文章编号:1000-5013(2014)06-0665-04 **doi**:10.11830/ISSN.1000-5013.2014.06.0665

采用阈下信道的两方口令认证密钥交换协议

项顺伯[1],赵晶英[2],柯文德[1]

(1. 广东石油化工学院 计算机与电子信息学院,广东 茂名 525000;
2. 广东石油化工学院 机电工程学院,广东 茂名 525000)

摘要: 提出一种基于阈下信道的两方口令认证密钥交换协议.协议中,服务器存储用户口令的验证值抵御服务器泄漏伪装攻击,用户的口令明文采用阈下信道生成签名信息传送给服务器,服务器计算出用户的口令明文恢复出阈下信息,再计算口令验证值以实现对用户身份的认证,从而建立起会话密钥.对所提协议的安全性和效率进行分析,结果表明:所提出的协议安全可行且有效.

关键词: 阈下信道;口令认证密钥交换协议;口令验证值;会话密钥

中图分类号: TP 309 **文献标志码**: A

两方口令认证密钥交换协议是服务器以用户的口令或口令验证值为认证信息去证实用户的身份,从而在两者间建立一个安全的会话密钥.两方口令认证密钥交换协议存在诸多针对口令的攻击,如服务器泄漏伪装攻击、字典攻击等.因此,设计一个安全的口令认证密钥交换协议是研究的难题.以口令验证值为内容的口令认证密钥交换协议是近年来的研究热点.阈下信道的概念是由Simmons首次提出的[1],它是指在基于公钥密码机制的数字签名、认证等密码体制中建立起的一种隐秘信道,除发送者和指定的接收者外,任何人都不知道传输的密码数据内容中是否存在阈下信息[2].自从阈下信道提出后,学者对其进行了相关的研究.杨建萍等[3]基于阈下信道问题提出一种口令认证方案.Lee等[4]提出一种两方口令认证密钥交换协议PAKA-X,该协议基于口令验证值问题,能抵御服务器泄漏伪装攻击.Kwon[5]提出一种一轮的基于验证值的口令认证密钥交换协议,并在理想哈希模型下证明了协议的安全性,该协议适用于传输层安全(TLS)的协议.粟栗等[6]提出一种改进的签密方案,利用该方案设计了一个门限阈下信道方案.谭示崇等[7]提出一种改进的PAKA-X协议,但改进的协议实现过程复杂,计算量大.李文敏等[8]提出一种基于验证值的三方口令认证密钥交换协议.Pointcheval等[9]综述了口令认证密钥交换协议的通用构造方法.Fujioka等[10]提出口令认证密钥交换协议的GC协议的通用结构,在CK+模型下证明其安全性.HUANG等[11]提出了应用于ad hoc网络的带有匿名门限阈下信道的多签名方案.张应辉等[12]研究了EDL签名中的阈下信道封闭协议问题.张兴爱等[13]研究了广播多重签名方案中阈下信道的封闭协议问题.本文基于阈下信道问题,以用户的口令明文作为阈下信息,提出一种基于阈下信道的两方口令认证密钥交换协议.

1 基于阈下信道的两方口令认证密钥交换协议

基于阈下信道的两方口令认证密钥交换协议,简称PAKE.协议中,用户U和服务器S组成一个系统,其交互流程图,如图1所示.协议由以下3个方面组成[3,5,9-10].

1.1 系统建立

系统选择大素数 p,q,满足 $q|p-1$,g 是 Z_q^* 的生成元,其阶为 q;系统选择1个无碰撞的单向哈希函数 $H:(0,1)^*-(0,1)^l$,公开参数 p,q,g,H,l.用户U选择 $x_U\in_R Z_p^*$ 作为其私钥,计算公钥 $y_U=$

收稿日期: 2014-04-01

通信作者: 项顺伯(1979-),男,讲师,主要从事计算机网络与密码协议的研究.E-mail:qingcheng33@163.com.

基金项目: 国家自然科学基金资助项目(61272382);广东省自然科学基金资助项目(S2012010009963);广东省茂名市科技计划项目(20130350)

$g^{x_U} \bmod p$,用户 U 的身份标识符为 ID_U,U 公开参数 y_U 和 ID_U.

