International Mathematical Forum, 2, 2007, no. 11, 525 - 532

Cryptanalysis of Two Password-Authenticated Key Exchange Protocols between Clients with Different Passwords

Tianjie Cao and Yongping Zhang

School of Computer Science and Technology, China University of Mining and Technology, Xuzhou Jiangsu 221008, China
tjcao@cumt.edu.cn

Abstract

In large-scale client-client communication environments, Password-Authenticated Key Exchange (PAKE) based on trusted server is very convenient in key management. For enhancing the efficiency and preventing various attacks, Wang and Mo proposed a three-PAKE protocol, Yoon and Yoo proposed a C2C-PAKE protocol. However, in this paper, we show that the Wang-Mo protocol and the Yoon-Yoo protocol exist impersonation attack.

Keywords: Information security; password; authentication; cryptanalysis

1. Introduction

Password-Authenticated Key Exchange (PAKE) enables two communication entities to authenticate each other and establish a session key via easily memorable passwords. The first PAKE protocol was introduced by Bellovin and Merritt in 1992 [1] known as Encrypted Key Exchange (EKE).

Two-party password-based authenticated key exchange (two-PAKE) protocol is quite useful for client-server architectures. However, in large-scale client-client communication environments where a user wants to communicate with many other users, Two-PAKE protocol is very inconvenient in key management that the number of passwords that the user would need to remember. Gong, Lomas, Needham, and Saltzer [3] proposed a three-party password-based key transfer protocol using server's public key. Later, Steiner, Tsudik and Waider [7] proposed a three-party PAKE (three-PAKE) protocol between two clients without server's

public key. Recently, Lee et al. [5] proposed an efficient three-PAKE protocol. Wang and Mo [8] show that Lee et al.'s protocol is vulnerable to the impersonation attack. Wang and Mo also proposed an improved method to withstand this attack.

To provide a cross-realm authentication, where clients from one environment (realm) wish to communicate with clients from other realms, Byun et al.[2] presented a Client-to-Client Password-Authenticated Key Exchange (C2C-PAKE) protocol. Kim et al. [4] showed that the C2C-PAKE scheme is vulnerable to a Denning-Sacco-style attack where the attacker is an insider with knowledge of the password of a client in a different realm. Kim et al. also proposed an improved C2C-PAKE protocol. Recently, Yoon and Yoo [9] demonstrated that Kim et al.'s C2C-PAKE protocol is vulnerable to one-way man-in-the-middle attack and password-compromise impersonation attack. Yoon and Yoo also presented an enhancement to resolve these problems.

In this paper, we show that the Wang-Mo protocol and the Yoon-Yoo protocol exist impersonation attack.

2. Cryptanalysis of Wang and Mo's Three -PAKE Protocol

2.1 Review of the Wang-Mo Protocol

Wang and Mo show that once Alice's verifier has stolen by the attacker Eve, the attacker Eve can impersonate Bob to communicate with Alice in Lee et al.'s protocol. To withstand this attack, Wang and Mo proposed an improved protocol.

Let p and q be two large prime integers such that $q|p-1$ and g be a generator with order q in Z_p^*. pwa, pwb are Alice and Bob's passwords. H is a secure one-way hash function. Before the running of the protocol, Alice and Bob send their verifiers v_A and v_B to authentication server AS through a secure channel where $v_A = g^{H(A, S, pwa)}$ and $v_B = g^{H(B, S, pwb)}$. AS stores v_A and v_B in a password table. We omit 'mod p' from expressions for simplicity.

(1)Alice chooses $a \in_R Z_p^*$, and computes $X_A = g^a$. Then, she sends the identity A and g^a to Bob.

(2)Bob chooses $b \in_R Z_p^*$, and computes $X_B = g^b$. Then, he sends X_B and (A, X_A, B, X_B) to Alice and AS, respectively.

(3)After receiving the messages, AS retrieves v_A and v_B from password table. Then AS computes $X_{SA} = (v_A)^c \oplus v_A$ and $X_{SB} = (v_B)^d \oplus v_B$, where c and $d \in_R Z_p^*$. AS sends X_{SA} and X_{SB} to Alice and Bob respectively. Finally, AS computes $K_{SA} = (X_A)^c = g^{ac}$ and $K_{SB} = (X_B)^d = g^{bd}$.

