Available online at www.sciencedirect.com
SCIENCE DIRECT®
ELSEVIER Applied Mathematics and Computation 171 (2005) 771–774
APPLIED MATHEMATICS AND COMPUTATION
www.elsevier.com/locate/amc

Cryptanalysis of the improved authenticated key agreement protocol

Ting-Yi Chang [a], Chou-Chan Yang [b], Ya-Wen Yang [c,*]

[a] *Department of Computer and Information Science, National Chiao Tung University, 1001 Ta Hsueh Road, Hsinchu, Taiwan, ROC*
[b] *Department of Information and Communication Engineering, Chaoyang University of Technology, 168 Gifeng E. Rd., Wufeng 413, Taichung County, Taiwan, ROC*
[c] *Graduate Institute of Networking and Communication Engineering, Chaoyang University of Technology, 168 Gifeng E. Rd., Wufeng 413, Taichung County, Taiwan, ROC*

Abstract

Hsu et al. recently pointed out that the Ku–Wang scheme is vulnerable to modification attack and further proposed an improvement on their scheme. However, this article will show the improvement which they claim is still vulnerable by off-line password guessing attack.
© 2005 Published by Elsevier Inc.

Keywords: Cryptography; Information security; Key agreement; Key exchange

1. Introduction

In 1976, the key agreement protocol was introduced by Diffie and Hellman [1]. The two parties can establish a secret session key over an insecure channel

* Corresponding author.
E-mail address: ccyang@cyut.edu.tw (C.-C. Yang).

0096-3003/$ - see front matter © 2005 Published by Elsevier Inc.
doi:10.1016/j.amc.2005.01.086

which is based on the difficulty of computing discrete logarithms over a finite field. However, Diffie and Hellman's scheme have a serious security flaw which is vulnerable to the man-in-middle attack. It results from the unauthenticated participants.

In order to prevent man-in-middle attacks, Seo and Sweeney [5] proposed a simple authenticated key agreement protocol, which additionally use the pre-shared password method to provide user authentication. In their scheme, two parties share a secret password before the protocol begins. The session key can be established with user authentication and two parties can verify the validity of session key. Unfortunately, Sun [6], Tseng [7], and Lu et al. [4] separately showed the fact that the Seo–Sweeney scheme is vulnerable to the mounting replay attack and dictionary attack. Indeed, the honest party can be fool into believing a wrong session key by replaying the message sent from honest party himself. At the same time, Tseng proposed an improved scheme to withstand the replay attack. On the other hand, Sun [6] and Lu et al. [4] pointed out the Seo–Sweeney scheme is vulnerable to off-line password guessing attack (dictionary attack). That is, an attacker can guess a password off-line until he/she gets the correct one.

Later, Ku and Wang [3] showed that Tseng's improved scheme is still vulnerable to backward replay attack and modification attack. The backward replay attack is that the honest party can be fool into believing a wrong session key by an adversary masquerades as the one communication party to replay the exchanged message. The modification attack is that an adversary can modify the exchanged message by interposing in the line between two communicating parties and fool one party into believing a wrong session key. To repair the security flaws, they further proposed an improved scheme to enhance the security.

In 2003, Hsu et al. [2] pointed out the Ku–Wang scheme is still vulnerable by the modification attack. Moreover, they improved the key validation stage of Ku and Wang's protocol by using the identities of two communicators and a one-way hash function. However, in this article, we will point out their improved scheme is vulnerable by the off-line password guessing attack.

The organization of this article is as follows. In the next section, we will brief review Hsu et al.'s scheme. In Section 3, we will show that the off-line password guessing attack threatens the security of their scheme. Finally, we shall give a brief conclusion in Section 4.

2. Brief review of Hsu et al.'s scheme

As the Diffie–Hellman scheme, the system publishes a one-way hash function $h(\cdot)$ and two values n and g, where n is a large prime and g is a generator with order $n-1$ in $GF(n)$. In the system, Alice and Bob separately have the identities id_A and id_B. They share a secret password P and a predetermined

way to generate the two integers $Q \bmod n$ and $Q^{-1} \bmod n$ before the protocol begins. The protocol is composed of two phases, the key establishment phase and the key validation phase, as follows.

