Cryptanalysis of and Improvement on Biometric-based User Authentication Scheme for C/S System

Youn sung Choi, Dongho Won

Abstract—Password-based authentication schemes are convenient, but vulnerable to simple dictionary attacks. Cryptographic secret keys are safe, but difficult to memorize. More recently, biometric information has been used for authentication schemes. Das proposed a biometric-based authentication scheme, but it has various vulnerabilities. Jiping et al. improved Das’s scheme, but some vulnerabilities remain. In this paper, we analyze the cryptanalysis of Jiping et al.’s authentication scheme and propose the security enhanced biometric-based user authentication scheme for the C/S System.

I. INTRODUCTION

Remote identity-based authentication schemes are based on using only passwords. The password-based authentication schemes are the simple and convenient method to have a user authenticated in order to provide services of a computing or communication system [1-7]. However, only passwords are easy to break by using simple dictionary attacks. To overcome this problem, cryptographic secret keys and passwords are used in the remote user authentication schemes [8-10]. But the long and random cryptographic keys are difficult to memorize. So they must be stored somewhere, it is very weak point. To solve problem, various biometric-based authentication schemes are proposed. Das proposed new authentication scheme but has various vulnerability [11], so Jiping et al. proposed the security improved biometric-based user authentication scheme for C/S system than Das’s scheme [12]. But Jiping et al.’s scheme still has security problems. In section 2, we study related works. In section 3, we briefly review the Jiping et al’s biometric-based remote user authentication scheme using smart cards. In section 4, we analyze the security vulnerability of Jiping et al.’s authentication scheme and suggest solution. Finally, we conclude the paper in section 5.

II. RELATED WORKS

A. Smart card Attack

Various researchers have observed that confidential information stored in all smart cards could be extracted by physically monitoring power consumption like SPA and DPA. When a user loses a smart card, an attacker can analyze it. So various schemes leave it vulnerable to off-line password attacks. And attacker can be authenticate to server without user’s ID and password.

B. Biometric-based Authentication

Biometrics refers to the quantifiable data related to human characteristics and traits. Example include to fingerprint, face recognition, DNA, palm print, hand geometry, iris, retina, odour/scent, typing rhythm, gait, and voice. Biometrics-based authentication is used in identification and access control. Biometric information cannot be lost or forgotten and is very difficult to copy or share and forge or distribute. And also, biometric information cannot be guessed easily and is not easier to break than others.

C. Das’s Biometric-based User Authentication Scheme

Das proposed biometric-based remote user authentication which is inherently more reliable and secure than usual traditional password-based remote authentication schemes. But this scheme has security vulnerability to replay attack, denial-of-service attack, user impersonation attack, and password change problem. Moreover, this scheme does not provide mutual authentication between the user and server.

III. REVIEW OF JIPING ET AL.’S SCHEME

Das proposes biometric-based authentication scheme but this scheme is various security problems. To solve these problems, Jiping et al proposed improved biometric-based authentication scheme [12]. For convenience, we use notations shown in Table 1.

<table>
<thead>
<tr>
<th>Table 1: Notation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notation</td>
</tr>
<tr>
<td>C_i</td>
</tr>
<tr>
<td>S_i</td>
</tr>
<tr>
<td>R_i</td>
</tr>
<tr>
<td>PW_i</td>
</tr>
<tr>
<td>ID_i</td>
</tr>
<tr>
<td>B_i</td>
</tr>
<tr>
<td>d(·)</td>
</tr>
<tr>
<td>τ</td>
</tr>
<tr>
<td>h(·)</td>
</tr>
<tr>
<td>X_i</td>
</tr>
<tr>
<td>R_i</td>
</tr>
<tr>
<td>R_s</td>
</tr>
<tr>
<td>A</td>
</tr>
<tr>
<td>A ⊕ B</td>
</tr>
</tbody>
</table>

A. Registration Phase

In the registration phase, remote user C_i has to perform the following registration steps. Figure 1 shows the registration phase of Das scheme.
C. Authentication Phase

In the authentication phase, remote user Ci and server Si have to perform the following authentication phase. When the remote server Si receives the login message \(<g_1, M_2, M_3, T>\) at time \(T^*\), it will perform the following steps as shown in Figure 3 to authenticate whether the user Ci is legitimate or not. Figure 3 show the authentication phase.

1. Check T. If \((T^* - T) \geq \Delta T\), the authentication phase is terminated, where \(\Delta T\) is the expected time interval for the transmission delay of the system. Otherwise, if \((T^* - T) \leq \Delta T\), the authentication steps will be performed.

2. Si checks the accuracy of Ci’s ID. It computes \(M_1 = h(g_1, X_1)\) using the secret value \(X_1\) maintained by the server Si and then computes \(M_2 = M_1 \oplus M_3\) and verifies whether \(M_2 = M_2\) or not. If it does not match, then Si rejects Ci’s login request. The verification is successful, the next step will be performed.

