Security Enhanced Anonymous User Authenticated Key Agreement Scheme Using Smart Card

Jaewook Jung, Donghoon Lee, Hakjun Lee, and Dongho Won

Abstract—Nowadays, the password-based remote user authentication mechanism using smart card is one of the simplest and convenient authentication ways to ensure secure communications over the public network environments. Recently, Liu et al. proposed an efficient and secure smart card based password authentication scheme. However, we find that Liu et al.’s scheme is vulnerable to the off-line password guessing attack and user impersonation attack. Furthermore, it also cannot provide user anonymity. In this paper, we cryptanalyze Liu et al.’s scheme and propose a security enhanced user authentication scheme to overcome the aforementioned problems. Especially, in order to preserve the user anonymity and prevent the guessing attack, we use the dynamic identity technique. The analysis shows that the proposed scheme is more secure and efficient than other related authentication schemes.

Index Terms—Authentication, off-line password guessing attack, smart card, user anonymity.

1. Introduction

With the rapid development of the Internet service and electronic commerce technology, many people rely on computer networks to exchange information, access resource, and process data in wireless networks now. Such public wireless networks may be intruded by malicious attackers and other unauthorized users. To ensure the secure environment, the password-based user authentication technique is one of the most widely adopted mechanisms to deal with the secret data over the public channels.

Since Lamport\textsuperscript{[1]} first proposed a user authentication protocol in 1981, numerous user authentication schemes have been proposed\textsuperscript{[2]-[9]} afterwards. In 2009, Xu \textit{et al}.\textsuperscript{[2]} proposed a smart-card-based password authentication scheme. They claimed that the scheme can resist various types of attacks even if the information stored in the smart card is revealed. However, in 2010, Song\textsuperscript{[3]} proved that Xu \textit{et al}.’s scheme\textsuperscript{[2]} cannot be secure against an impersonation attack, and then Song\textsuperscript{[3]} proposed an improved scheme. In the same year, Sood \textit{et al}.\textsuperscript{[4]} also found that Xu \textit{et al}.’s scheme\textsuperscript{[2]} cannot resist the off-line guessing attack and forgery attack, and then presented an enhanced scheme. Unfortunately, in 2013, Chen \textit{et al}.\textsuperscript{[5]} demonstrated that Song’s scheme\textsuperscript{[3]} is vulnerable to stolen smart card attack. Chen \textit{et al}.\textsuperscript{[5]} also proved that Sood \textit{et al}.’s scheme\textsuperscript{[4]} does not provide mutual authentication, which means that a legitimate user has no way to verify the validity of the server. Then Chen \textit{et al}.\textsuperscript{[6]} proposed a robust smart-card-based remote user password authentication scheme. However, in 2013, Li \textit{et al}.\textsuperscript{[5]} pointed out that Chen \textit{et al}.’s scheme\textsuperscript{[5]} cannot ensure the perfect forward secrecy and detect the wrong password in login phase. Besides that, the password change of Chen \textit{et al}.’s scheme\textsuperscript{[5]} is inefficient since the user has to communicate with the server to update his/her password. Then Li \textit{et al}.\textsuperscript{[5]} proposed an enhanced user authentication scheme.

Recently, Liu \textit{et al}.\textsuperscript{[7]} pointed out that Li \textit{et al}.’s scheme\textsuperscript{[5]} is insecure against the man-in-the-middle attack and insider attack. To address the weaknesses in the Li \textit{et al}.’s scheme\textsuperscript{[5]}, Liu \textit{et al}. proposed an improved smart card based password authentication scheme\textsuperscript{[7]}. However, after careful analysis, we find that Liu \textit{et al}.’s scheme is vulnerable to off-line password guessing attack and user impersonation attack as well as it fails to preserve user anonymity in login phase. In order to eliminate all the above problems existed in Liu \textit{et al}.’s scheme, a security enhanced anonymous user authenticated key agreement scheme is proposed.

The remainder of the paper is organized as follows: Section 2 describes a review of Liu \textit{et al}.’s scheme. Section 3 points out the weaknesses of Liu \textit{et al}.’s scheme. The proposed scheme and security analysis of the proposed scheme are presented in Sections 4 and 5, respectively. Lastly, Section 6 concludes this paper.

2. Review of Liu \textit{et al}.’s Scheme

This section describes Liu \textit{et al}.’s authentication scheme\textsuperscript{[7]} which involves four phases: Registration, login, authentication, and password change. For convenience, the notations used throughout this paper are summarized in Table 1.

