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

Tung-Huang Feng[1], Wan-Yu Chao[3], and Min-Shiang Hwang[1,2]
(Corresponding author: Min-Shiang Hwang)

Department of Computer Science and Information Engineering, Asia University, Taiwan, ROC.[1]

Department of Medical Research, China Medical University Hospital, China Medical[2]

Department of Management Information Systems, National Chung Hsing University, Taiwan, ROC[3]

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

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. In 2006, Tsai et al. (Tsai et al. 2006) classified password authentication schemes into three classes: RSA-based password authentication schemes (Hwang 1999, Shen, et al. 2003, Yang, et al. 2004), ElGamal-based password authentication schemes (Hwang & Li 2000, Kumar 2004, Yang, et al. 2003), and hash-based password authentication schemes (Kim & Koç 2005, Lee, et al. 2002, Lee, et al. 2013, Lin, et al. 2006, Mangipudi & Katti 2006, Zhuang, et al. 2014).

There are many user authentication schemes have been proposed (Sood, et al. 2011, Tao & Adams 2008). Some of these schemes are used smart card for storing user's secure information (He, et al. 2011, Hwang et al. 2010, Hwang et al. 2005, Kumar, et al. 2011, Lee, et al. 2002, Ramasamy & Muniyandi 2012, Shen, et al. 2003-1, Tang, et al. 2013, Wang & Yang 2006, Yang, et al. 2012). Some of these schemes are applied to multi-server environment (Feng, et al. 2014, He et al. 2013, Lin, et al. 2003). Some of these schemes are based on biometrics (Li, et al. 2010, Li & Hwang 2010, Prakash 2014). Some of these schemes are based on neural networks (Li et al. 2001, Lin et al. 2005). Some of these schemes are applied to mobile environment (Hwang, et al. 2002, Lee, et al. 2006, Li & Chu 2009, Liao, et al. 2006, Wu, et al. 2005).

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, ID_U, CID_U, S_U, h_U) to the user U. We denote these parameters in the smart card as follows:

$n = p \times q$, where p and q are two large prime number which is generated by KIC.

e: a public key chosen by KIC.

g: a primitive element in both F_p and F_q.

ID_U: an identity of user U which is generated by KIC.

$CID_U = h(PW_U) \oplus h(ID_U \oplus d)$.

PW_U: the user's password which is chosen by the user U.

d: the private key, such that ed mod $\Phi(n) = 1$, where $\Phi()$ is the Euler's totient function and $\Phi(n)=(p-1)(q-1)$.

$S_U = h(ID_U \oplus d)^d$.

$h_U = g^d$.

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 PW_U. Next, the user's smart card generates and sends the login request message $M_1 = \{ID_U, X_U, Y_U, n, e, g, T_U\}$ to the server S. We denote these parameters in the login request message as follows:

$X_U = g^r$, where *r* is a random number which is generated by the smart card.

$Y_U = S_U h_U^{rh(h(ID_U \oplus d), T_U)}$, where T_U 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 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:

$$(Y_U)^e = h(ID_U \oplus d)\ X_U^{h(h(ID_U \oplus d), T_U)}.$$

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, ID_U, 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 $M_1 = \{ID_U, X_U, Y_U, n, e, g, T_U\}$ by intercept from the Internet between the user U and the server S.

Step2. Guess a password PW'_U and obtain CID' as follows.

$$\begin{aligned} CID'_U &= CID_U \oplus h(PW_U) \\ &= [h(PW_U) \oplus h(ID_U \oplus d)] \oplus h(PW'_U) \end{aligned}$$

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

$$(Y_U)^e = CID'_U\, X_U^{h(CID'_U, T_U)} \qquad (1)$$

If the above equation holds, the attacker guesses the correct password 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

$$(Y_U)^e = h(ID_U \oplus d)\ X_U^{h(h(ID_U \oplus d), T_U)} \qquad (2)$$

If the correct password is guessed, $h(PW'_U) = h(PW_U)$:

$$\begin{aligned} CID'_U &= CID_U \oplus h(PW_U) \\ &= [h(PW_U) \oplus h(ID_U \oplus d)] \oplus h(PW'_U) \\ &= h(ID_U \oplus d) \end{aligned}$$

The right side of Equation (1) is

$$\begin{aligned} &CID'_U\, X_U^{h(CID'_U, T_U)} \\ &= h(ID_U \oplus d)\ X_U^{h(h(ID_U \oplus d), T_U)} \end{aligned}$$

