Cryptanalysis of Tseng-Wu Group Key Exchange Protocol

Chung-Huei Ling[1], Shih-Ming Chen[1], and Min-Shiang Hwang[1,2]
(Corresponding author: Min-Shiang Hwang)

Department of Computer Science and Information Engineering, Asia University[1]
No. 500, Lioufeng Rd., Wufeng, Taichung 41354, Taiwan
(Email: mshwang@asia.edu.tw)
Department of Medical Research, China Medical University Hospital, China Medical University[2]
No. 91, Hsueh-Shih Road, Taichung 40402, Taiwan
(Received May 17, 2015; revised and accepted Aug. 21 & Sept. 8, 2015)

Abstract

Recently, Tseng and Wu pointed out that the second protocol of Biswas's two-party keys scheme based on the Diffie-Hellman technique has a security weakness and proposed a new protocol to remedy the weakness. In this article, we point out that Tseng-Wu's protocol is vulnerable to a man-in-the-middle attack. An attacker could intercept, delete, or modify the communicated messages between two communicating party or among the group members.

Keywords: Diffie-Hellman key-exchange, group key, man-in-the-middle attack, multiple two-party keys

1 Introduction

When two communicating parties want to communicate with each other privately, they first need to establish a session key for secure communication in future. The session key is used to encrypt/decrypt their communicating messages with symmetric-key cryptosystem, such as DES, RC4 [1], or AES. [19]. It's important for securely obtaining the common session key between two communicating parties. In 1976, Diffie and Hellman first proposed a key agreement protocol to solve this problem [6]. Two participants exchange their public parameter through a public channel to generate a shared session key between them [5, 7, 9, 10, 11, 16, 21, 22, 26].

The Diffie and Hellman's key agreement protocol is only applied between two communicating parties. We said that the Diffie and Hellman's key agreement protocol is a 2-party key agreement protocol [2, 6, 12, 17, 25]. Recently, many group key management and distribution protocols had been proposed for multi-party [8, 13, 23, 27]. In the multi-party key agreement protocols, session keys are computed dynamically through cooperation of all participants [4, 15].

In 2008, Biswas [3] proposed two key agreement protocols based on the two-party Diffie-Hellman technique. The Biswas's first protocol allows two participants to generate 15 shared keys through the exchange of two pair of public parameters through a public channel. Although, Biswas's first protocol is superior to Diffie-Hellman protocol which only generates a single shared key through the exchange of one pair of public parameters. However, the Biswas's first protocol is vulnerable to the man-in-the-middle attack [20]. The man-in-the-middle attack is that an attacker secretly relays and alters the communicating messages between two communicating parties [14, 18, 28].

The Bitwas's second protocol is an extension of the two-party Diffie-Hellman technique to generate a group key for participants of a large group. However, Tseng and Wu pointed out that the Bitwas's second protocol has a weakness and proposed a new protocol to remedy the weakness in 2010 [24].

The rest of this paper is organized as follows. In Section 2, we review Tseng-Wu group key exchange protocol. In Section 3, we show a man-in-the-middle attack on Tseng-Wu's Protocol. Finally, our brief conclusions will be drawn in Section 4.

2 Review of Tseng-Wu Group Key Exchange Protocol

In this section, we review the Tseng and Wu's group key exchange protocol based on the two-party Diffie-Hellman technique [24]. The protocol allows a group members to generate a shared group session key K. The detailed steps are described as follows and in Figure 1.

1) Each participant U_i $(i = 1, 2, 3, ..., (n-1))$ selects a random value $x_i \in Z_q^*$, and then computes and sends $X_i = g^{x_i} \bmod p$ to the group controller U_n. The group controller U_n also selects a random value $x_n \in$

