Off-line Password Guessing Attack on An Efficient Key Agreement Protocol for Secure Authentication

Rongxing Lu and Zhenfu Cao
(Corresponding author: Rongxing Lu)

Department of Computer Science and Engineering, Shanghai Jiao Tong University
No. 1954, Huashan Road, Shanghai 200030, P.R. China, (Email: {rxlu, cao-zf}@cs.sjtu.edu.cn)

(Received Aug. 11, 2005; revised and accepted Sept. 14 and Oct. 25, 2005)

Abstract

In 2004, Kim, Huh, Hwang and Lee proposed an efficient key agreement protocol for secure authentication. In this paper, we shall show that their proposed protocol cannot resist the off-line password guessing attack and therefore present a modified protocol to avoid this attack.
Keywords: Authenticated key agreement, cryptanalysis, off-line password guessing attack

1 Introduction

Key agreement is one of the fundamental problems considered in cryptography. The well best-known protocol for key agreement is the Diffie-Hellman protocol, which allows two parties to establish a shared secret by exchanging messages over an insecure channel without the need for any prior communication. However, the basic Diffie-Hellman protocol has a weakness of possible man-in-the middle attack. To solve this problem, many authenticated key agreement protocols using certificates [1] or pre-shared secret passwords between two parties [2, 3, 4] have been put forward over the past years.

Recently, Kim, Huh, Hwang and Lee [5] have proposed an efficient password-based key agreement protocol for secure authentication. Although Kim *et al.*'s protocol has the same stability as the existing methods [3, 4] and with much efficient processing performance, yet it is still an insecure protocol. In this paper, we shall point out that Kim *et al.*'s protocol cannot resist the off-line password guessing attack.

The rest of the paper is organized as follows. In Section 2, we first briefly review Kim *et al.*'s protocol. Then, we shall show that their scheme is vulnerable to the off-line password guessing attack and present a modified protocol in Section 3. Finally, we shall draw our conclusions in Section 4.

2 Brief Review of Kim et al.'s Protocol

In this section, we shall briefly review Kim *et al.*'s efficient key agreement protocol for secure authentication [5]. At the beginning, we first introduce some used notations.

2.1 Notations

- *Alice*(A), *Bob*(B): two communication parties.
- n : a secure large prime number.
- g, g_1 : two generators in $\mathbb{Z}_n^*$ of order $n-1$.
- $\mathcal{D}$: a uniformly distributed dictionary of size $|\mathcal{D}|$.
- P : a low-entropy password shared between *Alice* and *Bob*, which is randomly chosen from $\mathcal{D}$.
- Q, Q^{-1} : two integers computed from P by a pubic predesignated method such that $Q \cdot Q^{-1} \equiv 1 \bmod n-1$.
- H : a secure one-way hash function.

2.2 Kim *et al.*'s Protocol

Kim *et al.*'s protocol is shown in Fig. 1, which consists of four steps as follows:

Step 1: *Alice* first chooses a random number $a \in \mathbb{Z}_n^*$, computes $X_1 = g^{aQ} \bmod n$ and sends it to *Bob*.

Step 2: On receiving X_1, *Bob* also chooses a random number $b \in \mathbb{Z}_n^*$, computes $Y_1 = g^{bQ} \bmod n$ and $X = X_1^{Q^{-1}} = g^{aQQ^{-1}} = g^a \bmod n$. Then, *Bob* sends (X, Y_1) back to *Alice*.

Alice		*Bob*
$X_1 = g^{aQ} \bmod n$	$\xrightarrow{X_1}$	
		$Y_1 = g^{bQ} \bmod n$
	$\xleftarrow{X,Y_1}$	$X = X_1^{Q^{-1}} \bmod n$
$X \stackrel{?}{=} g^a \bmod n$		
$Y = Y_1^{Q^{-1}} \bmod n$	$\xrightarrow{Y}$	
$Key_1 = Y^a = g^{ab} \bmod n$		$Y \stackrel{?}{=} g^b \bmod n$
		$Key_2 = X^b = g^{ab} \bmod n$

Figure 1: Kim *et al.*'s protocol [5]

Step 3: When *Alice* receives (X, Y_1), she first checks $X \stackrel{?}{=} g^a \bmod n$. If it does hold, *Alice* authenticates *Bob*. Then, *Alice* computes $Y = Y_1^{Q^{-1}} \bmod n$ and sends it to *Bob*. At the same time, *Alice* also computes the session key $Key_1 = Y^a = g^{ab} \bmod n$.

