An improved and secure smart card-based authentication scheme

Sandeep K. Sood
Department of Computer Science and Engineering,
G.N.D.U. Regional Campus,
Gurdaspur, India
E-mail: san1198@gmail.com
E-mail: san1198@yahoo.co.in

Abstract: Kim and Chung (2009) found that Yoon and Yoo’s scheme (2005) easily reveals a user’s password and is susceptible to masquerading user attack, masquerading server attack and stolen verifier attack. Therefore, Kim and Chung proposed a new remote user authentication scheme. They claimed that the proposed scheme resolves all aforementioned security flaws, while keeping the merits of Yoon and Yoo’s scheme. However, we found that Kim and Chung’s scheme is susceptible to masquerading user attack, masquerading server attack, offline dictionary attack using stolen smart card and parallel session attack. This paper improves Kim and Chung’s scheme that resolves the aforementioned security flaws, while keeping the merits of Kim and Chung’s scheme. The security of the proposed protocol depends upon two security parameters which makes difficult for an attacker to launch attacks on the proposed scheme. Therefore, the attacker can not get any meaningful authentication information from eavesdropping.

Keywords: cryptography; password; authentication protocol; smart card; hash function.


Biographical notes: Sandeep K. Sood received his MTech in Computer Science and Engineering from the Guru Jambheshwar University Hisar (Haryana), India in 1999. He has completed his PhD in the Department of Electronics and Computer Engineering at the Indian Institute of Technology Roorkee, India. His research interests include authentication protocols, computer and network security, cryptography and computer networks.

1 Introduction

Smart cards have been widely used in many e-commerce applications and network security protocols due to their low cost, portability, efficiency and the cryptographic properties. Smart card stores some sensitive data corresponding to the user that assist in user authentication. The user (card holder) inserts his smart card into a card reader machine and submits his identity and password. Then smart card and card reader machine
perform some cryptographic operations using submitted arguments and the data stored inside the memory of smart card to verify the authenticity of the user.

Lamport (1981) proposed a password-based authentication scheme that authenticates remote users over an insecure communication channel. Lamport’s scheme removes the problems of password table disclosure and communication eavesdropping. Since then, a number of remote user authentication schemes have been proposed to improve security, efficiency and cost. Hwang and Li (2000) found that Lamport’s scheme is susceptible to risk of password table modification and the cost of protecting and maintaining the password table is large. Therefore, they proposed a cost effective remote user authentication scheme using smart card that is free from the mentioned risk. Hwang and Li’s scheme can withstand replay attack and also authenticate the remote users without maintaining a password table. Sun (2000) proposed an efficient smart card-based remote user authentication scheme to improve the efficiency of Hwang and Li’s scheme.

Chien et al. (2002) found that Sun’s scheme only achieves unilateral user authentication so that only authentication server authenticates the legitimacy of the remote user. Chien et al. also proposed a remote user authentication scheme and claimed that their scheme provides mutual authentication, requires no verification table, password selection freedom and uses only few hash operations. Hsu (2004) demonstrated that Chien et al.’s scheme is susceptible to parallel session attack so that the intruder without knowing the user’s password can masquerade as the legitimate user by creating a valid login message from the eavesdropped communication between the authentication server and the user. Lee et al. (2004a, 2004b) improved Chien et al.’s scheme by eliminating the parallel session attack. Yoon and Yoo (2005) found that Lee et al.’s schemes are susceptible to masquerading server attack and proposed an improvement on Lee et al.’s schemes. Kim and Chung (2009) found that Yoon and Yoo’s scheme easily reveals a user’s password and is susceptible to masquerading user attack, masquerading server attack and stolen verifier attack. Therefore, Kim and Chung proposed a new remote user authentication scheme. They claimed that the proposed scheme resolves all aforementioned security flaws, while keeping the merits of Yoon and Yoo’s scheme. However, we found that Kim and Chung’s scheme is susceptible to masquerading server attack, masquerading user authentication scheme and offline dictionary attack using stolen smart card. This scheme is also found to be susceptible to parallel session attack. This paper improves Kim and Chung’s scheme that resolves the aforementioned problems, while keeping the merits of Kim and Chung’s scheme.

Hsiang and Shih (2009) proposed a smart card-based remote user authentication scheme. Their scheme is found to be vulnerable to impersonation attack and offline guessing attack. This scheme also delays the checking of legitimacy of the user to authentication phase. Xu et al. (2009) also proposed an exponential-based smart card authentication scheme and claimed that it can resist the various feasible attacks. Sood et al. (2010) found that Xu et al.’s scheme is also found to be vulnerable to forgery attack and proposed an improved scheme.

