# 新的口令认证密钥协商协议

谭示崇，张 宁，王育民

(西安电子科技大学综合业务网理论与关键技术国家重点实验室 西安 710071)

【摘要】针对服务器泄漏攻击，给出了抵抗这种攻击的方法，提出了一个新的基于口令的认证密钥协商协议。在该方案中，用户记住自己的口令，而服务器仅仅存储与口令对应的验证信息。分析结果表明，该方案可以抵抗服务器泄漏攻击、字典攻击和Denning-Sacco攻击等，并且具有前向安全性等性质。

**关 键 词** 字典攻击； 密钥协商； 口令认证； 服务器泄漏攻击

**中图分类号** TN911.22 **文献标识码** A

# A New Password-Based Authenticated Key Agreement Protocol

TAN Shi-chong，ZHANG Ning，WANG Yu-min

(State Key Lab. of Integrated Service Networks, Xidian University Xi'an 710071)

**Abstract** Attack, a method of resisting server compromise attack is given and a new password-based authenticated key agreement protocol is proposed. In this protocol, one side (the client) stores a plaintext version of the password, while the other side (the server) only stores a verifier for the password. The analysis of this new protocol shows that the protocol is secure against server compromise attack, dictionary attack,and the Denning-Sacco attack, and provides the property of the perfect forward secrecy.

**Key words** dictionary attack; key agreement; password authentication; server compromise attack

近年来，基于口令的认证密钥协商协议的设计和分析受到越来越多的关注。在认证和密钥协商协议中利用口令是很自然的，因为这些口令易于记忆。在实际中，基于口令的方案适合在许多环境中实现，特别是在一些缺乏设备来安全地存储随机的长期密钥的环境之中。但是，因为口令空间很小，很容易受到字典攻击或口令猜测攻击。文献[1]提出了第一个基于口令的认证密钥交换协议，即EKE协议；文献[2]提出了一个改进的协议。许多研究人员对基于口令的密钥协商协议也做了大量的研究，并取得了不少成果[3-9]。

本文提出一个改进的基于口令的认证密钥协商协议。

## 1 EPAKA协议

在文献[10]的基于口令的认证密钥协商协议(EPAKA协议)中，假设$A$、$B$为协议的两个诚实的执行者，其中$A$为用户，$B$为网络服务器；$H$ 是抗碰撞的单向杂凑函数；$\pi$ 是用户的口令；$V$ 为服务器保存的验证信息(verifier)，$V = g^v = g^{H(A,B,\pi)}$，$v = H(A,B,\pi)$，则EPAKA协议的执行过程如下：

(1) A选择 $a \in_R Z_p^*$，计算：

$$X_A = g^a \oplus V$$

然后将它的身份 $\mathrm{ID}_A$ 和 $X_A$ 发送给$B$。

(2) 在收到$A$发送的消息后，$B$从自己保存的口令文件中取出$A$的验证信息，选择 $b \in_R Z_p^*$，计算 $X_B = V^b \oplus V$，并将 $X_B$ 发送给$A$；然后进行$B$计算：

$$K_B = (X_A \oplus V)^b = g^{ab}$$
$$V_A' = H(A, X_B, K_B)$$
$$V_B = H(B, X_A, K_B)$$

(3) 收到$B$发送的 $X_B$ 后，进行$A$计算：

$$K_A = (X_B \oplus V)^{aH(A,B,\pi)^{-1}} = g^{ab}$$
$$V_A = H(A, X_B, K_A)$$

并且将 $V_A$ 发送给 $B$，然后计算：

$$V_B' = H(B, X_A, K_A)$$

(4) 收到$A$发送的 $V_A$ 后，$B$验证 $V_A = V_A'$。如果 $V_A = V_A'$，$B$确信 $K_A$ 得到了证实，然后将 $V_B$ 发送给$A$。

收稿日期：2006－11－16；修回日期：2007－04－20

基金项目：国家自然科学基金(60473027 )

作者简介：谭示崇(1979－)，男，博士生，主要从事密码协议的设计与分析等方面的研究.

(5) 收到$B$发送的$V_B$后，$A$验证$V_B=V_B'$，如果$V_B=V_B'$，$A$确信$K_B$得到证实。

(6) $A$和$B$计算共同的会话密钥：

$$K=H(K_A)=H(K_B)=H(g^{ab})$$

在EPAKA协议中，文献[10]称该协议能够抵抗服务器泄漏攻击，也就是说，攻击者即使能够窃取服务器上的口令文件，也不能直接利用该文件上的信息来直接冒充对应的用户。

## 2 对EPAKA协议的一种有效攻击

文献[11]提出了一个对EPAKA协议的有效攻击。攻击者可以对EPAKA协议实施服务器泄漏攻击(server compromise)。假设攻击者Eve已经获得了服务器$B$的口令文件，并从中取得了用户$A$的验证信息$V$，Eve的目标是向$B$冒充$A$。攻击过程如下：

