

改进的跨域口令认证密钥交换协议

刘卫红, 王立斌, 马昌社

(华南师范大学计算机学院, 广州 510631)

摘要: 描述一个跨域口令认证密钥交换协议, 在其基础上对跨域 C2C-PAKE 协议的安全模型进行改进。通过引入公钥密码体制, 结合离散对数高可靠等特点, 提出改进的跨域口令认证密钥交换协议。该协议步骤简单, 具有语义安全性、密钥保密性, 实现了服务器与用户之间的双向认证, 能对抗不可检测在线字典攻击等常见攻击。安全性分析表明该协议是安全有效的。

关键词: 跨域; 口令认证; 密钥交换; 安全协议

Improved Cross-realm C2C-PAKE Protocol

LIU Wei-hong, WANG Li-bin, MA Chang-she

(Computer School, South China Normal University, Guangzhou 510631, China)

【Abstract】 This paper describes a cross-realm C2C-PAKE protocol. Based on it, it improves the formal model and proposes an improved protocol which is introduced public key mechanism to system security and combined with the high reliability of discrete logarithm. The protocol is simple and is analyzed with semantic security and key confidentiality. It also achieves the mutual authentication between server and client, and it can resist common attacks such as undetected online dictionary attack. Security analysis shows it is safe and effective.

【Key words】 cross-realm; password authentication; key exchange; security protocol

1 概述

跨域口令认证密钥交换协议(简称 C2C-PAKE 协议), 主要用于不同域间持不同口令的用户在各自域中服务器的协助下协商和共享会话密钥。Byun 等提出一种 C2C-PAKE 协议^[1], 随后, Wang 等指出该协议不能抵抗恶意服务器攻击并改进了协议, Kim 等发现该改进协议仍存在 Denning-Sacco 等攻击, 因此, 提出新 ID_i 协议。

2006 年 Kim 等的改进协议被 Yoon 等指出不能抵御口令泄露伪造攻击和单向中间人攻击。Byun 等重新提出新的改进协议^[2], 并对改进协议进行了形式化证明^[3]。然而不久后文献^[4]就指出该协议会遭受不可检测的在线字典攻击, 还提出只有在非对称体制下才能防止密钥泄露伪造攻击并给出了一个改进方案。文献^[5]给出一个跨域 C2C-PAKE 协议, 其安全性在严格定义的形式化安全模型中得到了证明。但文献^[2, 5]中的方案不久后就被文献^[6]证明仍不能防止不可检测在线字典攻击, 其中, 文献^[5]方案不能抵抗未知密钥分享攻击。

本文阐述了 Byun 的改进跨域 C2C-PAKE 协议的交互过程, 在其基础上改进了 Yinyin 等人的跨域 C2C-PAKE 协议的安全模型, 给出了一个新协议并在新的安全模型中分析了其安全性。

2 Byun 跨域 C2C-PAKE 协议

本文先讨论文献^[3]中的安全协议, 所有协议都基于 DDH 假设, 符号说明如下: A, B 表示参与通信的用户; $A \rightarrow B: M$ 表示 A 给 B 发送消息 M ; ID_i 表示用户 i 的 ID; pw_i 表示用户 i 与 S_i 共享的口令; S_i 表示用户 i 所在域内的服务器, 主要存储该域中用户的 ID 和口令; \oplus 表示异或操作; $MAC_k(M)$ 表示消息 M 和密钥 K 的 MAC 函数值(密码校验和); P 表示大

素数; g 表示有限域 $GF(P)$ 的生成元; g^x 表示 $g^x = g^x \pmod{p}$; H 表示 Hash 函数; L 或 L' 表示一个机密参数, 作为服务器间密文的生命周期; $Ticket_i$ 表示另一服务器传递给用户 i 所在域中服务器的密文; $x \in Z_p^*$ 表示在 Z_p^* 中随机选取元素 x ; “ \parallel ” 表示消息的级联; M_i 表示用户 i 加密的消息。