The masquerading and dictionary attacks are the major concerns in smart card-based authentication protocols. A solution is required in which it is not possible for the attacker to launch different attacks on smart card-based authentication protocol. The aim of this paper is to provide a secure smart card-based password authentication solution for the user authentication. The main feature of the proposed protocol is that the legitimate client can easily login on to the server. The security of the proposed protocol depends upon two security parameters which makes difficult for an attacker to launch attacks on the
An improved and secure smart card-based authentication scheme

Moreover, the user and the server agree on the common session key. Afterwards, all the subsequent messages between the user and the server are encrypted with this session key. Therefore, either the user or the server can retrieve the original message because both of them know the common session key.

The rest of this paper is organised as follows. In Section 2, a brief review of Kim and Chung’s scheme is given. Section 3 describes the cryptanalysis of Kim and Chung’s scheme. In Section 4, the improved scheme is proposed. The security analysis of the proposed improved scheme is presented in Section 5. The comparison of cost and functionality of the proposed scheme with the other related schemes is shown in Section 6. Section 7 concludes the paper.

2 Review of Kim and Chung’s scheme

In this section, we examine a simple remote user authentication scheme proposed by Kim and Chung (2009). Kim and Chung’s scheme consists of four phases viz. registration phase, login phase, verification phase and password change phase as summarised in Figure 1. The notations used in this section are listed in Table 1.

Figure 1 Kim and Chung’s scheme

Table 1 Notations

<table>
<thead>
<tr>
<th>$U_i$</th>
<th>$i^{th}$ user</th>
</tr>
</thead>
<tbody>
<tr>
<td>$S$</td>
<td>Server</td>
</tr>
<tr>
<td>$ID_i$</td>
<td>Unique identification of user $U_i$</td>
</tr>
<tr>
<td>$P_i$</td>
<td>Password of user $U_i$</td>
</tr>
<tr>
<td>$N$</td>
<td>Random number unique to user</td>
</tr>
<tr>
<td>$x$</td>
<td>Master secret of registration server $S$</td>
</tr>
<tr>
<td>$H(\ )$</td>
<td>One-way hash function</td>
</tr>
<tr>
<td>$\oplus$</td>
<td>XOR operation</td>
</tr>
<tr>
<td>$</td>
<td>$</td>
</tr>
</tbody>
</table>
2.1 Registration phase

A user $U_i$ has to submit his identity $ID_i$ and password $P_i$ to the server $S$ for registration over a secure communication channel. The server $S$ computes $K_1 = H(ID_i \oplus x) \oplus N$, $K_2 = H(ID_i \oplus x \oplus N) \oplus H(P_i \oplus H(P_i))$ and $R = K_1 \oplus H(P_i)$, where $N$ is a unique random number corresponding to the user $U_i$. Then, the server $S$ issues the smart card containing secret parameters ($K_1$, $K_2$, $R$, $H(\cdot)$) to the user $U_i$ through a secure communication channel.

2.2 Login phase

The user $U_i$ inserts his smart card into a card reader to login on to the server $S$ and submits his identity $ID_i$ and password $P_i$. The smart card computes $K_1^* = R \oplus H(P_i^*)$ and verifies the calculated value of $K_1^*$ with the stored value of $K_1$ in its memory. If both values match, the legitimacy of the user is assured and smart card proceeds to the next step. Otherwise, the login request from the user $U_i$ is rejected. Afterwards, smart card computes $C_1 = K_2 \oplus H(P_i \oplus H(P_i))$, $C_2 = H(C_1 \oplus T_1)$, where $T_1$ is current date and time of the input device and sends the login request message $(ID_i^*, T_1, K_1, C_2)$ to the service provider server $S$.

2.3 Verification phase

After receiving the login request from the user $U_i$, the service provider server $S$ verifies the received value of $ID_i^*$ with stored value of $ID_i$ in its database. Then, the server $S$ checks the validity of timestamp $T_1$ by checking $(T - T_1) \leq \delta T$ where $T$ is current date and time of the server $S$ and $\delta T$ is permissible time interval for a transmission delay. Afterwards, the server $S$ computes $N' = K_1 \oplus H(ID_i \oplus x)$, $C_2^* = H(H(ID_i \oplus x \oplus N') \oplus T_1)$ and checks if $C_2^*$ is equal to the received value of $C_2$. If they are not equal, the server $S$ rejects the login request and terminates this session. Otherwise, the server $S$ acquires the current time stamp $T_2$, computes $C_3 = H(H(ID_i \oplus x \oplus N') \oplus C_2 \oplus T_2)$ and sends the message $(C_3, T_2)$ back to the smart card of user $U_i$. On receiving the message $(C_3, T_2)$, smart card checks the validity of timestamp $T_2$ by checking $(T'' - T_2) \leq \delta T$, where $T''$ denotes the client’s smart card current timestamp. Then, the client’s smart card computes $C_3^* = H(C_1 \oplus C_2 \oplus T_2)$ and compares the computed value of $C_3^*$ with received value of $C_3$. This equivalency authenticates the legitimacy of the service provider server $S$ and the login request is accepted else the connection is interrupted.