(1) 攻击者Eve选择$a\in_R Z_p^*$，计算：

$$X_A=V^a\oplus V$$

然后，将$\mathrm{ID}_A$和$X_A$发送给$B$，企图向$B$冒充$A$。

(2) 收到Eve发送的消息后，$B$从自己保存的口令文件中取出$A$的验证信息，选择$b\in_R Z_p^*$，计算$X_B=V^b\oplus V$，并且将$X_B$发送给Eve，然后计算：

$$K_B=(X_A\oplus V)^b=(V^a\oplus V\oplus V)^b=V^{ab}$$

$$V_A'=H(A,X_B,K_B)$$

$$V_B=H(B,X_A,K_B)$$

(3) 收到$B$发送的$X_B$后，Eve计算：

$$K_A=(X_B\oplus V)^a=(V^b\oplus V\oplus V)^a=V^{ab}$$

$$V_A=H(A,X_B,K_A)$$

并且将$V_A$发送给$B$。然后Eve计算：

$$V_B'=H(B,X_A,K_A)$$

(4) 收到Eve发送的$V_A$后，$B$验证$V_A=V_A'$。因为$K_A=K_B$，所以$V_A=V_A'$，因此$B$就确信$K_A$得到了证实，然后将$V_B$发送给$A$，接着$B$就可以计算会话密钥：

$$K=H(K_B)=H(V^{ab})$$

(5) 收到$B$发送的$V_B$后，Eve验证$V_B=V_B'$。如果$V_B=V_B'$，那么Eve确信$K_B$得到了证实。显然，Eve成功地向$B$冒充了$A$，并且Eve能够计算共同的会话密钥：

$$K=H(K_A)=H(V^{ab})$$

上述攻击过程成功执行后，Eve和$B$都可以计算出共享的会话密钥，而服务器$B$则错误地认为它正与用户$A$共享该会话密钥。经过分析可以知道，EPAKA协议之所以不能抵抗服务器泄漏攻击，是因为在该协议中，攻击者可以首先计算$X_A$，从而将会话密钥限制为一个预定的形式，在此后的对话中，攻击者仅仅利用已经从服务器获得的验证信息$V$就可以计算相关的值，而并不需要知道该用户的口令$\pi$。

## 3 一个改进的基于口令的认证密钥协商协议

下面给出一个改进的基于口令的认证密钥协商(PAKA)协议。假设$H_0$、$H_1$、$H_2$、$H_3$是抗碰撞的单向杂凑函数；$k$是安全参数，则该协议执行过程如下：

用户$A$ 服务器$B$

$a\in_R Z_p^*$ $b\in_R Z_p^*$

$X_A=g^a\oplus V$ $\xrightarrow{ID_A,X_A}$ $\mu=g^b$，

$\sigma=(X_A\oplus V)^b$，

$c\in_R\{0,1\}^k$，

$d=g^{H_0(A,B,c)}$，

$k=c\oplus H_1(A,B,X_A,\mu,\sigma,d,V^{H_0(A,B,c)},V)$

$\xleftarrow{\mu,\ d,\ k}$

$\sigma=\mu^a$，

$c=k\oplus H_1(A,B,X_A,\mu,\sigma,d,d^v,V)$，

验证

$d=g^{H_0(A,B,c)}$，

$k'=H_2(A,B,X_A,\mu,\sigma,d,k,c,V)$，

$K=H_3(A,B,X_A,\mu,\sigma,c,V)$

$\xrightarrow{k'}$

验证

$k'=H_2(A,B,X_A,\mu,\sigma,d,k,c,V)$

$K=H_3(A,B,X_A,\mu,\sigma,c,V)$

(1) $A$选择$a\in_R Z_p^*$，计算$X_A=g^a\oplus V$，然后将他的身份$\mathrm{ID}_A$和$X_A$发送给$B$。

(2) 收到$A$发送的消息后，$B$从自己保存的口令文件中取出$A$的验证信息，选择$b\in_R Z_p^*$,计算$\mu=g^b$，$\sigma=(X_A\oplus V)^b$，选择$c\in_R\{0,1\}^k$，计算：

