基于 PKI、PMI 的数字图书馆安全管理①

Security Managment for Data Library Based on PKI and PMI

梁　冰　(南华大学 图书馆 湖南 衡阳 421001)

廖湘柏　(南华大学 电气工程学院 湖南 衡阳 421001)

摘　要： 为了解决网络应用系统的安全问题，需要对应用系统进行一定的改造。论文探讨了基于 PKI 和 PMI 的数字图书馆安全易管理模型,提出基于 PKI 和 PMI 技术体系的访问控制方案。使用公钥证书实现对用户的身份认证，使用属性证书实现用户的授权访问。

关键词： PKI PMI 管理 图书馆 安全 模型

随着通信技术和信息存储技术的发展，未来图书馆的网络化、无纸化、虚拟化的特征也更加突出。同时大多数图书馆的门户 WEB 服务站点是独立于图书馆的管理系统开发的，馆内的采访、编目、咨询、阅览、流通等业务环节通过图书馆的管理系统连接,而外界用户能够访问该管理系统数据只有 OPEC,见图 1。

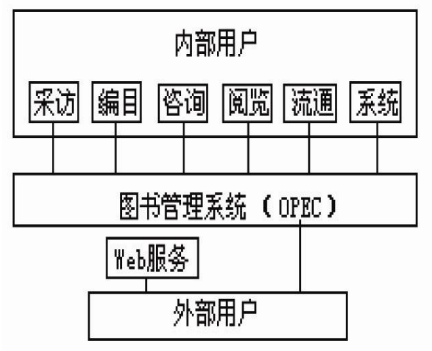


图 1　传统数字图书馆模型

由于共享数据很少，难以满足业务发展和管理的需求。需要一个能通过权限控制可以把内外用户统一在一起的系统，不仅可以管理数字资源，也可以管理印刷资源，同时又可以方便地向读者提供服务。防止不经许可非法获取资源的现象出现[1],保证资源访问过程的安全。系统还要能够了解访问用户的身份以及对应的访问权限，在对用户的请求进行访问决策的时候采用正确的控制策略。

1　PKI和PMI技术

1.1 PKI 技术

PKI(PublicKeyInfrastructure)公钥基础设施是提供公钥加密和数字签名服务的系统或平台，目的是通过自动管理密钥和证书，为用户建立起一个安全的网络运行环境，使用户可以在多种应用环境下方便的使用加密和数字签名技术，从而保证网上数据的机密性、完整性、有效性[2]。数据的机密性是指数据在传输过程中，不能被非授权者偷看，数据的完整性是指数据在传输过程中不能被非法篡改，数据的有效性是指数据不能被否认[3]。它由公开密钥密码技术、数字证书、证书发放机构(CA)和关于公开密钥的安全策略等基本成分共同组成。一个典型、完整、有效的 PKI 应用系统至少应具有以下部分：公钥密码证书管理、黑名单的发布和管理、密钥备份和恢复、密钥自动更新、历史密钥管理、支持交叉认证。

1.2　PMI 技术

PMI(Privilege Management Infrastructure)特权管理基础设施是基于属性证书(AC)的授权管理平台，它以 PKI 体系为基础，向所有应用提供与应用相关的授权服务。能够在用户请求服务时进行权限验证，

① 基金项目:湖南省教育厅高等学校科学研究项目(08C759);湖南省高校数字化图书馆专题特色库科研项目
收稿时间:2008-08-15

成为用户和服务提供者间的安全通信基础。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、使用和撤消等。2000 年颁发的 ITU-T X.509 V4 版对属性证书的格式进行了标准化[4]，属性证书主要包含有以下数据内容，见表 1。

表 1　X.509 属性证书的数据结构

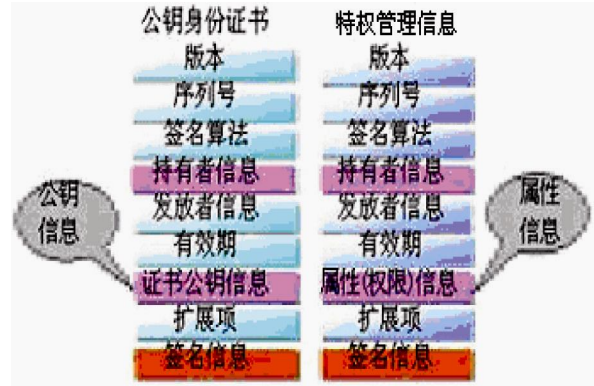
字段	注解
AttCertVersion	属性证书的版本
Holder	属性证书的持有者
Issuer	属性证书的签发者
SignatureAlgorithm	该属性证书的签名算法
SerialNumber	由属性机构分配的唯一的序列号
AttrCert Validity Period	该属性证书的有效期
Attributes	该证书一系列的权限属性
IssuerUniqueID	该证书发布者的唯一标识符
Extension	扩展项
SignatureValue	该证书的签名值

