基于安全机制的财税库银联网系统的设计与实现①

高兆乾　(山东省枣庄市国家税务局 计划统计科 山东 枣庄 277800)

摘　要： 财税库银联网系统是联系财政、税务和人民银行、商业银行的大型数据库应用系统，保证系统的安全稳定运行是非常重要的。根据系统面临的安全风险的特点，提出了计算机硬件、网络传输、数据库管理系统和密码学具体应用的方法，这些方法加强了财税库银联网系统的安全机制，保证了税款的安全、及时缴入国库。

关键词： 安全机制；财税库银联网系统；密码学

Design and Implementation of the Network System Among Finance Bureau, Taxation, National Treasury and Bank Based on Security Mechanism

GAO Zhao-Qian (National Taxation of Zaozhuang, Zaozhuang 277800, China)

Abstract: The network system among Finance Bureau, Taxation, National Treasury and Bank is a large database application which links the finance bureau, taxation bureau, national treasury and commercial banks. It is important to eusure security and stability of the system. Considering the security risks of the information system, we put forward a few methods on the computer hardware, network transmission, database management systems and cryptography. These methods can enhance the security of the information system. At the same time, they guarantee the safety of the taxes and timely payment.

Keywords: security mechanism; the network system among finace bureau; taxation; National Treasury; Bank; cryptography

税务信息系统建设实现了税务部门内部信息集中与信息共享，实现了税务和相关经济部门之间及公众间的信息交换，提高了纳税服务水平。保证时刻处理和存储重要税收数据的税务数据库应用系统的安全和保密成为一个至关重要的问题。财税库银联网依赖计算机及相关网络，同时联网系统涉及财政、人民银行、税务局和商业银行(社)四方，涉及的层次包括省、市、区县和乡镇，涉及到的资金流和信息流是国家税款，必须保证税款及时、准确、完整的入库，这就要求联网系统保证可靠性和不可否认性。本文从财税库银联网面临的安全风险入手，根据安全风险提出有建立财税库银联网系统安全机制的方法。

1　财税库银联网系统面临的各种安全风险

1.1 物理环境安全风险

现在税务已经实现“无纸化办公”，税务工作依赖计算机硬件及存储介质、网络设备的安全运行，保证计算机硬件及存储介质、网络设备的安全就显得非常重要。计算机硬件及运行环境是财税库银联网系统运行的基础，主要面临的安全风险包括计算机硬件的安全缺陷和环境对计算机硬件的安全威胁。

1.2 网络传输风险

随着 Internet 的发展普及，越来越多的税务核心业务向互联网转移，各种基于网络的应用系统如雨后春笋般涌现出来，面向纳税人提供各种信息服务。可

① 收稿时间:2009-11-24;收到修改稿时间:2009-12-27

以说网络系统是财税库银联网系统的外部环境和基础，财税库银联网系统要发挥其强大作用离不开网络系统的支持，系统的用户(如异地用户、分布式用户)也要通过网络才能访问数据库的数据。财税库银联网系统安全问题主要面临来自网络传输过程中出现的数据截留、篡改及身份假冒、非授权访问、病毒攻击等。

1.3 操作系统风险

操作系统风险主要是因为操作系统的漏洞及操作系统的安全配置不当引起的。操作系统设计中的漏洞很容易被利用，成为数据安全的薄弱点。另一个就是操作系统的安全配置不当，制定的访问控制与用户验证机制安全性不强。操作系统的安全性低就不能有效防御计算机病毒、木马等，极易发生崩溃，从而造成数据库应用系统安全风险。

1.4 数据库管理系统风险

数据库管理系统风险主要是数据库管理系统安全设计风险和数据库设备的安全风险和推理通道。

数据库管理系统设计缺陷产生的可能一是非法用户可能获取数据库的合法用户账号和口令访问数据库，攻击者通过数据库系统存在的后门和隐通道(如隐藏的超级用户账号、非公开的系统访问途径等)，从应用服务器或数据库服务器获取数据；另一个可能是数据库设计缺陷和访问控制机制的不完善，数据库设计缺陷可能会造成数据访问过程中的数据不一致，访问控制不完善的方面是数据库管理员(DBA)可以任意访问所有数据，往往超出其职责范围，同样造成安全隐患。

