Cryptanalysis of Security Enhancement for a Modified Authenticated Key Agreement Protocol

Kou-Min Cheng[1], Ting-Yi Chang[2], and Jung-Wen Lo[3]
(Corresponding author: Jung-Wen Lo)

Department of Information Management, Chaoyang University of Technology[1]
168 Gifeng E. Rd., Wufeng, Taichung County Taiwan 413, R.O.C.
Graduate Institute of e-Learning, Changhua University of Education[2]
No.1 Jin-De Road, 500 Changhua City, Taiwan, R.O.C.
Department of Information Management, National Taichung Institute of Technology[3]
129 Sec. 3, San-min Rd., Taichung, Taiwan 404, R.O.C. (Email: asalo@ntit.edu.tw)
(Received Dec. 10, 2009; revised and accepted Jan. 3, 2010)

Abstract

Recently, Chang et al. proposed a security enhancement in Ku and Wang's authenticated key agreement protocol. Two parties employ the pre-shared password to agreement a common session key via insecure network. However, in this article, we will show that Chang et al.'s scheme is suffer from the backward replay attack and the off-line password guessing attack.

Keywords: Cryptography, information security, key agreement, key exchange, password

1 Introduction

The Diffie-Hellman key agreement protocol [6] is a method for establishing a common session key to be shared between two parties (named, Alice and Bob) over an insecure network. Then, they can use the session key to be the symmetrical key (such as DES, Rijndael) to establish a secure communication channel. The common session key can be determined either party based on her/his own secret key and the partner's public key. The security of session key comes from the intractability of the discrete logarithm problem. However, two parties in the Diffie-Hellman scheme do not authenticate each other, an adversary (named, Eve) can mount the man-in-middle attack to share a common session between Alice and Bob by masquerading Alice and Bob. Therefore, to authenticate the identity of the party is necessarily [1, 3, 4, 5, 7, 9, 11, 13, 14, 16, 18, 19, 20, 21].

Seo and Sweeney [15] proposed a simple authenticate key agreement scheme, which uses the pre-shared secret password technology to ensure the identity of the party and verification of the session key. However, Tseng [17] pointed out that verification of the session key could not be achieved in their protocol by mounting the replay attack. The adversary can successfully convince the honest party of a wrong session key. Tseng further proposed an improved scheme to repair the security flaw in Seo and Sweeney's protocol.

Unfortunately, Ku and Wang [12] pointed that Tseng's improved protocol is still vulnerable to the backward replay attack without modification and the modification attack. Under the backward replay attack, the adversary can impersonate one communicating party to fool the other one into believing the wrong session key by replaying the exchanged message. Under the modification attack, the adversary interposes in the line between two communicating parties and modifies the exchanged message to convince one party of a wrong session key. They further proposed an improved scheme to withstand those attacks.

Recently, Hsu et al. [8] and Chang et al. [2] separately pointed that Ku and Wang's improved protocol is still vulnerable to the modification attacks. At the same time, they separately proposed the security enhancement in Ku and Wang's protocol. However, in this article, we will point that Chang et al.'s enhancement is suffer from the backward replay attack and the off-line password guessing attack (dictionary attack). Similar to Ku and Wang's backward replay attack in Tseng protocol, the adversary can impersonate one communicating party to fool the other one into believing the wrong session key. By mounting the off-line password guessing attack, the adversary can guess a password off-line until he/she gets the correct one.

The organization of this article is as follows. In Section 2, we shall take a brief look at Chang et al.'s protocol. In Section 3, we shall show that the backward replay attack and the off-line password guessing attack crumble the security of Chang et al.'s scheme. Finally, we shall present our conclusion in Section 4.

2 Review Chang et al.'s Protocol

Initially, system chooses two public values g and n, where n is a large prime and g is a primitive element in $GF(n)$. Alice and Bob pre-shared a common password P and a predetermined way to generate two integers $Q \bmod n-1$ and $Q^{-1} \bmod n-1$ from the password P. Q must be unique value yielded by P, and relatively prime to $n-1$. The protocol is composed of two phases, the key establishment phase and the key verification phase, as follows.

The key establishment phase:

1) Alice chooses a random number a, computes $X_1 = g^{aQ} \bmod n$, and sends X_1 to Bob.
2) Bob chooses a random number b, computes $Y_1 = g^{bQ} \bmod n$, and sends Y_1 to Alice.
3) When Y_1 is received, Alice computes $Y = Y_1^{Q^{-1}} = g^b \bmod n$ and $K_A = Y^a = g^{ab} \bmod n$.
4) When X_1 is received, Bob computes $X = X_1^{Q^{-1}} = g^a \bmod n$ and $K_B = X^b = g^{ab} \bmod n$.

