Abstract. The user authentication scheme has been widely applied to verify the users’ legality. In order to enhance the security, the smart card has widely used in an authentication scheme. Recently, Liu et al. shown that some weaknesses existed in Li et al.’s scheme. They also proposed an efficient and secure user authentication scheme with smart card. Their scheme is more efficient and secure than other schemes. However, we find the security of their scheme is also existed. In this article, we will prove their scheme is vulnerable to the replaying attack.

Keywords: Password, Smart Card, User Authentication

1 Introduction

The user authentication scheme has been widely applied to verify the users’ legality. There are many password-based user authentication schemes have been proposed to verify the remote users’ identification [1-16]. However, the password is easy to be exposed by guessing attack. In order to enhance the security, the smart card has widely used in an authentication scheme [18-30].

Recently, Chen et al. proposed a robust smart-card-based remote user password authentication scheme [5]. However, Li et al. pointed out some weaknesses (i.e., forward secrecy and wrong password login problem) in Chen et al.’s scheme [14]. Li et al. also proposed an enhanced smart card based user authentication scheme [14]. However, Liu et al. shown that Li et al.’s scheme was unable to against the man-in-the-middle and insider attacks [17]. They also proposed an efficient and secure user authentication scheme with smart card. Their scheme is more efficient and secure than
other schemes. However, we find the security of their scheme is also existed. In this article, we will prove their scheme is vulnerable to the replaying attack.

The rest of this paper is organized as follows. In Section 2, we briefly review Liu et al.’s user authentication scheme. In Section 3, we analyze and show that some security weaknesses in Liu et al.’ user authentication scheme. Finally, we present our conclusions in Section 4.

2 Review of Liu-Chang-Chang Scheme

In this section, we briefly review Liu et al.’s user authentication scheme (Liu-Chang-Chang Scheme) with smart card [17]. There are three participants in Liu-Chang-Chang’s user authentication scheme: a user (U for short), a smart card (C for short), and a server (S for short). The scheme consists of four phases, namely the registration, the login phase, the authentication phase, and the password change phase. The notations used in this paper are listed in Table 1.

Table 1. The notations used in this paper

<table>
<thead>
<tr>
<th>Notations</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>U_i</td>
<td>The user i</td>
</tr>
<tr>
<td>ID_i</td>
<td>The identity of the user i</td>
</tr>
<tr>
<td>PW_i</td>
<td>The password of the user i</td>
</tr>
<tr>
<td>S</td>
<td>The providing service server</td>
</tr>
<tr>
<td>X</td>
<td>The server’s master secret key</td>
</tr>
<tr>
<td>Ti &amp; T_s</td>
<td>The timestamp of the user I and server, respectively.</td>
</tr>
<tr>
<td>Sk</td>
<td>The shared session key</td>
</tr>
<tr>
<td>h(.)</td>
<td>A collision-free one-way hash function</td>
</tr>
<tr>
<td>⊕</td>
<td>An XOR operation</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The Registration Phase:

In this phase, the server S makes a smart card for a new user (U_i). The smart card contains four parameters, {B_i, C_i, h(.), r}, where B_i = A_i ⊕ h(r || PW_i); A_i = h(ID_i ⊕ x)||h(x); C_i = h(A_i || ID_i || h(r||PW_i)); h(.) denotes a collision-free one-way hash function; r denotes a random number; ID_i and PW_i are user’s identity and password, respectively. The registration phase is executed as follows.

The Login Phase:

In this phase, a user (U_i) wants to login the server via public Internet. The login phase is executed as follows and illustrated in Figure 2.

1) The user Ui sends the login request parameters, ID_i and PW_i to the smart card.
2) The smart card computes \( A’i \) and \( C’i \) as follows: 
\[
A’i = Bi \oplus h(r || PWi); \quad C’i = h(A’i \parallel IDi \parallel h(r || PWi)).
\]
Next, the smart card checks whether \( C’i \) is equal to \( Ci \). If \( C’i \) is equal to \( Ci \), the smart card continues to execute Step 3, otherwise, the smart card terminates this login request.

