Comments on four multi-server authentication protocols using smart card

*Jue-Sam Chou [1], Yalin Chen[2], Chun-Hui Huang [3], Yu-Siang Huang[4]

[1] Department of Information Management, Nanhua University Chiayi 622 Taiwan, R.O.C

*: corresponding author

jschou@mail.nhu.edu.tw

Tel: 886+ (0)5+272-1001 ext.56536

[2] Institute of information systems and applications, National Tsing Hua University
d949702@oz.nthu.edu.tw

[3] Department of Information Management, Nanhua University Chiayi 622 Taiwan, R.O.C

g64451519@mail1.nhu.edu.tw

[4] Department of Information Management, Nanhua University Chiayi 622 Taiwan, R.O.C

cydy80271@gmail.com

Abstract

Recently, researchers have proposed several nice multi-server authentication protocols. They claim that their protocols are secure and can withstand various attacks. However, after reviewing their schemes, we found that they although are perfect whereas flawed. Due to this observation, in this paper, we list the weakness found in these recent literatures.

Keywords: *multi-server, password authentication protocol, smart card, password change, key agreement*

1. Introduction

A two-party password authentication protocol for client-server architecture is usually not sufficient when network size increases, especially for an open network such as Internet. Thus, researchers have proposed several multi-server authentication protocols [1-23] to cope with this problem. In 2003, Li *et al*. [5] proposed a multi-server protocol based on the ElGamal digital signature and geometric transformations on an Euclidean plane. Unfortunately, their protocol is broken by Cao and Zhong [8]. In 2004, Juang *et al*. [13] proposed an efficient multi-server scheme and claimd that their scheme is secure, but Chen *et al.* [24] point out it suffers from smart-card-lost attack. In 2004 and 2005, Tsaur *et al*. [3, 4] proposed two multi-server schemes. However, both of their schemes are based on the Lagrange interpolating polynomial which is computationally intensive, and are broken by Chou *et al.* [16]. In 2006 and 2007, Cao *et al*. [9] and Hu *et al*. [7] each proposed an authentication scheme for a multi-server environment. Both schemes assume that all servers are trustworthy. Nevertheless, this assumption is not always true, as stated in [1]. In 2008, Lee *et al*. [6] proposed an authenticated key agreement scheme for multi-server using mobile equipment. However, their scheme cannot freely add any server. Because when a server is added, all users who want to login to this new server have to re-register at the registration center for obtaining a new smart card. This increases the registration center's card-issue cost. Also, in 2008, Tsai [1] proposed an efficient multi-server authentication scheme and claimed that his protocol can withstand seven known attacks. Yet, Chen *et al.* [15] and Wang *et al.* [17] finds it is vulnerable to the server spoofing attack. In addition, Tsaura *et al.* [21] also find it is vulnerable to the man-in-the-middle attack**.** In 2009, Liao *et al*. [2] proposed a secure dynamic ID scheme for multi-server environment. They claimed their protocol is secure. However, Chen *et al.* [15] and Hsiang and Shih [14] both find it suffers server spoofing attack by an insider server. Further, [14] propose an improvement on the protocol. In recent two years, litratures [19-22] each not only point out the security flaws in previous schemes (as stated above) but also propose a secure protocol in multi-server environment. Lee *et al.* [19] and Sood *et al.* [20] both find the improvement in [14] is still insecure In 2011. Tsaura *et al.* [21] pointed out [13] have man-in-the-middle attack, and Li *et al.* [22] indicated that [20] has leak-of-verifier attack and stolen smart card attack in 2012. Finally also in 2012, Hwang *et al.* [18] propose an improved multi-server authentication protocol based on bilinear pairings, and Liao *et al.* [23] propose a novel multi-server authentication scheme for mobile clients. However, after examining schemes [19-23], this study found there still existing some deficiency in each proposal. In this paper, we will first show the deficiencies found, then show our scheme and examine its security.

The rest of this paper is organized as follows: Section 2 demonstrates the vulnerabilities existing in schemes [19-23]. Section 3 demonstrates a novel protocol and Section 4 analyzes its security. The discussions and comparisons are made in Section 5. Finally, a conclusion is given in Section 6.

2. Deficiencies in literatures [19-23]

In this section, we demonstrate the deficiency in each scheme.

- Lee *et al.*'s protocol **[19]**

Lee *et al.*'s protocol is a secure dynamic ID based scheme, but might suffer insider attak. Because any insider server has the secrecy h(x || y) and h(y), a malicious insider server S_m can intercept the message $\{CID_i, P_{ij}, Q_i, N_i\}$ sent from the user, and calculate $T_i = P_{ij} \oplus h(h(y) \| N_i \| SID_j)$ and $A_i = h(T_i \| h(y) \| N_i)$. Consequently, S_m can obtain $h(b \oplus PW_i)$ by computing $CID_i \oplus h(T_i \| A_i \| N_i)$, and then computes $B_i = h(h(b \oplus PW_i) \| h(x \| y))$. Then, S_m can masquerade as the user to login any server by generating a random N_i' and computing the corresponding login message.