(4)Alice computes $K_{AS} = (X_{SA} \oplus v_A)^{t_A^{-1}a} = g^{ac}$ and $v_{AS} = H(A, B, S, X_A, X_B, g^c, K_{AS})$. Alice sends v_{AS} to AS. Similarly, Bob computes $K_{BS} = (X_{SB} \oplus v_B)^{t_B^{-1}b} = g^{ad}$ and $v_{BS} = H(B, A, S, X_B, X_A, g^d, K_{BS})$. Bob sends v_{BS} to AS. Note that $t_A = H(A, S, pwa)$ and $t_B = H(B, S, pwb)$.

(5)AS verifies whether v_{AS} and v_{BS} are true or not. If they are true, AS sends v_{SA} and v_{SB} to Alice and Bob respectively, where $v_{SA} = H(S, A, B, X_A, X_B, K_{SA})$ and $v_{SB} = H(S, B, A, X_B, X_A, K_{SB})$.

(6)Alice and Bob verify whether v_{SA} and v_{SB} are true or not respectively. If they are true, Alice computes $K_{AB} = (X_B)^a = g^{ba}$ and Bob computes $K_{BA} = (X_A)^b = g^{ab}$. Finally, Alice and Bob negotiate a common session key $K = H(A, B, S, K_{AB}) = H(A, B, S, K_{BA})$. We use figure 1 to introduce Wang and Mo's protocol.

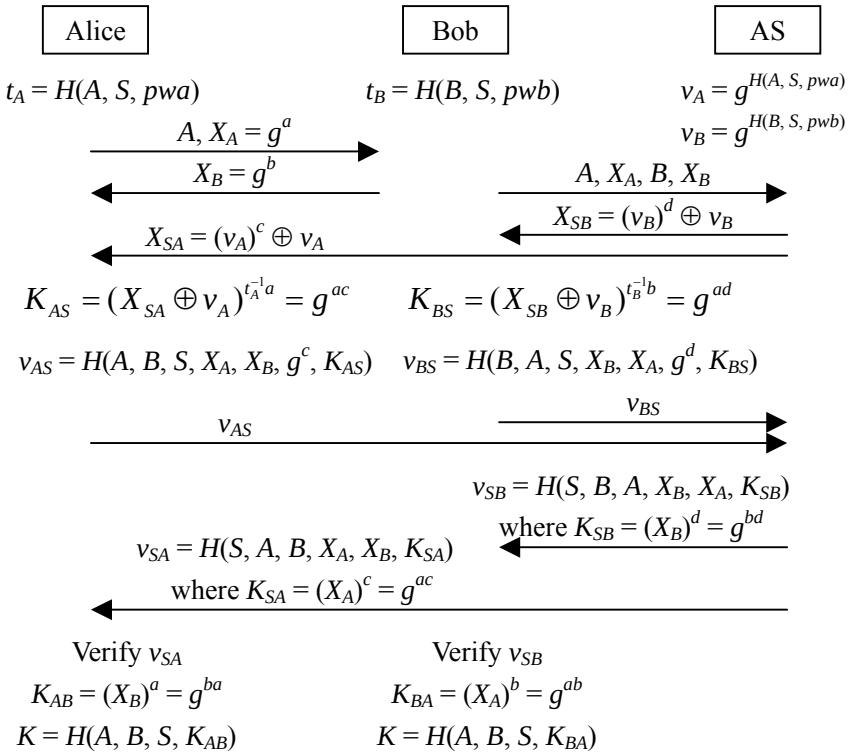

Fig.1 The Wang-Mo Protocol

2.2 Cryptanalysis

We show that the Wang-Mo Protocol exists the impersonation attack (see Figure 2). Once Alice's verifier v_A has stolen by the attacker. The attacker can impersonate Bob to communicate with Alice by performing the following steps.

(1)* When Alice wants to communicate with Bob. Alice sends the identity A and $X_A = g^a$ to Bob. Eve intercepts it.

(2)* Eve chooses a random number $b \in_R Z_p^*$ and sends $X_B = g^b$ to Alice.

(3)* Eve chooses a random number $c \in_R Z_p^*$ and sends $X_{SA} = (v_A)^c \oplus v_A$ to Alice.

(4)* Alice computes $K_{AS} = (X_{SA} \oplus v_A)^{t_A^{-1}a} = g^{ac}$ and $v_{AS} = H(A, B, S, X_A, X_B, g^c, K_{AS})$. Alice sends v_{AS} to AS. Eve intercepts it.