Step 4: If *Bob* receives Y from *Alice*, he checks the equality $Y \stackrel{?}{=} g^b \bmod n$. If it holds, *Bob* authenticates *Alice*. Then, *Bob* can compute the session key $Key_2 = X^b = g^{ab} \bmod n$.

3 Attack on Kim *et al.*'s Protocol

In this section, we shall show that Kim *et al.*'s protocol is vulnerable to the off-line password guessing attack and therefore present a modified protocol to resist this attack.

3.1 Off-line Password Guessing Attack

In Kim *et al.*'s protocol, since all exchanged messages are transmitted over an open network, an adversary can easily obtain a valid information pair $\{X_1, X\}$ such that $X_1 = g^{aQ} \bmod n$ and $X = g^a \bmod n$ for some Q. On the other hand, since Q is computed by a low-entropy secret password $P \in \mathcal{D}$ with a public predesignated method, the adversary can guess a password $P^\star$ from $\mathcal{D}$, and derive the corresponding $Q^\star$, then verify it by checking $X_1 = X^{Q^*} \bmod n$. If it holds, the adversary has guessed the correct secret password $P^\star = P$. Otherwise, the adversary repeatedly guesses a new password $P^\star$ from $\mathcal{D}$ until $X_1 = X^{Q^*} \bmod n$ holds.

Off-line Password Guessing Attack$(X_1, X, \mathcal{D})$
for $i := 0$ **to** $|\mathcal{D}|$
$P^\star \leftarrow \mathcal{D}$; $Q^\star \leftarrow P^\star$
if $X_1 = X^{Q^\star} \bmod n$ **then return** $P^\star$

Therefore, the off-line password guessing attack is effective to Kim *et al.*'s protocol.

3.2 Our Modified Protocol

To avoid the off-line password guessing attack, in this subsection, we present a modified protocol by introducing a hash function H and another generator g_1 in $\mathbb{Z}_n^*$. The modified protocol is shown in Fig. 2, and the detailed steps are described as follows:

Step 1: *Alice* first chooses a random number $a \in \mathbb{Z}_n^*$, computes $X_1 = g^{aQ} \bmod n$, $X_2 = {g_1}^a \bmod n$ and sends them to *Bob*.

Step 2: On receiving (X_1, X_2), *Bob* computes $X_1' = {X_1}^{Q^{-1}} = g^a \bmod n$, also chooses two random numbers $b_1, b_2 \in \mathbb{Z}_n^*$, computes $Y_1 = g^{b_1} {g_1}^{b_2} \bmod n$ and $Y_2 = {X_1'}^{b_1} {X_2}^{b_2} = g^{ab_1} {g_1}^{ab_2} \bmod n$. Then, *Bob* sends $(H(A\|B\|X_1\|X_2\|Y_1\|Y_2\|0), Y_1)$ back to *Alice*.

Step 3: When *Alice* receives $(H(A\|B\|X_1\|X_2\|Y_1\|Y_2\|0), Y_1)$, she first computes $Y_2' = {Y_1}^a = g^{ab_1} {g_1}^{ab_2} \bmod n$ and checks $H(A\|B\|X_1\|X_2\|Y_1\|Y_2\|0) = H(A\|B\|X_1\|X_2\|Y_1\|Y_2'\|0)$. If it does hold, *Alice* authenticates *Bob*. Then, *Alice* sends $H(A\|B\|X_1\|X_2\|Y_1\|Y_2'\|1)$ to *Bob*. At the same time, *Alice* also computes the session key $Key_1 = H(A\|B\|X_1\|X_2\|Y_1\|Y_2')$.

Step 4: If *Bob* receives $H(A\|B\|X_1\|X_2\|Y_1\|Y_2'\|1)$ from *Alice*, he checks the equality $H(A\|B\|X_1\|X_2\|Y_1\|Y_2'\|1) = H(A\|B\|X_1\|X_2\|Y_1\|Y_2\|1)$. If it holds, *Bob* authenticates *Alice*. Then, *Bob* can compute the session key $Key_2 = H(A\|B\|X_1\|X_2\|Y_1\|Y_2)$. Since $Y_2 = Y_2' = g^{ab_1} {g_1}^{ab_2} \bmod n$, the correctness follows.

3.3 Security Analysis

The modified protocol can not only resist the Off-line password guessing attack but also enjoy the merits of Kim *et al.*'s protocol [5]. Here based upon the one-wayness of the hash function H and the hardness of the discrete logarithm (DL) problem and the computational Diffie-Hellman (CDH) problem in $\mathbb{Z}_n^*$, we shall formally analyze the security of our modified protocol in terms of the following security properties: Perfect forward secrecy, Replay attacks, On-line password guessing attacks, Off-line password guessing attacks, Denning-Sacco attacks [6] and other attacks [7, 8].

