基于PKI技术的学分制管理系统的安全解决方案*

刘 念** 李 涛 赵 奎 许 春

(四川大学计算机学院 成都 6100651)

【摘要】 针对目前学分制网络管理系统中存在的安全性问题进行了讨论，并运用PKI技术提出了一套可行的改进方案。该方案对用户的身份验证采用了数字证书管理，对关键数据进行数字签名，数据传输采用了安全连接，实现了数据真实性、完整性、不可否认性。目前越来越多的高校实行学分制改革，该方案的实施对保证学分制的安全性具有一定的实用性和借鉴性。

关 键 词 公钥； 身份认证；安全套接层；学分制；管理系统

中图分类号 TP393 08 文献标识码 A

A PKI Based Security Solution for Credit Management System

Liu Nian Li Tao Zhao Kui Xu Chun

(College. Of Computer, Sichuan University Chengdu 610065)

Abstract This paper discusses the problem in the credit management system of the universities and presents a security solution for them. The solution is based on the public key infrastructure technology. In the solution, the validation of user identity adopts the figure certificate, and the key data is figure validated. The data transmission adopts the secure socket layer. The authenticity, integrality and the undeniableness is realized. The credit management is the trend of the universities of China, and more and more universities put the credit system in practice. The implementation of the security solution, which assures the security of the credit management system, is of significant practical value.

Key words public key infrastructure; certification authority; secure sockey layer; credit; management system

随着高等教育改革的进一步深化，社会对人才培养提出了更高的要求。为适应现代信息社会的需求，许多高校开始改变以前的学年学分制，实行完全学分制，以建立全新的、更加灵活的人才培养机制，学分制的实施依托的是一套完整的学分制综合教务管理系统。与过去的学年制教务管理相比，学分制系统大多采用的浏览器/服务器(Browser/Server, B/S)结构突破了原先教务系统使用地域的局限性，使整个校园网乃至Internet上的用户都可访问本学分制系统，加强了系统数据共享的能力。

学分制管理系统中，学生选课、查询成绩、查询学籍，教师登录成绩及查询授课时间、地点等都直接在网上进行，方便了教师和学生，提高了办事效率，增加了教务管理工作的透明度。但是网上数据的开放也带来了安全上的隐忧，目前该系统在安全管理上存在四个方面的不足：

1) 学生和教师的密码都是通过系统预置，然后通知学生和教师，密码在传递过程中可能泄漏；

2) 由于密码是采用数据库的字段作为载体记录，因此密码的长度受到数据库字段长度的限制。如果用

2003年3月15日收稿

* 四川省科技厅科学基金资助项目，编号：00C084

** 男 29岁 硕士 助理研究员 主要从事计算机网络与互联网方面的研究

户的安全意识比较薄弱，采用的密码常常具有一定的规律，如以生日、电话号码等作为密码，容易被人猜到或者穷举法测试出来；

3) 在使用过程中，浏览器和服务器之间的数据传递采用明文传递，密码可能被窃听造成泄漏；

4) 由于只是采用简单的密码认证，教师录入的成绩无法确认是教师本人所录入，其数据的真实性需要重新书面签字确认，增加了工作量。

这些不足造成学生的密码被更改、课程被增加、修改、删除，更严重的是，如果教师的密码泄漏则会直接导致学生成绩被修改等严重后果。公钥基础设施(Public Key Infrastructure，PKI)为搭建一个安全的网上学分制管理系统提供了一种可行的办法。

1　系统原理

PKI是一种遵循既定标准的密钥管理平台，它能够为所有网络应用提供加密和数字签名等密码服务及所必需的密钥和证书管理体系。该平台采用证书管理公钥，通过第三方的可信任机构—认证中心，把用户的公钥和用户的其他标识信息捆绑在一起，在Internet网上验证用户的身份。公用密钥加密技术使用不对称的密钥来加密和解密，每对密钥包含一个公钥和一个私钥，公钥是公开且广泛分布的，而私钥从来不公开，只有用户知道。用公钥加密的数据只有私钥才能解密，反之亦然[1]。

PKI基础设施解决了信息的四个问题：

1) 保密性：只有收件人才能阅读信息；

2) 认证性：确认信息发送者的身份；

3) 完整性：信息在传递过程中不会被篡改；

4) 不可抵赖性：发送者不能否认已发送的信息。

数字证书认证中心(Certification Authority，CA)是PKI的核心。CA中心为每个使用公开密钥的用户发放一个数字证书，数字证书的作用是证明证书中列出的用户名称与证书中列出的公开密钥相对应。CA中心的数字签名使得攻击者不能伪造和篡改数字证书。同样CA允许管理员撤销发放的数字证书。