2.1 Registration Phase

Step 1. The user $U_i$ selects his/her ID$_i$ and PW$_i$ and generates random number $r$. Then $U_i$ computes $h(r||PW_i)$ and
Table 1: Notations

<table>
<thead>
<tr>
<th>Notations</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$U_i$, $S$</td>
<td>The user and server</td>
</tr>
<tr>
<td>ID, $PW_i$</td>
<td>The identity and password of the user</td>
</tr>
<tr>
<td>$x, y$</td>
<td>The secret key of the server</td>
</tr>
<tr>
<td>$T_c, T_i'$</td>
<td>Time-stamp of the user and the server</td>
</tr>
<tr>
<td>$r, a$</td>
<td>The random numbers created by the server</td>
</tr>
<tr>
<td>$\Delta T$</td>
<td>The maximum of transmission delay time</td>
</tr>
<tr>
<td>$h()$</td>
<td>One-way hash function</td>
</tr>
<tr>
<td>$\oplus$</td>
<td>XOR operation</td>
</tr>
<tr>
<td>$sk$</td>
<td>Session key shared between $U$ and $S$</td>
</tr>
<tr>
<td>$\beta'$</td>
<td>The random number created by the server</td>
</tr>
</tbody>
</table>

The smart card computes $A_i = h(ID_i \oplus x)[h(x), B_i = A_i \oplus h(r)[PW_i], and C_i = h(A_i||[ID_i||h(r)[PW_i]])$. The smart card stores $\{B_i, C_i, h()\}$ into a smart card and issues this smart card to the user $U_i$ through a secure channel.

Step 3. The user $U_i$ stores the random number $r$ into the card. Finally, the smart card contains $\{B_i, C_i, h()\}$.

2.2 Login Phase

Step 1. The user $U_i$ inserts his/her smart card into a card reader and inputs ID and PW. The smart card computes $A_i' = B_i \oplus h(r)[PW_i]$ and $C_i' = h(A_i||[ID_i||h(r)[PW_i]])$, then compares $C_i'$ with the stored value $C_i$. If this condition is hold, the smart card acknowledges the legitimacy of $U_i$ and proceeds with the next steps. Otherwise, it terminates this phase.

Step 2. The smart card generates a random number $a$, computes $D_i = h(ID_i \oplus a)$ and $E_i = A_i \oplus a \oplus r$. Then the server $S$ sends the authentication message $\{D_i, E_i, T_i\}$ to the server $S$.

2.3 Authentication Phase

Step 1. The server $S$ checks the validity of timestamp $|T_i' - T_i| \leq \Delta T$ and computes $A_i = h(ID_i \oplus x)[h(x), \alpha' = E_i \oplus A_i \oplus T_i, D_i' = h(ID_i \oplus \alpha')$, then compares $D_i'$ with the received value $D_i$. If this condition is hold, the server acknowledges the legitimacy of $U_i$ and proceeds with the next step. Otherwise, this phase is terminated.

Step 2. The server $S$ generates a random number $\beta$, computes $F_i = h(ID_i \oplus \beta)$ and $G_i = A_i \oplus \beta \oplus T_i$. Then the server $S$ sends the authentication message $\{F_i, G_i, T_i\}$ to $U_i$.

Step 3. The user $U_i$ checks the validity of timestamp $|T_i' - T_i| \leq \Delta T$ and computes $\beta' = A_i' \oplus G_i \oplus T_i, F_i' = h(ID_i \oplus \beta')$, then compares $F_i'$ with the received value $F_i$. If this condition is hold, the $U_i$ acknowledges the legitimacy of $S$, and proceeds with the next step. Otherwise, it terminates this phase.

Step 4. Finally, the user $U_i$ computes a session key $sk = h(\alpha' || \beta' || h(A_i \oplus ID_i))$ and the server $S$ also computes the same shared session key $sk = h(\alpha' || \beta || h(A_i \oplus ID_i))$.

2.4 Password Change Phase

Step 1. The $U_i$ inserts his/her smart card into a card reader and inputs ID and password PW.

Step 2. The smart card computes $A_i' = B_i \oplus h(r)[PW'_i], C_i' = h(A_i'||[ID_i||h(r)[PW'_i]])$, then compares $C_i'$ with the stored value $C_i$. If it is hold, $U_i$ selects a new password $PW''_i$. Otherwise, this phase is terminated.

Step 3. The smart card computes $B_i'' = A_i' \oplus h(r)[PW''_i]$ and $C_i'' = h(A_i''||[ID_i||h(r)[PW''_i]])$. Finally, the smart card replaces $(B_i, C_i)$ with $(B''_i, C''_i)$ respectively.

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

In this section, the weaknesses of Liu et al.’s scheme are demonstrated. We find that Liu et al.’s scheme cannot resist the off-line password guessing attack and user impersonation attack as well as it fails to preserve user anonymity. The details of these weaknesses are described as follows.

