

文章编号:1001-9081(2006)11-2589-03

多证书系统中安全登录中间件的研究与设计

王春新,徐孟春,殷石昌

(信息工程大学 信息工程学院,河南 郑州 450002)

(chxinwang@163.com)

摘 要:研究了公开密钥基础设施和特权管理基础设施的特点,设计了两种证书的实现格式,并在此基础上设计了一个基于代理证书的安全登录中间件。通过对访问域内证书的合成实现单点登录和基于属性证书的授权,解决了多证书系统中的单点登录问题。

关键词:公钥基础设施;特权管理基础设施;单点登录;中间件;多证书系统

中图分类号: TP393.08 **文献标识码:** A

Research and design of safety sign-on middleware based on multi-certificate

WANG Chun-xin, XU Meng-chun, YIN Shi-chang

(College of Information Engineering, Information Engineering University, Zhengzhou Henan 450002, China)

Abstract: Based on the research of the characteristics of Public Key Infrastructure (PKI) / Privilege Management Infrastructure (PMI), the formats of two certificate were designed, and a safety sign-on middleware based on proxy certificate was developed. It can achieve single sign-on (SSO) and authorization based on attributes certificate with the composed certificate in usable field. It solves the SSO problem in the multi-certificate system.

Key words: PKI; PMI; single sign-on(SSO); middleware; multi-certificate

0 引言

公钥基础设施(Public Key Infrastructure, PKI)已经成为网络应用中不可缺少的安全支撑系统。它通过方便灵活的密钥和证书管理方式,提供了在线身份认证的有效手段,为访问控制、抗抵赖、保密性等安全机制在系统的实施奠定了基础。

特权管理基础设施(Privilege Management Infrastructure, PMI)是建立在 PKI 提供的可信任的身份认证服务的基础上的,以属性证书的形式来实现授权的管理。PMI 体系和模型的核心内容是实现属性证书的有效管理,包括属性证书的产生、使用、吊销、失效等。

就如现实生活一样,网络中的每个用户都有自己的属性。属性决定了用户的权力。PMI 的最终目标就是提供一种有效的体系结构来管理用户的属性。然而,随着网络的发展和细分,现实中不同的身份属性导致了用户在不同应用中拥有不同的权限,为了各自的安全,各个应用部门分别设立不同的属性证书颁发机构,从而形成多证书共存共用的网络环境。证书的增多带来了一系列新的问题,特别是增加了实现单点登录的难度,针对这种情况,我们设计了安全登录中间件,实现单点登录和基于属性证书的授权。本文阐述了安全登录中间件中认证和授权部分的设计思想和实现方式。

1 PKI 与 PMI

1.1 PKI 技术

PKI 是一种安全技术,它由公开密钥密码技术、数字证书、证书发放机构和关于公开密钥的安全策略等共同组成。

PKI 是利用公钥技术实现安全的一种体系,是一种基础设施。

PKI 主要包括四个部分:X. 509 格式的证书和证书废除列表 CRL, CA 操作协议,CA 管理协议,CA 政策制定。一个完整的 PKI 系统一般由如下几个部分组成:

数字证书 PKI 系统中的最基本元素,所有安全实现都要以数字证书为基础;

证书颁发机构(Certificate Authority, CA) 是 PKI 中非常重要的角色,它是一个可信的第三方权威机构,具有验证用户证书申请、签发证书、定期发布证书失效列表、响应用户证书吊销请求等功能,同时还可为用户存储证书备份、进行密钥恢复;

证书注册机构(Registration Authority, RA) 相当于 CA 的一个代理机构,帮助 CA 完成证书申请的登记和审计工作,并将验证过的证书申请交由 CA 签发;

目录服务 用于存储证书以使用户查询,同时发布证书失效列表等;

证书策略 一个 PKI 系统可以根据实际应用的具体需要制定不同的证书策略,包括证书扩展项的选用、CA 的部署、证书路径长度等。

1.2 PMI 技术

PKI 主要解决身份认证,尽管可以在公钥证书中加入授权信息,但这样做存在两个问题,一是授权信息有效期通常比公钥证书有效期短得多;二是公钥证书的颁发机构 CA 不一定是掌握用户授权信息的权威部门,因此,在 2000 年的 X.509 v4 中,提出了权限管理基础设施的概念,定义了一种短生存期的数字证书——属性证书(Attributes Certificate, AC)专门