- *Perfect forward secrecy*: Perfect forward secrecy is provided in the situation that even though a pass-

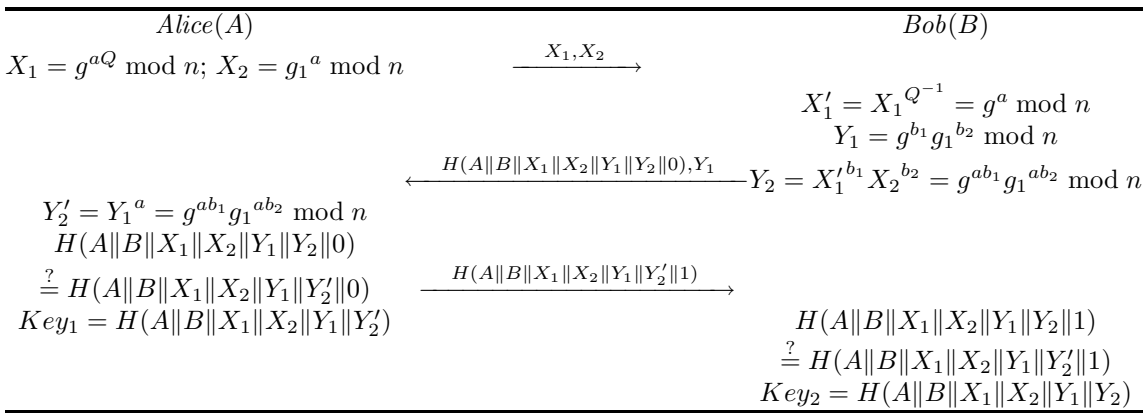

Figure 2: Our modified protocol

word is compromised, an adversary still cannot derive any previous session keys. In our modified protocol, suppose that an adversary knows a password, he tries to find previous session keys from the information collected by passive attack in past communication sessions. However, due to the hardness of DL and CDH problems, he cannot do these. Therefore, similarly as Kim *et al.*'s original protocol, our modified protocol also provides the property of perfect forward secrecy.

- *Replay attacks*: Replay attacks fail since the freshness of the ephemeral parameters a, b_1 and b_2 of both parties are preserved in g^{aQ}, ${g_1}^a$ and $g^{b_1}{g_1}^{b_2}$. Here, without loss of generality, we assume that an adversary intercepts $X_1 = g^{aQ} \bmod n$, $X_2 = {g_1}^a \bmod n$ in Step 1 and uses it to impersonate *Alice*. Since the adversary has no knowledge of the password, he cannot compute a right $H(A\|B\|X_1\|X_2\|Y_1\|Y_2'\|1)$ from Y_1 in Step 3 for *Bob*'s verification. Hence our modified protocol can resist the replay attack.

- *On-line password guessing attacks*: On-line password guessing attacks are detectable in the modified protocol. If an adversary tries to guess and obtain the password shared between *Alice* and *Bob*, he shall use the guessed password to compute $H(A\|B\|X_1\|X_2\|Y_1\|Y_2\|0)$ to *Alice* or $H(A\|B\|X_1\|X_2\|Y_1\|Y_2'\|1)$ to *Bob* for verification. However, the probability of guessing the correct password is only $\frac{1}{|\mathcal{D}|}$, if the guessing is wrong, *Alice* or *Bob* can easily detect that there is an adversary trying to guess the password. Therefore, On-line password guessing attacks cannot succeed.

- *Off-line password guessing attacks*: Off-line password guessing attacks can be avoided in our modified protocol. Observe the protocol, it is hard to derive g^{b_1}, ${g_1}^{b_2}$ from $Y_1 = g^{b_1}{g_1}^{b_2} \bmod n$, then the relation for helping guess the password is not available to an adversary. Therefore, it is impossible for an adversary to get the right password because of the uncertainty of b_1, b_2 and the difficulty of solving the DL problem. As a result, our modified protocol can resist the off-line password guessing attack encountered in Kim *et al.*'s protocol.

- *Denning-Sacco attacks*: Denning-Sacco attacks [6] are the case that an adversary, who compromised an old session key, attempts to compute the password and confirm the correctness of the guessed password. To analyze this, suppose that an adversary knows a session key $H(A\|B\|X_1\|X_2\|Y_1\|g^{ab_1}{g_1}^{ab_2} \bmod n)$ and information collected by passive attack in past communication sessions, i.e., $g^{aQ}, {g_1}^a$, $g^{b_1}{g_1}^{b_2}$, $H(A\|B\|X_1\|X_2\|Y_1\|Y_2\|0), H(A\|B\|X_1\|X_2\|Y_1\|Y_2'\|1)$. However, with them, he still cannot attack due to the one-wayness of H and the hardness of DL and CDH problems in $\mathbb{Z}_n^*$. Therefore, our modified protocol is secure against this attack.

