第30卷第1期 东北大学学报(自然科学版) Vol. 30, No. 1
2009年1月 Journal of Northeastern University(Natural Science) Jan. 2009

一种改进的跨域口令密钥交换协议

刘广伟, 周恩光, 闫 虹, 周福才
(东北大学 信息科学与工程学院, 辽宁 沈阳 110004)

摘 要: 跨域的端到端的口令认证密钥交换(C2C-PAKE)协议,可实现不同区域的两个客户通过不同的口令协商出共享的会话密钥.首先对Byun2007的C2C-PAKE协议进行了描述,并针对其安全性进行了分析,发现该协议易遭受口令泄露伪造攻击的安全漏洞,提出了一种高效的改进的跨域口令认证密钥交换协议.该协议引入公钥密码体制能够有效抵抗口令泄露伪造攻击和不可检测在线字典攻击,且只需要6步通信.安全性分析表明该协议是安全有效的.

关 键 词: 安全协议;跨域;口令认证密钥交换;口令泄露伪造攻击;敌手
中图分类号: TP 309.2 **文献标识码**: A **文章编号**: 1005-3026(2009)01-0042-04

An Improved Cross-Realm Client-to-Client Password-Authenticated Key Exchange Protocol

LIU Guang-wei, ZHOU En-guang, YAN Hong, ZHOU Fu-cai
(School of Information Science & Engineering, Northeastern University, Shenyang 110004, China. Correspondent: ZHOU Fu-cai, E-mail: fczhou@mail.neu.edu.cn)

Abstract: The client-to-client password-authenticated key exchange (C2C-PAKE) protocol enables two clients from different realms to agree on a shared common session key. Describing the C2C-PAKE protocol of Byun2007, its security is analyzed and it is found that the protocol is easy to suffer the attacks due to password-compromised impersonation and undetected on-line dictionary. An improved C2C-PAKE protocol is therefore proposed to introduce the public key mechanism into system security to resist those attacks effectively, especially only six operational steps are needed in relevant communication. As shown in security analysis, the protocol proposed is available to meet the security requirements.

Key words: security agreement; cross-realm; password-authenticated key exchange; password-compromise impersonation attack; adversary

随着网络的发展,移动网络、家庭网络等也得到了飞速发展.在无处不在的网络中,端到端的安全越来越被人们所重视.2002年,Byun等学者[1]首次提出了一种跨域环境中基于口令认证的密钥交换协议,简称为C2C-PAKE(client-to-client password-authenticated key exchange)协议.协议的目的是使跨域环境中的两个客户,在没有共享秘密的情况下,在各自域服务器的协助下建立起一个安全的通讯信道,协议中两个客户拥有不同的口令.随后,Wang等学者[2]即指出该协议不能抵御来自另一个域的服务器所发动的字典攻击.2004年Kim等学者[3]又指出该协议不能抵御Denning-Sacco攻击[4],并提出了改进协议.而2006年Yoon等学者[5]又指出Kim的改进协议不能抵御口令泄露伪造攻击和单向中间人攻击,并提出了新的改进协议.2006年,Byun等学者重新提出了一个高效且比较完善的协议[6],并在2007年首次对跨域口令密钥交换协议进行了形式化的安全证明[7].2007年Yang等人也提出了一种能抵御多种已知攻击的协议[8].然而Phan等人[9]和Yoneyama等人[10]指出文献[1,3,5-6,8]容易遭受不可检测的在线字典攻击.同时,文

收稿日期: 2007-05-24
基金项目: 国家自然科学基金资助项目(60773218); 国家高技术研究发展计划项目(2001AA115300); 辽宁省自然科学基金资助项目(20062023).
作者简介: 刘广伟(1965-),男,辽宁沈阳人,东北大学博士研究生; 周福才(1964-),男,吉林长春人,东北大学教授,博士.

献[11]发现上述协议[1,3,5-6]容易遭受口令泄露伪造攻击,提出在非对称体制下才能防止密钥泄露伪造攻击并给出一个需要 9 步通信的改进方案.文献[7-8]仍然存在口令泄露伪造攻击.本文提出了一种高效的改进的跨域口令认证密钥交换协议,协议只需要 6 步通信.该协议可以抵御多种已知攻击,包括不可检测的在线字典攻击和口令泄露伪造攻击.

