校园一卡通系统的安全性分析与设计

杨延朋
（辽宁科技大学 网络信息中心，辽宁 鞍山 114051）

【摘　要】文章以设计安全的校园一卡通系统为背景，从软件系统、硬件系统及管理手段等方面入手，剖析了校园一卡通系统在设计和使用上存在的安全漏洞，同时介绍了校园一卡通安全系统在中心数据库、应用软件系统设计、卡片及读卡设备、交易记录、网络环境、防病毒等几个方面的实现策略。该系统的安全性分析和设计，有利于数字化校园的整体发展。此方法也可以作为其他系统的参考模式，应用到相类似的系统之中。

【关键词】校园网；一卡通系统；安全性
【中图分类号】TP393　　【文献标识码】A　　【文章编号】1002-0802(2009)02-0328-03

Analysis and Design on Security for Campus-card System

YANG Yan-peng
(Network Information Center, Liaoning University Of Science and Technology, Anshan Liaoning 114051, China)

【Abstract】Based on the secure Campus-card system, this paper analyzes the security holes on the design and use of the campus-card system from different aspects, including software system, hardware system and the administration etc. Meanwhile, the implementation strategies of the campus-card security system are described from different angles, including the center database, software system, the card reader, transaction record, network environment and anti-virus measure, etc.. The security analysis and design of the campus-card system profits the overall development of the digital campus. This method, as a reference model, could be used in other systems similar to the campus-card system.

【Key words】campus network; campus-card system; security

0 引言

随着计算机技术、网络技术及通讯技术的发展，数字化校园已经在高校内全面规划和启动。校园一卡通系统作为整个数字化校园的核心应用项目，设计上必须符合数字化校园的整体设计思想。该系统不仅仅是消费系统，还要具备管理功能，更要与学校管理信息系统紧密结合起来。因此，该系统具有消费、身份识别、个人信息查询、缴费等主要功能。

作为数字化校园建设的基础和核心设施之一，校园一卡通系统涉及到大多数在校学习、工作和生活的人员，并为学校教学、管理、门禁、餐饮及其它公共服务提供身份证明和支付手段，所以对安全性有非常高的要求，可以说，安全性是校园一卡通系统的生命线[1]。在校园一卡通系统的设计和建设过程中，要把安全性放在首位，通过技术和管理手段，保证系统能够高效、安全和可靠地运行。

系统的安全性设计首先应充分考虑到各方面的因素，包括卡片、读卡机具、应用系统服务器、中心数据存储、系统管理软件、应用系统软件和运行管理等。其次，技术手段和管理手段相结合，通过加强安全管理来保证系统的安全性设计得以有效实行。

1 安全策略的分析与设计

1.1 中心数据库

中心数据库存储了全部的身份信息和交易信息，是一卡通系统的中枢，其安全性对整个一卡通系统有决定性的影响[2]。

数据库的安全是指保护数据库，以防止非法使用所造成的数据漏洞、修改、损害。计算机系统中普遍存在安全性问题，特别当拥有许多共享数据库中的大量数据时，安全问题显得尤为突出。在 ORACLE 多用户数据库系统中，安全机制完成以下

收稿日期：2008-09-09。
作者简介：杨延朋（1972－），男，工程师，主要从事校园网设计、安全方面的研究工作。

任务：防止非授权的数据存取、防止非授权的模式对象存取、控制磁盘使用、控制系统资源的使用、审计用户动作。

数据库安全可以分为数据库系统安全和数据安全。系统安全包括在系统级别上，控制数据库的存取和使用机制，如有效的用户名与密码组合、用户模式对象的可用磁盘空间数量、用户的资源限制。系统安全机制检查用户是否被授权连接数据库，数据库审计是否是活动的，用户可以执行哪个系统操作。数据安全包括在模式对象级别上，控制数据库的存取和使用机制，如哪个用户有权存取指定的模式对象，在模式对象上允许每个用户采取的动作，每个模式的审计动作。

1.2 软件系统设计

软件系统既包括一卡通系统的系统软件，也包括与一卡通系统相关的各个数字化校园的应用系统软件。就一卡通系统的系统软件，可以从登录控制、操作员权限控制、数据库防篡改和登记操作日志等方面来考虑。从登录控制的角度，通过对客户机登录采取控制，对非法的客户机加以拒绝，以防止非法的客户机向服务器发送业务请求。