After this phase, Alice and Bob establish a common session key $K_A = K_B = g^{ab} \bmod n$.

The key verification phase:

1) Alice computes $Y_2 = (aY)^{Q^{-1}} \bmod n$ and sends it to Bob.
2) Bob computes $X_2 = (bX)^{Q^{-1}} \bmod n$ and sends it to Alice.
3) When X_2 is received, Alice obtains b by computing $b = (X_2)^Q / X \bmod n$ and checks the validity by the equation $g^b = Y \bmod n$.
4) When Y_2 is received, Bob obtains a by computing $a = (Y_2)^Q / Y \bmod n$ and checks the validity by the equation $g^a = X \bmod n$.

If the above verifications are correct, Alice and Bob are convinced that the session key $K_A = K_B = g^{ab} \bmod n$ is correct.

3 Security Flaws

In this section, we show that Chang et al.'s protocol is vulnerable to the backward replay attack and the off-line password guessing attack. Two attacks are separately mounted by Eve as follows.

The backward replay attack without modification: Upon intercepting $X_1 = g^{aQ} \bmod n$ in Step 1 of the key establishment phase, Eve impersonates as Bob to send $Y_1' = X_1 = g^{aQ} \bmod n$ to Alice. When Y_1' is received in Step 3 of the key establishment phase, Alice computes $Y = Y_1'^{Q^{-1}} = g^a \bmod n$ and $K_A = Y^a = g^{a^2} \bmod n$.

Upon intercepting $Y_2 = (aY)^{Q^{-1}} = (ag^a)^{Q^{-1}} \bmod n$ in Step 1 of the key verification phase, Eve impersonates as Bob to send $X_2' = Y_2 = (ag^a)^{Q^{-1}} \bmod n$ to Alice. When X_2 is received in Step 3 of the key verification phase, Alice computes $b = (X_2')^Q / X = ((ag^a)^{Q^{-1}})^Q / g^a = a \bmod n$ and checks the validity by the equation $g^a = Y \bmod n$. Obviously, the verification is correct. Alice will be fooled into believing the wrong session key K_A. On the other hand, Eve also can impersonate Alice to fool Bob into believing the wrong session key K_B.

The off-line password guessing attack: When Eve intercepts the messages X_1, Y_1, and Y_2 in an honest execution of the protocol between Alice and Bob, she can perform an off-line password guessing attack as follows. Eve first guesses the password P' and derives the corresponding $Q' \bmod n$ and $Q'^{-1} \bmod n$. Then, she can off-line verify the correctness of the guessed password P' by checking the following equation:

$$(X_1)^{Q'^{-1}} = g^{(Y_2)^{Q'} / (Y_1)^{Q'^{-1}}} \bmod n.$$

If it holds, Eve has guessed the correct password P'. From left-hand side of the above equation, we can obtain

$$\begin{aligned} (X_1)^{Q'^{-1}} &= (g^{aQ})^{Q'^{-1}} \bmod n, \\ &= g^a \bmod n. \end{aligned}$$

From right-hand side of the above equation, we can obtain

$$\begin{aligned} g^{(Y_2)^{Q'} / (Y_1)^{Q'^{-1}}} &= g^{(aY)^{Q^{-1}Q'} / (g^{bQ})^{Q'^{-1}}} \bmod n, \\ &= g^{(ag^b)/(g^b)} \bmod n, \\ &= g^a \bmod n. \end{aligned}$$

For the same reason, Eve can check the guessed password whether the following equation

$$Y_1^{Q'^{-1}} = g^{X_2^{Q'} / X_1^{Q'^{-1}}} \bmod n$$

holds or not by intercepting the messages Y_1, X_1, and X_2.

4 Conclusion

In fact, people hardly find the long random strings to be their passwords; rather, they prefer natural language phrases that they can remember easily. Nevertheless, natural language phrases as password are draw from a rather limited set of possibilities. In this article, we have separately shown that the backward replay attack and the off-line password guessing attack in Chang et al.'s protocol. Those attacks seriously threaten the security of their protocol.

References

[1] T. Cao and P. Shen, "Cryptanalysis of two RFID authentication protocols," *International Journal of Network Security*, vol. 9, no. 1, pp. 95–100, 2009.

[2] C. C. Chang, K. F. Hwang, and I. C. Lin, "Security enhancement for a modified authenticated key agreement protocol," *International Journal of Computational and Numerical Analysis and Applications*, vol. 3, no. 1, pp. 1–7, 2003.

