Security Weaknesses and Improvements of a Fingerprint-based Remote User Authentication Scheme Using Smart Cards

Hyung-Kyu Yang, Young-Hwa An
Division of computer-media engineering Kangnam University, hkyang@kangnam.ac.kr
Division of computer-media engineering Kangnam University, 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 2006, Khan et al.[12] proposed an improved fingerprint-based remote user authentication scheme using smart cards that is achieved mutual authentication between the user and the server, while eliminating the drawback of Lee et al.’s scheme[9]. Later, in 2008, Xu et al.[13] pointed out that Khan et al.’s scheme cannot withstand the parallel session attack and the impersonation attack. In this paper, we also analyze the security weaknesses of Khan et al.’s scheme, and we have shown that Khan et al.’s scheme is still vulnerable to the forgery attack, the off-line password guessing attack, the parallel session attack, and the insider attack. And, we propose the improved scheme to overcome these security weaknesses, while preserving all their merits, even if the secret information stored in the smart card is revealed.

Keywords: Authentication, Biometrics, Smart Card, Forgery Attack

1. Introduction
With the rapid development of network technology, user authentication scheme in e-commerce and m-commerce has been becoming one of important security issues. However, the security weaknesses in the remote user authentication scheme have been exposed seriously due to the careless password management and the sophisticated attack techniques. Many schemes[1-8] 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[9-15]. 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 2002, Lee et al.[9] proposed a fingerprint-based authentication scheme using smart cards. However, Lin et al.[10] in 2004 and Ku et al.[11] in 2005 pointed out that Lee et al.’s scheme cannot withstand the masquerading attack, in which an attacker can impersonate a legitimate user without knowing the password and passing the fingerprint verification. Later, Khan et al.[12] in 2006 also showed that Lee et al.’s scheme was vulnerable to the server spoofing attack. And Khan et al. proposed an improved fingerprint-based remote user authentication scheme using smart cards that is achieved mutual authentication between the user and the server, while eliminating the drawback of Lee et al.’s scheme. But, in 2008, Xu et al.[13] pointed out that Khan et al.’s scheme cannot withstand the parallel session attack and the impersonation attack.

In this paper, we also analyze the security weaknesses of Khan et al.’s scheme and we have shown that Khan et al.’s scheme is still vulnerable to the forgery attack, the off-line password guessing attack, the parallel session attack, and the insider attack. To analyze the security of Khan et al.’s scheme, we assume that an attacker could extract the secret values stored in the smart card by monitoring the power...
consumption[16-17] and intercept messages communicating between the user and the server. And, we propose the improved scheme to overcome these security weaknesses, while preserving all their merits, even if the secret information stored in the smart card is revealed.

This paper is organized as follows. In section 2, we briefly review Khan et al.’s scheme. In section 3, we describe the security weaknesses of Khan et al.’s scheme. The improved scheme is presented in section 4, and its security analysis and performance evaluations are given in section 5. Finally, the conclusions are given in section 6.

2. Reviews of Khan et al.’s Scheme

In 2006, Khan et al.[12] proposed an efficient and practical fingerprint-based remote user authentication scheme using smart cards. This scheme is divided into three phases: registration phase, login phase, and authentication phase. The notations used throughout this paper are as follows:

- U: The user
- S: The server
- ID: Identity of user
- PW: Password of user
- x: Secret key kept by server
- F: Fingerprint template of user
- h(): One-way hash function
- ⊕: Exclusive-OR operation

2.1 Registration Phase

This phase works whenever the user initially registers to the remote server.

1. The user submits his identifier ID and password PW to the server through a secure channel. Also the user imprints his fingerprint at the sensor.
2. The server computes $A = h(ID \oplus x)$ and $V = A \oplus h(PW \oplus F)$.
3. The server issues the smart card containing the information $\{ID, A, V, F, h()\}$ to the user.
4. 

2.2 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, keys in his ID and PW’, and imprints his fingerprint at the sensor.
2. The smart card computes $B = V \oplus h(PW' \oplus F)$, and verifies whether B equals A or not. If it holds, this phase continues.
3. The smart card computes $C_1 = h(B \oplus T)$, where T is the current time.
4. The smart card sends message $m = \{ID, C_1, T\}$ to the server.

