Improvement of a three-party key exchange protocol

Sida Lin
Zhejiang Natural Science Foundation committee, Hangzhou, China

Qi Xie†
Graduate School of Hangzhou Normal University,Hangzhou, China
Corresponding E-mail: qixie68@yahoo.com.cn

Abstract

Recently， Lu and Cao proposed a novel three-party key exchange protocol. Guo et al pointed out that their protocol cannot resist man-in-the-middle attack and undetectable on-line dictionary attack, and then an improved protocol was proposed in 2008.However, we show that Guo et al's protocol is still vulnerable to undetectable on-line dictionary attack. To overcome the security flaw, an improved scheme is proposed.

1. Introduction

Three-party key exchange protocol with password authentication is that two clients share an easy-to-remember password with a trusted server and can securely exchange keys via the server[1][2]. Since it is widely used to send secret messages using the session key among parties over an insecure public network, therefore, lots of key exchange protocols have been proposed[3-8].

Since users usually choose easy-to-remember passwords, therefore, password based authenticated key exchange protocols suffer from password guessing attack. For example, Steiner et al's, Abdalla et al's[3], Byun et al's[4] and Yin et al's[5] protocols cannot resist the password guessing attacks[6][7]. Lin et al[8] and Ding et al[9] thought that the password guessing attacks have three classes:

- Detectable on-line dictionary attack: An attacker attempts to use a guessed password in an on-line transaction. He verifies the correctness of his guess using the response from server. A failed guess can be detected and logged by the server.
- Undetectable on-line dictionary attack: An attacker tries to verify a password guess in an on-line transaction. However, a failed guess can not be detected and logged by the server.
- Off-line dictionary attack: An attacker guesses a password and verifies his guess off-line. No participation of server is required, so the server does not notice the attack.

Recently, Lu and Cao[10] proposed a novel three-party key exchange protocol. However, Guo et al pointed out that their protocol cannot resist man-in-the-middle attack and undetectable on-line dictionary attack. To fix the security flaws, Guo et al [11] proposed that the identities of two clients are added to the hash function in the messages from server, and two clients create the message authentication codes enable the server to verify the message authentication codes, then they proposed an improvement protocol. In this paper, we show that Guo et al's protocol is still vulnerable to undetectable on-line dictionary attack. To overcome the security flaw, an improved scheme is proposed.

2. Brief review of Guo et al's protocol

2.1.Notation

The notations used in Guo et al's protocol as follows:

- G, g, p :a finite cyclic group G generated by an element g of prime order p.
- M, N :two elements in G.
- S : a trusted server.
- A, B :two clients.
- pw_1 :the password shared between A and S.
- pw_2 :the password shared between B and S.
- $MAC_{key}(\cdot)$:message authentication code.
- k_{AS} : the $MAC_{key}(\cdot)$ key shared between A and S.
- k_{BS} : the $MAC_{key}(\cdot)$ key shared between B and S.

- H, H' :two secure one-way hash functions.
- ||: concatenation operation.

2.2 . Guo et al's three-party key exchange protocol

Guo et al's three-party key exchange protocol is described as follows:

- Step1: $A \rightarrow B : A \| X \| \delta_A$

A chooses a random number x ,computes $X = g^x \cdot M^{pw_1}$ and $\delta_A = MAC_{k_{AS}}(X)$. Then he sends $A \| X \| \delta_A$ to B .

- Step2: $B \rightarrow S : A \| X \| \delta_A \| B \| Y \| \delta_B$

B chooses a random number y ,computes $Y = g^y \cdot N^{pw_2}$ and $\delta_B = MAC_{k_{BS}}(Y)$. Then he sends $A \| X \| \delta_A \| B \| Y \| \delta_B$ to S .

- Step3: $S \rightarrow B : X' \| Y'$

Upon receiving $A \| X \| \delta_A \| B \| Y \| \delta_B$, the server S first verifies the validity of δ_A and δ_B , then he computes $g^x = X / M^{pw_1}$ with the password pw_1 and $g^{xz} = (g^x)^z$ with the random number z , $g^y = Y / N^{pw_2}$ with the password pw_2 and $g^{yz} = (g^y)^z$ with the random number z , respectively. Next, S computes $X' = g^{yz} \cdot H(A, B, S, g^x)^{pw_1}$ and $Y' = g^{xz} \cdot H(B, A, S, g^y)^{pw_2}$. Finally S sends $X' \| Y'$ to B .

- Step4: $B \rightarrow A : X' \| \alpha$

Upon receiving $X' \| Y'$, B computes $g^{xz} = Y' / H(B, A, S, g^y)^{pw_2}$ and $\alpha = H(A, B, g^{xyz})$. Then he forwards $X' \| \alpha$ to A .

