Cryptanalysis of a Three-party Password-based Authenticated Key Exchange Protocol

Debiao He[1,2], Yuanyuan Zhang[1], and Jianhua Chen[1]
(Corresponding author: Debiao He)

School of Mathematics and Statistics, *Wuhan University, Wuhan, China*[1]
State Key Laboratory of Information Security, Institute of Information Engineering[2]
Chinese Academy of Sciences, Beijing, China
(Email: hedebiao@163.com)
(Received May 25, 2012; revised and accepted Fereteary 19, 2013)

Abstract

Key exchange protocols allow two or more parties communicating over a public network to establish a common secret key called a session key. Due to their significance in building a secure communication channel, a number of key exchange protocols have been suggested over the years for a variety of settings. Recently, Lo et al. proposed a three-party password-based authenticated key exchange (3PAKE) protocol, where two users, each shares a human-memorable password with a server, can generate a session key for future communication with the help of the server. They claimed that their scheme could resist various attacks. However, this work shows that Lo et al.'s protocol is vulnerable to an off-line password guessing attack. The analysis show Lo et al.'s protocols is not suitable for practical applications.

Keywords: Cryptanalysis, guessing attack, off-line password, password

1 Introduction

Password-based authenticated key exchange (PAKE) protocol allows two or more parties authenticate each other and generate a strong session key through a shared human-memorable password in an insecure channel. It has been widely used in people's life since passwords are able to be freely chosen and can be fairly easily memorized without any assistant storage device.

In 1992, Bellovin et al. [2] proposed the first two-party password-based authenticated key exchange (2PAKE) protocol. Since then, many 2PAKE protocols [1,3,8-10,19] have been proposed. However, 2PAKE protocols are inconvenient and costly for use in large scale peer to peer systems. Since 2PAKE protocols require each pair of potential communicating parties to share a password, a large number of parties result in an even larger number of passwords to be shared. To solve the problem, Steiner et al. [17] proposed a three-party password-based authenticated key exchange (3PAKE) protocol. However, Ding et al. [6] pointed out that Steiner et al.'s protocol cannot resist the undetectable on-line password guessing attacks. Later, Lin et al. [11] also demonstrated that Steiner et al.'s protocol is vulnerable to t the off-line password guessing attacks. To improve security, Lin et al. also proposed an improved 3PAKE protocol using public key cryptosystem. However, Lin et al. protocol is inefficient owing to the heavy computation cost of public key cryptosystem. To improve performance, Lee et al. [14] presented two enhanced 3PAKE protocols without public key cryptosystem. Later, Wen et al. [18] proposed a 3PAKE protocol using Weil pairing. Unfortunately, Nam et al. [15] pointed out that Wen et al.'s protocol cannot resist the man-in-the-middle attack. To balance the tradeoff between security robustness and system efficiency, Lu et al. [13] proposed a simple 3PAKE protocol. There is no public key cryptosystem and symmetric cryptosystem are required. Lu et al. claimed that their protocol could resist various attacks. However, many researchers have shown that Lu et al.'s protocol suffers from man-in-the-middle attack and undetectable on-line password guessing attacks [4,7,16]. To improve security and performance efficiency on data computation and transmission round, Chang [5] proposed an improved 3PAKE protocol based on Lu et al.'s protocol. Recently, Lo et al. [12] demonstrated that Chang's protocol suffers from man-in-the-middle attack, undetectable on-line password guessing attacks, and off-line password guessing attacks. To improve security, Lo et al. also proposed an improved protocol. 3PAKE Lo et al. claimed that their protocol could overcome the weaknesses in Chang's protocol. However, in this paper, we will show Lo et al.'s protocol is still vulnerable to the off-line password guessing attack.

The organization of the paper is sketched as follows. The Section 2 gives a brief review of Lo et al.'s protocol. An off-line password guessing attack on Lo et al.'s protocol is shown in Section 3. Finally, we give some conclusions in Section 4.

2 Review of Lo et al.'s protocol

In this section, we will briefly review Lo et al.'s protocol. In order to facilitate future references, frequently used notations are listed below with their descriptions.

- A, B : two communication parties;
- S : the trusted server;
- ID_A, ID_B, ID_S : the identities of A, B and S, respectively;
- P_A, P_{A1} : two passwords securely shared by A and S;
- P_B, P_{B1} : the passwords securely shared by B and S;
- $E_P(\cdot)$: a symmetric encryption scheme with a password P;
- p : a large prime;
- q : a prime, where $q \mid p-1$;
- g : an element of order q with modulus p.
- G : a finite cyclic group generated by g in Z_p;
- $f_K(\cdot)$: a pseudo-random function (PRF) with three parameters indexed by secret key K;
- $H(\cdot)$: a one-way hash function;

As shown in Figure 1, the following steps will be executed if A and B want to authenticate each other and generate a session key.

