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*]

1Department of Computer Science and Information Engineering, Asia University, Taiwan
500, Lioufeng Rd., Wufeng, Taichung, Taiwan 41354, R.O.C.

2Department of Medical Research, China Medical University Hospital, China Medical University
No.91, Hsueh-Shih Road, Taichung, Taiwan 40402, R.O.C.

Email: mshwang@asia.edu.tw

* The corresponding author: Prof. Min-Shiang Hwang

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 existed in Li et al.'s scheme. They also proposed an efficient and secure user authentication scheme with smart card. Their scheme is more efficient and secure than other schemes. However, we find the security of their scheme is also existed. In this article, we will prove 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. There are 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, Chen et al. proposed a robust smart-card-based remote user password authentication scheme [5]. 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]. They also proposed an efficient and secure user authentication scheme with smart card. Their scheme is more efficient and secure than

other schemes. However, we find the security of their scheme is also existed. In this article, we will prove their scheme is vulnerable to the replaying attack.

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

2 Review of Liu-Chang-Chang Scheme

In this section, we briefly review Liu et al.'s user authentication scheme (Liu-Chang-Chang Scheme) with smart card [17]. There are three participants in Liu-Chang-Chang's user authentication scheme: a user (U for short), a smart card (C for short), and a server (S for short). The scheme consists of four phases, namely the registration, the login phase, the authentication phase, and the 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 and illustrated in Figure 2.

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 ⊕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 ⊕ α); Ei = A' I ⊕ α ⊕Tc, where Tc denotes the current timestamp of the smart card and α 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 Figure 3. 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 β and computes Fi and Gi as in Figure 3. 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 β'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 || β || h(Ai⊕ IDi)).

3 Cryptanalysis of Liu-Chang-Chang Scheme

In this section, we will show that Liu-Chang-Chang's user authentication scheme [17] cannot withstand 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.

Step1. 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.

Step2. The hacker computes a new E'I as follows:

$$E'I = Ei \oplus Ti \oplus Th$$

$$= (A'I \oplus \alpha \oplus Ti) \oplus Ti \oplus Th$$

$$= A'I \oplus \alpha \oplus Th$$

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}.

Step3. 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.

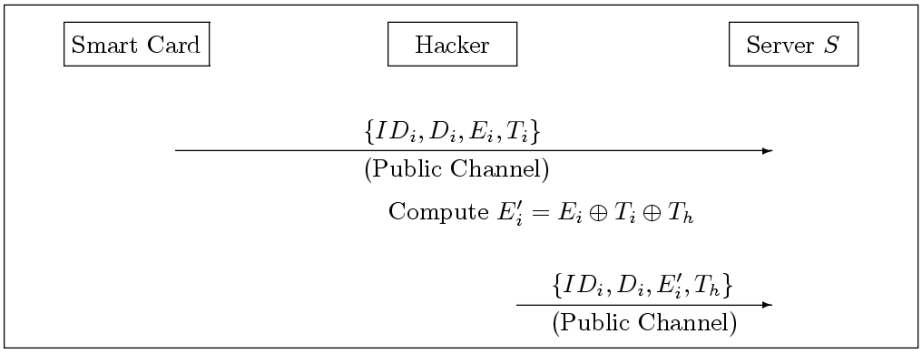

Figure 4: The replaying attack when the hacker intercepts {IDi, Di, Ei, Ti}

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

Step1. 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.

Step2. The hacker computes a new G'i as follows:

$$G'i = Gi \oplus Ts \oplus Th$$

$$= (Ai \oplus \beta \oplus Ts) \oplus Ts \oplus Th$$

$$= Ai \oplus \beta \oplus Th$$

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

Step3. 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 shown that there is a weakness in Liu-Chang-Chang's user authentication scheme [17]. Their scheme cannot withstand 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.

