Journal of Southeast University (English Edition) Vol. 24, No. 3, pp. 322 – 324 Sept. 2008 ISSN 1003—7985

Improved key exchange protocol for three-party based on verifier authentication

Liu Xiumei[1] Zhou Fucai[2] Chang Guiran[1]

([1] Computer Center, Northeastern University, Shenyang 110004, China)

([2] School of Information Science and Engineering, Northeastern University, Shenyang 110004, China)

Abstract: To prevent server compromise attack and password guessing attacks, an improved and efficient verifier-based key exchange protocol for three-party is proposed, which enables two clients to agree on a common session key with the help of the server. In this protocol, the client stores a plaintext version of the password, while the server stores a verifier for the password. And the protocol uses verifiers to authenticate between clients and the server. The security analysis and performance comparison of the proposed protocol shows that the protocol can resist many familiar attacks including password guessing attacks, server compromise attacks, man-in-the-middle attacks and Denning-Sacco attacks, and it is more efficient.

Key words: key exchange for three-party; password-based authentication; verifier

Most password-based authentication key exchange (PAKE) protocols[1-7] are based on easy-to-remember passwords for authentication, and they need to store client passwords to the host server. Sun et al. [8] pointed out that it would be more dangerous when the server was compromised, and they proposed a new verifier-based EKE protocol, which stored verifiers instead of passwords to the server and used the server's public key to improve security. However, Lee et al. [9] pointed out that a public key put a burden on the clients, and they also presented a verifier-based protocol, which had complicated formulae for encrypting codes and lower efficiency.

1 Review of Lee et al. 's Protocol

In Lee et al. 's protocol, the server stored the verifiers of clients. Fig. 1 shows the protocol. Notations used in the protocol are defined as follows:

- A, B, S are the identities of Alice, Bob, and AS, respectively;
- x_A, x_B are the passwords of A and B;
- t_A, t_B are the private keys of A and B, while $t_A = h(A, S, x_A)$ and $t_B = h(B, S, x_B)$;
- V_A, V_B are the verifiers of A and B, while $V_A = g^{t_A}$ and $V_B = g^{t_B}$;
- a, b, c, d are the random values chosen by Alice, Bob and AS, respectively.

Lee et al. 's protocol does not require the server's public key and can resist server compromise attacks. However, the protocol has complicated formulae for encrypting code, higher computational costs and lower efficiency.

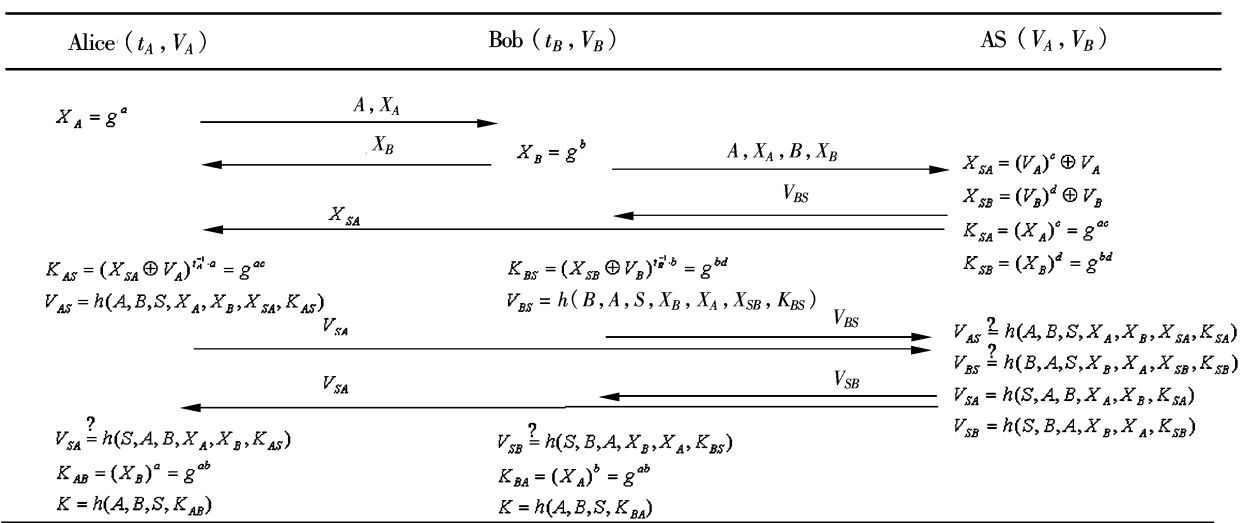

Fig. 1 Lee et al. 's three-party verifier-based key exchange protocol

Received 2008-04-15.

Biographies: Liu Xiumei (1976—), female, graduate; Chang Guiran (corresponding author), male, professor, chang@neu.edu.cn.

Foundation items: The National High Technology Research and Development Program of China (863 Program) (No. 2001AA115300), the Natural Science Foundation of Liaoning Province (No. 20031018, 20062023).

Citation: Liu Xiumei, Zhou Fucai, Chang Guiran. Improved key exchange protocol for three-party based on verifier authentication [J]. Journal of Southeast University (English Edition), 2008, 24(3): 322 – 324.