数据库设备的安全风险是入侵者可以直接利用操作系统的漏洞窃取数据库文件，或者篡改数据库文件内容。

推理是指用户通过间接的方式获取其不该访问的数据，数据库安全中的推理是指用户根据低密级的数据和模式的完整性约束推导出高密级的数据，造成未经授权的信息泄露，这种推理的路径称为“推理通道”。

1.5 应用系统安全风险

应用系统安全风险主要来自系统开发中的程序错误及设计缺陷。

一个很微小的错误都可能造成很大的安全问题，攻击者可以利用缓冲区溢出将对应于机器代码指令的数据写入溢出空间，从而将攻击代码植入攻击程序的地址空间，然后攻击者通过寻求攻击代码被执行的方法来获得目标系统的控制权。系统设计缺陷造成的攻击包括不完全输入验证、“检查时刻到使用时刻”错误及专门针对该系统相关文件的恶意代码。

1.6 管理风险

管理风险一是领导干部和工作人员信息安全和保密的意识还比较淡薄，存在“重应用、轻安全”的倾向；二是对网络环境下信息安全和保密工作的重要性认识不足，缺乏基本的防范技能，有的甚至有章不循，有禁不止。以上这些管理方面的风险严重制约着财税库银联网系统的安全。

2 财税库银联网系统安全机制概述

通过对财税库银联网系统面临的风险分析，我们可以看到，物理环境安全、网络传输安全、操作系统安全、数据库管理系统安全、应用系统安全及安全管理制度是财税库银联网系统安全机制的重要组成部分。只有各个安全环节周密设计，才能够从根本上建立可靠的财税库银联网系统安全防线。

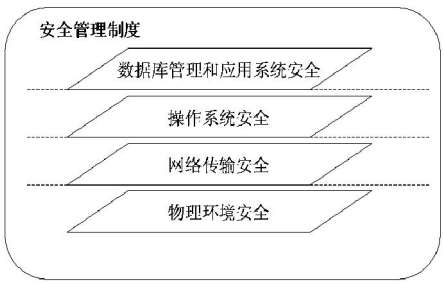

图 1 财税库银联网系统安全模型

2.1 物理环境安全

在物理环境安全方面，保证工作日 24 小时通信线路可靠、软硬件设备安全、设备能够备份及具有防灾害能力、防干扰能力，保证数据库设备的运行环境适宜(温度、湿度、烟尘)、不间断电源保障等。使用链路冗余、模块冗余、设备冗余和数据冗余等方式保证计算机硬件和网络设备的安全可用。采用硬件与软件技术相结合的防复制技术，比如在计算机中安装专门的加密、解密处理芯片，密钥也封装于芯片中。在机房的管理上，加强出入管理，使用智能卡和生物特征作为用户验证的方式，限制人员随意进出，保证重要区域设备和资料的安全。加强机房的环境管理，防止电气干扰，机房应该按防静电要求装修(如使用防静电

地板)，有独立的和良好的接地系统，机房中各种电气和用电设备都接在统一的地线上。防止泄露方面，因为整个房间屏蔽的费用比较高，可以采用设备屏蔽的方法，把需要屏蔽的计算机和外部设备放在体积较小的屏蔽箱内。

