基于商场收银POS前置机系统的安全技术研究

于会军[1,2]，申群太[1]

(1.中南大学 信息科学与工程学院，湖南 长沙 410083；2.湖南工业大学 电气与信息工程学院，湖南 株洲 412008)

摘 要：对前置机系统的数据传输安全性和交易安全性、完整性进行了分析，并对其安全技术进行了研究。最后通过研究和实验，证明收银POS前置机安全技术对商场受理银行卡业务是安全可靠的。

关键词：前置机系统；安全性；完整性；冲正技术；存储转发机制

中图分类号：TN915.08 **文献标识码**：A **文章编号**：1673-9833(2007)04-0093-04

Research on Security-Technology of IBDCS Based on Cash-Register POS in the Market

Yu Huijun[1,2]，Shen Quntai[1]

(1.College of Information Science and Engineering，Central South University，ChangSha 410083，China；
2. School of Electrical and Information Engineering，Hunan University of Technology，Zhuzhou Hunan 412008，China)

Abstract：The security of the data transfer, dealing the security and completion of the transaction on IBDCS are analyzed; and it also puts some research on the security technology. Through study and practice, it proves that this technology is secure and dependable to the market which accepts bank-card service.

Key words：IBDCS；security；completion；Reversing-an-entry technology；memory-transition mechanism

1 背景知识

银行卡作为集存取款、消费、信贷、转帐、理财等功能于一体的支付工具，体现了传统金融业务与现代信息技术的完美结合，已渗透到社会经济生活的各个方面。近年来，为了进一步适应激烈的市场竞争、提高商业进销存管理水平，各商业流通企业逐步更新或安装了收银系统，这为在收银机上实现POS交易功能提供了良好的外部条件和环境，为银企在银行卡业务合作方面开辟了新的领域。目前，收银系统和POS系统的一体化渐成趋势[1]。

收银POS一体化项目，以现有商场的收银系统为基础，通过对收银机的改造，即安装密码键盘和刷卡器，增设商户端银行卡前置机来达到受理银行卡交易的硬件要求；其次，在收银机上安装银行卡受理驻留程序，在商户端银行卡前置机上安装银行卡处理程序，从而完成受理银行卡交易的软件配置；最后是网络通信条件，即申请一条X.25或DDN专线，以便和代理银行的授权前置机或当地银行卡网络中心相连，从而实现银行卡受理业务的实时交易。

商场收银POS前置机是实现银行传统业务向外拓展普遍采用的一种中间设备。它实现的主要功能有网络通信、报文认证、交易数据格式转换、个人密码PIN变换等。在该系统开发中，银行卡实时交易的信息安全问题，是需要重点研究和解决的问题。因此，本文对商场收银POS前置机系统的安全技术问题进行研究，以期保证交易过程中持卡人的资金安全， 提高商户使用银行卡的方便性、降低推广成本、提高使用效率，为企业创造更大的经济效益。

2 信息安全

信息安全涉及计算技术、密码技术、控制理论和管理科学等多门学科。

收稿日期：2007-04-28

作者简介：于会军（1975-），男，河南驻马店人，湖南工业大学教师，中南大学硕士生，主要研究方向为控制工程.

当前的网络安全技术发展趋势，主要由静态安全向动态安全转变，由组件安全向整体安全转变。信息安全一般是指网络信息的保密性、完整性、真实性、可用性和不可抵赖性[2]。保密性是指其内容不会被未授权的第三方非法窃取；完整性是指信息在传输过程中不会被篡改、破坏，不出现信息包的丢失、重复、乱序等；真实性是指确定交易者的真实身份和相应权限，以防冒名顶替；网络信息的可用性包括对静态信息的可获得、可操作性和对动态信息内容的可见性；不可抵赖性是指信息发出方、接收方不能抵赖已经发送的或已经收到的信息[2]。

3 前置机系统的安全性和交易完整性

为保障银行卡实时交易的信息安全，在商场收银POS前置机系统开发中，我们针对前置机系统的数据传输安全性、交易安全性和完整性进行了分析，并在对其安全技术进行研究的基础上，采取以下安全信息解决方案。

3.1 数据传输和交易的安全性

收银POS一体化项目通过商场内部网络与银联的专线来实现银行卡业务受理，一般是租用专线来传送信息，但所谓的专用线路是一种合法使用上的专有，它既不能完全防止不法分子非法使用专用线路，也不能完全防范不法分子对专用线路上传输的数据进行截获或篡改。此外，一笔银行卡交易数据，要在交易终端节点、银联、发卡银行等多个交易方之间传送、转发，为保证持卡人在内的各方利益，银行卡交易网络必须制定相应的安全传输规范。