1　Byun2007 协议分析

1.1　Byun2007 协议描述

下面给出协议中所使用的符号定义:

A,B:诚实的客户;

ID_A,ID_B:A 和 B 的身份标识;

PW_A,PW_B:A 和 B 的口令;

E_x:用密钥 x 进行对称加密;

KDC_A,KDC_B:密钥分发中心,分别存储 A 和 B 的口令;

K: KDC_A 和 KDC_B 之间共享的对称密钥;

$Ticket_B$:分发给 A 的 Kerberos 票据,作为获得 B 服务的凭证;

L: $Ticket_B$ 的生命周期;

$MAC_k(m)$:使用密钥 k 计算消息 m 的验证码;

p,q:足够大的素数,满足 $q|(p-1)$;

G: Z_p^* 的一个子群,阶为 q;

g:群 G 的生成元;

H, H_1, H_2:安全的单向哈希函数;

C:攻击者或敌手.

除了指数外所有的表达式都是 mod p 的.为了表达上的简便,本文中省略了"mod p".Byun2007 的协议描述如下:

1) A 选择一个随机数 $x \in Z_p^*$.计算 g^x 和 $M_1 = E_{PW_A}(g^x)$,然后将 M_1, ID_A, ID_B 发送给 KDC_A.

2) KDC_A 解密 M_1 得到 g^x.然后选择一个随机数 $y \in Z_p^*$,计算出 g^y, $E_y = E_{PW_A}(g^y)$ 以及 $R = H(g^{xy})$.KDC_A 再次选择一个随机数 $k \in Z_p^*$ 用作消息验证码的加密密钥,计算出 $E_R = E_R(k, ID_A, ID_B)$,并生成 $Ticket_B = E_k(ID_A, ID_B, k, L)$.然后,$KDC_A$ 将 E_y, E_R, $Ticket_B$ 发送给 A.

3) A 收到消息后,首先计算出 R,然后解密 E_R 得到分发的 MAC 密钥 k.A 将 $E_R(g^y)$ 发送给 KDC_A 进行身份确认.如果 KDC_A 对 A 身份验证成功,则 KDC_A 确认与 A 的通话.

4) A 选择一个随机数 $a \in Z_p^*$,计算出 $E_a = (g^a \| MAC_k(g^a))$,然后将 ID_A, E_a, $Ticket_B$ 发送给 B.

5) B 选择一个随机数 $x' \in Z_p^*$,计算 $E_{x'} = E_{PW_B}(g^{x'})$,然后将 E_x 和 $Ticket_B$ 发送给 KDC_B.

6) KDC_B 使用与 KDC_A 共享的会话密钥 K 解密 $Ticket_B$ 得到 k, L, ID_A.KDC_B 首先验证 L 和 ID_A 以判定 $Ticket_B$ 的合法性.如果 $Ticket_B$ 验证合法,则 KDC_B 选择一个随机数 $y' \in Z_p^*$,计算出 $E_{y'} = E_{PW_B}(g^{y'})$, $R' = H(g^{x'y'})$ 以及 $E_{R'} = E_R(k, ID_A, ID_B)$.然后 KDC_B 将 E_y 和 E_R 发送给 B.

7) B 解密 E_y 得到 g^y 和 R',然后将 $E_R(g^{y'})$ 发送给 KDC_B 进行密钥确认.KDC_B 解密 $E_R(g^{y'})$ 后验证 $g^{y'}$ 是否正确.

8) B 解密 E_R 得到 k,接着利用 k 检验先前接收到的 E_a 中 g^a 的正确性.如果正确,则 B 选择一个随机数 $b \in Z_p^*$,计算出与 A 共享的会话密钥 $SK = H(ID_A \| ID_B \| g^a \| g^b \| g^{ab})$ 和 $E_b = (g^b \| MAC_k(g^b))$.最后 B 将 E_b 发送给 A.A 在收到 E_b 后,可以通过计算生成一个相同的会话密钥 SK.