- Sood *et al.***'s** protocol **[20]**

Li et al. [22] indicate that [20] suffers leak-of-verifier attack, stolen smart card attack, and has incorrect authentication and session key agreement phase.

- Tsaur *et al.***'s** protocol **[21]**

  Tsaur et al.'s protocol suffers the smart card lost password guessing attack. Because if the attacker intercepted M_{ij} = { E_T_{ij}, A_{ij}, UID_i, Ev_{ij} (ru_k , $h(UID_i)$)}, then from the stored values {UID_i, μ_i , E_T_{ij} , and A_{ij}} in the smart card, he can guess UID_i's password PW_i as gpw and compute h(gpw). He computes hUID'=$h(UID_i)$, and calculates v_i '=$\mu_i \oplus h(gpw)$ and v_{ij} '=$h(v_i$ ', $SID_j)$ to decrypt Ev_{ij} (ru_k , $h(UID_i)$) in M_{ij}. He verifies whether $h(UID_i)$ in the decryption result is equal to the computed hUID'. If it is, the attacker can confirm that the user's password is gpw.

- Li *et al.*'s protocol [22]

  Li *et al.*'s protocol is efficient and secure, but it maight suffer impersonation attack. We describe the reasons as follows:

  From the values D_i, b, h(y), C_i, D_i, and E_i stored in the smart card, a user ID_i can obtain $h(y \| x)$ by first computing $A_i = h(b \| P_i)$ and $B_i = D_i \oplus h(ID_i \| A_i)$, where P_i is ID_i's password. Then, after S_j has sent login message (F_i, G_i, P_{ij}, CID_i, SID_j, K_i, M_i) to CS, ID_i can obtain $h(y \| x)$ by computing $B_i \oplus P_{ij} \oplus h(h(y) \| N_{i1} \| SID_j)$, where N_{i1} is a random number generated by the smart card and $P_{ij} = E_i \oplus h(h(y) \| N_{i1} \| SID_j)$. On the other hand, when acting as an attacker, from the login request message sent from S_j to the CS, an insider having h(y) stored in the smart card can compute ID_i's relevant parameters $N_{i1} = h(y) \oplus F_i$, $E_i = P_{ij} \oplus h(h(y) \| N_{i1} \| SID_j)$, $B_i = E_i \oplus h(y \| x)$, and $A_i = CID_i \oplus h(B_i \| F_i \| N_{i1})$. After obtaining A_i , B_i, E_i, and N_{i1}, the insider computes $h(A_i \| B_i \| N_{i1})$ and $(N_{i2} \oplus N_{i3}) = T_i \oplus h(A_i \| B_i \| N_{i1})$, where $T_i = N_{i2} \oplus N_{i3} \oplus h(A_i \| B_i \| N_{i1})$ is in the submitted message from CS to server S_j. Then, the insider can compute the session key $sk = h(h(A_i \| B_i) \| (N_{i1} \oplus N_{i2} \oplus N_{i3}))$. Moreover, for possessing A_i , B_i, E_i, the insider can gererate a random N_{i1}', compute $F_i = h(y) \oplus N_{i1}'$, $G_i = h(B_i \| A_i \| N_{i1}')$, $P_{ij} = E_i \oplus h(h(y) \| N_{i1}' \| SID_j)$, and $CID_i = A_i \oplus h(B_i \| F_i \| N_{i1}')$. That is, even though the insider does not know whom CID_i stands for, the insider can impersonate a legal user to login to the server successfully. Besides, it requires that the CS must be kept on-line. This might cause the CS to be a bottleneck in the system.

- Liao *et al.*'s protocol [23]

  Liao et al. proposed a perfect multi-server scheme for mobile clients, but a deficiency of suffering password guessing attack may exist. Because, once the smart card of a user is lost, an insider server, who knows the user's ID_i and T_i (in the ID table sent from the register server RS to all the service servers periodically over a secure channel), the value set $\{ID_i, RegID_i, b_i\}$ stored in the smart card, and has ever intercepted the user's login message (ID_i, M_i, B_{ij}, R_i) to the service server SS_j, can launch a password guessing attack. We depict the scenario as follows. The insider server guesses a password gpw, computes $DIDi = RegID_i \oplus h(gpw \| b_i) \cdot Pub_{RS}$, $d_{ij} = h(ID_i \| SID_j \| M_i \| R_i)$, and $B_{ij} - d_{ij} \cdot DID_i = r_i \cdot DID_i$. He then can confirm the correctness of gpw by verifying whether equation $e(r_i \cdot DID_i, P) = e(M_i, T_i \cdot Pub_{RS})$ holds. If it does, the insider server can assure that the password gpw he guesses is right. We deduce the equation as follows.

  $e(r_i \cdot DID_i, P) = e(r_i \cdot Tis_{RS} \cdot QID_i, P) = e(r_i \cdot QID_i, Tis_{RS} \cdot P) = e(M_i, T_i \cdot Pub_{RS})$,

  where $DID_i = (Ti \cdot s_{RS}) \cdot QID_i$ is computed by RS in user registration phase.

