C_i \) and \( S_i \). And as we discussed in section 4.1, the attacker can figure out user password \( PW_i \) if the attacker get the user’s smart card. The attacker can perform the login and authentication phase using only \( ID_i \) and \( PW_i \) without \( B_i \). It is reason that \( B_i \) is not necessary.

\[ \text{Attacker} \]

obtains \( ID_i \) in communication between \( C_i \) and \( S_i \)
gets (steals) user’s smart card
obtains information from smart card using SPA and DPA
\[ \to \text{get} r_i, e_i, h(\cdot), ID_i, K, P, h(\cdot) \]
attacker can produce this formula
\[ \to r_i = h(ID_i \| h(PW_i \| K)) \]
attacker don’t know only user’s password
attacker executes off-line password attack
\[ \to \text{figures out user’s password } PW_i \]
\[ \to \text{attacker knows } ID_i \text{ and } PW_i \]
generates a random number \( a_A \in Z_n^* \)
computes \( R PW_i = h(PW_i \| K) \)
computes \( M_A1 = e_i \oplus h(f_i \| R PW_i) \), \( M_A2 = a_A P \)
computes \( M_A3 = h(M_A1 \| M_A2) \)
\[ \langle ID_i, M_A2, M_A3 \rangle \]

\[ \text{checks the format of } ID_i \]
\[ \text{computes } M_A = h(ID_i \| X_S) \]
\[ \text{checks whether } M_S = h(M_A \| M_A2) \]
\[ \text{generates a random number } b \in Z_n^* \]
\[ \text{computes } M_5 = bP, M_6 = h(M_A \| M_A2 \| M_5) \]
\[ \langle M_5, M_6 \rangle \]

\[ \text{checks whether } M_6 = h(M_A1 \| M_A2 \| M_5) \]
\[ SK = h(\alpha A M_6) = h(bM_A2) = h(\alpha A bP) \]

Fig. 5 Authentication without biometrics
necessary to make the message for login and authentication between $C_i$ and $S_i$. The attacker can compute $RPW_i$ using $PW_i$ and $K$. $K$, $e_i$, $f_i$ and $P$ are stored information in smartcard.

$$RPW_i = h(PW_i||K)$$

Using $RPW_i$, $e_i$ and $f_i$, the attacker can $M_{A1}$,

$$M_{A1} = e_i \oplus h(f_i||RPW_i)$$

And then, the attacker generates a random number $a_A$ and computes $M_{A2}$ using $a_A$ and $P$,

$$M_{A2} = a_A P$$

Using $M_{A1}$ and $M_{A2}$, the attacker computes $M_{A3} = h(M_{A1}||M_{A2})$ and send $ID_i$, $M_{A1}$ and $M_{A3}$ to $S_i$. $S_i$ checks and verify the message whether it is correct or not. $S_i$ cannot find out that the message is made by the attacker. So the attacker is authenticated by $S_i$. And then, computes $M_5$ and $M_6$. Next, $S_i$ send $M_5$ and $M_6$ to the attacker. The attacker make session key $SK$ using this message.

$$SK = h(a_A M_3)$$

Finally, the attacker is authenticated with $S_i$ and can communicate with $S_i$ using $SK$.

### 4.3 Denial-of-service

In Li et al.’s protocol, $S_i$ only checks user $ID_i$ and $M_3$. When $S_i$ verifies the message $M_3$, $S_i$ uses only $ID_i$, $X_i$ and $M_2$. So, $S_i$ cannot check whether $<ID_i, M_2, M_3>$ is previous message or not. Thus, after the attacker monitors sniffing attack and obtains $ID_i$, $M_2$, and $M_3$, the attacker can make a lots of same message and send them to $S_i$. It makes server $S_i$ denial-of-service. Fig 6 describes the detailed steps of denial-of-service on Li et al.’s scheme. When $S_i$ receives $A_1$, $A_2$, $A_3$… and $A_n$, $S_i$ perform various action per each message. $S_i$ performs generating the random number once and the scalar multiplication once.

executes sniffing attack in public communication
\[\rightarrow\text{obtains } ID_i, M_2, M_3 \text{ between } C_i \text{ and } S_i\]
\[A_1 = <ID_i, M_2, M_3>\]
\[A_2 = <ID_i, M_2, M_3>\]
\[A_3 = <ID_i, M_2, M_3>\]
\[... A_n = <ID_i, M_2, M_3>\]
\[\Rightarrow\text{checks the format of } ID_i\]
\[\Rightarrow\text{computes } M_4 = h(ID_i || X_s)\]
\[\Rightarrow\text{checks whether } M_3 = h(M_4 || M_2)\]
\[\Rightarrow\text{generates a random number } b \in Z_n^*\]
\[\Rightarrow\text{computes } M_5 = bP, M_6 = h(M_5 || M_2 || M_3)\]

Per 1 attacker’s login messages, $S_i$ executes
\[\rightarrow\text{generating random number [once]}\]
\[\rightarrow\text{scalar point multiplication [once]}\]
\[\rightarrow\text{hash function [3 times]}\]
\[\rightarrow\text{generating reply message [once]}\]
\[\langle M_5, M_6 \rangle\]

Fig. 6 Denial-of-service attack

And $S_i$ executes a one-way hash function 3 times and generates reply message once. The one-way hash function is less important for $S_i$, but generating a random number and executing the scalar multiplication requires to consume a lot of computational cost of the server.

