文章编号: 1673-1549(2011)01-0062-04

一种 PKI体系下的私钥安全存取方案

郑丽萍, 易　虹

(河南工业大学信息科学与工程学院, 郑州　450001)

摘　要: 针对私钥安全存取问题, 提出了一种私钥安全存取方案。该方案引入了私钥托管箱技术, 为私钥的集中管理和私钥的漫游提供了保证; 引入的门限技术避免了私钥托管箱单点服务失败造成私钥丢失的问题, 同时防范了私钥托管箱服务器系统内部的攻击; 采用加强口令的身份认证方案进一步为私钥访问和传输提供了安全保证。

关键词: 私钥; 托管箱; 门限技术; 强口令认证

中图分类号: TP309.7; TP391　　文献标识码: A

PKI(Public Key Infrastructure)技术是目前解决网络安全问题的一个有效途径, PKI利用公钥概念与技术[1]来实施和提供安全服务的基础设施。非对称密码体制是支撑 PKI安全技术的核心, 其主要特点是加密和解密使用不同的密钥。每个用户保存着一对密钥: 公钥和私钥。公钥是公开, 用作加密密钥; 而私钥是保密的, 需由用户自己保存, 用作解密密钥。如果私钥泄漏, 则整个的 PKI安全体系就会土崩瓦解。如何实现对私钥的安全存取, 同时又便于使用, 是 PKI系统最为关键的问题之一。

1　私钥安全存取方案

1.1　私钥安全存储系统原型

本文提出了一种私钥安全存取方案, 该方案的私钥存储借鉴了门限技术和私钥托管技术, 私钥采用密钥管理中心 KMC集中产生, 将私钥分成 n个共享份存储在 n个私钥托管箱中, 之后 KMC删除对应的私钥, 只保存用户口令[2-3]。用户身份认证是基于一个新的口令加强算法, 该算法通过客户端和多个服务器的交互增强用户口令, 重新组合来获得新的一组增强口令[4-5]。用户与多个加强服务器和私钥托管箱服务器交互认证后, k个私钥托管箱采用对应的加强码加密私钥片将其传送到客户端, 客户端解密获得用户私钥。私钥的安全存取系统架构如图 1所示。

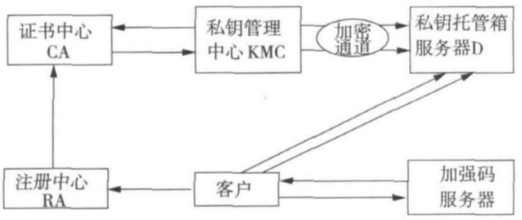

图 1　私钥的安全存取原型设计

1.2　用户注册

假设 Alice为 PKI系统的一个用户, A为 Alice的客户端代理, 用户注册的流程如图 2所示。

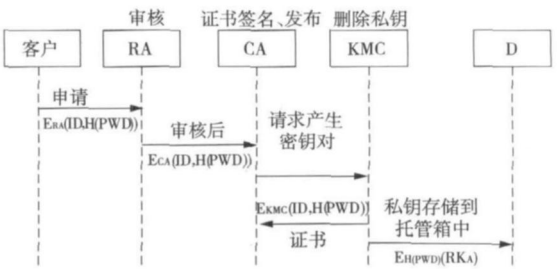

图 2　用户注册

(1) 用户 Alice向 RA注册, 申请证书。输入用户的 ID值 ID(A)和口令 PWD, 客户端计算 H(PWD)。

(2) A把申请信填好递交给 RA, 包括 ID(A)和 H(PWD), 信息用 RA的公钥加密。

(3) RA审核该信息, 审核通过后则把用户的证书

收稿日期: 2010-11-12

基金项目: 河南工业大学校科研基金资助项目 (08XJC008)

作者简介: 郑丽萍 (1976-), 女, 河南焦作人, 讲师, 硕士, 主要从事信息安全方面的研究。

© 1994-2011 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

申请信息 ID(A)和 H(PWD)用 RA 的私钥签名, 再用 CA的公钥加密后发送给 CA。

(4) CA接到证书申请后, 对待签发的证书(其中公钥信息域为空)及 ID(A)和 H(PWD)进行签名, 再用 KMC的公钥加密后发给 KMC, 请求 KMC产生密钥对。

