Cryptanalysis of a Provably Secure Gateway-Oriented Password-Based Authenticated Key Exchange Protocol

Debiao He
School of Mathematics and Statistics, Wuhan University,
Wuhan, People's Republic of China
hedebiao@163.com

***Abstract*—Recently, Chien et al. proposed a gateway-oriented password-based authenticated key exchange (GPAKE) protocol, through which a client and a gateway could generate a session key for future communication with the help of an authentication server. They also demonstrated that their scheme is provably secure in a formal model. However, in this letter, we will show that Chien et al.'s protocol is vulnerable to the off-line password guessing attack. To overcome the weakness, we also propose an efficient countermeasure.**

Keywords-Password-based; Authenticated key exchange; Gateway; Off-line password guessing attack

I. INTRODUCTION

A gateway-oriented password-based authenticated key exchange (GPAKE) protocol is a three-party protocol, which allows a client and a gateway to establish a session key with the help of an authentication server.

Abdalla et al. [1] proposed security requirements of GPAKE protocols and proposed the first GPAKE protocol in 2005. Although Abdalla et al. had proved the session key semantic security of their scheme in a formal model, Byun et al. [2] pointed out that Abdalla et al.'s protocol cannot withstand an undetectable on-line guessing attack. To improve security, Byun et al. also proposed an improved scheme. However, Wu et al. [3] found that Byun et al.'s protocol still cannot resist the on-line undetectable guessing attack. In 2008, Abdalla et al. [4] further improved their scheme to enhance security and anonymity. Recently, Chien et al. [5] demonstrated that Abdalla et al.'s protocol [4] is still vulnerable to an undetectable on-line guessing attack. Chien et al. [5] also proposed a new GPAKE protocol to overcome the weakness. They also proved that their protocol is provably secure if the computational Diffie-Hellman problem (CDHP) is hard. In this letter, we review the GPAKE scheme and show that it does actually leak information of password to a malicious gateway. Especially, we show that the GPAKE scheme is susceptible to an off-line password guessing attack by a malicious gateway. We also propose an efficient countermeasure to overcome the weaknesses.

II. REVIEW OF CHIEN ET AL.'S PROTOCOL

This section reviews Chien et al.'s protocol. For convenience, we introduce some notations used in this letter.

- p : a large prime;
- q : a prime, where $q \mid p-1$;
- g : an element of order q with modulus p;
- C : the client;
- G : the gateway;
- S : the trusted server;
- ID_C, ID_G, ID_S : the identities of C, G and S separately;
- pw : the password shared between C and S;
- K_{GS} : the secret key shared between G and S;
- $h_1(\cdot), h_2(\cdot)$: two secure hash functions;
- sid : the session identity.

If the client C and the gateway G want to generate a session key for future communication with the help of the server S, as shown in Fig. 1, the following steps will be executed.

1). C sends the request message $Msg_1 = \{sid, ID_C\}$ to G.

2). G sends the message $Msg_2 = \{sid, ID_C, ID_G\}$ to S.

3). Upon receiving the message Msg_2, S generates a random number $z \in Z_q^*$, computes $Z = g^z \bmod p$, $\overline{Z} = g^z \cdot g^{h_1(pw)} \bmod p$ and sends $Msg_3 = \{sid, \overline{Z}\}$ to G.

4). After receiving Msg_3, G generates a random number $y \in Z_q^*$, computes $Y = g^y \bmod p$ and sends $Msg_4 = \{sid, ID_C, ID_G, Z, Y\}$ to C.