2.4 Password change phase

A user $U_i$ inserts his smart card into a card reader and enters his identity $ID_i^*$ and password $P_i^*$ corresponding to his smart card. The smart card computes $K_1^* = R \oplus H(P_i^*)$ and compares the calculated value of $K_1^*$ with the stored value of $K_1$ in
An improved and secure smart card-based authentication scheme

its memory to verifies the legitimacy of the user \( U_i \). Once the authenticity of the card holder is verified then the user \( U_i \) can instruct the smart card to change his password. Afterwards, the smart card asks the card holder to resubmit a new password \( P^\text{new}_i \) and smart card computes

\[
R^* = K_1 \oplus H\left(P^\text{new}_i\right) \quad \text{and} \quad K^*_2 = K_2 \oplus H\left(P \oplus H\left(P_i\right)\right) \oplus H\left(P^\text{new}_i \oplus H\left(P^\text{new}_i\right)\right).
\]

Finally, the value of \( R \) and \( K_2 \) stored in the smart card is updated with \( R^* \) and \( K^*_2 \).

3 Cryptanalysis of Kim and Chung’s scheme

Kim and Chung (2009) claimed that their protocol can resist various known attacks. However, this protocol is found to be flawed for masquerading user attack, masquerading server attack and offline dictionary attack using stolen smart card. This scheme is also found to be susceptible to parallel session attack. The proposed scheme in Section 4 provides security based on two secure parameters \( (C_1, C_2) \), while the security of Kim and Chung’s scheme depends on only one secure parameter \( C_1 \). Therefore, Kim and Chung’s scheme is susceptible to the following attacks.

3.1 Masquerading user attack

The attacker can intercept a valid login request message \( (ID^*_i, T_i, K_1, C_2) \) of the user \( U_i \) from the public communication channel. Now, he can launch offline dictionary attack on \( C_2 = H(C_1 \oplus T) \) to know the value of \( C_1 \), which is always same corresponding to the user \( U_i \). After getting the value of \( C_1 \), the attacker can frame and send the fabricated valid login request message \( (ID^*_i, T_0, K_1, C^*_2) \) to the service provider server \( S \) without knowing the password \( P_i \) of the user \( U_i \), where \( T_0 \) is a current timestamp and \( C^*_2 = H(C_1 \oplus T_0) \). Therefore, the attacker can successfully make a valid login request by masquerading as a legitimate user \( U_i \) to the service provider server \( S \).

3.2 Masquerading server attack

The attacker can intercept a valid login request message \( (ID^*_i, T_i, K_1, C_2) \) of the user \( U_i \) from the public communication channel. Now, he can launch offline dictionary attack on \( C_2 = H(C_1 \oplus T) \) to know the value of \( C_1 \). After getting the value of \( C_1 \), the attacker can frame and send the fabricated valid response message \( (C_3, T_2) \) back to the smart card of user \( U_i \), where \( T_2 \) is a current timestamp and \( C_3 = H(C_1 \oplus C_2 \oplus T_2) \). Therefore, the attacker can successfully masquerade as the service provider server \( S \) to the legitimate user \( U_i \).

3.3 Offline dictionary attack

A user \( U_i \) may lose his smart card, which is found by an attacker or an attacker steals the user’s smart card. An attacker can extract the stored values through some technique like
by monitoring their power consumption and reverse engineering techniques as pointed out by Kocher et al. (1999) and Messerges et al. (2002). He can extract \( K_1 = H(ID_i \oplus x) \oplus N \), \( K_2 = H(ID_i \oplus x \oplus N) \oplus H(P_i \oplus H(P_i)) \) and \( R = K_1 \oplus H(P_i) \) from the memory of smart card because smart card contains \((K_1, K_2, R, H())\). Then, an attacker can find out the password information \( H(P_i) \) of user as \( H(P_i) = R \oplus K_1 \). Now, an attacker can guess different values of \( P_i \) and checks its correctness by verifying it with the actual value of \( H(P_i) \).

