

文章编号: 1005—0523(2005)05—0121—03

财政收费系统中的信息安全策略研究

李黎青

(华东交通大学, 江西 南昌 330013)

摘要: 阐述了一个财政收费系统安全策略体系架构, 并对系统中可能出现的安全问题进行了详细的论述, 同时给出了解决方案。

关 键 词: 信息安全工程; 信息安全; AES; MD5

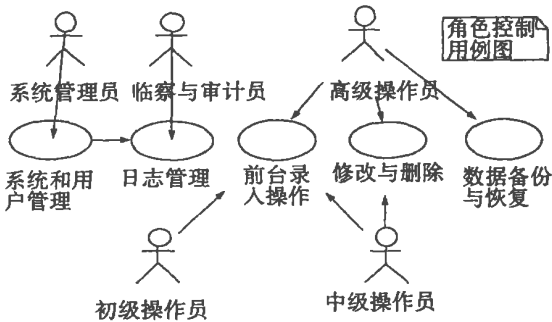
中图分类号: TP391 **文献标识码:** A

1 引 言

我国的县级财政系统是国家财政系统的基本单位, 担负着国家基本财政收费管理工作。传统的收费方式主要是各单位分散进行, 且大部分操作都是以手工方式进行, 这种方式直接导致机构工作效率低下, 透明度不高, 财务管理混乱。随着我国经济的发展和各行各业信息化改造的呼声越来越高, 开发一些适合地方县级财政金融部门使用的收费软件系统具有重要的现实意义。由于信息共享、网络化、安全稳定、专业化是这类系统的共同特征, 因此网络环境下的安全问题便更加不容忽视。

2 角色控制

角色控制在金融系统中的角色非常重要, 历史上在很多金融系统中由于其混乱的角色控制和不完善的用户管理带来的金融犯罪问题很严重。角色控制的思想来源于 UNIX 操作系统, 其目的是在一个系统中能够做到权限的有效分配, 相互制约。下图为我们在 ROSE 下生成的角色控制用例图。



系统管理员担负的任务是有效地对系统进行设置和管理, 对用户进行添加和删除但不能修改或知悉其密码, 系统管理员的操作与业务数据无关, 另外, 系统管理员可以读取一部分与其相关的系统日志; 监察与审计员的任务是管理系统日志, 但不参与任何数据操作; 初级操作员只能录入业务数据; 中级操作员可以录入、修改和删除数据; 高级操作员除此之外可以进行数据的备份和恢复操作。以上权限设置比较符合金融机构的业务特点, 具体实现方法是采用一组全局操作信号向量进行控制, 根据信号量的值进行相应操作, 信号向量 flagVetor 的数据结构如下:

{username;String(用户名)}

收稿日期: 2005—05—22

作者简介: 李黎青(1964—), 女, 湖北沔阳人, 高级工程师, 主要研究方向: 数据加密, 图像压缩。

flag¹: Boolean(是否可进行系统和用户管理);
flag²: Boolean(是否可进行日志管理);
flag³: Boolean(是否可进行业务数据录入操作);
flag⁴: Boolean(是否可进行业务数据修改和删除操作);
flag⁵: Boolean(是否可进行业务数据备份与恢复操作);
state: Boolean(用户是否在线).

3 数据的安全体系

3.1 加密算法简介

在该系统中,我们要用到以下成熟的加密算法和数字签名算法,现分别作简要说明(不涉及具体的密码学细节):

1) AES(高级加密标准): 2000 年 10 月, NIST(美国国家标准和技术协会)宣布通过从 15 种候选算法中选出一项新的分组加密标准,新的标准将会代替密钥长度变的太短的旧的 DES 算法, Rijndael 被选中成为将来的 AES. 这个加密体系是一种分组加密方法, 因为信息的内容是以 128 位长度的分组为加密单元的, 加密密钥长度有 128, 192 或 256 位多种选择. 它具有速度快, 并且能有效的对抗性差分攻击.

2) MD5(信息一摘要算法): 在 90 年代初由 Rivest 开发出来, 主要作用是生成消息摘要, 判断数据的完整性(该算法山东大学的王小云教授曾经找到其弱碰撞, 但是通过仔细研究发现, 对实际应用影响并不大, 攻击只具有理论上的意义).

3) BLOWFISH: 由世界密码学泰斗 Schneier 设计的一种分组对称加密算法, 它运行速度快而且非常安全, 目前对算法的攻击尚无任何实质进展, 密钥长度可以根据需要来改变, 密钥最高可达到 448bit.