2.2 网络传输安全

网络传输安全上，首先定义安全的网络结构，然后认真评估网络安全风险，特别是关键设备的可靠性。为更有效的控制网络攻击和网络病毒，我们在内网与外网配置全状态检测型防火墙，在内、外网防火墙间架设网络防病毒软件，并在网络中安装一台可以与现有设备联动的网络入侵检测系统，通过防火墙做到事前控制，通过防毒软件做到事中处理，再通过入侵防御设备及时发现网络系统中存在的漏洞和安全隐患并及时修正，建立起一个完善的防护体系。比如，通过将数据加密，构建虚拟专用网 VPN，使用 VPN 的隧道技术与网上报税系统建立安全连接，从而保证网上报税的整个过程交易的安全性。利用非军事区(DMZ：Demilitarized Zone)将面向外部广域网的服务器和后端的数据库支持服务系统隔离，作为内部和外部网络之间的缓冲区。

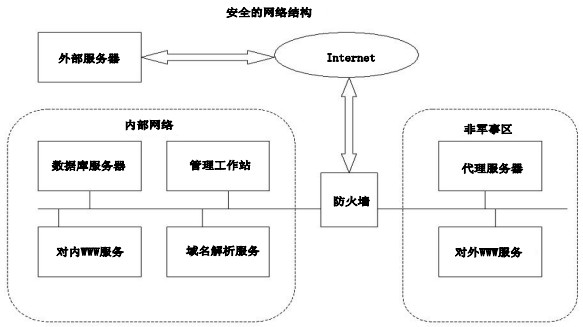

图 2　安全的网络结构

2.3 操作系统

操作系统方面，大部分税务系统的数据库服务器安装的操作系统为 Windows NT、Windows 2000 和 UNIX，所以主要是采用操作系统安全加固、安全配置和桌面防护的方法。一是提供尽可能强的访问控制和审计机制，二是对操作系统进行安全配置，比如在 Windows 系统中使用强度大的登陆口令，禁止 Guest 用户等方法进行安全配置，同时部署专业的入侵检测系统用于监测和阻止各种攻击，实时地阻止 TCP/IP 数据包。三是通过及时升级操作系统、安装防病毒软件及定时查杀病毒、及时升级病毒特征库防范病毒危害操作系统。

2.4 数据库管理系统

数据库管理系统方面，一是建立严格的用户认证机制，可以在数据库管理系统中对“口令”采取一些控制措施，可以有最小长度限制、次数限定、选择字符、有效期、双口令和封锁用户系统等，同时以加密形式存储“口令”，也可以存储“口令”的单向 Hash 值。还可以应用数字证书来证明实体所宣称的身份与其持有的公钥的匹配关系，使得实体的身份与证书中的公钥相互绑定。

二是加强数据库管理系统的存取控制。根据税务应用系统用户岗位职责明确的组织机构特点，我们应用 RBAC(Role-based Access Control，基于角色的存取控制)。RBAC 可以在税收人员和权限之间增加了一个中间桥梁——角色。权限被授予角色，而管理员通过指定税收人员为特定角色来为其授权。平时根据组织中的不同工作创建角色，然后根据税收人员的责任和资格分配角色，税收人员可以轻松地进行角色转换。而随着新应用和新系统的增加，角色可以分配更多的权限，也可以根据需要撤销相应的权限。还可以在数据库底层使用视图和存储过程用于增强系统的安全性。视图、存储过程可以限制底层表的可见列，从而限制用户能查询的数据列的种类，还能通过应用 Where 子句限制表返回的行。

三是采用数据库库外加密。根据执行加密部件在数据库系统中所处的层次和位置，通过对比各种体系结构的运行效率、可扩展性和安全性，可以选择库外加密的方式。库外加密的加／解密过程在客户端或专门的加密服务器实现，减少了数据库服务器与 DBMS 的运行负担,还可以将加密密钥与所加密的数据分开保存，提高安全性。在加密粒度的选择上，在目前条件下，为了得到较高的安全性和灵活性，采用最多的加密粒度是数据元素，如果只有少数属性需要加密，属性加密是可选的方法。