2.3 Authentication Phase

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

1. The server verifies the validity of ID, and checks the validity of the time interval between T and T’, where T’ is a time stamp when the server receives message.
2. The server computes $C_1^* = h(h(ID \oplus x) \oplus T)$, and checks whether the computed value $C_1^*$ equals $C_1$ or not. If it holds, the user’s login request is accepted.
3. For mutual authentication, the server computes $C_2 = h(h(ID \oplus x) \oplus T')$, and sends the message $\{C_2, T'\}$ back to the user, where $T'$ is a current time.

4. Upon receiving the message $\{C_2, T'\}$, the user verifies the validity of the time interval, and then checks whether the computed value $h(B \oplus T')$ equals $C_2$ or not. If it holds, the mutual authentication is completed.

3. Security Weaknesses of Khan et al.’s Scheme

To analyze the security of Khan et al.’s scheme, we assume that an attacker could extract the secret values stored in the smart card by monitoring the power consumption[16-17] and intercept messages communicating between the user and the server.

3.1 Forgery Attack

In Khan et al.’s scheme, the attacker without knowing user's password can impersonate as the legal user. As described above, we assume that an attacker can extract the secret values $A, V, F$ from the legal user's smart card by some means. With these secret values, the attacker can perform the user impersonation attack easily as the following steps.

1. The attacker computes easily $C_1^* = h(A \oplus T^*)$, where $T^*$ is the current time stamp. Then, the attacker sends the forged message $m_1^* = \{ID, C_1^*, T^*\}$ to the remote server.
2. Upon receiving the message $m_1^*$, the attacker can successfully impersonate as the legal user, because the remote server will be convinced that the message $m_1^*$ is sent from the legal user for login.

Also, the attacker can perform the server masquerading attack easily as the following steps.
3. The attacker computes easily $C_2^* = h(A \oplus T'^*)$, where $T'^*$ is the current time stamp. Then, the attacker sends the forged message $m_2^* = \{C_2^*, T'^*\}$ to the user.
4. Upon receiving the message $m_2^*$, the attacker can successfully masquerade as the legal remote server, because the user will be convinced that the message $m_2^*$ is sent from the legal server for mutual authentication.

Hence, the attacker can perform the user impersonation attack and the server masquerading attack. Therefore Khan et al.’s scheme does not provide the mutual authentication between the user and the remote server.

3.2 Password Guessing Attack

For attack, we assume that an attacker can extract the secret values $A, V, F$ from the legal user's smart card by some means. With these secret values, the attacker can easily find out $PW$ by employing the password guessing attack, in which each guess $PW^*$ for $PW$ can be verified by the following steps.

1. The attacker computes the parameter $V^* = A \oplus h(PW^* \oplus F)$ from the registration phase.
2. The attacker verifies the correctness of $PW^*$ by checking $V = V^*$.
3. The attacker repeats the above steps until a correct password $PW^*$ is found.

Thus, the attacker can perform the off-line password guessing attack.

3.3 Parallel Session Attack

In Khan et al.’s scheme, the attacker simply eavesdrops on the remote server’s response message $\{C_2, T'^*\}$ for mutual authentication between the user and the server, and immediately starts a parallel session sending the forged login request message $\{ID, C_2, T'^*\}$ to the server. Since $C_2$ equals $h(h(ID \oplus x) \oplus T')$, the remote server believes that the login request message $\{ID, C_2, T'^*\}$ comes from another instance of the user as long as the message arrives at the remote server before the timer expires. The vulnerability of Khan et al.’s
scheme against this parallel session attack is mainly because that two authenticators \(C_1, C_2\) exchanged between two authenticating parties are computed using the same expression/ \(h(h(ID \oplus x) \oplus \text{timestamp})\).

### 3.4 Insider Attack

In the registration phase, if the user's password \(PW\) and fingerprint template \(F\) are revealed to the server, the insider of the server may directly obtain \(PW\) and \(F\). Therefore the insider as an attacker can impersonate the user to access the user’s other accounts in other server if the user uses the same password for the other accounts. Thus, the proposed scheme is not secure for the insider attack.