5). Upon receiving Msg_4, C generates a random number $x \in Z_q^*$, computes $Z = \frac{\overline{Z}}{g^{h_1(pw)}} \bmod p$, $X = g^x \bmod p$, $sk_{CS} = h_1(sid \| ID_C \| ID_S \| X \| Z \| Z^x)$, $sk_{CG} = h_1(sid \| ID_C \| ID_G \| X \| Y \| Y^x)$, $sk''_{CG} = h_2(sid \| ID_C \| ID_G \| X \| Y \| Y^x)$, $M_1 = h_1(sid \| ID_C \| ID_S \| X \| Z \| Z^x \| sk_{CS})$ and $M_2 = h_1(sid \| ID_C \| ID_G \| X \| Y \| Y^x \| sk_{CG})$. At last, C sends $Msg_5 = \{sid, X, M_1, M_2\}$ to G.

6). After receiving Msg_5, G computes $sk_{CG} = h_1(sid \| ID_C \| ID_G \| X \| Y \| X^y)$, $sk''_{CG} = h_2(sid \| ID_C \| ID_G \| X \| Y \| X^y)$, and checks whether M_2 and $h_1(sid \| ID_C \| ID_G \| X \| Y \| X^y \| sk_{CG})$ are equal. If they are not equal, G stops the session. Otherwise, G computes $M_3 = h_1(Y, K_{GS})$ and sends the message $Msg_6 = \{sid, X, M_1, Y, M_3\}$ to S.

7). After receiving Msg_6, S computes $sk_{CS} = h_1(sid \| ID_C \| ID_S \| X \| Z \| X^z)$ and checks whether M_1 and $h_1(sid \| ID_C \| ID_S \| X \| Z \| X^z \| sk_{CS})$ are equal. If they are not equal, S stops the session. Otherwise, S checks whether M_3 and $h_1(Y, K_{GS})$ are equal. If they are not equal, S stops the session. Otherwise, S computes $M_4 = h_1(sid \| ID_C \| ID_G \| Y \| X^z \| sk_{CS})$ and sends the message $Msg_7 = \{sid, M_4, \text{success}\}$ to G.

8). After receiving Msg_7, G computes $M_5 = h_1(sid \| ID_C \oplus ID_G \| Y^x \| sk_{CG})$ and sends $Msg_8 = \{sid, M_3, M_4, \text{success}\}$ to C.

9). After receiving Msg_8, C checks whether the equations $M_4 = h_1(sid \| ID_C \| ID_G \| Y \| Z^x \| sk_{CS})$ and $M_5 = h_1(sid \| ID_C \oplus ID_G \| X^y \| sk_{CG})$ are equal. If one of the two equations does hold, C stops the session. Otherwise, S is authenticated and C confirm the session key $sk_{CG} = h_1(sid \| ID_C \| ID_G \| X \| Y \| Y^x)$.

III. CRYPTANALYSIS OF CHIEN ET AL.'S PROTOCOL

In password authentication and update schemes that the client is allowed to choose his password, the client tends to choose a password that can be easily remembered for his convenience [6]. However, these easy-to-remember passwords are potentially vulnerable to password guessing attack, in which an adversary can try to guess the client's password and then verify his guess. The password guessing attack can be classified into the on-line password guessing attack and the off-line password guessing attack according. In the on-line password guessing attack, the adversary guesses a password and verifies its correctness through the on-line manner. In the off-line password attack, the adversary intercepts some password-related messages exchanged between the participants, and then iteratively guesses the password and verifies whether his guess is correct or not in an off-line manner. On-line password guessing attacks can be easily thwarted by limiting the number of continuous login attempts within a short period. In an offline password guessing attack, since there is no need for the server to participate in the verification, the server cannot easily notice the attack [6]. Although Chien et al. claimed that their scheme could resist various attacks; in the following, we will propose an off-line password guessing attack against the Chien et al.'s protocol where a malicious gateway of GPAKE is able to legally gain information about the password. Our attack consists of two phases. The detail is described as follows.

- **First phase**

1) Upon receiving the request message $Msg_1 = \{sid, ID_C\}$ sent by C, G generates two random numbers $y, z \in Z_q^*$ and computes $Y = g^y \bmod p$, $\overline{Z} = g^z \bmod p$. Then, G sends the message $Msg_4 = \{sid, ID_C, ID_G, Z, Y\}$ to C.