(5) KMC用其私钥解密, 并验证 CA的签名, 得到证书及相关信息, 从密钥池中随机选一个密钥对, 公钥记为 PK_A、私钥记为 RK_A, 并用 H(PWD)进行加密 RK_A, 即 EH(PWD)(RK_A)。

(6) KMC 把刚分配给该请求的公钥与证书传给 CA, CA就可以发布证书了。

(7) CA发布证书, 并以某种方式通知用户。

1.3 用户私钥的安全存储

将在注册阶段产生的加密私钥 EH(PWD)(RK_A)采用门限方法产生 n个共享部分, 分别存储到 n个私钥托管箱 D1, D2, …, Dn中, 同时 KMC中对应的加密私钥 EH(PWD)(RK_A)删除。采用(k, n)门限算法, 利用其中 k个私钥托管箱中私钥片可以重组加密私钥 EH(PWD)(RK_A)。为了便于描述, 假设 n= 4, k= 2, 即将加密私钥 EH(PWD)(RK_A)采用门限方法产生 4个共享部分, 分别存储到私钥托管箱 D1、D2、D3、D4, 只要从 2个私钥托管箱获得私钥片, 即可组成完整的加密私钥 EH(PWD)(RK_A)。为了安全, n和 k也可以选择适当大的值。

1.4 私钥安全分发过程

当用户需要用私钥解密信息, 或进行签名时, 需要从 n个私钥托管箱中任选 k个, 获取 k个私钥片进行重组成为完整的私钥。私钥的安全分发如图 3所示。

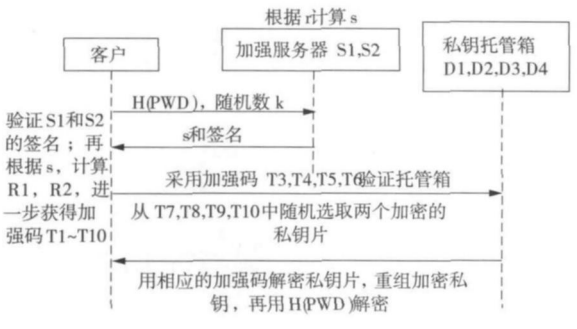

图 3　私钥的安全分发

(1) 用户 Alice通过代理客户端 H(PWD)和一个随机数 m计算 r1和 r2, 并传送口令给加强服务器。口令强化服务器根据 r1和 r2计算 s1和 s2的值, 并用其对应的私钥签名后传送给客户端。客户端验证 S1和 S2的签名, 并根据 s1和 s2值计算强化口令 R1和 R2。

(2) 代理客户端 A根据强化口令 R1、R2计算出强化安全码 T1、T2、T3、T4、T5、T6、T7、T8、T9和 T10。服务器发送各自的验证码 T1和 T2到客户端, 客户端对口令增强服务器 S1、S2进行身份认证码; 私钥托管箱服务器发送各自的验证码 T3、T4、T5和 T6到客户端, 客户端对其进行身份认证。同时, 加强码服务器 S1和 S2以及私钥托管箱服务器 D1、D2、D3和 D4对用户上传的加强码 T1– T6对用户身份进行验证。

(3) 用户加强安全码 T1– T6通过口令增强服务器和私钥托管箱服务器验证后, 对于不合法的用户给予拒绝, 记录相关信息, 防止其进一步模仿登陆。对于合法的用户, 根据门限技术和 n= 4, k= 2的假设, 从 4个私钥托管箱 D1– D4中选择 2个私钥托管箱中的加密私钥片。

(4) 利用选中的私钥托管箱对应的加强码 Ti和 Tj(7< = i, j< = 10)对加密的私钥片进一步进行加密 Ei(EH(PWD)(RK_{Ai}))和 Ej(EH(PWD)(RK_{Aj})), 通过安全通道传送到客户端 A。同时私钥托管箱服务器删除加密私钥片的加强码 T7– T10, 即私钥托管箱服务器不保存, 每次使用时在客户端生成。

