Weakness of a three-party password-based authenticated key exchange protocol

S. Wu

***Abstract*—To guarantee the quality of the growing popular communication services, quite recently, Huang presented a simple and efficient three-party password-based authenticated key exchange protocol in International Journal of Communications and Systems. In this letter, we first show her protocol is still vulnerable to a partition attack (offline dictionary attack), by which the adversary can easily determine the correct password.**

***Index Terms*—password-based; authenticated key exchange; three-party; dictionary attack.**

I. Introduction

The password-based authenticated key exchange(PAKE) is a protocol which allows two communicating parties to prove to one another that they know the passwords (that is, password-based authentication), and to generate a fresh symmetric key securely such that it is known only to these parties (that is, key agreement). The intrinsic problem with password-based protocols is that the memorable password, associated with each user, has low entropy, so that it is not easy to protect the password information against dictionary attacks—the notorious password guessing attacks by which attackers could search the relatively small space of human-memorable passwords.

The first PAKE protocol, know as Encrypted Key Exchange (EKE), which was suggested by Bellovin and Merritt [1]. Subsequently, many other two-party PAKE protocols have been proposed(e.g. [2], [3], [4], [5], [6]). Because two-party PAKE protocols are only suitable for the client-server architecture, many researchers have recently begun to study the three-party PAKE (3PAKE) protocols(e.g. [7], [8], [9], [10], [11], [12], [13], [14]), in which a trusted server(TS) exists to mediate between two communication parties to allow mutual authentication and each user only needs to share one password with the common server. However, not all of the cna simultaneously achieve security and efficiency.

To guarantee the quality of the growing popular communication services, it is urgent to construct low-computation and communication for three-party key exchange protocol, two remote users and a TS. Most recently, to the best of our knowledge, Huang [15] proposed a simple three-party password-based key exchange (3PAKE) protocol, which is more efficient than previously proposed schemes. She claimed that her protocol could resist against various dictionary attacks and was suitable for some practical scenarios. Unfortunately, we find that some security weaknesses still remain in her protocol. In this letter, we show her protocol is still vulnerable to a partition attack (offline dictionary attack), by which the adversary can easily determine the correct password. As a result, the authentication mechanism of the protocol is completely compromised because the adversary can impersonate that user with the knowledge of its password.

S. Wu is with the Department of Computer Science, Information Science Institute, China, e-mail: pqywsh@gmail.com.

Manuscript received Aug. 26, 2009.

II. Review of Huang's protocol

This section describes the 3PAKE protocol proposed by Huang [15], starting with some notations.

A. Notations

The notations used in their protocol are described as in the following:

- A, B: two identity of clients (users).
- TS: a TS (remote server).
- pw_A(pw_B): the password shared between user A(resp. B) and TS.
- p: a large prime number such that $p-1$ has a large prime factor q ($q \geq 2^{256}$).
- g: a generator with order q in $GF(p)$.
- G: the cyclic group generated by g;
- $\oplus$: an exclusive-or operator.
- $h()$: a public one-way hash function.

B. Protocol description

There are three entities involved in the protocol: the authentication server TS, and two users A(initiator) and B(responder) who wish to establish a session key between them. Each user's password is assumed to be shared with the server TS via a secure channel. As illustrated on Fig. 1, A and B authenticate each other with TS's help, then A and B can share a common session key K. The details will be described in the following steps. Here, we just follows the description in [15].

Step 1.User A chooses a random number x and computes $R_A = (g^x \mod p) \oplus h(pw_A, A, B)$, then sends (A, R_A) to user B.

Step 2.User B also selects a random number y and computes $R_B = (g^y \mod p) \oplus h(pw_B, A, B)$, then forwards (A, R_A, B, R_B) to TS.

Step 3.Upon receiving (A, R_A, B, R_B), the TS first uses pw_A and pw_B to compute $g^x = R_A \oplus h(pw_A, A, B)$ and $g^y = R_B \oplus h(pw_B, A, B)$, respectively. Then, TS chooses another random number z and computes $a = g^{xz} \mod p, b = g^{yz} \mod p$. Finally, TS send (Z_A, Z_B) to user B, where $Z_A = b \oplus h(pw_A, g^x)$ and $Z_B = a \oplus h(pw_B, g^y)$.