2.1. Key establishment phase

(e.1) Alice randomly selects an integer a and computes $X = g^{aQ} \bmod n$. Then, she sends X to Bob.
(e.2) Bob randomly selects an integer b and computes $Y = g^{bQ} \bmod n$. Then, he sends Y to Alice.

After receiving Y and X, Alice and Bob can separately compute the session key $K_A = (Y^{Q^{-1}})^a = g^{ab} \bmod n$ and $K_B = (X^{Q^{-1}})^b = g^{ab} \bmod n$.

2.2. Key validation phase

(v.1) Alice computes the hash value $A = h(id_A, K_A)$ and sends it to Bob.
(v.2) Bob computes the hash value $B = h(id_B, K_B)$ and sends it to Alice.

After receiving A, Bob computes the hash $h(id_A, K_B)$ and then verifies the consistency between the computed $h(id_A, K_B)$ and the received A. If the result is positive, Bob is convinced that K_B is validated. After receiving B, Alice computes the hash $h(id_B, K_A)$ and then verifies the consistency between the computed $h(id_B, K_A)$ and the received B. If the result is positive, Alice is convinced that K_A is validated.

3. The off-line password guessing attack

In this section, we show that Hsu et al.'s protocol is vulnerable to off-line password guessing attack. Assume that Eve is an adversary, who interposes in the communicating line between Alice and Bob.

In the key establishment phase, Eve intercepts $X = g^{aQ} \bmod n$ in Step (e. 1) sent by Alice and records it. Upon intercepting message Y in Step (e. 2) sent by Bob, Eve impersonates Bob to exchange message with Alice. Eve randomly selects an integer e and compute $Y' = g^e \bmod n$ to replace Y. After receiving Y', Alice computes $K_A = (Y'^{Q^{-1}})^a = g^{eQ^{-1}a} \bmod n$. In the key validation phase, upon intercepting message $A = (id_A, K_A) = (id_A, g^{eQ^{-1}a} \bmod n)$ in Step (v. 1) sent by Alice, Eve can perform an off-line password guessing attack as follows. Eve first guess a password P and derives a corresponding $Q \bmod n$; thus, she can verify the correctness of the guessed password by checking whether $A = (id_A, (X^e)^{Q^{-2}} \bmod n)$ holds or not. If it holds, Eve has guessed the correct password P because of $A = h(id_A, (X^e)^{Q^{-2}} \bmod n) = h(id_A, g^{aeQ^{-1}} \bmod n)$.

For the same reason, Eve also can impersonate Alice to exchange the message with Bob. Upon intercepting message B, Eve can verify the correctness of the guessing password.

4. Conclusion

People find passwords difficult to use long random strings; rather, they prefer natural language phrases that they can recognize easily. Nevertheless, natural language phrases as password are drawn from a rather limited set of possibilities. In this article, we have presented the off-line password guessing attack to subvert the security of Hsu et al.'s scheme. The adversary can guess a password off-line until he/she gets the correct one.

Acknowledgement

This research was partially supported by the National Science Council, Taiwan, ROC, under contract no. NSC90-2213-E-324-004.

References

[1] W. Diffie, M.E. Hellman, New directions in cryptography, IEEE Transactions on Information Theory IT-22 (6) (1976) 644–654.
[2] Chien-Lung Hsu, Tzong-Sun Wu, Tzong-Chen Wu, Chris Mitchell, Cryptanalysis of enhancement for simple authenticated key agreement algorithm, Applied Mathematics and Computation 142 (2–3) (2003) 305–308.
[3] Wei-Chi Ku, Sheng-De Wang, Cryptanalysis of modified authenticated key agreement protocol, IEE Electronics Letters 36 (21) (2000) 1770–1771.
[4] Eric Jui-Lin Lu, Cheng-Chi Lee, Min-Shiang Hwang. Cryptanalysis of some authenticated key agreement protocols, International Journal of Computational and Numerical Analysis and Applications, in press.
[5] D. Seo, P. Sweeney, Simple authenticated key agreement algorithm, IEE Electronics Letters 35 (13) (1999) 1073–1074.
[6] H. Sun, On the security of simple authenticated key agreement algorithm, in: Proceedings of the Management Theory Workshop'2000, 2000.
[7] Yuh-Min Tseng, Weakness in simple authenticated key agreement protocol, IEE Electronics Letters 36 (1) (2000) 48–49.