笔者认为，金融交易数据的传输，关键是安全性方面的问题，且其安全性控制关键为以下3个方面：

1）数据的保密性。对用户密码这一敏感数据需要加密传输，以防止除接收方之外的第三方截获密码。

2）数据的完整性。用MAC防止非法用户对POS交易报文的帐户、金额、交易类型、主机的应答处理等进行无意或恶意的假冒、篡改、删除，防止数据传送过程中信息的丢失和重复，保证交易报文完整。

3）数据的可鉴别性。操作员对敏感数据进行电子签名，如对交易帐号、交易金额、交易时间和日期、交易终端号、交易流水号等进行有效的电子签名，为银行主机提供可靠的鉴别手段[3]。

通过分析，根据以上3个方面的安全控制原则，本文对安全性研究提出以下安全性解决方案。

3.1.1 交易安全性

双向认证 为保证收银终端POS密钥传输的安全，应用中我们引进双向认证的概念，也就是：在主机认证收银终端POS可靠性的同时，收银终端POS也必须认证银行主机的可靠性，防止伪终端或伪主机的交易非法处理。[4]

信息校验码 信息校验码即MAC，是确保信息在传输过程中没有误码、数据丢失、被篡改的一种标准。在银行卡网络中传送的每一个报文，都要附加MAC信息，而MAC信息是将关键性的报文和全报文经一定的算法运算后生成的。国际上通行的算法是DES算法。在实现时，对于传入银行卡网络中心的每一个交易报文，都生成了MAC；前置机系统对于银行卡中心传来的每一个交易报文也都进行了MAC校验。

密钥管理 在银行卡交易过程中，所有由终端采集的交易敏感信息如PIN密文、银行卡二/三磁道信息以及MAC密文等信息，只能够在采集、传输的过程当中在内存中存在，不能够在日志文件、数据库当中进行物理存储，或在显示器、打印机等设备上输出。故交易传输的敏感信息必须要经过一套密钥体系来保证安全传输的敏感信息[4]。

1）密钥体系

系统对传输数据的加密涉及到的密钥包括：主密钥（MK）、密钥加密密钥（KEK）和工作密钥（WK）。

主密钥（MK），用于对密钥加密密钥（KEK）进行加密保护，每台加密机只设置一个MK。MK存储在硬件加密机中，受硬件保护，不能被读取。MK由3段合成，应由不同人员掌握。

密钥加密密钥（KEK），用于对工作密钥（WK）进行加密保护，存储在加密机和密码键盘中。在商户端前置机的终端信息表当中，应登记每一台收银终端所对应的KEK索引号。KEK由两段合成，分别由不同人员掌握。KEK用于对工作密钥（WK）进行加密保护。KEK必须有安全保护措施，只能写入并参与运算，不能被读取。

工作密钥（Working Key），分为PIN加密工作密钥（PIK）和MAC加密工作密钥（MAK）两类，由收银终端签到时从银联POSP后台处理系统获得。

PIN的加密。PIN加密在加密键盘中完成，算法与银联直联POS终端规范保持一致，前置机不进行PIN加密。（限于篇幅，此处不详述。）

MAC 的算法。收银终端到前置机之间的报文传送，采用基于MAC的数据验证机制，收银终端上送的报文结构的pos_mac字段中存放MAC值。（限于篇幅，收银终端到前置机之间的MAC具体算法在此不详述。）

2）各类密钥的关系及一致性

安全机制所用相关符号定义如下：

Ek(data) -- 表示data被密钥k加密；

Dk(data) -- 表示data被密钥k解密；

KEK -- 加密机和密码键盘中的密钥加密密钥；

PIK -- 当前PIN工作密钥明文；

MAK -- 当前 MAC 工作密钥明文。

采用对称密钥体系，密钥关系如表 1 所示。

表 1　密钥关系表

Table 1　Key relation table

密钥名称	存储方式	维护方式	作用	保护方式
加密机主密钥(MK)	加密机	手工录入或 IC 卡注钥	保护 KEK	硬件
密钥加密密钥(KEK)	加密机和密码键盘	手工录入或 IC 卡注钥	保护 PIK、MAK	硬件
工作密钥(MAK)	加密机和密码键盘	动态下载计算 MAC	KEK 保护	数据库硬件
工作密钥(PIK)	密码键盘	动态下载保护 PIN	KEK 保护	数据库硬件

