Security Weaknesses of an Improved Biometrics-based User Authentication Scheme without Concurrency System

Young-Hwa An*
*Computer Media Information Engineering, Kangnam University, 111, Gugal-dong, Giheung-gu, Yongin-si, Gyounggi-do, 446-702, Korea
yhan@kangnam.ac.kr

Abstract—Recently, many biometrics-based user authentication schemes using smart cards have been proposed to improve the security weaknesses in user authentication system. In 2010, Chang et al. proposed an improved biometrics-based user authentication scheme without concurrency system which can withstand the forgery attack, the off-line password guessing attack, the replay attack, etc. In this paper, we analyze the security weaknesses of Chang et al.’s scheme, and we will show that Chang et al.’s scheme is still vulnerable to the user impersonation attack, the server masquerading attack and the biometric guessing attack, and does not provide the mutual authentication between the user and the remote server.

Keywords—Authentication, Biometrics, User Impersonation Attack, Server Masquerading Attack, Mutual Authentication

I. INTRODUCTION

With the increasing of users using commercial services through networks, the user authentication scheme using smart card has been becoming one of important security issues. However, security weaknesses have been exposed in the user authentication scheme due to the careless password management and the sophisticated attack techniques. Several schemes[1]-[7] have been proposed to improve security, efficiency, and cost.

Recently, personal biometrics information, such as fingerprints, faces, irises, hand geometry, and palm-prints, etc. has been used to design biometrics-based user authentication schemes[8]-[13]. There are several advantages of using biometrics key as compared to traditional passwords.

• Biometric keys cannot be lost or forgotten.
• Biometric keys are very difficult to copy or share.
• Biometric keys are extremely hard to forge or distribute.
• Biometric keys cannot be guessed easily.
• Someone’s biometrics is not easy to break than others.

As described above, biometrics-based remote user authentication schemes are inherently more reliable and secure than traditional password-based remote user authentication schemes.

In 2004, Jin et al.[8] proposed two-factor authentication scheme using fingerprint data and tokenized pseudo random number. Using this new scheme proposed by Jin et al., in 2010, Li and Hwang[11] proposed an efficient biometrics-based remote user authentication scheme using smart cards. However, in 2010, Chang et al.[12] pointed out that Li and Hwang’s scheme allowed an attacker to perform the off-line password guessing attack. And Chang et al. proposed an improved biometrics-based user authentication scheme without concurrency system that is secure against the forgery attack, the off-line password guessing attack, and the replay attack.

In this paper, if an attacker can access a user’s smart card and extract the values stored in the smart card by monitoring the power consumption or analyzing the leaked information[14]-[16], we show that Chang et al.’s scheme is not secure against the user impersonation attack, the server masquerading attack, and the biometrics guessing attack. And we can show that Chang et al.’s scheme also does not provide the mutual authentication between the user and the remote server.

This paper is organized as follows. In section II, we briefly review Chang et al.’s scheme. In section III, we describe the security weaknesses of Chang et al.’s scheme. Finally, conclusions are made in section IV.

II. REVIEW OF CHANG ET AL.’S SCHEME

In this section, we briefly review Chang et al.’s scheme[12]. The security of this scheme is based on hash function and random nonce to withstand the forgery attack, the off-line password guessing attack and the replay attack. Chang et al.’s scheme is divided into three phases: registration phase, login phase, and authentication phase. We present the illustration of registration phase in Fig. 1, and login and authentication phase in Fig.2. And the notations used in this paper are listed below:

• U: The user
• S: The server
• R: The registration centre
• ID: Identity of user
• X: Secret information kept by the server
• Q: Biometric information of the user
• \( N_u \): A nonce chosen by user
• \( N_s \): A nonce chosen by server
• \( h() \): One-way hash function
• \( \parallel \): Concatenation
• \( \oplus \): Exclusive-OR operation

### A. Registration Phase

This phase works whenever a user registers to the registration centre and obtains the smart card.

1) The user submits his identifier \( ID \) and the personal biometrics \( Q \) to the registration centre through a secure channel.

2) Upon receiving the submitted information, the registration centre selects a random number \( R_1 \), and then computes:

\[
f = Q \oplus R_1 \]
\[
m = h(ID \parallel X_s) \oplus f
\]

where \( R_1 \) is the first time random secret to protect the biometrics.

3) The registration centre issues the information \( \{ID, h(), R_1, f, m\} \) to the smart card and sends it to the user through a secure channel.

### B. Login Phase

This phase works whenever the user wants to login to the remote server.

1) The user inserts his smart card into a card reader and provides the personal biometrics \( Q \) on the specific device.

2) The smart card computes \( f' = Q \oplus R_1 \), and verifies whether \( f' \) equals \( f \) or not.

3) If it holds, the user generates a random nonce \( N_u \) and computes \( S_1 = m \oplus f' \oplus N_u \).

4) And then, the user sends the message \( \{ID, S_1\} \) to the remote server.

### C. Authentication Phase

This phase works whenever the remote server received the user’s login request.

1) The server checks the format of \( ID \).

2) If it holds, the server computes \( C_1 = h(ID \parallel X_s) \oplus S_1 \) using \( h(ID \parallel X_s) \).