在登录控制的基础上，采用对操作员进行权限控制的方式来控制操作员对一卡通系统的访问，使得不同的操作员只能在自己的权限范围内对系统进行操作。为防止发生数据库的合法用户非法修改数据库的重要数据，可对数据库的重要数据表加以校验。此外，系统将对所有的操作保存详细的记录，以便在发生问题后进行追查。

对于已有的与一卡通系统相关的数字化校园应用系统，可以通过提供一整套应用编程接口，使得应用系统经过小范围的改造，就能接入整个一卡通系统。由于应用系统在接入一卡通系统时只能使用指定的接口，因而也只能完成许可范围内的操作，这样就消除了它们非法访问一卡通系统中心数据库的可能性。

1.3 卡片及读卡设备

现在一卡通系统中所采用的卡片多数为非接触式射频IC卡，主要考虑卡中信息在存储及交易过程中的完整性、有效性和真实性，防止对卡片的伪造以及对卡中的信息进行非法修改和使用。

POS 机是一卡通系统内需要对卡片进行读写操作的机具中装备数量最大、使用频率最高的设备，所以POS机本身的稳定运行和存储数据的安全可靠，成为一卡通系统安全性重要的指标之一。一方面，通过在读写电路上采取从电源稳定到读写保护等一系列设计，可以降低出错的概率；另一方面，采用在卡内使用备份数据也可以保证卡上的金额读写不出现差错。

黑名单管理是各类读卡机具都需要具备的一个重要功能。由于读卡机具内的数据存储空间有限，又因为丢卡产生黑名单数量部是在增加，所以如果不采取措施控制黑名单的数量，终有一天会出现读卡机具数据存储器满，新挂失的卡片不能进入黑名单的情况[3]。而且，当名单数量达到一定数量后，读卡速度会受到影响，从而降低读卡机具的处理速度。为控制黑名单的数量，一方面，可采用设置卡片使用有效期的方法，在卡片开户时写明有效期。当卡片超出有效期又没有重新注册时，读卡机具会自动拒绝使用，系统会自动从读卡机具内清除这些黑名单。另一方面，可采用批次的概念，将一届学生设置为一个批次，当该届学生离校后，将该批次号挂失，同时从挂失库中清除该批次卡号。

1.4 交易数据

为了确保交易数据存储的安全，POS机内应包含大容量的非易失性存储空间，以存储足够的脱机交易记录和黑名单。在内部的数据存储器空闲存储空间不多时，POS 机应自动产生提示信息。在内部的数据存储器已经满时，POS 机应自动报警并拒绝消费，保证已经存储的数据的安全可靠。存储脱机交易流水信息时，在每条记录中增加通过加密算法生成的校验码，以识别对数据存储器的非法修改。

为保证读卡机具与中心数据库服务器和应用系统服务器之间的数据通信安全，读卡机具在系统中进行注册，未注册的机具卡片无法使用。为了防止对交易记录从POS机到数据通讯网关的传输过程中被篡改，发生的交易记录的安全问题，在普通的POS机中，每产生及上传一笔交易记录时，每笔记录中均应采用校验码，然后上传至数据通讯网关。数据通讯网关通过验证校验码，以确保采集到的校验记录的完整性和合法性[4-5]。

为应对数据传输过程中因网络故障而导致的数据丢失，在POS机的硬件设计中应增加重复采集的功能。即在采集脱机交易流水时，只是移动指针，采集完毕后流水仍存在于POS机的数据存储器内，以便对全部或指定范围的流水记录重新采集。

1.5 网络环境

目前，一卡通系统大多依托校园网进行建设，校园网中的网络环境如路由器、交换机及网络线路应安全稳定。为确保数据传输的安全，中心数据库服务器、圈存机、语音服务、银校转账前置机等专用设备还应铺设有一定冗余的专网线路，专网线路和各业务部门采用虚拟专用网（VLAN）相连。对于无法实现专网线路的场所，一定要在原有网络环境的基础上，通过 VLAN 手段和基于源 IP 地址和目的IP地址的访问控制列表来完成对用户及一卡通系统中数据访问限制[6]。

1.6 网络防病毒

计算机病毒，特别是网络病毒，已经成了信息时代的公害。新一代病毒所运用的技术使其传播速度极快，伪装更巧妙，破坏力更强，攻击更加频繁。在一卡通系统中，因为有些终端不可避免的挂在校园网上，所以网络防病毒也就成了系统不可或缺的一部分。所以，应使用企业版网络防病毒产品，来提供稳定集成的网络防护。