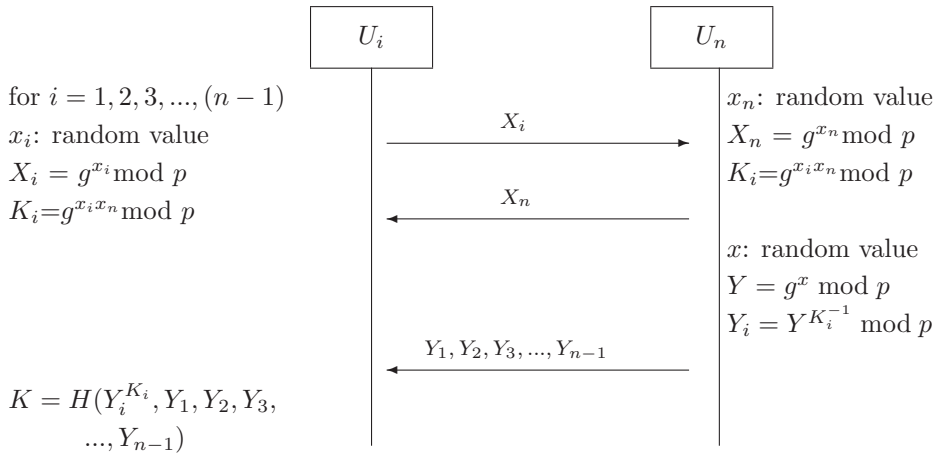

Figure 1: Tseng-Wu group key exchange protocol

Z_q^* and sends $X_n = g^{x_n} \bmod p$ to each participant U_i. Then, each U_i and U_n can compute a two-party shared key $K_i = g^{x_i x_n} \bmod p$ $(i = 1, 2, \cdots, (n-1))$. Here, p is a large positive integer; g is a group generator.

2) U_n selects a random value $x \in Z_q^*$ and computes $Y = g^x \bmod p$ and $Y_i = Y^{K_i^{-1}} \bmod p$, for $i = 1, 2, \cdots, (n-1)$. Then, U_n broadcasts $(Y_1, Y_2, \cdots, Y_{n-1})$ to each participant. Finally, each participant U_i $(i = 1, 2, \cdots, (n-1))$ can compute the group key $K = H(Y_i^{K_i}, Y_1, Y_2, \cdots, Y_{n-1})$.

3 Man-in-the-Middle Attack on Tseng-Wu Protocol

In this section, we show that Tseng and Wu's protocol is not secure against a man-in-the-middle attack. We assume that an adversary U_A could intercept and modify the communications among the group members. Then, the adversary could derive the group key to destroy the Tseng and Wu's protocol. The attack scenario is outlined in Figure 2. A more detailed description of the attack is as follows:

1) An adversary U_A stands the middle between each participant U_i, $i = 1, 2, \cdots, (n-1)$ and the group controller U_n.

2) The adversary U_A randomly chooses a random value x_a. He/she computes $X_a = g^{x_a} \bmod p$.

3) Each U_i wants to send X_i to U_n. U_A intercepts X_i and sends X_a to U_n.

4) U_n then sends X_n to each U_i. In the same way, the adversary U_A also intercepts X_n and sends X_a to each U_i.

5) Then, U_n and U_A can compute a two-party shared key $K_i' = g^{x_n x_a} \bmod p$.

6) Each U_i and U_A can compute a two-party shared key $K_i" = g^{x_i x_a} \bmod p$ $(i = 1, 2, \cdots, (n-1))$.

7) U_n computes Y and Y_i and wants to send Y_i to each U_i, $i = 1, 2, \cdots, (n-1)$. U_A intercepts Y_i and computes $Y_i' = (Y_i^{K_i'})^{K_i"^{-1}} \bmod p$ for each U_i, $i = 1, 2, \cdots, (n-1)$.

8) Then, U_A broadcasts $(Y_1', Y_2', \cdots, Y_{n-1}')$ to each participant U_i.

9) Finally, each participant U_i $(i = 1, 2, \cdots, (n-1))$ can compute the group key $K = H(Y_i^{'K_i"}, Y_1', Y_2', \cdots, Y_{n-1}')$.

10) On the other hand, U_A can also compute the group key

$$K = H(Y_i^{K_i'}, Y_1', Y_2', Y_3', ..., Y_{n-1}').$$

Since $Y_i^{'K_i"} = Y_i^{K_i'}$, the group key K between each U_i and U_A is the same value. Then, the adversary can use the group key to decrypt the communications among the group members. Therefore, the protocol is not secure against the man-in-the-middle attack.