密钥之间的关系如图 1 所示。

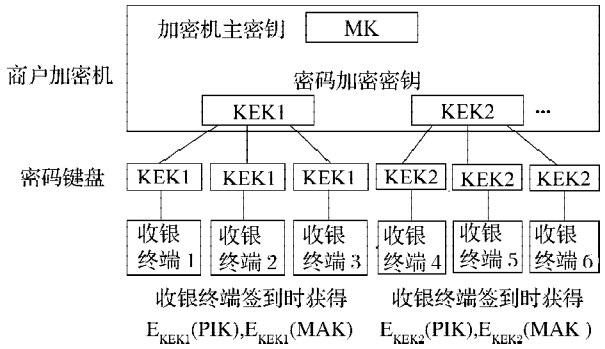

图 1　安全机制下密钥关系图

Fig. 1　Key relation map in safety mechanism

MIS 商户系统内，可以采用每台收银终端一个 KEK 的方式，也可以采用多个收银终端共用一个 KEK 的方式。

3.1.2　数据传输的安全性

1）利用硬件加密的方法

持卡人交易过程中的资金安全采用硬件加密的方式来实现，在交易的传输过程中都采用加密通道，前端收银 POS 采用了小密码键盘加密，交易到后台由硬件加密机对请求的交易包进行解密，整个数据传输采用了加密措施，难于被破解和截获，如果万一在传输过程中发生交易包的外泄或交易包被截取，交易包的 MAC 值校验就不会得到通过，这样，很好地保证了持卡人的资金安全[5]。其硬件结构如图 2 所示。

其中，硬件加密机用于保护密钥、PIN 的加密和解密以及消息鉴别。所有这些操作都在硬件加密机中完成，以保证密钥和 PIN 的明码只出现在加密机中，防止明码的泄露。硬件加密机应通过国家商用密码委员会的安全认证并允许在国内金融机构中使用。此外还必须满足以下要求：

i)支持单字节（B64）和双字节（B128）密钥；

ii)支持 PIN 的规定，验证、转换 PIN 的密文；

iii)支持 MAC 的规定，验证和产生 MAC；

iv)能对密钥作验证；

v)受到非法攻击时，加密机内部保护的密钥自动销毁。

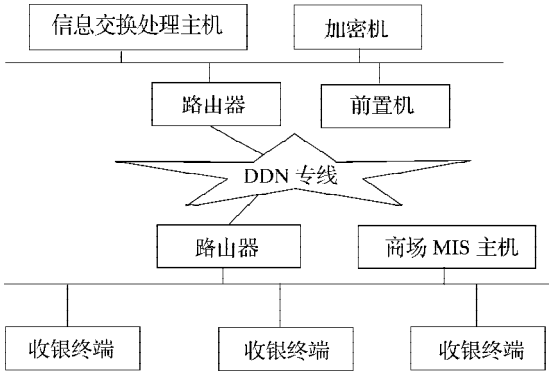

图 2　收银 POS 一体化系统硬件配置体系结构

Fig. 2　Hardware configuration constructure of cashier POS integrated system

2)利用通讯处理机制

商户内部网络与前置处理系统网络的通信配置上，仅开通由前置机到后台处理系统的单向 TCP/IP 和指定端口的基本套接字接口访问，路由器、防火墙等网络设备配置上应禁止除前置机之外的其他直联商户内部网络上的设备对后台处理系统的访问。采用 TCP/IP 协议，连接方式为短连接或长连接。通信双方以客户/服务器方式建立 TCP 连接，前置机作为 CLIENT 端，后台处理系统作为 SERVER 端。应答与请求在同一个连接中完成。由后台处理系统统一为每一个商户分配一个指定的端口[6]。

3)利用金融交易的专用通道和加密通道

网络内部主机均采用高性能容错处理机，具有高度冗余特性，能够保证全天候运行。网络系统内部骨干网为高速数据网络，网络设备关键节点均采用双机热备结构，避免单点故障。银联与银行，银联与各分店（或总店）之间的数据传输，均采用国密委批准使用的加密机（或加密键盘）进行加密，报文具有 MAC 鉴别码，保证数据不被破解和修改，且数据的传输使用专用线路。