### 3.4 Parallel session attack

The attacker can masquerade as a legitimate user by creating a valid login message from the eavesdropped communication between the user and the server without knowing the user’s password. He can intercept the login request message \((ID_i^*, T_1, K_1, C_2)\) from the user \( U_i \) to the server \( S \). Then, he starts a new session with the server \( S \) by sending a login request by replaying the login request message \((ID_i^*, T_1, K_1, C_2)\) with in the valid time frame window. After receiving the login request, the server \( S \) check the validity of \( ID_i^* \) and the timestamp \( T_1 \) by checking \((T' - T_1) < \delta T\), where \( T' \) denotes the server’s current timestamp. The server \( S \) computes \( N' = K_1 \oplus H(ID_i \oplus x) \), \( C_2^* = H(ID_i \oplus x \oplus N' \oplus T_1) \) and compares \( C_2^* \) with the received value of \( C_2 \) to check the legitimacy of the user \( U_i \). This equivalency authenticates the masquerading user and the attacker can successfully make a valid login request by masquerading as a legitimate user \( U_i \) to the service provider server \( S \).

### 4 Proposed scheme

In this section, we describe a new remote user authentication scheme which resolves the above security flaws of Kim and Chung’s scheme. The proposed protocol precludes the weaknesses of Kim and Chung’s scheme with improved security. Figure 2 shows the entire protocol structure of the new authentication scheme. Legitimate user \( U_i \) can easily login on to the service provider server using his smart card, identity and password. The notations used in this section are listed in Table 1. The proposed protocol consists of four phases viz. registration phase, login phase, verification and session key agreement phase and password change phase.

#### 4.1 Registration phase

A user \( U_i \) has to submit his identity \( ID_i \) and password \( P_i \) to the server \( S \) via a secure communication channel to register itself to the server \( S \).

**Step 1 \( U_i \rightarrow S: ID_i, P_i \)**

The server \( S \) computes the security parameters
An improved and secure smart card-based authentication scheme

\[ K_1 = H(ID \oplus x) \oplus N, \ K_2 = H(ID \oplus x \oplus N) \oplus H(P), \]
\[ K_3 = H(ID, x | N) \oplus H(ID, | P) \]
and \( R = K_1 \oplus H(ID, | P) \oplus H(P). \)

where \( N \) is a random number unique to the user \( U_i \). Then the server \( S \) issues the smart card containing security parameters \((K_1, K_2, K_3, R, H())\) to the user \( U_i \) through a secure communication channel.

**Step 2** \( S \rightarrow U_i: \) smart card

*Figure 2* Proposed improvement in Kim and Chung's scheme

<table>
<thead>
<tr>
<th>User ( U_i ) Knows</th>
<th>Smart Card Stores</th>
<th>Service Provider Server ( S ) Stores ( ID_1 ) &amp; Knows ( x )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( ID_1 ) and ( P_1 )</td>
<td>( K_1 = H(ID \oplus x) \oplus N )</td>
<td>Computes ( K_1 = H(ID \oplus x) \oplus N )</td>
</tr>
<tr>
<td>(Registration Phase)</td>
<td>( K_2 = H(ID, x \oplus N) \oplus H(P_1) )</td>
<td>( K_2 = H(ID, x \oplus N) \oplus H(P_1) )</td>
</tr>
<tr>
<td>Substitute ( ID_1 ) and ( P_1 )</td>
<td>( K_3 = H(ID, x</td>
<td>N) \oplus H(ID,</td>
</tr>
<tr>
<td>(Login Phase) Enter ( ID_1^<em>, P_1^</em> )</td>
<td>( R = K_1 \oplus H(ID,</td>
<td>P_1) \oplus H(P_1) )</td>
</tr>
</tbody>
</table>

\( K_1 = K_1^* \oplus R \oplus H(ID_2^* \oplus P_1^* \oplus H(P_1^*)) \)

Verifies \( K_1^* = K_1 \)

Computes \( C_1 = K_2 \oplus H(P_1^*) \)
\( C_2 = K_2 \oplus H(ID_1 | P_1) \)
\( C_3 = H(C_1 | T_1 | C_2) \)

\( ID_1^*, T_1, K_1, C_3 \)

Verifies \( (T^* \cdot T_2) \cdot C_3 \cdot T \)

Computes \( C_4 = H(C_2 | T_2 | C_1) \)

Verifies \( C_4 = C_4^* \)

Computes Session Key
\( S_k = H(C_1 | T_2 | C_2 | T_1) \)

**4.2 Login phase**

A user \( U_i \) inserts his smart card into a card reader to login on to the server \( S \) and submits his identity \( ID_1^* \) and password \( P_1^* \). The smart card computes
\( K_1^* = R \oplus H(ID_1^* | P_1^* \oplus H(P_1^*) \)
and verifies the calculated value of \( K_1^* \) with the stored value of \( K_1 \) in its memory to verifies the legitimacy of the user \( U_i \).
Step 1  Smart card checks  \( K_i^* = K_1 \)

After verification, smart card computes \( C_1 = K_2 \oplus H(P_i) \), \( C_2 = K_3 \oplus H(ID_i | P_i) \) and \( C_3 = H(C_1 | T_1 | C_2) \), where \( T_1 \) is current date and time of the input device. Then smart card sends the login request message \( (ID_i^*, T_1, K_1, C_3) \) to the service provider server \( S \).