### 4.4 Insider attack

In Li et al, an insider attacker of the server $S_i$ can know secret information $X_s$ and $ID_i$ using $S_i$’s database and obtain $ID_i$ in public communication between $C_i$ and $S_i$. Using these information, the attacker can authenticated with all of server, which associated with registration center $R$. Fig 7 describes the detailed steps of insider attack on Li et al.’s scheme An inside attack can make login message $< ID_{ci}, M_2, M_3 >$ using $ID_{ci}$, $X_s$, $P$, $h(\cdot)$, and random number a generated by attacker. $ID_{ci}$ means one of legitimacy user’s ID. The inside attacker can compute $M_1 = e_i \oplus h(f_i||RPW_i)$ using $ID_c$ and $X_s$ because $M_1 = h(ID_c || X_s)$. 


When $S_{S1}$ and $S_{S2}$ receive $<ID_{Ci}, M_2, M_3>$, they checks and verify the accuracy of message but they cannot figure out that the message is made by the inside attacker. So $S_{S1}$ and $S_{S2}$ compute $<M_{S^{S1}5}, M_{S^{S1}6}>$ and $<M_{S^{S2}5}, M_{S^{S2}6}>$ and send to the inside attacker. The attacker can calculate the session key, which is used for communication.

$M_1 = e_i \oplus h(f_i || RPW_i) = h(ID_i || X_i)$ And the attacker generates random number $a$ and computes $M_2$ and $M_3$. Next, the attacker send $<ID_{Ci}, M_2, M_3>$ to any server like $S_{S1}$ and $S_{S2}$, which the attacker wants to login and authenticate.

Fig. 7 Insider attack
with the servers. The session key between the attacker and $S_{S1}$ is as follows,

$$SK = h(aM^{S1}P) = h(bS_{S1}M_{P}) = h(abS_{1}P)$$

The session key between the attacker and $S_{S2}$ is as follows,

$$SK = h(aM^{S2}P) = h(bS_{S2}M_{P}) = h(abS_{2}P)$$

Thus, inside attacker can login and authenticate with any server including $S_{1}$ and $S_{2}$.

### 4.5 Absence of anonymity

To provide secure communication between $C_{i}$ and $S_{i}$, anonymity is a desirable security feature in addition to providing secure user identification and key agreement during a user’s login and authentication procedure.

### 5 Requirement for enhancing security

Li et al.’s proposes efficient remote user authentication scheme using ECC and hash function. But it has various vulnerability, so it is necessary to enhance the security of scheme. To resist off-line password attack, all formulas related with $PW_{i}$ needs to be protected by $B_{i}$. Otherwise, $PW_{i}$ and $B_{i}$ need to be used together as follows,

$$r_{i} = h(ID_{i}||h(PW_{i}||B_{i}||K))$$

To solve authentication without biometric problem, it is necessary to use $B_{i}$ for making the message of login and authentication between $C_{i}$ and $S_{i}$. Otherwise, it is needed that $M_{2}$, $M_{3}$ and $SK$ are made by not only user $ID_{i}$ and $PW_{i}$ but also $B_{i}$ like as follows. To resist denial-of-service, $S_{i}$ has to check the freshness of user’s messages. Thus, it is necessary to add current timestamp to the login and authentication message of the users. To solve insider attack, it is necessary to add the secret information the only legitimate user can know or compute. Otherwise, user $C_{i}$ has to know the secret information, which cannot be known or computed by server $S_{i}$.

### 6 Proposed scheme

In this section, to solve Li et al.’s security problem, we propose security enhanced robust three-factor remote user authentication scheme with key agreement for multimedia system.

#### 6.1 Registration phase

The registration procedure of proposed scheme is described in Fig. 8

![Fig. 8 Proposed Registration phase](image)

**Fig. 8 Proposed Registration phase**

#### 6.2 Login phase

The Login procedure of proposed scheme is described in Fig. 9

![Fig. 9 Proposed Login Phase](image)

**Fig. 9 Proposed Login Phase**
6.3 Authentication phase

The Authentication procedure of proposed scheme is described in Fig. 10.

![Diagram of Authentication Phase]

Fig. 10 Proposed Authentication Phase

6.4 Password change phase

The password change procedure of proposed scheme is described in Fig. 10.

![Diagram of Password Change Phase]

7 Conclusion

To improve An’s authentication scheme, Li et al. proposed robust three-factor remote user authentication scheme with key agreement for multimedia system using ECC, but it has various problems. In this paper, we analyze the authentication scheme of Li et al. and executes cryptanalysis of security vulnerability. Last, we introduce requirement of authentication scheme for enhancing security and proposed security enhanced robust three-factor remote user authentication scheme with key agreement and anonymity.

7 REFERENCES


