ISSN 1392 – 124X INFORMATION TECHNOLOGY AND CONTROL, 2008, Vol.37, No.4

ON SECURITY OF A PRACTICAL THREE-PARTY KEY EXCHANGE PROTOCOL WITH ROUND EFfiCIENCY

Cheng-Chi Lee

Asia University, Department of Information and Communication Engineering
No. 500, Lioufeng Raod, Wufeng Shiang, Taichung, Taiwan, R.O.C.

Ya-Fen Chang

National Taichung Institute of Technology, Department of Computer Science and Information Engineering
Taichung 404, Taiwan, R.O.C.

Abstract. Recently, Chang proposed a practical three-party key exchange (C-3PEKE) protocol with round efficiency. Unfortunately, this paper shall show that C-3PEKE is not secure and suffers from off-line password guessing attacks.

Keywords: Password, key exchange, 3PEKE, password guessing attack.

1. Introduction

Recently, Chang proposed a practical three-party key exchange (C-3PEKE) protocol with round efficiency [1]. It allows two parties A and B to share an easy-to-remember password with a trusted server S. S acts as a coordinator between two communication parties to complete mutual authentication. Once authentication is achieved, two parties can share a session key to encrypt and decrypt their communication. A practical 3PEKE protocol should comply with the following requirements [1]:

(1) The session key should be agreed by the communication parties instead of being assigned by the server directly.

(2) Except the password, no extra secret information should be needed - the public key for example.

(3) The server has to authenticate both communication parties.

(4) Computation and round efficiencies should be provided at the same time.

Password guessing attacks can be divided into three classes: (1) detectable on-line password guessing attacks, (2) undetectable on-line password guessing attacks, and (3) off-line password guessing attacks. Among the three classes, off-line password guessing attacks are the most critical ones [2, 3]. Chang had shown that C-3PEKE not only meets all above requirements, but also withstands the three attacks. As a result, C-3PEKE is a practical three-party key exchange protocol with round efficiency. It is superior to others [1]. However, the authors shall show that C-3PEKE suffers from off-line password guessing attacks. We will show it in Section 3.

The rest of this paper is organized as follows. We review C-3PEKE in Section 2. In Section 3, we show our off-line password guessing attacks on C-3PEKE. Finally, some conclusions are drawn in Section 4.

2. A Review of C-3PEKE

In this section, we review Chang's practical three-party key exchange (C-3PEKE) protocol. The notations used throughout this paper are listed in Table 1. The details of C-3PEKE are given as follows:

Step 1: A sends (ID_A, ID_B, N_A) to S as request.

Step 2: After receiving A's request, S computes K_{AS}=${N_A}^{R_{S_1}} \bmod p$=$g^{R_{S_1}R_A} \bmod p$. Then, S sends (ID_A, N_A, $E3_{P_A}(N_{S_1})$, $E3_{P_B}(N_{S_2})$, $f_{K_{AS}}(ID_A$, ID_B, $N_A)$) to B.

Step 3: Upon receiving S's message, B first decrypts $E3_{P_B}(N_{S_2})$ using his/her password P_B to get N_{S_2}. Then B computes K_{BS}=${N_{S_2}}^{R_B} \bmod p$= =$g^{R_{S_2}R_B} \bmod p$ and K_{AB}=${N_A}^{R_B} \bmod p$=$g^{R_AR_B} \bmod p$. Next, B sends (ID_B, N_B, $E3_{P_A}(N_{S_1})$, $f_{K_{AS}}(ID_A, ID_B, N_A)$, $f_{K_{AB}}(ID_A$, ID_B, $N_A)$, $f_{K_{BS}}(ID_A, ID_B, N_{S_2})$) to A.

Step 4: Upon receiving the message, A first decrypts $E3_{P_A}(N_{S_1})$ using P_A to get N_{S_1}. Then A computes K_{AS}=${N_{S_1}}^{R_A} \bmod p$=$g^{R_{S_1}R_A} \bmod p$ and K_{AB}=${N_B}^{R_A} \bmod p$=$g^{R_AR_B} \bmod p$. Firstly, A uses K_{AS} to compute $f_{K_{AS}}(ID_A, ID_B, N_A)$ and verifies if the computation result is equal to the received one. If it is correct, A believes that he/she is communicating with a legitimate S; otherwise, A regards S illegal and terminates the protocol. Secondly, A uses K_{AB} to compute $f_{K_{AB}}(ID_A, ID_B, N_A)$ and verifies if the

Table 1. The Notations

Notations	Description
A, B	communication parties
S	the trusted server
ID_A/ID_B/ID_S	the identity of A/B/S
P_A/P_B	the password securely shared by A/B with S
$E3_P()$	a symmetric encryption scheme with a password P
p	a large prime
g	an element of order q with modulus p
G	a finite cyclic group generated by g in Z_p
R_A/R_B	the random exponents chosen by A/B
R_{S_1}, R_{S_2}	two random exponents chosen by S
N_A, N_B	N_A=g^{R_A} mod$p$, N_B=g^{R_B} mod$p$
N_{S_1}, N_{S_2}	N_{S_1}=$g^{R_{S_1}}$ mod$p$, N_{S_2}=$g^{R_{S_2}}$ mod$p$
$f_K(\cdot)$	a pseudo-random function (PRF) indexed by K
K_{AS}/K_{BS}	a one-time strong key shared by A/B and S
K_{AB}	a session key shared by A and B

computation result is equal to the received one. If it is correct, A believes that he/she is communicating with a legitimate B; otherwise, A regards B illegal and terminates the protocol. After authenticating S and B, A sends (ID_A, ID_B, N_B, $f_{K_{AS}}(ID_A, ID_B, N_{S_1})$, $f_{K_{BS}}(ID_A, ID_B, N_{S_2})$, $f_{K_{AB}}(ID_A, ID_B, N_B)$) to S.