该协议简要描述如下:

(1) $A \rightarrow S_A: E_x, ID_A, ID_B$, 说明:

$$x \in Z_p^*, E_x = E_{pw_A}(g^x)$$

(2) $S_A \rightarrow A: E_y, E_R, Ticket_B$, 说明:

$$y \in Z_p^*, E_y = E_{pw_A}(g^y), R = H(g^{xy}), k \in Z_p^*$$

$$E_R = E_R(k, ID_A, ID_B), Ticket_B = E_K \langle k, ID_A, ID_B, L \rangle$$

(3) $A \rightarrow S_A: E_R(g^y)$, 说明:

$$R = H(g^{xy})$$

(4) $A \rightarrow B: ID_A, E_a, Ticket_B$, 说明:

$$a \in Z_p^*, E_a = g^a \parallel MAC_k(g^a)$$

(5) $B \rightarrow S_B: E_{x'}, Ticket_B$, 说明:

$$x' \in Z_p^*, E_{x'} = E_{pw_B}(g^{x'})$$

(6) $S_B \rightarrow B: E_{y'}, E_{R'}$, 说明:

$$y' \in Z_p^*, E_{y'} = E_{pw_B}(g^{y'}), R' = H(g^{x'y'})$$

$$E_{R'} = E_{R'}(k, ID_A, ID_B)$$

基金项目: 国家自然科学基金资助项目“高效可证明紧致安全的数字签名技术研究”(60703094)

作者简介: 刘卫红(1984-), 女, 软件设计师、硕士, 主研方向: 密码学, 信息安全; 王立斌、马昌社, 副教授、博士

收稿日期: 2010-04-23 **E-mail:** lbwang@gmail.com

(7) $B \rightarrow S_B: E_{R'}(g^{y'})$, 说明:

$$R' = H(g^{xy'})$$

(8) $B \rightarrow A: E_b$, 说明:

$$b \in Z_p^*, E_b = g^b \parallel MAC_k(g^b)$$

B 计算 $sk = H(ID_A \parallel ID_B \parallel g^a \parallel g^b \parallel g^{ab})$, A 收到 E_b 之后, 通过计算生成一个相同的会话密钥:

$$sk = H(ID_A \parallel ID_B \parallel g^a \parallel g^b \parallel g^{ab})$$

该协议基于离散对数求解的困难性假设, 被称为一个可证明安全的 C2C-PAKE 协议, 然而, 不久后被指出 EC2C-PAKE 可能受到口令泄露伪造等攻击。

3 跨域 C2C-PAKE 协议的安全模型

本文沿用 Bellare 等人提出的 BRP 模型, 在文献[3, 5]的基础上进行改进。

3.1 通信模型

令 A, B 表示不同域中的 2 个用户, 他们分别与各自所属域中的服务器 S_A 和 S_B 共享口令 pw_A 和 pw_B 。所有用户的口令都是从同一个服从 D_{pw} 分布的小字典 D 中选取的。本文假定服务器是被动的, 不会主动伪装自己域中的用户发起攻击。每次协议的执行都看成一个实例(Instance), 称为预言机(Oracle), 记为 Π_i^j (协议参与方 U_i (用户或者服务器) 的第 j 个实例), 一个跨域 C2C-PAKE 协议是在 A, B, S_A, S_B 4 个参与方实例间交互的协议。协议运行后, A 和 B 间建立起一个会话密钥 sk , 并都拥有了会话标志符 sid 以及伙伴标志符 pid , 其中拥有相同 pid 的实例在会话中互相传递消息。假定攻击者 E 可以控制除服务器间的私有信道以外的整个通信环境, 并且可以发起多个协议实例的并行运行。在协议运行期间, 协议参与方和攻击者之间的交互仅通过 Oracle 询问来实现, 这些 Oracle 询问刻画了实际攻击中攻击者的能力。攻击者 E 可以发起的询问如下:

