Improved Password-Authenticated Key Agreement
Using Smart Cards

Kai Chai1, Wen-Chung Kuo2, Chun-Pei Hsiang3, Jiin-Chiou Cheng3, Jar-Ferr Yang1

1 Institute of Computer and Communication Engineering, Department of Electrical
Engineering, National Cheng Kung University, Taiwan, R.O.C.
chainkai@crypto.ee.ncku.edu.tw
jfyang@ee.ncku.edu.tw

2 Department of Computer Science and Information Engineering, National Yunlin University
of Science & Technology, Taiwan, R.O.C.
simonkuo@yuntech.edu.tw

3 Department of Computer Science and Information Engineering, Southern Taiwan
University, Taiwan, R.O.C.
{m99g0105, chiou}@webmail.stut.edu.tw

Abstract. Using smart cards for authentication has become a common trend. Although this system brings conveniences, it also increases the risk in the case of lost cards. In this paper, we analyze the lost smart card attack from Juang et al.’s scheme [4] that proposes password authenticated key agreement. In order to bolster the security of the entire system, we mitigated some of its weaknesses.

Keywords: key exchange, elliptic curve cryptosystem, smart card, authentication.

1 Introduction

In 2008, Juang et al. (for short JCL-scheme)[4], point out the major drawbacks are loss of anonymity for the user and high computation and communication cost in Fan et al.’s scheme. To improve upon these drawbacks, Juang et al. proposed a scheme that not only can provide identity protection but also keep lower communication and computation cost by using elliptic curve cryptosystems. They also proposed a solution for minimizing the risk of lost cards. The use of a fixed server key allows an offline attack to be mounted against the server key when an attacker possesses the user card. Therefore, we propose to improve JCL-scheme and mitigate the exposure of the entire system when a smart card is compromised.

2 Review and Analysis of the JCL-scheme

A review and analysis of the JCL-scheme is given in this section.
2.1 The JCL-scheme

The JCL-scheme consists of five phases: parameter generation, registration, pre-computation, log-in, and the password-changing phase. Due to space limitation, if the readers want to understand the JCL-scheme deeply, please refer to [4].

2.2 Security Analysis of the Juang et al. Scheme

The system may be compromised by extracting information from the smart card in order to falsify server authentication. Specifically, in the case of known \( ID_i \) and \( CI_i \) (these messages are stored on the smart card), the attacker will attempt to solve \( V_i = h(ID_i, s, C_i) \). The attacker can seek out the secret server key \( s \) using offline attack. After the secret value \( s \) is known, the attacker can freely tamper with the internal value of \( b_i \), compromising the security of the entire system.

3 The Proposed Scheme

We improve on JCL-scheme and propose an enhanced password-authentication key agreement scheme in this paper. This scheme not only maintains all the benefits of the JCL-scheme but also can enhance the security of the server when the smart card contents are disclosed. Our proposed scheme also consists of the same four phases: parameter generation, registration, pre-computation and log-in.

(i). Parameter Generation Phase:

1. The server selects three numbers: a larger prime number \( P \) and \( a \in Z_p \) and \( b \in Z_p \) must satisfy \( 4a^2 + 27b^2 (mod P) \neq 0 \), and \( E_P: y^2 = x^3 + ax + b \).
2. The server generates a point \( G \) from order \( n \), and satisfies \( O = n \times G \).
3. The server selects \( x_i \) as the private key, and the public key is \( P_{S_i} = (x_i \times G) \).
4. The server publishes the parameters \( (P_{S}, P, E_P, G, n) \).

(ii). Registration Phase:

The user can use the smart card to send identification information for the server to authenticate.

Step 1 The smart card chooses \( b \) and calculates \( T_1 = h(PW || b^{-1}) \). Then the smart card sends \( (ID_i, h(PW || b^{-1}), T_1) \) to the server.

Step 2 The server chooses \( S_2 \) and computes \( T_2 = T_1 \times T_1 \times ^2, V_i = h(ID_i, T_1, C_i) \) and \( b_i = E_v(h(PW || b) || T_2 || ID_i || C_i || h(ID_i || C_i || h(PW || b))) \).

Step 3 The user receives \( (ID_i, C_i, b_i, V_i) \) and then stores these parameters and \( b \) into the smart card.

(iii). Pre-computation Phase:

The smart card chooses a random number \( r \) and calculates \( e = (r \times G) \) and \( c = (r \times P_{S}) = r \times x \times G \). Then \( e, c \) is stored in card memory for use in the log-in phase.

(iv). Log-in Phase:

The user \( i \) wants to login to the server and must use his own smart card and password.

Step 1 After calculating \( E_v(e) \), the smart card sends \( E_v(e) \) and \( b_i \) to the server.

Step 2 The server obtains \( (T_2 || ID_i || C_i || h(PW || b)) \), \( T_i = T_2 \times S_2 \) and \( V_i = h(ID_i, T_i, C_i) \).

Then, the server chooses \( u \) and computes \( c = (e \times x) = (r \times x \times G) \), \( M_s = h(c || u || V_i) \),
Step 3 The smart card calculates and checks $M_s$. If $M_s$ is true, the smart card calculates $M_U = h(h(PW_i||b)||T_1||c||u)$ and $S_k = h(V_i,c,u)$.

Step 4 Obtain a session key $S_k = h(V_i,c,u)$ when $M_U$ is true.

4 Security Analysis and Comparison

The following table compares the properties of the proposed scheme and previous schemes. Where C1: low communication and computation cost; C2: users can choose the passwords; C3: no time-synchronization problem; C4: mutual authentication; C5: identity protection; C6: session key agreement; C7: preventing offline dictionary attack against the smart card information.

<table>
<thead>
<tr>
<th></th>
<th>Hwang &amp; Li scheme</th>
<th>Juang scheme</th>
<th>Fan et al. scheme</th>
<th>Sun scheme</th>
<th>Chien et al. scheme</th>
<th>Juang et al. scheme</th>
<th>Our scheme</th>
</tr>
</thead>
<tbody>
<tr>
<td>C1</td>
<td>X</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
</tr>
<tr>
<td>C2</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>C3</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>C4</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>C5</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>C6</td>
<td>X</td>
<td>O</td>
<td>O</td>
<td>X</td>
<td>O</td>
<td>O</td>
<td>O</td>
</tr>
<tr>
<td>C7</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

5 Conclusion

In our scheme, even if the attacker holds the user’s card, and mounts an offline attack to obtain the server key, it will not result in risk to the entire system. We use Juang et al.’s mechanism to revoke cards and ensure the privacy of the user. Possession of a smart card does not allow knowledge of the second secret key in the server, so the attacker cannot break the security of the system.

Acknowledgment: This work was supported by NSC 100-2221-E-224-016.

References