Name of Workshop:

Workshop on Cryptology and Information Security

Title of the Paper:

Enhanced Authentication Key Agreement Protocol

Short Abstract:

Ku and Wang pointed out Tseng's protocol can't prevent two simple attacks. They also proposed a new protocol that can prevent those attacks. In this paper, the authors proposed an enhanced protocol that not only can prevent those attacks, but also has better efficiency in computation.

Authors:

Ren-Junn Hwang, Sheng-Hua Shiau and Kai-Jun Lin

Department of Computer Science and Information Engineering, Tamkang University, 151 Ying-chuan Road, Tamsui, Taipei County, Taiwan 251, Republic of China

E-mail: victor@mail.tku.edu.tw, 689190345@s89.tku.edu.tw

TEL: 886-2-26269951, 886-2-26228936

Contact Author:

Sheng-Hua Shiau

Department of Computer Science and Information Engineering, Tamkang University, 151 Ying-chuan Road, Tamsui, Taipei County, Taiwan 251, Republic of China

E-mail: 689190345@s89.tku.edu.tw

TEL: 886-2-26228936

Keywords:

Key agreement, Authentication.

Enhanced Authentication Key Agreement Protocol

Ren-Junn Hwang Sheng-Hua Shiau and Kai-Jun Lin

Abstract

Ku and Wang pointed out Tseng's protocol can't prevent two simple attacks. They also proposed a new protocol that can prevent those attacks. In this paper, the authors proposed an enhanced protocol that not only can prevent those attacks, but also has better efficiency in computation.

1. Introduction

In 1999, Seo and Sweeney [1] proposed a simple authenticated key agreement algorithm by using a pre-shared password, that is based on the Diffie-Hellman scheme [2] and provide authentication. In 2000, Tseng [3] pointed out a weakness in Seo-Sweeney protocol. In the validation phase, if an attacker replying the message sent by an honest party, the honest party will be fooled. Tseng then propose a new protocol that change the key validation phase. Later, Ku and Wang [4] indicated that Tseng's protocol still vulnerable to two simple attacks: backward replay without modification [5] and modification attack. They also proposed a protocol that can prevent those attacks. In this letter, we will propose an enhanced protocol by using bitwise Exclusive Or operations[6] that not only can prevent the attack present above, but also has better efficiency in computation.

2. Tseng's and Ku-Wang's protocols

Assume that Alice and Bob denote two parties, and have shared a common password S. The system has the same public values p and g as in the original Diffie-Hellman scheme

[2], where p is a large prime and g is a generator with order p-1 in $GF(p)$. The key establishment phase Ku-Wang's protocol likes Tseng's. We describe it as follows:

Step 1: Alice and Bob each compute two integers Q and Q^{-1} mod(p-1) from common password S, where Q is computed in a predetermined way and is relatively prime to p-1.

Step 2: Alice selects a random integer a and sends Bob

$$X_a = g^{aQ} \bmod p$$

Step 3: Bob also selects a random integer b and sends Alice

$$X_b = g^{bQ} \bmod p$$

Step 4: Alice computes the session key Key_a as follows:

$$Y_b = X_b^{Q^{-1}} \bmod p = g^{b} \bmod p$$

$$Key_a = Y_b^{a} \bmod p = g^{ab} \bmod p$$

Step 5: Bob computes the session key Key_b as follows:

$$Y_a = X_a^{Q^{-1}} \bmod p = g^{a} \bmod p$$

$$Key_b = Y_a^{b} \bmod p = g^{ab} \bmod p$$

The key validation phase of Tseng's protocol is

Step 1: Alice sends Y_b to Bob,

Step 2: Bob sends Y_a to Alice,

Step 3: Alice and Bob check whether $Y_a = g^a \bmod p$ and $Y_b = g^b \bmod p$ hold or not, respectively.