1) A generates a random number $R_A \in Z_q$, computes $N_A = g^{R_A} \bmod p$, and sends the message $\{ID_A, ID_B, E_{P_A}(N_A)\}$ to S. At the same time, B generates a random number $R_B \in Z_q$, computes $N_B = g^{R_B} \bmod p$, and sends the message $\{ID_A, ID_B, E_{P_B}(N_B)\}$ to S.

2) Upon receiving $\{ID_A, ID_B, E_{P_A}(N_A)\}$ and $\{ID_A, ID_B, E_{P_B}(N_B)\}$, S uses the corresponding passwords P_A and P_B to retrieve N_A and N_B from $E_{P_A}(N_A)$ and $E_{P_B}(N_B)$, respectively. S generates a random number $R_S \in Z_q$ and computes $N_A^{R_S} = g^{R_A R_S} \bmod p$, $N_B^{R_S} = g^{R_B R_S} \bmod p$, $K_{AS} = N_A^{P_{A1}} = g^{R_A P_{A1}} \bmod p$ and $K_{BS} = N_B^{P_{B1}} = g^{R_B P_{B1}} \bmod p$. At last, S sends $X = g^{R_B R_S} \cdot f_{K_{AS}}(ID_A, ID_B, N_A)$ and $Y = g^{R_A R_S} \cdot f_{K_{BS}}(ID_A, ID_B, N_B)$ to A and B individually.

3) Upon receiving S's message, A and B first utilizes the shared password P_{A1} and P_{B1} to compute $K_{AS} = N_A^{P_{A1}} = g^{R_A P_{A1}} \bmod p$ and $K_{BS} = N_B^{P_{B1}} = g^{R_B P_{B1}} \bmod p$. Then, A computes $g^{R_B R_S} = X / f_{K_{AS}}(ID_A, ID_B, N_A)$. Similarly, B calculates $g^{R_A R_S} = Y / f_{K_{BS}}(ID_A, ID_B, N_B)$. After that, A computes current session key $K = (g^{R_B R_S})^{R_A} = g^{R_A R_B R_S} \bmod p$ and a verification message $\alpha = H(ID_A, ID_B, K)$, and sends α to B. At the same time, B computes current session key $K = (g^{R_A R_S})^{R_B} = g^{R_A R_B R_S} \bmod p$ and a verification message $\beta = H(ID_A, ID_B, H(K))$, and sends β to A. Depend on α and β, both of A and B can guarantee entity authentication and session key validation. If the verification processes of α and β are successfully examined, A and B believe that they actually share a secret session key $K = g^{R_A R_B R_S} \bmod p$.

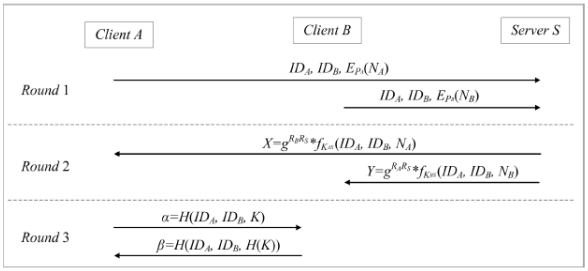

Figure 1: Lo et al.'s protocol

3 Cryptanalysis of Lo et al.'s Protocol

In Lo et al.'s protocol, the user could choose his password freely. For convenience, he would like to choose a password can be remembered easily. However, the easy-to-remember password is vulnerable to password guessing attacks. There are two types of the password guessing attack, i.e. the on-line password guessing attack and the off-line password guessing attack. In the first one, the adversary tries to use guessed passwords iteratively to pass the verification in an on-line manner. Therefore, the attack could be thwarted by limiting the number of continuous login attempts within a short period. In the second one, the adversary intercepts some message transmitted between the user and the server and then iteratively guesses the user's password and verifies the correctness in an off-line manner. The attack is more dangerous than the first one since the server cannot find the attack. In this section, we will show Lo et al.'s protocol is vulnerable to the off-line password guessing attack.

We assume that an attacker C has total control over the communication channel among A, B and S, which means that he can insert, delete, or alter any messages in the channel. Then C could intercept the message $\{ID_A, ID_B, E_{P_A}(N_A)\}$ sent by A, where $N_A = g^{R_A} \bmod p$ and R_A is a random number generated by A. Then, the adversary can guess a password P_A^* and computes $N_A^* = D_{P_A^*}(E_{P_A}(N_A))$. If the guessed password P_A^* is the correct password, N_A^* will be in the group G. Otherwise, N_A^* may be a value is not in G (It is easy to say that C could check whether N_A^* is in G by checking if both of the equations $N_A^* < p$ and $(N_A^*)^q = 1 \bmod p$ hold). Let P_A^* be an incorrect password. Then N_A^* is in G with the