- Step5: $A \rightarrow B : \beta$

Upon receiving $X' \| \alpha$, A first computes $g^{yz} = X' / H(A, B, S, g^x)^{pw_1}$ and checks whether $\alpha = H(A, B, g^{xyz})$ holds or not. If it does not hold, terminates the protocol. Otherwise, he convinced that g^{xyz} is valid, and obtains the session key $SK_A = H'(A, B, g^{xyz})$. Finally, he computes $\beta = H'(B, A, g^{xyz})$ and sends it to B .

When B receives β from A , he checks whether $\beta = H'(B, A, g^{xyz})$ holds or not. If it does not hold, terminates the protocol. Otherwise, he obtains the session key $SK_B = H'(A, B, g^{xyz})$.

3. Attacks on the Guo et al's protocol

In this section, we show that Guo et al's three-party key exchange protocol cannot resist undetectable on-line dictionary attack. The attacks are described as follows.

3.1. Aattack one

Assume that B is a malicious client and wants to guess A 's password pw_1 , he can obtain many messages $A \| X_i \| \delta_{Ai}$ generated by A in insecure network when A and other valid clients perform the key exchange protocol.

For one of the message $A \| X \| \delta_A$ generated by A , B guesses A 's password pw_1' , and computes $\overline{X} = X / M^{pw_1'} = g^{x'}$ for unknown x' . Then he chooses a random number y , computes $Y = g^{x'y} \cdot N^{pw_2}$ and $\delta_B = MAC_{k_{BS}}(Y)$. Finally B sends $A \| X \| \delta_A \| B \| Y \| \delta_B$ to S .

Upon receiving $A \| X \| \delta_A \| B \| Y \| \delta_B$, the server S first verifies the validity of δ_A and δ_B , then he computes $g^x = X / M^{pw_1}$ with the password pw_1 and $g^{xz} = (g^x)^z$ with the random number z , $g^{x'y} = Y / N^{pw_2}$ with the password pw_2 and $g^{x'yz} = (g^{x'y})^z$ with the random number z ,respectively. Next, S computes $X' = g^{x'yz} \cdot H(A, B, S, g^x)^{pw_1}$ and $Y' = g^{xz} \cdot H(B, A, S, g^{x'y})^{pw_2}$. Finally S sends $X' \| Y'$ to B .

Upon receiving $X' \| Y'$, B computes $g^{xz} = Y' / H(B, A, S, g^{x'y})^{pw_2}$ and $g^{x'yz} = X' / H(A, B, S, g^{x'})^{pw_1'}$, then checks whether $g^{x'yz} = (g^{xz})^y$ hold or not. If it holds, B conforms that the guessed password pw_1' is the correct one. Other wise, B repeatedly performs the above processes using other messages $A \| X_i \| \delta_{Ai}$ generated by A without being noticed by S .

3.2. Attack two

Assume that B is a malicious client and wants to guess A 's password pw_1. When A and a legitimate user C operate the key exchange protocol in the first two steps. B chooses a random number y, computes $Y = g^y \cdot N^{pw_2}$ and $\delta_B = MAC_{k_{BS}}(Y)$. He then intercepts the incoming message $A \| X \| \delta_A \| C \| Z \| \delta_C$ and forges message $A \| X \| \delta_A \| B \| Y \| \delta_B$, then sends it to S

Upon receiving $A \| X \| \delta_A \| B \| Y \| \delta_B$, the server S operates step 3 as specified in the protocol, and sends $X' \| Y'$ to B, where $X' = g^{yz} \cdot H(A,B,S,g^x)^{pw_1}$ and $Y' = g^{xz} \cdot H(B,A,S,g^y)^{pw_2}$.

Upon receiving $X' \| Y'$, B computes $g^{xz} = Y' / H(B,A,S,g^y)^{pw_2}$ and $\alpha = H(A,C,g^{xyz})$. Next, B guesses A 's password pw_1', and computes $\overline{X} = X / M^{pw_1'} = g^{x'}$ for unknown x', $\overline{X'} = g^{yz} \cdot H(A,C,S,g^{x'})^{pw_1'}$, where $\overline{X'} = X' \cdot d$ and $H(A,B,S,g^{x'})^{pw_1'} \cdot d = H(A,C,S,g^{x'})^{pw_1'}$. Then he forwards $\overline{X'} \| \alpha$ to A. On the other hand, B randomly chooses $\overline{\overline{X'}}$ and $\overline{\overline{Y'}}$, and sends $\overline{\overline{X'}} \| \overline{\overline{Y'}}$ to C. C may not obtain the valid session key, but he may not detect B 's malicious trial.