身份标识符为 ID_S 的服务器 S 选择私钥 $x_S \in_R Z_p^*$,其公钥 $y_S = g^{x_S} \bmod p$,S 公开参数 y_S 和 ID_S. pw 为用户 U 的口令明文,U 计算口令 pw 的验证值 $v = g^{H(ID_U \| ID_S \| pw)}$,并通过秘密信道把 v 传给服务器 S 保存.

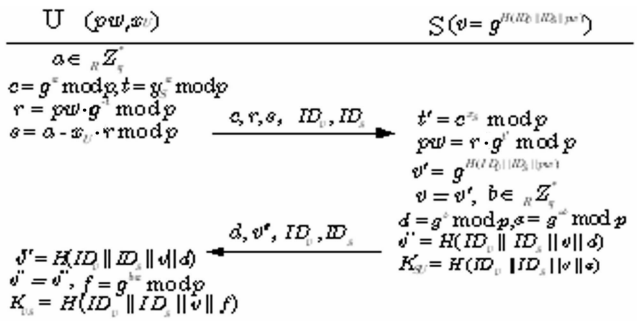

图 1 PAKE 的交互流程图

Fig. 1 Interactive flow chart of PAKE

1.2 含有阈下信息签名的产生

用户 U 选择 $a \in_R Z_q^*$,计算 $c = g^a \bmod p$ 和 $t = y_S^a \bmod p$,计算 $r = pw \cdot g^{-t} \bmod p$,$s = a - x_U \cdot r \bmod p$,则含有阈下信息的签名为$(c,r,s)$,用户 U 向服务器 S 发送信息$(c,r,s,ID_U,ID_S)$.

服务器 S 收到用户 U 的签名消息后进行阈下信息的恢复,服务器通过其私钥 x_S 计算 $t' = c^{x_S} \bmod p$,再计算用户的口令明文 $rpw = r \cdot g^{t'} \bmod p$ 即可恢复出阈下信息.

1.3 会话密钥的建立

服务器 S 通过恢复出的 pw 计算 $v' = g^{H(ID_U \| ID_S \| pw)}$,比较 v 和 v',若 $v \neq v'$,终止协议的执行;否则实现对用户身份的验证.在证实用户的身份后,服务器 S 选择 $b \in_R Z_q^*$,计算 $d = g^b \bmod p$,$e = g^{ab} \bmod p$,$v'' = H(ID_U \| ID_S \| v \| d)$,S 向用户 U 发送消息$(d,v'',ID_U,ID_S)$,并计算与用户 U 的会话密钥 $K_{SU} = H(ID_U \| ID_S \| v \| e)$.

用户 U 收到消息后,首先计算 $v''' = H(ID_U \| ID_S \| v \| d)$,如果 $v'' \neq v'''$,终止协议的执行;否则,计算 $f = g^{bx_U} \bmod p$,并将计算出的 $K_{SU} = H(ID_U \| ID_S \| v \| f)$作为其与服务器的会话密钥.明显,$e = g^{bx_U} \bmod p = f$,所以,用户和服务器计算出的会话密钥是一致的.

2 协议安全性分析

2.1 含有阈下信息签名的安全性分析

2.1.1 *含有阈下信息签名的不可伪造性* 因为只有合法用户才拥有自己的口令明文,攻击者没有用户的口令明文,无法伪造有效的签名.假设攻击者随机选择一个口令 pw',与用户的口令 pw 相比,$pw' \neq pw$,攻击者选择 $a \in_R Z_q^*$,计算 $c' = g^a \bmod p$,$t = y_S^a \bmod p$,$r' = pw' \cdot g^{-t} \bmod p$,接着计算 $s' = k - x_U \cdot r' \bmod p$,则含有阈下信息的伪造签名为$(c',r',s')$.

服务器 S 收到含有阈下信息的签名消息后计算 $t' = c'^{x_S}$,然后计算出阈下信息,用户的口令 $pw' = r' \cdot g^{-t'} \bmod p$,接着服务器 S 计算 $v' = H(ID_U \| ID_S \| pw')$.通过比较发现 $v \neq v'$,证实用户的身份失败,从而终止协议的执行.因此,攻击者无法针对合法用户伪造出有效的签名.

2.1.2 *含有阈下信息签名的公开可验证性* PAKE 中,任何人都可以通过获得的公开信息去计算 $c = g^s \cdot y_U^r \bmod p$,以实现签名有效性的验证.因为 $g^s \cdot y_U^r \bmod p = g^{k - x_U r} \cdot g^{x_U r} \bmod p = g^a \bmod p = c$,所以协议中阈下信息的签名具有公开可验证性.