4 Conclusions

In this article, we have showed the security weakness of Tseng-Wu's protocol. Tseng-Wu's protocol cannot resist the man-in-the-middle attack. Through the attack, an attacker can intercept, delete, modify or alter the communicated messages between two communicating party or among the group members.

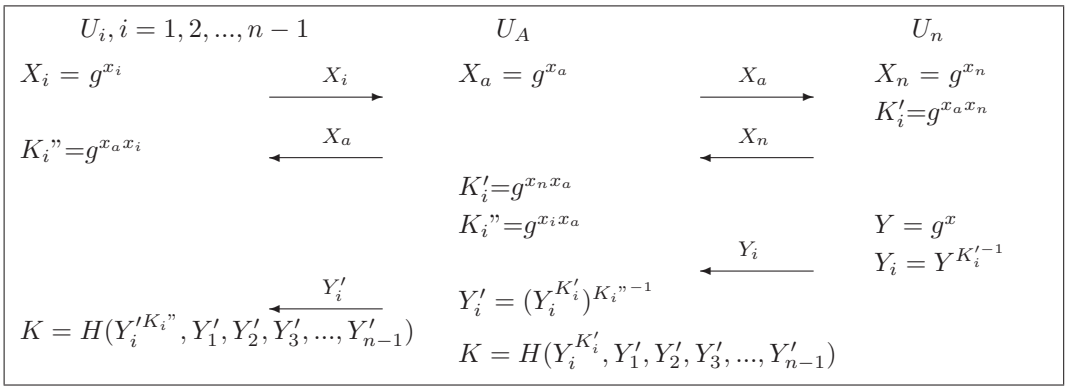

Figure 2: Man-in-the-middle attack on Tseng-Wu protocol

Acknowledgements

This research was partially supported by the National Science Council, Taiwan, R.O.C., under contract no.: MOST 103-2221-E-468 -026, NSC 103-2622-E-468-001-CC2, and NSC 103-2622-H-468-001-CC2.

References

[1] A. Aboshosha, K. A. ElDahshan, E. K. Elsayed, A. A. Elngar, "EA based dynamic key generation in RC4 ciphering applied to CMS," *International Journal of Network Security*, vol. 17, no. 4, pp. 405–412, 2015.

[2] K. Azimian, J. Mohajeri, and M. Salmasizadeh, "Weak composite Diffie-Hellman," *International Journal of Network Security*, vol. 7, no. 3, pp. 383–387, 2008.

[3] G. P. Biswas, Diffie-Hellman technique: extended to multiple two-party keys and one multi-party key," *IET Information Security*, vol. 2, no. 1, pp. 12–18, 2008.

[4] C. C. Chang, L. Harn, and T. F. Cheng, "Notes on "Polynomial-Based Key Management for Secure Intra-Group and Inter-Group Communication", *International Journal of Network Security*, vol. 16, no. 2, pp. 143–148, 2014.

[5] K. M. Cheng, T. Y. Chang, and J. W. Lo, "Cryptanalysis of security enhancement for a modified authenticated key agreement protocol", *International Journal of Network Security*, vol. 11, no. 1, pp. 55–57, 2010.

[6] W. Diffie and M. E. Hellman, "New directions in cryptography", *IEEE Transactions on Information Theory*, vol. IT-22, pp. 644–654, Nov. 1976.

[7] M. S. Farash, M. A. Attari, "A pairing-free ID-based key agreement protocol with different PKGs", *International Journal of Network Security*, vol. 16, no. 3, pp. 168–173, 2014.

[8] A. Gawanmeh, A. Bouhoula, and S. Tahar, "Rank functions based inference system for group key management protocols verification", *International Journal of Network Security*, vol. 8, no. 2, pp. 187–198, 2009.

[9] C. Guo, C. C. Chang, "A novel threshold conference-key agreement protocol based on generalized chinese remainder theorem", *International Journal of Network Security*, vol. 17, no. 2, pp. 165-173, 2015.

[10] L. C. Huang and M. S. Hwang, "An efficient MQV key agreement scheme", *International Journal of Network Security*, vol. 16, no. 2, pp. 157-160, 2014.

[11] Q. Jiang, J. Ma, G. Li, and L. Yang, "Robust two-factor authentication and key agreement preserving user privacy", *International Journal of Network Security*, vol. 16, no. 3, pp. 229–240, 2014.

