An Improved Low Computation Cost User Authentication Scheme for Mobile Communication

Chia-Yin Lee*, Chu-Hsing Lin**, and Chin-Chen Chang*

*Department of Computer Science and Information Engineering, National Chung Cheng University, 621 Chiayi, Taiwan 
{licy, ccc}@cs.ccu.edu.tw

**Department of Computer Science and Information Engineering, Tunghai University, 407 Taichung, Taiwan 
chlin@mail.thu.edu.tw

Abstract

Most of existing user authentication schemes require high computation cost of exponentiation operations for the purpose of security. However, it is not suitable for mobile devices. In this article, we propose a low computation cost user authentication scheme for mobile communication. Our scheme uses only one-way hash functions and smart cards and can be implemented efficiently. The proposed scheme not only resolves the weakness appeared in existing methods but also suits for mobile communication.

1. Introduction

User authentication is an important topic for communication security and there are many schemes existed for the purpose in the literatures. In 1981, Lamport [1] proposed a user authentication scheme for communication in insecure channel. His scheme could resist against replaying attacks; however, it needs a password table for the verification step. Later, several ID-based authentication schemes [2]-[5] have been proposed to avoid this kind of drawback. One of the characteristics that passwords are assigned to the registered users by the server is a common disadvantage in most of the existing user authentication schemes. In 2003, Wu and Chieu [6] proposed a user authentication scheme with smart cards to improve the disadvantage. Their scheme lets users be able to choose and change their passwords freely. However, Yang and Wang [7] have pointed out the scheme suffers from the forgery attack in 2004. Besides, their scheme requires costly exponentiation computation and thus it is not suitable for mobile devices [8], [9] with low computation capability. In this article, we propose an improved low cost user authentication scheme for mobile devices, shown in Figure 1, which can solve these problems and spend low computational cost.

2. A Review of Related Work

In 2003, Wu and Chieu proposed a scheme with smart cards for user authentication. Their scheme consists of three phases: the registration phase, the login phase, and the authentication phase.

Figure 1. User authentication architecture
In the first phase, the user $U_i$ submits his/her identity $ID_i$ and a chosen password $PW_i$ to the server for registration. On receiving the registration request, the server performs the following steps:

1) Compute $A_i = h(ID_i \parallel x)$, where $x$ is the server's secret key and $h(\cdot)$ is a collision resistant one-way hash function.
2) Compute $B_i^* = g^{A_i \cdot PW_i} \mod p$, where $g$ is a public primitive element in $GF(p)$ and $p$ is a large prime number.
3) The server issues each user $U_i$ a smart card, which contains $U_i$'s personal information $\{ID_i, A_i, B_i, h(\cdot), p, g\}$.

In the login phase, the user $U_i$ inserts his/her smart card into the card reader and keys in his/her identity $ID_i$ with the corresponding password $PW_i^*$, and then the smart card performs the following operations:

1) Compute $B_i^* = g^{A_i \cdot PW_i^*} \mod p$, and $C_i = h(T \oplus B_i) \mod p$ (where $T$ is the timestamp which includes current date and time).
2) Send the message $m = \{ID_i, B_i^*, C_i, T\}$ to the server.

In the authentication phase, the server authenticates the user with the following steps:

1) Test the validity of $ID_i$, if the format of $ID_i$ is not correct, the server rejects the login request.
2) Test the timestamp $T$ with $T^\prime$ (current date and time). If the time interval $(T^\prime - T) \geq \Delta T$, where $\Delta T$ denotes the expected valid time interval for transmission delay, then the server rejects the login request.
3) Compute $C_i^* = h(T \oplus B_i^*)$ and check whether $C_i^* = C_i$ or not. If they are equal, it means that the password $PW_i^*$ is equal to $PW_i$. Then the system accepts the login request. Otherwise, it rejects the login request.

The security of their scheme was based on the discrete logarithm problem (DLP) and the one-way hash function. Now, we demonstrate how the possible attacks can be succeeded. And thus an intruder can pass the authentication phase by a modified login-message to masquerade a legal user.

2.1 The Forgery Attack

An intruder can collect the login message $m = \{ID_i, B_i^*, C_i, T\}$, from that he (or she) can obtain the correct value of $B_i$ since $B_i^* = B_i$ for a legal user in the login phase. After that, the intruder can forge the verifiable value $C_i^*$ by computing $C_i^* = h(T \oplus B_i^*)$, where $T^\prime$ is the update timestamp. Therefore, the intruder can send the message $m^* = \{ID_i, B_i^*, C_i^*, T\}$ to the server. We can see that, with this $m^*$, he (or she) will pass through the verification phase and then masquerade successfully the legal user $U_i$.

From the above analysis, we know that Wu-Chieu scheme suffers from the forgery attack. Besides, their scheme uses two times of exponential computation in the registration phase and the login phase. It means that the system might not be efficient for mobile devices with low computation capability. Due to the above reasons, we propose a more efficient scheme, which is not only against the possible attacks but also can reduce the computation cost. We describe the proposed scheme in the next section.

3. The Proposed User Authentication Scheme

We propose an improved low computation cost user authentication scheme for mobile communication. We show it in Figure 2. The proposed scheme is also divided into three phases: the registration phase, the login phase, and the authentication phase. Besides, the notations of the scheme are the same as those in Wu-Chieu scheme.

