



ISSN: 2319-5967

ISO 9001:2008 Certified

International Journal of Engineering Science and Innovative Technology (IJESIT)

Volume 2, Issue 1, January 2013

A Study of Cryptanalysis with Security Enhancement for a Modified Authenticated Key Agreement Protocol

Abhishek Shukla , Mohd.Vakil, Sakil Ahmad Ansari

Abstract— A 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 the scheme is suffer from the backward replay attack and the offline password guessing attack.

Index Terms— Cryptography, Information Security, Key Agreement, Key Exchange, Password.

I. INTRODUCTION

The Diffie-Hellman key agreement protocol [5] 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 [2, 3, 4, 7, 8, 10, 11, 15, and 14]. Seo and Sweeney [12] 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 [13] 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 [9] 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. [6] and Chang et al. [1] 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 offline 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 offline password guessing attack, the adversary can guess a password offline 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 offline password guessing attack crumble the security of Chang et al.'s scheme. Finally, we shall present our conclusion in Section 4.



ISSN: 2319-5967

ISO 9001:2008 Certified

International Journal of Engineering Science and Innovative Technology (IJESIT)

Volume 2, Issue 1, January 2013

II. 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.

III. SECURITY FLAWS

In this section, we show that Chang et al.'s protocol is vulnerable to the backward replay attack and the offline 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



ISSN: 2319-5967

ISO 9001:2008 Certified

International Journal of Engineering Science and Innovative Technology (IJESIT)

Volume 2, Issue 1, January 2013

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

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

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

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

IV. 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 drawn 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.

ACKNOWLEDGMENT

Part of this research was supported by the National Science Council, Taiwan, R.O.C., under contract no. NSC91-2213-E-324-003.

REFERENCES

- [1] Chin-Chen Chang, Kuo-Feng Hwang, and Iuon-Chang Lin. Security enhancement for a modified authenticated key agreement protocol. *International Journal of Computational and Numerical Analysis and Applications*, 3(1):1{7, 2003.
- [2] Atul Chaturvedi and Sunder Lal. An authenticated key agreement protocol using conjugacy problem in braid groups. *International Journal of Network Security*, 6(2):181-184, 2008.
- [3] Kim-Kwang Raymond Choo. Revisit of McCullagh-Barreto two-party ID-based authenticated key agreement. *International Journal of Network Security*, 1(3):154-160, 2005.
- [4] Kim-Kwang Raymond Choo. Revisiting Lee, Kim, & Yoo authenticated key agreement protocol. *International Journal of Network Security*, 2(1):64-68, 2006.
- [5] W. Diffie and M. E. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, IT-22(6):644{654, Nov. 1976.
- [6] Chien-Lung Hsu, Tzong-Sun Wu, Tzong-Chen Wu, and Chris Mitchell. Cryptanalysis of enhancement for simple authenticated key agreement algorithm. *Applied Mathematics and Computation*, 142(2-3):305{308, 2003.
- [7] Min-Shiang Hwang, Chih-Wei Lin, and Cheng-Chi Lee Improved Yen-Joye's authenticated multiple-key agreement protocol. *IEE Electronics Letters*, 38(23):1429-1431, 2002.
- [8] Wen-Sheng Juang and Jing-Lin Wu. Efficient user authentication and key agreement with user privacy protection. *International Journal of Network Security*, 7(1):120-129, 2008.
- [9] Wei-Chi Ku and Sheng-De Wang. Cryptanalysis of modified authenticated key agreement protocol. *IEE Electronics Letters*, 36(21):1770-1771, 2000.
- [10] Eric Jui-Lin Lu and Min-Shiang Hwang. An improvement of a simple authenticated key agreement algorithm. *Pakistan Journal of Applied Sciences*, 2(1):64-65, 2002.
- [11] Kumar V. Mangipudi, Rajendra S. Katti, and Huirong Fu. Authentication and key agreement protocols preserving anonymity. *International Journal of Network Security*, 3(3):259-270, 2006.
- [12] D. Seo and P. Sweeney. Simple authenticated key agreement algorithm. *IEE Electronics Letters*, 35(13):1073-1074, 1999.
- [13] Yuh-Min Tseng. Weakness in simple authenticated key agreement protocol. *IEE Electronics Letters*, 36(1):48-49, 2000.



ISSN: 2319-5967

ISO 9001:2008 Certified

International Journal of Engineering Science and Innovative Technology (IJESIT)

Volume 2, Issue 1, January 2013

- [14] Shengbao Wang, Zhenfu Cao, and Haiyong Bao. Efficient certificate less authentication and key agreement (CL-AK) for grid computing. International Journal of Network Security, 7(3):342{347, 2008.
- [15] Shengbao Wang, Zhenfu Cao, and Feng Cao. Efficient identity-based authenticated key agreement protocol with pkg forward secrecy. International Journal of Network Security, 7(2):181-186, 2008.

AUTHOR BIOGRAPHY



Abhishek Shukla, He did his Master of Computer Application (MCA) from Dr. Ram Manohar Lohia Avadh University, Faizabad, U.P., India in 2007 and pursuing Ph.D. from Singhania University, Pachari Beri, (Rajasthan), India. His major field of study is Cryptography and network security. His current research area is secure mailing protocol and application. He has more than five year experience. He is working as Lecturer, R.D. Engineering College, Ghaziabad, (U.P.) India. Mr. Shukla is the life-time member of IAENG, IACSIT, EASST, CSTA, IAOE and SDIWC. Mr. Shukla is also as a Associate Editor of **International Journal of Modern Education and Computer Science** journal and Editor of **International Journal of Societal Applications of Computer Science**. He is the author/co-author of more than 12 publications in International and 02 publications in National journals and conferences.



Mohd. Vakil He did his B.Tech (Computer Sc. & Engg.) from KNIT Sultanpur Dr. Ram Manohar Lohia Avadh University, Faizabad, U.P., India in 2001 , M. Tech KNIT Sultanpur (UPTU, Lucknow) in 2007 and pursuing Ph.D. from Mewar University since February 2009, India. His major field of study is Cryptography and network security. His current research area is secure mailing protocol and application. He has more than 10 years experience in Teaching. He is working as Head and Associate Professor, R.D. Engineering College, Ghaziabad, (U.P.) India. Mr. Vakil is the member of Indian Society of Technical Education He is the author/co-author of more than 04 publications in International journals.



Sakil Ahmad Ansari He did his B.Tech (Computer Sc. & Engg.) from Ideal Institute of Technology Ghaziabad U.P., India in 2009 and pursuing M.Tech. from Al-Falah Engineering College Faridabad, India. His major field of study is Cryptography and network security. His current research area is secure mailing protocol and application. He has more than five year experience. He is working as Lecturer, R.D. Engineering College, Ghaziabad, (U.P.) India.