3. Si computes \(M_4 = h(R_s \mid T_s)\) and \(M_5 = M_4 \oplus M_6\), where \(T_s\) is the timestamp of the server Si, and then Si sends message \(<M_4, M_5, M_7, T_s>\) to user Ci.

4. After receiving the message \(<M_4, M_5, M_7, T_s>\) at time \(T^{**}\), Ci checks the freshness of \(T_s\) by verifying \((T^{**} - T_s) \geq \Delta T\). If it holds, the following session is terminated; otherwise Ci computes \(M_8 = M_2 \oplus M_5\) and then verifies whether \(M_8 = M_5\). If it does not hold, Ci terminates the session. Otherwise, it goes to the next step.

5. Ci computes \(M_9 = M_3 \oplus M_2\) and then verifies whether \(M_9 = M_5\). If it does not hold, Ci is rejected by Ci; otherwise, if it holds, Ci computes \(M_{10} = h(R_c \parallel T^*)\), where \(T^*\) is the current timestamp of the user Ci, and then computes \(M_{11} = M_2 \oplus M_7 \oplus M_{10}\) and sends the message \(<M_{11}, R_c, T^*>\) to the remote server Si.

Step 6. When Si receives the message \(<M_{11}, R_c, T^*>\) at time \(T^{***}\), it checks \((T^{***} - T^*) \times \Delta T\). If it holds, the authentication phase is terminated. Otherwise, if it does not hold, Si computes \(M_{12} = h(R_c || T^*)\) and then computes \(M_{13} = M_4 \oplus M_5 \oplus M_{12}\). After computing \(M_{13}\), then Si verifies whether \(M_{13} = M_{12}\). If it holds, Si accepts Ci’s login request; otherwise, Si rejects the login request.

D. Password Change Phase

In Jiping et al.’s scheme, user Ci can freely change the password \(PW_{old}\) to a new one \(PW_{new}\). The password change procedure is performed as follows.

1. Ci inserts the smart card into the card reader and offers user’s personal biometrics \(B_i\). The smart card computes \(f(T)\).
h(B′) and verifies it by checking d(f′, fi) ≤ τ. Where f1 = h(B)
(2) If it holds, Ci inserts old password PWold and new
password PWnew, Otherwise the password change procedure
is terminated.
(3) Smart card performs r′ = h(PWnew) ⊕ f1; and checks
d(r′, ri) ≤ τ. ri is the information stored in the smart card.
(4) If it holds, the smart card computes r′ = h(PWnew) ⊕ f1,
e′ = e, ⊕ ri(= h(IDi || X3)), and e′′ = e′ ⊕ r1.
(5) Finally, replace e with e′′ and ri with r′ in the smart card.

IV. CRYPTANALYSIS OF JIPING ET AL.'S SCHEME

Jiping et al enhanced the security of Das’s authentication
scheme and proposed the new authentication scheme. But
Jiping et al’s authentication scheme still has security problem.
These problems are server masquerading attack, stolen smart
card attack and authentication without login phase.

A. Server Masquerading Attack
Attacker can masquerade as legitimate server if attacker
knows h(g, || X3). It is reason that server authenticates user
using only h(g, || X3). Figure 4 shows the phase of server
masquerading attack. Firstly, attacker intercepts client’s
message <g, M2, M3, T2>. Then, attacker calculates h(g, || X3)
using M2 ⊕ M3. Because h(g, || X3i) = e, ⊕ r1 = M2 ⊕ M3.
The attacker computes M′2, M′3, and T′ using h(g, || X3) and
sends them to client. The client and authenticates messages.
And the attacker receives M2, R, and T′, then attacker
checks the success to masquerades as server. The
client is authenticated with the attacker. In Jiping et al’s
scheme, the attacker can execute server masquerading attack.
To solve this problem, it is necessary to add another security
information to authenticate with server and client. The
Attacker has to not compute the security information using
communicate message between server and client.

B. Stolen Smartcard Attack
Kocher et al. and Messerges et al. 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 loses his smart card, all
secrets in the smart card may be revealed by attacker [13,14].

In Jiping et al.’s scheme, a smart card stores various secrets
for the login and authentication of user. The smart card for
user IDi includes (h(i), f1, g, e, r, τ, d(·)). So if attacker gets
or steals user’s smart card, attacker can obtain and know f1, g,
e, r of user. The attacker can calculate h(PWi) and h(IDi), then
attacker executes off-line password attack using rainbow table,
dictionary attack and brute attack. So the attacker can obtain
IDi and PWi. It is reason that IDi and PWi are protected using
h(·). To solve this problem, it is necessary to add random
number with high-entropy. Figure 5 shows the phase of stolen
smart card attack.

gets(steals) user’s smart card
obtains information from smart card using SPA and DPA
→ gets h(·), f1, g1, e1, r1, τ and d(·)
Attacker knows f1, g1, r1
r1 = h(PW1) ⊕ f1
→ h(ID1) = g1
→ h(PW1) = r1 ⊕ f1
executes off-line password attack
→ figures out user’s ID and password ID1, PW1