[3] A. Chaturvedi and S. Lal, "An authenticated key agreement protocol using conjugacy problem in braid groups," *International Journal of Network Security*, vol. 6, no. 2, pp. 181–184, 2008.

[4] K. K. R. Choo, "Revisit of McCullagh-Barreto two-party ID-based authenticated key agreement," *International Journal of Network Security*, vol. 1, no. 3, pp. 154–160, 2005.

[5] K. K. R. Choo, "Revisiting Lee, Kim, & Yoo authenticated key agreement protocol," *International Journal of Network Security*, vol. 2, no. 1, pp. 64–68, 2006.

[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] S. Hong, "Queue-based group key agreement protocol," *International Journal of Network Security*, vol. 9, no. 2, pp. 135–142, 2009.

[8] C. L. Hsu, T. S. Wu, T. C. Wu, and C. Mitchell, "Cryptanalysis of enhancement for simple authenticated key agreement algorithm," *Applied Mathematics and Computation*, vol. 142, no. 2-3, pp. 305–308, 2003.

[9] M. S. Hwang, C. W. Lin, and C. C. Lee, "Improved Yen-Joye's authenticated multiple-key agreement protocol," *IEE Electronics Letters*, vol. 38, no. 23, pp. 1429–1431, 2002.

[10] M. S. Hwang and H. Y. Liu, "Authenticated encryption schemes: Current status and key issues," *International Journal of Network Security*, vol. 1, no. 2, pp. 61-73, 2005.

[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] W. C. Ku and S. D. Wang, "Cryptanalysis of modified authenticated key agreement protocol," *IEE Electronics Letters*, vol. 36, no. 21, pp. 1770–1771, 2000.

[13] Eric J. L. Lu and M. S. Hwang, "An improvement of a simple authenticated key agreement algorithm," *Pakistan Journal of Applied Sciences*, vol. 2, no. 1, pp. 64–65, 2002.

[14] K. V. Mangipudi, R. S. Katti, and H. Fu, "Authentication and key agreement protocols preserving anonymity," *International Journal of Network Security*, vol. 3, no. 3, pp. 259–270, 2006.

[15] D. Seo and P. Sweeney, "Simple authenticated key agreement algorithm," *IEE Electronics Letters*, vol. 35, no. 13, pp. 1073–1074, 1999.

[16] J. L. Tsai, "Efficient nonce-based authentication scheme for session initiation protocol," *International Journal of Network Security*, vol. 9, no. 1, pp. 12–16, 2009.

[17] Y. M. Tseng, "Weakness in simple authenticated key agreement protocol," *IEE Electronics Letters*, vol. 36, no. 1, pp. 48–49, 2000.

[18] S. Wang, Z. Cao, and H. Bao, "Efficient certificateless authentication and key agreement (CL-AK) for grid computing," *International Journal of Network Security*, vol. 7, no. 3, pp. 342–347, 2008.

[19] S. Wang, Z. Cao, and F. Cao, "Efficient identity-based authenticated key agreement protocol with PKG forward secrecy," *International Journal of Network Security*, vol. 7, no. 2, pp. 181–186, 2008.

[20] S. Wu and Y. Zhu, "Proof of forward security for password-based authenticated key exchange," *International Journal of Network Security*, vol. 7, no. 3, pp. 335–341, 2008.

[21] Z. Yong, J. F. Ma, and S. J. Moon, "An improvement on a three-party password-based key exchange protocol using weil pairing," *International Journal of Network Security*, vol. 11, no. 1, pp. 14–19, 2010.

Kou-Min Cheng received the M.S. degree from the Information Management at Chaoyang University of Technology, Taichung, Taiwan, Republic of China. His current research interests include e-commerce and and information security.

Ting-Yi Chang received his M.S. from the Graduate Institute of Computer Science and Information Engineering at Chaoyang University of Technology, and his Ph.D in the Department of Computer Science at National Chiao Tung University, Taiwan. Currently, he is an Assistant Professor with the Graduate Institute of e-Learning, National Changhua University, Taiwan. His current research interests include e-Learning, information security, cryptography, and mobile communications.

Jung-Wen Lo received his B.S. degree in Information and Computer Engineering in 1987 from Chung Yuan Christian University, Chung-Li, Taiwan and the M.S. degree in Computer Science & Information Systems in 1994 from Texas A&M University at Commerce, Texas, U.S.A. He is working for his Ph.D. program in the Department of Computer Science at National Chung Hsing University, Taichung, Taiwan. He was an Associate Engineer in Product Development Department of Institute for Information Industry from 1994 to 1996. Since August 1998, he has been an Instructor of the Department of Information Management at National Taichung Institute of Technology, Taichung, Taiwan. His research interests include electronic commerce, network security and computer networks.