A user friendly remote authentication scheme with smart cards against impersonation attacks

Chien-Lung Hsu

Department of Information Management, Chang Gung University, 259, Wen-Hwa 1st Road, Kwei-Shan, Tao-Yuan 333, Taiwan, ROC

Abstract

In 2000, Sun proposed an efficient remote user authentication scheme using smart cards without requiring a password table. However, the password of a user is an un-human lengthy password instead of a human memorized password, since it is determined by the system. Recently, Wu and Chieu proposed a user friendly remote authentication scheme with smart cards to achieve the user friendliness that users can freely choose and change their human memorized passwords. This article, however, will show that Wu and Chieu’s scheme is vulnerable to two impersonation attacks. We further propose an improvement to withstand the impersonation attacks and achieve Wu and Chieu’s claimed security requirements.

Keywords: Authentication; Password; Smart card; Impersonation attack; Cryptanalysis

E-mail addresses: clhsu@mail.cgu.edu.tw, clhsu_journal@yahoo.com.tw
1. Introduction

In 1981, Lamport [1] proposed a remote password authentication scheme to authenticate the legitimacy of remote users over an insecure channel. However, his scheme must keep a password table for verifying the legitimacy of a login user. There are three drawbacks inherent in Lamport’s scheme [1] as follows. (i) It suffers from the risk of a tampered password table. (ii) It requires additional costs and efforts to protect and maintain the password table. (iii) When the number of users joined the system is extremely large, the password table will be greatly expanded and the task of managing the password table will become increasingly complicated. To eliminate above drawbacks, Hwang and Li [2] proposed a new remote user authentication scheme using smart cards. Hwang and Li’s scheme [2] not only requires no password table but also withstands the replay attack. Later, Sun [3] proposed an efficient remote user authentication scheme using smart cards to improve the efficiency of Hwang and Li’s scheme [2]. However, the password of a user is an un-human lengthy password instead of a human memorized password, since it is determined by the system.

Recently, Wu and Chieu [4] proposed a user friendly remote authentication scheme without using a password table to permit users to freely choose and change the preferred passwords. Wu and Chieu’s scheme [4] not only achieves the user authentication, but also eliminates the drawback of Sun’s scheme [3].

In this paper, however, we will show that Wu and Chieu’s scheme [4] is vulnerable to two impersonation attacks. In the first proposed attack, any attacker can arbitrarily forge a valid login message for gaining access right without being detected. In the second proposed attack, an attacker can first intercept one valid login message sent by a legal user and then masquerade as the legal user by forging a valid login message. Hence, Wu and Chieu’s scheme [4] violates the claimed security requirements. Finally, we proposed an improvement to withstand the proposed attacks and achieve Wu and Chieu’s claimed security requirements.

In Section 2, we will briefly review Wu and Chieu’s scheme [4]. In Section 3, we will demonstrate the impersonation attacks on Wu and Chieu’s scheme [4]. In Section 4, we will present an improvement to withstand the proposed attacks. Finally, we give conclusions in Section 5.

2. Review of Wu and Chieu’s user authentication scheme

Wu and Chieu’s user authentication scheme [4] is divided into three phases: the registration, the login, and the authentication phases. In the registration phase, each new user submits his identifier and his chosen password to the server for registration. The authentication server AS will issue a smart card containing some secret information to the registering user. In the login phase, a remote user attaches his smart card to the input device and enters his identifier and password.
The smart card will create a valid login message and send it to AS for gaining the access right. In the authentication phase, AS checks the validity of the login message sent by the user and determines whether the user is authorized to gain the access right. These three phases are described as follows.

2.1. Registration phase

Let \( p \) and \( g \) be public system parameters, where \( p \) is a large prime and \( g \) is a primitive element in \( \text{GF}(p) \). Let \( h \) be a collision resistant one-way hash function \([5,6]\), where the hashed value of the concatenation of messages \( m_1 \) and \( m_2 \) is denoted as \( h(m_1, m_2) \). In this phase, a new user \( U_i \) submits his identifier \( ID_i \) and his chosen password \( PW_i \) to AS via a secure manner. On receiving \( \{ID_i, PW_i\} \) sent from the user \( U_i \), the server AS performs the following Steps:

1. Compute \( A_i = h(ID_i, x) \), where \( x \) is the secret key owned and maintained only by the authentication server AS.
2. Compute
   \[
   B_i = g^{A_i h(PW_i)} \mod p. \tag{1}
   \]
3. Issue a smart card containing the information \( \{ID_i, A_i, B_i, h(\cdot), p, g\} \) to the user \( U_i \).

