An Improved Password Authentication Scheme for Smart Card

Cheng-Yi Tsai[1], Chiu-Shu Pan[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. One of technologies to guarantee that only the legal users can access resources from the remote server is user authentication scheme. Many user authentication schemes are based on the use of smart card to withstand replay attack and password guessing attacks in last decades. Recently, Huang et al. proposed a timestamp-based user authentication with smart card. Their scheme is more secure and efficient 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 password guessing attack. Finally, we will propose an improved scheme to eliminate the security vulnerability. Furthermore, the improved scheme could be used in the multi-server environments.

Keywords: Password, Smart Card, Timestamp, User Authentication

1 Introduction

One of technologies to guarantee that only the legal users can access resources from the remote server is user authentication scheme. There are many user authentication schemes have been proposed to authenticate the remote users [1-9]. Some of these schemes are based on smart card to withstand replay attack and password guessing attacks in last decades [10-24]. Some of these schemes are used for multi-server environments [25-29].

Recently, Huang et al. proposed a timestamp-based user authentication with smart card [30]. Their scheme is an improved of Awasthi et al.'s scheme [30] which will be suffer impersonated attack and don't allow changing password freely for the user. They claimed their scheme is more secure and efficient than other schemes. However, we find the security of their scheme is also existed. In this article, we will prove their

adfa, p. 1, 2011.

scheme is vulnerable to the password guessing attack when the user U loses his/her smart card. Finally, we will propose an improved scheme to eliminate the security vulnerability. Furthermore, the improved scheme could be used in the multi-server environments.

2 Review of Huang-Chang-Yu Scheme

There are three participants in Huang-Chang-Yu'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 four phases, namely the initialization phase, registration phase, the login and authentication phase, and the updated password phase [30].

Initialization Phase: In this phase, the KIC generates e, d, n, and g. Here, n=p q, which p and q are two large primes; e and d are the system's public key and private key, respectively.

Registration Phase: In this phase, the KIC make a smart card for a new user (U_i). The smart card contains four parameters, {n, e, S_i, ID_i}, where $Si=(CID_i^d \bmod n) \oplus f(PW_i)$; $CID_i = f(ID_i \oplus d)$; f() denotes a one-way function; ID_i and PW_i are user's identity and password, respectively.

Login and Authentication Phase: In this phase, a user (Ui) wants to login the system via public Internet. The user Ui does the following steps:

1) The user U_i sends the login request parameters, M={n, e, T_c, Y_i, ID_i}, to the server S. Here, $Y_i = X_i f(ID_i, T_c) \bmod n$; $X_i=S_i \oplus f(PW_i)$; T_c denotes the current timestamp of the client.

2) Upon receiving the login request with M={n, e, T_c, Y_i, ID_i}. The server checks whether ID_i is in a correct format or not and whether T_c is the current time stamp of the server with a reasonable time delay threshold or not. If it's not hold, the server rejects this login request.

3) The server computes $CID_i = f(ID_i \oplus d)$ and verifies $(Y_i)^e =? f(ID_i \oplus d)f(ID_i, T_c) \bmod n$. If it holds, the server accepts the login request; otherwise, the server stops this procedure.

4) The server sends M' = {R, T_s} to the user U_i, where $R=f(ID_i, T_s)^d \bmod n$; T_s denotes a timestamp of the server.

5) Upon receiving the parameter M', the server checks whether T_s is the current time stamp of the client with a reasonable time delay threshold or not. If it's not hold, the server rejects this login request.

6) The user U_i checks whether the equation $R^e \bmod n =? f(ID_i, T_s)$ or not. If it holds, U_i authenticates the server is a legal server.

3 Cryptanalysis of Huang-Chang-Yu Scheme

In this section, we will show that Huang-Chang-Yu's user authentication scheme [30] cannot withstand the password guessing attack when the user U_i loses his/her smart card. If an attacker steals a user's smart card, he/she could try to guess the user password. Next, we show that Zhuang-Chang-Wang-Zhu's scheme cannot withstand the password guessing attack as follows.

Step1. The attacker inserts the smart card to client and then inputs the user identity U_i and a guessing password PW_i.

Step2. The attacker monitors and intercepts between the server and client. If the server sends $M' = \{R, T_s\}$ to the user U_i, this means the guessing password is correct; otherwise the guessing password is incorrect.

Step3. If the guessing password is incorrect, the attacker guesses the other password and repeats the Steps 1 – 2.

In addition to the vulnerable to the password guessing attack, Huang-Chang-Yu's user authentication scheme is only used in single server.

4 The Proposed Scheme

In order to eliminate the security vulnerability of Huang-Chang-Yu's user authentication scheme, we will propose an improved user authentication scheme for multi-server environments in this section. Like Huang-Chang-Yu's scheme, there are also three participants: KIC, a server S, and a user U; and four phases in the proposed scheme: initialization phase, registration phase, the login and authentication phase, and the updated password phase [30]. The initialization and the updated password phases of the improved scheme are the same as that of Huang-Chang-Yu's scheme.

