Cryptanalysis of Authenticated Key Agreement Protocols
(一些具身份認證之金鑰協議協定之安全性分析)

Her-Tyan Yeh(葉禾田)

Department of Computer Science and Information Engineering
National Cheng Kung University
Tainan, Taiwan 70101
htyeh@ismail.csie.ncku.edu.tw

Hung-Min Sun(孫宏民)

Department of Computer Science and Information Engineering
National Cheng Kung University
Tainan, Taiwan 70101
hmsun@mail.ncku.edu.tw

Tzonelih Hwang(黃宗立)

Department of Computer Science and Information Engineering
National Cheng Kung University
Tainan, Taiwan 70101
hwangtl@server2.iie.ncku.edu.tw

ABSTRACT

In 1999, Seo and Sweeney proposed a simple authenticated key agreement protocol that enables two parties, who share a password in advance, to authenticate each other and to share a common session key vie the Diffie-Hellman problem. Recently, Jseng showed that the Seo-Sweeney protocol is insecure against forgery and consequently proposed a modified protocol to repair it. Later, Ku and Wang addressed that Jseng's protocol is also insecure against forgery and therefore an improved version was proposed. In this paper, we show that the three authenticated key agreement protocols, proposed by Seo et al., Tseng, and Ku et al. respectively, are insecure against off-line password guessing attacks if weak passwords are applied.

***Keywords*:** Authentication, Key Agreement, Password, Guessing Attacks

中文摘要

1999 年，Seo 和 Sweeney 提出一個簡單的身份認證之金鑰協議之協定。此協定可以讓事先分享密碼之兩方互相認證身份而分享協議之金鑰。最近，Jseng 指出 Seo 和 Sweeney 之方法有偽造身份之安全問題而提出一修正版。後來，Ku 和 Wang 再指出 Jseng 之修正版也有偽造身份之安全問題而再提出一改進版本。在本論文中，我們證明了假如使用人們容易記憶之密碼，則 Seo 和 Sweeney、Jseng、Ku 和 Wang 所提出之方法都會遭受到字典攻擊法攻擊而是不安全的。

關鍵字: 身份認證、金鑰協議、密碼、字典攻擊

1. Introduction

In 1976, Diffie and Hellman [5] introduced a key agreement protocol in which two parties can establish a secret session key over an insecure channel. However, the Diffie-Hellman key exchange scheme does not authenticate the participants and is vulnerable to man-in-the-middle attacks. Several methods for user authentication have been proposed. Password-based mechanism is the most widely used method for user authentication since it allows people to choose and remember their own passwords without any assistant device.

In 1999, Seo and Sweeney [11] proposed a simple authenticated key agreement protocol (the Seo-Sweeney protocol in short) that enables two parties, who share a password in advance, to authenticate each other and to share a common session key vie the Diffie-Hellman problem [5]. In the Seo-Sweeney protocol, two parties exchange two messages to establish the session key. Besides, the exchange of another two messages makes the two parties to verify the validity of the session key. Recently, Jseng [9] addressed a weakness in the key validation steps and showed that the Seo-Sweeney protocol is insecure against forgery. By replying to the

message sent from the honest party, the adversary can fool the honest party into believing a wrong session key. He then consequently proposed a modified protocol to repair it. Later, Ku and Wang [10] addressed that Jseng's protocol is also insecure against forgery. Additionally, an enhanced version (the Ku-Wang protocol in short) to the Seo-Sweeney protocol was proposed. All these three protocols are suitable for the case when strong passwords are applied. Therefore, they didn't address on password guessing attacks. However, people often tend to choose easy-to-remember passwords (or refereed to as "weak passwords"), which are vulnerable to password guessing attacks. In the past, a variety of authenticated key agreement protocols [1-4,7-8,12] have been proposed to defeat off-line password guessing attacks (it is natural that on-line password guessing attacks can not be defeated by means of protocols). In this paper, we show that the three authenticated key agreement protocols, proposed by Seo *et al.*, Tseng, and Ku *et al.* respectively, are insecure against off-line password guessing attacks if they use weak passwords.

The rest of this paper is organized as follows. In section 2, we briefly review Seo-Sweeney's, Jseng's and Wu's schemes. In section 3, we examine the security of the above three schemes. Finally, we conclude this paper in section 4.