The above equation is equal to Equation (2). Therefore, Equation (1) holds. However, if the attacker could not guess the correct password, $h(PW'_U) \neq h(PW_U)$:

$$\begin{aligned} CID'_U &= CID_U \oplus h(PW_U) \\ &= [h(PW_U) \oplus h(ID_U \oplus d)] \oplus h(PW'_U). \end{aligned}$$

The right side of Equation (1) is

$$\begin{aligned} &CID'_U\, X_U^{h(CID'_U, T_U)} \\ &= [h(PW_U) \oplus h(ID_U \oplus d)] \oplus h(PW'_U) \\ &\qquad X_U^{h([h(PWU) \oplus h(IDU \oplus d)] \oplus h(PW'U), T_U)} \end{aligned}$$

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, ID_U, 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.

$$\begin{aligned} CID'_U &= CID_U \oplus h(PW_U) \\ &= [h(PW_U)\oplus h(ID_U\oplus d)] \oplus h(PW_U) \\ &= h(ID_U\oplus d) \end{aligned}$$

Step3. The user's smart card generates a random number r and computes X_U as follows.

$$X_U = g^r \bmod n.$$

Step4. The user's smart card computes Y_U as follows.

$$Y_U = CID'_U\, h_U^{rh(CID'_U, T_U)},$$

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:

$$(Y_U)^e= (CID'_U)^e\, X_U^{h(CID'_U), T_U).} \quad (3)$$

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

$$\begin{aligned} (Y_U)^e &= (CID'_U)^e\, h_U^{rh(CID'_U, T_U)}, \\ &= (CID'_U)^e\, X_U^{h(CID'_U, T_U)} \end{aligned}$$

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 (Messerges, 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

Chen, T.H. & Lee, W.B. (2008). A new method for using hash functions to solve remote user authentication. *Computers and Electrical Engineering* 34: 53–62.

Feng, T.H., Ling, C.H., Hwang, M.S. (2014). Cryptanalysis of Tan's improvement on a password authentication scheme for multi-server environments. *International Journal of Network Security* 16(4): 318-321.

He D, Zhao W, and Wu S. (2013). Security analysis of a dynamic ID-based authentication scheme for multi-server environment using smart cards. *International Journal of Network Security* 15(5): 282-292.

He, D., Chen, J. Hu, J. (2011). Weaknesses of a remote user password authentication scheme using smart card. *International Journal of Network Security* 13(1): 58-60.

Hwang, M.S. (1999). A remote password authentication scheme based on the digital signature method. *International Journal of Computer Mathematics* 70(4): 657-666.

Hwang M.S., Chong S.K., and Chen T.Y. 2010. Dos-resistant ID-based password authentication scheme using smart cards. *Journal of Systems and Software* 83: 163-172.

Hwang, M.S., Lee, C.C., Yang, W.P. (2002). An improvement of mobile users authentication in the integration environments. *International Journal of Electronics and Communications* 56(5): 293-297.

Hwang, M.S. & Li, L.H. (2000). A new remote user authentication scheme using smart cards. *IEEE Transactions on Consumer Electronics* 46(1): 28-30.

Hwang, M.S., Lo, J.W., Liu, C.Y., Lin, S.C. (2005). Cryptanalysis of a user friendly remote authentication scheme with smart card. *Pakistan Journal of Applied Sciences* 5(1): 99-100.

Kumar, M. (2004). New remote user authentication scheme using smart cards. *IEEE Transactions on Consumer Electronics* 50(2): 597–600.

Kim, M. & Koç, Ç.K. (2005). A simple attack on a recently introduced hash-based strong-password authentication scheme. *International Journal of Network Security* 1(2): 77-80.

Kumar, M., Gupta, M.K., Kumari, S. (2011). An improved efficient remote password authentication scheme with smart card over insecure networks. *International Journal of Network Security* 13(3): 167-177.

Lee, C.C., Li, L.H., Hwang, M.S. (2002). A remote user authentication scheme using hash functions. *ACM Operating Systems Review* 36(4): 23-29.

Lee, C.C., Liu, C.H., Hwang, M.S. (2013). Guessing attacks on strong-password authentication protocol. *International Journal of Network Security* 15(1): 64-67.

Lee, C.C., Hwang, M.S., Liao, I.E. (2006). Security enhancement on a new authentication scheme with anonymity for wireless environments. *IEEE Transactions on Industrial Electronics* 53(5): 1683-1687.

Lee, C.C., Hwang, M.S., Yang, W.P. (2002). A flexible remote user authentication scheme using smart cards. *ACM Operating Systems Review* 36(3): 46-52.