(5)* Eve sends $v_{SA} = H(S, A, B, X_A, X_B, K_{SA})$ to Alice, where. $K_{SA} = (X_A)^c = g^{ac}$.

(6)* Alice verifies v_{SA}. Alice computes $K_{AB} = (X_B)^a = g^{ba}$ and Eve computes $K_{BA} = (X_A)^b = g^{ab}$. In the end, Eve would successfully authenticate itself to Alice as Bob, and also share a secret session key $K = H(A, B, S, K_{AB}) = H(A, B, S, K_{BA})$ with Alice.

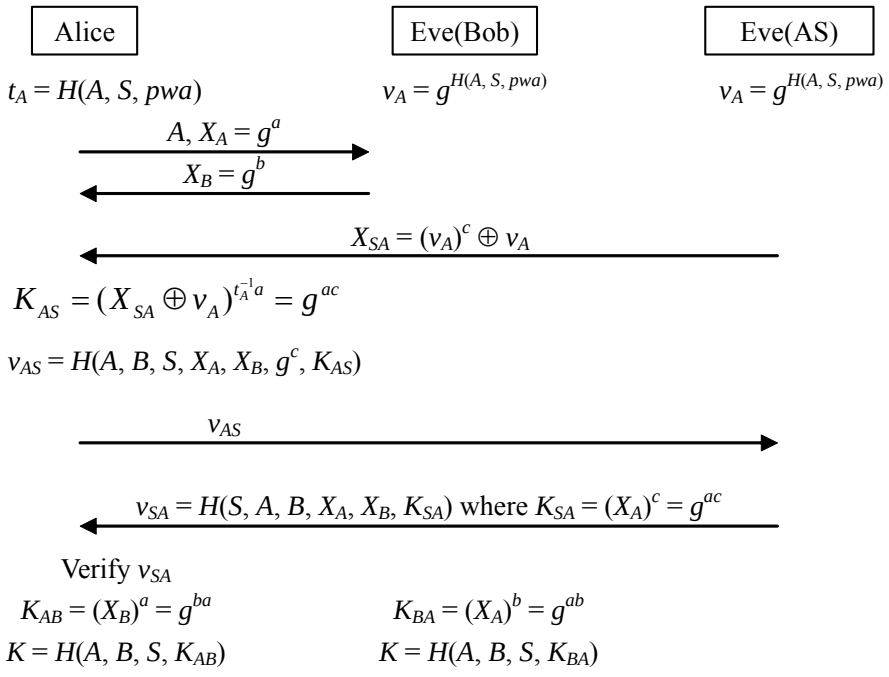

Fig.2 Impersonation attack in the Wang-Mo protocol

3. Cryptanalysis of Yoon and Yoo's C2C-PAKE Protocol

3.1 Review of the Yoon-Yoo Protocol

Yoon and Yoo [9] demonstrated that Kim et al.'s C2C-PAKE protocol [4] is vulnerable to one-way man-in-the-middle attack and password-compromise impersonation attack. They proposed an improved protocol (see Figure 3).

Let KDC_A, KDC_B are two key distribution centers which store A, pwa, B, pwb. E_X is a symmetric encryption with secret value X. K is the symmetric secret key shared between KDC_A and KDC_B. $Ticket_B$ is Kerberos ticket issued to Alice for service from Bob. L is a lifetime of TicketB.

The Yoon-Yoo's C2C-PAKE protocol involves the following steps.

(1) Alice chooses $x \in_R Z_p^*$, and computes g^x and $M_1 = E_{pwa}(g^x)$. Then, she sends M_1, A and B to KDC_A.

(2) KDC_A obtains g^x by decrypting $E_{pwa}(g^x)$. KDC_A chooses $r \in_R Z_p^*$, computes g^{xr} and $M_2 = E_{pwa}(g^r)$, and makes Kerberos ticket $Ticket_B = E_K(g^{xr}, g^r, A, B, L)$. Finally, KDC_A sends M_2, $Ticket_B$ and L to Alice.

(3) Upon receiving the message from KDC_A, Alice obtains g^r by decrypting M_2 and computes g^{xr}. Then, Alice stores g^{xr} and L, and forwards A and $Ticket_B$ to Bob.

(4) Bob chooses $y \in_R Z_p^*$ and computes $M_2 = E_{pwb}(g^y)$. Then, he sends A, B, M_2, and $Ticket_B$ to KDC_B.