Ku and Wang pointed out some weakness of Tseng's protocol and altered the key validation phase as follows: [4]

Step 1: Alice computes

$$W = (Key_a)^{Q} \bmod p = g^{abQ} \bmod p$$

and then she sends W to Bob.

Step 2: Bob checks whether $W^{Q^{-1}} \bmod p = Key_b$ holds or not. If it holds, Bob sends Y_a to Alice.

Step 3: Alice checks whether $Y_a = g^a \bmod p$ holds or not.

3. Our enhanced protocol

Let Alice and Bob denote two parties, and have a common pre-shared password S. In our enhanced protocol, two parties has the same public values p and g as in the original Diffie-Hellman scheme [2], where p is a large prime and g is a generator with order p-1 in $GF(p)$. We describe our protocol in two phases as follows:

Key establishment phase:

Step 1: Alice and Bob each compute integer Q from pre-shared password S, where Q is computed in a predetermined way, and Q is unique and has the same bit form with p.

Step 2: Alice selects a random integer a, and sends X_a to Bob

$$X_a = (g^a \bmod p) \oplus Q,$$

where $\oplus$ denotes the bitwise Exclusive Or operation.

Step 3: Bob selects a random integer b, and sends X_b to Alice

$$X_b = (g^b \bmod p) \oplus Q$$

Step 4: Alice computes the session key Key_a as follows:

$$Y_b = X_b \oplus Q = g^b \bmod p$$

$$Key_a = Y_b^a \bmod p = g^{ab} \bmod p$$

Step 5: Bob computes the session key Key_b as follows:

$$Y_a = X_a \oplus Q = g^a \bmod p$$

$$Key_b = Y_a^b \bmod p = g^{ab} \bmod p$$

Key validation phase:

Step 1: Alice computes W and sends to Bob

$$W = Key_a \oplus Q = (g^{ab} \bmod p) \oplus Q$$

Step 2: Bob computes Z and sends to Alice

$$Z = Y_a \text{ ﹡ } (g^b \bmod p) = (g^a \bmod p)\text{﹡}(g^b \bmod p) = g^{a+b} \bmod p$$

Step 3: Alice checks whether $Z = Y_b$ ﹡ $(g^a \bmod p) = (g^b \bmod p)$﹡$(g^a \bmod p)$ holds or not. Bob checks whether $W \oplus Q = Key_b$ holds or not.

4. Discussions

This section we analysis the security of the proposed scheme in Subsection 4.1. Subsection 4.2 shows the complexity analysis of the proposed scheme.

4.1 Security Analysis

Ku and Wang pointed out that if the attacker re-sends X_a to Alice as Bob's X_b in Step3 of Tseng's key establishment phase and re-sends Y_a to Alice as Bob's Y_b in Step 2 of Tseng's validation phase, then Alice generates a wrong session key but she can not detect it is incorrect in Step 3 of Tseng's validation phase.[4] In our enhanced protocol, if the attacker masquerades as Bob to resend X_a back to Alice as Bob's X_b in Step 3 . Alice computes

$$Y_b = X_b \oplus Q = X_a \oplus Q = g^a \bmod p,$$

$$Key_a = Y_b^a \bmod p = g^{a^2} \bmod p.$$

Alice sends $W = Key_a \oplus Q = (g^{a^2} \bmod p) \oplus Q$ to Bob in Step 1 of our key validation phase. If the attacker masquerades as Bob to resend W back to Alice as Z in Step 2, then Alice check out that the value Z is not equal to X_a﹡$g^a \bmod p (= g^{a+a} \bmod p)$. Alice does not believe the wrong session key. Similarly, if the attacker masquerades as Alice, Bob will not believe the wrong session key, either. Our protocol withstands the backward reply without modification attack.[4,5]