3.1 Failure to Preserve User Anonymity

User anonymity is a highly desirable property for user authentication scheme, as the leakage of user’s identity may allow an unauthorized entity to track the user’s login record and behavior pattern. However, in Liu et al.’s scheme, user’s identity ID is in plaintext form in the login request $\{ID_i, D_i, E_i, T_i\}$. Using an eavesdropping attack, the attacker can maliciously monitor the public channels and also identify some of the valuable information in messages transmitted over these public channels. In this manner, an attacker can eavesdrop on login messages to collect the plaintext identities without difficulty. For this reason, user anonymity cannot be preserved in Liu et al.’s scheme.

3.2 Off-Line Password Guessing Attack

In Liu et al.’s scheme, the attacker can obtain the information $\{B_i, C_i, h()\}$ in the smart card after physically monitoring power consumption and intercept login request message $\{ID_i, D_i, E_i, T_i\}$. Then the off-line password guessing attack can be done by performing the following steps:

Step 1. The attacker extracts the stored parameters $\{B_i, C_i, h()\}$ from the stolen smart card by using the power consumption attack.

Step 2. The attacker obtains the exact user’s identity ID by executing the steps discussed in subsection 3.1.

Step 3. The attacker selects a password candidate PW'$_i$.

Step 4. By using the obtained user’s identity ID, the attacker computes $C'_i = h(B_i \oplus h(r)[PW'_i])||[ID_i||h(r)[PW'_i]]$. Then, the attacker repeats above steps from step 3 to step 4 until the computed result $C'_i$ equals the stored $C_i$.

If they are equal, PW'$_i$ = PW$_i$, this means that the attacker has successfully obtained the user’s password PW$_i$ by off-line password guessing attack.

3.3 User Impersonation Attack

In this subsection, we demonstrate that an attacker can successfully login to the server $S$ by using the stolen smart card of a user $U_i$. The steps are as follows:
4. Proposed Scheme

In this section, we propose a security enhanced authentication and key agreement scheme to overcome the security weaknesses in Liu et al.’s scheme\(^7\). The proposed scheme also consists of four phases: Registration, login, authentication, and password change. The notations in the scheme are summarized in Table 1. Fig. 1 provides an illustration of login and authentication phases of the proposed scheme.

4.1 Registration Phase

Step 1. The user \(U_i\) selects his/her ID and PW, and generates a random number \(r\). Then \(U_i\) computes \(h(r)\) and sends a registration request \([ID, h(r)\|PW]\) to the server \(S\) through a secure channel.

Step 2. The server \(S\) computes \(A_i = h(x_i)\), \(B_i = h(ID_i\|h(r)\|PW_i)\), and \(C_i = h(h(r)\|PW_i)\|A_i\). The server \(S\) stores \([B_i, C_i, h(\cdot)\) into a smart card and issues this smart card to the user \(U_i\) through a secure channel.

Step 3. The user \(U_i\) stores the random number \(r\) into the card. Finally, the smart card contains \([B_i, C_i, h(\cdot), r]\).

4.2 Login Phase

Step 1. The user \(U_i\) inserts his/her smart card into a card reader and inputs ID, and PW. The smart card computes \(A_i' = h(ID_i\|h(r)\|PW_i)\) \& \(B_i\), \(C_i' = h(h(r)\|PW_i)\|A_i')\) then compares \(C_i'\) with the stored value \(C_i\). If this condition is hold, the smart card acknowledges the legitimacy of the \(U_i\), and proceeds with the next steps. Otherwise, it terminates this phase.

Step 2. The smart card generates a random number \(\alpha\) and computes \(D_i = ID_i \oplus \alpha\), \(E_i = A_i \oplus \alpha\), and \(F_i = h(ID_i\|A_i\|T_i)\). Then the server \(S\) sends the login request message \([D_i, E_i, F_i, T_i]\) to the server \(S\).

4.3 Authentication Phase

Step 1. The server \(S\) checks the validity of timestamp \([T_i' - T_i] \leq \Delta T\) and computes \(\alpha'E_i = E_i \oplus h(x_i)\|y\). \(D_i' = h(ID_i\|A_i'\|T_i)\), then compares \(F_i'\) with the received value \(F_i\). If this condition is hold, the procedure goes to the next steps. Otherwise, this phase is terminated.

Step 2. The server \(S\) generates a random number \(\beta\), and computes \(G_i = h(ID_i\|\beta)\) and \(H_i = h(x_i)\|\beta\|T_i\). Then the server \(S\) sends the authentication message \([G_i, H_i, T_i]\) to \(U_i\).

Step 3. The user \(U_i\) checks the validity of timestamp \([T_i' - T_i] \leq \Delta T\) and computes \(\beta'E_i = E_i \oplus H_i\|\beta\|T_i\), and \(G_i' = h(ID_i\|\beta')\), then compares \(G_i'\) with the received value \(G_i\). If this condition is hold, \(U_i\) acknowledges the legitimacy of the \(S\), and proceeds with the next step. Otherwise, it terminates this phase.