Step 2  Smart card \( \rightarrow S \): \( ID_i^*, T_1, K_1, C_3 \)

4.3 Verification and session key agreement phase

After receiving the login request from the user \( U_i \), the service provider server \( S \) verifies the received value of \( ID_i^* \) with stored value of \( ID_i \) in its database. The server \( S \) checks the validity of timestamp \( T_1 \) by checking \( (T' - T_1) \leq \delta T \), where \( T' \) is current date and time of the server \( S \) and \( \delta T \) is permissible time interval for a transmission delay. Afterwards, the server \( S \) computes \( N^* = K_1 \oplus H(ID_i \oplus x) \), \( C'_1 = H(ID_i \oplus x \oplus N^*) \), \( C'_2 = H(ID_i \oplus x \oplus N^*) \), \( C'_3 = H(C'_1 | T_1 | C'_2) \) and checks if \( C'_3 \) is equal to the received value of \( C_3 \).

Step 1  Server \( S \) checks  \( C'_3 = C_3 \)

If they are not equal, the server \( S \) rejects the login request and terminates this session. Otherwise, the server \( S \) acquires the current time stamp \( T_2 \) and computes \( C_4 = H(C'_2 | T_2 | C'_1) \) and sends the message \( (C_4, T_2) \) back to the smart card of user \( U_i \).

Step 2  \( S \rightarrow \) smart card: \( C_4, T_2 \)

On receiving the message \( (C_4, T_2) \), the user \( U_i \)'s smart card checks the validity of timestamp \( T_2 \) by checking \( (T'' - T_2) \leq \delta T \) where \( T'' \) is current date and time of the server \( S \) and \( \delta T \) is permissible time interval for a transmission delay. Afterwards, the user \( U_i \)'s smart card computes \( C'_4 = H(C_2 | T_2 | C_1) \) and compares the computed value of \( C'_4 \) with the received value of \( C_4 \).

Step 3  Smart card checks  \( C'_4 = C_4 \)

This equivalency authenticates the legitimacy of the service provider server \( S \) and the login request is accepted else the connection is interrupted. Finally, the user \( U_i \) and the server \( S \) agree on the common session key as \( S_k = H(C_1 | T_2 | C_2 | T) \).

4.4 Password change phase

The user \( U_i \) can change his password without help of the server \( S \). The user \( U_i \) inserts his smart card into a card reader and enters his identity \( ID_i^* \) and password \( P_i^* \) corresponding to his smart card. Smart card computes \( K_i^* = R \oplus H(ID_i^* | P_i^*) \oplus H(P_i^*) \) and compares
the calculated value of $K'_1$ with the stored value of $K_1$ in its memory to verifies the legitimacy of the user $U_i$. Once the authenticity of the card holder is verified then the user $U_i$ can instruct the smart card to change his password. Afterwards, the smart card asks the card holder to resubmit a new password $P^\text{new}_i$ and then smart card computes

$$R^* = K_1 \oplus H\left(ID_i | P^\text{new}_i\right) \oplus H\left(P^\text{new}_i\right), K^*_2 = K_2 \oplus H\left(P^*_i\right) \oplus H\left(P^\text{new}_i\right)$$ and

$$K^*_3 = K_3 \oplus H\left(ID_i | P^*_i\right) \oplus H\left(ID_i | P^\text{new}_i\right).$$

Afterwards, smart card updates the values of $R^*$, $K^*_2$ and $K^*_3$ stored in its memory with $R^*$, $K^*_2$ and $K^*_3$. The proposed scheme checks the validity of identity $ID^*_i$ and password $P^*_i$ before updating the password of the user $U_i$. In Kim and Chung’s scheme, smart card verifies only the password $P^*_i$ of the user $U_i$ and updates the password without verifying the identity $ID^*_i$ of the user $U_i$.

5 Security analysis

Smart card is a memory card that uses an embedded micro-processor from smart card reader machine to perform required operations specified in the protocol. Kocher et al. and Messerges et al. pointed out that all existing smart cards can not prevent the information stored in them from being extracted such as by monitoring their power consumption. Some other reverse engineering techniques are also available for extracting information from smart cards. This means that once a smart card is stolen by an attacker, he can extract the information stored in it. A good password authentication scheme should provide protection from different possible attacks relevant to that protocol.