- *Other attacks*: In our modified protocol, we have adopted the approach in [9, 10, 11] to resist other attacks [7, 8]. We include the identities $A\|B$ of *Alice* and *Bob* in the hash function H to resist unknown key share attacks [7] and reflection attacks [8]. We also include the transcripts $X_1\|X_2\|Y_1$ in the hash function H to provide freshness and data origin authentication.

4 Conclusions

In this paper, we have shown that Kim *et al.*'s password-based key agreement protocol [5] is vulnerable to the off-line password guessing attack. To avoid such an attack, we also presented a modified protocol. According to the security analysis, it is obvious that our modified protocol is secure enough to withstand all possible attacks.

Acknowledgment

We thank Jolyon Clulow for pointing out the error in the original version of the paper and helpful advice on

this version, and Raymond Choo for his kindly comments on our modified protocol. We also thank anonymous reviewers for their valuable comments and suggestions that improve the presentation of this paper. This work is also supported in part by the National Natural Science Foundation of China for Distinguished Young Scholars under Grant No. 60225007, the National Research Fund for the Doctoral Program of Higher Education of China under Grant No. 20020248024, and the Science and Technology Research Project of Shanghai under Grant Nos. 04JC14055 and 04DZ07067.

References

[1] W. Diffie, P. C. Van Oorschot, and M. J. Wiener, "Authentication and authenticated key exchanges", *Design, Codes and Cryptography*, vol. 2, pp. 107–125, 1992.

[2] S. Bellovin and M. Merritt, "Encrypted key exchange: password-based protocols secure against dictionary attacks", in *Proc. of IEEE Conf. on Research in Security and Privacy*, pp. 72–84, 1992.

[3] D. H. Seo, and P. Sweeney, "Simple authenticated key agreement algorithm", *Electronics Letters*, vol. 35, no. 13, pp. 1073–1074, 1999.

[4] I. C. Lin, C. C. Chang, and M. S. Hwang, "Security enhancement for the simple authentication key agreement algorithm", in *Proc. of the 24th Annual International Computer Software and Application confernece*, pp. 113–115, 2000.

[5] Y. S. Kim, E. N. Huh, J. H. Hwang, and B. W. Lee, "An efficient key agreement protocol for secure authetnication", in *ICCAS 2004*, LNCS 3043, pp. 746–754, Springer-Verlag, 2004.

[6] D. Denning and G. Sacco, "Timestamps in key distribution protocols", *Communications of the ACM*, vol.24, no.8, 533–536, 1981.

[7] C. Boyd and A. Mathuria, *Protocols for authentcation and key establishment*, Springer-Verlag, June 2003.

[8] H. Krawczyk, "Sigma: The 'sign-and-mac' approach to authenticated Diffie-Hellman and its use in the ike-protocols", in *Crypto 2003*, LNCS 2729, pp. 400–425, Springer-Verlag, 2003.

[9] K.-K. R. Choo, C. Boyd, and Y. Hitchcock, "On session key contruction in provably secure protocols", in *1st International Conference on Cryptology in Malaysia - Mycrypt 2005*, LNCS 3715, pp. 116–131, Springer-Verlag, 2005.

[10] K.-K. R. Choo, "Revist of McCullagh-Barreto two-party ID-based authenticated key agreement protocols",*International Journal of Network Security*, vol.1, no.3, 154–160, Nov. 2005.

[11] K.-K. R. Choo, "Revisting Lee, Kim, & Yoo authenticated key agreement protocol", *International Journal of Network Security*, vol.2, no.1, 64–68, Jan. 2006.

Rongxing Lu received his B.S. and M.S. degrees in computer science from Tongji University in 2000 and 2003 respectively. Currently, he is a doctoral candidate in the Department of Computer and Engineering, Shanghai Jiao Tong University. His research interests lie in cryptography and network security.

Zhenfu Cao is the professor and the doctoral supervisor of Computer Software and Theory at Department of Computer Science of Shanghai Jiao Tong University. His main research areas are number theory and modern cryptography, theory and technology of information security etc. He is the gainer of Ying-Tung Fok Young Teacher Award (1989), the First Ten Outstanding Youth in Harbin (1996), Best Ph.D thesis award in Harbin Institute of Technology (2001) and the National Outstanding Youth Fund in 2002.