Security Improvement of Remote User Authentication Scheme based on Smart Cards

Young-Do Joo, Young-Hwa An

Abstract Recently Lin et al. [9] proposed a simple remote user authentication scheme using smart cards. But the proposed scheme has not satisfied security requirements which should be considered in the user authentication scheme using the password based smart card. In this paper, we show that Lin et al.'s scheme is insecure against off-line password guessing attack. In their scheme, any legal user's password may be derived from the password guessing when his/her smart card is stolen and the secret information is leaked from the smart card by an attacker. Accordingly, we demonstrate the vulnerability of their scheme and present an enhancement to resolve such security weakness. Our proposed scheme can withstand various possible attacks including password guessing attack. Furthermore, this improved scheme can provide mutual authentication to improve the security robustness. Performance evaluation shows that the proposed scheme is relatively more effective than Lin et al.'s scheme.

Key Words : Authentication, Smart Card, Password Guessing Attack, Replay Attack

I. Introduction

With the rapid growth of computer networks, the achievement of secrecy and authentication has become increasingly important. In untrustworthy public network, a user authentication which can prevent unauthorized network access is the most important part as far as security is concerned. A remote user authentication scheme allows a server to check the authenticity of a remote user through insecure channels like Internet. The identities of the communication parties must be verified before they start a new connection to make sure that no harm is done. A variety of password-based authentication schemes have been developed[1-11].
Since Lamport[1] proposed his remote authentication scheme in 1981, several schemes have been proposed to improve the security, the cost or the efficiency. One of the features of these schemes is that a verification table should be securely stored in the server. If the verification table is stolen by an attacker, the system will be partially or totally broken.

In 2006, Lin et al. proposed a new remote user authentication scheme[9] using smart card that can withstand many possible intrusions including a stolen-verifier attack, based on Lin-Shen-Hwang’s protocol[5]. In this paper, however, we show that Lin et al.’s scheme is vulnerable to the password guessing attack, and forgery attack/impersonation attack. In addition, Lin et al.’s scheme is insecure because the authentication server stores the user’s password verifier and authenticates only the user. To remedy these flaws, we propose an improvement of Lin et al.’s remote user authentication scheme whereby the user’s password verifier is not stored in the server side and mutual authentication between the server and the user is implemented to provide higher security.

The rest of this paper is organized as follows. We review and analyze Lin et al.’s scheme in section II. In section III, we present an improved protocol to enhance Lin et al.’s scheme. The security analysis and performance evaluations of our scheme is provided in section IV. Finally, brief conclusions are given in section V.

II. Review of Lin et al.’s Scheme

1. Lin et al.’s scheme

Lin et al.’s scheme is composed of two phases: registration phase and the authentication phase. The detailed procedures of each phase are described as follows. In their scheme, there are a server S and a set of users U. For readers’ understanding, the abbreviations and notations used through this article are summarized in Table 1.

| U_i  | user i               |
| ID_i | identity of the entity i |
| P_i  | password of the entity i |
| S    | authentication server |
| x    | secret key of S       |
| N_i, N_i' | random numbers of the entity i |
| h()  | one-way hash function |
| ||   | concatenation         |
| ⊕    | exclusive-or operation |

- Registration Phase

Suppose a new user, U_i wants to register with the server, S for accessing services.

(1) The user sends a message (ID_i,h(P_i||N_i)) to the server for registration through a secure channel.

(2) The server stores the message h(P_i||N_i) into the database after the identity of the user is verified. Then, the server calculates K by equation (1).

\[ K = h(x||ID_i) ⊕ h(P_i||N_i) \]  (1)

where x is a secret value and is maintained by the server.

And then the server, S issues the smart card written by the computed value of K to the user, U_i.

- Authentication Phase

To access a server, U_i inserts his/her smart card in to a login device and keys in the password, P_i.

(1) The user sends a message (ID_i,C_2,C_3) to the server for authentication. Here, C_2 and C_3 are calculated according to the following equations.

\[ C_1 = K ⊕ h(P_i||N_i) \]  (2)
\[ C_2 = h(K) ⊕ h(P_i||N_i') \]  (3)
\[ C_3 = h(C_1 ⊕ h(P_i||N_i')) \]  (4)

where N_i' is a new random nonce used against a replay attack.

(2) Upon receiving the login request (ID_i,C_2,C_3) from U_i, the server performs the following operations to identify the login user.

(i) First, checks the format of ID_i. If it does not pass
the test, then disconnect this connection.
(ii) Check the identity of the login user by verifying $C_2$. The server may derive $h(P||N')$ by XORing $h(h(x||ID_{i})\oplus h(P||N_{i}))$ with $C_2$.

Then, compute $C_3'$ as follows:

$$C_3'=h(x||ID_{i})\oplus h(P||N')$$

(5)

If $C_3$ equals $C_3'$, $U_i$ is authenticated and gains the right to access the server. Finally, update the stored verifier $h(P||N_{i})$ with $h(P||N'_{i})$ for the next login.