### 5. The Proposed Scheme

In this section, we propose an improved Khan et al.’s scheme which can withstand the forgery attack, the password guessing attack, the parallel session attack and the insider attack. The proposed scheme is divided into three phases: registration phase, login phase and authentication phase. The registration phase is illustrated in Fig. 1. Also, the login and authentication phase is illustrated in Fig. 2.

#### 4.1 Registration Phase

This phase works whenever the user initially registers to the remote server.

1. The user submits his identity \(ID\) and \(h(b \oplus PW)\) to the remote server through a secure channel, where a random number \(b\) is generated by the user. Also the user imprints his fingerprint at the sensor.
2. The server computes \(A = h(ID \oplus x)\) and \(V = A \oplus h(h(b \oplus PW) \oplus F)\), where \(x\) is a secret key of server.
3. The server issues the smart card to the user through a secure channel, where the smart card contains \(\{ID, V, F, h()\}\).
4. The user stores \(b\) into his smart card.

#### 4.2 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 enters his \(ID\) and \(PW\), and imprints his fingerprint \(F\) at a sensor.
2. The smart card computes \(B = V \oplus h(h(b \oplus PW) \oplus F)\), and \(C_1 = h(B \oplus T_1)\), where \(T_1\) is the current time.
3. The smart card sends a message \(m_1 = \{ID, C_1, T_1\}\) to the server.
4.3 Authentication Phase

This phase works whenever the remote server received the user’s login request. Upon receiving the message $m_1$ from the user, the remote server performs the following steps.

1. The server checks the validity of $ID$, and then verifies the time stamp $T_1$ with the current time $T'$. If $(T' - T_1) \leq \Delta T$, the server accepts the login request, where $\Delta T$ denotes the expected valid time interval for transmission delay.

2. The server computes $B^* = h(ID \oplus x)$, and $C_1^* = h(B^* \oplus T_1)$.

3. The server checks whether $C_1^* = C_1$ or not. If they are equal, the user's login request is accepted.

4. The server computes $C_2 = h(B^* \oplus C_1^* \oplus T_2)$, where $T_2$ is the current time stamp, and then sends a message $m_2 = \{C_2, T_2\}$ to the user. Upon receiving the message $m_2$ from the server, the user performs the following steps.

5. The user verifies the time stamp $T_2$ with the current time $T''$. If $(T'' - T_2) \leq \Delta T$, then the smart card computes $C_2^* = h(B \oplus C_1 \oplus T_2)$.

6. The user checks whether $C_2^* = C_2$ or not. If they are equal, the server is authenticated and allowed to access the smart card.
5. Security Analysis and Performance Evaluations of the Proposed Scheme

In this section, we will analyze the security of the proposed scheme based on secure one-way hash function, and evaluate the performance of the proposed scheme.

5.1 Security Analysis

To analyze the security of the proposed scheme, we assume that an attacker could extract the secret values stored in the smart card by some means[16-17] and intercepts the messages \( m_1, m_2 \) communicating between the user and the server.

** Forgery Attack:**

The attacker can extract the secret values \( V, F, b \) from the legal user's smart card by some means and intercept the message \( m_1, m_2 \) between the user and the server under the described assumption. Without knowing the user's password, the attacker attempts to make the forged message \( \{ ID, C_1^*, T_1^* \} \) for logging in to the server. However, the attacker cannot make the \( C_1^* = h(B \oplus T_1^*) \), because the attacker does not know the remote server's secret value \( x \). Hence, the attacker has no chance to login by launching the user impersonation attack. Also, the attacker attempts to make the forged message \( \{ C_2^*, T_2^* \} \) for authenticating.
to the user. However, the attacker cannot make the $C_2^* = h(B \oplus C_1^* \oplus T_2^*)$, because the attacker does not know the remote server’s secret value $x$. Hence, the attacker has no chance to authenticate by launching the server masquerading attack.

Therefore, the proposed scheme is secure for the user impersonation attack and the server masquerading attack.

