Cryptanalysis of Tan's Improvement on a Password Authentication Scheme for Multi-server Environments

Tung-Huang Feng[1], Chung-Huei Ling[1], and Min-Shiang Hwang[1,2]
(Corresponding author: Min-Shiang Hwang)

Department of Computer Science & Infoarmation Engineering, Asia University[1]
No. 500, Lioufeng Raod, Wufeng Shiang, Taichung, Taiwan, R.O.C.
Department of Health Services Administration, China Medical University[2]
(Email: mshwang@asia.edu.tw)
(Received Apr. 2, 2014; revised and accepted May 6, 2014)

Abstract

Smart cards have been applied on password authentication in recent years. A user can input his/her identity and password to require services from the remote server. There are various attacks through an insecure network to obtain a user's information. Therefore, many schemes are proposed to guarantee secure communication. However, a lot of schemes are not secure. Recently, Tan proposed an improved password authentication using a smart card for multi-server environments. In this paper, we show the weakness of Tan's scheme, and his scheme cannot resist a password guessing attack.

Keywords: Authentication, multi-server, password

1 Introduction

As Internet development is rapidly fast, a user can obtain various services from a server through Internet. However, transferring information between users and servers through an insecure network may suffer some attacks [4, 5, 6, 13, 19]. Using password authentication with a smart card is an efficient scheme to support these services. In 1981, Lamport [15] proposed an approach which can use the password to authenticate between a user and a remote server. After that, a series of studies [8, 11, 13, 14, 17, 31, 32, 34, 35]. have been researched on password authentication using a smart cart based on a remote server. However, a user wants to get some services from different remote servers, he/she needs to use a different password to login a different server. Some researches use the neural network to authenticate with password [22, 27]. Some researches are to authenticate with password in multi-server environments [2, 3, 28]. Some schemes are based on public cryptosystems [7, 36]. Some schemes are based on hash function and symmetric cryptosystems [25, 26, 29, 40, 41, 42]. There are some biometrics-based remote user authentication schemes [20, 21, 30]. Some schemes are based on identification cryptosystems [1, 12, 24].

Many schemes [10, 18, 23, 37, 38] proposed result in insecure problems between a user and a server. In recent years, Wang et al. [39] proposed a password authentication key agreement scheme using a smart card for multi-servers, and this scheme is based on quadratic residue. In addition, Tan [33] found out Wang et al.'s scheme can't withstand an impersonation attack, and doesn't provide perfect forward security. Tan proposed an improvement scheme based on Diffie-Hellman assumptions [9, 16]. However, we find out Tan's scheme cannot resist a password guessing attack. In this paper, we will demonstrate Tan's scheme, and show the security weakness of Tan's scheme.

In this paper, the structure of article is depicted as follows. In Section 2, we will briefly review Tan's scheme. In Section 3, we will show how the password guessing attack occurs in Tan's scheme. Finally, our conclusion will describe at the last section.

2 Review of Tan's Password Authentication Scheme

For analyzing the security weakness of Tan's scheme [33], we will introduce the scheme in this section. Tan's password authentication scheme is based on a smart card for multi-server environments. A user in this scheme is called U_i, a server is called S_j and a registration center is called RC. Two master keys, x and y which are held by RC. ID_i and SID_j are identity of user i and server j, respectively. All users and servers have public information. In addition, q is prime order in a large field F_q, g is a generator and $h(\cdot)$ is a security hash function.

Besides, this scheme has two cases, the first time login

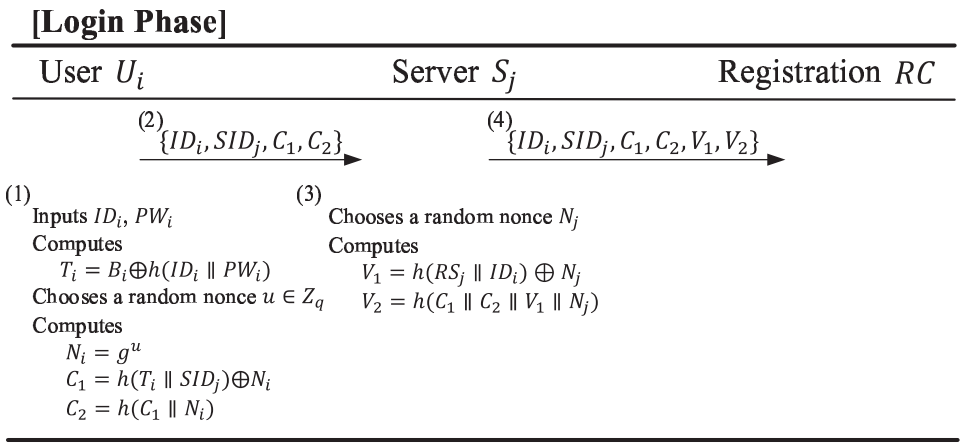

Figure 1: The login phase of Tan's scheme

and the non-first time login. There are four phases of their scheme: registration phase, login phase, authentication phase, and password change phase. All the cases have the same registration phase and password change phase.

