An Improvement of a Simple Authenticated Key Agreement Algorithm *

Eric Jui-Lin Lu Min-Shiang Hwang †

Department of Information Management
Chaoyang University of Technology
168 Gifeng E. Rd., Wufeng,
Taichung County, Taiwan 413 , R.O.C.
Email: mshwang@mail.cyut.edu.tw
Fax: 886-4-23742337

August 17, 2001

*This research was partially supported by the National Science Council, Taiwan, R.O.C., under contract no.: NSC90-2213-E-324-004.

†Responsible for correspondence.

An Improvement of a Simple Authenticated Key Agreement Algorithm

Abstract

Soe and Sweeney's Simple Authenticated Key Agreement (SAKA) algorithm, based on the Diffie-Hellman method, is a password-based key agreement algorithm which is simpler than other published methods and prevents the man-in-the-middle attacks. However, SAKA is vulnerable to guessing attacks if passwords are poorly chosen. In this article, we further improve the SAKA method which is simpler than the SAKA algorithm and can defeat both the man-in-the-middle and guessing attacks.

Keywords: Cryptography, key exchange, man-in-the-middle attack, guessing attack.

1 Introduction

The Diffie-Hellman method [2] was proposed to provide two authenticated parties to agree on a session key in an insecure channel. However, since the exchanged messages were not authenticated by the two parties, it is vulnerable to the man-in-the-middle attacks.

To overcome this shortcoming, two major approaches had been taken [5]. One approach, such as the station-to-station protocol developed by Diffie et al. [3], utilizes certificates from a trusted third party to certify the ownership of the keys. Therefore, the middle man cannot longer impersonate the messages without being noticed. However, this approach suffers from the difficulty of extension to a larger system.

The other approach, such as the encrypted key exchange method developed by Bellovin and Merritt [1], assumes a secret password has been shared in advance by two parties and all exchanged messages can be encrypted by this shared secret password. Though this approach defeats the man-in-the-middle attacks, it is too complicated and patented.

Seo and Sweeney proposed a simple authenticated key agreement (SAKA) algorithm [9] which is based on the Diffie-Hellman method. SAKA assumes Alice and Bob share a common password P in advance. Both Alice and Bob calculates Q and Q^{-1} from P by using the same equation. By incorporating Q and Q^{-1}, SAKA algorithm is described as follows:

1. Alice chooses a random number r_a and sends Bob

$$X_a = g^{r_a Q} \bmod n$$

2. Bob chooses a random number r_b and sends Alice

$$X_b = g^{r_b Q} \bmod n$$

3. Alice calculates

$$K_a = X_b^{r_a Q^{-1}} \bmod n$$

4. Bob calculates

$$K_b \quad = \quad X_a^{r_b Q^{-1}} \bmod n$$

Soe and Sweeney show that the middle man can neither guess the public values such as ($g^a \bmod n$) nor alter the values without being noticed. Also, SAKA generates the same amount of traffic as the Diffie-Hellman method with only two communications required to agree on a session key. Furthermore, Bob and Alice can validate the session key if ciphered messages cannot be decrypted correctly.

Though the SAKA algorithm is superior than other published schemes, it suffers from the guessing attacks if the chosen password P is small [4, 7, 6, 8]. If the chosen P is large enough, we do not see the necessity of calculating both Q and Q^{-1}. With the public value g replaced by P, the size of P is no longer a concern and the computation overhead is smaller since both Q and Q^{-1} are not required.

In the following section, we describe an improved key agreement algorithm which is simpler than SAKA. Note that the simplicity of this algorithm does not degrade any features provided by SAKA.

2 The Improvement

Similar to SAKA, we require Alice and Bob pre-share a common password P. By using a large prime number n which is made publicly available, our method is similar to the Diffie-Hellman method and is described as follows:

1. Alice chooses a random large number r_a and sends Bob

$$X_a = P^{r_a} \bmod n$$

2. Bob chooses a random large number r_b and sends Alice

$$X_b = P^{r_b} \bmod n$$

3. Alice calculates

$$K_a = X_b^{r_a} \bmod n$$

4. Bob calculates

$$K_b = X_a^{r_b} \bmod n$$

Since

$$\begin{aligned} K_a &= X_b^{r_a} \bmod n \\ &= P^{r_b r_a} \bmod n \\ &= X_a^{r_b} \bmod n \\ &= K_b, \end{aligned}$$

Alice and Bob agree on a session key in two communications.

