An Improved Hou-Wang's User Authentication Scheme

Min-Shiang Hwang[1,2], Hung-Wei Yang[1], and Cheng-Ying Yang[3]

[1]Department of Computer Science & Information Engineering, Asia University, Taiwan
[2]Depart. of Medical Research, China Medical Univ. Hospital, China Medical Univ., Taiwan
[3]Department of Computer Science, University of Taipei, Taiwan
cyang@utaipei.edu.tw

Abstract. It's easy to access Internet resources in the cloud environment. And it's important to protect the legal users' privacy and confidentiality. Recently, Hou and Wang proposed a robust and efficient user authentication scheme based on elliptic curve cryptosystem. Their scheme was practical and easy to implement. They claimed that their scheme could against off-line password guessing, DoS, server spoofing, replay, parallel session and impersonation attacks. In this article, we will show that Hou-Wang's scheme is vulnerable to the guessing attack with smart card. In this article, we also propose an improved Hou-Wang's user authentication scheme to withstand the vulnerability in their scheme.

Keywords: Password, Smart Card, User Authentication.

1 Introduction

It's easy to access Internet resources in the cloud environment. In order to protect the users could have the access right to obtain the resources provided by the remote server, the remote user authentication schemes were proposed [1-11]. Furthermore, it's also important to protect the legal users' privacy and confidentiality. To authenticate a user from Internet, many user authentication schemes had been proposed in past decades. Many schemes were applied a smart card to authenticate the legal users [12-21]. One of these schemes was developed for multi-servers [22-27]. One of these schemes was developed for biometrics [28-30]. One of these schemes was applied passwords for generating session key [31-32].

In 2012, Li, Liu, and Wu proposed a secure remote user authentication to withstand the spoofing attack, forgery attack, and password guessing attack [33]. Unfortunately, Feng, Chao, and Hwang found the security of Li-Liu-Wu's scheme was vulnerable to password guessing attacks [34]. In 2012, Yoon et al. proposed an efficient remote user authentication scheme [35]. Unfortunately, Chen, Liang, and Hwang found their scheme is insecure to against the password guessing attack [36]. In 2014, Huang, Chang, Yu proposed a user authentication scheme which is based on timestamp [37]. Huabg et al. claimed their scheme could withstand the impersonated attack and more secure than other schemes. However, Feng, Liang, Hwang found that their scheme was vulnerable to the legal user's smart card and password guessing attack [38].

Recently, Hou and Wang proposed a robust and efficient user authentication scheme based on elliptic curve cryptosystem [39]. Hou-Wang's scheme is practical. They claimed that their scheme could against the off-line password guessing, DoS, spoofing, replay, parallel session, and impersonation attacks. In this article, we will show that Hou-Wang's scheme is vulnerable to the guessing attack with smart card. In this article, we also propose an improved Hou-Wang's user authentication scheme to withstand the vulnerability in their scheme.

2 Review of Hou-Wang Scheme

There are two main participants in Hou-Wang's scheme: a user U_i and server S [39]. We briefly describe Hou-Wang's scheme as follows.

The Registration Phase. In this registration phase, a new user (U_i) needs to apply to the server for as a legal user. After the phase, the server will make and issue a smart card for the new user (U_i). The smart card contains the following five parameters: {B_i, H(), G, E_k(), and D_k()}, here $B_i = E_{Ai}(H(x \| n_i) \| n_iG)$; $A_i = H(ID_i \| PW_i)$; where H() denotes a hash function; ID_i and PW_i denote an identity and password of the new user, respectively. x and n_i denote a server's master secret key and a random number for U_i, respectively. G denotes a public base point of elliptic curve; E_k() and D_k() denote an enciphering and deciphering algorithms with the secret key k, respectively. The server S maintains and keeps a registration table with two columns: $H(ID_i \oplus x)G$ and n_i.