2.1 The First Time Login

In the registration phase, the registration center RC computes $RS_j = h(SID_j \| y)$ as secret information and sends it to the server S_j through a secure channel. And then, user i submits his identity ID_i and registers to RC. U_i receives $h(ID_i \| x)$ which is computed by RC. U_i chooses PW_i and used $h(ID_i \| x)$ to compute $B_i = h(ID_i \| x) \oplus h(ID_i \| PW_i)$. A smart card contains $\{B_i, ID_i, h()\}$.

If user U_i wants to login the server S_j, he/she will insert his/her smart card and key his/her identity ID_i and password PW_i. And smart card will execute those steps described in Figure 1. In order to save space, we ignore to introduce the authentication phase and password change phase. Please refer them in Tan's scheme [33].

2.2 The Non-First Time Login

Not the first time login is something different from the first time login. After the first time login, RC doesn't need to participate for the login as the first time. If U_i wants to obtain the service from servers, he/she just needs to communicate with the server.

3 Analysis of Tan's Scheme

In this section, we will demonstrate that Tan's scheme is vulnerable to the password guessing attack.

Before the attack is executed, we assume that attacker steals the user's smart card and extracts these information stored in a smart card by some means. And then the attacker can execute the password guessing attack as follows.

Password Guessing Attack If the attacker wants to guess a user's password, he/she will interpret the login message $\{ ID_i, SID_j, C_1, C_2 \}$ in login phase between U_i and S_j, and $\{ ID_i, SID_j, C_1, C_2, V_1, V_2 \}$ between S_j and RC. He first guesses the password PW^*, and computes $h(ID_i \| PW^*)$ and $B_i \oplus h(ID_i \| PW^*) = h(ID_i \| x)$. And then, the attacker calculates $N_i^* = C_1 \oplus h(T_i^* \| SID_j)$ and $C_2 = h(C_1 \| N_i^*)$. If the equation is hold, the attacker can get the correct password. If not, the attacker will restart computing $h(ID_i \| PW^*)$ to $C_2 = h(C_1 \| N_i^*)$ until the equation is hold.

4 Conclusion

In this paper, we first have shown the Tan's scheme [33] is vulnerable to the password guessing attack. The attacker can obtain a user's correct password through this attack. From analysis of Tan's Scheme in this paper, it is shown that Tan's scheme is insecure to protect a user's password. The security analysis can help this scheme find out the weakness improved and applied in the other related area.

Acknowledgments

This study was supported by the National Science Council of Taiwan under grant NSC102-2221-E-468-020 and NSC101-2622-E-468-002-CC3. The authors gratefully acknowledge the anonymous reviewers for their valuable comments.

References

[1] C. C. Chang and C. Y. Lee, "A smart card-based authentication scheme using user identify cryptography," *International Journal of Network Security*, vol. 15, no. 2, pp. 139–147, 2013.

[2] T. Y. Chen, C. C. Lee, M. S. Hwang, and J. K. Jan, "Cryptanalysis of a secure dynamic ID based remote user authentication scheme for multi-server environment," in *The Fourth International Conference on Innovative Computing, Information and Control (ICICIC-2009), Kaohsiung, Taiwan*, pp. 725–728, 2009.

[3] T. Y. Chen, C. C. Lee, M. S. Hwang, and J. K. Jan, "Towards secure and efficient user authentication scheme using smart card for multi-server environments," *The Journal of Supercomputing*, vol. 66, no. 2, pp. 1008–1032, 2013.

[4] M. L. Das, "Comments on improved efficient remote user authentication schemes," *International Journal of Network Security*, vol. 6, no. 3, pp. 282–284, 2008.

[5] D. He, J. Chen, and J. Hu, "Weaknesses of a remote user password authentication scheme using smart card," *International Journal of Network Security*, vol. 13, no. 1, pp. 58–60, 2011.

[6] M. S. Hwang, "Cryptanalysis of remote login authentication scheme," *Computer Communications*, vol. 22, no. 8, pp. 742–744, 1999.

[7] M. S. Hwang, "A remote password authentication scheme based on the digital signature method," *International Journal of Computer Mathematics*, vol. 70, pp. 657–666, 1999.

[8] 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, pp. 163–172, Jan. 2010.