2. Security Analysis

To evaluate the security of smart card based user authentication, we assume that an attacker may possess the capabilities to thwart the security schemes.

(1) An attacker has total control over the communication channel between the users and the server in the login and authentication phases. That is, he may intercept, insert, delete, or modify any message across the communication procedures.

(2) An attacker may (i) either steal a user’s smart card and then extract valuable information from the smart card, (ii) or steal a user’s password, but can not commit both of (i) and (ii) at a time.

Obviously, if both of the user’s smart card and his password was stolen at the same time, then there is no way to prevent an attacker from impersonating a valid user. Therefore, a remote user authentication scheme should be secure if only one case out of (i) and (ii) is happening.

In this section, we will show that the Lin et al.’s scheme is vulnerable to the password guessing attack. As pointed out in references[12][13], all existing smart cards contain security weakness in that the secret values stored in it could be extracted by monitoring the power consumption, can find out $P_i$ by employing the off-line password guessing attack, in which each guess $P'_i$ for $P_i$ can be verified by the following procedures.

Step 1. The legal user, $U_i$ calculates $C_2$, $C_3$ for login to the authentication server as usual and send the login request message $(ID_i,C_2,C_3)$ to the authentication server.

Step 2. At that time, the attacker $U_a$ intercepts the login request message and gets the $C_2$, and $C_3$.

Step 3. Finally, $U_a$ can catch the user’s password by employing the off-line password guessing attack. The attacking scenario is as follows.

(1) The attacker $U_a$ guesses $P'_i$ as the user’s password $P_i$.

(2) And calculates $C_1'=K\oplus h(P'_i||N_i)$, $B'=C_2\oplus h(K)$, and $C_3'=h(C_1'\oplus B')$.

(3) And verifies the correctness of $P'_i$ by checking $C_3'=C_3$.

(4) Repeats steps above (1) through (3) until a correct password $P'_i$ is found. Finally, the attacker can devise the correct password, $P_i$.

Therefore, we emphasize that the Lin et al.’s remote user authentication scheme using smart card is vulnerable to the off-line password guessing attack. In their scheme, the attacker can successfully masquerade as the legitimate user with the user’s password and the smart card in hand.

III. Improvement of Lin et al.’s Scheme

In this section, we propose an enhancement of Lin et al.’s scheme which not only can withstand the off-line password guessing attack, but authenticate the user and the server each other.

Our scheme is divided into three phases: registration phase, login phase and authentication phase. The registration phase is illustrated in Fig. 1. The login
phase and the authentication phase are depicted in Fig. 2.

![Fig. 1. Registration Phase of the Proposed Scheme](image)

**Fig. 1. Registration Phase of the Proposed Scheme**

**Registration Phase**

Suppose a new user $U_i$ wants to register with the server $S$ for accessing services.

1. The user, $U_i$ calculates a verifier $h(PW_i)$ and sends it along with his/her identifier $ID_i$ to the server $S$. These private data must be sent over a secure channel.

2. $S$ calculates and writes $K_i$ into a smart card and issues it to $U_i$, by equations (6) and (7)

   \[
   X_i = h(ID_i, x) \tag{6}
   \]

   \[
   K_i = X_i \oplus h(PW_i) \tag{7}
   \]

   where $x$ is a secret key maintained by the server.

**Login Phase**

To access a server, $U_i$ inserts his/her smart card into the smart card reader and keys in his/her $ID_i$ and password $PW_i$. Then, the smart card performs the following operations.

1. The smart card chooses a random nonce $N_i$.
2. Calculates $X_i = K_i \oplus h(PW_i)$ and $C_i = X_i \oplus N_i$.
3. Calculates $V_i = h(ID_i, C_i, N_i)$ for authenticating the user to the server.
4. Then, $U_i$ sends a message $(ID_i, V_i, C_i)$ to $S$.

**Authentication Phase**

Upon receiving the login request message $(ID_i, V_i, C_i)$ from $U_i$, the server executes the following steps to identify the login user.

1. The authentication server checks the format of $ID_i$. If it does not pass the test, then disconnect this connection.
2. Then, the server calculates $N_i' = C_i \oplus X_i$ and $V_i' = h(ID_i, C_i, N_i')$.
3. Checks the equality: $V_i' = V_i$. If it holds, $U_i$ is authenticated and allowed to access the server.
4. Chooses a random nonce $N_s$ and calculate $C_s = X_i \oplus N_s$.
5. Calculates $V_s = h(ID_i, C_s, C_i, N_s)$ for authenticating the server to the user.
6. Then, sends a message $(V_s, C_s)$ to the user.

Upon receiving the message $(V_s, C_s)$ from the server $S$, the user’s smart card performs the following operations.