(5) 客户端利用加强码 Ti和 Tj解密加密私钥片 Ei(EH(PWD)(RK_{Ai}))和 Ej(EH(PWD)(RK_{Aj})), 重新组合生成完整的用户口令加密的私钥 EH(PWD)(RK_A)。

(6) 客户端 A根据用户口令 PWD计算出相应的 H(PWD), 解密加密私钥 EH(PWD)(RK_A), 即可获得用户 Alice自己的私钥。

1.5 私钥的更新与归档

用户的私钥到期时, 可向私钥托管箱提出更新私钥申请。首先用户与加强口令服务器和私钥托管箱进行双方认证, 然后用户提出更新私钥申清, 通过 KMC实现相应的更新与归档处理。过期的私钥并不能丢弃不要, 因为过去的加密文件需要其解密, 因此, 过期的私钥需要长期保存。为了保存过期的私钥, 在私钥托管箱中专门设置一个历史档案库, 保存对应私钥托管箱中的过期私钥片, 其详细流程如图 4所示。

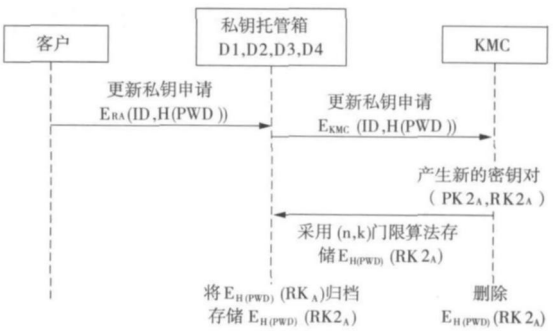

图 4　私钥更新与归档

(1) 用户 Alice与加强口令服务器和私钥托管箱服务器进行交互认证后, 提出申请更新私钥。

(2) 私钥托管箱服务器用 KMC的公钥加密私钥更新申请, 并将其提交给 KMC。

© 1994-2011 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

(3) KMC利用自己的私钥解密私钥更新申请,从密钥池中重新选取一个密钥对 PK_{2A} 和 RK_{2A},并通过 H(PWD)加密,产生加密私钥 EH(PWD)(RK_{2A}),并用KMC的私钥签名加密私钥 EH(PWD)(RK_{2A})。

(4) 与用户注册相同,将加密私钥 EH(PWD)(RK_{2A})的私钥根据(n, k)门限技术分片存入相应的私钥托管箱中,KMC中对应的加密私钥 EH(PWD)(RK_{2A})删除。

(5) 私钥托管箱将过时的加密私钥 EH(PWD)(RK_{2A})的私钥片加上时间戳,存入私钥托管箱中的历史档案库中,以备解密私钥更新前的文件。

1.6 用户口令的更新

用户与加强口令服务器和私钥托管箱服务器双方进行交叉认证后,可向私钥托管箱提出更新用户口令的申请,其详细流程如图 5所示。

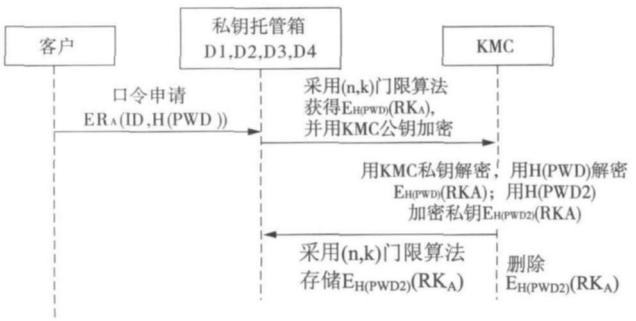

图 5 用户口令更新

(1) 用户 Alice首先利用原始口令 PWD与加强口令服务器和私钥托管箱服务器进行交叉认证。

(2) 认证通过后,用户 Alice向私钥托管箱提出更新用户口令申请。

(3) 私钥托管箱根据门限技术从 k个私钥托管箱中获取加密私钥片,传送到 KMC。

(4) KMC根据用户 Alice的 H(PWD)解密 EH(PWD)(RK_A),获得 RK_A。

(5) KMC根据用户输入新的口令 PWD2,计算 H(PWD2),并用 H(PWD2)加密 RK_A,获得加密私钥 EH(PWD)(RK_A)。

(6) 与用户注册相同,将加密私钥 EH(PWD)(RK_A)通过门限技术分片存入相应的私钥托管箱中,覆盖原来的 EH(PWD)(RK_A)私钥片。KMC中对应的加密私钥 EH(PWD)(RK_A)删除。