C. Authentication without Login Phase.
In Jiping et al.’s scheme, attacker can be authenticate with
server without login phase. To skip the login phase, the
attacker need to still or get the user’s smart card. In other
words, if the attacker obtain user’s smart card, the attacker
can be authenticate to server without user’s IDi, PWi and user’s
biometric information Bi. Figure 6 shows the phase of
authentication without login phase.

gets(steals) user’s smart card
obtains information from smart card using SPA and DPA
→ gets h(·), f1, g1, e1, r1, τ and d(·)
computes M1, M2, M3
→ generates random number R
→ M1 = e1 ⊕ r1
→ M2 = h(R) ⊕ T
→ M3 = M1 ⊕ M2

sends login and authentication message to S1
→ (g1, M2, M3, T)
attacker receives S1’s message
→ (M4, M6, M7, T)
computes M11, R, T'
→ generates timestamp T'
→ M10 = h(R, T')
→ M11 = M8 ⊕ M10

sends authentication message to S1
→ (M11, R, T')
→ attacker can be authenticated with S1

Fig. 6. Authentication without login phase
Firstly, attacker gets or steals the user’s smart card and obtains information from smart card using SPA and DPA. So the attacker can generate and compute the $R_c, M_1, M_2$ and $M_3$ using this information. And the attacker sends $(g_i, M_2, M_1, T)$ to the server. Then, the attacker receives $(M_4, M_6, M_7, T_4)$ and then, the attacker can computes $(M_11, R_c, T')$ and send these messages to server. So attacker can be authenticated to the server without user’s ID, PW, and the user’s biometric information $B$. To solve this problem, it is necessary to add information of user’s PW or $B_i$ to authentication messages.

V. PROPOSED SCHEME

In this section, to solve Jiping et al.’s security problem, we propose security enhanced biometric-based user authentication Scheme for the C/S System.

A. Proposed registration phase

The registration procedure of proposed scheme is described in Fig. 7

1. choose $ID_i, PW_i$
2. generates $B_i, K$
3. computes $PW_i = h(PW_i) || K$

\[ \langle ID_i, B_i, PW_i \rangle \]

4. computes $f_i, g_i, r_i, R_i, P_i$ and $e_i$
5. $g_i = h(ID_i)$
6. $r_i = h(PW_i) \oplus f_i \oplus R_i$
7. $e_i = h(g_i || X_i) \oplus r_i \oplus R_i$
8. $z_i = h(Y_i) \oplus R_i$

\[ \text{smart card: } [h(\cdot), f_i, g_i, e_i, r_i, P_i, z_i, r_i, \text{other}] \]

\[ \text{input } K \text{ to smart card} \]

B. Proposed login phase

And now, the login procedure of proposed scheme is described in Fig. 8

1. inserts the smart card and $B_i$
2. verifies whether $d(B_i, B_i) < r_i$?
3. if it holds, then $C_i$ inputs his/her password $PW_i$
4. computes $R = Rexp(B_i, P_i)$
5. computes $r'_i = h(PW_i) \oplus f_i \oplus R_i$ and verifies whether $d(r_i, r'_i) \neq r_i$?
6. if it holds, the smart card computes the following:
7. $M_1 = e_i \oplus r'_i \oplus h(R_i) = h(g_i || X_i)$
8. $M_2 = h(R_i || T)$
9. $M_3 = h(M_2 \oplus h(SID_i || Y_i)$
10. $AUD_i = g_i \oplus h(R_i || T)$

\[ \langle AUD_i, M_2, M_3, T \rangle \]

C. Proposed authentication phase

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

1. when receiving $(AUD_i, M_2, M_3, T)$, checks $(T^* - T) > \Delta T$?
2. computes $g_i = AUD_i \oplus h(h(SID_i || Y_i) || T)$
3. computes $M_4 = h(g_i || X_i), M_5 = M_4 \oplus h(h(SID_i || Y_i) || T)$, and verifies whether $M_5 = M_5'$?
4. computes $M_6 = h(R_i || T)$
5. computes $S_1 = M_4 \oplus h(h(SID_i || Y_i) || T) \oplus T_5 \oplus T_6
6. then, $M_7 = M_4 \oplus M_5$

VI. CONCLUSION

In this paper, we analyze the cryptanalysis of Jiping et al.’s biometric-based user authentication scheme for the client/server system. Jiping et al. proposed an improved authentication scheme to solve the problem of vulnerabilities in Das’s scheme. However, Jiping et al.’s scheme has some remaining security problems: the server-masquerading attack, stolen smart-card attack and authentication without login phase. To solve this problem, it is necessary to add secret information to the registration, login and authentication phases. And we proposed security enhanced biometric-based user authentication Scheme for the C/S System.

REFERENCES


