Cryptanalysis and Improvement of the Li-Liu-Wu User Authentication Scheme

Tung-Huang Feng¹, Wan-Yu Chao³, and Min-Shiang Hwang¹,²
(Corresponding author: Min-Shiang Hwang)

¹Department of Computer Science and Information Engineering, Asia University, Taiwan, ROC
²Department of Medical Research, China Medical University Hospital, China Medical
³Department of Management Information Systems, National Chung Hsing University, Taiwan, ROC

ABSTRACT: It’s important to authenticate the legitimacy of remote users over public Internet. Password-based authentication scheme (PBAS) is one of schemes to authenticate the legitimacy of remote users. PBAS have been widely deployed to verify the legitimacy of remote users. Recently, Chen et al. proposed a YS-like user authentication scheme using smart cards. However, Li, et al. have proved that their scheme is vulnerable to the forgery attack, the server spoofing attack, and the password guessing attack. Li, et al. also proposed a modified scheme to eliminate the security vulnerability. Unfortunately, we find the security of their scheme is also existed. In this article, we will prove their scheme is vulnerable to the password guessing attack. At last, we will propose an improved scheme to eliminate the security vulnerability.

1 INTRODUCTION


Recently, Chen et al. proposed a YS-like user authentication scheme using smart cards (Chen & Lee 2008). However, Li, et al. have proved that their scheme is vulnerable to the forgery attack, the server spoofing attack, and the password guessing attack (Li, et al. 2012). Li, et al. also proposed a modified scheme to eliminate the security vulnerability. Unfortunately, we find the security of their scheme is also existed. In this article, we will prove their scheme is vulnerable to the password guessing attack. At last, we will propose an improved scheme to eliminate the security vulnerability.

The remainder of the paper is organized as follows. In Section 2, we briefly review Li-Liu-Wu’s user authentication scheme. An attack on Li-Liu-Wu’s user authentication scheme is proposed in Section 3. In Section 4, we propose an improved Li-Liu-Wu’s user authentication scheme. Finally, we give a brief conclusion in Section 5.

2 REVIEW OF LI-LIU-WU’S SCHEME

There are three participants in Li-Liu-Wu’s user authentication scheme: a key information center (KIC for short), a server (S for short), and a user (U for short). The scheme involves three phases, namely the registration phase, the login phase, and the authentication phase (Li, et al. 2012).

Registration Phase: In this phase, the user U initially registers with KIC over a secure communication channel. The main purpose of this phase is that KIC generates and sends a smart card with the secure information (n, e, g, IDU, CIDU, SU, hU) to
the user U. We denote these parameters in the smart card as follows:

\[ n = p \times q, \text{ where } p \text{ and } q \text{ are two large prime numbers which is generated by KIC.} \]
\[ e: \text{ a public key chosen by KIC.} \]
\[ g: \text{ a primitive element in both } F_p \text{ and } F_q. \]
\[ \text{ID}_U: \text{ an identity of user U which is generated by KIC.} \]
\[ \text{CID}_U = h(\text{PW}_U) \oplus h(\text{ID}_U \oplus d). \]
\[ \text{PW}_U: \text{ the user’s password which is chosen by the user U.} \]
\[ d: \text{ the private key, such that } ed \mod \phi(n) = 1, \text{ where } \phi(n) = \text{the Euler’s totient function and } \phi(n) = (p-1)(q-1). \]
\[ S_U = h(\text{ID}_U \oplus d)^d. \]
\[ h_U = g^d. \]

Login Phase: In this phase, the user U inserts his smart card into a smart card reader in their computer and then inputs his password \( \text{PW}_U \). Next, the user’s smart card generates and sends the login request message \( M_1 = \{ \text{ID}_U, \text{X}_U, \text{Y}_U, n, e, g, \text{T}_U \} \) to the server S. We denote these parameters in the login request message as follows:

\[ \text{X}_U = g^r, \text{ where } r \text{ is a random number which is generated by the smart card}. \]
\[ \text{Y}_U = S_U h_U^{h(\text{ID}_U \oplus d) \cdot \text{T}_U}, \text{ where } \text{T}_U \text{ is the current time stamp}. \]

Authentication Phase: In this phase, the server S verifies the authenticity of the login message \( M_1 \) requested by the user U as follows.