The Login Phase. In this phase, when the user (U_i) wants to have the access right to obtain the resources provided by the remote server, U_i keys in his/her identity (ID_i) and password (PW_i) to the client devise with smart card. The smart card sends {C_i, D_i} to the server S: Ai = $H(ID_i \| PW_i)$; $B_i = E_{Ai}(H(x \| n_i) \| n_iG)$; $H(x \| n_i) \| n_iG = D_{Ai}(B_i)$; C_i = t G; K_i = t Pub_s; $D_i = E_{Ki}(ID_i \| H(x \| n_i))$, where t denotes a random nonce in Z_p*. Pubs is the server's public key, Pub_s = x G.

The Authentication and Session Key Exchange Phase. In this authentication and session key exchange phase, the server (S) verifies U_i as follows.

1) After receiving {C_i, D_i}, the server calculates and obtains the deciphering key K_i, U_i, and $H(x \| n_i)$ as follows: $K'_i = x\ C_i$; $ID'_i \| H(x'\|n'_i) = D_{K'i}(D_i)$. Next, S computes $H(ID'_i \oplus x)G$ and retrieves the random number ni of U_i from the registration table.
2) S computes $H(x \| n_i)$ and then verifies $H(x \| n_i)$ is whether or not equal to $H(x' \| n'_i)$. If it is not holds, S terminates this phase. Next, S sends {E_i, F_i} to U_i, where E_i = s G; $F_i = s\ C_i + n_i\ G$, where s denotes a random nonce in Z_p*.
3) The smart card checks E_i and F_i. The server also authenticates the legal user. Finally, the server and smart card share the session key SK = stG.

3 The Weakness and the Improved of Hou-Wang Scheme

In this section, we show the weakness of Hou-Wang's remote user authentication scheme [39]. The main weakness of Hou-Wang's scheme is that their scheme could not against the on-line password guessing attack with user's smart card (SC for short). A user U_i's smart card may be lost or stolen by an adversary. The adversary could try to guess the user's password.

1). The adversary inserts the user U_i's smart card to his/her client device. Next, the adversary keys in the identity of the user U_i and guesses a password PW'_i.

2). SC sends $\{C_i, D_i\}$ to the server S: $A'_i = H(ID_i \| PW'_i)$; $B_i = E_{Ai}(H(x \| n_i) \| n_iG)$; $H'(x \| n_i) \| n'_iG = D_{A'i}(B_i)$; $C_i = t\,G$; $K_i = t\,Pub_s$; $D_i = E_{Ki}(ID_i \| H'(x \| n_i))$.

3). The server performs Steps 1) and 2) in the authentication and session key exchange phase to verify the user (adversary) legally. If the guessing password by the adversary is correct, the adversary will receive $\{E_i, F_i\}$ from the server. Otherwise, the adversary guesses the other password PW'_i and repeats Step 1).

In order to improve the weakness of Hou-Wang's remote user authentication scheme, we propose an improvement of Hou-Wang's scheme in this section. The password changing and the smart revocation phases are the same as that in Hou-Wang's scheme.

The Registration Phase. In this phase, a new user (U_i) needs to apply to the server for as a legal user. After the phase, the server will make and issue a smart card for U_i. The smart card contains $\{B_i, H(), G, E_k(), \text{and } D_k()\}$, where $B_i = E_{Ai}(H(x \| n_i) \| n_iG)$; $A_i = H(ID_i \| PW_i)$. The server S maintains and keeps a registration table with three columns: $H(ID_i \oplus x)G$, ni, and counter (see Table 1). The counter is used to record the times of failing to login the server.

Table 1. The registration table.

User's Identity	Nonce	Counter
$H(ID_1 \oplus x)G$	n_1	0
$H(ID_2 \oplus x)G$	n_2	2
:	:	:
$H(ID_i \oplus x)G$	n_i	1
:	:	:
$H(ID_m \oplus x)G$	n_m	0

The Login Phase. This phase is similar to that of Hou-Wang scheme. In this phase, when U_i wants to have the access right to obtain the resources provided by the remote server, U_i keys in his/her identity (ID_i) and inputs his/her password (PW_i) to the client devise with smart card. The smart card sends $\{C_i, D_i\}$ to the server S: $A_i = H(ID_i \| PW_i)$; $H(x \| n_i) \| n_iG = D_{Ai}(B_i)$; $C_i = t\,G$; $K_i = t\,Pub_s$; $D_i = E_{Ki}(ID_i \| H(x \| n_i))$.

