Improvement of modified authenticated key agreement protocol

Chien-Lung Hsu[‡], Tzong-Sun Wu*, Tzong-Chen Wu[‡], Chris Mitchell[†]

[‡] Department of Information Management
National Taiwan University of Science and Technology
Taipei, Taiwan 106, Republic of China

* Department of Information Management
Huafan University
Taipei, Taiwan 223, Republic of China

[†] Information Security Group
Royal Holloway, University of London
Egham, Surrey TW20 0EX, UK

*Correspondence to:
Assistant professor Tzong-Sun Wu, Ph. D.
Department of Information Management
Huafan University
No. 1, Huafan Road, Shihtin Hsiang, Taipei Hsien, 223
Taiwan, Republic of China
E-mail: tswu99@seed.net.tw
Tel: +886-2-2663-2102 ext 4356
Fax: +886-2-2663-1119

Improvement of modified authenticated key agreement protocol

Chien-Lung Hsu[‡], Tzong-Sun Wu*, Tzong-Chen Wu[‡], Chris Mitchell[†]

Abstract

Recently, Ku and Wang showed that Tseng's modified authenticated key agreement protocol is vulnerable to two attacks and proposed an improvement to withstand these attacks. However, this letter will show that this improvement is still vulnerable to the modification attack, which is contrary to their claims. Additionally, we proposed an improvement to eliminate this security flaw.

Keywords: Authenticated key agreement, Modification attack, Cryptanalysis

1. Introduction

Diffie-Hellman key agreement protocol [1] is the first practical asymmetric cryptographic technique for allowing two parties who never met in advance to establish a common secret key over an insecure channel. However, the original Diffie-Hellman protocol is vulnerable to the *man-in-middle attack*, i.e., an adversary interposing in the line between two communicating parties could masquerade as one communicating party to cheat the other one. This attack is caused by the fact that the Diffie-Hellman protocol does not authenticate the participants.

To strengthen Diffie-Hellman key agreement protocol, Seo and Sweeney [2] employed a pre-shared secret password method to provide user authentication. In their protocol, two communicating parties, who share a common secret password in advance, can exchange two messages to establish the session key. Moreover, they can validate the session key by exchanging two extra messages. Unfortunately, Tseng [3] pointed out that the key validation of the Seo-Sweeney protocol is vulnerable to the replay attack. Under this attack, the adversary can successfully convince the honest party of a wrong session key. To prevent this attack, Tseng proposed an improvement to enhance the key validation.

Recently, Ku and Wang [4] demonstrated two attacks on Tseng's enhancement. The first one is called backward replay without modification, in which the adversary can masquerade as one communicating party to fool the other one into believing the wrong session key by replaying the exchanged message. The second one is called modification attack, in which the adversary interposing in the line between two communicating parties can manipulate the exchanged message to convince one party of a wrong session key. They further proposed a countermeasure to eliminate these security flaws inherent in Tseng's improved protocol. However, this letter will show that their method is still vulnerable to the modification attack, which is contrary to their claims. We first gave brief description of their scheme and then proposed an improvement to strengthen the protocol.

2. Brief review of Ku-Wang scheme

Let n be a large prime and $g \in Z_n$ a generator with order n – 1. Assume that two communicating parties, Alice and Bob, share a common password P in advance. Alice and Bob can precompute two integers Q and $Q^{-1} (\bmod n)$ from P in any predetermined way before performing the key agreement protocol. Detailed description of this protocol is given below.

(1) *Key establishment*: Procedure of establishing the session key shared between Alice and Bob is described as follows.

$$\begin{tikzcd}[column sep=huge]
\boxed{\text{Alice}} \arrow[r, shift left, "\text{(k.1) } X_1 = g^{aQ} \bmod n"] & \boxed{\text{Bob}} \arrow[l, shift left, "\text{(k.2) } Y_1 = g^{bQ} \bmod n"]
\end{tikzcd}$$

Alice randomly chooses an integer a, computes $X_1 = g^{aQ}$ mod n, and then sends message (k.1) to Bob. By the same way, Bob sends message (k.2) to Alice, where b is a random number chosen by Bob. After that, Alice first computes $Y = Y_1{}^{Q^{-1}} = g^b$ (mod n) and then derives the session key K_1 by $K_1 = Y^a$ mod n. Similarly, Bob can obtain the session key $K_2 = X^b$ mod n, where $X = X_1{}^{Q^{-1}} = g^a$ (mod n). Note that the shared session key is regarded as $K_1 = K_2 = g^{ab}$ (mod n).

(2) *Key validation*: To check the validity of the established session key, Alice and Bob should cooperatively perform the following protocol:

$$\begin{tikzcd}[column sep=huge]
\boxed{\text{Alice}} \arrow[r, shift left, "\text{(v.1) } X_2 = K_1{}^Q \bmod n"] & \boxed{\text{Bob}} \arrow[l, shift left, "\text{(v.2) } X = X_1{}^{Q^{-1}} \bmod n"]
\end{tikzcd}$$

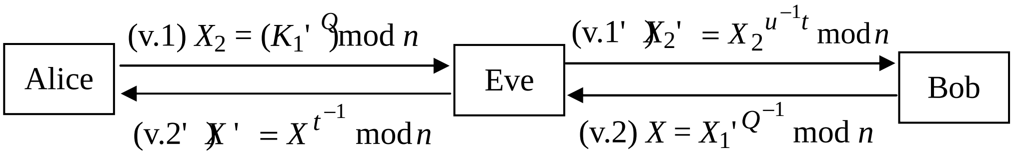
Alice computes $X_2 = K_1{}^Q$ mod n and then sends message (v.1) to Bob. Upon receiving message (v.1) from Alice, Bob checks whether if $X_2{}^{Q^{-1}}$ mod $n = K_2$. If it holds, Bob is convinced that K_2 is validated and then sends message (v.2) to Alice. On the other side, if $X = g^a$ (mod n) holds, then Alice believes that K_1 is verified.