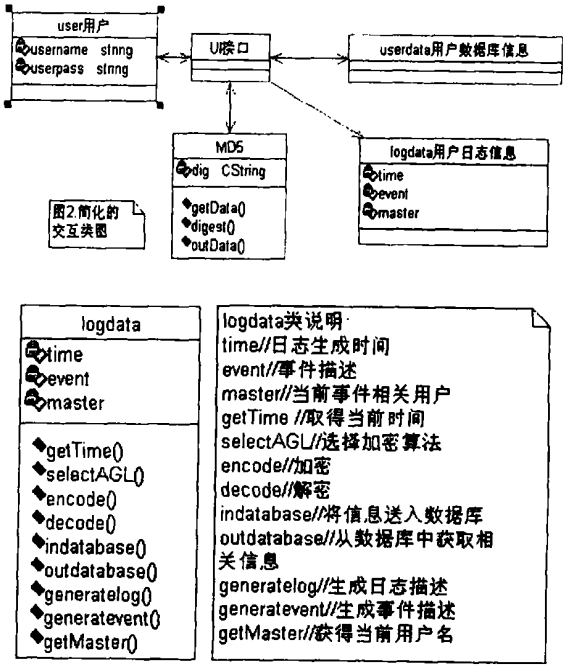
3.2 用户数据的安全

以下为简化的交互类图(不是严格意义上的类图), 其过程如下: 用户提交信息后, 有一个 USER 类实例保留信息, 并通过实现公共操作 UI 接口函数查询用户数据库, 看用户名是否存在, 用户名存在则用 MD5 算法计算 username+userpass 的消息摘要, 再将该消息摘要与用户数据库中保存的摘要信息比对, 正确则返回正确标志, 并记录到日志数据库中, 接着初始化用户全局信号向量 flagVetor, 错误则给出错误提示.

3.3 日志系统数据的安全

日志系统主要的作用是忠实记录所有重要的

用户行为, 因此日志系统对于金融系统的重要性是不言而喻的. 首先哪些行为必须被记录是个非常关键的问题. 一般而言, 用户何时登陆何时退出是很重要的, 因为发现问题后最大的嫌疑人就是该时间段的用户. 另外, 每项业务数据的添加、删除、修改和备份恢复操作都应该被记录到日志系统. 可用一个日志类如下图来表示.

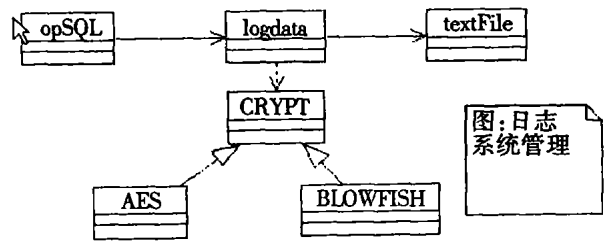


在系统中, 一旦出现 SQL 操作(opSQL 类), 首先就要生成一个日志类实例(logdata 类), SQL 操作完成后, 马上对日志类实例进行初始化, 首先通过 getTime 函数获得当前的系统时间, 并通过 getMaster 函数获得当前的操作用户, 并生成事件描述和日志描述, 接着选择加密算法(CRYPT 类), 对日志描述进行加密(AES 类或者 BLOWFISH 类), 保存为文本文件(textFile). 另外对于一般的系统日志, 则记录到管理员可以看到的数据库表中, 过程如下图(日志系统管理).

3.4 业务数据的安全

除了用户的个人信息需要进行加密外, 保存在数据库中的业务信息一般是不进行加密的. 主要是因为频繁的加密解密操作会影响到数据库操作的速度. 但是对于某些特定的业务数据, 可以给出选择加密或者不加密的提示, 让用户决定是否加密. 在这里, 对于要加密的数据信息的存储方式, 应该采用流文件格式. 业务数据必须加密则是在备份业务数据和生成特定上报文件的时候. 主要方法是采用 AES 和 BLOWFISH 进行, 其过程比较简单, 在此

不赘述.