The other weakness of Tseng's protocol [4] is that if the attacker replaces X_a with X_a', which Alice sent in Step 2 of Tseng's Key establishment phase. Bob believes the wrong

session key, although Alice does not believe the session key in Step 3 of Tseng's Key validation phase. In our enhanced protocol, if the attacker replaces X_a as X_a', Bob computes the session key $Key_b'=(X_a' \oplus Q)^b \bmod p$. Alice sends $W=g^{ab} \bmod p \oplus Q$ to Bob in Step 1 of our Key validation phase. Bob checks $W \oplus Q=g^{ab} \bmod p$ and it is not equal to Key_b', he does not believe the wrong session key in Step 3 of our Key validation phase. Bob sends $Z=(X_a' \oplus Q)\, g^b \bmod p$ to Alice in Step 2 of our Key validation phase. Alice checks Z is not equal to $Y_b \gtrless g^a \bmod p$, she does not believe the wrong session key in Step 3 of our Key validation phase, either. Similarly, if the attacker replaced the message send by Bob in our Key establishment phase, both Alice and Bob will not believe the wrong session key. Our enhanced protocol withstands Ku-Wang's modification attack. [4]

4.2 Complexity analysis

In Ku-Wang's protocol, Key establishment phase needs 2 modular inverse computations, 1 modular multiple computation and 7 modular exponential computations, Key validation phase needs 2 modular exponential computations. In our new protocol, Key establishment phase needs 4 modular exponential computations and 4 Exclusive Or operations, Key validation phase needs 2 modular multiple computations and 2 Exclusive Or operations. Ghanem and Wahab [6] propose that Exclusive Or operation is secure and very fast to compute. So, our new protocol is faster than Ku-Wang's protocol. We show the comparison in Table 1.

Table 1: Comparison between Ku-Wang's protocol and our enhanced protocol

		Ku-Wang's protocol	Our enhanced protocol
Key establishment phase	Alice	1 modular inverse 4 modular exponential	2 modular exponential 2 Exclusive Or operations
	Bob	1 modular inverse 1 modular multiple 3 modular exponential	2 modular exponential 2 Exclusive Or operations
	Total	2 modular inverse 1 modular multiple 7 modular exponential	4 modular exponential 4 Exclusive Or operations
Key validation phase	Alice	1 modular exponential	1 Exclusive Or operation 1 modular multiple
	Bob	1 modular exponential	1 Exclusive Or operation 1 modular multiple
	Total	2 modular exponential	2 Exclusive Or operations 2 modular multiple

* The computation complexity of the modular inverse is equal to the modular exponential.

5. Conclusions

Tseng present a weakness in Seo-Sweeney protocol, Ku-Wang present two simple attacks that Tseng's protocol can't prevent. Our enhanced protocol can prevent those attacks. In Key validation phase of our enhanced protocol, Step 1 and Step 2 can run in parallel, but Ku-Wang's protocol should run sequentially. By using Exclusive Or operation, our protocol needs lower computation loads, it can run faster than Ku-Wang's protocol.

Reference

1 SEO, D.H., and SWEENEY, P.: 'Simple authenticated key agreement algorithm', *Electronics Letters*, Vol. 35, No.13, 1999, pp.1073-1074

2 DIFFIE, W., and HELLMAN, M.E.: 'New directions in cryptography', *IEEE Transactions on Information Theory*, IT-22, (6), 1976, pp. 644-654

3 TSENG, Y.M.: 'Weakness in simple authenticated key agreement protocol',

Electronics Letters, Vol. 36, No. 1, 2000, pp. 48-49

4 KU, W.C., and WANG, S.D.: 'Cryptanalysis of modified authenticated key agreement protocol', *Electronics Letters*, Vol. 36, No. 21, 2000, pp. 1770-1771

5 GONG, L.: 'Variations on the themes of message freshness and replay', *Proceedings of IEEE Computer Security Foundations Workshop*, June 1993, pp. 131-136

6 GHANEM, S.M., and WAHAB, H.A.: 'A simple XOR-based technique for distributing group key in secure multicasting', *Proceedings of the Fifth IEEE Symposium on Computers and Communications*. ISCC 2000, 3-6 July, 2000, pp. 166-171