The Authentication and Session Key Exchange Phase. In this authentication and session key exchange phase, S verifies Ui as follows (see Fig. 1).

1). After receiving $\{C_i, D_i\}$, the server calculates and obtains the deciphering key K_i, the U_i identity, and $H(x \| n_i)$ as follows: $K'_i = x\,C_i$; $ID'_i \| H(x' \| n'_i) = DK'_i(D_i)$.

2). S computes $H(ID'_i \oplus x)G$ and retrieves the random number n_i of U_i from Table 1.

3). S computes $H(x \| n_i)$ and then verifies $H(x \| n_i)$ is whether or not equal to $H(x' \| n'_i)$. If it is not holds, the server stops this procedure and adds 1 to the counter in Table 1. If the counter is greater than 3, the server removes the user's information from registration table. The user needs to re-makes a registration for sharing the server's resource.

4). The server S sends {E_i, F_i} to the user U_i, where E_i = s G; F_i = s C_i + n_i G, where s denotes a random nonce in Z_p*.

5). The smart card computes F'_i = tE_i + n_i and then checks F'_i is whether or not equal to F_i. If it holds, computes and sends the verification message R_i to the server: R_i = H(tE_i || E_i || C_i).

6). The server computes R'_i = H(sC_i || E_i || C_i) and checks R'_i whether equal to R_i. If it holds, S thus authenticates the legal user.

7). The server and the smart card share the session key SK = stG.

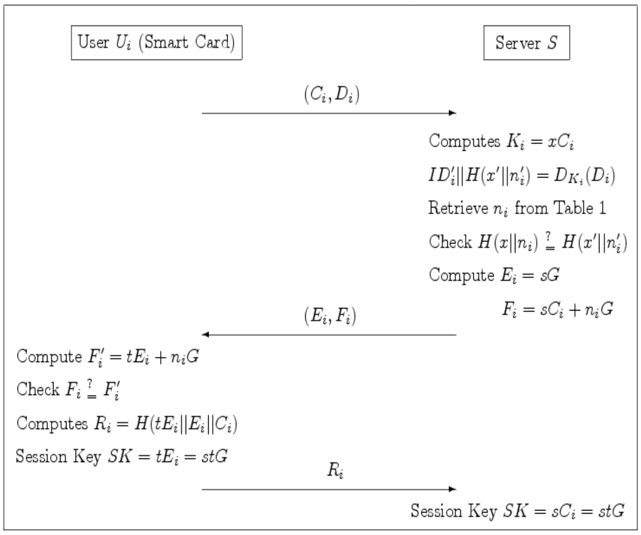
User U_i (Smart Card)
Server S
(C_i, D_i)
Computes $K_i = xC_i$
$ID_i'||H(x'||n_i') = D_{K_i}(D_i)$
Retrieve n_i from Table 1
Check $H(x||n_i) \overset{?}{=} H(x'||n_i')$
Compute $E_i = sG$
$F_i = sC_i + n_iG$
(E_i, F_i)
Compute $F_i' = tE_i + n_iG$
Check $F_i \overset{?}{=} F_i'$
Computes $R_i = H(tE_i||E_i||C_i)$
Session Key $SK = tE_i = stG$
R_i
Session Key $SK = sC_i = stG$

Fig. 1. The authentication and session key exchange phase of our scheme. Subsequent paragraphs, however, are indented.

4 Conclusions

In summary, we have shown that the weakness of Hou-Wang's remote user authentication scheme. Hou-Wang’s scheme could not against the on-line password guessing attack with smart card. In this article, we also proposed an improvement of Hou-Wang’s remote user authentication scheme to improve the weakness in Hou-Wang’s scheme.

