# Cryptanalysis of an Efficient and Secure Smart Card Based Password Authentication Scheme

Chi-Wei Liu[1], Cheng-Yi Tsai[1], and Min-Shiang Hwang[1,2(✉)]

[1] Department of Computer Science and Information Engineering, Asia University, 500, Lioufeng Road, Wufeng, Taichung 41354, Taiwan, R.O.C.
mshwang@asia.edu.tw
[2] Department of Medical Research, China Medical University Hospital, China Medical University, No. 91, Hsueh-Shih Road, Taichung 40402, Taiwan, R.O.C.

**Abstract.** The user authentication scheme has been widely applied to verify the users' legality. In order to enhance the security, the smart card has widely used in an authentication scheme. Recently, Liu et al. shown that some weaknesses exist in Li et al.'s scheme. An efficient and secure user authentication scheme with a smart card presented by them is more efficient and secure than other schemes. However, the security issues of their scheme proposed by them also exist, so we will demonstrate that their scheme is vulnerable to the replaying attack.

**Keywords:** Password · Smart card · User authentication

## 1 Introduction

The user authentication scheme has been widely applied to verify the users' legality. Many password-based user authentication schemes have been proposed to verify the remote users' identification [1–16]. However, the password is easy to be exposed by guessing attack. In order to enhance the security, the smart card has widely used in an authentication scheme [18–30].

Recently, a robust smart-card-based remote user password authentication scheme [5] was proposed by Chen et al. However, Li et al. pointed out some weaknesses (i.e., forward secrecy and wrong password login problem) in Chen et al.'s scheme [14]. Li et al. also proposed an enhanced smart card based user authentication scheme [14]. However, Liu et al. shown that Li et al.'s scheme was unable to against the man-in-the-middle and insider attacks [17]. An efficient and secure user authentication scheme with a smart card proposed by them is more efficient and secure than other schemes. However, the security issues of their scheme proposed by them also exist, so we will exhibit that, their scheme is vulnerable to the replaying attack.

The rest of this paper is organized as follows. In Sect. 2, we briefly review Liu et al.'s user authentication scheme. In Sect. 3, we analyze and show that some security weaknesses in Liu et al.' user authentication scheme. Finally, we present our conclusions in Sect. 4.


F. Xhafa et al. (eds.), *Recent Developments in Intelligent Systems and Interactive Applications*, Advances in Intelligent Systems and Computing 541, DOI 10.1007/978-3-319-49568-2_26

## 2 Review of Liu-Chang-Chang Scheme

In this section, Liu et al.'s user authentication scheme (Liu-Chang-Chang Scheme) with a smart card [17] has been briefly reviewed. Liu-Chang-Chang's user authentication scheme has three participants: a user (U for short), a smart card (C for short), and a server (S for short). The scheme is composed of four phases such as registration, login phase, authentication phase, and e password change phase. The notations used in this paper are listed in Table 1.

**Table 1.** The notations used in this paper

| Notations | Meaning |
|---|---|
| $U_i$ | The user *i* |
| $ID_i$ | The identity of the user *i* |
| $PW_i$ | The password of the user i |
| S | The providing service server |
| X | The server's master secret key |
| Ti & $T_s$ | The timestamp of the user I and server, respectively |
| Sk | The shared session key |
| h(.) | A collision-free one-way hash function |
| $\oplus$ | An XOR operation |
| $\|$ | The message concatenation operation |

**The Registration Phase:** In this phase, the server S makes a smart card for a new user ($U_i$). The smart card contains four parameters, $\{B_i, C_i, h(.), r\}$, where $B_i = A_i \oplus h(r \| PW_i)$; $A_i = h(ID_i \oplus x) \| h(x)$; $C_i = h(A_i \| ID_i \| h(r \| PW_i))$; h(.) denotes a collision-free one-way hash function; r denotes a random number; $ID_i$ and $PW_i$ are user's identity and password, respectively. The registration phase is executed as follows.

**The Login Phase:** In this phase, a user ($U_i$) wants to login the server via public Internet. The login phase is executed as follows.