User A	User B	Trusted server TS
pw_A	pw_B	
$x \in Z_q^*$	$y \in Z_q^*$	$z \in Z_q^*$
1. $R_A = g^x \oplus h(pw_A, A, B)$ $\xrightarrow{A, R_A}$		
	2. $R_B = g^y \oplus h(pw_B, A, B)$ $\xrightarrow{A, R_A, B, R_B}$	
		3. $g^x = R_A \oplus h(pw_A, A, B)$ $g^y = R_B \oplus h(pw_B, A, B)$ $a = g^{xz}, b = g^{yz}$ $Z_A = b \oplus h(pw_A, g^x)$ $Z_B = a \oplus h(pw_B, g^y)$ $\xleftarrow{Z_A, Z_B}$
	4. $a = Z_B \oplus h(pw_B, g^y)$ $K = a^y = g^{xyz}$ $S_B = h(K, B)$ $\xleftarrow{Z_A, S_B}$	
5. $b = Z_A \oplus h(pw_A, g^x)$ $K = b^x = g^{xyz}$ verify: $S_B = h(K, B)$ $S_A = h(K, A)$ $\xrightarrow{S_A}$		
	check : $S_A = h(K, A)$	

Fig. 1. Huang's protocol.

Step 4.When B receives (Z_A, Z_B), it uses its password pw_B and g^y to obtain $a = Z_B \oplus h(pw_B, g^y)$, and uses the random number y to compute the common session key $K = a^y = (g^{xz})^y = g^{xyz} \mod p$ and $S_B = h(K, B)$. Next, user B forwards (Z_A, S_B) to user A.

Step 5.After receiving (Z_A, S_B), user A also uses its password pw_A and g^x to derive $b = Z_A \oplus h(pw_A, g^x)$, and uses the random number x to obtain the common key $K = b^x = (g^{yz})^x = g^{xyz} \mod p$. Then, A checks whether $S_B = h(K, B)$ holds or not. If it does not hold, A terminates the protocol. Otherwise, A is convinced that $K = g^{xyz}$ is a valid session key. Then, A computes $S_A = h(K, A)$ and sends it to user B.

Step 6.Upon receiving S_A, user B verifies whether $S_A = h(K, A)$ holds or not. If it does not hold, B terminates the protocol. Otherwise, K is a valid session key. Both the users A and B can use this session key K for secure communication. Here, K is only used for one session.

III. Weaknesses of Huang's protocol.

In this section, we demonstrate the adversary can guess correct password off-line by performing a partition attack on Huang's protocol[15]. In her scheme, the adversary just needs to wiretap a valid session and he is able to use the gathered information to partition the password space (the dictionary) into feasible and infeasible passwords. Finally the correct password will be recovered after a number of valid sessions have been observed from the intersection of the feasible partition of the passwords for each session.

In Huang's protocol[15], the value g is not a generator of $GF(p)$ but only a generator of a subgroup G of order q over $GF(p)$, which opens door to a partition attack. An adversary can mount such an attack as follows. Firstly, the adversary obtains R_A and Z_A by wiretapping an exchange between A and B, where $R_A = (g^x \mod p) \oplus h(pw_A, A, B)$ and $Z_A = b \oplus h(pw_A, g^x)$. Next, the adversary guesses a password pw_A^* and then uses it to compute $\alpha = R_A \oplus h(pw_A^*, A, B)$ and $\beta = Z_A \oplus h(pw_A^*, \alpha)$. If the guessed password pw_A^* is A's correct password, both α and β will be in G. If pw_A^* is not A's correct password, it is likely that the computation will result in either a value α or a value β which is not in G, including those values equal to or larger than p. For such a value in $GF(p)$, the attacker can check whether it is in the subgroup G, by raising it to the power q and checking whether 1 is obtained. Thus it can be seen that the probability that 1 is obtained, for an incorrect password, is $\frac{q}{p+c} < \frac{q}{p-1} \leq \frac{1}{2}$, where c the number of possible values not in $GF(p)$(i.e. equal to or larger than p). We say pw_A^* is a feasible password only when $\alpha < p, \beta < p$, $\alpha^q \mod p = 1$ and $\beta^q \mod p = 1$. Otherwise it is marked as an infeasible password. Thus the possible space of valid passwords is reduced by a factor of $(\frac{q}{p+c})^2 \leq \frac{1}{4}$, on average, by observing one exchange session. Over a number of sessions the space of valid passwords will be narrowed down to a single password at a logarithmic rate. Let $\mathcal{D}$ be a set of passwords. Hence, after test over n_t sessions, $(\frac{q}{p+c})^{2n_t}|\mathcal{D}|$ passwords are remained. Let n_m be an integer such that $(\frac{q}{p+c})^{2n_m}|\mathcal{D}| \approx 1$. Then, we can determine the correct password by testing $n_m = \frac{\log_2 |\mathcal{D}|}{2\log_2(\frac{p+c}{q})} \leq \frac{\log_2 |\mathcal{D}|}{2}$ sessions. The size of dictionary is 2^{40} (or 2^{50}) in practice. Therefore, we can determine the correct password by performing the above procedure 20 (or 25) times.

Obviously, the above attack shows that Huang's scheme cannot resist off-line dictionary attacks. Similar partition attacks are possible if the value of p is not chosen carefully so that c/p is significant. In this case, if trial computation α or β with candidate passwords leads to values equal to or larger than p, then these candidate passwords may be eliminated.