3) The smart card computes \( Di \) and \( Ei \) as follows: 
\[
Di = h(IDi \oplus \alpha); \quad Ei = A’i \oplus \alpha \oplus Tc,
\]
where \( Tc \) denotes the current timestamp of the smart card and \( \alpha \) denotes a random number.

4) The smart card sends \( IDi, Di, Ei \) and \( Ti \) to the server \( S \).

**The Authentication Phase:**

Upon receiving the message, \( \{IDi, Di, Ei, Tc\} \), from User (Ui), the server \( S \) executes this authentication phase as follows.

1) The server checks \( IDi \) format and the timestamp \( Tc \) whether or not in valid time. If both conditions are not hold, the server \( S \) rejects the login request.

2) The server computes \( Ai, \alpha’, \) and \( Di’ \) as in Figure 3. Next, the server checks \( D’i \) whether equals to \( Di \). If the equation is not hold, the server \( S \) rejects the login request.

3) The server randomly selects \( \beta \) and computes \( Fi \) and \( Gi \) as in Figure 3. Next, the server \( S \) sends \( \{Fi, Gi, Ti\} \) vis public channel to user Ui.

4) The user Ui the timestamp \( Ts \) whether or not in valid time. If this condition is not hold, the user terminates this session.

5) The user computes \( \beta’ \) and \( F’i \). Next, the user checks \( F’i \) whether equals to \( Fi \). If this condition is true, the user Ui confirms the server \( S \) is legit.

6) The server \( S \) and the user Ui compute the session key \( sk = h(\alpha || \beta || h(Ai \oplus IDi)) \).

3 **Cryptanalysis of Liu-Chang-Chang Scheme**

In this section, we will show that Liu-Chang-Chang’s user authentication scheme [17] cannot withstand the replaying attack when the hacker intercepts \( \{IDi, Di, Ei, Ti\} \) between smart card and server \( S \) and \( \{F, G, Ts\} \) between user Ui and server \( S \). The first replaying attack is listed as follows.

Step1. When the smart card sent the message, \( \{IDi, Di, Ei, Ti\} \), to the server \( S \) in the login phase, the hacker intercepts \( \{IDi, Di, Ei, Ti\} \) between smart card and server \( S \) via public channel.

Step2. The hacker computes a new \( E’i \) as follows:
\[
E’i = Ei \oplus Ti \oplus Th
= (A’i \oplus \alpha \oplus Ti) \oplus Ti \oplus Th
= A’i \oplus \alpha \oplus Th
\]
Here, $Th$ denotes the timestamp of Hacker’s device. Next, the hacker sends the forged message $\{ID_i, D_i, E’i, Th\}$ to replace the intercepted $\{ID_i, D_i, E_i, T_i\}$.

Step3. The server $S$ will check successfully the equation in Steps 1) and 2) in the authentication phase. Thus, the server will be deceived by the hacker.

Figure 4: The replaying attack when the hacker intercepts $\{ID_i, D_i, E_i, T_i\}$

The second replaying attack is similar to the first replaying attack. The attack listed as follows.

Step1. When the server $S$ sent the message, $\{Fi, Gi, Ts\}$, to the user $Ui$ in the authentication phase, the hacker intercepts it between server $S$ and user $Ui$ via public channel.

Step2. The hacker computes a new $G’i$ as follows:

$$G’i = Gi \oplus Ts \oplus Th$$

$$= (Ai \oplus \beta \oplus Ts) \oplus Ts \oplus Th$$

$$= Ai \oplus \beta \oplus Th$$

The hacker sends the forged message $\{Fi, G’i, Th\}$ to replace the intercepted $\{Fi, Gi, Ts\}$.

Step3. The user $Ui$ will check successfully the equation in Steps 4) and 5) in the authentication phase. Thus, the user $Ui$ will be deceived by the hacker.

4 Conclusion

We have shown that there is a weakness in Liu-Chang-Chang’s user authentication scheme [17]. Their scheme cannot withstand the replaying attack when the hacker intercepts $\{ID_i, D_i, E_i, T_i\}$ between smart card and server $S$ and $\{F, G, Ts\}$ between user $Ui$ and server $S$. 

Acknowledgments

This study was supported by the National Science Council of Taiwan under grant MOST 104-2221-E-468-004 and MOST 103-2221-E-468-026.

5 References