(1) The user Ui sends the login request parameters, IDi and PWi to the smart card.
(2) The smart card computes A'i and C'i as follows: A'I = Bi $\oplus$ h(r $\|$ PWi); C'I = h(A'I $\|$ IDi $\|$ h(r $\|$ PWi)). Next, the smart card checks whether C'I is equal to Ci. If C'I is equal to Ci, the smart card continues to execute Step 3, otherwise, the smart card terminates this login request.
(3) The smart card computes Di and Ei as follows: Di = h(IDi $\oplus$ $\alpha$); Ei = A'I $\oplus$ $\oplus$ Tc, where Tc denotes the current timestamp of the smart card and $\alpha$ denotes a random number.
(4) The smart card sends IDi, Di, Ei and Ti to the server S.

**The Authentication Phase:** Upon receiving the message, {IDi, Di, Ei, Tc}, from User (Ui), the server S executes this authentication phase as follows.

(1) The server checks IDi format and the timestamp Tc whether or not in valid time. If both conditions are not hold, the server S rejects the login request.
(2) The server computes Ai, α', and Di' as in Fig. 1. Next, the server checks D'I whether equals to Di. If the equation is not hold, the server S rejects the login request.
(3) The server randomly selects $\beta$ and computes Fi and Gi as in Fig. 1. Next, the server S sends {Fi, Gi, Ti} vis public channel to user Ui.
(4) The user Ui the timestamp Ts whether or not in valid time. If this condition is not hold, the user terminates this session.
(5) The user computes $\beta$'and F'I. Next, the user checks F'I whether equals to Fi. If this condition is true, the user Ui confirms the server S is legit.
(6) The server S and the user Ui compute the session key sk = h(α ‖ $\beta$ ‖ h (Ai ⊕ IDi)).

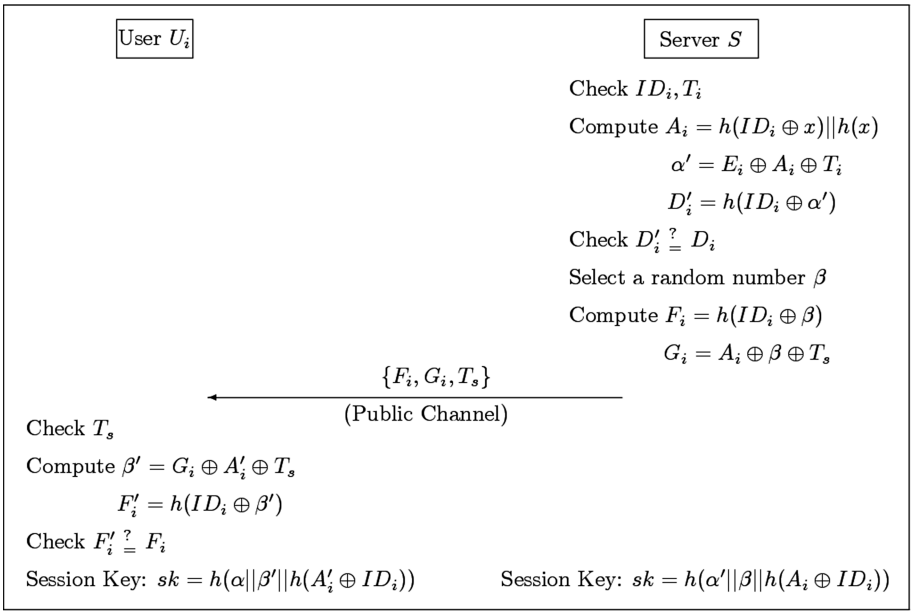


**Fig. 1.** The authentication phase of Liu-Chang-Chang's scheme

## 3 Cryptanalysis of Liu-Chang-Chang Scheme

In this section, it is demonstrated that the user authentication scheme proposed by Liu-Chang-Chang's [17] cannot resist the replaying attack when the hacker intercepts {IDi, Di, Ei, Ti} between smart card and server S and {F, G, Ts} between user Ui and server S. The first replaying attack is listed as follows.

Step 1. When the smart card sent the message, {IDi, Di, Ei, Ti}, to the server S in the login phase, the hacker intercepts {IDi, Di, Ei, Ti} between smart card and server S via public channel.

Step 2. The hacker computes a new E'I as follows:

$$\begin{aligned} \text{E'I} &= \text{Ei} \oplus \text{Ti} \oplus \text{Th} \\ &= (\text{A}'\text{I} \oplus \alpha \oplus \text{Ti}) \oplus \text{Ti} \oplus \text{Th} \\ &= \text{A}'\text{I} \oplus \alpha \oplus \text{Th} \end{aligned}$$

Here, Th denotes the timestamp of Hacker's device. Next, the hacker sends the forged message {IDi, Di, E'i, Th} to replace the intercepted {IDi, Di, Ei, Ti}.