(1) $Send(\Pi_i^j, m)$: 这种询问刻画了对用户的主动攻击, 攻击者发送一个消息 m 给用户实例 U_i (用户或服务器), Π_i^j 将会按协议的规范执行, 并响应相关的回答, 若成功执行协议, 结果是攻击者可以得到 U_i 的 sid 和 pid 。

(2) $Reveal(\Pi_i^j)$: 这个询问刻画的是用户间会话密钥的泄漏。仅当 Π_i^j 成功完成协议并拥有会话密钥 sk_i , 这个询问才有效并且返回给攻击者此会话密钥。

(3) $Corrupt(\Pi_i^j)$: 这个询问刻画的是对用户的一种主动攻击, 允许攻击者 A 随意 $Corrupt$ 合法的参与方。此询问的结果是攻击者可以得到被 $Corrupt$ 掉的参与方的口令, 如果是强 $Corrupt$ 查询, 攻击者还能得到此参与方的内部状态。本文主要考虑弱 $Corrupt$ 询问。

(4) $Execute(A, B, S_A, S_B)$: 这种询问刻画的是被动攻击, 攻击者通过窃听可以访问参与方实例 A 和 B 之间以及它们分别与服务器之间的真实运行。这个询问的结果是攻击者得到真实协议运行时参与方之间交换的消息。

(5) $Test(\Pi_i^j)$: 若 Π_i^j 已成功执行协议, 并拥有了一个会话密钥 sk_i , 此查询的操作为: 首先在第 1 次进行此询问前秘密选取随机比特 b , 如果 $b=0$, 返回用户实例持有的会话密钥 sk_i ; 如果 $b=1$, 返回一个与此用户实例持有的会话密钥同等长度的随机数, 这个询问主要用来度量一个用户实例的会话

密钥的语义安全性。由于为攻击者增加了 $Corrupt$ 询问能力, 因此需要重新定义模型中所用到的安全概念。

伙伴关系(partnering): 如果满足下面的 3 个条件, 称 2 个用户实例 U_1^i 和 U_2^j 是伙伴:

- (1) U_1^i 和 U_2^j 同时接受;
- (2) U_1^i 和 U_2^j 共享同样的会话标志符 sid ;
- (3) 当且仅当伙伴身份分别是对方时, U_1^i 和 U_2^j 才接受。

新鲜性(freshness): 协议运行后, 称一个 Π_i^j 是新鲜的(或者持有一个新鲜的会话密钥), 当且仅当:

- (1) U_1^i 已经接受, 无论是否存在一个伙伴 U_2^j ;
- (2) 攻击者未对 U_1^i 的任何实例 Π_1^i 进行 $Reveal$ 查询;
- (3) 攻击者未对 U_1^i 的伙伴 U_2^j 的任何实例 Π_2^j 进行 $Reveal$ 查询;
- (4) 同一个会话中任何参与方被攻击者进行 $Test$ 查询之前都未被进行 $Corrupt$ 查询。

3.2 安全性定义

一个跨域 C2C-PAKE 协议被称为是安全的, 如果它满足下列 4 个条件:

- (1) 语义安全性: 对外部恶意攻击者来说, 会话密钥和随机数不可分。
- (2) 密钥保密性: 密钥具有前向安全性, 且能抗重放攻击, 服务器和非真正通信用户得不到用户间的会话密钥。
- (3) 对抗离线字典攻击、不可检测在线字典攻击。
- (4) 服务器与用户以及用户与用户之间的身份认证。

4 改进的跨域 C2C-PAKE 协议及其安全性分析

4.1 改进的跨域 C2C-PAKE 协议

本文通过引入公钥体制, 对 C2C-PAKE 协议改进如下, 其中, P_{S_i} 代表服务器 S_i 的公钥; S_{S_i} 代表服务器 S_i 的私钥。注: Step1 与 Step1' 代表 2 个步骤无先后关系, 其余类似。