Li, C.T. & Chu, Y.P. (2009). Cryptanalysis of threshold password authentication against guessing attacks in ad hoc networks. *International Journal of Network Security* 8(2): 166-168.

Li, C.T. & Hwang, M.S. (2010). An online biometrics-based secret sharing scheme for multiparty cryptosystem using smart cards. *International Journal of Innovative Computing, Information and Control* 6(5): 2181-2188.

Li, C.T. & Hwang, M.S. (2010). An efficient biometrics-based remote user authentication scheme using smart cards. *Journal of Network and Computer Applications* 33: 1-5.

Li, J., Liu, S., Wu, S. (2012). Cryptanalysis and improvement of a YS-like user authentication scheme. *International Journal of Digital Content Technology and its Applications* 7(1): 828-836.

Li, L.H., Lin, I.C., Hwang, M.S. (2001). A remote password authentication scheme for multi-server architecture using neural networks. *IEEE Transactions on Neural Networks* 12(6): 1498-1504.

Liao, I.E., Lee, C.C., Hwang, M.S. (2006). A password authentication scheme over insecure networks. *Journal of Computer and System Sciences* 72(4): 727-740.

Lin, I.C., Hwang, M.S., Li, L.H. (2003). A new remote user authentication scheme for multi-server architecture. *Future Generation Computer Systems* 19(1): 13-22.

Lin, I.C., Ou, H.H., Hwang, M.S. (2005). A user authentication system using back-propagation network. *Neural Computing & Applications* 14(3): 243-249.

Lin, C.W., Tsai, C.S., Hwang, M.S. (2006). A new strong-password authentication scheme using one-way hash functions. *International Journal of Computer and Systems Sciences* 45(4): 623-626.

Mangipudi, K.V. & Katti, R.S. (2006). A hash-based strong password authentication protocol with user anonymity. *International Journal of Network Security* 2(3): 205-209.

Messerges, T.S., Dabbish, E.A., Sloan R.H. (2002). Examining smart-card security under the threat of power analysis attacks. *IEEE Transactions on Computers* 51(5): 541–552.

Prakash, A. (2014). A biometric approach for continuous user authentication by fusing hard and soft traits. *International Journal of Network Security* 16(1): 65-70.

Ramasamy, R. & Muniyandi, A.P. (2012). An efficient password authentication scheme for smart card. *International Journal of Network Security* 14(3): 180-186.

Shen, J.J., Lin, C.W., Hwang, M.S. (2003). Security enhancement for the timestamp-based password authentication scheme using smart cards. *Computers & Security* 22(7): 591-595.

Shen, J.J., Lin, C.W., Hwang, M.S. (2003-1). a modified remote user authentication scheme using smart cards. *IEEE Transactions on Consumer Electronics* 49(2): 414-416.

Sood, S.K., Sarje, A.K., Singh, K. (2011). Inverse cookie-based virtual password authentication protocol. *International Journal of Network Security* 13(2): 98-108.

Tang, H., Liu, X., Jiang, L. (2013). A robust and efficient timestamp-based remote user authentication scheme with smart card lost attack resistance. *International Journal of Network Security* 15(6): 446-454.

Tao, H. & Adams, C. (2008). Pass-Go: A proposal to improve the usability of graphical passwords. *International Journal of Network Security* 7(2): 273-292.

Tsai, C.S., Lee, C.C., and Hwang, M.S. 2006. Password authentication schemes: Current status and key issues, *International Journal of Network Security* 3(2): 101-115.

Wang, R.C. & Yang, C.C. (2006). Cryptanalysis of two improved password authentication schemes using smart cards. *International Journal of Network Security* 3(3): 283-285.

Wu, H.C., Liu, C.Y., Chiou, S.F. (2005). Cryptanalysis of a secure one-time password authentication scheme with low-communication for mobile communications. *International Journal of Network Security* 1(2): 74-76.

Yang, C.C., Chang, T.Y., Hwang, M.S. (2003). The security of the improvement on the methods for protecting password transmission. *Informatica* 14(4): 551-558.

Yang, L., Ma, J.F., Jiang, Q. (2012). Mutual authentication scheme with smart cards and password under trusted computing. *International Journal of Network Security* 14(3): 156-163.

Yang, C.C., Yang, H.W., Wang, R.C. (2004). Cryptanalysis of security enhancement for the timestamp-based password authentication scheme using smart cards. *IEEE Transactions on Consumer Electronics* 50(2): 578–579.

Zhuang, X., Chang, C.C., Wang, Z.H., Zhu, Y. (2014). A simple password authentication scheme based on geometric hashing function. *International Journal of Network Security* 16(4): 271-277.