数字证收签发中心(Registration Authority，RA)，数字证书注册审批机构。RA负责证书申请者的信息录入、审核以及证书发放等工作，同时，对发放的证书完成相应的管理功能[2]。

安全套接层(Secure Socket Layer，SSL)是目前使用最广泛的、普通的Web安全协议。每一个SSL通信都受到服务器认证、保密性和完整性服务的保护，这些保护是依赖于基于服务器的密钥对的使用来进行的。

2　系统设计

该学分制网络管理系统是在原有的管理系统上提出的一种更优化、更安全的管理系统方案，力求在保证效率的前提下，实现数据传递和存储的安全。

2.1　系统结构

系统采用三层客户端/服务器(Client/Server, C/S)结构。数据库服务器用于运行ORACLE数据库，存放所有学分制系统数据。应用程序服务器运行了OAS(ORACLE APPLICATION SERVER)，也是SSL的服务器端。OAS是建构在网络运算架构下的应用服务器，以符合CORBA2.0 标准的ORB为基础，将应用程序和插件以及所有系统服务作为分布式对象来进行调用。本系统采用了PL/SQL插件，PL/SQL是ORACLE对关系数据库关系语言SQL的过程化的扩充。这样的设计能使应用处理分散于数部主机，从而有效、经济地解决性能瓶颈，并保证了可扩展性。CA服务器和RA服务器用作发放证书和身份认证。该方案提供了一个可扩展的、稳定可靠的、易于管理的平台[3]。

2.2　系统功能

系统功能模块如图1所示。

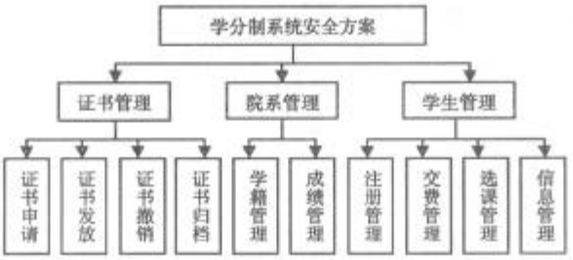

图1 系统功能结构图

2.2.1 证书管理

在数字证书认证的过程中，证书认证中心(CA)作为权威的、公正的、可信赖的第三方，其作用是至关重要的。在本系统中，证书管理是实现系统安全的最关键的部分。

证书申请采用在线申请方式，用户通过自己的浏览器到服务器上下载标准表格并填表申请。在用户的信息写入CA的申请信息数据库后，CA中心将发放用户名和密码，RA将这两个代码当面提交给证书申请者。证书申请者通过浏览器安装Root CA的证书，填入用户名和密码，自助式地下载自己的证书，证书介质可存入软盘或其他介质中。这样能避免原来密码发放过程中的泄密。实行学分制，与之相配套的是弹性学制，因此在证书的有效期必须与学生的学籍信息相关联。在证书的有效期内，由于私钥丢失泄密等原因，必须废除证书。证书持有者提出废除申请，经同意撤销后，可以重新申请证书[4]。

2.2.2 学生信息管理

学生个人信息管理是面对学生的收费、注册、选课、学籍、成绩、考试等全方位的信息管理。目前高校连年扩招，学生具有数量多、分布广、流动性大等特点，基于B/S结构的客户端程序能够充分适应以上特点，学生通过网络就可以了解到自己大部分的个人信息，方便快捷高效。

学分制环境下，学生的个人数据是学生在校期间个人能力发挥的真实体现，其数据真实的重要性不言而喻。学生学费缴纳改变为以学分为依据缴纳学费的办法，要求数据非常准确，缴纳人的身份不能被冒充。选课管理是学分制系统中的核心部分，是学籍管理、成绩管理、收费管理等的基础和依据，其数据的准确性很重要。因此，学生在浏览器客户端连接上系统时，必须提供系统签发的CA数字证书，保证其身份的真实性和不可抵赖性，解决了以前的简单密码认证带来的问题[5]。

2.2.3 院系教务管理

院系教务管理是各院系教务人员对本院系学生总体情况的管理，能够对学生的学籍、成绩数据进行修改、查询、统计、分析等。目前的学分制系统中院系级的数据管理大多是采用C/S结构的客户端管理程序，很少有完全采用B/S结构的管理程序，其主要问题就在于数据的安全性。