四是加强数据库的审计。审计机制应该至少记录用户标识和认证、客体访问、授权用户进行并会影响系统安全的操作，以及其他安全相关事件。对于每个记录的事件，审计记录中需要包括事件时间、用户、事件类型、事件数据和事件的成功／失败情况。对于

标识和认证事件，必须记录事件源的终端 ID 和源地址等。对于访问和删除对象的事件，则需要记录对象的名称。为了达到审计目的，一般必须审计到对数据库记录与字段一级的访问。对于审计粒度与审计对象的选择，需要妥善解决系统运行效率与存储空间消耗之间的矛盾。

五是数据库的备份与恢复。应该充分将冷备份、热备份和逻辑备份三种方式结合，对于必须保持每天 24 小时、每周 7 天全天候运行的数据库服务器来说，一般采用热备份和逻辑备份。对于只在工作日固定时间段运行的服务器采取冷备份的方法。

2.5 应用系统

应用系统的安全方面，一是在开发初期对财税库银联网系统可能的安全风险进行评估，主要是评估应用系统的脆弱性、应用系统面临的威胁以及脆弱性被威胁源利用后所产生的实际负面影响，并根据安全事件发生的可能性和负面影响的程度来识别应用系统的安全风险，提出符合实际的安全需求；二是制定详细的安全规划，在规划过程中，要积极的引入应用系统安全监理，保证安全机制的落实及工作质量；三是在财税库银联网系统的使用过程中，要加强信息系统的安全审计，将审计中发现的安全问题及时予以整改。

2.6 安全管理

必须做好安全制度的建设和落实，一是在思想上树立安全意识；二是根据国家的相关法规制度，制定适合税务数据库应用系统的安全标准，另外，还要建立相应的安全应急机制，应对各种突发事件；三是加强计算机安全培训，建立健全多种形式的计算机安全技术、安全管理的岗位培训和定期轮训制度。

3 财税库银联网系统安全机制的应用实例

财税库银联网系统的安全机制具体采用了访问控制、用户验证、操作系统、数据存储、网络设置的方法。

3.1 访问控制

财税库银联网系统制定了严格的访问控制策略，将用户划分为不同的主体，主体隶属于用户组，给用户组赋予相应的权限，并且根据各个用户权限的大小、所属单位进行权限的授予。用户要访问的资源定义为客体，主体访问客体必须经过权限控制，只有主体只能访问权限内的客体。

3.2 用户验证

财税库银联网系统用户的登陆口令经过加密后存储在数据库表中。系统管理员看到的用户口令是加密后的一段字符串，这样能保证用户口令的安全。在系统里写入了一个加密函数，加密函数将用户设置的口令转换为密文，口令的加密算法采用了传统对称密码体制，安全强度大，能够保护密码的安全。口令的加密函数应用密码学上的置换和替代相结合的方法，首先将用户设置的口令明文中的各元素进行“换位”，即通过对明文重新排列组合达到隐藏明文内容所表达含义的加密方法，然后，将“换位”后的密文在进行替代，即将第一次加密后的密文的内容用新的符号或者符号组合替代。在这里模拟部分实现代码来说明加密过程：

```
Function-Encrypt(Src:String;Key:String):string;--加密函数，输入的第一参数是需要加密的明文
var --声明变量
……
begin
KeyLen:=Length(Key);
if KeyLen = 0 then key:='…';---key 为一段字符串
KeyPos:=0;
SrcPos:=0;
SrcAsc:=0;
Range:=256;
Randomize;
offset:=Random(Range);--取随机数
dest:=format('%1.2x',[offset]); --格式化 dest
for SrcPos := 1 to Length(Src) do
begin
SrcAsc:=(Ord(Src[SrcPos]) + offset) MOD 255;--生成的密文在一定范围内
if KeyPos < KeyLen then KeyPos:= KeyPos + 1 else KeyPos:=1;
SrcAsc:= SrcAsc xor Ord(Key[KeyPos]);--逻辑运算
dest:=dest + format('%1.2x',[SrcAsc]);--将生成的密文连接
offset:=SrcAsc;
end;
……
Result:=Dest; 函数返回密文
```