**Password Guessing Attack:**

The attacker can extract the secret values $V, F, b$ from the legal user's smart card by some means under the described assumption. Then the attacker attempts to derive the user’s password $PW$ using $V = A \oplus h(h(b \oplus PW) \oplus F)$ in the registration phase. However, the attacker cannot guess the user’s password $PW$ using the secret values extracted from the legal user's smart card, because the attacker does not know the server’s secret value $x$. Hence, the proposed scheme is secure for the off-line password guessing attack.

**Parallel Session Attack:**

We assume that a message $m_1 = \{ID, C_1, T_1\}$ in the login phase is sent by a user as the request, which is followed by a server response $m_2 = \{C_2, T_2\}$ in the authentication phase. In the proposed scheme, the parallel session attack can be plotted by an attacker if two authenticators $C_1, C_2$ exchanged between two authenticating parties are computed using the same expression $\{h(h(ID \oplus x) \oplus timestamp)\}$. However, the expression of authenticator $C_1 (= h(B \oplus T_1))$ in the login phase is different from the expression of authenticator $C_2 (= h(B^* \oplus C_1^* \oplus T_2^*))$ in the authentication phase. Hence, the proposed scheme is secure for the parallel session attack.

**Insider Attack:**

Generally, if user's password $PW$ is revealed to the server, the insider of the server may directly obtain $PW$ and impersonate the user to access the user’s other accounts in other server if the user uses the same password for the other accounts. But, the proposed scheme is secure for the insider attack, because this scheme asks user to submit $h(b \oplus PW)$ instead of $PW$ revealed to the server.

From the above discussions, the security comparison of the proposed scheme to Khan et al.’s scheme is summarized in Table 1. We can see that the proposed scheme is relatively more secure than Khan et al.’s scheme.

<table>
<thead>
<tr>
<th>kind of attack</th>
<th>Khan et al.’s scheme</th>
<th>the proposed scheme</th>
</tr>
</thead>
<tbody>
<tr>
<td>forgery attack</td>
<td>possible</td>
<td>impossible</td>
</tr>
<tr>
<td>password guessing attack</td>
<td>possible</td>
<td>impossible</td>
</tr>
<tr>
<td>parallel session attack</td>
<td>possible</td>
<td>impossible</td>
</tr>
<tr>
<td>insider attack</td>
<td>possible</td>
<td>impossible</td>
</tr>
<tr>
<td>mutual authentication</td>
<td>impossible</td>
<td>possible</td>
</tr>
</tbody>
</table>

5.2 Performance Evaluations

In this section, we evaluate the efficiency of the proposed scheme in terms of the computational complexities by comparing with Khan et al.’s scheme. In Table 2, we can see that the proposed scheme requires some more operations than the operations of Khan et al.’s scheme, because the proposed scheme does provide the security against the various attacks.
Table 2. Performance comparison of the proposed scheme to Khan et al.’s scheme

<table>
<thead>
<tr>
<th>kind of phase</th>
<th>Khan et al.’s scheme</th>
<th>the proposed scheme</th>
</tr>
</thead>
<tbody>
<tr>
<td>registration phase</td>
<td>2TH+3TX</td>
<td>3TH+4TX</td>
</tr>
<tr>
<td>login phase</td>
<td>2TH+3TX</td>
<td>3TH+4TX</td>
</tr>
<tr>
<td>authentication phase</td>
<td>5TH+5TX</td>
<td>4TH+6TX</td>
</tr>
</tbody>
</table>

* TH: the time for performing a one-way hash function, TX: the time for performing an exclusive-OR operation

6. Conclusions

In this paper, we analyzed the security weaknesses of Khan et al.’s scheme. And we have shown that Khan et al.’s scheme is still insecure against the forgery attack, the off-line password guessing attack, the parallel session attack, and the insider attack. Also, we proposed the improved scheme to overcome these security weaknesses, while preserving all their merits, even if the secret information stored in the smart card is revealed. As a result of security analysis, the proposed scheme is secure for the forgery attack, the off-line password guessing attack, the parallel session attack, and the insider attack. And we can see that the proposed scheme requires some more operations than the operations of Khan et al.’s scheme due to enhance the security against the various attacks.

7. References