Masquerading user attack

In this type of attack, the attacker masquerades as a legitimate user and forges the authentication messages using the information obtained from the authentication scheme. The attacker can intercept a valid login request message $(ID^*_i, T_1, K_1, C_3)$ of the user $U_i$ from the public communication channel. The attacker has to guess the correct values of $C_1$ and $C_2$ at the same time to launch offline dictionary attack on $C_3 = H(C_1 | T_1 | C_2)$ because the attacker requires correct values of $C_1$ and $C_2$ to frame fabricated valid login request message $(ID^*_i, T_1, K_1, C_3)$. It is not possible to guess two parameters correctly at the same time in real polynomial time. Therefore, the proposed protocol is secure against masquerading user attack.

Masquerading server attack

The attacker can intercept a valid login request message $(ID^*_i, T_1, K_1, C_3)$ of the user $U_i$ from the public communication channel. Now the attacker has to guess the correct values of $C_1$ and $C_2$ at the same time to launch offline dictionary attack on $C_3 = H(C_1 | T_1 | C_2)$ because the attacker requires correct values of $C_1$ and $C_2$ to frame fabricated valid
response message \((C_4^i, T_2)\), where \(C_4^i = H(C_2 | T_2 | C_1)\). It is not possible to guess two parameters correctly at the same time in real polynomial time. Therefore, the proposed protocol is secure against masquerading server attack.

**Offline dictionary attack**

A user may lose his smart card, which is found by the attacker or the attacker steals the user’s smart card. The attacker can extract the stored values through some technique such as by monitoring their power consumption and reverse engineering techniques as pointed by Kocher et al. and Messerges et al. The attacker can extract \(K_1 = H(ID_i \oplus x \oplus N)\), \(K_2 = H(ID_i \oplus x \oplus N) \oplus H(P_i)\), \(K_3 = H(ID_i | x | N) \oplus H(ID_i | P_i)\) and \(R = K_1 \oplus H(ID_i | P_i) \oplus H(P_i)\) from the memory of smart card. Even after gathering this information, the attacker has to guess \(ID_i\) and \(P_i\) correctly at the same time. It is not possible to guess two parameters correctly at the same time in real polynomial time. Therefore, the proposed protocol is secure against offline dictionary attack.

**Parallel session attack**

In this type of attack, the attacker first listens to communication between the client and the server. After that, he initiates a parallel session to imitate the legitimate user to login on to the server by resending the captured messages transmitted between the client and the server within the valid time frame window. The attacker can masquerade as a legitimate user by replaying a login request message \((ID_i, T_i, K_1, C_3)\) within the valid time frame window but cannot compute the agreed session key \(S_k = H(C_1 | T_2 | C_2 | T_1)\) because the attacker does not know the values of \(C_1\) and \(C_2\). Therefore, the proposed protocol is secure against parallel session attack.

**Denial of service attack**

In this type of attack, the attacker updates password verification information on smart card to some arbitrary value so that the legitimate user cannot login successfully in subsequent login request to the server. In the proposed scheme, smart card checks the validity of the user’s identity \(ID_i\) and password \(P_i\) before password update procedure. Suppose the attacker has obtained the smart card of the legitimate user \(U_i\). The attacker can insert the smart card of user \(U_i\) into the card reader and has to guess the identity \(ID_i\) and password \(P_i\) correctly corresponding to the user \(U_i\). Since the smart card computes \(K_i^* = R \oplus H(ID_i | P_i) \oplus H(P_i)\) and compares the calculated value of \(K_i^*\) with the stored value of \(K_i\) in its memory to verify the legitimacy of the user \(U_i\) before the smart card accepts the password update request. It is not possible to guess identity \(ID_i\) and password \(P_i\) correctly at the same time in real polynomial time. Therefore, the proposed protocol is secure against denial of service attack.

**Man-in-the-middle attack**

In this type of attack, the attacker intercepts the messages sent between the client and the server and replay these intercepted messages with in the valid time frame window. The
An improved and secure smart card-based authentication scheme

In the proposed protocol, the attacker can intercept the login request message \((ID_i^*, T_1, K_1, C_1)\) from the user \(U_i\) to the server \(S\). Then he starts a new session with the server \(S\) by sending a login request by replaying the login request message \((ID_i^*, T_1, K_1, C_1)\) with in the valid time frame window. The attacker can authenticate itself to the server \(S\) as well as to the legitimate client but can not compute the session key \(S_k = H(C_1 | T_2 | C_2 | T_1)\) because the attacker does not know the values of \(C_1\) and \(C_2\). Therefore, the proposed protocol is secure against man-in-the-middle attack.

