An Improved Protocol for Password Authentication Using Smart Cards

Zi-Yao Cheng[1], Yun Liu[1], Chin-Chen Chang[2, 4, *], and Shih-Chang Chang[3]

[1] Department of Electronic and Information Engineering,
Key Laboratory of Communication and Information Systems,
Beijing Municipal Commission of Education,
Beijing Jiaotong University,
Beijing 100044, China
{09111024, liuyun}@bjtu.edu.cn

[2] Department of Information Engineering and Computer Science,
Feng Chia University,
Taichung 407, Taiwan, ROC
alan3c@gmail.com

[3] Department of Computer Science and Information Engineering,
National Chung Cheng University,
Chiayi 621, Taiwan, ROC
chang.coby@gmail.com

[4] Department of Computer Science and Information Engineering,
Asia University,
Taichung 41354, Taiwan, ROC

Received 10 October 2011; Revised 12 November 2011; Accepted 15 December 2011

Abstract. In recent years, several password authentication schemes for remote login and verification have been widely implemented for systems that control and access to Internet applications. Therefore, how to assure the security protection of these related operations in computer networks has been extensively investigated by many engineers in these two decades. Recently, an advanced smart card based password authentication scheme is proposed by Song. He claimed that the proposed scheme performs secure operations and activities over the insecure network communications. However, Song's scheme is still vulnerable to the off-line password guessing attack, and it is lack of perfect forward secrecy and system reparability. In this paper, we state the security weaknesses of Song's scheme, and then propose an improvement of the password based authentication scheme which not only inherits the criteria of authentication scheme such as mutual authentication and session key agreement but also protects against the risk of various attacks over the insecure Internet environment. Furthermore, we analyze the security and performance aspects to prove that our proposed scheme is more secure, efficient and practical for applications of networks communications.

Keywords: Mutual authentication, password, smart card, security, key agreement

References

[1] L. Lamport, "Password Authentication with Insecure Communication," *Communications of the ACM*, Vol. 24, No. 11, pp. 770-772, 1993.

[2] C.C. Chang and S.J. Hwang, "Using Smart Cards to Authenticate Remote Passwords," *Computer and Mathematics with Applications*, Vol. 26, No. 3, pp. 19-27, 1993.

[3] 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.

*Correspondence author

[4] M. Kumar, "New Remote User Authentication Scheme Using Smart Cards," *IEEE Transactions on Consumer Electronics*, Vol. 50, No. 2, pp. 597-600, 2004.

[5] A. K. Awasthi and S. Lal, "An Enhanced Remote User Authentication Scheme Using Smart Cards," *IEEE Transactions on Consumer Electronics*, Vol. 50, No. 2, pp. 583-586, 2004.

[6] N.Y. Lee and Y.C. Chiu, "Improved Remote Authentication Scheme with Smart Card," *Computer Standards & Interfaces*, Vol. 27, No. 2, pp. 177-180, 2005.

[7] S.W. Lee, H.S. Kim, K.Y. Yoo, "Improvement of Chien et al.'s Remote User Authentication Scheme Using Smart Cards," *Computer Standards & Interfaces*, Vol. 27, No. 2, pp. 181-183, 2005.

[8] J. Xu, W.T. Zhu, D.G. Feng, "An Improved Smart Card Based Password Authentication Scheme with Provable Security," *Computer Standards & Interfaces*, Vol. 31, No. 4, pp. 723-728, 2009.

[9] R. Song, L. Korba, G. Yee, "Analysis of Smart Card-based Remote User Authentication Schemes," in *Proceedings of the 2007 International Conference on Security and Management*, Las Vegas, Nevada, USA, pp. 323-329, 2007.

[10] C.C. Chang, C.Y. Lee, Y.C. Chiu, "Enhanced Authentication Scheme with Anonymity for Roaming Service in Global Mobility Networks," *Computer Communications*, Vol. 32, No. 4, pp. 611-618, 2009.

[11] X.X. Li, W.D. Qiu, D. Zheng, K.F. Chen, J.H. Li, "Anonymity Enhancement on Robust and Efficient Password-authenticated Key Agreement Using Smart Cards", *IEEE Transactions on Industrial Electronics*, Vol. 57, No. 2, pp. 793-800, 2010.

[12] R.C. Wang, W.S. Juang, C.L. Lei, "Robust Authentication and Key Agreement Scheme Preserving the Privacy of Secret Key," *Computer Communications*, Vol. 34, No. 3, pp. 274-280, 2011.

[13] C.C. Chang and T.F. Cheng, "A Robust and Efficient Smart Card Based Remote Login Mechanism for Multi-server Architecture," *International Journal of Innovative Computing, Information and Control*, Vol. 7, No. 8, pp. 4589-4602, 2011.

[14] R. Song, "Advanced Smart Card Based Password Authentication Protocol," *Computer Standards & Interface*s, Vol. 32, No. 5-6, pp. 321-325, 2010.

[15] C.C. Chang and J.S. Lee, "An Efficient and Secure Remote Authentication Scheme Using Smart Cards," *Information & Security*, Vol. 18, pp. 122-133, 2006.

[16] B. Schneier, Applied Cryptography, Protocols, Algorithms, and Source Code in C, John Wiley and Sons Inc., 2nd Edition, New York, USA, pp. 15, 1996.