In the registration phase, the user $U_i$ submits his/her identity $ID_i$ and a chosen password $PW_i$ to the server. According to the submitted values $ID_i$ and $PW_i$, the server performs the following steps:

1) Use the server's secret key $x$ to obtain $A_i$ by computing $A_i = h(ID_i \parallel x)$, where $h(\cdot)$ is a one-way hash function with an output sized 512 bits, e.g. SHA-512 [10].
2) Compute $B_i = h(A_i \parallel h(PW_i))$.
3) The server issues a smart card with the secure
Figure 2. The proposed authentication scheme

The proposed scheme can resist against not only all the attacks described in Wu-Chieu scheme but also the possible attacks by modifying the login message \( m \). We will analyze it as follows.

1) It is hard to derive the server’s secret key \( x \) from the hash value of \( A_1 = h(ID_i \parallel x) \), by using the security characteristic of the one-way hash function (e.g. SHA-512).

2) It is also difficult to guess a legal user’s password \( PW_i \) from the equation \( B_i^* = h(A_1 \parallel h(PW_i')) \), the reason is the same as the above statement 1).

3) Replaying attacks (An intruder might replay an old login message \( m = \{ID_i, C_2, C_1, T\} \) to the server) cannot work because it will make Step1 of the authentication phase fail.

4) No one can compute a valid \( C_i = h(T \oplus B_i) \), because it must be derived from \( PW_i \) and \( A_1 \). However, \( PW_i \) and \( A_1 \) cannot be obtained if the server’s secret key \( x \) is unknown.

5) An intruder might collect the legal login message \( m = \{ID_i, C_2, C_1, T\} \) and try to modify it into \( m_0 = \{ID_i, C_2, C_1, T_0\} \) (where \( T_0 \) is the current date and time). In this case, he (or she) has to compute a correct value of \( C_{i_0} = h(T_0 \oplus B_i) \). However, the parameter \( B_i = B_i^* \) cannot be obtained from \( C_2 \) because the value of \( A_1 \) is unknown.

6) An intruder might forge the message \( m_0 = \{ID_i, C_{2r}, C_{1r}, T_0\} \), where \( C_{2r} = 0 \). In this case, due to the parameter \( B_i^* = (C_{2r} \oplus A_1) = A_1 \), he (or she) has to compute the verifiable value \( C_{1r} = h(T_0 \oplus B_i^*) = h(T_0 \oplus A_1) \). However, he (or she) cannot obtain the correct value of \( C_{1r} \) because the parameter \( A_1 \) is unknown.

7) Since \( B_i^* \) and \( A_1 \) are the message digests of SHA-512 (i.e. 512 bits in length), the probability of guessing correct values of \( B_i^* \) and \( A_1 \) from \( C_2 \) is less than \( \frac{1}{2^{512}} \times \frac{1}{2^{512}} \). It is difficult to obtain the correct values of \( B_i^* \) and \( A_1 \) by just knowing \( C_2 \).
Table 1. Efficiency comparison of our scheme and Wu-Chieu’s

<table>
<thead>
<tr>
<th>Phases</th>
<th>Wu-Chieu scheme</th>
<th>Our scheme</th>
</tr>
</thead>
<tbody>
<tr>
<td>Registration</td>
<td>$1T_{\text{EXP}} + 1T_{\text{MUL}} + 2T_{\text{H}}$</td>
<td>$3T_{\text{H}}$</td>
</tr>
<tr>
<td>Login</td>
<td>$1T_{\text{EXP}} + 1T_{\text{MUL}} + 2T_{\text{H}} + 1T_{\text{XOR}}$</td>
<td>$3T_{\text{H}} + 2T_{\text{XOR}}$</td>
</tr>
<tr>
<td>Authentication</td>
<td>$1T_{\text{H}} + 1T_{\text{XOR}}$</td>
<td>$2T_{\text{H}} + 2T_{\text{XOR}}$</td>
</tr>
<tr>
<td>Total cost</td>
<td>$2T_{\text{EXP}} + 2T_{\text{MUL}} + 5T_{\text{H}} + 2T_{\text{XOR}}$</td>
<td>$8T_{\text{H}} + 4T_{\text{XOR}}$</td>
</tr>
</tbody>
</table>

5. Cost Comparisons

In this section, we compare the computational cost of the three phases (registration, login and authentication) for our scheme with Wu-Chieu’s. We define some notations as follow.

$T_{\text{EXP}}$: the modular exponential computation.
$T_{\text{H}}$: the one-way hash function $h()$.
$T_{\text{MUL}}$: the multiplication computation.
$T_{\text{XOR}}$: the exclusive-or ($\oplus$).

The comparative results are shown in Table 1. We know that a modular exponential computation is much more time consuming than a one-way hash function. Besides, the exclusive-or ($\oplus$) operations can be performed very efficiently. From Table 1, our proposed scheme requires only one-way hash functions and exclusive-or operations that can be implemented efficiently.

6. Conclusions

In this article, we have shown the drawbacks of the Wu-Chieu scheme and then propose a novel scheme to solve the problems. We also analyze the security and computation cost required for the proposed scheme. From Table 1, we can see that our scheme is much more efficient than Wu-Chieu scheme since it uses only low-cost functions and thus can be executed very efficiently. In a word, our scheme can be easily implemented on a mobile device with low computation capability.

Reference