1.2　对 Byun2007 协议的安全漏洞分析

Byun2007 的 C2C-PAKE 协议容易遭受口令泄露伪造攻击.

口令泄露伪造攻击是指若客户 A 的口令 PW_A 泄露,那么窃取 PW_A 的敌手就能冒充 B 与 A 进行会话.同理,若客户 B 的口令 PW_B 泄露,那么窃取 PW_B 的敌手 C 就可以冒充 A 与 B 进行会话.

假设在 Byun2007 的协议中 A 的口令 PW_A 被敌手 C 所窃取:

1) 协议描述的第二步,敌手 C 将 A 发送的 $E_{PW_A}(g^x)$ 截获并解密得到 g^x.则 C 可首先假冒 KDC_A,C 随机选择 $r \in Z_p^*$,计算出 $E_r = E_{PW_A}(g^r)$ 以及 $R' = H(g^{xr})$.然后选择一随机数 $k' \in Z_p^*$,计算出 $E_R' = E_R(k', ID_A, ID_B)$.C 不需要拥有 KDC_A 与 KDC_B 之间的对称密钥 K 来生成一个真实的 $Ticket_B$,他可以任意伪造一个 $Ticket_B'$.随后敌手 C 将 E_y', E_R' 以及 $Ticket_B'$ 传送给 A.

2) A 收到 C 发来的消息后,解密 E_R' 得到 k',A 将 k 作为消息验证码 MAC 的密钥,然后随机选取 $a \in Z_p^*$,计算出 E_a,随后 A 将 E_a 发送给 B.

3) C 截获 E_a,解密出 g^a 后直接跳到通讯过程的第 8)步.C 再随机选择 $b \in Z_p^*$,利用 k 计算 E_b,随后将 E_b 传送给 A.

4) A 收到 E_b 后,利用 k 对 E_b 进行验证,结果是正确的.

这样敌手 C 就成功假冒了 B 与 A 建立了一条通讯信道,共享密钥是 $SK = H(ID_A \| ID_B \| g^a \| g^b \| g^{ab})$,A 认为正在与 B 进行通话,而实际上是正在与 C 通话.

同理,假设敌手 C 窃取了 B 口令 PW_B:

1) 敌手 C 选择两个随机数 a 和 k',计算 $E_a = (g^a \| MAC_{k'}(g^a))$,并伪造出一个 $Ticket'_B$.然后 ε 将 ID_A, E_a, $Ticket'_B$ 传给 B.

2) B 收到消息后,选择一个随机数 x',计算出 $E_{x'} = E_{PW_B}(g^{x'})$,然后将 E_x 和 $Ticket'_B$ 传送给 KDC_B.

3) 敌手 C 将 B 发给 KDC_B 的消息截获,解密 E_x 求出 $g^{x'}$,然后 C 选择一随机数 r,计算出 $E_r = E_{PW_B}(g^r)$ 和 $R' = H(g^{x'r})$.然后敌手利用存储的 k 计算 $E'_R = E_{R'}(k', ID_A, ID_B)$.随后敌手将 E_r 和 E'_R 发送给客户 B.

4) B 收到 E_r 和 E'_R 后,解密得到 g^r.然后解密 E'_R 得到 k',B 用 k 验证 $E_a = g^a \| MAC_k(g^a)$ 成功后,选择一个随机数 $b \in Z_p^*$,发送消息 $E_b = g^b \| MAC_{k'}(g^b)$.

5) 敌手 C 将 E_b 截获,这样在敌手 C 和 B 共享会话密钥 $SK = H(ID_A \| ID_B \| g^a \| g^b \| g^{ab})$,敌手 C 成功地假冒了 A,而 B 却认为正在与 A 通话.

B 的口令泄露后,敌手就可以在任意时间假冒 A 发动攻击,而 A 的口令泄露后,敌手 C 只能在 A 发起和 B 通讯后冒充 B.可见敌手 C 获得 B 的口令会具有更大的威胁性和破坏性.