Step 5: Upon receiving the message, S computes K_{BS}=${N_B}^{R_{S_2}}$ mod$p$=$g^{R_{S_2}R_B}$ mod$p$. Firstly, S uses K_{AS} to compute $f_{K_{AS}}(ID_A, ID_B, N_{S_1})$ and verifies if the computation result is equal to the received one. If it is correct, S believes that he/she is communicating with a legitimate A; otherwise, S regards A illegal and terminates the protocol. Secondly, S uses K_{BS} to compute $f_{K_{BS}}(ID_A, ID_B, N_{S_2})$ and verifies if the computation result is equal to the received one. If it is correct, S believes that he/she is communicating with a legitimate B; otherwise, S regards B illegal and terminates the protocol. After authenticating A and B, S sends (ID_A, $f_{K_{AB}}(ID_A, ID_B, N_B)$, $f_{K_{BS}}(ID_A, ID_B, N_B)$) to B. After receiving the message, B uses K_{BS} to compute $f_{K_{BS}}(ID_A, ID_B, N_B)$ and verifies if the computation result is equal to the received one. If it is correct, B believes that he/she is communicating with a legitimate S; otherwise, B regards S illegal and terminates the protocol. Next, B uses K_{AB} to compute $f_{K_{AB}}(ID_A, ID_B, N_B)$ and verifies if the computation result is equal to the received one. If it is correct, B believes that he/she is communicating with a legitimate A; otherwise, B regards A illegal and terminates the protocol.

Finally, A and B can share the session key K_{AB} to encrypt and decrypt their communicated messages.

3. Off-line Password Guessing Attacks on C-3PEKE

In this section, we shall show that Chang's 3PEKE is not robust enough against off-line password guessing attacks from an evil E. An evil E can intercept transmitted messages from public channel and then break password by playing off-line guessing attacks. E can guess a password P' until the guessing password P' is equal to the correct password P. Otherwise, E repeatedly guesses a new P' off-line. Suppose that E tends to get A's password P_A. How C-3PEKE suffers from off-line password guessing attacks is given as follows:

Step 1: E wiretaps that parties A and B communicate with S. E can intercept ID_A and ID_B.

Step 2: E forges A communicate with S. He/she chooses a new random number R'_A and computes N'_A=$g^{R'_A}$ mod$p$. Then E forges A to send (ID_A, ID_B, N'_A) to S.

Step 3: After receiving E's request, S computes K_{AS}=${N'_A}^{R_{S_1}}$ mod$p$=$g^{R_{S_1}R'_A}$ mod$p$. Then, S sends (ID_A, N'_A, $E3_{P_A}(N_{S_1})$, $E3_{P_B}(N_{S_2})$, $f_{K_{AS}}(ID_A, ID_B, N'_A)$) to B. Since E wiretaps their communications, he/she can intercept $E3_{P_A}(N_{S_1})$ and $f_{K_{AS}}(ID_A, ID_B, N'_A)$.

Step 4: Once E intercepts $E3_{P_A}(N_{S_1})$ and $f_{K_{AS}}(ID_A, ID_B, N'_A)$, he/she can play off-line guessing attacks.

In the following, why this attack works is demonstrated. E guesses a password P'. He/She first decrypts $E3_{P_A}(N_{S_1})$ using P'. If P'=P_A, he/she can get N_{S_1}. Then E can compute K_{AS}=${N_{S_1}}^{R'_A}$ mod$p$= =$g^{R_{S_1}R'_A}$ mod$p$. Next, E computes $f_{K_{AS}}(ID_A, ID_B, N'_A)$ and verifies if the computation result is equal to the intercepted one. If it is correct, E believes that

he/she had guessed a correct password P_A; otherwise, E repeatedly guesses a new P' off-line till E can guess a correct password P_A. In the same way, E can get B's password P_B. Therefore, C-3PEKE suffers from off-line password guessing attacks. C-3PEKE is insecure.

4. Conclusions

Chang had proposed a secure, efficient, and practical three-party key exchange protocol. However, this paper had shown that her scheme suffers from off-line password guessing attacks.

Acknowledgment

This work was supported in part by Taiwan Information Security Center (TWISC), National Science Council under the grant NSC 97-2218-E-468-010.

References

[1] **Y.F. Chang.** A Practical Three-party Key Exchange Protocol with Round Efficiency. *International Journal of Innovative Computing, Information and Control*, *Vol*.4, *No*.4, *April* 2008, 953–960.

[2] **Y. Ding, P. Horster.** Undetectable on-line password guessing attacks. *ACM Operating Systems Review*, *Vol*.29, *No*.4, 1995, 77–86.

[3] **C.S. Tsai, C.C. Lee, M.S. Hwang.** Password Authentication Schemes: Current Status and Key Issues. *International Journal of Network Security*, *Vol*.3, *No*.2, *Sept*. 2006, 101–115.

Received August 2008.