5 References

1. Asimi Ahmed, Asimi Younes, Amghar Abdellah, Yassine Sadqi, "Strong Zero-knowledge Authentication Based on Virtual Passwords", International Journal of Network Security, Vol. 18, No. 4, pp. 601-616, 2016.
2. Ruhul Amin, "Cryptanalysis and Efficient Dynamic ID Based Remote User Authentication Scheme in Multi-server Environment Using Smart Card", International Journal of Network Security, Vol. 18, No. 1, pp. 172-181, 2016.
3. Nuril Anwar, Imam Riadi, Ahmad Luthfi, " Forensic SIM Card Cloning Using Authentication Algorithm", International Journal of Electronics and Information Engineering, Vol. 4, No. 2, pp. 71-81, 2016.
4. Chin-Chen Chang, Wei-Yuan Hsueh, Ting-Fang Cheng, "An Advanced Anonymous and Biometrics-based Multi-server Authentication Scheme Using Smart Cards", International Journal of Network Security, Vol. 18, No. 6, pp. 1010-1021, 2016.
5. B. L. Chen, W. C. Kuo and L. C. Wuu, "Robust smart-card-based remote user password authentication scheme," International Journal of Communication Systems, in press. (http://dx.doi.org/10.1002/dac.2368).
6. T.H. Feng, C.H. Ling, M.S. Hwang, Cryptanalysis of Tan's improvement on a password authentication scheme for multi-server environments, International Journal of Network Security, vol. 16, pages 318-321, 2014.
7. D. He, W. Zhao, and S. Wu, Security analysis of a dynamic ID-based authentication scheme for multi-server environment using smart cards, International Journal of Network Security, vol.15, pages 282-292, 2013.
8. H.F. Huang, H.W. Chang, P.K. Yu, Enhancement of timestamp-based user authentication scheme with smart card, International Journal of Network Security. vol. 16, pages 463-467, 2014
9. M.S. Hwang, S.K. Chong, and T.Y. Chen, Dos-resistant ID-based password authentication scheme using smart cards, Journal of Systems and Software, vol. 83, pages 163-172, 2000.
10. M.S. Hwang, L.H. Li, A new remote user authentication scheme using smart cards, IEEE Transactions on Consumer Electronics, vol. 46, pages 28-30, 2000.
11. C.T., Li, M.S. Hwang, An online biometrics-based secret sharing scheme for multiparty cryptosystem using smart cards, International Journal of Innovative Computing, Information and Control, vol. 6, pages 2181-2188, 2010.
12. C.T., Li, M.S. Hwang, An efficient biometrics-based remote user authentication scheme using smart cards, Journal of Network and Computer Applications, vol. 33, pages 1-5, 2010.
13. L.H. Li, I.C. Lin, M.S. Hwang, A remote password authentication scheme for multi-server architecture using neural networks, IEEE Transactions on Neural Networks, vol. 12, pages 1498-1504, 2001.
14. X. Li, J. Niu, M. K. Khan, and J. Liao, "An enhanced smart card based remote user password authentication scheme," Journal of Network and Computer Applications, in press. (http://dx.doi.org/10.1016/j.jnca.2013.02.034.)

15. I.C. Lin, M.S. Hwang, L.H. Li, A new remote user authentication scheme for multi-server architecture, Future Generation Computer Systems, vol. 19, pages 13-22, 2003.
16. Jie Ling, Guangqiang Zhao, "An Improved Anonymous Password Authentication Scheme Using Nonce and Bilinear Pairings", International Journal of Network Security, Vol. 17, No. 6, pp. 787-794, 2015.
17. Yanjun Liu, Chin-Chen Chang and Shih-Chang Chang, An Efficient and Secure Smart Card Based Password Authentication Scheme, International Journal of Network Security, Vol. 19, No. 1, pp. 1-10, 2017.
18. Yanrong Lu, Xiaodong Yang, and Xiaobo Wu, "A Secure Anonymous Authentication Scheme for Wireless Communications Using Smart Cards", International Journal of Network Security, Vol. 17, No. 3, pp. 237-245, 2015.
19. Eric Opoku Osei, James Benjamin Hayfron-Acquah, "Cloud Computing Login Authentication Redesign", International Journal of Electronics and Information Engineering, Vol. 1, No. 1, pp. 1-8, 2014.
20. A. Prakash, A biometric approach for continuous user authentication by fusing hard and soft traits, International Journal of Network Security, vol. 16, pages 65-70, 2014.
21. J.J. Shen, C.W. Lin, M.S. Hwang, Security enhancement for the timestamp-based password authentication scheme using smart cards, Computers & Security, vol. 22, pages 591-595, 2003.
22. J.J. Shen, C.W. Lin, M.S. Hwang, A modified remote user authentication scheme using smart cards, IEEE Transactions on Consumer Electronics, vol. 49, pages 414-416, 2003.
23. Martin Stanek, "Weaknesses of Password Authentication Scheme Based on Geometric Hashing", International Journal of Network Security, Vol. 18, No. 4, pp. 798-801, 2016.
24. H. Tang, X. Liu, L. Jiang, A robust and efficient timestamp-based remote user authentication scheme with smart card lost attack resistance, International Journal of Network Security, vol. 15, pages 446-454, 2013.
25. Ying Wang and Xinguang Peng, "Cryptanalysis of Two Efficient Password-based Authentication Schemes Using Smart Cards", International Journal of Network Security, Vol. 17, No. 6, pp. 728-735, 2015.
26. Jianghong Wei, Wenfen Liu, Xuexian Hu, "Secure and Efficient Smart Card Based Remote User Password Authentication Scheme", International Journal of Network Security, Vol. 18, No. 4, pp. 782-792, 2016.
27. Heri Wijayanto, Min-Shiang Hwang, "Improvement on Timestamp-based User Authentication Scheme with Smart Card Lost Attack Resistance", International Journal of Network Security, Vol. 17, No. 2, 2015, pp. 160-164, 2015.
28. C.C. Yang, T.Y. Chang, M.S. Hwang, The security of the improvement on the methods for protecting password transmission, Informatica, vol. 14, pages 551-558, 2003.
29. Hongfeng Zhu, Yifeng Zhang, and Yan Zhang, "A Provably Password Authenticated Key Exchange Scheme Based on Chaotic Maps in Different Realm", International Journal of Network Security, Vol. 18, No. 4, pp. 688-698, 2016.
30. X. Zhuang, C.C. Chang, Z.H. Wang, Y. Zhu, A simple password authentication scheme based on geometric hashing function, International Journal of Network Security, vol. 16, pages 271-277, 2014.