**Replay attack**

In this type of attack, the attacker first listens to communication between the client and the server and then tries to imitate the user to login on to the server by resending the captured messages transmitted between the client and the server. Replaying a message of one session into another session is useless because the user’s smart card and the server \(S\) uses current time stamp values as \(T_1\) and \(T_2\) in each new session, which make all the messages dynamic and valid for a small interval of time. Moreover, the attacker can not compute the agreed session key \(S_k = H(C_1 | T_2 | C_2 | T_1)\) because the attacker does not know the values of \(C_1\) and \(C_2\). Old messages can not be replayed successfully in any other session and hence the proposed protocol is secure against message replay attack.

**Leak of verifier attack**

In this type of attack, the attacker may have some techniques to steal verification table from the server. If the attacker steals the verification table from the server, he can use the stolen verifiers to impersonate a participant of the scheme. In the proposed protocol, the service provider server \(S\) knows secret \(x\) and only stores user identity \(ID_i\) in its database. The attacker does not have any technique to find the value of \(x\). In case verifier is stolen by breaking into smart card database, the attacker does not have sufficient information to calculate the user’s identity \(ID_i\) and password \(P_i\). Therefore, the proposed protocol is secure against leak of verifier attack.

**Server spoofing attack**

In server spoofing attack, an attacker can manipulate the sensitive data of the legitimate users by setting up fake servers. Malicious server can not generates the valid value of \(C_4 = H(C_1^* | T_2^* | C_1^*)\) meant for smart card because malicious server does not know the value of \(C_1^*\) and \(C_2^*\) corresponding to that user’s smart card. The proposed protocol provides mutual authentication between the client and the server. Therefore, the proposed protocol is secure against server spoofing attack.

**Malicious user attack**

A malicious privileged user \(U_i\) having his own smart card can gather information like \(K_1 = H(ID_i \oplus x) \oplus N, K_2 = H(ID_i \oplus x \oplus N) \oplus H(P_i), K_3 = H(ID_i | x | N) \oplus H(ID_i | P_i)\) and \(R = K_1 \oplus H(ID_i | P_i) \oplus H(P_i)\) from his smart card. This malicious user cannot extract the
value of $x$ because he does not know the value of $N$. Also the malicious user cannot generate smart card specific value of $C_3 = H(C_1 \mid T_1 \mid C_2)$ to masquerade as other legitimate user $U_i$ to the service provider server $S$ because the values of $C_1$ and $C_2$ is smart card specific. Therefore, the proposed protocol is secure against malicious user attack.

**Online dictionary attack**

In this type of attack, the attacker pretends to be legitimate client and attempts to login on to the server by guessing different words as password from a dictionary. In the proposed protocol, the attacker has to get the valid smart card of user $U_i$ and then has to guess the identity $ID_i$ and password $P_i$ corresponding to that user’s smart card. Even after getting the valid smart card by any mean, the attacker gets a very few chances (maximum of three) to guess the identity $ID_i$ and password $P_i$ because smart card gets locked after certain number of unsuccessful attempts. Moreover, it is not possible to guess identity $ID_i$ and password $P_i$ correctly at the same time in real polynomial time. Therefore, the proposed protocol is secure against online dictionary attack.

6 Cost and functionality analysis

An efficient authentication scheme must take communication and computation cost into consideration during user’s authentication. The cost comparison of the proposed protocol with the related smart card-based authentication schemes is summarised in Table 2.

<table>
<thead>
<tr>
<th>Proposed protocol</th>
<th>Kim-Chung</th>
<th>Yoon-Yoo</th>
<th>Lee et al.</th>
</tr>
</thead>
<tbody>
<tr>
<td>E1</td>
<td>512 bits</td>
<td>384 bits</td>
<td>256 bits</td>
</tr>
<tr>
<td>E2</td>
<td>6 * 128 bits</td>
<td>6 * 128 bits</td>
<td>5 * 128 bits</td>
</tr>
<tr>
<td>E3</td>
<td>$5T_H + 7T_X$</td>
<td>$4T_H + 6T_X$</td>
<td>$T_H + 4T_X$</td>
</tr>
<tr>
<td>E4</td>
<td>$5T_H + 4T_X$</td>
<td>$4T_H + 6T_X$</td>
<td>$2T_H + 4T_X$</td>
</tr>
<tr>
<td>E5</td>
<td>$6T_H + 3T_X$</td>
<td>$4T_H + 6T_X$</td>
<td>$2T_H + 5T_X$</td>
</tr>
<tr>
<td>Chein et al.</td>
<td>Hsiang-Shih</td>
<td>Xu et al.</td>
<td>Sood et al.</td>
</tr>
<tr>
<td>E1</td>
<td>128 bits</td>
<td>384 bits</td>
<td>512 bits</td>
</tr>
<tr>
<td>E2</td>
<td>5 * 128 bits</td>
<td>5 * 128 bits</td>
<td>8 * 128 bits</td>
</tr>
<tr>
<td>E3</td>
<td>$T_H + 2T_X$</td>
<td>$4T_H + 4T_X$</td>
<td>$T_E + 2T_H$</td>
</tr>
<tr>
<td>E4</td>
<td>$2T_H + 3T_X$</td>
<td>$4T_H + 4T_X$</td>
<td>$3T_E + 5T_H$</td>
</tr>
<tr>
<td>E5</td>
<td>$3T_H + 3T_X$</td>
<td>$4T_H + 3T_X$</td>
<td>$3T_E + 4T_H$</td>
</tr>
</tbody>
</table>