2.2 前向安全性

PAKE 中,前向安全性是指在某次会话过程中,即使攻击者知道了用户的口令明文 pw,也无法计算该次会话之前的会话密钥.因为每次会话中,服务器和用户分别选择的随机数 a 和 b 都不完全相同,又因为离散对数困难问题,攻击者无法从 $c = g^a \bmod p$ 和 $d = g^b \bmod p$ 中分别计算出 a 和 b,于是攻击者

无法计算出 $e=g^{ab} \bmod p$ 和 $f=g^{ba} \bmod p$，从而攻击者无法计算出最终的会话密钥 K_{US}. 所以，文中的 PAKE 是前向安全的.

2.3 抵御字典攻击

字典攻击是指攻击者针对用户的口令发起的攻击，通过猜测和分析去获得用户的口令明文，字典攻击可分为在线字典攻击和离线字典攻击两种. 在线字典攻击是指攻击者随机选择一个口令，通过截获的公开信息伪装成合法用户与服务器会话，通过多次试探，从而猜测出用户的口令. 离线字典攻击是指攻击者通过分析截获的公开会话信息，从中分析计算出用户的口令明文.

2.3.1 *抵御在线字典攻击*　假设攻击者随机 1 个口令 $pw' \neq pw$，通过截获用户的公开信息 (c, r, s, ID_U, ID_S)，伪造出另一组含有阈下信息的签名 (c, r', s', ID_U, ID_S). 其中：$r'=pw' \cdot g^{-t} \bmod p$；$s'=k-x_U \cdot r' \bmod p$. 服务器收到该签名信息后，通过计算恢复出阈下信息，即用户口令明文 pw'. 接着，服务器计算用户口令验证值 $v'=H(ID_U \| ID_S \| pw')$，通过比较发现 $v' \neq v$，服务器认为用户身份信息不安全，从而终止协议的执行，攻击者的在线字典攻击无法成功. 事实上，如果攻击者尝试该类攻击，就陷入了签名的伪造性. 前文已经分析过，文中 PAKE 签名是不可伪造的，所以，文中的 PAKE 是能抵御在线字典攻击的[8].

2.3.2 *抵御离线字典攻击*　文中的 PAKE 中，攻击者无法实施离线字典攻击，因为用户和服务器会话过程中，仅 $r=pw \cdot g^{-t} \bmod p$ 和 $v''=H(ID_U \| ID_S \| pw \| d)$ 含有用户的口令明文. 由于 r 是阈下信息，攻击者无计可施，又因哈希函数的特性，攻击者无法选择 pw'，使得 $v''=H(ID_U \| ID_S \| pw \| d)=H(ID_U \| ID_S \| pw' \| d)$. 因此，PAKE 能抵御离线字典攻击.

2.4 抵御服务器泄漏伪装攻击

抵御服务器泄漏伪装攻击是指服务器遭受攻击或恶意泄漏后，用户的口令验证值泄漏给攻击者，攻击者伪装成合法用户去登录服务器. PAKE 协议中，假设服务器存储的用户口令验证值 $v=H(ID_U \| ID_S \| pw)$ 泄漏给攻击者，由于哈希函数的特性，攻击者无法获得正确的口令明文，如果攻击者伪装成合法用户去登录服务器，必然随机选择一个口令 $pw' \neq pw$，然后伪造一个含有阈下信息的签名 (c', r', s'). 前文已经分析过，PAKE 中的签名不可伪造，于是攻击者的伪装是不成功的. 因此，文中的 PAKE 能抵御服务器泄漏伪装攻击.

3 协议运行效率分析

所提出的 PAKE 中，协议的主要计算体现在指数运算、点乘运算和哈希运算等上. 用户签名的产生需要 3 次指数运算，2 次点乘运算，服务器恢复阈下信息需要 2 次指数运算和 1 次点乘运算，省去了签名验证的大量运算. 建立会话密钥时，服务器只需 2 次指数运算和 3 次哈希函数的运算，用户仅需 1 次点乘运算和 2 次哈希运算.

文献[5]的协议用了 9 次指数运算，3 次哈希运算，3 次点乘运算，3 次除运算，与文中的 PAKE 相比，计算量稍大一些. 文献[7]改进的协议中，指数运算有 9 次，哈希运算有 10 次，尽管没有使用点乘运算，但用了 4 次异或运算. 与文献[7]的协议相比，文中协议计算量小，因而效率更高.