院系管理中涉及到最多的是学生的成绩，这也是评价学生在校学习情况的最直接的依据。成绩的录入是每学期期末任课教师或院系教务管理人员根据网上提供的选课名单进行的。基于PKI技术的成绩登录在每份成绩单上都附有提供成绩的教师的数字签名，具有不可抵赖性，数据完全真实。该方案解决了目前教务处收到成绩后重新打印成绩数据请教师签名核实数据的繁重工作的问题。

3.3 系统实现

图2所示为系统实现的数据流程图。

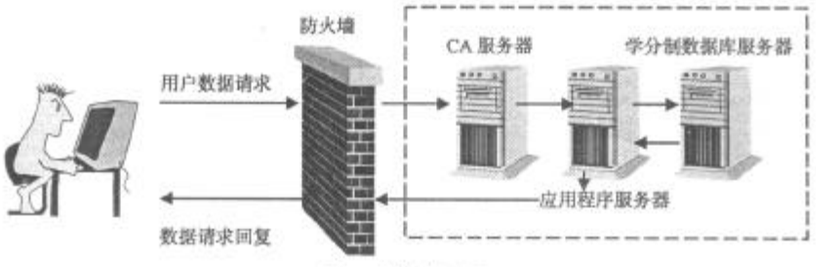

图2 数据流程图

1) 客户端在浏览器端发出一个要求SSL连接的请求，该请求通过防火墙的验证后提交到服务器。SSL的服务器端将一个回应和包含了自己身份和公钥的证书发给浏览器，并发出请求要求浏览器提供用户证书。

2) 客户端检查服务器证书后，提供自己的数字证书，将其发送给服务器。服务器检查签署客户证书的CA通过后，即建立起了一条SSL数据传输通道。

3) 加密后客户端请求发送到应用程序服务器，OAS在进程池中分配一个进程为客户端和数据库建立连接。ORACLE数据库运行PL/SQL程序包，将生成结果发送给OAS，由连接进程将结果封装成HTTP响应发送给客户端。

4) 具体教师登录成绩为例，教师的客户端与服务器的整个对话都是建立SSL加密的数据传输上，保证了数据传输的真实性和完整性。服务器对教师身份的认证，保证了教师身份的真实性。教师登录成绩单上签署教师的CA数字签名，保证了成绩数据的真实性、完整性和不可抵赖性，整个过程都由系统自动完成，教师只需提供系统签发的CA证书即可，易于使用。学生管理和院系管理的其他过程与此类似。

可见，以上过程是用户数据从请求到返回的数据流程。用户从请求到取得数据，必须经过防火墙身份认证、身份认证、应用程序的数据验证，保证了数据的真实性、完整性和不可抵赖性,数据更加安全可靠。

4 结 束 语

针对目前学分制系统中存在的一些安全问题，基于PKI技术的学分制管理的安全解决方案是一种可靠和可行的办法。它解决了目前学分制系统中存在的密码传递的不可靠性、弱口令、密码使用的泄漏、身份认证的真实性等问题。使系统更加安全可靠，系统数据更加可信，为目前高校学分制管理提供了一条高效且安全的思路。学分制改革是目前高校人才培养改革的趋势，越来越多的学校开始实行学分制并开始建设本校的学分制管理系统，该系统具有普遍的适用性，具有较广阔的应用前景。

参 考 文 献

[1] William S. 网络安全要素——应用与标准[M]. 北京: 人民邮电出版社, 2000

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

[3] Warwick F, Michael S. 安全电子商务——为数字签名和加密构造基础设施[M]. 北京: 人民邮电出版社, 2002

[4] Bradley D B. Oracle8i Web开发指南[M]. 北京:机械工业出版社, 2001

[5] 陈怀楚. 清华大学学分制综合教务系统说明书[Z].清华大学计算机中心，2001

编　辑　漆　蓉

·科研成果介绍·

高效合成孔径雷达成像处理方案研究

主研人员：黄顺吉　鲍厚兵　付毓生　夏金祥　皮亦鸣　杨　新　韩周安　丁东涛　张晓玲　龙　卉　姚　刚　黄健熹　张海呈　邹　琪　龚晓静

高效合成孔径雷达成像处理方案在分析现有并行计算机体制的基础上，针对曙光3000型并行机，对高效SAR成像处理方法进行了研究，对星载SAR仿真数据进行了处理测试，得到了较好的测试结果。该成果为我国应用系统的方案论证提供了参考依据。

·渠　涌·