3.3 操作系统

针对操作系统安全风险，一是制定相应的用户权限策略，对操作系统的超级用户权限进行合理分散与适度制约，降低可能出现的超级用户“大权旁落”的威胁风险与破坏程度；二是及时对操作系统进行升级，安装防病毒软件及定时查杀病毒、及时升级病毒特征库防范病毒危害操作系统，同时部署专业的入侵检测系统用于监测和阻止各种攻击；三是加强操作系统的安全审计，加强的系统日志的分析，及时发现存在的不安全因素，针对安全漏洞制定详细的方案，防止对联网系统的安全运行的损害。

3.4 数据备份

财、税、库、银联网各方日交换以及处理的数据量在几万条到几十万条记录，特别是税款申报期内，财税库银联网系统业务量很大，必须保证数据库的数据安全，我们使用 sql server 2000 自带的数据库备份功能，根据财、税、库、银联网四方的业务情况，每天在财税库银联网系统空闲的时间段让数据库进行数据自动备份。同时，数据库自动备份和人工备份相结合，在财税库银联网系统升级之前，对数据库文件进行人工备份。

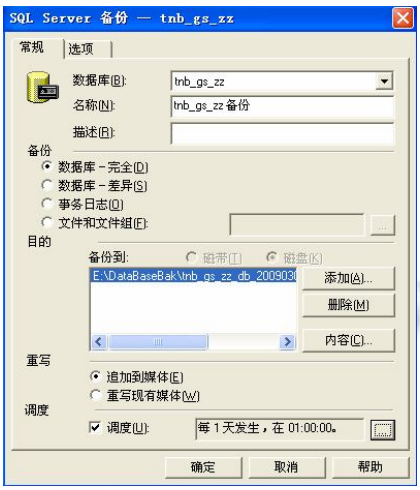

图 3　数据备份

3.5 网络设置

财税库银联网各方的服务器通过自己单位的防火墙、路由器连接到一起，而且财税库银联网各方的服务器是放在非军事区里，利用非军事区(Demilitarized Zone，DMZ)将面向外部的其他联网参与单位的服务器和自己单位的内部数据库支持服务系统隔离，作为内部和外部网络之间的缓冲区，这样做自己单位的网络和财税库银联网系统的网络独立，保证单位内部网络的安全，同时保证财税库银联网服务器的安全。

同时，将网络地址转换技术(Net Address Transfer，NAT)应用于联网系统，NAT 将一个地址或多个地址转换成另一个地址，非军事区的联网服务器 IP 地址通过防火墙的网络地址转换功能将真实的 IP 地址隐藏起来，财税库银联网服务器联网各方看到的地址是经过转换后的地址。

4　结论

通过财税库银联网系统安全机制的应用，保证了财税库银联网系统地安全运行。要持续地关注安全技术和安全管理，深化结合与应用，才能够最大程度上保证财税库银联网系统安全。

参考文献

1 高兆乾.税收应用系统中的数据库安全机制浅析. 电脑知识与技术, 2008,4(4):781－782,785.

2 山东省人民代表大会常务委员会. 山东省信息化促进条例.[200-10-27].http://www.agri.gov.cn/zcfg/dffg/t20081127_1180460.htm.

3 Gong L, Ellison G, M Dageforde. 朱岱译. 深入 Java 2 平台安全—体系架构、API 设计和实现. 第二版.北京:电子工业出版社, 2004.

4 Stinson DR. 冯登国译.密码学原理与实践. 第二版.北京:电子工业出版社, 2006.

5 Silberschatz, Korth HF, Sudarsha S. 杨冬青,唐世渭等译.数据库系统概念.第四版.北京:机械工业出版社, 2003.

6 管有庆,王晓军,董小燕.电子商务安全技术.北京:北京邮电大学出版社, 2005.