$$d=g^{H_0(A,B,c)}$$

$$k=c\oplus H_1(A,B,X_A,\mu,\sigma,d,V^{H_0(A,B,c)},V)$$

然后，$B$将$\mu,d$和$k$发送给$A$。

(3) 收到$B$发送的$\mu,d$和$k$后，$A$计算：

$$\sigma=\mu^a$$

$$c=k\oplus H_1(A,B,X_A,\mu,\sigma,d,d^v,V)$$

验证$d=g^{H_0(A,B,c)}$，如果该等式成立，则$A$继续计算：

$$k'=H_2\left(A,B,X_A,\mu,\sigma,d,k,c,V\right)$$

并且将$k'$发送给$B$。然后，$A$计算会话密钥：

$$K = H_3(A,B,X_A,\mu,\sigma,c,V)$$

(4) 收到$A$发送的$k'$后，$B$验证：

$$k' = H_2(A,B,X_A,\mu,\sigma,d,k,c,V)$$

如果该等式成立，那么服务器$B$确信它正在与用户$A$通信，并计算会话密钥：

$$K = H_3(A,B,X_A,\mu,\sigma,c,V)$$

# 4　安全性分析

## 4.1　PAKA协议提供了前向安全性

假设攻击者Eve获得了用户$A$的口令$\pi$，Eve能够获得$A$和$B$之间的消息包括：

$$X_A = g^a \oplus V$$

$$\mu = g^b$$

$$d = g^{H_0(A,B,c)}\ k = c \oplus H_1(A,B,X_A,\mu,\sigma,d,V^{H_0(A,B,c)},V)$$

$$k' = H_2(A,B,X_A,\mu,\sigma,d,k,c,V)$$

然而，攻击者根据这些数据无法计算出$\sigma$和$c$，所以不能获得以前的会话密钥。

## 4.2　PAKA协议能抵抗Denning-Sacco攻击

为了抵抗Denning-Sacco攻击，协议应该满足以下要求：即使泄漏了会话密钥，攻击者也不能计算或者猜测出口令。假设攻击者知道了某个会话密钥$K = H_3(A,B,X_A,\mu,\sigma,c,V)$；另外，攻击者还可以获得$A$和$B$之间传递的消息，但是，攻击者利用这些消息不能计算和猜测出该用户的口令。

## 4.3　PAKA协议能抵抗服务器泄漏攻击

在本文提出的协议中，如果攻击者Eve获得服务器中存储的口令文件，它就知道了客户$A$的验证信息$V$。然而，Eve不能冒充为$A$，因为它不知道$V$，因此不能计算：

$$c = k \oplus H_1(A,B,X_A,\mu,\sigma,d,d^v,V)$$

所以，本文提出的改进协议能抵抗服务器泄漏攻击。

此外，攻击者Eve根据所能获得的消息是无法验证他所猜测的口令的，因此，本文提出的协议还能抵抗字典攻击。

# 5　结 束 语

针对一个对文献[10]提出的基于口令的认证密钥协商协议的服务器泄漏攻击，提出了一个改进的基于口令的认证密钥协商协议。用户只需记住自己的口令，而服务器仅仅存储与口令对应的验证信息。本协议可以抵抗服务器泄漏攻击、字典攻击和Denning-Sacco攻击等，并且具有前向安全性等性质。

## 参 考 文 献


[1] BELLOVIN S, MERRITT M. Encrypted key exchange: password-based protocols secure against dictionary attacks[C]//Proceedings of the IEEE Symposium on Research in Security and Privacy. Oakland: IEEE Computer Society, 1992: 72-84.

[2] BELLOVIN S, MERRITT M. Augumented encrypted key exchange:a password-based protocol secure against dictionary attacks and password file compromise[C]// Proceedings of CCS'93. New York: ACM Press, 1993: 244-250.

[3] JABLON D. Strong password-only authenticated key exchange[J]. ACM Computer Communication Review, 1996, 26(5): 5-20.

[4] BELLARE M, POINTCHEVAL D, ROGAWAY P. Authenticated key exchange secure against dictionary attacks[C]//Advances in Cryptology–EUROCRYPT'00. Bruges & Belgium: Springer-Verlag, 2000.

[5] BOYKO V, MACKENZIE P, PATEL S. Provably-secure password anthentiation and key exchange using Diffie-Hellman[C]//EUROCRYPT2000. Bruges,Belgium: Springer-Verlag, 2000.

[6] KATZ J, OSTROVSKY R, YUNG M. Efficient password-authenticated key exchange using human-memorable passwords[C]//EUROCRYPT 2001. Berlin: Springer- Verlag, 2001.

[7] Raimondo M, Gennaro R. Provably secure thre-shold password-authenticated key exchange[C]//EUROCRYPT 2003. New York: Springer-Verlag, 2003.

[8] GENNARO R, LINDELL Y. A framework for password-based authenticated key exchange[C]//EUROCRYPT2003. New York: Springer-Verlag, 2003.

[9] BRESSON E, CHEVASSUT O, POINTCHEVAL D. New security results on encrypted key exchange[C]//PKC2004. Singapore: Springer-Verlag, 2004.

[10] LEE S W, KIM W H, KIM H S, et al. Efficient password-based authenticated key agreement protocol[C]// ICCSA'04. Perugia: Springer-Verlag, 2004.

[11] SHIM K A, SEO S H. Security analysis of password-authenticated key agreement protocols[C]// CANS2005. Xiamen: Springer-Verlag, 2005.


编　辑　熊思亮