Cryptanalysis of Biswas's Multi-party Keys Scheme Based on the Diffie-Hellman Technique

Hsieh-Tsen PAN[1, a], Jia-Rong SUN[1, b], Min-Shiang HWANG[1,2,c,*]

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

[2]Department of Medical Research, China Medical University Hospital, China Medical University, Taichung 40402, Taiwan

[a]email: osric@elinkcom.com.tw, [b]email: asiaphd10026@gmail.com, [c]mshwang@asia.edu.tw

*The corresponding author: Prof. Min-Shiang Hwang

Keywords: Diffie-Hellman Key-exchange; Group Key; Man-in-the-middle Attack; Multiple two-party keys

Abstract. Biswas proposed two protocols based on the two-party Diffie-Hellman technique: (1) key agreement with multiple two-party keys and (2) a contributory group key exchange protocol. Then, Tseng and Wu pointed out that the second protocol has a security weakness and proposed a new protocol to remedy the weakness. In this paper, the authors point out that the Biswas's first protocol is vulnerable to a man-in-the-middle attack. Through the attack, an attacker can intercept, modify, or delete the communicated messages between two communicating party or among the group members.

Introduction

In fact, the ability to dynamically and publicly establish a session key for secure communication is a big challenge between two participants. The session key is to encrypt and decrypt their communicated messages by using symmetric-key cryptosystem such as the AES [18]. Since that, two communicating parties can communicate with each other privately. However, In Internet, how do two communicating parties securely obtain the common session key between them? In 1976, Diffie and Hellman proposed a key agreement protocol to solve this problem [5]. It allows two participants exchange two public keys through a public channel to generate a shared key between them [4, 6, 8-10, 15, 19, 20, 23, 24].

A brief discussion of the Diffie-Hellman protocol is as follows. Let A and B be the two participants that wish to establish a secure shared key between them. Both A and B agree on two large positive integers, n and g such that n is a prime number and g is a group generator. A/B randomly chooses a private key x/y, which is smaller than n. Both A and B exchange their public keys $X = g^x \bmod n$ and $Y = g^y \bmod n$. After that, both A and B can compute their shared key $K_{AB} = Y^x = g^{yx} \bmod n$, and $K_{BA} = X^y = g^{xy} \bmod n$. Then, they can use the shared key K for secure communication [1, 5, 11, 16].

Except 2-party key agreement protocol, there are many group key management and distribution protocols had been proposed for multi-party [7, 12, 21, 25]. In these protocols, keys are computed dynamically through cooperation of all protocol participants [3, 14].

In 2008, Biswas [2] proposed two protocols based on the two-party Diffie-Hellman technique: (1) key agreement with multiple two-party keys and (2) a contributory group key exchange protocol. In the first protocol, it is an extension of the Diffie-Hellman protocol. It allows two participants generate 15 shared keys through the exchange of two pair of public keys through a public channel. On the other hand, the original Diffie-Hellman protocol can only generate a single shared key through the exchange of one pair of public keys. It is seen that the Biswas's protocol is superior to the original Diffie-Hellman protocol. However, this paper shall show that the Biswas's protocol is vulnerable to the man-in-the-middle attack [13, 17, 26]. We explain the security weakness in Section 3 in detail. In the second protocol, it is an extension of the two-party Diffie-Hellman technique to generate a group key for participants of a large group. In 2010, Tseng and Wu [22] pointed out that the second protocol has a security weakness and proposed a new protocol to remedy the weakness.

The rest of this paper is organized as follows. In Section 2, we review the Biswas's protocol. In Section 3, we shall show our security analysis of the Biswas's protocol. Finally, our brief conclusions will be drawn in Section 4.

Review of Biswas's Multiple Two-Party Keys

At present the main means is low click type and the lever type, low click type is on the bottom of the ball through attack the ball flew over obstacles, this method is able to pick the ball's advantages and makes the energy loss in institutions least, the shortcoming is the ball high requirement of the shape of the electromagnetic valve [19]. Therefore, the development of a high-performance control system of soccer robot has become an urgent desire for soccer robot fans.

In this section, we review the Biswas's multiple two-party keys [2]. Now, we suppose that Bob and Alice want to establish 15 common session keys by sending four Diffie-Hellman public keys. First, Alice and Bob exchange two pairs of public keys and use them to agree four base keys. Next, 11 additional shared keys can be derived by multiplying the four base keys in different combinations. Finally, Alice and Bob can perform the following steps to establish 15 common session keys.