[9] M. S. Hwang, C. C. Lee, and Eric J. L. Lu, "Cryptanalysis of the batch verifying multiple DSA-type digital signatures," *Pakistan Journal of Applied Sciences*, vol. 1, no. 3, pp. 287–288, 2001.

[10] M. S. Hwang, C. C. Lee, and Y. L. Tang, "An improvement of SPLICE/AS in WIDE against guessing attack," *International Journal of Informatica*, vol. 12, no. 2, pp. 297–302, 2001.

[11] M. S. Hwang and L. H. Li, "A new remote user authentication scheme using smart cards," *IEEE Transactions on Consumer Electronics*, vol. 46, no. 1, pp. 28–30, 2000.

[12] M. S. Hwang, J. W. Lo, and S. C. Lin, "An efficient user identification scheme based on ID-based cryptosystem," *Computer Standards & Interfaces*, vol. 26, no. 6, pp. 565–569, 2004.

[13] M. S. Hwang, J. W. Lo, C. Y. Liu, and S. C. Lin, "Cryptanalysis of a user friendly remote authentication scheme with smart card," *Pakistan Journal of Applied Sciences*, vol. 5, no. 1, pp. 99–100, 2005.

[14] M. Kumar, "An enhanced remote user authentication scheme with smart card," *International Journal of Network Security*, vol. 10, no. 3, pp. 175–184, 2010.

[15] L. Lamport, "Password authentication with insecure communication," *Commun. ACM*, vol. 24, no. 11, pp. 770–772, 1981.

[16] C. C. Lee, M. S. Hwang, and L. H. Li, "A new key authentication scheme based on discrete logarithms," *Applied Mathematics and Computation*, vol. 139, no. 2, pp. 343–349, 2003.

[17] C. C. Lee, M. S. Hwang, and W. P. Yang, "A flexible remote user authentication scheme using smart cards," *ACM Operating Systems Review*, vol. 36, no. 3, pp. 46–52, 2002.

[18] C. C. Lee, L. H. Li, and M. S. Hwang, "A remote user authentication scheme using hash functions," *ACM Operating Systems Review*, vol. 36, no. 4, pp. 23–29, 2002.

[19] C. C. Lee, C. H. Liu, and M. S. Hwang, "Guessing attacks on strong-password authentication protocol," *International Journal of Network Security*, vol. 15, no. 1, pp. 64–67, 2013.

[20] C. T. Li and M. S. Hwang, "An efficient biometrics-based remote user authentication scheme using smart cards," *Journal of Network and Computer Applications*, vol. 33, no. 1, pp. 1–5, 2010.

[21] C. T. Li and 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, pp. 2181–2188, May 2010.

[22] L. H. Li, I. C. Lin, and M. S. Hwang, "A remote password authentication scheme for multi-server architecture using neural networks," *IEEE Transactions on Neural Networks*, vol. 12, no. 6, pp. 1498–1504, 2001.

[23] X. Li, Y. Xionga, J. Ma, and W. Wang, "An efficient and security dynamic identity based authentication protocol for multi-server architecture using smart cards," *Journal of Network and Computer Applications*, vol. 35, no. 2, pp. 763–769, 2012.

[24] I-En Liao, C. C. Lee, and M. S. Hwang, "Security enhancement for a dynamic ID-based remote user authentication scheme," in *International Conference on Next Generation Web Services Practices (NWeSP 2005), Seoul, Korea*, pp. 437–440, Aug. 23-27 2005.

[25] C. W. Lin, J. J. Shen, and M. S. Hwang, "Security enhancement for optimal strong-password authentication protocol," *ACM Operating Systems Review*, vol. 37, no. 3, pp. 12–16, 2003.

[26] C. W. Lin, C. S. Tsai, and M. S. Hwang, "A new strong-password authentication scheme using one-way hash functions," *International Journal of Computer and Systems Sciences*, vol. 45, pp. 623–626, July 2006.

[27] I. C. Lin, H. H. Ou, and M. S. Hwang, "A user authentication system using back-propagation network," *Neural Computing & Applications*, vol. 14, no. 3, pp. 243–249, 2005.

[28] I. C. Lin, M. S. Hwang, and L. H. Li, "A new remote user authentication scheme for multi-server architecture," *Future Generation Computer Systems*, vol. 19, no. 1, pp. 13–22, 2003.

[29] Y. L. Tang M. S. Hwang, C. C. Lee, "A simple remote user authentication scheme," *Mathematical and Computer Modelling*, vol. 36, pp. 103–107, 2002.

[30] A. Prakash, "A biometric approach for continuous user authentication by fusing hard and soft traits," *International Journal of Network Security*, vol. 16, no. 1, pp. 65–70, 2014.