（下转第 332 页）

表 3 关联规则结果显示（手机报）

	Support（%）		Confidence（%）
	From	= = >	To
1	14.70		45.38
[5]	= = >	[3]	
2	19.65		60.66
[5]	= = >	[4]	
3	19.88		61.37
[5]	= = >	[9]	
4	22.49		69.43
[5]	= = >	[2]	

3.3 计算过程与结果

1）根据关联规则结果，选取的相关产品有彩信，GPRS，彩铃，短信。根据移动现行资费清单，可以计算得出平均价格如下表4。

表 4 产品价格表

产品	彩信	GPRS	彩铃	短信	手机报
平均价格（元）	6	10	6	12	3

2）对数据源进行统计可以得出手机报，彩信，GPRS，彩铃，短信的销售量如下：

表 5 产品销售量

产品	彩信	GPRS	彩铃	短信	手机报
销售量	137914	149853	297832	503492	151047

3）将以上数据分别代入公式(4)，可以计算出手机报与彩信、GPRS、彩铃、短信关联的交叉销售价值系数如下：

表 6 交叉销售价值系数

交叉销售系数	彩信	GPRS	彩铃	短信
手机报	0.8286	2.006	2.4202	9.2574

将以上结果进行相加，代入公式(5)可得结果为14.51。

3.4 结论分析

经过以上计算可知运营商每销售1元的手机报，除了获得1元的销售收入之外，同时将获得14.51元的交叉销售收入，远远大于产品的会计价值，即产品给运营商带来的实际价值远大于其账面价值。因此，单以产品的会计价值进行核算衡量的话，将无法体现其带来的真正价值。如果忽视交叉销售等因素对产品总价值的影响，运营商进行决策的准确性与全面性将难以得到保证。

4 结语

本文以通信产品销售的历史数据为基础，运用关联规则对通信产品交叉销售价值进行研究，通过建立一个简单清晰的模型，进而计算通信产品的交叉销售系数,得出通信产品的交叉销售价值，进而验证了数据挖掘中的关联规则在通信行业中的应用，并希望通过本模型能为运营商提供一种简便清晰的通信产品交叉销售价值的计算方法，为优化产品组合，营销策划等问题提供更加充分全面的决策依据。

参考文献

[1] Han J,Kam ber M.Data mining:concepts and techniques[M].San Francisco:Morgan Kaufmann Publishers,2001.

[2] 齐佳音,舒华英.客户价值评价、建模及决策[M].北京:北京邮电大学出版社,2005.

[3] 罗布·马蒂森.电信业客户流失管理——电信管理精选译丛[M].北京:人民邮电出版社,2006.

[4] 舒华英. 电信业继续加快转型步伐[J]. 中国新通信, 2006,(01).

[5] 石铁峰,石月皎. 关联规则数据挖掘应用研究[J]哈尔滨职业技术学院学报, 2007,(04).

[6] 钱明辉,孟捷. 交叉销售视角下企业多元化战略风险研究[J].财经问题研究, 2007,(01).

[7] 赵晋霞. 基于数据库营销的交叉销售研究[D].天津商学院, 2006.

（上接第 329 页）

2 结语

作为数字化校园的基础和核心系统——一卡通系统，从分析、设计到实现要充分体现安全性理念。在一卡通安全管理体制的监督保障下，一卡通系统的建设对未来数字化校园的提升和完善起着非常重要的推动作用。

参考文献

[1] 李宏芳. 一种高安全的校园一卡通设计[J]. 计算机与现代化, 2005（2）: 78-80.

[2] 卫星. 校园一卡通平台设计[J]. 四川师范大学学报(自然科学版), 2003,26（3）: 315-318.

[3] 辽宁科技大学一卡通系统设计方案[DB/OL]. [2008-02-03]. http://www.newcap. com.cn.

[4] 王景中,徐小青. 基于智能 IC 卡的网络数据安全保密系统[J]. 计算机应用, 2001,21（7）:53-55.

[5] 戴红. 清华大学校园一卡通实施方案介绍[J]. 金卡工程,2001,（11）:37-47.

[6] COMER D E.用 TCP/IP 进行网际互联:第一卷[M].北京:电子工业出版社,2001.