其中“Holder”最常用的方式是通过一个序列号指向该持有者的公钥证书,对持有者的身份进行认证。这种方法将 PKI 和 PMI 结合在一起。“Issuer”可以通过一个 GeneralName 来表示,里面可以包含发布者的 DNS 或 IP 等信息[5]。“Attributes”的实际意义和值不是权限而是 AA 赋予证书申请者的角色，其属性类型可以是服务认证信息、访问身份、组、角色、等级等等。X.509 标准既支持角色规范证书 RSC（Role Specification Certificate）又支持角色分配证书 RAC(Role Assignment Certificate)，“Extension”可以按照需要指向上级 AA 颁发者的 RSC 或 RAC，也可以标识实体是否有权授予其权限、指定证书撤消列表(CRL)的分发点或者指向和某角色对应的角色规范证书。

1.3 PKI 和 PMI 两者的特点和关系

首先，PKI 和 PMI 都是单位内部网安全运行的技术基石，是网络应用的核心安全技术。两者都有着相似的层次化授权管理结构、相同的证书字段内容和相同的信息绑定机制等。与 PKI 的 CA 中心相似，PMI 也存在一个发证中心，称为属性权威 AA，用来实现属性证书的产生、管理、存储、分发和撤消等功能。其次在应用中，两种有效证书和失效证书都可以存放在 LDAP 目录服务器，供验证方查询。

另一方面，从形式上看 PKI 和 PMI 有很多相似之处，但实质上有着本质的区别。PKI 是 PMI 实施的基础，PMI 是 PKI 应用的延伸。PKI 实现的是身份鉴别，证明“你是谁”。而 PMI 实现的是授权管理，能享受什么服务，控制“你能做什么”。两种证书的异同点见图 2 所示。



公钥证书类似于护照	属性证书类似于签证
公钥证书(护照)由统一机构发放，用于证明持有者身份。	属性证书(签证)可根据具体操作权限不同，由不同的机构发放，用于证明持有者权限。
公钥证书(护照)一般包含了持有者相对固定的信息，有效期较长。	属性证书(签证)包含了持有者的权限信息，可能会经常变化，有效期较短。

图 2　PKI 证书与 PMI 证书的区别

PKI 提供的证书在证实用户身份的基础上可以实现数字信封、数字签名、抗否认等应用，还可提供数据机密性、完整性的安全服务。

PMI 提供的证书主要用于为个性化应用服务建立一套与系统开发和管理无关的授权体系，实施应用整合。AA 通过管理属性证书的生命周期来实现权限生命周期的管理，也就是说 AC 的申请、签发、发布、注销、验证过程对应着传统的权限申请、产生、存储、撤消和使用的过程。在现实应用中，角色信息相对较稳定，并且角色与权限之间的关系相对固定，从而将用户的权限改变被简化成用户角色的更改，增强了灵活性和可操作性，减少了因人而设系统管理的重复工作。

同时使用上述两种不同的证书可以将“用户--权限”的关系转换为“用户--角色”与“角色--权限”的两个子关系。

2　双证管理的安全模型

2.1 模型结构

首先，建立相应的 CA 中心和 AA 中心。然后根据图书馆业务环节和外部用户访问的不同需求，划分访问群体为不同的角色，对各种角色赋以相应的权限，建立角色规范，颁发角色规范证书 RSC(Role Specification Certificate)。给各种服务设备和用户颁发公钥证书 PKC(Public Key Certificate)和角色分配证书 RAC(Role Assignment Certificate)。根据安全应用的需求建立 LDAP 服务器，身份、特权验证服务器，应用服务器和数据资源服务器，见图 3。

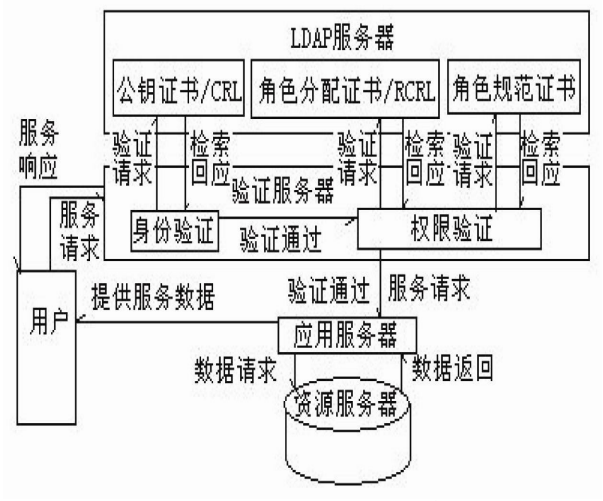


图 3　双证管理的安全模型

当用户需要得到应用服务时，必须先向验证服务器提交请求和 PKC 证书,进行访问身份认证，有些应用还会要求用户和服务器的双向验证。验证服务器收到请求和用户的 PKC 证书后，与存放 PKC 库的 LDAP 服务器进行服务器的双向认证，确保双方服务器身份的真实可靠。然后身份验证模块提交用户身份的验证请求，到 LDAP 服务器的 PKC 库和 CRL 库核实有用户数字签名的证书真实性和有效性。不符合要求的，验证服务器向用户发送拒绝服务消息。