Notes: E1 memory needed in the smart card
E2 communication cost of the authentication
E3 computation cost of the registration
E4 computation cost of the user
E5 computation cost of the service provider server.
Assume that the identity ID, password P, secret keys x, timestamp values and output of secure one-way hash function are all 128-bit long. Let $T_E$, $T_H$ and $T_X$ denote the time complexity for exponential operation, hash function and XOR operation respectively. Typically, time complexity associated with these operations can be roughly expressed as $T_E >> T_H >> T_X$. In the proposed protocol, the parameters stored in the smart card are $K_1$, $K_2$, $K_3$, $R$ and the memory needed (E1) in the smart card is $512 (= 4 \times 128)$ bits. The communication cost of authentication (E2) includes the capacity of transmitting message involved in the authentication scheme. The capacity of transmitting message $\{ID', T_1, K_1, C_3\}$ and $\{C_4, T_2\}$ is $768 (= 6 \times 128)$ bits. The computation cost of registration (E3) is the total time of all the operations executed in the registration phase. The computation cost of registration is $5 T_H + 7 T_X$. The computation cost of the user (E4) and the service provider server (E5) is the time spent by the user and the service provider server during the process of authentication. Therefore, both the computation cost of the user and that of the service provider server are $5 T_H + 4 T_X$ and $6 T_H + 3 T_X$ respectively. The proposed protocol requires more computation than that of Kim and Chung’s scheme but it is highly secure as compared to the related schemes (Chien et al., 2002; Lee et al., 2004a, 2004b; Yoon and Yoo, 2005; Kim and Chung, 2009; Hsiang and Shih, 2009; Xu et al., 2009). The proposed protocol is free from masquerading user attack, masquerading server attack, offline dictionary attack and parallel session attack, while the latest scheme proposed by Kim and Chung (2009) suffers from these attacks. The functionality comparison of the proposed protocol with the related smart card-based authentication schemes is summarised in Table 3.

### Table 3  Functionality comparison among related smart card-based authentication schemes

<table>
<thead>
<tr>
<th>Proposed protocol</th>
<th>Kim-Chung</th>
<th>Yoon-Yoo</th>
<th>Lee et al.</th>
<th>Chein et al.</th>
<th>Hsiang-Shih</th>
<th>Xu et al.</th>
<th>Sood et al.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identity verification in login phase</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Session key agreement</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Masquerading user attack</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Masquerading server attack</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Offline dictionary attack</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Denial of service attack</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Parallel session attack</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Identity verification in login phase | No | No | No | Yes |
Session key agreement | No | No | Yes | Yes |
Masquerading user attack | Yes | Yes | Yes | No |
Masquerading server attack | Yes | Yes | Yes | No |
Offline dictionary attack | Yes | Yes | No | No |
Denial of service attack | Yes | No | No | No |
Parallel session attack | Yes | No | No | No |
7 Conclusions

Commercial network and e-commerce applications require secure and practical remote user authentication solutions. Smart card-based password authentication is one of the most convenient ways to provide multi-factor authentication for the communication between a client and a server by acquiring the smart card, knowing the identity and password. Yoon and Yoo (2005) proposed a remote user authentication scheme that provides mutual authentication, secret key forward secrecy and fast detection of wrong password. Kim and Chung (2009) found that Yoon and Yoo’s scheme easily reveals a user’s password and is susceptible to masquerading user attack, masquerading server attack and stolen verifier attack. Then Kim and Chung (2009) proposed a new remote user authentication scheme and claimed that the proposed scheme resolves all aforementioned security flaws, while keeping the merits of Yoon and Yoo’s scheme. However, we found that Kim and Chung’s scheme is also susceptible to masquerading user attack, masquerading server attack, offline dictionary attack and parallel session attack. In this paper, we improved Kim and Chung’s scheme that resolves the aforementioned security flaws, while keeping the merits of Kim and Chung’s scheme. The proposed protocol is simple and fast if the user possesses a valid smart card, a valid identity and correct password for its authentication. The proposed protocol is practical and efficient because only one way hash functions and XOR operations are used in its implementation. Security analysis proved that the proposed protocol is secure and practical.

References