Acknowledgments. This work was partially supported by the Ministry of Science and Technology, Taiwan, under grant MOST 106-2221-E-468-002.

References

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

3. Zhuang, X., Chang, C.C., Wang, Z.H., Zhu, Y.: A simple password authentication scheme based on geometric hashing function. International Journal of Network Security 16, 271-277 (2014).
4. Ling, C.H., Chao, W.Y., Chen, S.M., Hwang, M.S.: Cryptanalysis of dynamic identity based on a remote user authentication scheme for a multi-server environment. In: Advances in Engineering Research Vol. 15, pp. 981-986. Atlantis Press (2015).
5. Liu, Y., Chang, C.C., Chang, S.C.: An efficient and secure smart card based password authentication scheme. International Journal of Network Security 19(1), 1-10 (2017).
6. Liu, C.W., Tsai, C.Y., Hwang, M.S.: Cryptanalysis of an efficient and secure smart card based password authentication scheme. In: Advances in Intelligent Systems and Computing, Recent Developments in Intelligent Systems and Interactive Applications, Vol. 541, pp. 188-193, Springer (2017).
7. Wei, J., Liu, W., Hu, X.: Secure and efficient smart card based remote user password authentication scheme. International Journal of Network Security 18(4), 782-792 (2016).
8. Tsai, C.Y., Pan C.S., Hwang, M.S.: An improved password authentication scheme for smart card. In: Advances in Intelligent Systems and Computing, Recent Developments in Intelligent Systems and Interactive Applications, Vol. 541, pp. 194-199, Springer (2017).
9. Thandra, P.K., Rajan, J., Satya Murty, S.A.V.: Cryptanalysis of an efficient password authentication scheme. International Journal of Network Security 18(2), 362-368 (2016).
10. Pan, C.S., Tsai, C.Y., Tsaur, S.C., Hwang, M.S.: Cryptanalysis of an efficient password authentication scheme. In: The 3rd IEEE International Conference on Systems and Informatics, pp. 732-737, Shaihai (2016).
11. Pan, H.T., Pan, C.S., Tsaur, S.C., Hwang, M.S.: Cryptanalysis of efficient dynamic ID based remote user authentication scheme in multi-server environment using smart card. In: 12th International Conference on Computational Intelligence and Security, Wuxi, China, pp. 590-593 (2017).
12. He, D., Chen, J., Hu, J.: Weaknesses of a remote user password authentication scheme using smart card. International Journal of Network Security 13, 58-60 (2011).
13. Hwang, M.S., Chong, S.K., Chen, T.Y.: Dos-resistant ID-based password authentication scheme using smart cards. Journal of Systems and Software. 83, 163-172 (2000).
14. Hwang, M.S., Li, L.H.: A new remote user authentication scheme using smart cards. IEEE Transactions on Consumer Electronics 46, 28-30 (2000).
15. Kumar, M., Gupta, M.K., Kumari, S.: An improved efficient remote password authentication scheme with smart card over insecure networks. International Journal of Network Security 13, 167-177 (2011).
16. Ramasamy, R., Muniyandi, A.P.: An efficient password authentication scheme for smart card. International Journal of Network Security 14, 180-186 (2012).
17. Shen, J.J., Lin, C.W., Hwang, M.S.: Security enhancement for the timestamp-based password authentication scheme using smart cards. Computers & Security 22, 591-595 (2003).
18. Shen, J.J., Lin, C.W., Hwang, M.S.: A modified remote user authentication scheme using smart cards. IEEE Transactions on Consumer Electronics 49, 414-416 (2003).
19. Tang, H., Liu, X., Jiang, L.: A robust and efficient timestamp-based remote user authentication scheme with smart card lost attack resistance. International Journal of Network Security 15, 446-454 (2013).
20. Yang, L., Ma, J.F., Jiang, Q.: Mutual authentication scheme with smart cards and password under trusted computing. International Journal of Network Security 14, 156-163 (2012).
21. Ghosh, D., Li, C., Yang, C.: A lightweight authentication protocol in smart grid. International Journal of Network Security 20(3), 414-422 (2018).