2 改进的 C2C-PAKE 协议

改进的 C2C-PAKE 协议引入公钥体系,改进后的协议能够有效抵御口令泄露伪造攻击.下面给出协议中特有的符号定义及协议描述:

在改进的协议中,PUB_{KDC_A}, PUB_{KDC_B} 分别为 KDC_A 和 KDC_B 的公钥;PRI_{KDC_A}, PRI_{KDC_B} 分别为 KDC_A 和 KDC_B 的私钥.

改进的 C2C-PAKE 协议包含 6 个基本通讯过程:

1) A 随机选择 3 个随机数 k, m, N_A 然后将 ID_A, ID_B, $E_{PUB_A} = E_{PUB_{KDC_A}}(PW_A, m, k, N_A)$ 发送给 KDC_A.

2) KDC_A 解密收到信息得到 k, m, N_A.然后,KDC_A 计算出 $E_m = E_m(ID_A, ID_B, N_A + 1)$,并生成 $Ticket_B = E_{PUB_{KDC_B}}(E_{PRI_{KDC_A}}(k, ID_A, ID_B, L))$,先用 KDC_A 的私钥签名,然后再用 KDC_B 的公钥加密,其中,L 为时间戳.最后,KDC_A 将 E_m 和 $Ticket_B$ 发送给 A.

3) A 用 m 解密 E_m,对 ID_A, ID_B, $N_A + 1$ 进行验证.然后 A 选择一随机数 $a \in Z_p^*$,计算出 $g^a \| MAC_k(g^a)$.A 将 $g^a \| MAC_k(g^a)$ 和 $Ticket_B$ 发送给 B.

4) B 收到 A 发送的消息后,选择两个随机数 n, N_B,将 $Ticket_B$, $E_{PUB_B} = E_{PUB_{KDC_B}}(PW_B, n, N_B)$ 发送给 KDC_B.

5) KDC_B 解密 E_{PUB_B} 后得到 n, N_B,解密 $Ticket_B$ 后得到 k,然后计算出 $E_n = E_n(ID_A, ID_B, k, N_B + 1)$ 并发送 E_n 给 B.

6) B 收到 E_n 后,解密得到 k 和 $N_B + 1$.验证 $N_B + 1$ 后,B 用密钥 k 解密出 g^a 的消息验证码,比较是否与 A 传送来的 $MAC_k(g^a)$ 相同.若相同,B 向 A 发送 $g^b \| MAC_k(g^b)$,同时 B 生成会话密钥 $SK = g^{ab}$.A 收到 $g^b \| MAC_k(g^b)$ 后验证 g^b,若验证通过,A 生成会话密钥 $SK = g^{ab}$.

3 安全性分析

改进协议的安全性基于服务器的私钥不能被敌手窃取的假设.以下详细分析改进协议的安全性.

1) 口令泄露伪造攻击.假设存在敌手 C 窃取到客户 A 的口令 PW_A,并且 C 可截获通讯过程中的所有信息.因为 C 没有 KDC_A 的私钥 PRI_{KDC_A},无法解密所截获的消息 E_{PUB_A},因而无法得到 N_A, k 和 m,从而无法假冒 KDC_A 或者 B 与 A 通讯;假设敌手 C 窃取到客户 B 的口令 PW_B,则与上述描述类似.

2) 重放攻击.因为协议中的 k, m, N_A, n, N_B 都是临时变量,所以进行重放攻击的概率可以忽略不计,C 不能假冒任何一方发动重放攻击.

3) 前向安全性.若 C 窃取了 PW_A 和 PW_B,则 C 可以获取之前产生的 g^a 和 g^b,但基于计算 Diffie-Hellman 假设,C 无法计算出之前的会话密钥 $SK = g^{ab}$,从而保证了协议的前向安全性.

4) 恶意服务器攻击.恶意服务器攻击是指服

务器 KDC_B(或 KDC_A)窃取另一个域中的客户口令.在改进协议中,假设 KDC_B 为恶意服务器,因为 KDC_B 无法获取 KDC_A 的私钥 PRI_{KDC_A},就无法解密 E_{PUB_A},因而无法获取客户 A 的口令 PW_A;若 KDC_A 为恶意服务器,则与上述描述类似.