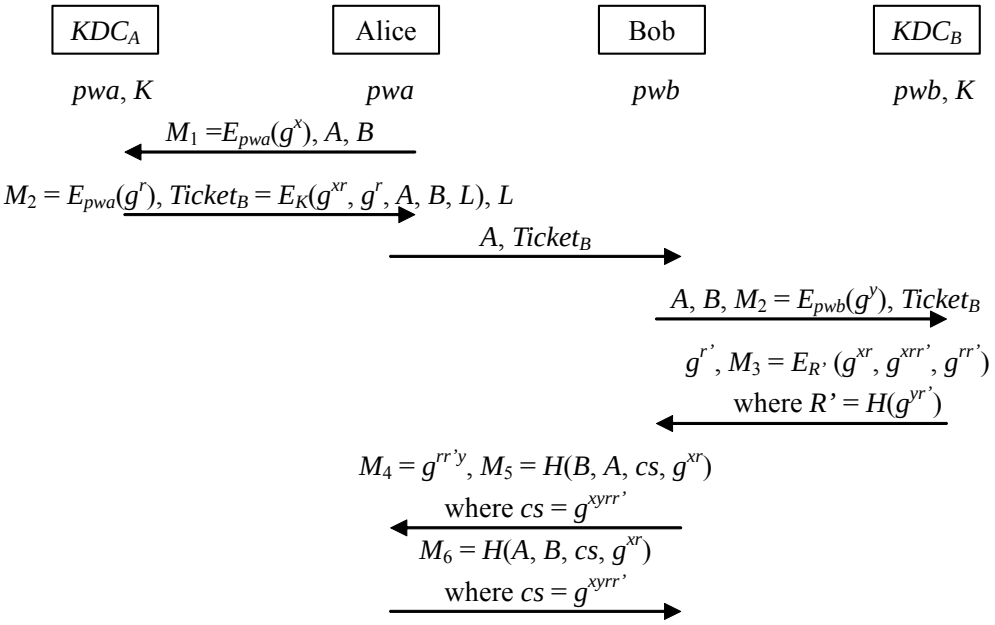

Fig.3 The Yoon-Yoo Protocol

(5) KDC_B obtains g^y, g^{xr} and g^r by decrypting M_2 and $Ticket_B$, respectively. Then, KDC_B chooses $r' \in_R Z_p^*$, computes $g^{r'}$, $g^{yr'}$, $g^{xrr'}$ and $g^{rr'}$, and makes $M_3 = E_{R'}(g^{xr}, g^{xrr'}, g^{rr'})$, where $R' = H(g^{yr'})$. Finally, KDC_B sends $g^{r'}$ and M_3 to Bob.

(6) Upon receiving the message from KDC_B, Bob computes $R' = H(^{gr'y})$, and obtains g^{xr}, $g^{xrr'}$ and $g^{rr'}$ by decrypting M_3. If it contains B, then Bob computes $cs = g^{xyrr'}$, $M_4 = g^{rr'y}$, and $M_5 = H(B, A, cs, g^{xr})$. Finally, Bob sends M_4 and M_5 to Alice for session key confirmation.

(7) After receiving M_4 and M_5, Alice computes $cs = g^{xyrr'}$. Then, Alice computes $H(B, A, cs, g^{xr})$ and verifies it with M_5. If it holds, Alice authenticates Bob. Finally, Alice computes $M_6 = H(A, B, cs, g^{xr})$, and sends it to Bob for session key confirmation.

(8) After receiving M_6, Bob computes $H(A, B, cs, g^{xr})$ and verifies it with M_6. If it holds, Bob authenticates Alice. After the Step 8, $SK = H(g^{xyrr'})$ is used as Alice and Bob's common secret session key.

3.2 Cryptanalysis

Suppose Alice's password is disclosed. Obviously, an adversary who knows this secret password can impersonate Alice to other entities. However, it is desired that this disclosure does not allow the adversary to impersonate other entities to Alice. We show the Yoon-Yoo protocol is also vulnerable to this impersonation attack (see Figure 4). The attack works as follows.

(1)* When Eve comprises pwa, she is able to get g^x form intercepted M_1.

(2)* Eve chooses r and $Ticket_B$, computes $M_2 = E_{pwa}(g^r)$. Eve sends M_2, $Ticket_B$ and L to Alice.

(3) * Alice obtains g^r by decrypting M_2 and computes g^{xr}. Then, Alice stores g^{xr} and L, and forwards A and $Ticket_B$ to Bob. Eve intercepts this message.