2. Related Works

2.1 The Seo-Sweeney Protocol

Assume that Alice and Bob share a secret password P before the protocol begins, and the system has the same public values n and g as the original Diffie-Hellman scheme [5], where n is a large prime and g is a generator with order n-1 in $GF(n)$. We describe the protocol as follows:

Key establishment phase

e.1. Alice and Bob each obtain two integers Q and Q^{-1} mod (n-1) from the common password P, where Q could be computed in predetermined way and is prime to n-1.

e.2. Alice selects a random integer a and sends Bob

$$X_1=g^{aQ} \bmod n$$

e.3. Bob also selects a random integer b and sends Alice

$$Y_1=g^{bQ} \bmod n$$

e.4. Alice computes the session key Key_1 as follows:

$$Y=Y_1^{Q^{-1}} \bmod n \ (= g^b \bmod n),$$

$$Key_1 = Y^a \bmod n.$$

e.5. Bob computes the session key Key_2 as follows:

$$X=X_1^{Q^{-1}} \bmod n \ (= g^a \bmod n),$$

$$Key_2 = X^b \bmod n$$

It is clear that $Key_1 = g^{ab} \bmod n = Key_2$. The common session key is thus established.

Key validation phase

v.1. Alice computes $Key_1^Q \bmod n$ and sends it to Bob.

v.2. Bob also computes $Key_2^Q \bmod n$ and sends it to Alice.

v.3. Each of Alice and Bob computes the other's key by applying Q^{-1} and compares it with his/her own session key.

2.2 The Jseng's Protocol

Jseng pointed out that the Seo-Sweeney protocol suffers from a weakness in the validation phase. Assume that an attacker (Eve) impersonate Bob to run the protocol. After receiving the message $Key_1^Q \bmod n$ sent by Alice (Step v.1), Eve may resend it to Alice in Step v.2. Although Eve cannot obtain a shared session key with Alice, Alice obtains a wrong session key and believes that it is shared with Bob. That is, verification of the session key cannot be achieved using the protocol. To overcome the above weakness, the verification steps of the session key are modified as follows:

v.1. Alice sends Y to Bob.

v.2. Bob sends X to Alice.

v.3. Alice and Bob check whether

$$X= g^a \bmod n \text{ and } Y= g^b \bmod n$$

hold or not, respectively.

2.3 The Ku-Wang Protocol

In [10], Ku-Wang pointed out that Jseng's protocol suffers from two weaknesses in the following.

1. *Backward replay without modification* [6]: Upon seeing X_1 sent by Alice in step (e.2), the adversary (Eve) can masquerade as Bob to re-send it back to Alice in step (e.3) as Y_1. Consequently, Alice will compute

   $Y = Y_1^{Q^{-1}} \bmod n$
   $(= X_1^{Q^{-1}} \bmod n = g^a \bmod n)$,

   $Key_1 = Y^a \bmod n \ (= g^{a^2} \bmod n)$,

   and send Y to Bob in step (v.1) . Then, Eve can masquerade as Bob to re-send Y back to Alice in step (v.2) as X. Since $Y = g^a \bmod n$ holds, Alice will be fooled into believing the wrong session key Key_1.

2. *Modification attack*:
   Upon seeing X_1 sent by Alice in step (e.2), Eve can replace it with any number $\in$ [1, n-1], say X_1'. In step (e.3), Bob sends Y_1 to Alice, and then Alice sends the corresponding response Y to Bob in step (v.1). In step (v.2), Bob will send X $(= (X_1')^{Q^{-1}} \bmod n)$ to Alice. Because $X \neq g^a \bmod n$, Alice will not believe Key_1. However, since $Y = g^b \bmod n$ holds, Bob will believe the wrong session key Key_2' $(= ((X_1')^{Q^{-1}})^b \bmod n)$. Although Eve cannot compute Key_2', she can still fool Bob into believing the wrong session key.

The following verification steps for the session key were proposed by Ku and Wang to overcome the above two weaknesses.
Enhanced key validation steps:

v.1. Alice computes

$Y_2 = Key_1^Q \bmod n \ (= g^{abQ} \bmod n)$

and then sends it to Bob.

v.2. Bob check whether $(Y_2)^{Q^{-1}} \bmod n = Key_2$ holds or not. If it holds, Bob believes that he has obtained the correct X_1 and Alice has obtained the correct Y_1, i.e. Bob is convinced that Key_2 is valid, and then sends X to Alice.

v.3. Alice checks whether $X = g^a \bmod n$ holds or not. If it holds, Alice believes that he has obtained the correct Y_1 and Bob has obtained the correct X_1, i.e. Alice is convinced that Key_1 is valid.