A can compute g^{xyz} and verify $\alpha = H(A,C,g^{xyz})$, if verification passes, he will compute $\beta = H'(C,A,g^{xyz})$ and sends it to C, or else terminates the protocol. If A sends β to C, B can intercept β ,and verify the validity by $\beta = H'(C,A,g^{xyz})$ .If it holds, B conforms that the guessed password pw_1' is the correct one. Otherwise, B repeatedly performs the above processes when A and a legitimate user operate the key exchange protocol.

4. Countermeasure and the improved protocol

To overcome the security flaws of Guo et al's three-party key exchange protocol, for the first attack, we change $X = g^x \cdot M^{pw_1}$ to $X = g^x \cdot M^{pw_1} \cdot g^{k_{AS}}$ and Y to $Y = g^y \cdot N^{pw_2} \cdot g^{k_{BS}}$. Since $g^x = X / M^{pw_1} \cdot g^{k_{AS}}$, therefore, the malicious client cannot guess the correct pw_1 and k_{AS} under the assumption of the intractability of solving the discrete logarithm problem. For the second attack, we let the server S also creates message authentication code of X' and Y' in step 3, which can overcome the malicious client to revise X' or Y'. The improved protocol as follows:

- Step1: $A \to B : A \| X \| \delta_A$, where $X = g^x \cdot M^{pw_1} \cdot g^{k_{AS}}$ with a random number x, and $\delta_A = MAC_{k_{AS}}(X)$.
- Step2: $B \to S : A \| X \| \delta_A \| B \| Y \| \delta_B$, where $Y = g^y \cdot N^{pw_2} \cdot g^{k_{BS}}$ with a random number y ,and $\delta_B = MAC_{k_{BS}}(Y)$.
- Step3: S verifies the validity of δ_A and δ_B, then $S \to B : X' \| Y' \| \delta_A' \| \delta_B'$, where $X' = g^{yz} \cdot H(A,B,S,g^x)^{pw_1}$ and $Y' = g^{xz} \cdot H(B,A,S,g^y)^{pw_2}$ with the random number z , $\delta_A' = MAC_{k_{AS}}(X')$, $\delta_B' = MAC_{k_{BS}}(Y')$.
- Step4: B verifies the validity of δ_B' and $B \to A : X' \| \alpha \| \delta_A'$, where $\alpha = H(A,B,g^{xyz})$.
- Step5: A verifies the validity of δ_A' , $\alpha = H(A,B,g^{xyz})$, obtains the session key $SK_A = H'(A,B,g^{xyz})$ and $A \to B : \beta$, where $\beta = H'(B,A,g^{xyz})$.

When B receives β from A, he checks whether $\beta = H'(B,A,g^{xyz})$ holds or not. If it does not hold, terminates the protocol. Otherwise, he obtains the session key $SK_B = H'(A,B,g^{xyz})$.

5. Conclusion

We have analyzed the security of Guo et al's three-party key exchange protocol. Their protocol is cannot resist undetectable on-line dictionary attack. To overcome the security flaws, we proposed an improved protocol.

6. References

[1] L.Gong,M.A.Lomas, R.Needham, J.Saltzerr, "Protecting poorly chosen secrets from guessing attacks." *IEEE Journal on Selected Areas in Communications*, 11(5)(1993):648-656.

[2] M.Steiner, G.Tsudik, M.Waidner, "Refinement and extension of encrypted key exchange." *ACM Operating Systems Review*, 29(3)(1995):22-30.

[3] M. Abdalla, D. Pointcheval, "Simple password-based encrypted key exchange protocols," *Topics in Cryptology – CT-RSA 2005*. In:LNCS. Springer-Verlag; 2005. p. 191–208.

[4] J.W. Byun, D.H. Lee, J. Lim, "Efficient and Provably Secure Client-to-Client Password-Based Key Exchange Protocol." *In: Proceedings of APWeb'06*. LNCS, vol. 3841; 2006. p. 830–6.

[5] Y. Yin, L.Bao, "Secure cross-realm C2C-PAKE protocol. " *In:Proceedings of ACISP'06*. LNCS, vol. 4058; 2006. p. 395–406.

[6] W.J. Wang, L. Hu, "Efficient and provably secure generic construction of three-party password-based authenticated key exchange protocols," *INDOCRYPT'06*. In: LNCS; 2006. p.118–32.

[7] R. C. Phan, B. M. Goi. "Cryptanalysis of two provably secure cross-realm C2C-PAKE protocols, " *INDOCRYPT'06*. In:LNCS; 2006. p. 104–17.

[8] C.L.Lin, H.M.Sun, M.Steiner, T.Hwang, "Three-party encrypted key exchange without server public-keys." *IEEE Communication Letters*, 5(12)(2001):497-499.

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

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

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