Step1 $A \rightarrow S_A: M_A$

说明: A 随机选取 Z_p^* 中的随机数 x 和 N_A , 然后将 $M_A = E_{P_{S_A}}(pw_A, N_A, g^x, ID_A, ID_B)$ 发送给 S_A 。

Step1' $B \rightarrow S_B: M_B$

说明: B 随机选取 Z_p^* 中的随机数 y 和 N_B , 然后将 $M_B = E_{P_{S_B}}(pw_B, N_B, g^y, ID_B, ID_A)$ 发送给 S_B 。

Step2 $S_A \rightarrow S_B: Ticket_B$

说明: S_A 收到 A 的消息后用自己的私钥 S_{S_A} 解密 M_A , 并查询用户口令, 若验证通过, 则选取 Z_p^* 中的随机数 r , 然后计算并发送 $Ticket_B = E_{P_{S_B}}(E_{S_{S_A}}(g^{xr}, ID_A, ID_B, L))$ 给 S_B 。

Step2' $S_B \rightarrow S_A: Ticket_A$

说明: S_B 收到 B 的消息后用自己的私钥 S_{S_B} 解密 M_B , 并查询用户口令, 若验证通过, 则选取 Z_p^* 中的随机数 r' , 然后计算并给 S_A 发送 $Ticket_A = E_{P_{S_A}}(E_{S_{S_B}}(g^{y'r'}, ID_B, ID_A))$ 。

Step3 $S_A \rightarrow A: M_{S_A}$

说明: S_A 用 Step2 中解密消息 M_A 获得的 N_A , 求得 $R_{S_A} = H(pw_A) \oplus H(N_A + 1)$, 计算 $M_{S_A} = E_{R_{S_A}}(g^{y'r'} \oplus H(pw_A))$ 发送给 A 。

Step3' $S_B \rightarrow B: M_{S_B}$

说明： S_B 用 Step2' 中私钥 S_{S_B} 解密消息 M_B 获得的 N_B ，求得 $R_{S_B} = H(pw_B) \oplus H(N_B + 1)$ ，计算 $M_{S_B} = E_{R_{S_B}}(g^{xrr'} \oplus H(pw_B))$ 发送给 B 。

A 用自己的口令 pw_A 和之前选择的随机数 N_A 计算出 R_{S_A} ，然后用它解密 S_A 发送给他消息 M_{S_A} 得到 $g^{xrr'}$ ，结合自己的随机数 x ，计算 $sk = (g^{xrr'})^x = g^{xyrr'}$ ，同理， B 计算 $sk = (g^{xrr'})^y = g^{xyrr'}$ ，最后，双方用 sk 作为共同协商的会话密钥进行安全通信。

4.2 改进协议的安全性分析

(1) 语义安全性

因为服务器都用自己的私钥加密消息，再用对方的公钥加密密文，这就保证了服务器间的通信信道是私有的认证信道。因此，改进协议相对于外部敌手来说在 BRP 模型意义下是语义安全的。

(2) 密钥保密性

1) 前向安全性：若 E 窃取了 pw_A 和 pw_B ，由于他没有 S_A 和 S_B 的私钥，因此无法解密所截获的消息得到 g^x 或 g^y ，更无法计算出之前的会话密钥 $sk = g^{xyrr'}$ ，从而保证了协议的前向安全性。

2) 重放攻击：因为协议中的 x, y, r, r' 都是临时随机变量，所以 E 不能假冒任何一方发动重放攻击。

3) 恶意服务器攻击：安全模型中已假定服务器是被动的，他不会伪装自己域中用户进行攻击。假设 S_A 为恶意服务器，由于他无法得到其他域中用户的口令或其他服务器的私钥，因此无法解密 Step3 中的 M_{S_A} 或计算 Step2 中的 Ticket，不存在恶意服务器攻击。