5) 离线字典攻击.敌手有两种类型,第一种是外部敌手,他不知道 PW_A 和 PW_B,想要得到 PW_A 和 PW_B;第二种是内部敌手,他知道 PW_A(或 PW_B).对外部敌手,因为他无法获取 KDC_A 的私钥 PRI_{KDC_A},无法解密 E_{PUB_A} 进而得到 PW_A.对于拥有 PW_A 的内部敌手,因为他无法获取 KDC_B 的私钥 PRI_{KDC_B},所以无法解密 E_{PUB_B} 得到 PW_B.

6) 不可检测在线字典攻击.敌手选择一个 PW'_A 作为 A 的候选口令,然后将 E_{PUB_A} 和 ID_A 发送给 KDC_A,KDC_A 验证 PW'_A,显然 PW'_A 和 KDC_A 存储的口令 PW_A 不符,KDC_A 检测到敌手对 PW_A 的攻击.

7) 服务器中间人攻击.文献[9]提出在 Byun2007 的协议中,服务器 KDC_A 和 KDC_B 能够发动中间人攻击.然而,其他的跨域协议[1,3,5,8]也都存在服务器中间人攻击,这是 C2C-PAKE 协议存在的缺陷.针对这个缺陷,将会在后续的论文中做详尽的分析和阐述.

4 结　论

本文提出了一种改进的跨域口令密钥交换协议,该协议能够有效地抵御多种攻击,包括口令泄露伪造攻击和不可检测在线字典攻击.经安全分析该协议是安全有效的.

参考文献:

[1] Byun J W, Jeong I R, Lee D H, *et al*. Password-authenticated key exchange between clients with different passwords[C] //International Conference on Information and Communications Security. Berlin : Springer-Verlag, 2002: 134 - 146.

[2] Wang S H, Wang J, Xu M Z. Weaknesses of a password-authenticated key exchange protocol between clients with different passwords[C] //ACNS 2004. Berlin: Springer-Verlag, 2004:414 - 425.

[3] Kim J Y, Kim S J, Kwak J, *et al*. Cryptanalysis and improvement of password authenticated key exchange between clients with different passwords[C] //International Conference on Computational Science and Its Applications. Berlin:Springer-Verlag, 2004:895 - 902.

[4] Denning D, Sacco G. Timestamps in key distribution protocols[J]. *Communications of the ACM*,1981,24(8): 533 - 536.

[5] Yoon E, Yoo K. A secure password-authenticated key exchange between clients with different passwords[C] // International Workshop on Metropolis/ Enterprise Grid and Applications. Berlin:Springer-Verlag, 2006:659 - 663.

[6] Byun J W, Lee D H, Lim J. Efficient and provably secure client-to-client password-based key exchange protocol[C] // APWeb 2006. Berlin:Springer-Verlag, 2006:830 - 836.

[7] Byun J W, Lee D H, Lim J I. EC2C-PAKA: an efficient client-to-client password-authenticated key agreement[J]. *Information Sciences*, 2007,177(19):3995 - 4013.

[8] Yang G, Feng D G, He X X. Improved client-to-client password-authenticated key exchange protocol[C] //The 2nd International Conference on Availability, Reliability and Security. Washington: IEEE Computer Society, 2007:564 - 574.

[9] Phan R C W, Goi B M. Cryptanalysis of an improved client-to-client password-authenticated key exchange (C2C-PAKE) scheme[C] //Applied Cryptography and Network Security. Berlin:Springer-Verla, 2005:33 - 39.

[10] Yoneyama K, Ota H, Ohta K. Secure cross-realm client-to-client password-based authenticated key exchange against undetectable on-line dictionary attacks[C] //Applied Algebra, Algebraic Algorithms, and Error Correcting Codes Symposium. Berlin: Springer-Verlag, 2007:257 - 266.

[11] Xu J, Zhang Z F, Feng D G. Analysis and improvement of client-to-client password authenticated key exchange protocols [C] //Security Protocols, the 3rd SKLOIS Workshop. Beijing: Graduate School of the Chinese Academy of Sciences, 2007:109 - 124.