[31] J. J. Shen, C. W. Lin, and M. S. Hwang, "A modified remote user authentication scheme using smart cards," *IEEE Transactions on Consumer Electronics*, vol. 49, no. 2, pp. 414–416, 2003.

[32] J. J. Shen, C. W. Lin, and M. S. Hwang, "Security enhancement for the timestamp-based password authentication scheme using smart cards," *Computers & Security*, vol. 22, no. 7, pp. 591–595, 2003.

[33] Z. Tan, "Improvenment on a password authentication scheme for multi-server environments," *Journal of Convergence Information Technology*, vol. 6, no. 1, pp. 218–228, 2011.

[34] H. Tang, X. Liu, and 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, no. 6, pp. 446–454, 2013.

[35] Y. L. Tang, C. W. Lin, and M. S. Hwang, "Security enhancement for the fingerprint-based remote user authentication scheme using smart cards," in *International Conference on Computer, Communication and Control Technologies (CCCT '03), Orlando, Florida (USA)*, pp. 104–107, July 31 - Aug. 2 2003.

[36] C. S. Tsai, C. C. Lee, and M. S. Hwang, "Password authentication schemes: Current status and key issues," *International Journal of Network Security*, vol. 3, no. 2, pp. 101–115, 2006.

[37] 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, 2008.

[38] W. J. Tsaur and C. C. Wu, "A secure smart-card-based password authenticated key agreement scheme in multi-server environments," in *IEEE 2th International Conference on Social Computing*, pp. 999–1003, 2010.

[39] R. C. Wang, W. S. Juang, and C. L. Lei, "User authentication scheme with privacy-preservation for multi-server environment," *IEEE Communication Letters*, vol. 13, no. 2, pp. 157–159, 2009.

[40] H. C. Wu, M. S. Hwang, and C. H. Liu, "A secure strong-password authentication protocol," *Fundamenta Informaticae*, vol. 68, pp. 399–406, 2005.

[41] C. C. Yang, T. Y. Chang, and M. S. Hwang, "Security of improvement on methods for protecting password transmission," *International Journal of Informatica*, vol. 14, no. 4, pp. 551–558, 2003.

[42] C. C. Yang, T. Y. Chang, J. W. Li, and M. S. Hwang, "Security enhancement for protecting password transmission," *IEICE Transactions on Communications*, vol. E86-B, no. 7, pp. 2178–2181, 2003.

Tung-Huang Feng received his M.S. in Information Management from Chao-Yang University of Technology, Taichung, Taiwan, ROC, in 2002. He is currently pursuing the Ph.D. degree from Computer Science & Information Engineering Department of Asia University, Wufeng, Taiwan. His research interests include information security, cloud computing, and Sensor Networks.

Chung-Huei Ling received his M.S. in Applied computer science and technology from Azusa Pacific University, Azusa, California , USA in 1990 and M.B.A in accounting from Northrop University, Los Angeles, California, USA in 1989. He is currently pursuing the Ph.D. degree from Computer Science and Information Engineering Department of Asia University, Wufeng, Taiwan. His research interests include information security, cloud computing, and radio frequency identification.

Min-Shiang Hwang received the B.S. in Electronic Engineering from National Taipei Institute of Technology, Taipei, Taiwan, Republic of China (ROC), in 1980; the M.S. in Industrial Engineering from National Tsing Hua University, Taiwan, in 1988; and the Ph.D. in Computer and Information Science from National Chiao Tung University, Taiwan, in 1995. He also studied Applied Mathematics at National Cheng Kung University, Taiwan, from 1984-1986. Dr. Hwang passed the National Higher Examination in field "Electronic Engineer" in 1988. He also passed the National Telecommunication Special Examination in field "Information Engineering", qualified as advanced technician the first class in 1990. From 1988 to 1991, he was the leader of the Computer Center at Telecommunication Laboratories (TL), Ministry of Transportation and Communications, ROC. He was also a chairman of the Department of Information Management, Chaoyang University of Technology (CYUT), Taiwan, during 1999-2002. He was a professor and chairman of the Graduate Institute of Networking and Communications, CYUT, during 2002-2003. He is currently a professor of the department of Management Information System, National Chung Hsing University, Taiwan, ROC. He obtained 1997, 1998, 1999, 2000, and 2001 Outstanding Research Awards of the National Science Council of the Republic of China. He is a member of IEEE, ACM, and Chinese Information Security Association. His current research interests include electronic commerce, database and data security, cryptography, image compression, and mobile computing. Dr. Hwang had published 170+ articles on the above research fields in international journals.