3 Analysis

In this section, we analyze the proposed algorithm with the SAKA algorithm in aspect of performance and cryptanalysis.

3.1 Performance Analysis

In the proposed algorithm, it is not necessary to calculate both Q and Q^{-1} for each key exchange. Furthermore, instead of computing g^{rQ} and $X^{rQ^{-1}}$, we compute P^r and X^r, respectively, and thus the multiplications in the exponential parts of the above computations are not longer required.

3.2 Cryptanalysis

Supposed a middle man eavesdrops messages in an insecure channel. When the middle man receives X_a in step 1, with only knowing the value of n, he cannot guess r_a since the problem is combined with the discrete logarithm and the secret password P. With the same argument, the middle man cannot guess the value of r_b either. If the middle man intercepts X_b, makes up a fake $X_m = F^{r_m} \bmod n$ where F is a fake password and r_m is a random number generated by the middle man, and sends X_m to Alice, Alice calculates the fake session key as

$$K_a' = X_m^{r_a} \bmod n.$$

Since the middle man cannot obtain r_a from $X_a (= P^{r_a} \bmod n)$, the middle man cannot agree with Alice on the fake session key K_a'.

Supposed that Alice sends a message M encrypted with K_a' (the ciphertext is $M^{K_a'}$). Since

$$\begin{aligned} M^{K_a'} &= M^{X_m^{r_a} \bmod n} \\ &= M^{F^{r_m r_a} \bmod n} \end{aligned}$$

and since the middle man knows only $X_a = P^{r_a} \bmod n$ but not r_a and P, the middle man cannot calculate K_a' to get M.

4 Conclusions

Soe and Sweeney's simple authenticated key agreement algorithm is based on the Diffie-Hellman method. With a pre-shared password between two parties, it allows two parties agree on a session key with only two communications, prevents the man-in-the-middle attacks, and is simpler than other published schemes. The major drawback of the SAKA algorithm is its vulnerability to the guessing attacks. In this article, we further improve Soe and Sweeney's scheme so that it is even simpler than the SAKA algorithm and defeats both the man-in-the-middle and guessing attacks.

References

[1] S. Bellovin and M. Merrit, "Encrypted key exchange: Password-based protocols secure against dictionary attacks," in *Proceedings of IEEE Computer Society Symposium on Research in Security and Privacy*, pp. 72–84, Oakland, May 1992.

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

[3] W. Diffie, P. C. Van Oorshot, and M. J. Wiener, "Authentication and authenticated key exchanges," *Designs, Codes and Cryptography*, vol. 2, pp. 107–125, 1992.

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

[5] Min-Shiang Hwang, C. C. Chang, and I. C. Lin, "Security enhancement for the simple authentication key agreement algorithm," in *The 24th IEEE Computer Society International Computer Software and Applications Conference (COMPSAC'2000)*, pp. 113–115, Taipei, Oct. 2000.

[6] Min-Shiang Hwang, Cheng-Chi Lee, and Yuan-Liang Tang, "An improvement of SPLICE/AS in WIDE against guessing attack," *International Journal of Informatica*, vol. 12, no. 2, pp. 297–302, 2001.

[7] Min-Shiang 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.

[8] G. Li, M. A. Lomas, R. M. Needham, and J. H. Saltzer, "Protecting poorly chosen secrets from guessing attacks," *IEEE Journal on Selected Areas in Communications*, vol. 11, pp. 648–656, June 1993.

[9] Dong Hwi Seo and P. Sweeney, "Simple authenticated key agreement algorithm," *Electronics Letters*, vol. 35, pp. 1073–1074, June 1999.