2) Upon receiving Msg_4, C generates a random number $x \in Z_q^*$, computes $Z = \frac{\overline{Z}}{g^{h_1(pw)}} \bmod p$, $X = g^x \bmod p$, $sk_{CS} = h_1(sid \| ID_C \| ID_S \| X \| Z \| Z^x)$, $sk_{CG} = h_1(sid \| ID_C \| ID_G \| X \| Y \| Y^x)$, $sk''_{CG} = h_2(sid \| ID_C \| ID_G \| X \| Y \| Y^x)$, $M_1 = h_1(sid \| ID_C \| ID_S \| X \| Z \| Z^x \| sk_{CS})$ and $M_2 = h_1(sid \| ID_C \| ID_G \| X \| Y \| Y^x \| sk_{CG})$. At last, C sends $Msg_5 = \{sid, X, M_1, M_2\}$ to G.

3) Upon receiving Msg_5, G could carry out the second phase to get the password.

- **Second phase**

1) G guesses a password pw^* from the uniformly distributed dictionary.

2) G computes $Z^* = \frac{\overline{Z}}{g^{h_1(pw^*)}} \bmod p$, $(Z^x)^* = \frac{X^z}{X^{h_1(pw^*)}} \bmod p$ and $(sk_{CS})^* = h_1(sid \| ID_C \| ID_S \| X \| Z^* \| (Z^x)^*)$.

3) G checks whether M_1 and $h_1(sid \| ID_C \| ID_S \| X \| Z^* \| (Z^x)^* \| (sk_{CS})^*)$ are equal. If they are equal, G finds the correct password. Otherwise, G repeats 1), 2) and 3) until the correct password is found.

It is obvious that if pw^* and pw are equal, we will have

$$Z = \frac{\overline{Z}}{g^{h_1(pw)}} \bmod p = \frac{\overline{Z}}{g^{h_1(pw^*)}} = Z^* \quad (1)$$

$$Z^x = \left(\frac{\overline{Z}}{g^{h_1(pw)}}\right)^x = \frac{\left(g^z\right)^x}{\left(g^{h_1(pw)}\right)^x} = \frac{\left(g^x\right)^z}{\left(g^x\right)^{h_1(pw)}} = \frac{X^z}{X^{h_1(pw)}} = \frac{X^z}{X^{h_1(pw^*)}} = (Z^x)^* \quad (2)$$

$$sk_{CS} = h_1(sid \| ID_C \| ID_S \| X \| Z \| Z^x) = h_1(sid \| ID_C \| ID_S \| X \| Z^* \| (Z^x)^*) = (sk_{CS})^* \quad (3)$$

and

$$M_1 = h_1(sid \| ID_C \| ID_S \| X \| Z \| Z^x \| sk_{CS}) = h_1(sid \| ID_C \| ID_S \| X \| Z^* \| (Z^x)^* \| (sk_{CS})^*) \quad (4)$$

Then we can conclude that Chien et al.'s protocol is venerable to the off-line password guessing attack.

IV. COUNTERMEASURE

In Chien et al.'s protocol, sk_{CS} is simply a linear combination of g^x, g^z, and $g^{h_1(pw)}$. The adversary can deduce it upon identifying two out of the three values correlating to g^x, g^z, and $g^{h_1(pw)}$. Then, having guessed what the password might be, the adversary can verify whether or not the guess is correct. To withstand such an attack, we just need to modify 3) and 5) of Chien et al.'s protocol as follows.

- In the step 3) of Chien et al.'s protocol, G compute $\overline{Z} = g^z \cdot h_1(pw) \bmod p$ instead of $\overline{Z} = g^z \cdot g^{h_1(pw)} \bmod p$.
- In the step 5) of Chien et al.'s protocol, C computes $Z = \frac{\overline{Z}}{h_1(pw)} \bmod p$ instead of $Z = \frac{\overline{Z}}{g^{h_1(pw)}} \bmod p$.