2 Improved Verifier-Based Key Exchange Protocol for Three-Party

Based on an overall consideration of security and efficiency, we present an improved and more efficient verifier-based key agreement protocol for three-party.

Before proceeding with this protocol, both Alice and Bob have to store their verifiers in the server AS for authentica-

tion. Alice and Bob respectively choose passwords pw_A and pw_B, compute the verifiers $V_A = g^{h(A, S, pw_A)}$ and $V_B = g^{h(B, S, pw_B)}$, and then send V_A and V_B to AS over a secure channel. The flows for the proposed protocol are depicted in Fig. 2. Parts of notations are defined as follows:

- t_A, t_B are the private keys of Alice and Bob generated respectively from their passwords, while $t_A = h(A, S, pw_A)$ and $t_B = h(B, S, pw_B)$;
- a, b, u are the random values chosen by clients and the server respectively;
- E_X is the symmetric encryption with X;
- sk_A, sk_B are the session keys generated by A and B respectively, while $sk_A = sk_B = g^{abu}$.

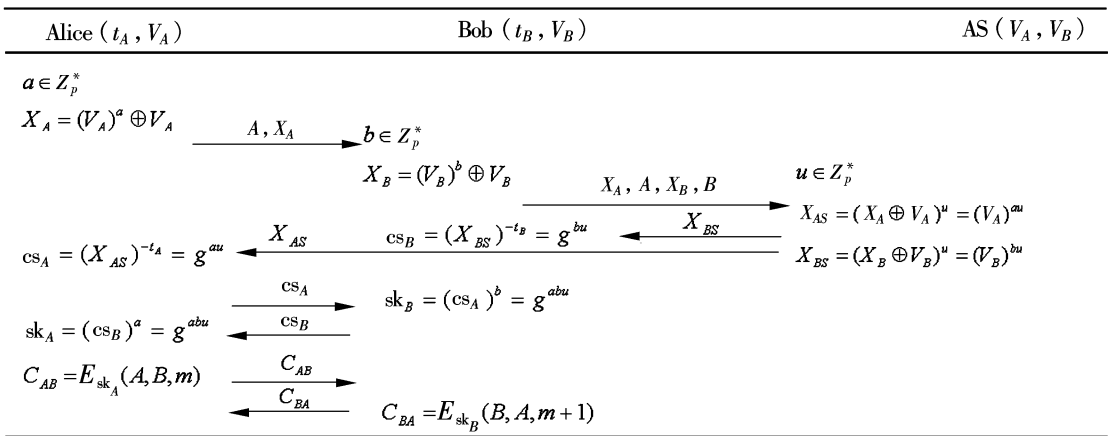

Fig. 2 Improved verifier-based key exchange protocol for three-party

We omit mod p for simplicity. The protocol proceeds as follows:

1) Alice chooses a random value $a \in Z_p^*$, computes and sends $X_A = (V_A)^a \oplus V_A$ to Bob with A.

2) Bob chooses a random value $b \in Z_p^*$, computes $X_B = (V_B)^b \oplus V_B$ and sends X_B and B to AS with the received messages.

3) AS obtains $(V_A)^a$ and $(V_B)^b$ by decrypting the message X_A and X_B with the stored verifiers V_A and V_B. Then AS chooses a random value $u \in Z_p^*$, and computes $X_{AS} = (X_A \oplus V_A)^u = (V_A)^{au}$ and $X_{BS} = (X_B \oplus V_B)^u = (V_B)^{bu}$. Finally, AS sends X_{AS} to Alice, and sends X_{BS} to Bob, respectively.

4) Alice computes and sends $cs_A = (X_{AS})^{-t_A} = g^{au}$ to Bob. Concurrently, Bob computes and sends $cs_B = (X_{BS})^{-t_B} = g^{bu}$ to Alice.

5) Upon the received message, Alice can compute the session key $sk_A = (cs_B)^a = g^{abu}$, then she computes and sends $C_{AB} = E_{sk_A}(A, B, m)$ to Bob.

6) Bob can also compute the session key $sk_B = (cs_A)^b = g^{abu}$ and reply the message $C_{BA} = E_{sk_B}(B, A, m+1)$ to Alice to validate the session key.

3 Security Analysis and Performance Comparison

3.1 Security analysis

Suppose that ε is an adversary, and the security properties of our protocol are based on DLP, DHP and the properties of a one-way Hash function.

1) Forward secrecy: If the passwords are leaked, ε still cannot compute the established session keys. Because a, b and u are ephemeral parameters.

2) Man-in-the-middle attack: Suppose that ε wants to impersonate B. ε uses a candidate pw'_B and computes V'_B. Then, ε chooses $b \in Z_p^*$, and computes and sends $X'_B = (V'_B)^b \oplus V'_B$ to S. S obtains $(V'_B)^{b'}$ by using the real V_B, computes and replies $X'_{BS} = (V'_B)^{b'u}$ to ε. And ε sends $cs'_B = g^{b'u}$ to A. Finally, $sk_A = g^{ab'u}$, and $sk_B = g^{abu}$ which is generated by ε. $sk_A \neq sk_B$, so ε cannot deceive A. In the case of impersonating A, the case is similar.