4 结束语

设计一个基于阈下信道问题的两方口令认证的密钥交换协议. 协议利用服务器存储用户口令的验证值，用户发送含有口令阈下信息的签名给服务器，服务器验证签名并通过恢复出的阈下信息实现对用户身份的认证. 通过分析可知：文中的协议避免了一些针对口令认证密钥交换协议的攻击，如服务器泄漏伪装攻击、字典攻击等；同时，与其他协议比较，文中的协议所需计算量小，效率更好. 文中的协议可以用于现有的用户端/服务器(U/S)的环境中，从而实现服务器对用户的身份认证及认证后的交互过程.

参考文献：

[1] SIMMONS G J. The prisoner's problem and the subliminal channel[C]// Proceedings IEEE Workshop Communica-

tions Security CRYPTO. New York:[s. n.],1983:51-67.
[2] SIMMONS G J. The history of subliminal channels[J]. IEEE Journal on Selected Areas in Communication,1998,16(4):452-462.
[3] 杨建萍,周贤伟,杨军. 基于阈下信道技术的身份认证机制研究[J]. 微电子学与计算机,2004,21(12):195-197.
[4] LEE S W,KIM W H,KIM H S,et al. Efficient password-based authenticated key agreement protocol[C]// International Conference on Computer Science and Applications. Perugia:Springer-Verlag,2004:617-626.
[5] KWON J O,SAKURAI K,LEE D H. One-round protocol for two-party verifier-based password-authenticated key exchange[C]// Communications and Multimedia Security. Heraklion:[s. n.],2006:87-96.
[6] 粟栗,崔国华,李俊,等. 基于签密的分布式安全门限阈下信道方案[J]. 小型微型计算机系统,2007,28(12):2153-2157.
[7] 谭示崇,张宁,王育民. 新的口令认证密钥协商协议[J]. 电子科技大学学报,2008,37(1):17-19.
[8] 李文敏,温巧燕,张华. 基于验证元的三方口令认证密钥交换协议[J]. 通信学报,2008,29(10):150-152.
[9] POINTCHEVAL D. Password-based authenticated key exchange[C]// Proceedings of 15th IACR International Conference on Practice and Theory of Public-Key Cryptography. Darmstadt:Springer-Verlag,2012:390-397.
[10] FUJIOKA A,SUZUKI K,XAGAWA K,et al. Strongly secure authenticated key exchange from factoring, codes, and lattices[C]// Proceedings of 15th IACR International Conference on Practice and Theory of Public-Key Cryptography. Darmstadt:Springer-Verlag,2012:467-484.
[11] HUANG Zhen-jie,CHEN Dan,WANG Yu-min. Multi-signature with anonymous threshold subliminal channel for ad-hoc environments[C]// 19th International Conference on Advanced Information Networking and Applications. Tamshui:IEEE Press,2005:67-71.
[12] 张应辉,马华,王保仓. EDL 签名中可证明安全的阈下信道封闭协议[J]. 计算机科学,2010,37(9):72-74.
[13] 张兴爱,张应辉,史来婧. 广播多重签名方案中阈下信道的封闭协议[J]. 计算机工程,2011,37(22):102-104.

Two-Party Password-Authenticated Key Exchange Protocol Based on the Subliminal Channel

XIANG Shun-bo[1], ZHAO Jing-ying[2], KE Wen-de[1]

(1. College of Computer and Electronic Information, Guangdong University of Petrochemical Technology, Maoming 525000, China;
2. College of Mechanical and Electrical Engineering, Guangdong University of Petrochemical Technology, Maoming 525000, China)

Abstract: A two-party password-authenticated key exchange protocol based on the subliminal channel was proposed. In the proposed protocol, the server stores the user's password verifier to withstand the server's compromise and guise attacks, the user's password cleartext is made to a signature message with the subliminal channel to transmit to the server, the server computes the user's password cleartext to renew the subliminal message, then the server calculates the password verifier to authenticate the user's identity, so a session key is made between the server and the user. The security and the efficiency of the proposed protocol were analyzed, it shows in the analysis that the proposed protocol is secure and effective.

Keywords: subliminal channel; password-authenticated key exchange protocol; password verifier; session key

(**责任编辑**: 钱筠 **英文审校**: 吴逢铁)