3. Conclusion

In this article, we have listed the weakness in recent four studies in multi-server environment. The analyses show that these schemes are deficient and need futher improvement.

References

[1] J.L. Tsai, "Efficient multi-server authentication scheme based on one-way hash function without verification table," *Computers & Security*, Vol. 27, No. 3-4, pp. 115-121, May-June 2008.

[2] Y.P. Liao, S.S. Wang, "A secure dynamic ID based remote user authentication scheme for multi-server environment," *Computer Standards & Interfaces*, Vol.

31, No. 1, pp. 24-29, January 2009.

[3] W.J. Tsaur, C.C. Wu, W.B. Lee, "An enhanced user authentication scheme for multi-server Internet services," *Applied Mathematics and Computation*, Vol. 170, No. 1-1, pp. 258-266, November 2005.

[4] W.J. Tsaur, C.C. Wu, W.B. Lee, "A smart card-based remote scheme for password authentication in multi-server Internet services," *Computer Standards & Interfaces*, Vol. 27, No. 1, pp. 39-51, November 2004.

[5] 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, No. 1, pp. 13-22, January 2003.

[6] J. H. Lee, D. H. Lee, "Efficient and Secure Remote Authenticated Key Agreement Scheme for Multi-server Using Mobile Equipment," *Proceedings of International Conference on Consumer Electronics*, pp. 1-2, January 2008.

[7] L. Hu, X. Niu, Y. Yang, "An Efficient Multi-server Password Authenticated Key Agreement Scheme Using Smart Cards," *Proceedings of International Conference on Multimedia and Ubiquitous Engineering*, pp. 903-907, April 2007.

[8] X. Cao, S. Zhong, "Breaking a remote user authentication scheme for multi-server architecture," *IEEE Communications Letters*, Vol. 10, No. 8, pp. 580-581, August 2006.

[9] Z.F. Cao, D.Z. Sun, "Cryptanalysis and Improvement of User Authentication Scheme using Smart Cards for Multi-Server Environments," *Proceedings of International Conference on Machine Learning and Cybernetics*, pp. 2818-2822, August 2006.

[10] C.C. Chang, J.Y. Kuo, "An efficient multi-server password authenticated key agreement scheme using smart cards with access control," *Proceedings of International Conference on Advanced Information Networking and Applications*, Vol. 2, No. 28-30, pp. 257-260, March 2005.

[11] R.J. Hwang, S.H. Shiau, "Password authenticated key agreement protocol for multi-servers architecture," *Proceedings of International Conference on Wireless Networks*, Vol. 1, No. 13-16, pp. 279-284, June 2005.

[12] C.C. Chang, J.S. Lee, "An efficient and secure multi-server password authentication scheme using smart cards," *Proceedings of International Conference on Cyberworlds*, No. 18-20, pp. 417-422, November 2004.

[13] W.S. Juang, "Efficient multi-server password authenticated key agreement using smart cards," *IEEE Transactions on Consumer Electronics*, Vol. 50, No. 1, pp. 251-255, February 2004.

[14] H.C. Hsiang, W.K. Shih, "Improvement of the secure dynamic ID based remote

user authentication scheme for multi-server environment," Computer Standards & Interfaces, Volume 31, Issue 6, November 2009, Pages 1118 – 1123.

[15] Y. Chen, C.H. Huang, J.S. Chou, "Comments on two multi-server authentication protocols," http://eprint.iacr.org/2008/544, December 2008.

[16] J.S. Chou, C.H. Huang, Y. Chen, "Cryptanalysis on two multi-server password based authentication protocols," *International Journal of Computer Science and Information Security*, Vol. 8, No. 2, pp. 16-20, MAY 2010.

[17] R.C. Wang, W.S. Juang, and C.L. Lei, "User Authentication Scheme with Privacy-Preservation for Multi-Server Environment," *IEEE Communications Letters*, Vol. 13, No. 2, pp. 157-159, February 2009

[18] C.H. Huang, J.S. Chou, Y. Chen, "Improved multi-server authentication protocol" *International journal of Security and Communication Networks*, Volume 5, Issue 3, pages 331–341, March 2012

[19] C.C. Lee, T.H. Lin, R.X. Chang, "A secure dynamic ID based remote user authentication scheme for multi-server environment using smart cards," *Expert Systems with Applications* 38 (2011) 13863–13870

[20] S.K. Sood, A. K. Sarje, K. Singh, "A secure dynamic identity based authentication protocol for multi-server architecture," *Journal of Network and Computer Applications* 34 (2011) 609–618

[21] W.J. Tsaura, J.H. Li, W.B. Lee, "An efficient and secure multi-server authentication scheme with key agreement," *The Journal of Systems and Software* 85 (2012) 876–882

[22] X. Li, Y. Xiong, J. Ma, W. Wang, "An efficient and security dynamic identity based authentication protocol for multi-server architecture using smart cards," *Journal of Network and Computer Applications* 35 (2012) 763–769

[23] Y.P. Liao, C.M. Hsiao, "A novel multi-server remote user authentication scheme using self-certified public keys for mobile clients'" *Future Generation Computer Systems*, article in press