收稿日期:2006-05-26;修订日期:2006-07-02

作者简介: 王春新(1975-),男,河南南阳人,硕士研究生,主要研究方向:计算机网络管理、电子政务; 徐孟春(1960-),男,河北唐山人,副教授,主要研究方向:计算机网络管理、电子政务; 殷石昌(1978-),男,云南石林人,硕士研究生,主要研究方向:计算机网络管理、电子政务。

用就是充当将证书中包含的主体公钥和主体身份信息绑定在一起的担保人。因为在网络环境中,往往需要多个证书颁发机构给不同的用户颁发标识证书,所以应考虑到多个 CA 的认证体系。每个站点可以按照本地的安全策略要求,自行决定可信任哪些 CA 颁发的证书,而不信任另一些 CA 颁发的证书。每个 CA 都将自己签发的标识证书放在一个在线的证书服务器中,以便用户验证和查询证书,为了实现单点登录,各个应用系统和主 LDAP 中建立映射,使某一时刻用户 A 拥有的证书集中在主 LDAP 中。

表 1 标识证书

版本号 V
证书序列号(每一个证书唯一的一个整数值, 由证书颁发机构产生) Sn
签名算法标识符(用于说明签发证书所使用的算法及相关参数) AI
颁发者名称(用于标识签发该证书的证书颁发机构的特定名称) CA
有效期(包括两个日期/时间值: Not Valid Before(不早于) 和 NotValid After(不晚于) TA
主体名称(标识拥有本证书的最终实体的特定名称) A
主体公钥信息(包含主体的公钥、算法标识符以及算法所使用的任何相关参数) Kp
颁发者唯一标识符(证书颁发者的唯一标识符) Issuer
主体唯一标识符(证书拥有者的唯一标识符) IDA
签名 SignCA CA 对[] 中 hash 值的签名

属性证书用于表明主体具有的属性。尽管它在结构上与标识证书类似,但却提供不同的功能。属性证书不包含实体的公钥,它主要用于将一个实体与系列属性绑定,这些属性指明了所有者的成员资格、角色、安全许可或者其他一些授权信息。

$$AC = \{ V, Sn, AI, CA, TA, A, Aa, Issuer, [hash(V, Sn, AI, CA, TA, A, Aa, Issuer)] SignCA \}$$

表 2 属性证书

版本号 V
属性证书序列号 Sn
签名算法标识符 AI
颁发者名称(颁发者标识证书序列号) CA
证书有效期 TA
属性所有者名称(所有者标识证书的序列号与签发者) A
属性 Aa
颁发者唯一标识符 Issuer
签名 SignCA CA 对[] 中 hash 值的签名

代理证书包含了被代理用户的标识证书和属性证书中的有关信息。以原标识证书格式为蓝本,增加一扩展项,将属性证书颁发机构及属性信息以代码形式加入扩展项内。代理证书由中心目录服务器的信任源点 SOA 颁发,因为代理证书中包含了代理所具有的基本身份、属性及属性值等信息,所以资源的访问控制决策者根据代理证书就可以做出授权决策。

代理证书的结构和格式与前面描述的标识证书的结构和格式基本类似,其工作实质是一 X509 v4 版的证书,但它在身份认证上实现了与属性证书同寿命的优点,在属性授权层面上实现了集中应用域内所有授权信息的优点,其结构如下:

$$PC = \{ V, Sn, AI, CA, TA, PA, PKp, Issuer, IDPA, other, [hash(V, Sn, AI, CA, TA, PA, PKp, Issure, IDPA, other)] SignCA \}$$

表 3 代理证书

版本号 V
证书序列号(每一个证书唯一的一个整数值, 由证书颁发机构产生) Sn
签名算法标识符(用于说明签发证书所使用的算法及相关参数) AI
颁发者名称(用于标识签发该证书的证书颁发机构的特定名称) CA
有效期(包括两个日期/时间值: Not Valid Before(不早于) 和 NotValid After(不晚于) TA
主体名称(标识拥有本证书的最终实体的特定名称) PA
主体公钥信息(包含主体的公钥、算法标识符以及算法所使用的任何相关参数) PKp
颁发者唯一标识符(证书颁发者的唯一标识符) Issuer
主体唯一标识符(证书拥有者的唯一标识符) IDPA
扩展项(包括密钥和策略信息、颁发者属性以及证书路径限制等) other
签名 SignCA CA 对[] 中 hash 值的签名

标识证书及属性证书的申请过程为:

- 1) 用户产生自己的 RSA 公钥、私钥对,将公钥 $P = (e, n)$ 以及其他身份信息提交给注册机构(Registration Authority, RA)。
- 2) 注册机构审核用户的身份信息,通过后继续,否则停止。
- 3) CA 根据用户身份信息和其公钥 P 生成用户证书,并将该证书返回给 RA,同时将该证书发布到目录服务器上。
- 4) RA 通过在线或离线的方式将证书返回给用户。