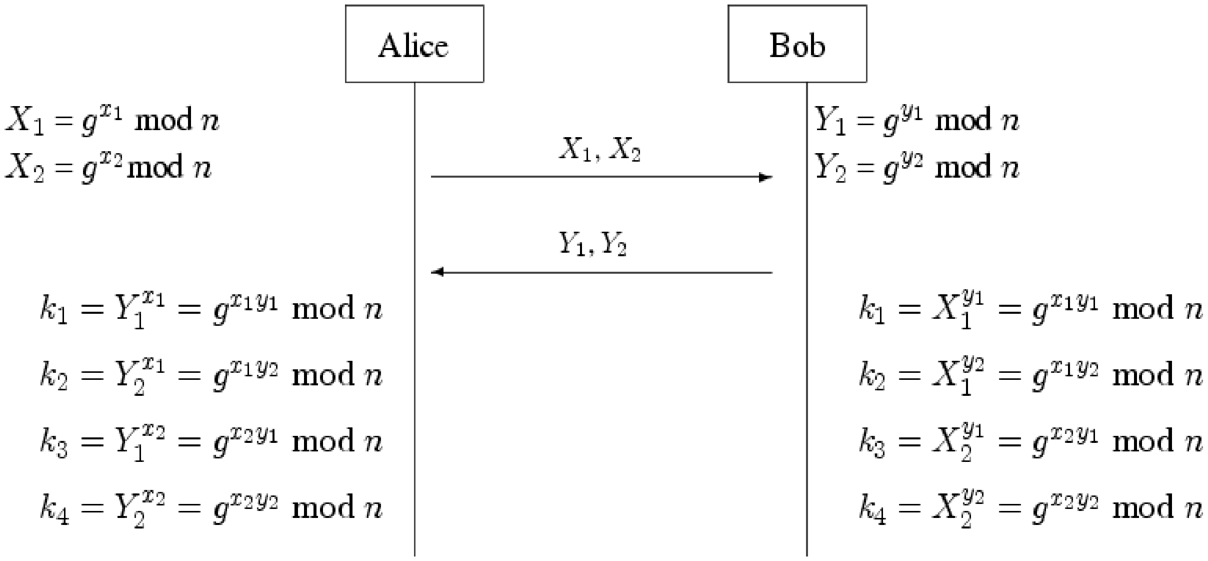
Alice
Bob
$X_1 = g^{x_1} \bmod n$
$X_2 = g^{x_2} \bmod n$
X_1, X_2
$Y_1 = g^{y_1} \bmod n$
$Y_2 = g^{y_2} \bmod n$
Y_1, Y_2
$k_1 = Y_1^{x_1} = g^{x_1 y_1} \bmod n$
$k_2 = Y_2^{x_1} = g^{x_1 y_2} \bmod n$
$k_3 = Y_1^{x_2} = g^{x_2 y_1} \bmod n$
$k_4 = Y_2^{x_2} = g^{x_2 y_2} \bmod n$
$k_1 = X_1^{y_1} = g^{x_1 y_1} \bmod n$
$k_2 = X_1^{y_2} = g^{x_1 y_2} \bmod n$
$k_3 = X_2^{y_1} = g^{x_2 y_1} \bmod n$
$k_4 = X_2^{y_2} = g^{x_2 y_2} \bmod n$

Figure 1: Generating four base keys of Biswas's protocol

1. Both Alice and Bob agree on two large positive integers, *n* and *g* such that *n* is a prime number and *g* is a group generator.
2. Alice randomly chooses two positive integers, x_1 and x_2, which are smaller than *n* and serves as Alice's private keys. Similarly, Bob chooses its own private keys y_1 and y_2.
3. Both Alice and Bob compute their public keys using ($X_1 = g^x{}_1 \, mod \, n, X_2 = g^x{}_2 \, mod \, n$) and ($Y_1 = g^y{}_1 \, mod \, n, Y_2 = g^y{}_2 \, mod \, n$, respectively.
4. They exchange their public keys through a public communication channel.
5. After receiving these public keys, both Alice and Bob compute their shared four base keys: *(k_1, k_2, k_3, k_4)* as follows. The procedures of generating four base keys are also shown in Figure 1.

$$k_1 = Y_1^{x_1} = X_1^{y_1} = g^{x_1 y_1} \bmod n$$
$$k_2 = Y_2^{x_1} = X_1^{y_2} = g^{x_1 y_2} \bmod n$$
$$k_3 = Y_1^{x_2} = X_2^{y_1} = g^{x_2 y_1} \bmod n$$
$$k_4 = Y_2^{x_2} = X_2^{y_2} = g^{x_2 y_2} \bmod n$$

