Cryptanalysis on Chang-Yang-Hwang Protected Password Change Protocol

Chih-I Wang, Chun-I Fan, and D. J. Guan

Recently, Chang et al. proposed an authenticated key agreement and protected password change scheme. They claimed that their scheme is simple and efficient. However, in this letter we point out that their protected password change protocol is insecure under the denial-of-service attack and the dictionary attack in some situations.

Keywords: Authentication, Passwords, Information security, Cryptography.

1 Introduction: Ubiquitous communication networks connect lots of distributed entities together such that they can exchange and share large amounts of information and resources. In order to guarantee security, it is necessary for any two distributed entities to mutually verify the identity of each other before they set up a new connection. User authentication is one of the most important security

issues in secure communications. Password-based mechanism is a widely used method for user authentication since it allows people to choose and remember their own passwords without any additional devices, such as smart cards.

After two entities have finished the authentication process, a session key is usually established to provide confidentiality of the communication between them over an open network. Diffie-Hellman scheme is a famous key agreement scheme that can help two entities establish a session key over an insecure network [1]. However, the scheme is vulnerable to the man-in-the-middle attack because the adversary can impersonate anyone of the two communication entities. In 1999, Seo and Sweeney proposed a simple authenticated key agreement protocol [2]. Through a shared password in advance, two entities can authenticate each other and establish a session key. Yeh et al. proposed another protocol that can resist the password guessing attack (or the dictionary attack) [3]. Recently, Chang et al. modified Yeh et al.'s scheme to improve the efficiency and also presented a new protected password change protocol [4]. However, in this letter we will show that their protected password change protocol is not secure under the denial-of-service attack and the dictionary attack in some situations.

The remainder of this letter is organized as follows. In Section 2, we briefly review Chang et al.'s scheme. Our cryptanalysis on their protected password change protocol is presented in Section 3. Finally, a concluding remark is given in Section 4.

2 Description of Chang et al.'s protected password change protocol: In this section, we describe Chang et al.'s protected password change protocol [4]. Firstly, the system publishes two large prime numbers p and q such that q divides $p-1$. Let g be a generator with order q in the Galois field $GF(p)$. Assume that Alice decides to change her password p_w shared by Bob to a new password p'_w. She needs to perform the following procedure with Bob.

Step 1. Alice$\longrightarrow$Bob: $(R_A \oplus p_w) \parallel (R_A \oplus p'_w)$.

Alice randomly chooses a number $a \in [1, q-1]$. She computes $R_A = g^a \bmod p$ and then sends $(R_A \oplus p_w) \parallel (R_A \oplus p'_w)$ to Bob where $\oplus$ is the exclusive-or operator and $\parallel$ is the concatenation operator.

Step 2. Bob$\longrightarrow$Alice: $R_B \parallel H(K_B, R_A)$.

After receiving $(R_A \oplus p_w) \parallel (R_A \oplus p'_w)$, Bob recovers R_A by computing $(R_A \oplus p_w) \oplus p_w$ and uses the recovered R_A to derive p'_w by computing $(R_A \oplus p'_w) \oplus R_A$. Then Bob chooses a number $b \in [1, q-1]$ at random. He computes $R_B = g^b \bmod p$ and $K_B = R_A^b \bmod p$, which is equal to $g^{ab} \bmod p$, and sends $R_B \parallel H(K_B, R_A)$ to Alice where H is a public one-way hash function.

Step 3. Alice$\longrightarrow$Bob: $H(K_A, R_B) \oplus p'_w$.

After receiving $R_B \parallel H(K_B, R_A)$, Alice computes $K_A = R_B^a \bmod p$, which is $g^{ab} \bmod p$, and verifies whether the received $H(K_B, R_A)$ is

equal to $H(K_A, R_A)$ or not. If it holds, Alice computes $H(K_A, R_B) \oplus p'_w$ and sends it to Bob.

After receiving $H(K_A, R_B) \oplus p'_w$, Bob uses the recovered p'_w in Step 2 to derive $H(K_A, R_B)$ by computing $(H(K_A, R_B) \oplus p'_w) \oplus p'_w$. Then he verifies whether the recovered $H(K_A, R_B)$ is equal to $H(K_B, R_B)$ or not. If it is equal, Alice and Bob have successfully changed their shared password p_w to the new password p'_w.

3 Cryptanalysis of Chang et al.'s protected password change protocol: In this section, we show two attacks on Chang et al.'s protected password change protocol. The details are described as follows.

3.1 The dictionary attack: In order to remember the passwords easily, users usually let their passwords contain some certain redundancy. Hence, if attackers can obtain an equation containing passwords and some other parameters where only the values of the passwords are unknown, the attackers can find the correct passwords by repeated choosing passwords in a password dictionary and testing if they are correct through the equation. This is referred to as the dictionary attack.

In Chang et al.'s protected password change protocol, the attackers can intercept $(R_A \oplus p_w) \parallel (R_A \oplus p'_w)$ in Step 1 and then computes $Y = (R_A \oplus p_w) \oplus (R_A \oplus p'_w)$ to obtain the equation $Y = p_w \oplus p'_w$ where only the values of p_w

and p'_w are unknown to the attackers. If Alice does not choose (p_w, p'_w) well such that only one or few password pairs satisfy the equation $Y = p_w \oplus p'_w$, then the attackers can guess the correct pair with non-negligible probability by performing the dictionary attack in $O(T^2)$ time where T is the number of words (or passwords) in the dictionary.

3.2 The denial-of-service attack: Another attack on Chang et al.'s protected password change protocol is the denial-of-service attack. The attackers replace $(R_A \oplus p_w) \parallel (R_A \oplus p'_w)$ transmitted in Step 1 with $(R_A \oplus p_w) \parallel (R_A \oplus p'_w \oplus k)$, where k is a number randomly chosen by the attackers. They then replace $H(K_A, R_B) \oplus p'_w$ transmitted in Step 3 with $H(K_A, R_B) \oplus p'_w \oplus k$.

Thus, from Bob's point of view, Alice's new password is $(p'_w \oplus k)$, but the new password kept by Alice is p'_w. It turns out that the shared password between Alice and Bob is inconsistent.

4 Conclusions: In this letter, we have shown that Chang et al.'s protected password change protocol is insecure under the denial-of-service attack. It is also vulnerable to the dictionary attack if the passwords are not chosen well.

References

[1] Diffie, W., and Hellman, M.E. : 'New directions in cryptography', *IEEE Transactions on Information Theory*, Nov. 1976, IT–22, pp. 644–654

[2] Seo, D., and Sweeney, P. : 'Simple authenticated key agreement algorithm', *Electronics Letters*, 1999, 38, (13), pp. 1073–1074

[3] Yeh, H.T., and Sun, H.M. : 'Simple authenticated key agreement protocol resistant to password guessing attacks', *ACM SIGOPS Operating Systems Review*, 2002, 36, (4), pp. 14–22

[4] Chang, T.Y., Yang, W.P., and Hwang, M.S. : 'Simple authenticated key agreement and protected password change protocol', *An international journal computers & mathematics with applications*, May 2005, Vol. 49, pp. 703–714

Authors' affiliations:

Chih-I Wang, Chun-I Fan, D. J. Guan (Department of Computer Science and Engineering, National Sun Yat-sen University, Kaohsiung, Taiwan 80424, ROC) ({cifan,guan}@cse.nsysu.edu.tw)