2.2. Login phase

If the user \( U_i \) wants to login the system for gaining the access right, he attaches his smart card to the card reader. After the user \( U_i \) keys in his identifier \( ID_i \) and password \( PW_i \), the smart card performs the following steps:

1. Compute
   \[
   B_i' = g^{A_i h(PW_i)} \mod p, \tag{2}
   \]
   \[
   C_i = h(T \oplus B_i), \tag{3}
   \]
   where \( T \) is the current date and time of the input device and the symbol “\( \oplus \)” is the bit-wise exclusive-or operation for two bit-string.
2. Send the login message \( \{ID_i, B_i', C_i, T\} \) to the server AS.

2.3. Authentication phase

Upon receiving the login message \( \{ID_i, B_i', C_i, T\} \) sent from \( U_i \), the authentication server AS performs the following steps:
1. Verify the format of the identifier $ID_i$. If $ID_i$ is invalid, then AS rejects $U_i$'s login request.

2. Check the validity of the time interval between $T$ and $T'$, where $T'$ is the time when AS received the login message. If $(T' - T) \geq \Delta T$, where $\Delta T$ denotes the expected valid time interval for transmission delay, then AS rejects $U_i$'s login request.

3. Compute
   \[ C_i^* = h(T \oplus B_i^*) \]
   and check if $C_i^*$ equals to the received $C_i$. If $C_i^* = C_i$, it implies that the password $PW_i^*$ is identical to $PW_i$. The server AS subsequently accepts the login request; otherwise AS rejects the login request (Fig. 1).

3. Impersonation attacks on Wu and Chieu’s scheme

   In the following, we will demonstrate that Wu and Chieu's authentication scheme [4] is vulnerable to the so-called impersonation attacks that an attacker $U_a$ without the knowledge of users’ passwords can masquerade as the legal user $U_i$. The proposed two impersonation attacks are given below.

3.1. Attack-1

   The attacker $U_a$ randomly chooses a number $B_i^* \in Z_p^*$ and computes $C_i = h(T \oplus B_i^*)$, where $T$ is the current date and time. After that, the attacker $U_a$ sends $\{ID_i, B_i^*, C_i, T\}$ to the AS for gaining the access right. Upon receiving $\{ID_i, B_i^*, C_i, T\}$ sent from $U_a$, the AS verifies the validity of $ID_i$ and $T$, and then computes $C_i^* = h(T \oplus B_i^*)$. The AS will accept the login message $\{ID_i, B_i^*, C_i, T\}$, since the computed $C_i^*$ equals to the received $C_i$. Hence, the attacker $U_a$ can successfully masquerade as the user $U_i$ and gain the access right without being detected. Illustration of the proposed attack-1 is depicted in Fig. 2. The proposed
Attack-1 can successfully attack on Wu and Chieu’s scheme [4], since AS cannot authenticate users. That is, AS does not use the secret information shared only known by the user \(U_i\) and the server AS to check the login message. If \(B_i^*\) in Eq. (4) is replaced by \(B_i = g^{A_i h(PW_i)} \mod p\) (where \(A_i = h(ID_i, x)\)) instead of \(B_i^*\) sent by the user \(U_i\) (or the attacker \(U_a\)), then Wu and Chieu’s scheme can withstand the proposed Attack-1. However, AS cannot compute \(B_i = g^{A_i h(PW_i)} \mod p\) without maintaining a password table containing the password \(PW_i\). If AS maintains a password table to compute \(B_i\) for withstanding this attack, Wu and Chieu’s scheme will violate the claimed security requirements.