(4)* Eve chooses y, $r' \in_R Z_p^*$, and computes computes $cs = g^{xyrr'}$, $M_4 = g^{rr'y}$, and $M_5 = H(B, A, cs, g^{xr})$. Eve sends M_4 and M_5 to Alice for session key confirmation.

(5)* After receiving M_4 and M_5, Alice computes $cs = g^{xyrr'}$. Alice computes $H(B, A, cs, g^{xr})$ and verifies it with M_5. Alice computes $M_6 = H(A, B, cs, g^{xr})$, and sends it to Bob for session key confirmation. Eve intercepts this message.

(6)* After receiving M_6, Eve computes $SK = H(g^{xyrr'})$ and masquerade as Bob to complete the protocol. In the end, Eve would successfully authenticate itself to Alice as Bob, and also share a secret session key with Alice, but all the while Alice thinking it is sharing a key with Bob.

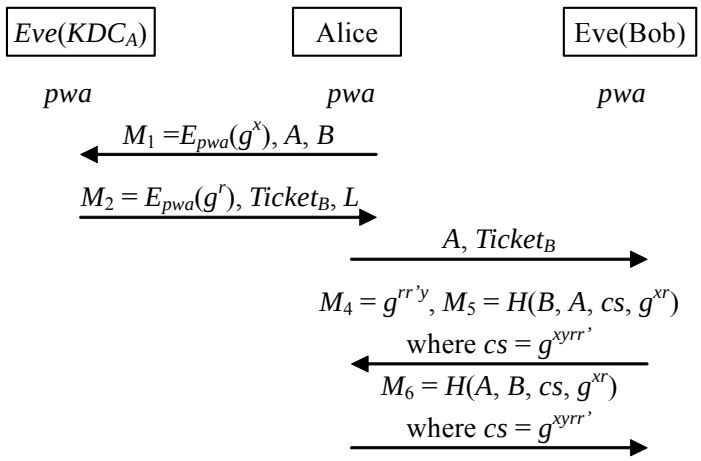

Fig.4 Impersonation attack in the Yoon-Yoo protocol

4. Conclusion

In this paper, we presented a cryptanalysis of two password-authenticated key exchange protocols newly published. Our results show that once Alice's verifier (or password) has stolen by the attacker, the attacker can impersonate another client to communicate with Alice.

Acknowledgments

This work was supported by the Science and Technology Foundation of CUMT and the Open Project of State Key Laboratory of Information Security.

References

[1] S. M. Bellovin and M. Merrit, Encrypted key exchange: password-based protocols secure against dictionary attacks, Proceedings of the IEEE Symposium on Research in Security and Privacy, (1992), 72-84.

[2] J.W. Byun, I.R. Jeong, D.H. Lee and C.S. Park. Password-Authenticated Key Exchange between Clients with Different Passwords. In Proceedings of ICICS 2002, LNCS 2513(2002), 134-146.

[3] L. Gong, M. Lomas, R. Needham and J. Saltzer, Protecting poorly chosen secrets from guessing attacks, IEEE Journal on Selected Areas in Communications, 11(5)(1993), 648-656.

[4] J. Kim, S. Kim, J. Kwak and D. Won, Cryptoanalysis and improvements of password authenticated key exchange scheme between clients with different passwords, In Proceedings of ICCSA 2004, LNCS3044(2004), 895-902.
[5] S.-W. Lee, H.-S. Kim and K.-Y. Yoo, Efficient verifier-based key agreement protocol for three parties without server's public key, Applied Mathematics and Computation, 167(2)(2005), 996-1003.
[6] R. C.-W. Phan and B. Goi, Cryptanalysis of an Improved Client-to-Client Password-Authenticated Key Exchange (C2C-PAKE) Scheme, In Proceedings of ACNS 2005, LNCS Vol. 3531(2005), 33-39.
[7] M. Steiner, G. Tsudik and M. Waidner, Refinement and extension of encrypted key exchange, ACM Operating Systems Review, 29 (3)(1995), 22-30.
[8] R-C Wang and K-R Mo, Security enhancement on efficient verifier-based key agreement protocol for three parties without server's public key, Int. Math. Forum, 1(17-20)(2006), 965 – 972.
[9] E.-J. Yoon and K.-Y. Yoo, A Secure Password-Authenticated Key Exchange Between Clients with Different Passwords, In Proceedings of APWeb Workshops 2006, LNCS 3842(2006), 659–663.

Received: June 17, 2006