高校科研管理系统的信息安全与保密探讨

赵晋琴[1]，唐红琴[2]
(1. 湖南第一师范学院 信息技术系，湖南 长沙 410205；2. 重庆大学 科技处，重庆 400044)

摘要：高校科研管理系统担负着高校的科研管理，单一的软件设计方案存在着很多的安全隐患，成为科研管理业务进行和开展的一个障碍。文章结合科研管理系统的特点，根据各种密码学算法的特性，从数据库的安全与保密以及网络的安全与加密两个方面，提出了解决科研管理系统存在的安全性问题的工作方案，并介绍在科研管理系统中的设计思路。

关键词：安全性；消息验证；身份验证；数字签名
中图分类号：G647 **文献标志码**：A **文章编号**：1005-2909(2009)03-0158-04

高校科研管理工作是对全校科技发展规划和科技管理政策的制定、实施，以及对科研项目、科研组织、科研效应等方面的管理，工作的好坏也将直接影响高校科学研究和科技创新能力的发挥水平。科研管理工作离不开信息化，科研管理系统是高校科研管理工作实现信息化的必然之路，肩负着对科学研究信息的收集、管理、研究、利用和向决策层提供真实准确的情报信息的重要职能。

一、高校科研管理系统的特点

高校科研管理系统是一个根据学校科研工作的管理模式、要求和方法进行设计开发的典型信息管理系统(MIS)，主要包括后台数据库的建立和维护以及前端应用程序的开发两个方面。通常情况下，高校科研管理系统应具备以下功能。

(1)科研管理系统具备完备的科研管理功能，可以实现对科研日常事务的管理，实现对本单位科研人员的各类科研项目、科研经费、科研成果、论文、专著、专利以及各种科技奖励等信息的集中管理。

(2)科研管理系统具备操作简单、使用方便的特点，可以通过简单的操作程序就能实现对科研信息的录入、查询和统计等不同功能，能自动生成正规的统计报表，及时为管理决策层提供所需信息。

(3)科研管理系统具备一定的兼容性和开放性。高校的科研项目往往来源于社会不同的行业和部门，不同的行业和部门对不同的科研项目也有各自不同的要求，这也要求高校科研管理系统应具有良好的兼容性和开放性，可以适应各类项目管理的不同需求，提高工作效率。

收稿日期：2009－05－10
基金项目：湖南省教育厅科技研究项目(05C046)
作者简介：赵晋琴(1964－)，男，湖南第一师范学院信息技术系高级工程师，主要从事电器控制、计算机网络安全研究，(E－mail)dysfzjq@163.com。

(4)科研管理系统是一个将人员、项目、成果和权限等管理有机结合的封闭系统。由于高校科研信息是高校管理工作的核心内容，为免受信息的非法盗窃和篡改，它往往只是对一个单位的内部职工进行授权使用的封闭系统。

正是由于高校科研管理系统的重要性以及同时应具备开放性和封闭性的特点，如何保护信息不被非法盗窃或篡改，自然成为了高校科研管理系统迫切需要解决的问题。本文根据各种密码学算法的特性，从数据库的安全与保密和网络的安全与加密两个方面进行信息安全与保密探讨，并以高校科研管理系统为例提出安全问题的解决方案和设计思路。

二、高校科研管理系统中存在的安全隐患和威胁

由于高校科研管理系统是以计算机和数据库通信网络为基础的应用管理系统，因而它是一个开放式的互联网络系统，与网络系统连接的任何终端用户都可以进入和访问网络中的资源。概括起来，高校科研管理系统所面临的威胁分为以下几类。

(一)通信过程中的威胁

高校科研管理系统用户在进行信息通信的过程中，常常会受到两方面的攻击：一是主动攻击。攻击者通过网络线路将虚假信息或计算机病毒卷入到高校科研管理系统的内部，破坏系统信息的真实性与完整性，造成系统无法正常运行，严重的甚至使系统处于瘫痪。二是被动攻击。攻击者非法窃取通信线路中的信息，使信息机密性遭到破坏，信息泄露而无法察觉，给用户带来巨大的损失。

(二)存储过程中的威胁

存储计算机系统中的信息易于受到与通信线路同样的威胁。非法用户在获取系统访问权后，浏览存储介质上的机密数据或专利软件，并且对有价值的信息进行统计分析，推断出所需的数据，这样就使信息的保密性、真实性、完整性遭到破坏。

(三)加工处理中的威胁

高校科研管理系统具有对信息进行分析、加工、处理能力，而信息在进行处理过程中，通常不具保护能力，易遭攻击。

除此之外，高校科研管理系统还会因为计算机硬件的缺陷、软件的脆弱和客观环境等因素损害，威胁系统安全。总之，对高校科研管理系统的威胁多种多样，我们要采取措施加以防御。

三、数据库的安全与保密

一般地讲，数据库系统由两部分组成：一部分是数据库；另一部分是数据库管理系统。数据库是数据的集合体；数据库管理系统是一个专门负责数据库管理和维护的计算机软件系统。数据库管理系统是数据库系统的核心，为用户及应用程序提供一种访问数据的方法，对数据库系统的功能和性能起着决定性的作用。它具有共享访问、最小冗余、数据一致性等优点[1]。