3.2. Attack-2

Consider the scenario that the attacker \(U_a\) intercepts one valid login message generated by \(U_i\) and then attempts to masquerade as the legal user \(U_i\) by forging a valid login message. From Eqs. (1) and (2), it can be seen that \(B_i^* = g^{A_i h(PW_i)} = g^{A_i h(PW_i)} = B_i \mod p\) provided that \(\{ID_i, B_i^*, C_i, T\}\) is verified and accepted by the server AS. Once \(U_a\) intercepts such a valid login message \(\{ID_i, B_i^*, C_i, T\}\), he can use \(B_i^*\) (i.e., \(B_i^* = B_i\)) to masquerade as the user \(U_i\) to login the system by sending \(\{ID_i, B_i^*, \tilde{C}_i, \tilde{T}\}\) to AS, where

\[
\tilde{C}_i = h(\tilde{T} \oplus B_i^*)
\]

and \(\tilde{T}\) is the current date and time. The login message \(\{ID_i, B_i^*, \tilde{C}_i, \tilde{T}\}\) will pass the user authentication of Wu and Chieu’s scheme [4] due to the fact that \(C_i^* = h(\tilde{T} \oplus B_i^*) = \tilde{C}_i\) according to Eqs. (4) and (5). Hence, the attacker \(U_a\) can successfully masquerade as \(U_i\) to gain the access right without being detected. Illustration of the proposed Attack-2 is depicted in Fig. 3. The proposed Attack-2 can successfully attack on Wu and Chieu’s scheme [4], since the secret information \(B_i\) shared between the user \(U_i\) and the server AS is leaked to the attackers. That is, if the login message \(\{ID_i, B_i^*, C_i, T\}\) sent from, \(U_i\) to AS is verified, anyone can be convinced that \(B_i^* = B_i\) according to Eqs. (1) and (2). Anyone with the knowledge of \(B_i\) is able to construct a valid login message and masquerade as the legal user, \(U_i\) for gaining the access right. To withstand

![Fig. 2. Illustration of the proposed Attack-1.](image-url)
the proposed Attack-2, it must exclude the information $B_i^*$ (or $B_i$) from the login message.

4. The proposed scheme

In the following, we will present an improvement to withstand the proposed impersonation attacks and achieve the user friendly remote authentication without maintaining a password table. The improvement also consists three phases as those of Wu and Chieu’s scheme [4]. Descriptions of these phases are given below.

4.1. Registration phase

Let $p$ be a large prime, $g$ a primitive element in $\text{GF}(p)$, and $h$ a collision resistant one-way hash function [5,6]. In this phase, a new user $U_i$ submits his identifier $ID_i$ and his chosen password $PW_i$ to AS via a secure manner. On receiving $\{ID_i, PW_i\}$ sent from the user $U_i$, the server AS performs the following steps:

1. Compute $A_i = h(ID_i, x)$, where $x$ is the secret key owned and maintained only by the authentication server AS.
2. Compute
   \[ B_i = g^{A_i h(PW_i)^{-1}} \mod p. \]  \hspace{1cm} (6)
3. Issue a smart card containing the information $\{ID_i, B_i, h(\cdot), p, g\}$ to the user $U_i$.

4.2. Login phase

If the user $U_i$ wants to login the authentication server AS for gaining the access right, he attaches his smart card to the card reader and keys in his identifier $ID_i$ and password $PW_i^*$. The smart card computes
\[ C_i^* = B_i^{h(PW_i^*)} \mod p, \]  
\[ D_i = h(T \oplus C_i^*), \]

where \( T \) is the current date and time of the card reader. Finally, the smart card sends the login message \( \{ID_i, D_i, T\} \) to the server AS.

### 4.3. Authentication phase

Upon receiving the login request \( \{ID_i, D_i, T\} \) sent from \( U_i \), the authentication server AS performs the following steps:

1. Verify the format of the identifier \( ID_i \). If \( ID_i \) is invalid, then AS rejects \( U_i \)'s login request.
2. Check the validity of the time interval between \( T \) and \( T' \), where \( T' \) is the timestamp when AS received the login request. If \( (T' - T) \geq \Delta T \) \((\Delta T \) denotes the expected valid time interval for transmission delay), then AS rejects \( U_i \)'s login request.
3. Compute
   \[ C_i = g^{h(ID_i, x)} \mod p. \quad \text{(9)} \]
   \[ D_i^* = h(T \oplus C_i). \quad \text{(10)} \]

Then, AS checks if \( D_i^* \) equals to the received \( D_i \). If \( D_i^* = D_i \), the server AS subsequently accepts the login request; otherwise AS rejects the login request (Fig. 4).