Step 3. The server S will check successfully the equation in Steps (1) and (2) in the authentication phase. Thus, the server will be deceived by the hacker (Fig. 2).

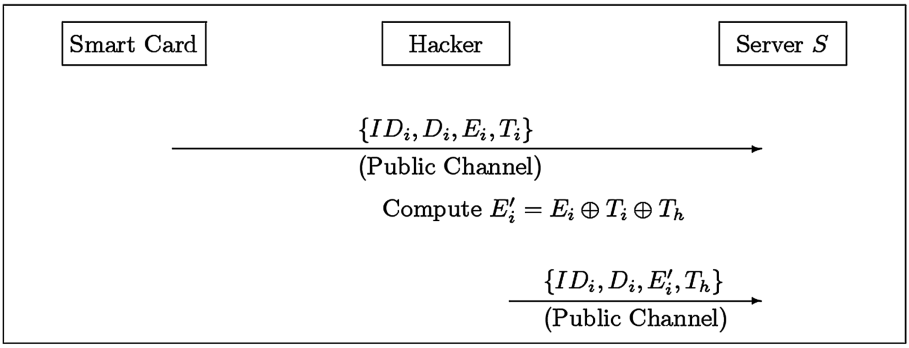


**Fig. 2.** The replaying attack when the hacker intercepts {IDi, Di, Ei, Ti}

The second replaying attack is similar to the first replaying attack. The attack listed as follows.

Step 1. When the server S sent the message, {Fi, Gi, Ts}, to the user Ui in the authentication phase, the hacker intercepts it between server S and user Ui via public channel.

Step 2. The hacker computes a new G'i as follows:

$$\begin{aligned} \text{G'i} &= \text{Gi} \oplus \text{Ts} \oplus \text{Th} \\ &= (\text{Ai} \oplus \beta \oplus \text{Ts}) \oplus \text{Ts} \oplus \text{Th} \\ &= \text{Ai} \oplus \beta \oplus \text{Th} \end{aligned}$$

The hacker sends the forged message {Fi, G'i, Th} to replace the intercepted {Fi, Gi, Ts}.

Step 3. The user Ui will check successfully the equation in Steps (4) and (5) in the authentication phase. Thus, the user Ui will be deceived by the hacker.

## 4 Conclusion

We have demonstrated that the user authentication scheme proposed Liu-Chang-Chang [17] have a weakness. Their scheme cannot resist the replaying attack when the hacker intercepts {IDi, Di, Ei, Ti} between smart card and server S and {F, G, Ts} between user Ui and server S.

**Acknowledgments.** This study was supported by the National Science Council of Taiwan under grant MOST 104-2221-E-468 -004 and MOST 103-2221-E-468 -026.