Step 4. Finally, the user \(U_i\) computes a session key \(sk = h(\alpha'\|\beta'|h(A_i'\|ID_i))\) and the server \(S\) also computes the same shared session key \(sk = h(\alpha'\|\beta'|h(h(x_i)\|ID_i')\).}

4.4 Password Change Phase

Step 1. The user \(U_i\) inserts his/her smart card into a card reader, inputs ID, and password PW, 

\[
\text{Fig. 1. Login and authentication phase of the proposed scheme.}
\]
5. Security Analysis of Proposed Scheme

In this section, we will analyze the proposed scheme in terms of security. Table 2 shows the security comparisons of the proposed scheme and other related schemes. The detail descriptions are as follows.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>User anonymity</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Mutual authentication</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Off-line password guessing attack</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Insider attack</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>User impersonation attack</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Replay attack</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

5.1 Preserve User Anonymity

Suppose that the attacker has intercepted the user $U_i$’s login request $\{D_i, E_i, F_i, T_i\}$. However, it is not feasible to derive $ID_i$ from the login request because the login request includes $D_i$ instead of $ID_i$. Therefore, the use of $D_i$ will ensure any information related to the user identity could not be acquired by the attacker.

5.2 Provide Mutual Authentication

In the scheme, the server $S$ can authenticate the user by checking whether the login request $\{D_i, E_i, F_i, T_i\}$ is correct. Also, the user $U_i$ can authenticate the server $S$ by checking whether the authentication message $\{F_i, G_i, T_i\}$ is correct.

5.3 Resistance to Off-Line Password Guessing Attack

To successfully carry out a password guessing attack in the proposed scheme, the attacker has to know the user’s ID. However, it is impossible for the attacker to obtain the user’s identity ID in the proposed scheme. Thus, the proposed scheme is secure against the off-line password guessing attack.

5.4 Resistance to Insider Attack

In the proposed scheme, the user $U_i$ sends the password information to the server $S$ in the form of $h(r||PW_i)$ instead of the form $PW_i$. Accordingly, the inside attacker is unable to acquire the user’s password $PW_i$.

5.5 Resistance to User Impersonation Attack

If an attacker tries to impersonate a legal user $U_i$ in order to cheat the server $S$, the attacker needs to modify $\{D_i, E_i, F_i, T_i\}$ to start a new session. In order to change these values, the attacker has to guess the secret key $x$. However, the probability of successfully guessing $x$ is negligible.

5.6 Resistance to Replay Attack

An attacker can intercept data packets and try to resend it to server in order to launch the replay attack. However, the login request message of the proposed scheme includes a current timestamp, i.e., $T_i$ of $\{D_i, E_i, F_i, T_i\}$. Hence, the proposed scheme can withstand against the replay attack.

6. Conclusions

We have proposed an enhanced user authentication scheme in order to remedy the security weaknesses of Liu et al.’s scheme. The proposed scheme achieves the mutual authentication and the user anonymity. In addition, the proposed scheme can withstand the password guessing attack, user impersonation attack, and insider attack even if the attacker obtains the user’s smart card. The security of the proposed scheme has been analyzed and the result shows that the scheme is more secure than other related schemes.

References


Jaewook Jung received the B.S. degree from Korea Aerospace University, Gyeonggi-do in 2010 and the M.S. degree from Sungkyunkwan University, Gyeonggi-do in 2012, both in electrical and computer engineering. He is currently pursuing the Ph.D. degree with the Department of Computer Engineering, Sungkyunkwan University. His research interests include cryptography, forensic, authentication protocol, and mobile security.

Donghoon Lee received the M.S. degree in information security engineering from Sungkyunkwan University in 2011. He is currently pursing the Ph.D. degree with the Department of Computer Engineering, Sungkyunkwan University. He worked as a security developer with Egloo Security and Nexon company from 2010 to 2013. His research interests include software security, malware detection, cryptography, and network security.

Hakjun Lee received the B.S. degree in software engineering from Korea National University of Transportation, Seoul in 2015. He is currently pursing the M.S. degree with the Department of Computer Engineering, Sungkyunkwan University. His research interests include cryptography, authentication protocol, and mobile payment.

Dongho Won received the B.S., M.S., and Ph.D. degrees from Sungkyunkwan University, all in electronic engineering. After working with Electronics and Telecommunication Research Institute for two years, he joined Sungkyunkwan University, where he is currently a leader professor with the Department of Computer Engineering. He also serves as the President of Korea Institute of Information Security and Cryptography. His research interests include cryptology and information security.