In the following, we show the modification could withstand the off-line password guessing attack described in the above section.

1) Upon receiving the request message $Msg_1 = \{sid, ID_C\}$ sent by C, G generates two random numbers $y, z \in Z_q^*$ and computes $Y = g^y \bmod p$, $\overline{Z} = g^z \bmod p$. Then, G sends the message $Msg_4 = \{sid, ID_C, ID_G, Z, Y\}$ to C.

2) Upon receiving Msg_4, C generates a random number $x \in Z_q^*$, computes $Z = \frac{\overline{Z}}{h_1(pw)} \bmod p$, $X = g^x \bmod p$, $sk_{CS} = h_1(sid \| ID_C \| ID_S \| X \| Z \| Z^x)$, $sk_{CG} = h_1(sid \| ID_C \| ID_G \| X \| Y \| Y^x)$, $sk''_{CG} = h_2(sid \| ID_C \| ID_G \| X \| Y \| Y^x)$, $M_1 = h_1(sid \| ID_C \| ID_S \| X \| Z \| Z^x \| sk_{CS})$ and $M_2 = h_1(sid \| ID_C \| ID_G \| X \| Y \| Y^x \| sk_{CG})$. At last, C sends $Msg_5 = \{sid, X, M_1, M_2\}$ to G.

G could guess a password pw^* and computes $Z^* = \frac{\overline{Z}}{h_1(pw^*)} \bmod p$. However, G could not compute $(Z^x)^* = \left(\frac{\overline{Z}}{h_1(pw^*)}\right)^x \bmod p = \frac{X^z}{\left(h_1(pw^*)\right)^x}$ since he has to compute $\left(h_1(pw^*)\right)^x$ from $X = g^x$ and $h_1(pw^*)$ and will face with the computational Diffie-Hellman problem. So G could not verify the correctness of pw^*. Thus, our countermeasure could withstand the attack described in the above section.

V. CONCLUSIONS

In the letter, we demonstrated that the Chien et al.'s GPAKE protocl is susceptible to an off-line password guessing attack. We also presented a countermeasure to withstand the attack.

[1] M. Abdalla, O. Chevassut, P. A. Fouque, and D. Pointcheval, "A simple threshold authenticated key exchange from short secrets," ASIACRYPT 2005, LNCS 3788, 2005, pp. 566-584.

[2] J. W. Byun, D. H. Lee, and J. I. Lim, "Security analysis and improvement of a gateway-oriented password-based authenticated key exchange protocol," IEEE Communication Letters, Vol. 10, No. 9, 2006, pp. 683-685.

[3] T. C. Wu and H. Y. Chien, "Comments on Gateway-Oriented Password-Based Authenticated Key Exchange Protocol," Proc. of the Fifth International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIHMSP09), 2009, pp.262-265.

[4] M. Abdalla, M. Izabach`ene, and D. Pointcheval, "Anonymous and Transparent Gateway-based Password-Authenticated Key Exchange," Proc. of CANS '08, LNCS 5339, Springer, 2008, pp. 133–148.

[5] H. Y. Chien, T. C. Wu, M. K. Yeh, "Provably Secure Gateway-Oriented Password-Based Authenticated Key Exchange Protocol Resistant to Password Guessing Attacks," Journal of Information Science and Engineering, http://www.iis.sinica.edu.tw/page/jise/FILE/acceptedpaper.html (In Press).

[6] T. Xiang, K. Wong, X. Liao, "Cryptanalysis of a password authentication scheme over insecure networks," Journal of Computer and System Sciences, Vol. 74, No. 5, 2008, pp. 657–661.