3) Denning-Sacco attack: In case of an outsider adversary, suppose that ε got sk, and intercepted all the transmitted messages. From the formulae in step 1) and step 2), we know that ε cannot obtain V_A or V_B; therefore ε cannot obtain pw_A or pw_B, unless ε knows a or b.

In case of an insider adversary with pw_A, ε can compute V_A and obtain$(V_A)^a$. However, ε cannot obtain$(V_B)^b$, therefore ε cannot obtain pw_B. In case of an insider adversary ε with pw_B, the case is similar.

4) Password guessing attack: Suppose that ε chooses a candidate pw'_A(or pw'_B) and tries to verify his guesses. However, ε has no way to verify his guesses since each party uses "$\oplus$" operation and ε cannot obtain a or b.

5) Server compromise attack: If AS is compromised, ε may know the clients' verifiers $V_A = g^{t_A}$ and $V_B = g^{t_B}$. However, ε cannot obtain $t_A = h(A, S, pw_A)$ and $t_B = h(B, S, pw_B)$ being used in step 4).

6) Replay attack: Because a, b, u are ephemeral parameters in a session, the probability of success with regard to a replay attack is trivially negligible.

3.2 Performance comparison

The computational costs of Lee et al.'s protocol and our improved protocol are summarized in Tab. 1. In comparison, our protocol is more efficient.

Tab. 1 Comparisons of computational costs

Factor	Lee's protocol			The proposed protocol		
	Alice	AS	Bob	Alice	AS	Bob
Exponentiation operation	3	4	3	2	2	2
Symmetric encrypt/decrypt	0	0	0	1	0	1
Hash function	4	4	4	1	0	1
Inverse operation	1	0	1	1	0	1
Numbers of exchange		9			8	

4 Conclusion

In most PAKE protocols for three-party, the protocols are vulnerable to password guessing attacks and server compromise attack. In this paper, we propose an improved and efficient verifier-based key exchange protocol for three-party. The security analysis and performance comparison of the proposed protocol shows that the protocol can resist many familiar attacks including password guessing attacks, server compromise attack, man-in-the-middle attack and Denning-Sacco attack, and it is more efficient.

References

[1] Bellovin S M, Merritt M. Encrypted key exchange: password-based protocols secure against dictionary attacks[C]//*IEEE Symposium on Security and Privacy*. New York: IEEE Press, 1992: 72 - 84.

[2] Jablon D. Strong password-only authenticated key exchange [J]. *Computer Communication Review*, 1996, **26**(5): 5 - 26.

[3] Lucks S. Open key exchange: how to defeat dictionary attacks without encrypting public keys[C]//*Proceedings of the Security Protocol Workshop*. Berlin: Springer-Verlag, 1997: 79 - 90.

[4] Abdalla Michel, Fouque Pierre-Alain, Pointcheval David. Password-based authenticated key exchange in the three-party setting[C]//*Lecture Notes in Computer Science*. Berlin: Springer-Verlag, 2005: 65 - 84.

[5] Bellovin S M, Merritt M. Augmented encrypted key exchange: a password-based protocol secure against dictionary attacks and password file compromise[R]. AT&T Bell Laboratories, 1994.

[6] Kwon T, Kang M, Jung S. An improvement of the password-based authentication protocol(K1P) on security against replay attacks[J]. *IEICE Transactions on Communications*, 1999, **E82-B**(7): 991 - 997.

[7] Jablon D. Extended password methods immune to dictionary attack[C]//*WETICE Enterprise Security Workshop*. Cambridge, MA, 1997: 248 - 255.

[8] Sun H M, Chen B C, Hwang T. Secure key agreement protocols for three-party against guessing attacks[J]. *The Journal of Systems and Software*, 2003, **75**(1/2): 63 - 68.

[9] Lee S W, Kim H S, Yoo K Y. Efficient verifier-based key agreement protocol for three parties without server's public key[J]. *Applied Mathematics and Computation*, 2005, **167**(1): 996 - 1003.

一种改进的基于验证值的三方密钥交换协议

柳秀梅[1] 周福才[2] 常桂然[1]

([1] 东北大学计算中心,沈阳 110004)

([2] 东北大学信息科学与工程学院,沈阳 110004)

摘要: 为防止服务器泄露攻击和口令猜测攻击,提出了一种基于验证值的三方密钥交换协议. 该协议用于实现2个客户通过与第三方服务器间的交互协商出会话密钥的过程. 协议中客户只需要记住自己的口令,而服务器端则存储与口令对应的验证值,客户与服务器之间的身份认证通过验证值来完成. 对协议的安全分析结果表明,该协议能抵御很多已知的攻击,包括服务器泄漏攻击、口令猜测攻击、中间人攻击以及 Denning-Sacco 攻击等. 对协议的效率评估表明该协议是高效的.

关键词: 三方密钥交换;基于口令认证;验证值

中图分类号: TN911. 22