The Registration Phase: In this phase, a new user U_i wants to join the system for getting the service on the server S_j. There are three steps in the registration phase. The registration phase is executed as follows.

1) The user U_i sends his/her identity ID_i to the server S_j (j = 1, 2, …, w). The server S_j computes $TID_{ij} = f(ID_i \oplus d_j)$. Then, the server returns TID_{ij} to the user. Here, TID_{ij} denotes the user U_i's temporary identity on the server S_j; and d_j is the server S_j's secret key.

2) The user U_i sends the TID_{ij} (j = 1, 2, …, w) to KIC. KIC make a smart card for the new user U_i. The smart card contains four parameters, {n, e, ID_i, K_{ij}, j = 1, 2, …, w}, where $K_{ij}=(TID_{ij})^d \mod n$.

3) The user U_i computes $TK_{ij} = K_{ij} \oplus f(PW_i)$ and stores TK_{ij} into the smart card. Here, TK_{ij} denotes a token for the user U_i getting the service on the server S_j. Notes, the password only known by the user. KIC and the server S_j do not know the password.

The Login Phase: In this phase, a user (U_i) wants to login the system via public Internet. The user U_i executes the login phase as follows and illustrated in Figure 2.

1) The user U_i inserts his/her smart card and inputs his/her ID_i and password PW_i to the smart card. The smart card checks K_{ij} =? $TK_{ij} \oplus f(PW_i)$. If the equation holds, this means the password is correct; otherwise the password is incorrect. The user needs to input his/her password again and repeats this step for at most three times. After three times fails, the smart card will be locked.

2) The user U_i sends the login request parameters, M={n, e, T_c, Y_i, ID_i}, to the server S_j. Here, $Y_i = K_{ij}^{f(IDi, Tc)} \bmod n$; T_c denotes the current timestamp of the client.

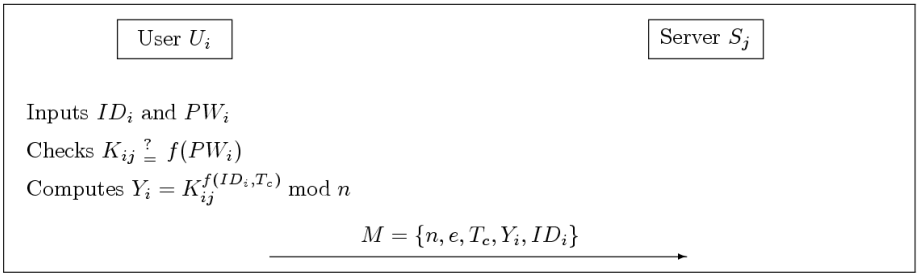

Figure 2: The login phase of the proposed scheme

The Authentication Phase: Upon receiving the login request with M={n, e, T_c, Y_i, ID_i} from user U_i, the server verifies the user in this phase as follows.

1) The server checks whether ID_i is in a correct format or not and whether T_c is the current time stamp of the user with a reasonable time delay threshold or not. If it's not hold, the server rejects this login request.

2) The server computes $TID_{ij} = f(ID_i \oplus d_j)$ and verifies $(Y_i)^e$ =? $f(ID_i \oplus d_j)^{f(IDi, Tc)} \bmod n$. If it holds, the server accepts the login request.

3) The server sends M' = {Z_i, S_j, T_s} to the user U_i, where $Z_i = f(ID_i \oplus d_j)^{f(Sj, Ts)} \bmod n$; T_s denotes a timestamp of the server.

4) Upon receiving the parameter M', the user checks whether T_s is the current time stamp of the server with a reasonable time delay threshold or not. If it's not hold, the user rejects this mutual authentication between the user and the server.

5) The user U_i checks whether the equation Z_i =? $(TID_{ij})^{f(Sj, Ts)} \bmod n$. If it holds, U_i authenticates the server is a legal server.

5 Conclusion

We have shown that there is a leak in Huang-Chang-Yu'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 for multi-server environments.

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.

6 References

1. 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.
2. 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.
3. 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.
4. 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.
5. 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.
6. 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.
7. Martin Stanek, "Weaknesses of Password Authentication Scheme Based on Geometric Hashing", International Journal of Network Security, Vol. 18, No. 4, pp. 798-801, 2016.
8. 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.
9. 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.
10. 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.
11. 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.
12. 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.
13. 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.
14. R. Ramasamy, A.P. Muniyandi, An efficient password authentication scheme for smart card, International Journal of Network Security, vol. 14, pages 180-186, 2012.

15. 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.
16. 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.
17. 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.
18. R.C. Wang, C.C. Yang, Cryptanalysis of two improved password authentication schemes using smart cards, International Journal of Network Security, vol. 3, pages 283-285, 2006.
19. 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.
20. 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.
21. 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.
22. 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.
23. 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.
24. 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.
25. 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.
26. 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.
27. 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.
28. 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.
29. 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.
30. 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
31. K. Awasthi, K. S. Srivastava, and R. C. Mittal, “An improved timestamp-based remote user authentication scheme,” Computers and Electrical Engineering, vol. 37, pp. 869-874, 2011.