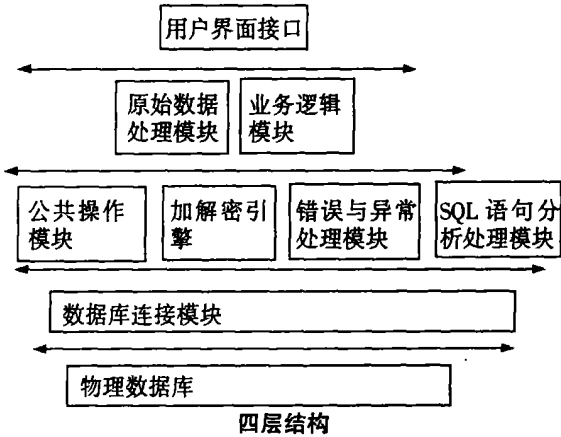


3.5 网络安全与数据传输的安全

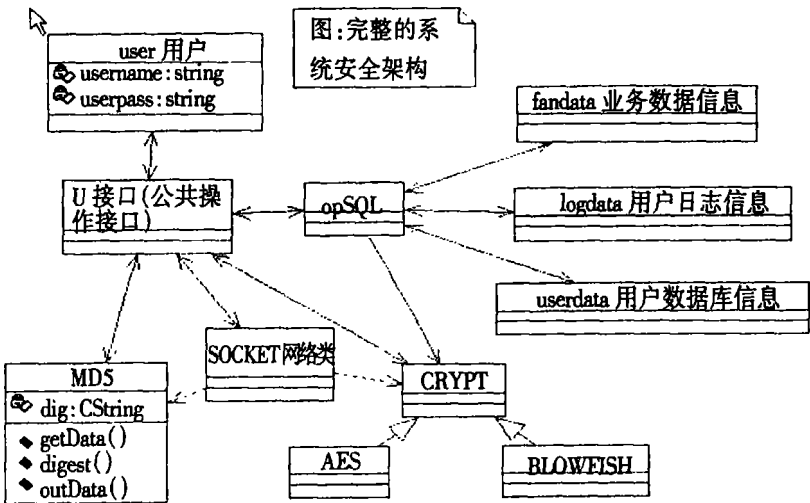
由于需要将重要的业务数据上报到财政部门及系统的分布式应用需要借助于网络(企业内部网),因此网络安全和数据传输安全是不容忽视的.可能出现的威胁包括:搭线窃听、中间人攻击、报文截获等,因此必须对需要传输的数据进行加密,并通过可靠信道传送密码.可以采用这样的作法进行:首先对需要传送的数据用 MD5 算法生成消息摘要,然后用 AES 算法对传送的数据进行加密,并将消息摘要和加密的数据发送给接收方,接受方对加密数据进行解密,再用 MD5 算法计算消息摘要,比较生成的消息摘要和接收到的消息摘要是否相同,确认数据是否完整.

4 安全财政收费系统的层次与完整的信息安全策略框架

该系统采用先进的组件模型分层,这样做有利于对系统业务变迁和系统扩张快速响应.如图,第 1 层为用户接口层,主要是为用户提供数据接口,获取用户输入;第 2 层是原始数据处理和业务逻辑处理,主要是对业务逻辑进行分析,对原始数据进行相应的处理;第 3 层包括公共操作、加解密引擎、错误与异常处理和 SQL 语句分析处理,主要是为了对第 2 层数据处理进行细节上的支持,第 3 层是数据库连接与管理,统一管理所有与物理数据库或者数据库服务器的连接与其它相应操作,第 4 层就是物理数据库与数据库服务器.



下面是相对应的信息安全策略类框架图:



参考文献:

[1] (美)Roger S.Pressman 著,梅宏译.软件工程—实践者的研究方法[M].北京:机械工业出版社,2002.

[2] 萨师煊,王珊著.数据库系统概论[M].北京:高等教育出版社,2003.

[3] 中国知网.数据库开发关键技术与应用[M].北京:人民邮电出版社,2004.

[4] [美]Bruce Schneier 著,吴世忠,等译.应用密码学[M].北京:机械工业出版社,2000.

[5] 冯登国,裴定一.密码学引论[M].北京:科技出版社,1993.

ing may be studied based on two basic related issues, i.e., the construction of granule and the computing of granule. In this paper, using rough set as tools, based on information system, a framework of granular computing has been provided. We define the granular language and its semantics, the granule calculus has define with logical connectives in this paper too. The application in data mining of granular computing has been discussed.

Key words: granular computing; data mining; rough set; information system

(上接第 120 页)

Management System for Artistic Student Recruiting Based on Web

XIAO Lei¹, FU Jun-dong²

(1. Office of Student Manage, 2. Office of Recruiting and Employ, East China Jiaotong Univ., Nanchang 330013, China)

Abstract: The scores Inputting work is important in artistic student recruiting, the workload of data inputting and checking is considerable. A system based on Web which enables multi-user input & check can make this work easier. The system's functions consist of data input, data check, data query and certificate making. It's proven that this system features with friendly interface, reliable and accurate data collection, and easy, safe and steady operation.

Key words: artistic student recruiting; management; checking; lookup

(上接第 123 页)

Information Security Strategy Research in Financial Charge System

LI Li-qing

(East China Jiaotong University, Nanchang 330013, China)

Abstract: This paper elaborated a security policy system overhead construction in financial charge system, discussed in detail the possibly appearing security problem and produced a solution.

Key words: information security project; information security; AES; MD⁵