2 私钥存取方案的安全性分析

2.1 KMC的安全性

KMC负责用户注册,管理用户的私钥,但是当私钥采用 H(PWD)加密存储到多个私钥托管箱后,KMC便删除了被加密的私钥 EH(PWD)(RK_A)。因此 KMC仅仅存储了用户口令的单向函数 H(PWD)的值,并没有存储用户的私钥,因此,不可能泄露用户的私钥。

2.2 门限方案的引入

门限方案的引入可以避免单一服务接点的失败。当某些私钥托管箱受到攻击和损坏时,只要能够保证 k个私钥托管箱正常工作,便可重组完整的私钥,用户的私钥将能保证正常使用。

门限方案技术的另一个特色是抵制内部犯罪。门限系统消除了权力集中,它的权力分散不同于一般的权力分散,是彻底的权力分散:如果得不到 k个共享部分,计算加密的私钥是完全办不到;同样,即使攻击者妥协了 k-1个私钥托管箱服务器,得到 k-1份的共享私钥片,攻击者也无法预测加密的私钥。所以,这种门限方案可以有效的增加系统的弹性,保证用户私钥的安全性。

2.3 私钥托管箱的引入

本文提出的私钥存储方案引入了私钥托管箱方案。私钥托管箱把用户私钥的安全管理、私钥备份、私钥恢复,以及私钥更新和存档功能有机地结合在一起,从而可以极大地方便 PKI用户的使用。

私钥托管箱可以满足用户在多个地点和任意时间使用私钥的需求。随着网络和移动电话的发展,人们获取信息的时间和地点随机性增加,基于网络的应用对移动性的要求已经成为基本需求。网络私钥托管箱以网络为数据出口,可自然地与各种网络应用衔接,保证漫游用户的需要[6]。

2.4 加强口令的身份交叉认证方案的安全性

本方案通过用户的简单口令与强口令服务器的交换,获得加强码,并与多个不同的服务器合作完成用户身份的认证,大大增强了用户身份认证时的安全性。

(1)用户合法,S1和 S2不合法。

客户端与假冒的加强口令服务器 S1′和 S2′交互,S1′和 S2′服务器可以根据用户的 H(PWD)和随机数 m计算 s1′和 s2′,由于 S1′和 S2′没有合法 S1和 S2的私钥,所以没有办法进行签名,或者说客户端可以通过其签名验证加强口令服务器的真实身份。

(2) S1和 S2合法,用户不合法

攻击者假冒用户与合法的加强口令服务器 S1和 S2进行交互,S1和 S2根据假冒用户的口令 H(PWD′)计算出加强码 T1′-T10′。假冒用户利用计算出的加强码 T1′和 T2′与加强口令服务器 S1和 S2交互进行身份认证,S1和 S2将 T1′和 T2′与用户注册时存储的 T1和 T2进行比较。由于用户不合法,所以不匹配。同理,利用加强码 T3′-T6′与私钥托管箱服务器 T3-T6进行比较,由于用户不合法,也不匹配。

© 1994-2011 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

(3) S1和 S2合法, 用户合法, 私钥托管箱服务器 D1、D2、D3和 D4不合法攻击者为了获取加密私钥片的加强码 T7- T10, 冒充私钥托管箱服务器 D1、D2、D3和 D4。由于用户第一次注册时, 生成了私钥托管箱服务器的认证码 T3- T6, 因此在用户传送加密私钥片的加强码 T7- T10之前, 先进行了私钥托管箱服务器的验证。攻击者由于没有加密私钥片的加强码 T3- T6, 所以无法获得用户对其的认证。