6. Once the four base keys are generated, both Alice and Bob can extend them to generate 11 additional shared keys as follows.

$$k_5 = k_1 \times k_2 = g^{x_1 y_1 + x_1 y_2} \bmod n$$
$$k_6 = k_1 \times k_3 = g^{x_1 y_1 + x_2 y_1} \bmod n$$
$$k_7 = k_1 \times k_4 = g^{x_1 y_1 + x_2 y_2} \bmod n$$
$$k_8 = k_2 \times k_3 = g^{x_1 y_2 + x_2 y_1} \bmod n$$
$$k_9 = k_2 \times k_4 = g^{x_1 y_2 + x_2 y_2} \bmod n$$
$$k_{10} = k_3 \times k_4 = g^{x_2 y_1 + x_2 y_2} \bmod n$$
$$k_{11} = k_1 \times k_2 \times k_3 = g^{x_1 y_1 + x_1 y_2 + x_2 y_1} \bmod n$$
$$k_{12} = k_1 \times k_2 \times k_4 = g^{x_1 y_1 + x_1 y_2 + x_2 y_2} \bmod n$$
$$k_{13} = k_1 \times k_3 \times k_4 = g^{x_1 y_1 + x_2 y_1 + x_2 y_2} \bmod n$$
$$k_{14} = k_2 \times k_3 \times k_4 = g^{x_1 y_2 + x_2 y_1 + x_2 y_2} \bmod n$$
$$k_{15} = k_1 \times k_2 \times k_3 \times k_4 = g^{x_1 y_1 + x_1 y_2 + x_2 y_1 + x_2 y_2} \bmod n$$

Finally, Alice and Bob can share the 15 common session keys (k_i, i = 1, 2, 3, ..., 15).

Man-in-the-Middle Attack on Biswas's Protocol

In this section, we shall show that the Biswas's protocol is not secure against a man-in-the-middle attack. We assume that the adversary Eve is a legitimate user. Eve wants to share the four base keys with Alice by masquerading as Bob and to share another four base keys with Bob by masquerading as Alice. Once Eve has their four base keys, she can also generate 11 additional shared keys between Alice and Bob. The attack scenario is outlined in Figure 2. A more detailed description of the attack is as follows:

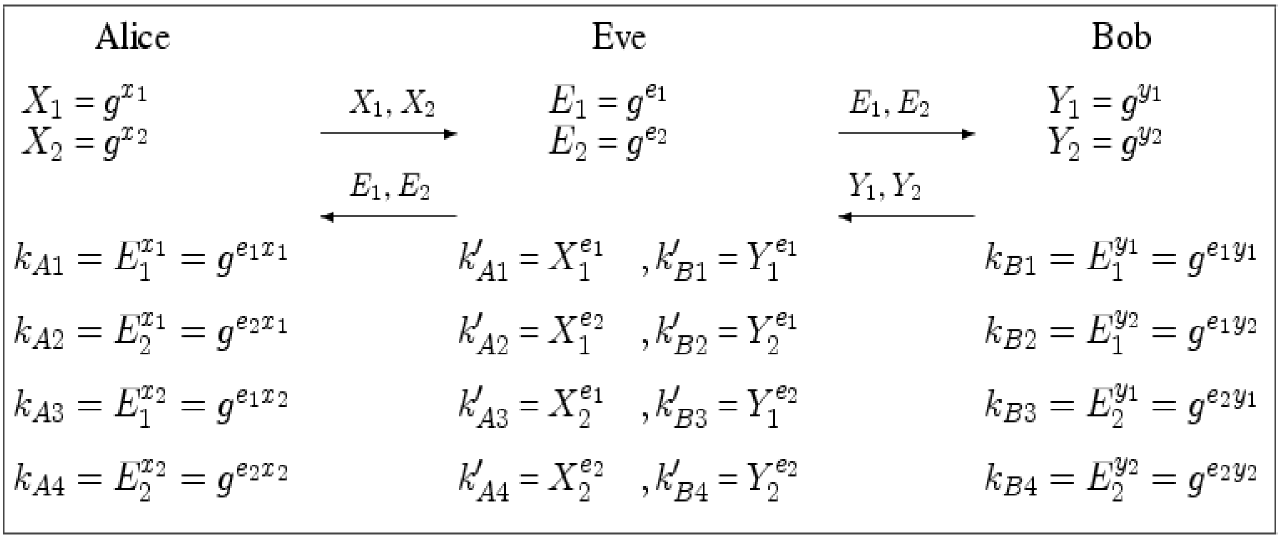

Figure 2: Man-in-the-middle attack on Biswas's protocol

1. As a preliminary step, the adversary Eve randomly chooses two positive integers, e_1 and e_2, which are smaller than n. She computes $E_1 = g^{e_1} \bmod n$ and $E_2 = g^{e_2} \bmod n$.
2. Alice sends Bob her public keys X_1 and X_2. Eve intercepts these public keys and sends Bob E_1 and E_2.
3. Bob sends Alice his public keys Y_1 and Y_2. Eve intercepts these public keys and sends Alice E_1 and E_2.
4. After receiving forged public keys from Eve, Alice can compute their shared four base keys $(k_{A1}, k_{A2}, k_{A3}, k_{A4})$ with Bob.

$$k_{A1} = E_1^{x_1} = g^{e_1 x_1} \bmod n$$

$$k_{A2} = E_2^{x_1} = g^{e_2 x_1} \bmod n$$

$$k_{A3} = E_1^{x_2} = g^{e_1 x_2} \bmod n$$

$$k_{A4} = E_2^{x_2} = g^{e_2 x_2} \bmod n$$

Once the four base keys are generated, Alice can extend them to generate 11 additional shared keys the same as former section.

5. After receiving forged public keys from Eve, Bob can compute their shared four base keys $(k_{B1}, k_{B2}, k_{B3}, k_{B4})$ with Alice.

$$k_{B1} = E_1^{y_1} = g^{e_1 y_1} \bmod n$$

$$k_{B2} = E_1^{y_2} = g^{e_1 y_2} \bmod n$$

$$k_{B3} = E_2^{x_1} = g^{e_2 y_1} \bmod n$$

$$k_{B4} = E_2^{x_2} = g^{e_2 y_2} \bmod n$$

Once the four base keys are generated, Bob can also extend them to generate 11 additional shared keys the same as former section.

6. Both Alice and Bob believe that they communicate with each other and share the 15 common session keys between them. However, Eve can also compute four base keys between Alice and Bob and extend them to generate 11 additional shared keys the same as former section. Eve can share four base keys $(k'_{A1}, k'_{A2}, k'_{A3}, k'_{A4})$ with Alice and four base keys $(k'_{B1}, k'_{B2}, k'_{B3}, k'_{B4})$ with Bob.

$$k'_{A1} = X_1^{e_1} = g^{e_1 x_1} \bmod n = k_{A1}$$

$$k'_{A2} = X_1^{e_2} = g^{e_2 x_1} \bmod n = k_{A2}$$

$$k'_{A3} = X_2^{x_1} = g^{e_1 x_2} \bmod n = k_{A3}$$

$$k'_{A4} = X_2^{e_2} = g^{e_2 x_2} \bmod n = k_{A4}$$

$$k'_{B1} = Y_1^{e_1} = g^{e_1 y_1} \bmod n = k_{B1}$$

$$k'_{B2} = Y_2^{e_1} = g^{e_1 y_2} \bmod n = k_{B2}$$

$$k'_{B3} = Y_1^{x_2} = g^{e_2 y_1} \bmod n = k_{B3}$$

$$k'_{B4} = Y_2^{e_2} = g^{e_2 y_2} \bmod n = k_{B4}$$

7. When Alice sends a message to Bob, encrypted in k_{Ai}, Eve intercepts it. Eve can decrypts it with k'_{Ai}, re-encrypts it with k'_{Bi}, and sends it on to Bob. Bob can decrypts it with k_{Bi}.
8. When Bob sends a message to Alice, encrypted in k_{Bi}, Eve intercepts it. Eve can decrypts it with k'_{Bi}, re-encrypts it with k'_{Ai}, and sends it on to Alice. Alice can decrypts it with k_{Ai}.

We can see that Eve can intercept, modify, or delete the communicated messages between Alice and Bob. This attack can work because Alice and Bob have no way to verify that they are talking to each other.

Conclusion

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

Acknowledgement

This research was partially supported by the Ministry of Science and Technology, 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] K. Azimian, J. Mohajeri, and M. Salmasizadeh, Weak composite Diffie-Hellman, *International Journal of Network Security*, vol. 7, no. 3, pp. 383－387, 2008.

[2] 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.

[3] 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.

[4] 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.

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

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] 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.

[11] 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.

[12] 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.

[13] 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.

[14] 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.

[15] 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.

[16] 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.

[17] 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.

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

[19] 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.

[20] 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.

[21] 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.

[22] 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.

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

[24] 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.

[25] 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.

[26] 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.