3.1.3　管理安全性

再完善的安全技术措施，也必须有相应管理措施来保证。安全管理体系是基于现有成熟的银行卡安全管理体系，具有完善的银行卡风险管理模式。

总的来说，整个系统通过巧妙的风险控制，使得前置机系统在商场网络内部的环境下受理银行卡业务具有较高的安全性，也具有很高的实用价值。

3.2　交易完整性

由于银行卡交易牵涉的环节较多，在交易的过程中有许多不确定的因素存在，因此，为了保证交易各

方的利益关系，特别是持卡人的资金完整性，我们提出了在交易完整性中通过冲正来实现交易的完整性。冲正机制采用终端和前置机两级冲正、冲正存储转发的机制[7]。

3.2.1 收银POS终端冲正

收银POS终端对于由于超时或MAC校验失败等原因未能完成的交易，将产生原交易的冲正通知，并在下次联机交易之前自动上送前置机。前置机将检查冲正交易对应的原始交易：

①若原始交易为一笔成功交易，则将该交易标记为待冲正交易，同时应答POS终端冲正成功。

②若原始交易为一笔失败交易，应答POS终端冲正成功，但不将该笔交易标记为待冲正交易。

③若原始交易为一笔正在上送，尚未收到应答的交易，则该交易转为待冲正交易，应答收银终端冲正成功。

④若原始交易已经标记为待冲正交易，应答收银POS终端冲正成功。

对于待冲正交易，由前置机向银联POSP后台处理系统存储转发冲正交易。

3.2.2 前置机的冲正

前置机对于由于超时或MAC校验失败等原因未能完成的交易，或收到收银POS终端的冲正请求要求进行冲正交易，转入待冲正流水表，向POSP后台处理系统发送POS冲正交易，收到POS中心的冲正应答后，如果应答码为“00”、“25”以及“12”，则认为冲正成功，不再上送冲正请求，否则认为冲正不成功，继续上送冲正请求直至规定的重发次数为止。

3.2.3 存储转发机制

当交易传递的某一环节不能将需要的信息传递到下一环节时，该环节将需要传递的信息暂时存储起来，并依据某一设定的条件(如一定的时间间隔或与下一环节连通的状态)，再次与下一环节进行通信，以期取得通信的成功。

4 实验结果

银行卡金融交易的数据安全传输包括两方面的内容，一是持卡人个人密码的密文传输，一是交易过程中的整个交易包的加密传输，即PIN和MAC的效验。我们的实验是通过银联内部网络环境，对PIN和MAC的传输进行验证[8]。

4.1 PIN的验证

由终端发起一笔消费交易，在交易之前，首先在加密小键盘中已注入主密钥，然后将工作密钥PINKEY通过实时交易从后台处理系统下载到MIS终端密码小键盘中。交易时持卡人在加密小密码键盘中输入个人密码，此时在密码键盘上接收持卡人输入个人密码的明文，输入个人密码后由用户按确认键，发送到前置机后台，后台收到后只能看到的是个人密码的加密密文，即从52域中接收到，接收到16位的加密信息：0D8A717A3B1B4F5E，然后转换为8位的压缩BCD码密文，从实验的过程中，个人密码的传输在交易的过程中不出现密码明文，我们最后通过实验得出结论：个人密码的传输是已密文传输，保证了个人密码在交易过程中的传输是安全可靠的。

4.2 MAC校验

由终端发起一笔消费交易，在交易之前，首先在加密小键盘中已注入主密钥，然后将工作密钥MACKEY通过实时交易从后台处理系统下载到MIS终端密码小键盘中，交易过程中不要用户输入任何信息，此信息会在交易过程中自动将整个交易包用MACKEY对其进行加密产生一个16位的加密密钥，然后转换为8位的压缩BCD码密文，自动放到64域，随交易报文一并传输到前置机后台，前置机后台收到交易请求包首先对其MAC密钥进行校验，校验通过最终实现扣款，然后返回交易报文到终端机上，终端机再一次对交易的包MAC进行校验，从此实验的过程中，我们最后得出结论：MAC校验是经过双重认证的，可以保证银行卡在商场使用时是安全可靠的。

5 结语

通过研究与实践表明，本文提出的基于商场收银POS的前置机系统的安全技术解决方案，交易等待时间短，数据传输安全可靠。

参考文献：

[1] 刘延焕,万建华. 中国银行卡产业发展研究报告[R]. 上海: 科学技术出版社，2006.

[2] Mike Hendry. 智能卡安全与应用[M]. 杨义先，邱志聪，钮心忻，等译. 北京:人民邮电出版社，2002.

[3] Q/CUP 009-2004，中国银联MIS商户系统技术规范[S].

[4] JR/T 0002-2001，银行卡联网联合技术规范之中国银联POS终端规范[S].

[5] 李海泉，李 健. 计算机网络安全与加密技术[M]. 北京：科学出版社，2001.

[6] 赵志友. 信用卡系统总体设计方案[M]. 长沙: 湖南省建设银行网络管理中心，2006.

[7] Lakhina A, Crovella M, Diot C. Diagnosing Network-Wide Traffic Anomalies[C]//In ACM SIGCOMM. Portland：Boston University，2004：50-75.

[8] 李也白. 智能卡应用系统[M]. 北京：清华大学出版社，2000.