The proposed improvement can also achieve the user friendliness that users can freely choose and change their human memorized passwords. When an authorized user \( U_i \) wants to change his password, he can submit his smart card
and new chosen password $PW'_i$ to the system via a secure channel. The system first computes the new $B'_i$ as $B'_i = g^{h(ID_i, x)h(PW'_i)^{-1}} \mod p$ and then replaces the original $B_i$ with the new $B'_i$ in $U_i$’s smart card. After that, the user $U_i$ can use the new password $PW'_i$ to login the system.

The security analysis of the proposed improvement is similar to that of Wu and Chieu’s scheme, the reader is encouraged to refer to [4]. Here, we only discuss the pointed out weaknesses against the proposed improvement.

The Proposed Attack-1 Analysis. Recall the scenario of the proposed Attack-1 that the attacker attempts to masquerade as the user $U_i$ by choosing a random number $C_i \in Z_p^*$, computing $D_i$ by Eq. (8), and sending $\{ID_i, D_i, T\}$ to the server AS. From Eqs. (9) and (10), the login message $\{ID_i, D_i, T\}$ will fail to pass the user authentication due to the fact that $C_i \neq C_i (= g^{h(ID_i, x)} \mod p)$ and $D_i \neq D'_i (= h(T \oplus C_i))$. Hence, the proposed improvement is secure against the proposed Attack-1.

The Proposed Attack-2 Analysis. From Eqs. (6) and (7), it can be seen that $C_i = B_i^{h(PW_i)} = g^{A_i} = g^{h(ID_i, x)(\mod p)}$, which is regarded as the secret information shared between the user and the server AS. Without the knowledge of $(g^{A_i} \mod p)$, the attacker cannot generate a valid login message. If an attacker attempts to derive $g^{A_i} \mod p$ from the intercepted login message $D_i = h(T \oplus C_i) = h(T \oplus (g^{A_i} \mod p))$, he will face the intractability of reversing the one-way hash function. Hence, the proposed improvement is secure against the proposed Attack-2 under the one-way hash function assumption.

We evaluate the comparison of computational complexities of the proposed scheme and Wu and Chieu’s scheme [4] in Table 1. The time for performing a bit-wise exclusive-or computation is ignored, since it is negligible as compared to the other computing time. From Table 1, we can see that the proposed improvement requires less the computational complexities for a smart card to generate a valid login message. The comparison of communication costs and storage of the proposed scheme and Wu and Chieu’s scheme [4] is listed in Table 2. From Table 2, the communication costs and the storage of the proposed scheme is smaller than those of Wu and Chieu’s scheme [4]. Therefore, the performance of a smart card of our improvement outperforms Wu and

<table>
<thead>
<tr>
<th>Table 1</th>
<th>The comparison of computational complexities</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The proposed scheme</td>
</tr>
<tr>
<td>Registration phase</td>
<td>$2T_H + T_M + T_E + T_I$</td>
</tr>
<tr>
<td>Login phase</td>
<td>$2T_H + T_E$</td>
</tr>
<tr>
<td>Authentication phase</td>
<td>$2T_H + T_E$</td>
</tr>
</tbody>
</table>

Notes: $T_H$ is the time for performing a one-way hash function $h$; $T_M$ is the time for performing a modular multiplication computation; $T_E$ is the time for performing a modular exponentiation computation; $T_I$ is the time for performing a modular inverse computation.
Chieu’s scheme in terms of the storage, the communication costs, and the computational complexities.

5. Conclusions

We have shown that Wu and Chieu’s scheme [4] is vulnerable to the proposed two impersonation attacks and is not able to achieve the security requirements as they claimed. Furthermore, we have proposed an improvement to withstand the impersonation attacks. The proposed scheme not only achieves the user authentication without maintaining a password table, but also achieves the user friendliness. The performance of a smart card of the proposed improvement is more efficient than that of Wu and Chieu’s scheme in terms of the storage, the communication costs, and the computational complexities.

References