probability $\frac{q}{p+c} < \frac{q}{p-1} \le \frac{1}{2}$, where c is the number of possible values not in F_p (i.e. equal to or larger than p). Let $\{ID_A, ID_B, E_{P_A}^{(i)}(N_A^{(i)})\}$ be n messages sent by A, where $i = 1, 2, \cdots, n$. Then the incorrect password P_A^* could pass all checks ($D_{P_A^*}(E_{P_A}^{(i)}(N_A^{(i)})) \in G$) with the probability $\left(\frac{q}{p+c}\right)^n \le \left(\frac{1}{2}\right)^n$. Once n is large enough (i.e. more than 20), $\left(\frac{1}{2}\right)^n$ could be ignorable. Let D be the set of candidate passwords. By the following steps, C could get the correct password with the probability $1-\left(\frac{1}{2}\right)^n \approx 1$.

1) C picks a candidate password P_A^* from D.

2) C checks whether all the equations $D_{P_A^*}(E_{P_A}^{(i)}(N_A^{(i)})) \in G$ hold, where $i = 1, 2, \cdots, n$. If all the equations hold, C find the correct password. Otherwise, C repeats 1) and 2) until the correct password is found.

From the above description, we know that C could get one of A 's passwords P_A by the off-line password guessing attack. By the same, C could also get one of B 's password P_B. Once getting P_A and P_B, C could get A 's another password P_{A1} and B 's another password P_{B1} through the following steps.

1) C generates two random numbers $R_A, R_B \in Z_q$ and computes $N_A = g^{R_A} \bmod p$, $N_B = g^{R_B} \bmod p$. Then C impersonate A and B to send $\{ID_A, ID_B, E_{P_A}(N_A)\}$ and $\{ID_A, ID_B, E_{P_B}(N_B)\}$ to S separately.

2) Upon receiving $\{ID_A, ID_B, E_{P_A}(N_A)\}$ and $\{ID_A, ID_B, E_{P_B}(N_B)\}$, S uses the corresponding passwords P_A and P_B to retrieve N_A and N_B from $E_{P_A}(N_A)$ and $E_{P_B}(N_B)$, respectively. S generates a random number $R_S \in Z_q$, computes $N_A^{R_S} = g^{R_A R_S} \bmod p$, $N_B^{R_S} = g^{R_B R_S} \bmod p$, $K_{AS} = N_A^{P_{A1}} = g^{R_A P_{A1}} \bmod p$ and $K_{BS} = N_B^{P_{B1}} = g^{R_B P_{B1}} \bmod p$. S sends $X = g^{R_B R_S} \cdot f_{K_{AS}}(ID_A, ID_B, N_A)$ and $Y = g^{R_A R_S} \cdot f_{K_{BS}}(ID_A, ID_B, N_B)$ to A and B respectively.

3) C intercepts the message $X = g^{R_B R_S} \cdot f_{K_{AS}}(ID_A, ID_B, N_A)$ and $Y = g^{R_A R_S} \cdot f_{K_{BS}}(ID_A, ID_B, N_B)$.

4) C guesses two passwords P_{A1}^* and P_{B1}^* from D for A and B respectively, where D the set of candidate passwords.

5) C computes $K_{AS}^* = N_A^{P_{A1}^*} \bmod p$, $K_{BS}^* = N_B^{P_{B1}^*} \bmod p$, $I = X / f_{K_{AS}^*}(ID_A, ID_B, N_A)$ and $J = Y / f_{K_{BS}^*}(ID_A, ID_B, N_A)$.

6) C checks whether $I^{R_B^{-1}} \bmod p$ and $J^{R_A^{-1}} \bmod p$ are equal, where R_A^{-1} and R_B^{-1} satisfy $R_A R_A^{-1} = 1 \bmod q$ and $R_B R_B^{-1} = 1 \bmod q$. If they are equal, C find the correct password P_{A1} and P_{B1}. Otherwise, C repeats 4), 5) and 6) until two correct passwords are found.

The attacker C may be a malicious user A. In this case, C just needs to get P_{B1} since he knows P_{A1}. Then the search space for the guessing attack is $|D|$, where D is the set of possible passwords and $|\cdot|$ represents the size of a set. Even though C does not know P_{A1}, the search space is $|D| \times |D|$. Generally speaking, $|D|$ is not so big unlike a space for cryptographic key. So C could get P_{A1} and P_{B1}. Then we could conclude that Lo et al.'s protocol is vulnerable to the off-line password guessing attack.

4 Conclusion

Recently, Lo et al. proposed a three-party password-based authenticated key exchange protocol and demonstrated its immunity against various attacks. However, after review of their protocol and analysis of its security, we show their protocol is venerable to the off-line password guessing attack. The analyses show that the protocol is insecure for practical application.