3. Cryptanalysis of the above three protocols

Password-based mechanism is the most widely used method for user authentication since it allows people to choose and remember their own passwords without any assistant device. However, people usually choose easy-to-remember passwords such that they are vulnerable to password guessing attacks. In the following, we will point out that all the above three protocols suffer from off-line password guessing attacks if weak passwords are applied. Note that the above three protocols have the same key establishment phase. Now, we describe our attacks as follows:

1. *The Seo-Sweeney protocol*:

   In the Seo-Sweeney protocol, upon seeing X_1 sent by Alice, Eve computes $Y_1 = g^b \bmod n$ and sends it to Alice in step e.3. After receiving Y_1, Alice computes the session key $Key_1 = g^{abQ^{-1}} \bmod n$ and sends the corresponding response $Key_1^Q \bmod n = g^{ab} \bmod n$ to Eve in step (v.1). Now, Eve can guess a password P off-line, obtain two integers Q and $Q^{-1} \bmod (n\text{-}1)$ and compute $((X_1)^{Q^{-1}})^b \bmod n$. If it is equal to $g^{ab} \bmod n$, then he gets the password right. Otherwise, he guesses another password again until he hits it.

2. *The Jseng's modified protocol*:

   In Jseng's modified protocol, upon seeing X_1 sent by Alice, Eve computes $Y_1 = g^b \bmod n$ and sends it to Alice in step e.2. After receiving Y_1, Alice computes
   $Y = (Y_1)^{Q^{-1}} \bmod n = g^{bQ^{-1}} \bmod n$
   and sends the corresponding response Y to Eve in step (v.1). Now, Eve can guess a password P off-line, obtain two integers Q and $Q^{-1} \bmod (n\text{-}1)$ and compute $(Y)^Q \bmod n$. If it is equal to Y_1, he gets the password right. Otherwise, he guesses

another password again until he hit it.

3. *The Ku-Wang protocol*:

In the Ku-Wang protocol, in addition to the key establishment phase, the first step (v.1) in key validation phase is the same as that of the Seo-Sweeney protocol. So, the password guessing attack is the same as that on the Seo-Sweeney protocol.

4. Conclusions

In this paper, we show that the previous three authenticated key agreement protocols, proposed by Seo et al., Tseng, and Ku et al. respectively, are insecure against off-line password guessing attacks if weak passwords are applied.

Acknowledgments

This work was supported in part by the National Science Council, Taiwan, under contract NSC-90-2213-E-006-111.

References

[1]. M. BELLARE, D. POINTCHEVAL, and P. ROGAWAY, “Authenticated Key Exchange Secure against Dictionary Attacks”, Advances in Cryptology-EUROCRYPT, pp. 139-155, 2000

[2]. S. BELLOVIN, and M. MERRITT, “Encrypted key Exchange: Password-based Protocols Secure against Dictionary Attacks”, Proceedings of IEEE Symposium on Research in Security and privacy, Oakland, 1992

[3]. S. BELLOVIN, and M. MERRITT, “Augmented Encrypted key Exchange: a Password-based Protocol Secure against Dictionary Attacks and Password File Compromise”, AT&T Bell Laboratories, 1993

[4]. V. BOYKO, P. MACKENZIE, and S. PATEL, “Provably Secure Password-Authenticated Key Exchange using Diffie-Hellman”, Advances in Cryptology-EUROCRYPT, pp. 156-171, 2000

[5]. W. DIFFIE, and M. E. HELLMAN, “New directions in cryptography”, IEEE Trans., IT-22, (6), pp. 644-654, 1976

[6]. L. GONG, “Variations on the themes of message freshness and replay”, Proc. IEEE Computer Security Foundations Workshop VI, pp. 131-136, June 1993

[7]. D. JABLON, “Strong Password-Only Authentication key Exchange”, ACM Computer Communication Review, 26, (5), pp. 5-26, 1996

[8]. D. JABLON, “Extended Password key Exchange Protocols Immune to Dictionary Attack”, Proceedings of the WETICE Workshop on Enterprise Security, Cambridge, MA, 1997

[9]. Y. M. JSENG, “Weakness in simple authenticated key agreement protocol”, Electron. Lett., 36, (1), pp. 48-49, 2000

[10]. W. C. KU, S. D. WANG, “Cryptanalysis of modified authenticated key agreement protocol”, Electron. Lett., 36, (21), pp. 1770-1771, 2000

[11]. D. H. SEO, P. SEWEENEY, “Simple authenticated key agreement algorithm”. Electronic Lett., 35, (13)., pp. 1073-1074, 1999

[12]. T. WU, “The secure remote password protocol”, Internet Society Symposium on Network and Distributed System Security, 1998