[12] W. S. Juang and J. L. Wu, "Efficient user authentication and key agreement with user privacy protection", *International Journal of Network Security*, vol. 7, no. 1, pp. 120-129, 2008.

[13] A. A. Kamal, "Cryptanalysis of a polynomial-based key management scheme for secure group communication", *International Journal of Network Security*, vol. 15, no. 1, pp. 68-70, 2013.

[14] 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.

[15] W. T. Li, C. H. Ling, and M. S. Hwang, "Group rekeying in wireless sensor networks: A survey", *International Journal of Network Security*, vol. 16, no. 6, pp. 401-410, 2014.

[16] J. P. Lin, J. M. Fu, "Authenticated key agreement scheme with privacy-protection in the three-party setting", *International Journal of Network Security*, vol. 15, no. 3, pp. 179-189, 2013.

[17] J. Liu and J. Li, "A better improvement on the integrated Diffie-Hellman-DSA key agreement protocol", *International Journal of Network Security*, vol. 11, no. 2, pp. 114–117, 2010.

[18] J. W. Lo, M. S. Hwang, and C. H. Liu, "An efficient key assignment scheme for access control in a large leaf class hierarchy", *Information Sciences*, vol. 181, no. 4, pp. 917–925, 2011.

[19] National Institute of Standards and Technology, *Specification for the Advanced Encryption Standard (AES)*, Federal Information Processing Standards Publication (FIPS) 197, Nov. 26, 2001. (`http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf`)

[20] H. T. Pan, J. R. Sun, and M. S. Hwang, "Cryptanalysis of Biswas's multi-party keys scheme based on the Diffie-Hellman technique", in *Advances in Engineering Research*, vol. 15, pp. 842–847, Atlantis Press, 2015.

[21] Y. K. Peker, "A new key agreement scheme based on the triple decomposition problem", *International Journal of Network Security*, vol. 16, no. 6, pp. 426–436, 2014.

[22] M. Rajaram and T. D. Suresh, "An interval-based contributory key agreement", *International Journal of Network Security*, vol. 13, no. 2, pp. 92–97, 2011.

[23] R. Srinivasan, V. Vaidehi, R. Rajaraman, S. Kanagaraj, R. Chidambaram Kalimuthu, and R. Dharmaraj, "Secure Group Key Management Scheme for Multicast Networks", *International Journal of Network Security*, vol. 11, no. 1, pp. 33–38, 2010.

[24] Y. M. Tseng and T. Y Wu, "Analysis and improvement on a contributory group key exchange protocol based on the Diffie-Hellman technique", *Informatica*, vol. 21, no. 2, pp. 247–258, 2010.

[25] T. Thomas, "Secure two-party protocols for point inclusion problem", *International Journal of Network Security*, vol. 9, no. 1, pp. 1–7, 2009.

[26] L. Wang and C. K. Wu, "Efficient key agreement for large and dynamic multicast groups", *International Journal of Network Security*, vol. 3, no. 1, pp. 8–17, 2006.

[27] F. Wang, C. C. Chang, Y. C. Chou, "Group authentication and group key distribution for ad hoc Networks", *International Journal of Network Security*, vol. 17, no. 2, pp. 199–207, 2015.

[28] C. Y. Yang, C. C. Lee, and S. Y. Hsiao, "Man-in-the-middle attack on the authentication of the user from the remote autonomous object", *International Journal of Network Security*, vol. 1, no. 2, pp. 81–83, 2005.

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.

Shih-Ming Chen received the B.S. degree in Information Management from Chaoyang University of Technology (CYUT), Taichung, Taiwan, Republic of China, in 1999; the M.S. in Information Management from Chaoyang University of Technology (CYUT), Taichung, Taiwan, Republic of China, in 2003. He is currently pursuing his PhD degree in Computer Science and Information Engineering from Asia University. His current research interests include information security and Science & Technology of Chinese studies.

Min-Shiang Hwang received the B.S. in Electronic Engineering from National Taipei Institute of Technology, Taipei, Taiwan, Republic of China, 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 project leader for research in computer security at TL in July 1990. He obtained the 1997, 1998, and 1999 Distinguished 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 database and data security, cryptography, image compression, and mobile communications.