1. The server S checks \( \text{T}_U \) is whether in the valid time interval of the current time or not.
2. The server S checks whether the following equation holds or not:
   \[ (Y_U)^e = h(\text{ID}_U \oplus d) \cdot \text{X}_U^{h(h(\text{ID}_U \oplus d) \cdot \text{T}_U)}. \]

3 CRYPTANALYSIS OF LI-LIU-WU’S SCHEME
In this section, we will show that Li-Liu-Wu’s user authentication scheme (Li, et al. 2012) cannot withstand the password guessing attack when the user U loses his/her smart card. If an attacker steals or finds out a user’s smart card, and extracts the stored values the information \( (n, e, g, \text{ID}_U, \text{CID}_U, S_U, h_U) \) through some ways (Messerges, et al. 2002). Next, we show that Li-Liu-Wu’s scheme cannot withstand the password guessing attack as follows.

Step1. Obtain the login request message \( M_1 = \{ \text{ID}_U, \text{X}_U, \text{Y}_U, n, e, g, \text{T}_U \} \) by intercept from the Internet between the user U and the server S.

Step2. Guess a password \( \text{PW}_U \) and obtain \( \text{CID}_U \) as follows.

\[ \text{CID}_U = \text{CID}_U \oplus h(\text{PW}_U) \]
\[ = [h(\text{PW}_U) \oplus h(\text{ID}_U \oplus d)] \oplus h(\text{PW}_U). \]

Step3. The server S checks whether the following equation holds or not:

\[ (Y_U)^e = \text{CID}_U \cdot \text{X}_U^{h(\text{CID}_U \oplus d) \cdot \text{T}_U}. \]

If the above equation holds, the attacker guesses the correct password \( \text{PW}_U \). Otherwise, the attacker does not yet guess the correct password. The attacker repeats Steps 2 and 3 until the correct password is found.

We show that Equation (1) holds implies the attacker guesses the correct password as follows. The left side of Equation (1) is

\[ (Y_U)^e = h(\text{ID}_U \oplus d) \cdot \text{X}_U^{h(h(\text{ID}_U \oplus d) \cdot \text{T}_U)}. \]

If the correct password is guessed, \( h(\text{PW}_U) = h(\text{PW}_U) \):

\[ \text{CID}_U = \text{CID}_U \oplus h(\text{PW}_U) \]
\[ = [h(\text{PW}_U) \oplus h(\text{ID}_U \oplus d)] \oplus h(\text{PW}_U) \]
\[ = h(\text{ID}_U \oplus d). \]

The right side of Equation (1) is

\[ \text{CID}_U \cdot \text{X}_U^{h(\text{CID}_U \oplus d) \cdot \text{T}_U} \]
\[ = h(\text{ID}_U \oplus d) \cdot \text{X}_U^{h(h(\text{ID}_U \oplus d) \cdot \text{T}_U). \]

The above equation is equal to Equation (2).

Therefore, Equation (1) holds. However, if the attacker could not guess the correct password, \( h(\text{PW}_U) \neq h(\text{PW}_U) \):

\[ \text{CID}_U = \text{CID}_U \oplus h(\text{PW}_U) \]
\[ = [h(\text{PW}_U) \oplus h(\text{ID}_U \oplus d)] \oplus h(\text{PW}_U). \]

The right side of Equation (1) is

\[ \text{CID}_U \cdot \text{X}_U^{h(\text{CID}_U \oplus d) \cdot \text{T}_U} \]
\[ = [h(\text{PW}_U) \oplus h(\text{ID}_U \oplus d)] \oplus h(\text{PW}_U). \]

The above equation is not equal to Equation (2). Therefore, Equation (1) does not hold. The attacker knows that it is incorrect password and he/she need to guess other passwords.