3) The server computes:

\[
S_2 = h(h(ID \parallel X_s) \parallel C_1) \oplus N_s
\]
\[
S_3 = h(h(ID \parallel X_s) \parallel C_1) \parallel N_s
\]

where \( N_s \) is a random nonce selected by the server.

4) The server sends the message \( \{S_2, S_3\} \) to the user.

5) Upon receiving the message, the server checks the format of \( ID \).

6) If it holds, the server authenticates the server as a legal server, and then computes \( S_4 = h((m \oplus f') \parallel X_s) \).

7) The server sends the message \( \{S_4\} \) to the server.

8) Upon receiving the message, the server verifies whether \( S_4 \) equals \( h((m \oplus f') \parallel X_s) \parallel N_s \) or not.

9) If it holds, the server authenticates the user as a legal user and accepts the user’s login request.

After performing the above phases, Chang et al.’s scheme provides the mutual authentication between the user and the server.

### III. Security Weaknesses of Chang et al.’s Scheme

In this section, we analyze the security of Chang et al.’s scheme. To analyze the security weaknesses, we assume that an attacker could obtain the secret values stored in the smart card illegally by monitoring the power consumption or analyzing the leaked information[14]-[16] and intercept the messages communicating between the user and the server.

#### A. User Impersonation Attack

As described above, we assume that the attacker can extract the secret values \( f, m \) from the user’s smart card illegally by some means and intercepts the message \( \{S_1\} \) communicating between the user and the server. The procedure of the user impersonation attack is like the...
Following steps. Also, the user impersonation attack is illustrated in Fig. 3.

**Figure 3. User Impersonation Attack and Server Masquerading Attack**

1) In the registration phase, the attacker computes easily $h(ID \parallel X_u)=f \oplus m$ using the extracted secret values $(f, m)$ from the legal user’s smart card.

2) And then, the attacker generates random nonce $N_u$, and then computes $S_{1a}=h(ID \parallel X_u) \oplus N_u$.

3) The attacker sends the forged message $\{ID, S_{1a}\}$ to the remote server.

4) Upon receiving the message, the remote server checks the format of ID. If it holds, the remote server will be convinced that the message is sent from the user. And then the remote server will compute $N_u^*=h(ID \parallel X_u, S_{1a})$ and make the return message $S_2, S_3$.

Therefore, the attacker without knowing the biometrics information of the user can impersonate as the legal user.

**B. Server Masquerading Attack**

As described in the above subsection, such as the user impersonation attack and the server masquerading attack, Chang et al.’s scheme fails to provide the mutual authentication between the user and the remote server. That is, if the attacker can extract the secret values $(f, m)$ from the legal user’s smart card, the attacker can impersonate the legal user easily by computing the equation $S_{1a}=h(ID \parallel X_u) \oplus N_u$. Also, if the attacker can extract the secret values $(f, m)$ from the legal user’s smart card and intercepts the message $\{S_1\}$ communicating between the user and the server, the attacker can masquerade the legal remote server easily by computing the equation $S_{2a}=h(ID \parallel X_u, S_{1a}) \oplus N_u$ and $S_{3a}=h(ID \parallel X_u) \parallel N_u^* \parallel N_3$.

**C. Biometrics Guessing Attack**

As described in the above subsection, such as the user impersonation attack and the server masquerading attack, Chang et al.’s scheme fails to provide the mutual authentication between the user and the remote server. That is, if the attacker can extract the secret values $(f, R_1)$ from the user’s smart card illegally by some means. Now, the attacker can easily find out the biometric information of the user by computing the $Q= f \oplus R_1$. In Chang et al.’s scheme, the biometrics is very important information because it is necessary to confirm personal identity in registration and login phase. If an attacker gets the secret biometrics information, the attacker can use it to impersonate a legal user who wants to register with this system.

**D. Mutual Authentication**

As described in above subsection, such as the user impersonation attack and the server masquerading attack, Chang et al.’s scheme fails to provide the mutual authentication between the user and the remote server. That is, if the attacker can extract the secret values $(f, m)$ from the legal user’s smart card, the attacker can impersonate the legal user easily by computing the equation $S_{1a}=h(ID \parallel X_u) \oplus N_u$. Also, if the attacker can extract the secret values $(f, m)$ from the legal user’s smart card and intercepts the message $\{S_1\}$ communicating between the user and the server, the attacker can masquerade the legal remote server easily by computing the equation $S_{2a}=h(ID \parallel X_u, S_{1a}) \oplus N_u$ and $S_{3a}=h(ID \parallel X_u) \parallel N_u^* \parallel N_3$.

**IV. Conclusions**

In 2010, Chang et al. proposed an improved biometrics-based user authentication scheme without concurrency system which can withstand the forgery attack, the off-line password guessing attack, the replay attack, etc. In this paper, we analyze the security weaknesses of Chang et al.’s scheme, and we have shown that Chang et al.’s scheme is still vulnerable to the user impersonation attack, the server masquerading attack and the biometrics guessing attack. In addition, we can see that Chang et al.’s scheme fails to provide the mutual authentication between the user and the remote server.

**Acknowledgment**

This work was supported by Kangnam University Research Grant in 2011.

**References**