(一)数据库的安全管理策略

采用集中控制方式：由数据库系统管理员控制系统的整个安全维护，并在数据库中生成用户表。

(二)数据库的存储控制策略

(1)最小特权策略：该策略是数据库安全保护的最主要策略，适合于任何系统的安全保护。该策略使用户只了解工作所需的信息，对于其他信息都加以屏蔽和保护，使信息泄露的可能性最小，从而使数据库完整性受到损害的程度也最小。

(2)封闭性策略：仅当用户有明确的授权后才能对该系统进行存取操作。

(3)取决于上下文的存取控制策略：该策略是指存取控制项的组合。一方面它限制了组合在一起的存取域；另一方面有时又要求某些属性组合在一起。

(三)数据库的加密

安全策略为数据库的安全提供了一定的保障，但是有经验的攻击者可能借助某种手段避开应用程序而直接进入系统访问数据。为了防止这样的信息泄露，可以采取对数据库进行加密的手段，将其变为密文。

(1)数据库内加密：一种方法是将数据元素加密，即将一条记录的某几个属性值作为一个文件进行加密。另一种方法是记录加密，即将一个记录作为一个文件来加密。

(2)硬件加密：设计硬件实现数据库的加密，如加密狗、加密卡等。

(四)数据库的恢复

尽管采用了一些保护措施来防止数据库的完整性和安全性被破坏，但有时一些破坏是不可能避免的，数据库恢复技术是一种可采取的补救措施。

(1)用操作系统提供的功能，将被错误删除或修改的数据恢复，或将送到回收站的数据恢复。

(2)定期地将整个数据库复制到软盘、优盘、移动硬盘上保存起来，或刻录到光盘上保存起来，当数据库遭到破坏后，就可以利用备份将数据恢复。

(3)利用各种数据库之间的关系，用未遭到破坏的数据库恢复已遭到破坏的数据库。

四、网络的安全技术简介

(1)身份识别技术:所有用户的信息,包括用户名、用户权限等全部由系统管理员统一登录到数据库,作为表存储下来。用户通过输入用户名和口令来进行身份认证,从而登陆系统。

(2)哈希函数:获取一条任意长度的输入信息,并输入固定长度的代码,这个固定长度输出就叫做源输入消息的消息摘要[2]。用户可使用哈希函数来提供消息的完整性,验证没有人在消息传送期间对消息进行篡改。

(3)公开密钥机制:公钥机制基本思想是利用求解某些数学难题的困难性,用户的加密密钥和解密密钥不再相同,从公钥求解私钥是非常困难的。

(4)素性检测:a. 随机选取一个整数 a,(1≤a≤n-1)。b. 计算(a/n);其中:(a/n)是定义的 Legendre 符号。c. 如果(a/n)≡$a^{(n-1)/2}$ mod n,则回到步骤 1,否则认为 n 是合数,退出[2];d. 重复步骤 a,b,c 共 t 次(t 次任意取),如果每次有(a/n)≡$a^{(n-1)/2}$ mod n,则一般认为 n 是素数。

(5)数字签名:数字签名是一个加密的消息摘要,附加在一个文档后面。它可以用于确认发送者的身份和消息的真实性、完整性、不可否认性。

五、高校科研管理系统安全设计方案

(一)高校科研管理系统安全保密机制

高校科研管理系统安全保密机制结构图如图 1 所示。

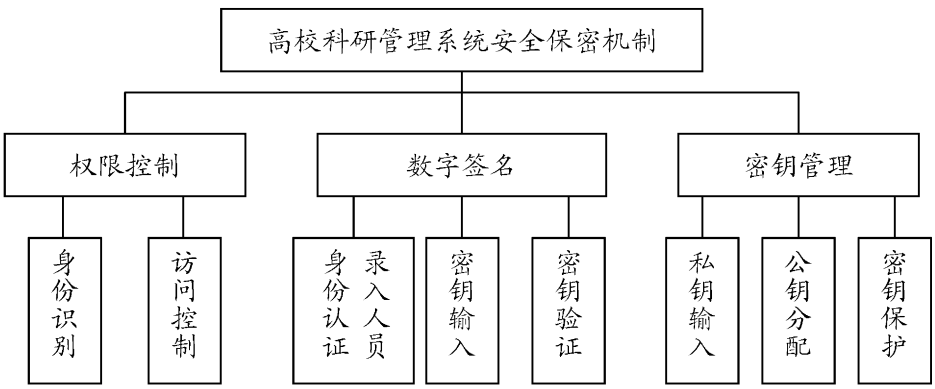

图 1 高校科研管理系统安全保密机制结构图

(二)身份认证

1. 基于用户标识和口令 P 的单向识别注册协议描述如下

(1)用户输入标识符 ID 和口令 P。

(2)查找口令文件,找到与 ID 值相对应的密文 Y。

(3)将口令 P 变成整数 P′。

(4)加密 P′:X = f(p′)≡$m_0^{p'}$ mod n。

(5)判断是否有 X = Y? 若是,则注册成功,否则注册失败。

2. 身份认证的实现

(1)用户输入 id 与口令 p,分别为 id. text,p. text。

(2)查找 id 对应的 y: rs. source = "select y from S_YHB_T where id = trim(id. text)"