4 THE PROPOSED SCHEME
In order to eliminate the security vulnerability of Li-Liu-Wu’s user authentication scheme, we will propose an improved user authentication scheme in this section. Like Li-Liu-Wu’s scheme, there are also three participants: KIC, a server S, and a user U; and three phases in the proposed scheme: the registration phase, the login phase, and the authentication phase.

Registration Phase: In this phase, the user U initially registers with KIC over a secure communication channel. The main purpose of this phase is that KIC generates and sends a smart card with the secure information \( (n, e, g, \text{ID}_U, \text{CID}_U, h_U) \) to the user U. These parameters in the smart card are the same as that in the registration phase of Li-Liu-Wu’s user authentication scheme. The difference of the proposed scheme and Li-Liu-Wu’s user authentication scheme is only one that the proposed scheme removes the parameter \( S_U \) from the smart card in Li-Liu-Wu’s user authentication scheme. The proposed scheme needs not the parameter \( S_U \) for authentication.

Login Phase: In this phase, the user U sends a login request message to the server S whenever the user U wants to access resources upon the server S. The login request message is produced by the following steps:
Step1. The user U inserts his/her smart card into a smart card reader in their computer and then inputs his/her password $PW_U$.

Step2. The user’s smart card computes $CID'_U$ as follows.
\[
CID'_U = CID_U \oplus h(PW_U) \\
= [h(PW_U) \oplus h(ID_U \oplus d)] \oplus h(PW_U) \\
= h(ID_U \oplus d)
\]

Step3. The user’s smart card generates a random number $r$ and computes $X_U$ as follows.
\[
X_U = g^r \mod n.
\]

Step4. The user’s smart card computes $Y_U$ as follows.
\[
Y_U = CID'_U h_U^{r CID'_U} u^T_U,
\]
where $T_U$ is the current time stamp.

Step5. The user’s smart card sends the login request message $M_1 = \{ID_U, X_U, Y_U, n, e, g, T_U\}$ to the server $S$.

Authentication Phase: In this phase, the server $S$ verifies the authenticity of the login message $M_1$ requested by the user U as follows.

Step1. The server $S$ checks $T_U$ is whether in the valid time interval of the current time or not.

Step2. The server $S$ computes $CID'_U$ as follows.
\[
CID'_U = h(ID_U \oplus d).
\]

Step3. The server $S$ checks whether the following equation holds or not:
\[
(Y_U)^e = (CID'_U)^e X_U^{h CID'_U} u^{-T} U (3)
\]

If so, the server $S$ accepts the user login request, otherwise, the server $S$ rejects the user U’s login request. The rest steps of the authentication phase are the same as that of the authentication phase in Li-Liu-Wu’s scheme.

We show that Equation (3) holds implies the legal user inputs a correct password as follows.

The left side of Equation (3) is
\[
(Y_U)^e = (CID'_U)^e X_U^{h CID'_U} u^{-T} U
\]
The above equation is thus equal to the right side of Equation (3). Therefore, the server $S$ verifies the legal user U.

The proposed scheme can against the password guessing attack when the user U loses his/her smart card. If an attacker steals or finds out a user’s smart card, and extracts the stored values the information (n, e, g, ID_U, CID_U, h_U) through some ways (Merges, et al. 2002). The attacker cannot guess a correct password by Equation (3). In spite of the guessing password whether correct or not, the verification Equation (3) always holds. Therefore, the attacker cannot to judge the correct password.

5 CONCLUSION

We have shown that there is a leak in Li-Liu-Wu’s user authentication scheme. Their scheme cannot withstand the password guessing attack when the user U loses his/her smart card. We also proposed an improved and secure user authentication scheme.

ACKNOWLEDGMENTS

This study was supported by the National Science Council of Taiwan under grant 103-2221-E-468 - 026, 103-2622-E-468-001-CC2, and 103-2622-H-468-001-CC2.

REFERENCE