(3) 对抗离线字典攻击、不可检测在线字典攻击

1) 离线字典攻击：对于不知道 pw_A 和 pw_B 的外部敌手，他想要得到 pw_A 和 pw_B ，但因为他无法获取 S_A 的私钥 S_{S_A} ，也就无法解密 M_A 进而得到 pw_A ；对于知道 pw_A (或 pw_B) 的内部敌手，因为他无法获取 S_B 的私钥 S_{S_B} ，所以无法解密 M_B 得到 pw_B 。

2) 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 M_A 发送给 S_A ，验证 pw'_A ，显然 pw'_A 和 S_A 存储的口令 pw_A 相符的概率几乎为 0， S_A 马上能检测到敌手对 A 的攻击。

(4) 服务器与用户以及用户与用户间的身份认证

易知用户用服务器的公钥加密用户口令和选取的随机数，同时服务器用用户的口令和用户选取的随机数加 1 的 hash 值加密用户的口令，这样就实现了服务器和用户间的身份认证。服务器间的信息是用自身私钥加密再用对方公钥加密密文而成，既向对方证明了自己的身份又保证只有对方才能看到密文，以此实现服务器间的身份认证。

5 结束语

本文提出一种改进的 C2C-PAKE 协议，结合了简单的口令认证、离散对数和公钥加密的高可靠等特点，并具有语义安全性、密钥保密性、前向安全性，能对抗重放攻击、恶意服务器攻击、离线字典攻击、不可检测在线字典攻击等常见攻击。通过服务器与用户的双向认证，该协议保证了传输数据的完整性和真实性，安全可靠地实现了跨域用户间的密钥协商与共享，为以后的跨域口令密钥交换协议的设计提供了参考。

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]//Proc. of ICICS'02. Berlin, Germany: Springer-Verlag, 2002.
- [2] Byun J W, Lee D H, Lim J. Efficient and Provably Secure Client-to-client Password-based Key Exchange Protocol[C]//Proc. of APWeb'06. Berlin, Germany: Springer-Verlag, 2006.
- [3] Byun J W, Lee D H, Lim J I. ECEC-PAKE: An Efficient Client-to-client Password-authenticated Key Agreement[J]. Information Sciences, 2007, 177(19): 3995-4013.
- [4] Yoneyama K, Ota H, Ohta K. Secure Cross-realm Client-to-client Password-based Authenticated Key Exchanged Against Undetectable On-line Dictionary Attacks[C]//Proc. of AAEECC'07. Berlin, Germany: Springer-Verlag, 2007.
- [5] Yin Yin, Li Bao. Secure Cross-realm C2C-PAKE Protocol[C]//Proc. of ACISP'06. Melbourne, Australia: [s. n.], 2006.
- [6] Phan R C W, Goi B. Cryptanalysis of Two Provably Secure C2C-PAKE Protocols[C]//Proc. of INDOCRYPT'06. Kolkata, India: [s. n.], 2006.
- [7] 卞仕柱, 王建东, 任勇军, 等. 强安全高效的认证密钥交换协议[J]. 计算机工程, 2010, 36(7): 136-138.

编辑 顾姣健

(上接第 161 页)

- [6] 胡江红, 张建新. 一个新的不可否认门限代理签名方案[J]. 兰州大学学报, 2008, 44(3): 77-80.
- [7] 陈海滨, 杨晓云, 梁中银, 等. 一种无证书的前向安全代理签名方案[J]. 计算机工程, 2010, 36(2): 156-157.
- [8] Shao Zuhua. Improvement of Efficient Proxy Signature Schemes Using Self-certified Public Keys[J]. Applied Mathematics and

Computation, 2005, 168(1): 222-234.

- [9] Hsu Chien-Lung, Wu Tzong-Sun. Self-certified Threshold Proxy Signature Schemes with Message Recovery, Nonrepudiation, and Traceability[J]. Applied Mathematics and Computation, 2005, 164(1): 201-225.

编辑 顾姣健