## References

1. Ahmed, A., Younes, A., Abdellah, A., Sadqi, Y.: Strong zero-knowledge authentication based on virtual passwords. Int. J. Netw. Secur. **18**(4), 601–616 (2016)
2. Amin, R.: Cryptanalysis and efficient dynamic ID based remote user authentication scheme in multi-server environment using smart card. Int. J. Netw. Secur. **18**(1), 172–181 (2016)
3. Anwar, N., Riadi, I., Luthfi, A.: Forensic SIM card cloning using authentication algorithm. Int. J. Electron. Inf. Eng. **4**(2), 71–81 (2016)
4. Chang, C.-C., Hsueh, W.-Y., Cheng, T.-F.: An advanced anonymous and biometrics-based multi-server authentication scheme using smart cards. Int. J. Netw. Secur. **18**(6), 1010–1021 (2016)
5. Chen, B.L., Kuo, W.C., Wuu, L.C.: Robust smart-card-based remote user password authentication scheme. Int. J. Commun. Syst. (in press). http://dx.doi.org/10.1002/dac.2368
6. Feng, T.H., Ling, C.H., Hwang, M.S.: Cryptanalysis of Tan's improvement on a password authentication scheme for multi-server environments. Int. J. Netw. Secur. **16**, 318–321 (2014)
7. He, D., Zhao, W., Wu, S.: Security analysis of a dynamic ID-based authentication scheme for multi-server environment using smart cards. Int. J. Netw. Secur. **15**, 282–292 (2013)
8. Huang, H.F., Chang, H.W., Yu, P.K.: Enhancement of timestamp-based user authentication scheme with smart card. Int. J. Netw. Secur. **16**, 463–467 (2014)
9. Hwang, M.S., Chong, S.K., Chen, T.Y.: Dos-resistant ID-based password authentication scheme using smart cards. J. Syst. Softw. **83**, 163–172 (2000)
10. Hwang, M.S., Li, L.H.: A new remote user authentication scheme using smart cards. IEEE Trans. Consum. Electron. **46**, 28–30 (2000)
11. Li, C.T., Hwang, M.S.: An online biometrics-based secret sharing scheme for multiparty cryptosystem using smart cards. Int. J. Innovative Comput. Inf. Control **6**, 2181–2188 (2010)
12. Li, C.T., Hwang, M.S.: An efficient biometrics-based remote user authentication scheme using smart cards. J. Netw. Comput. Appl. **33**, 1–5 (2010)
13. Li, L.H., Lin, I.C., Hwang, M.S.: A remote password authentication scheme for multi-server architecture using neural networks. IEEE Trans. Neural Netw. **12**, 1498–1504 (2001)
14. Li, X., Niu, J., Khan, M.K., Liao, J.: An enhanced smart card based remote user password authentication scheme. J. Netw. Comput. Appl. (in press). http://dx.doi.org/10.1016/j.jnca.2013.02.034
15. Lin, I.C., Hwang, M.S., Li, L.H.: A new remote user authentication scheme for multi-server architecture. Future Gener. Comput. Syst. **19**, 13–22 (2003)
16. Ling, J., Zhao, G.: An improved anonymous password authentication scheme using nonce and bilinear pairings. Int. J. Netw. Secur. **17**(6), 787–794 (2015)

17. Liu, Y., Chang, C.-C., Chang, S.-C.: An efficient and secure smart card based password authentication scheme. Int. J. Netw. Secur. **19**(1), 1–10 (2017)
18. Lu, Y., Yang, X., Wu, X.: A secure anonymous authentication scheme for wireless communications using smart cards. Int. J. Netw. Secur. **17**(3), 237–245 (2015)
19. Osei, E.O., Hayfron-Acquah, J.B.: Cloud computing login authentication redesign. Int. J. Electron. Inf. Eng. **1**(1), 1–8 (2014)
20. Prakash, A.: A biometric approach for continuous user authentication by fusing hard and soft traits. Int. J. Netw. Secur. **16**, 65–70 (2014)
21. Shen, J.J., Lin, C.W., Hwang, M.S.: Security enhancement for the timestamp-based password authentication scheme using smart cards. Comput. Secur. **22**, 591–595 (2003)
22. Shen, J.J., Lin, C.W., Hwang, M.S.: A modified remote user authentication scheme using smart cards. IEEE Trans. Consum. Electron. **49**, 414–416 (2003)
23. Stanek, M.: Weaknesses of password authentication scheme based on geometric hashing. Int. J. Netw. Secur. **18**(4), 798–801 (2016)
24. Tang, H., Liu, X., Jiang, L.: A robust and efficient timestamp-based remote user authentication scheme with smart card lost attack resistance. Int. J. Netw. Secur. **15**, 446–454 (2013)
25. Wang, Y., Peng, X.: Cryptanalysis of two efficient password-based authentication schemes using smart cards. Int. J. Netw. Secur. **17**(6), 728–735 (2015)
26. Wei, J., Liu, W., Hu, X.: Secure and efficient smart card based remote user password authentication scheme. Int. J. Netw. Secur. **18**(4), 782–792 (2016)
27. Wijayanto, H., Hwang, M.-S.: Improvement on timestamp-based user authentication scheme with smart card lost attack resistance. Int. J. Netw. Secur. **17**(2), 160–164 (2015)
28. Yang, C.C., Chang, T.Y., Hwang, M.-S.: The security of the improvement on the methods for protecting password transmission. Informatica **14**, 551–558 (2003)
29. Zhu, H., Zhang, Y., Zhang, Y.: A provably password authenticated key exchange scheme based on chaotic maps in different realm. Int. J. Netw. Secur. **18**(4), 688–698 (2016)
30. Zhuang, X., Chang, C.C., Wang, Z.H., Zhu, Y.: A simple password authentication scheme based on geometric hashing function. Int. J. Netw. Secur. **16**, 271–277 (2014)