其中:S_YHB_T 为用户数据库表,rs 为数据库游标,rs. source 表示游标的指向。

(3)将口令 p 取整:pb = format(p. text,"0#")其中:format 为变换格式的函数。

(4)将 pb 加密:pbj = Exp(pb)。

(5)比较 pbj 与 Y:

```
if pbj = Y then MDIForm. show
else exit sub
```

其中:MDIForm 为主窗体,MDIForm. show 表示通过验证,否则程序关闭。

3. 访问控制

(1)在用户登陆之前,首先由系统管理员分配给他访问的权限,当用户登陆之时,输入用户名及密码。通过验证则可登陆主界面,否则系统关闭。

(2)每位用户拥有一对密钥加密,私钥由个人妥善保管,公钥存放在系统数据库中。

(3)在查询信息时必须具备访问权限。

(4)当用户要求修改、删除内容时,除了要有私钥之外,还要求用户拥有修改权限,这是通过给有相应权限的人员进行数字签名来实现的。该私钥归个人保管,公钥存放在数据库中,如果通过检验,那么可以进行相应的修改、删除操作。如果身份不对,则拒绝操作。

(5)对于系统概貌信息的管理,也有对该项操作的权限控制给身份识别。如果身份不对,则拒绝访问;如果身份正确,那么可以进入系统概貌信息管理子系统,进行相应的操作,比如修改系统信息等。

4. 数字签名

(1)基于数字签名算法的描述。

本系统采用 DSA 算法,其使用的参数含义如下:

P:L 位的一个素数;

Q:P－1 位的素数因子;

G:g 为 h 的(p－1)/q 次方再取 p 的模,其中 h 是小于 p－1 的任意数,并且 g>1;

X:小于 q 的数

Y:y 为 g 的 x 次方再取 p 的模;

前 3 个参数 P、Q 和 G 是公开的,密钥设为 X,公钥设为 Y。对信息 m 进行加密的过程如下:

a. 发送方发送一个随机数 k,并且 k<q

b. 发送方生成签名:

$r = (g^k \bmod p) \bmod q$

$s = (k^{-1}(m + xr)) \bmod q$

c. 接收方通过计算机验证这些签名:

$w = s^{-1} \bmod q$

$u1 = (m * w) \bmod q$

$u2 = (r * w) \bmod q$

$v = ((g^{u1} * y^{u2}) \bmod p) \bmod q$

若 v=r 则签名被证实。

(2)数字签名的实现。

a. 发送方生成数 k,此值可以确定,这样 r 值也可确定下来,这样可以减少运算量。

b. 生成签名使用一函数 f1(g,p,q,k)计算 r 的值,并存储于数据库中,由系统管理员定期更新 r 的值。

录入信息为 m. text,变为整数为 format(m. text,"0#")。

使用函数 f2(k,m. text,x,f1,q)生成 s。

c. 验证签名:使用函数 f3(f2,q,m,w,f1,g,y)生成 v

if f1(g,p,q,k) = f3(f2,q,m,w,f1,g,y),'则通过验证,在添加的数据库记录上进行签名

then insert"用户名" into id from JW_CJ_T

else exit sub '否则拒绝添加记录

5. 密钥管理

用户输入密钥 s. text 管理员通过函数 f4(g,p,x)计算出 y,添加入数据库中,如果用户需要修改或者忘记私钥,则向系统管理员提出申请,由管理员再次进行密钥修改,普通用户无权进行修改。

六、结语

在加强高校科研管理系统的安全与保密方案中,采取了权限控制、数字签名、密钥管理等多种安全技术,为高校科研管理系统的安全与保密提供了有效的保护措施。为了更好地搞好高校科研管理系统安全与保密工作,要坚持技术层面的防范和行政管理并重的原则,采取有效的技术保密手段,完善保密制度,强化保密意识,做到以防为主、追查为辅,确保科研管理系统中的保密信息不泄密出去。

参考文献:

[1]臧劲松. 数据库系统安全的研究与分析[J]. 计算机安全, 2008(07):26－30.

[2]徐茂智. 信息安全概论[M]. 北京:人民邮电出版社. 2007.

Research on Information Security and Secrecy of Science Research Management System in University

ZHAO Jin-qin[1], TANG Hong-qin[2]

(*1. Department of Information Technology, Hunan First Normal University, Changsha 410205, China*;

2. Department of Science and Technology Research, Chongqing University, Chongqing 400044, China)

Abstract: The science research management system takes on the affairs of science research management in university. But single scheme for software design has a lot of safety risks, and becomes a block to carry on the work of science research management. In this paper, considering the characteristics of science research management system and the feature of all kinds of encryption algorithms, a solution to clear up the problems of database safety and network security in the science research management system is presented, and a design idea is given.

Keywords: security; message verifying; identity verifying; digital signature

(编辑　欧阳雪梅)