Acknowledgments

The authors thank Prof. Min-Shiang Hwang and the anonymous reviewers for their valuable comments. This research was supported by the Open Funds of State Key Laboratory of Information Security (No. 2013-3-3) and the Specialized Research Fund for the Doctoral Program of Higher Education of China (No. 20110141120003).

Reference

[1] M. Bellare, D. Pointcheval, and P. Rogaway, "Authenticated key exchange secure against dictionary attacks," in *Proceedings of Eurocrypt '00*, LNCS 1807, pp. 139-155, 2000.

[2] S. M. Bellovin and M. Merritt. Encrypted key exchange: password-based protocols secure against dictionary attacks. In *Proceedings of the 1992 IEEE symposium on research in security and privacy*, pages 72-84, 1992.

[3] V. Boyko, P. MacKenzie, and S. Patel. Provably secure password-authenticated key exchange using Diffie-Hellman. In *Proceedings of the Eurocrypt '00*, LNCS 1807, pages 156-171, 2000.

[4] H. R. Chung and W. C. Ku. Three weaknesses in a simple three-party key exchange protocol. *Information Science*, 178(1): 220-229, 2008.

[5] Y. F. Chang. A practical three-party key exchange protocol with round efficiency. *International Journal of Innovative Computing, Information and Control*, 4(4): 953-960, 2008.

[6] Y. Ding and P. Horster. Undetectable on-line password guessing attacks. *ACM Operating Systems Review*, 29(4): 77-86, 1995.

[7] H. Guo, Z. Li, Y. Mu, and X. Zhang. Cryptanalysis of simple three-party key exchange protocol. *Computers and Security*, 27(1-2): 16-21, 2008.

[8] IEEE P1363.2: Password-Based Public-Key Cryptography. (http://grouper.ieee.org/groups/1363/passwdPK/)

[9] S. Jiang and G. Gong. Password based key exchange with mutual authentication. In *Proceedings of SAC '04*, LNCS 3357, pages 267-279, 2005.

[10] J. Katz, R. Ostrovsky, and M. Yung. Efficient password-authenticated key exchange using human-memorable passwords. In *Proceedings of the Eurocrypt '01*, LNCS 2045, pages 475-494, 2001.

[11] C. L. Lin, H. M. Sun, and T. Hwang. Three party-encrypted key exchange: attacks and a solution. *ACM Operating Systems Review*, 34(4): 12-20, 2000.

[12] N. W. Lo and K. H. Yeh. A practical three-party authenticated key exchange protocol. *International Journal of Innovative Computing, Information and Control*, 6(6): 2469-2483, 2010.

[13] R. X. Lu and Z. F. Cao. Simple three-party key exchange protocol. *Computers and Security*, 26(1): 94-97, 2007.

[14] T. F. Lee, T. Hwang, and C. L. Lin. Enhanced three-party encrypted key exchange without server public keys. *Computers and Security*, 23(7): 571-577, 2004.

[15] J. Nam, Y. Lee, S. Kim, and D. Won. Security weakness in a three-party pairing-based protocol for password authenticated key exchange. *Information Sciences*, 177(6): 1364-1375, 2007.

[16] C. W. Phan Raphael, W. C. Yau, and B. M. Goi. Cryptanalysis of simple three-party key exchange protocol (S-3PAKE). *Information Science*, 178(13): 2849-2856, 2008.

[17] M. Steiner, G. Tsudik, and M. Waidner. Refinement and extension of encrypted key exchange. *ACM Operating Systems Review*, 29(2): 22-30, 1995.

[18] H. A. Wen, T. F. Lee, and T. Hwang. Provably secure three-party password-based authenticated key exchange protocol using Weil pairing. *IEE Proceedings-Communications*, 152(2): 138-143, 2005.

[19] M. Zhang. New approaches to password authenticated key exchange based on RSA. In *Proceedings of the Asiacrypt '04*, LNCS 3329, pages 230-244, 2004.

Debiao He received his Ph.D. degree in applied mathematics from School of Mathematics and Statistics, Wuhan University in 2009. He is currently a lecturer of Wuhan University. His main research interests include cryptography and information security, in particular, cryptographic protocols.

Yuanyuan Zhang received the M.S. degree in applied mathematics from Wuhan University, Wuhan, China in 2002. She is currently pursuing the Ph. D. degree in applied mathematics from Wuhan University, Wuhan, China. Her research interests are in the areas of cryptography, information security and network security.

Jianhua Chen received the B.Sc. degrees in applied mathematics from Harbin Institute of Technology, Harbin, China, in 1983, and received the M.Sc and the Ph.D. degree in applied mathematics from Wuhan University, Wuhan, China, in 1989 and 1994, respectively. Currently, he is a professor of Wuhan University. His current research interests include number theory, information security and network security.