身份验证通过后，验证服务器要进行权限验证过程。权限验证模块根据用户 PKC 中的 ID 属性，到 PMI 的 LDAP 服务器中匹配该用户的 RAC 证书和检索 RCRL，核实 RAC 证书的有效性，包括证书的有效期、是否被撤消、是否被篡改等。若存在上述情况之一，验证服务器拒绝服务。否则认可用户的角色，权限验证模块根据用户的角色再次到 PMI 的 LDAP 服务器检索角色规范 AC 库，根据角色规范证书 RSC 获取该用户访问权限的集合。

验证服务器的权限验证模块将用户提交的访问请求和访问权限集合相比较，如访问请求超出访问权限集合的范围，验证服务器拒绝服务。否则通知应用服务器从资源数据库中向用户提供所需要的数据信息。

2.2 模型应用

利用以上的模型结构，在图书馆区域外可以使用图书馆的管理系统进行业务管理。

使用 PKI 给用户和服务器发放的数字证书，通过 ssl 方式进行双向身份认证，保证数据的完整性。在用“tomcat”架构的验证服务器上，除了“jdbc”驱动程序要放在服务器的正确类路径下、证书的密钥文件“.keystore”要拷贝到 tomcat-home/conf 文件夹，同时需配置“server.xml”文件的以下相关内容。

```
……
<!-- Define a SSL Coyote HTTP/1.1 Connector on port 8443 -->
<Connector port="8443"
    maxThreads="150"
minSpareThreads="25" maxSpareThreads="75"
    enableLookups="false"
disableUploadTimeout="true"
    acceptCount="100"    debug="0"
scheme="https" secure="true"
    clientAuth="true"
    sslProtocol="TLS" keystoreFile=
“d:\tomcatSSL\tomcatserverkeystore.jks”。
    keystorePass="195602"/>
……
```

其中：“8443”是 ssl 连接的默认端口号，也可设置其它的端口号，“d:\tomcatSSL\tomcatserver keystore.jks”是密钥文件存储路径，“195602”是设置的密钥文件存储口令，服务测试为:https://IP: 8443。

用户权限的管理可根据图书馆内部的业务环节和外部用户访问的不同需求，将访问群体划分为采访、

(下转第 45 页)

(上接第 132 页)

编目、咨询、阅览、流通、客户 1、……等不同的角色，对各种角色赋以相应的权限，建立角色规范，颁发角色规范证书 RSC(Role Specification Certificate)。并给用户颁发相应的角色分配证书 RAC(Role Assignment Certificate)存储在 PMI 的 LDAP 服务器上提供特权验证服务查询。

3 应用分析

利用以上的双证管理模式，目前在小范围环境进行了部分功能的搭建和测试，采用 PMI 证书与 PKI 证书结合的方式，具备下列优势:

(1) 身份认证、数据签名采用 PKI 的公钥证书实现，相关平台、用户能够相互确认身份。

(2) 权限认证采用 PMI 的属性证书实现和保证。

(3) 不同的用户可以具备不同的访问权限。

(4) 不同的用户在同样的访问点可以具备不同的内容访问权限。

(5) 公钥证书和属性证书的分开管理可以使得两种证书的生命周期不相同，更加利于管理和贴合实际，利于用户的角色转变。

(6) 用户的授权(属性证书的发放)由平台进行，而权限(属性证书)的验证在不同的访问点处就可以完成。

但繁琐的验证过程可能造成系统负担。基础设施本身的安全确认及信息传输是整个系统安全的根本。利用失效的公钥证书假冒顶替和利用失效的属性证书进行访问攻击都是潜在的安全隐患，也是需进一步研究探讨的问题。

参考文献

1 张兰.数字资源存储管理系统研究.信息系统,2005,(2):199－201.

2 CarlisleAdamsSteveLloyd.冯登国译.公开密钥基础设施概念、标准和实施.北京:人民邮电出版社,2001.

3 关振胜.公钥基础设施PKI与认证机构CA.北京:电子工业出版社,2002.

4 Boeyen SX.509 (2000):4th Edition Overview of PKI & PMI Frameworks.http://www.entrust.com.

5 Chadwick DW, Otenko A. The PERMIS X.509 Role Based Privilege Management. SACMAT 2002. Monterey. CA. 2002:135－140.