1. The user’s smart card calculates $N_s' = C_s \oplus X_i$ and $V_s' = h(ID_i, C_s, C_i, N_s')$.
2. Then, checks the equality: $V_s' = V_s$. If it holds, the server is authenticated and allowed to access the smart card.

IV. Security Analysis and Performance Evaluation

1. Security Analysis

The proposed scheme suggests an enhancement to Lin et al.’s scheme in order to eliminate the security risk described in the previous section. We examine the security robustness of our scheme to endure the
well-known attacks such as password guessing attacks, replay attacks and forgery attacks.

■ Password Guessing Attack
Assume that an attacker intercepts a login request \((ID, V_i, C_i)\) over a public network and \(K_i\) from the user’s smart card. However, the attacker cannot derive the password \(PW_i\) of the login user from \(V_i, C_i\) and \(K_i\). This is because the attacker does not know \(N_i\) and \(x\), where \(x\) is stored in private within the server.

■ Replay Attack
The user’s smart card updates the random nonce to resist the replay attack at each login. As \(U_i\) regenerates the random number \(N_i\) and the consequent computation of \(C_i\), the server’s response during the previous session cannot be replayed for any upcoming next session. That is, replaying the previous login request by the eavesdropper is infeasible due to the freshness of the random nonce.

■ Forgery Attack
An attacker \(U_a\) may impersonate the legitimate user \(U_i\) by forging a login request \((ID, V_a, C_a)\) and sending it to the server. The server will execute the authentication phase for identifying the login user. However, the forged login request \((ID, V_a, C_a)\) cannot pass, because the verifying equation does not hold \((V_a = V_{a'}\). Therefore, an attacker has no chance to login by launching an impersonation attack. Similarly, an attacker is also unable to masquerade the server to the user.

■ Security Comparison
The analysis of security properties of Lin et al.’s scheme and the proposed scheme is summarized in Table 2. In contrast to Lin et al.’s scheme, the proposed scheme is relatively more secure. In addition, the proposed scheme provides mutual authentication between the user and the server.

<table>
<thead>
<tr>
<th>Security Properties</th>
<th>Lin et al.’s Scheme</th>
<th>Proposed Scheme</th>
</tr>
</thead>
<tbody>
<tr>
<td>password-guessing attack</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>replay attack</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>forgery attack</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>mutual authentication</td>
<td>not supported</td>
<td>supported</td>
</tr>
</tbody>
</table>

2. Performance Evaluation
In this section, we evaluate the performance of the proposed scheme and Lin et al.’s scheme. Table 3 shows the computational complexities of both schemes. As you see, the proposed scheme is more efficient than Lin et al.’s scheme. In the login and authentication phase, our scheme requires only six THs and five TEs. This computation includes four THs and three TEs for the mutual authentication between the user and the server.

<table>
<thead>
<tr>
<th>Phase</th>
<th>Lin et al.’s Scheme</th>
<th>Proposed Scheme</th>
</tr>
</thead>
<tbody>
<tr>
<td>Registration</td>
<td>2TH+1TE</td>
<td>2TH+1TE</td>
</tr>
<tr>
<td>Login and Authentication</td>
<td>7TH+6TE</td>
<td>6TH+5TE</td>
</tr>
</tbody>
</table>

<TH: time for performing a one-way hash function>  
<TE: time for performing an exclusive-OR operation>

V. Conclusions
Lin et al. proposed the remote user authentication scheme using smart card recently. But their scheme has not met security requirements in order to achieve successfully the remote user authentication by the password based smart card.

In this paper, we examined the vulnerability of Lin et al.’s authentication scheme against the password guessing attack and proposed an improved scheme to resolve the security problems.

Furthermore, our scheme can provide mutual authentication which is necessary to guarantee higher
security in some situations. The attacker can manipulate the sensitive data of legitimate users via setting up fake server in other words, through server spoofing attacks. Therefore, a secure remote user authentication scheme with smart cards must have the ability to work against such attacks. So, our scheme is more secure in terms of security properties and more efficient according to performance evaluation than Lin et. al’s scheme, while keeping the merits of their scheme.

References

저자 소개

주 영 도(정회원)
- 한양대학교 전자통신공학과 학사
- 미국 University of South Florida 컴퓨터공학과 석사
- 미국 Florida State University 전산학과 박사
- KT 통신망 연구소 선임연구원
- 시스코 시스템즈 코리아 상무
- 화웨이 기술 코리아 부사장
- 현 강남대학교 컴퓨터미디어공학부 교수
<주관심분야 : 정보보안, 네트워크 보안, 정보검색>

안 영 화(정회원)
- 성균관대학교 전자공학과 박사
- 해군사관학교 전자공학과 교수
- 강남대학교 학술정보처장
- 강남대학교 전산정보원장
- 미국 Florida State University 방문교수
- 현 강남대학교 컴퓨터미디어공학부 교수
<주관심분야 : 시스템 보안, 네트워크 보안, 정보보안>