代理证书申请过程:

- 1) 用户首先用标识证书和属性证书登录,调用登录中间件,在主 LDAP 上获得身份认可,并获取用户的公钥。
- 2) 中间件向 CA 提交生成代理证书的信息,CA 根据用户信息和公钥生成临时的代理证书,并将证书返回给中间件,同时将代理证书放入主 LDAP 的特定区域。
- 3) 中间件负责完成用户需要的系统登录,登录过程结束时中间件负责删除主 LDAP 上临时证书存放区域的信息,并将登录过程的有关信息写入审计部分备案。

2.3 登录中间件的会话过程

完整的委托授权与撤销会话过程(如图 4)如下:

- 1) 用户向应用系统 1 发出登录请求,第 1 次登录整个应用域。
- 2) 应用系统访问控制接口调用中间件,将用户登录信息提交中间件。
- 3) 中间件收到登录请求后,首先进行身份认证,查找用户所拥有的在时间有效期内所有证书,确认用户的应用域内拥有的权限。
- 4) 中间件根据返回的结果生成代理证书 PC,自动产生对于整个访问域有效的唯一标识 PC_ID,并提取所有属性证书的权限,在 PC 的 other 项中上填写权限信息等。
- 中间件同时将登录代理和代理证书写入主 LDAP 的临时证书区域,任何应用系统对登录中间件的调用均先查询该区域,以验证用户是否是在应用系统内第一次登录,如果该区域有用户的代理证书,则表明用户已经在其他应用系统登录,登录新的应用系统只需调用代理证书即可。
- 5) 中间件将授权信息返回应用系统 1。
- 6) 应用系统 1 根据权限返回用户请求的操作结果。
- 7) 用户登录访问有效域内的其他应用系统。
- 8) 应用系统自动调用安全登录中间件。