2.5 客户端使用过程中的安全性

合法用户和客户端需要使用私钥时, 根据加强码 T1和 T2的值, 用户与加强口令服务器进行交叉认证; 根据加强码 T3、T4、T5和 T6的值, 用户与私钥托管箱服务器进行交叉认证。通过认证后, 从 2个私钥托管箱中下载加密的私钥片, 在客户端采用对应的解密码 T7- T10解密, 组成完整的加密私钥 $EH(PWD)(RK_A)$, 最后用单项哈希函数 H(PWD)解密, 获得用户的私钥, 存放在客户端机器的内存中某个位置以便使用, 当用户使用后退出客户端时, 客户端自动安全地清除内存中私钥的相关信息。由于私钥不保存到客户端机器的硬盘中, 使得私钥的相关信息不会遗留在客户端机器中, 从而减少了私钥被窃取的可能性。

3 方案仿真实验

为了测试本文中提出的私钥存取方案的性能, 实现了一个基于该方案的 PKI系统下电子邮件仿真系统。该系统中电子邮件服务器端采用 Windows Server 2005搭建, 注册中心 RA和密钥生成中心 KMC、8个私钥托管服务器、4个加强码服务器采用的开发工具和开发包是 OpenSSL和 VC。发送和接受电子邮件过程中设计以下角色: 发送电子邮件的用户 Alice@key.com, 接收电子邮件的用户 Bob@key.com, 私钥托管服务器端 Di(i= 1, 2…8), 加强口令服务器端 Si(i= 1, …4)。

首先用户 Alice和 Bob通过客户端进行注册申请私钥和证书, 门限技术将私钥 (8, 5)按照 4次多项式将密码分成 8份并加密存储在 8个私钥托管箱中。之后 Alice采用 Bob的公钥加密发给 Bob的电子邮件, Bob通过注册时的口令向加强码服务器进行交叉身份认证后, 获取自己的私钥, 解密电子邮件。在进行系统测试时, 妥协 4个私钥托管箱, 私钥重组任然正常提供; 假冒用户和加强码服务器都不能获得合法的私钥, 与其它私钥分配方案相比, 该方案的安全性更强。

4 结束语

本文所提出的基于私钥托管技术的私钥安全存储方案为私钥的集中管理和漫游提供了保证; 在私钥存储中利用门限技术防范了系统内部攻击, 同时避免了单点服务失败造成私钥的丢失; 加强口令的身份认证方案为私钥访问和传输提供了安全保证, 从而保证了里在 PKI体系下的私钥安全存取。

参考文献:

[1] 李天增, 王 瑜. RSA密码体制的安全性分析和算法实现 [J]. 四川理工学院学报: 自然科学版, 2009, 22(1): 41-43.

[2] 柴争义, 白 浩, 张浩军. 一种 CA私钥的容侵保护机制 [J]. 计算机应用. 2008, 28(4): 910-914.

[3] 黄 河, 王亚弟, 韩继红, 等. 一种基于门限担保证书的分布式私钥元分配方案 [J]. 计算机应用, 2008, 28(6): 1385-1391.

[4] 杨宗凯, 谢海涛, 程文青, 等. 一种基于身份的分布式会议密钥分发方案 [J]. 计算机科学, 2007, 34(1): 115-116.

[5] 王 滨, 张远洋. 一次性口令认证方案的分析与改进 [J]. 计算机工程, 2006, 32(14): 149-150.

[6] 冯 宾, 刘曙光, 李小兵. 对 PKI私钥漫游的研究 [J]. 微电子学与计算机, 2005, 22(11): 79-81.

An Accessing and Storing Private Key Security Scheme Under PKI

ZHENG Li-ping, YIH ong

(Department of Information Science and Technology, Henan University of Technology, Zhengzhou 450001, China)

Abstract For private key security issues, an accessing and storing the private key security scheme is advanced. This scheme introduces private key safe technology, which makes it possible to manage and roam private key. This scheme introduces threshod technology, which avoids private key losing caused by the failure of single point of service, and is also against attacking internally by private key safes system. This strengthening password algorithm about user authentication provides security guarantees private key security on the procedure of accessing and transmission.

Key words private key; custody case; threshod technology; strengthening password authentication

© 1994-2011 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net