22. Feng, T.H., Ling, C.H., Hwang, M.S.: Cryptanalysis of Tan's improvement on a password authentication scheme for multi-server environments. International Journal of Network Security 16, 318-321 (2014).
23. He, D., Zhao, W., Wu, S.: Security analysis of a dynamic id-based authentication scheme for multi-server environment using smart cards. International Journal of Network Security15, 282-292 (2013).
24. Li, L.H., Lin, I.C., Hwang, M.S.: A remote password authentication scheme for multi-server architecture using neural networks. IEEE Transactions on Neural Networks 12, 1498-1504 (2001).
25. Lin, I.C., Hwang, M.S., Li, L.H.: A new remote user authentication scheme for multi-server architecture. Future Generation Computer Systems 19, 13-22 (2003).
26. Amin, R.: Cryptanalysis and efficient dynamic ID based remote user authentication scheme in multi-server environment using smart card. International Journal of Network Security 18(1), 172-181 (2016).
27. Mohan, N.B.M., Chakravarthy, A.S.N., Ravindranath, C.: Cryptanalysis of design and analysis of a provably secure multi-server authentication scheme. International Journal of Network Security 20(2), 217-224 (2018).
28. Li, C.T., Hwang, M.S.: An online biometrics-based secret sharing scheme for multiparty cryptosystem using smart cards. International Journal of Innovative Computing, Information and Control 6, 2181-2188 (2010).
29. Li, C.T., Hwang, M.S.: An efficient biometrics-based remote user authentication scheme using smart cards. Journal of Network and Computer Applications 33, 1-5 (2010).
30. Prakash, A.: A biometric approach for continuous user authentication by fusing hard and soft traits. International Journal of Network Security 16, 65-70 (2014).
31. Zhu, H., Zhang, Y.: An improved two-party password-authenticated key agreement protocol with privacy protection based on chaotic maps. International Journal of Network Security 19(4), 487-497 (2017).
32. Wu, M., Chen, J., Wang, R.: An enhanced anonymous password-based authenticated key agreement scheme with formal proof. International Journal of Network Security 19(5), 785-793 (2017).
33. Li, J., Liu, S., Wu, S.: Cryptanalysis and improvement of a YS-like user authentication scheme. International Journal of Digital Content Technology and its Applications 7(1), 828-836 (2012).
34. Feng, T.H., Chao, W.Y., Hwang, M.S.: Cryptanalysis and improvement of the Li-Liu-Wu user authentication scheme. In: International Conference on Future Communication Technology and Engineering, pp. 103-106, Shenzhen China (2014).
35. Yoon, E.J., Kim, S.H., Yoo, K.Y.: A security enhanced remote user authentication scheme using smart cards. International Journal of Innovative Computing, Information and Control 8(5), 3661-3675 (2012).
36. Chen, T.Y., Ling, C.H., Hwang, M.S.: Weaknesses of the Yoon-Kim-Yoo remote user authentication scheme using smart cards. In: IEEE Workshop on Electronics, Computer and Applications, Ottawa, Canada, pp. 771-774 (2014).
37. Huang, H.F., Chang, H.W., Yu, P.K: Enhancement of timestamp-based user authentication scheme with smart card. International Journal of Network Security 16, 463-467 (2014).
38. Feng, T.H., Ling, C.H., Hwang, M.S.: An improved timestamp-based user authentication scheme with smart card. In: The 2nd Congress on Computer Science and Application, pp. 111-117, Sanya, China (2014).
39. Hou, G., Wang, Z.: A robust and efficient remote authentication scheme from elliptic curve cryptosystem. International Journal of Network Security 19(6), 904-911 (2017).