- [2] ZHANG K. Threshold proxy signature schemes[A]. 1997 Information Security Workshop[C]. Japan, 1997. 191 – 197.
- [3] ZHANG K. Nonrepudiable proxy signature schemes based on discrete logarithm problem[EB/OL]. <http://citeseer.nj.nec.com/360090.html>, 1997.
- [4] SUN HM. Design of time-stamped proxy signatures with traceable receivers[J]. IEE Proceedings of Computers & Digital Techniques, 2000, 147(6): 462 – 466.
- [5] LIN WD, JAN JK. A security personal learning tools using a proxy blind signature scheme[A]. Proceedings of International Conference on Chinese Language Computing[C]. Illinois, USA, 2000, 273 – 277.
- [6] YI LJ, BAI GQ, XIAO GZ. Proxy multi-signature scheme: a new type of proxy signature scheme[J]. Electron Letters, 2000, 36(6): 527 – 528.
- [7] HWANG SJ, SHI CH. A simple multi-proxy signature scheme[A]. Proceedings of the Tenth National Conference on Information Security[C]. Hualien(Taiwan China), 2000. 134 – 138.
- [8] LEE B, KIM H, KIM K. Strong proxy signature and its application[A]. ACISP 2001[C], 2001. 603 – 608.
- [9] PARK HU, LEE IY. A digital nominative proxy signature scheme for mobile communication information[A]. ICICS 2001, LNCS 2229[C]. Berlin: Springer-Verlag, 2001. 451 – 455.
- [10] SHUM K, WEI KW. A strong proxy signature scheme with proxy signer privacy protection[A]. WETICE 2002[C], 2002. 55 – 56.
- [11] WANG HX, PIEPRZYK J. Efficient one - time proxy signatures[A]. ASIACRYPT2003, LNCS 2894[C]. Berlin: Springer-Verlag, 2003. 507 – 522.
- [12] ZHANG FG, KIM K. Efficient ID-based blind signature and proxy signature from bilinear parings[A]. ACISP 2003, LNCS 2727[C]. Berlin: Springer-Verlag, 2003. 312 – 323.
- [13] WANG GL. Designated - verifier proxy signatures for e - commerce[A]. IEEE 2004 International Conference on Multimedia and Expo[C], 2004.
- [14] HWANG SJ, CHEN CC. A new multi-proxy multi-signature scheme[A]. 2001 National Computer Symposium: Information Security[C], 2001. F019 – F026.
- [15] LI X, CHEN K, SUN L. Certificateless signature and proxy signature schemes from bilinear pairings[J]. Lithuanian Mathematical Journal, 2005, 45(1): 76 – 83.
- [16] CHAUM D, VAN ANTWERPEN H. Undeniable signatures[A]. CRYPTO1989, LNCS 435[C]. Berlin: Springer-Verlag, 1989. 212 – 216.
- [17] CHAUM D. Zero-knowledge undeniable signatures[A]. EUROCRYPT 1990, LNCS 473[C]. Berlin: Springer-Verlag, 1991. 458 – 464.
- [18] BOYAR J, CHAUM D, DAMGARD I, *et al.* Convertible undeniable signatures[A]. CRYPTO 1990, LNCS 537[C]. Berlin: Springer-Verlag, 1990. 189 – 208.
- [19] HARN L, YANG S. Group-oriented undeniable signature schemes without the assistance of a mutually trusted party[A]. AUSCRYPT 1992, LNCS 718[C]. Berlin: Springer-Verlag, 1993. 133 – 142.
- [20] CHAUM D. Designated confirmer signatures[A]. EUROCRYPT 1994, LNCS 950[C]. Berlin: Springer-Verlag, 1994. 86 – 89.
- [21] SAKURAI K, YAMANE Y. Blind decoding, blind undeniable signatures, and their applications to privacy protection[A]. Information Hiding 1996, LNCS 1174[C]. Berlin: Springer-Verlag, 1996. 257 – 264.
- [22] WANG G, QING S, WANG M, *et al.* Threshold undeniable RSA signature scheme[A]. ICICS 2001, LNCS 2229[C]. Berlin: Springer-Verlag, 2001. 221 – 232.
- [23] LIBERT B, QUISQUATER JJ. Identity based undeniable signatures[A]. CT-RSA 2004, LNCS 2964[C]. Berlin: Springer-Verlag, 2004. 112 – 125.
- [24] MONNERAT J, VAUDENAY S. Generic homomorphic undeniable signatures[A]. ASIACRYPT 2004, LNCS 3329[C]. Berlin: Springer-Verlag, 2004. 354 – 371.
- [25] MONNERAT J, VAUDENAY S. Undeniable signatures based on characters: how to sign with one bit[A]. PKC 2004, LNCS 2947[C]. Berlin: Springer-Verlag, 2004. 69 – 85.
- [26] LAGUILLAUMIE F, VERGNAUD D. Time - selective convertible undeniable signatures[A]. CT-RSA 2005, LNCS 3376[C]. Berlin: Springer-Verlag, 2005. 154 – 171.
- [27] KUROSAWA K, HENG SH. 3-move undeniable signature scheme[A]. EUROCRYPT 2005, LNCS 3494[C]. Berlin: Springer-Verlag, 2005. 181 – 197.
- [28] Mao W. Modern Cryptography: Theory and Practice[M]. New Jersey: Prentice Hall, 2003. 129.
- [29] SCHNORR CP. Efficient signature generation by smart cards[J]. Journal of Cryptography, 1991, 4(3): 161 – 174.
- [30] OGATA W, KUROSAWA K, HENG S H. The security of the FDH variant of chaum's undeniable signature scheme[A]. PKC 2005, LNCS 3386[C]. Berlin: Springer-Verlag, 2005. 328 – 345.

(上接第 2591 页)

9)安全中间件将其代理证书提交应用系统,应用系统验证其身份和授权信息,完成登录。中间件同时记录用户登录应用系统的个数。

10)应用系统返回用户请求的操作结果。

11)用户可以随时退出系统,当中间件登记的用户登录系统个数为 0 时,中间件自动删除用户代理和代理证书。

12)中间件将一次登录的相关信息存储在审计数据库中。

13)会话过程结束。

3 结语

本文针对目前 PKI/PMI 应用的现状,提出了在多证书系

统中实现单点登录和授权的实现方案,引入了安全登录中间件和代理证书的概念,使用代理证书实现动态权限的认证。这种新的框架能有效解决多证书系统中实现安全的单点登录问题。

参考文献:

- [1] 张志勇, 普杰信. 委托授权在 PMI 体系架构中的研究与应用[J]. 计算机工程, 2006, 32(5): 152 – 154.
- [2] 吴鹏, 王晓峻, 苏新宁. 基于 PKI/PMI 的 web 应用安全解决方案[J]. 计算机工程与应用, 2006, 42(6): 1 – 3.
- [3] 李婉婷. 基于 J2EE 的安全中间件的研究与实现[J]. 计算机工程与设计, 2005, 26(6): 1548 – 1550.