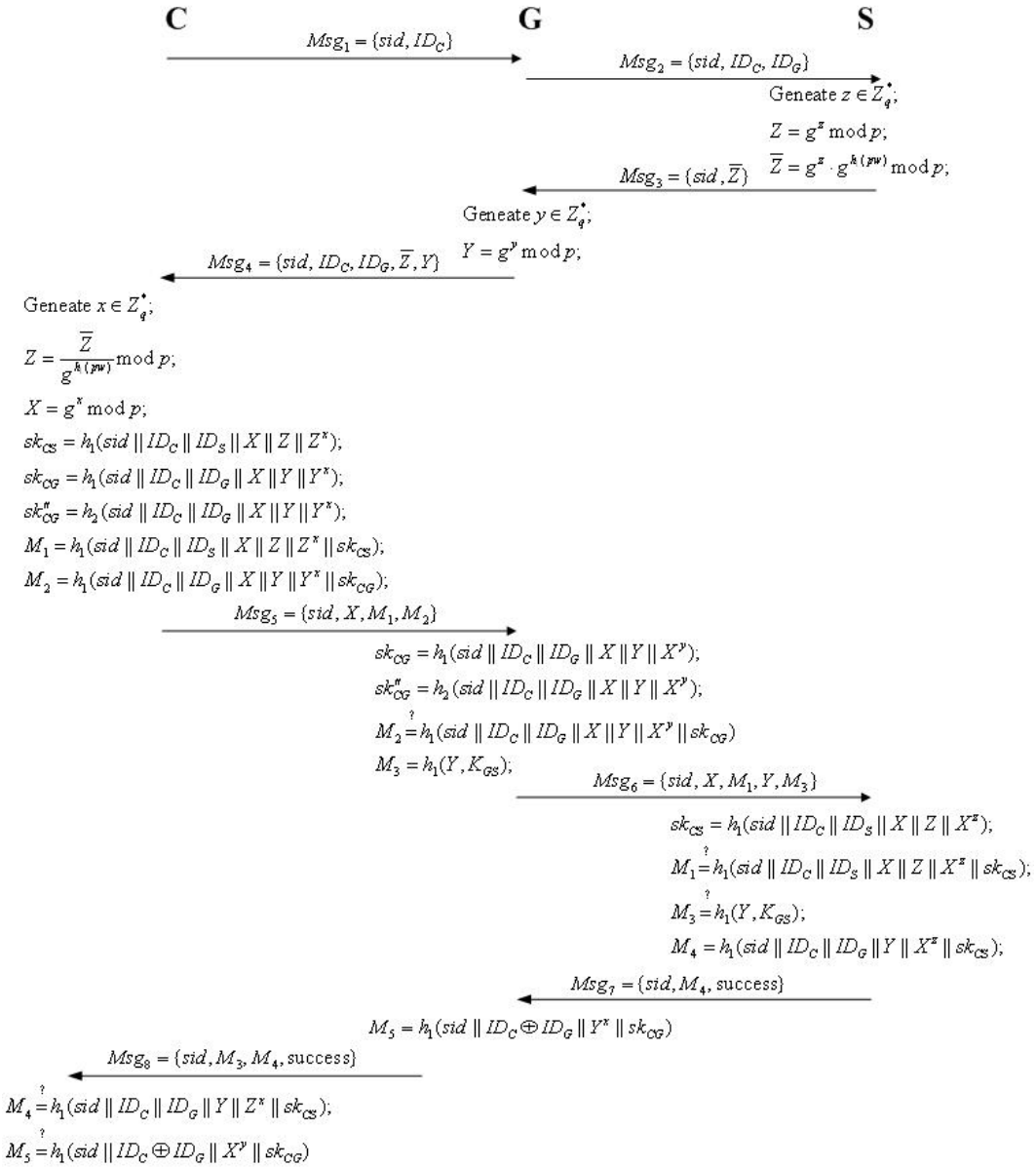

Fig. 1.Chien et al.'s protocol