To avoid the attack, it is suggested that g has to be a generator of $GF(p)$ and p is chosen carefully so that c/p is almost negligible. As a result, the attacker can not distinguish feasible and infeasible passwords by testing for subgroup membership any more. In this case, however, TS can not detect any malicious trial either. And the attacker can mount an undetectable on-line dictionary attack easily, by which an adversary is able to legally gain information about the password by repeatedly and indiscernibly asking queries to the authentication server. Until now, undetectable on-line dictionary attacks have been widely studied, and examples of undetectable on-line dictionary attacks are referred to some previous works [16], [17], [18], [19].

IV. Conclusion

In this letter, we have demonstrated that Huang's three-party password-based authenticated protocol is still vulnerable to a partition attack (offline dictionary attack). Through our attack, the adversary can easily determine the correct password. With the knowledge of its password, the adversary can impersonate that user. Therefore, the protocol is completely insecure.

References

[1] S. M. Bellovin and M. Merritt. Encrypted key exchange: Password-based protocols secure against dictionary attacks. *Proc. 1992 IEEE Symposium on Security and Privacy*, pp. 72-84. IEEE Computer Society Press, May 1992.

[2] K. Kobara and H. Imai. Pretty-simple password-authenticated key-exchange under standard assumptions. *IEICE Transactions*, E85-A(10):2229-2237, Oct. 2002. Also available at http://eprint.iacr.org/2003/038/.

[3] Bellare M, Pointcheval D, Rogaway P. Authenticated key exchange secure against dictionary attacks. Proceedings of the 2000 Advances in Cryptology (EUROCRYPT'2000). Berlin, Germany:Springer-Verlag, 2000: 139-155.

[4] E. Bresson, O. Chevassut, and D. Pointcheval. New security results on encrypted key exchange. *Proc. PKC 2004*, LNCS 2947, pp. 145-158. Springer-Verlag, Mar. 2004.

[5] M. Abdalla and D. Pointcheval. Simple Password-Based Encrypted Key Exchange Protocols. *Proc. of Topics in Cryptology - CT-RSA 2005*, LNCS 3376, pp. 191-208, Springer-Verlag.

[6] M. Abdalla, O. Chevassut, and D. Pointcheval. One-time verifier-based encrypted key exchange. *Proc. of PKC '05*, LNCS 3386, pp. 47–64. Springer-Verlag, 2005.

[7] C.L. Lin, H.M. Sun, M. Steiner, T. Hwang. Three-party encrypted key exchange without server's public keys. *IEEE Communications Letters*,5(12):497-499, 2001.

[8] Bresson E, Chevassut O, Pointcheval D. New security results on encrypted key exchange. Proceedings of the 7th International Workshop on Theory and Practice in Public Key Cryptography (PKC'2004),Singapore, 2004. Berlin, Germany: Springer-Verlag, 2004: 145-158.

[9] S.W. Lee, H.S. Kim, K.Y. Yoo . Efficient verifier-based key agreement for three parties without server's public key. *Applied Mathematics and Computation*, 167(2):996-1003, 2005.

[10] T.F. Lee , T. Hwang, C.L. Lin . Enhanced three-party encrypted key exchange without server's public keys. *Computers and Security*, 23(7):571-577, 2004.

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

[12] Abdalla M, Fouque P-A, Pointcheval D. Password-based authenticated key exchange in the three-party setting. Proceedings of the 8th International Workshop on Theory and Practice in Public Key Cryptography (PKC'2005). Berlin, Germany: Springer-Verlag, 2005:65-84. Full version appeared in IEE Information Security, Volume 153, Issue 1, pp. 27–39, March 2006.

[13] Abdalla M, Pointcheval D. Interactive Diffie-Hellman Assumptions with Applications to Password-based Authentication. Proceedings of the 9th International Conference on Financial Cryptography (FC'2005), Roseau, Dominica, 2005. Berlin, Germany: Springer-Verlag, 2005:341-356.

[14] R. Lu, Z. Cao. Simple three-party key exchange protocol. *Computers and Security*, 26:94-97, 2007.

[15] H.-F. Huang. A simple three-party password-based key exchange protocol. *International Journal of Communications and Systems*, John Wiley & Sons, 2009.

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

[17] H.-R. Chung, W.-C. Ku. Three weaknesses in a simple three-party key exchange protocol, Information Science, 2008, Vol. 178, pp. 220-229.

[18] C.-W. Phan Raphael, W.-C. Yau , Bok-Min G.. Cryptanalysis of simple three-party key exchange protocol (S-3PAKE), Information Science 2008, Vol. 178, pp. 2849-2856.

[19] H.-S. Kim, J.-Y. Choi. Enhanced password-based simple three-party key exchange protocol, Computers and Electrical Engineering (2009), Vol. 35, pp. 107-114.