3. Modification attack and the improvement

Let Eve be an active adversary who interposes the communication between Alice and Bob. In the key establishment, Eve could manipulate the exchanged messages to plot the modification attack as follows.

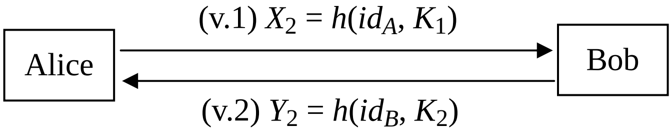
$$\begin{tikzcd}[column sep=huge]
\boxed{\text{Alice}} \arrow[r, shift left, "\text{(k.1) } X_1 = g^{aQ} \bmod n"] & \boxed{\text{Eve}} \arrow[l, shift left, "\text{(k.2') } Y_1' = Y_1{}^u \bmod n"] \arrow[r, shift left, "\text{(k.1') } X_1' = X_1{}^t \bmod n"] & \boxed{\text{Bob}} \arrow[l, shift left, "\text{(k.2) } Y_1 = g^{bQ} \bmod n"]
\end{tikzcd}$$

Upon intercepting message (k.1) sent by Alice, Eve can replace it with message (k.1'), where t is a random integer arbitrarily chosen by her. Similarly, Eve chooses another random integer u, computes $Y_1' = Y_1^u \bmod n$, and replaces message (k.2) sent by Bob with message (k.2'). Here, the session key obtained by Alice is $K_1' = g^{abu} \pmod{n}$, while that obtained by Bob is $K_2' = g^{abt} \pmod{n}$. To convince Alice and Bob of K_1' and K_2', Eve will intervene in the key validation as follows.


Alice
Eve
Bob
(v.1) $X_2 = (K_1')^Q \bmod n$
(v.1') $X_2' = X_2^{u^{-1}t} \bmod n$
(v.2') $X' = X^{t^{-1}} \bmod n$
(v.2) $X = X_1'^{Q^{-1}} \bmod n$

On seeing message (v.1) sent by Alice, Eve replaces it with message (v.1'). Similarly, Eve replaces messages (v.2) with (v.2'). Since $X_2'^{Q^{-1}} = g^{abt} = K_2' \pmod{n}$, Bob will be fooled into believing that his obtained key K_2' is verified. Similarly, Alice is also deceived that K_1' is validated, since $X' = X^{t^{-1}} = g^a \pmod{n}$, where $X = X_1'^{Q^{-1}} = g^{at} \pmod{n}$. It is to see that although Eve cannot obtain K_1' or K_2', she can still fool Alice and Bob into believing their wrong session keys.

Improved key validation stage: To overcome this modification attack, the improved key validation is given as follows:



Alice uses her identifier id_A and K_1 to compute $X_2 = h(id_A, K_1)$, where h is a one-way hash function. Then, Alice sends message (v.1) to Bob. Similarly, Bob uses his identifier id_B and K_2 to compute $Y_2 = h(id_B, K_2)$ and then sends message (v.2) to Alice. Finally, Alice and Bob can validate their obtained session keys by checking if $Y_2 = h(id_B, K_1)$ and $X_2 = h(id_A, K_2)$, respectively.

4. Discussions and conclusions

Consider the scenario of the modification attack as mentioned above, Eve must compute g^{abt} mod n and send $X_2' = h(id_A, g^{abt} \bmod n)$ to Bob. However, it is impossible to obtain g^{abt} mod n since the problem is based on the intractability of solving the discrete logarithm problem and the difficulty of compromising the password. Hence, Eve cannot fool Bob into believing a wrong session key. For the same reason, Eve cannot cheat Alice to accept a wrong session key. Thus, the proposed improvement is secure against the modification attack. As compared with that of Ku and Wang's key validation, the computation complexities of the proposed improvement reduces two exponentiation operations but requires two more one-way hash function operations.

References

1 W. Diffie, M. Hellman, "New directions in cryptography", *IEEE Transactions on Information Theory*, Vol. IT-22, No. 6, 1976, pp. 644-654.

2 D.H. Seo, P. Sweeney, "Simple authenticated key agreement algorithm", *Electronics Letters*, Vol. 36, No. 13, 1999, pp. 1073-1074.

3 Y.M. Tseng, "Weakness in simple authenticated key agreement protocol", *Electronics Letters*, Vol. 36, No. 1, 2000, pp. 48-49.

4 W.C. Ku, and S.D. Wang, "Cryptanalysis of modified authenticated key agreement protocol", *Electronics Letters*, Vol. 36, No. 21, 2000, pp. 1770-1771.