银行业务系统终端方式下安全防护技术的研究

Security protection Technology Research of Bank Operation System under Terminal Mode

王超美　（国防科技大学计算机学院 410073、中国工商银行金华市分行信息科技处 321000）
胡华平　（国防科技大学计算机学院 410073）

摘要：在分析银行业务终端安全隐患的基础上，本文提出了银行业务终端的安全防护对策，该防护策略主要包括业务终端的防伪技术、业务终端访问控制技术，并对业务终端的安全访问给出了设计方案。目前该方案已经在工商银行某市分行业务系统中得到应用，对防止内部人员作案，提高业务系统安全性提供了有效的手段。

关键词：终端方式　系统安全　防护对策　银行业务系统

1　引言

当前我国银行系统基本上采用字符终端作为临柜业务工作用机，通过 RS232 串口与业务前置机进行通信。随着各家银行数据的集中，各省分行以下的机构将很难接触到数据库的业务数据，越来越多的安全视点应该在终端访问的安全上。可是当前防火墙、黑客防范、链路密码机、VPN 网络加密机等基于 TCP/IP 网络防范技术的安全产品，对于防范内部作案或内外勾结作案收效甚微，对终端的访问控制更是没有涉及到。因此银行业务系统终端的安全是十分重要的，需要对终端访问控制方面进行深入的研究。

2　终端方式下的安全隐患分析

由于通信防护措施不到位、缺少合法终端的认证、访问时间的控制等，这些给犯罪分子提供了可乘之机。案例 1：某银行员工郝某伙同非银行员工的弟弟，安装开关通过搭线方式将非法终端串接在自己的终端上，利用中午客户少的时间，由郝某将线路切换到弟弟的非法终端上，弟弟通过网点隔壁的非法终端虚存 72 万资金，下午通过其他网点取走虚存的 26 万资金；案例 2：银行员工周某通过平时偷看同所员工翁某的密码，在储蓄所人员晚上下班后潜入所内，盗取储蓄所主任保管的该所准备用于代扣一户一表电费的活期存折 138 个，用窃取的翁某的操作卡和密码，在 138 个活期存折中虚存了 650 多万元。第二天，周某等在市区 31 个储蓄所，从虚存的活期存折中取款 67 笔共 289 万元。第一个案子是犯罪分子利用非法终端直接处理银行业务，第二个案子是犯罪分子在非营业时间（下班后）利用盗取的他人操作卡作案，这些犯罪案件给银行的存款安全敲响了警钟。

金融网点的业务系统安全，除了与终端通信密切相关，还与应用系统直接相关，主要存在以下几种安全风险：

- 系统对柜员的身份认证机制存在缺陷，柜员以磁条卡登录签到，而磁条卡易被复制伪造，因而大大降低了柜员签到认证的可靠性；
- 没有对存折打印机进行控制，使不法分子利用存折打印机作案有了可乘之机；
- 网点内部管理不健全，安全防范意识不强。

从目前银行业务终端的连接方式来看，可以归结为三种，即"多用户卡＋多路复用器"方式、终端服务器方式、网络终端直接连接方式等，以上三种方式均在不同程度上存在一些安全隐患分析。

2.1　采用"多用户卡＋多路复用器"方式连接终端

图 1　"多用户卡＋多路复用器"连接

图 1 给出了采用"多用户卡＋多路复用器"方式连接终端的示意图，图中业务前置机内插有多用户卡，它通过多路复用器进行远程连接。营业网点通过多路复用器连接终端，在每个终端上又挂接四种交易设备——键盘、密码键盘、刷卡器和存折打印机。其中，键盘、密码键盘、刷卡器是输入设备，存折打印机是输出设备。

终端和业务前置机之间通过简单的 RS232 串行通信方式连接。而 RS232 串行通信主要的安全风险表现为：一是由于明码传输，存在被窃听的可能；二是由于对终端没有提供完备的认证机制，存在假冒终端的可能。以上两种安全风

险,可能直接导致两种不同的犯罪方法——搭线窃听和通过在外接终端搭线伪造业务。搭线窃听通过从通信线路获取敏感信息,作为实施进一步犯罪的基础。通过在外接终端搭线伪造业务则一般采用内外勾结方式作案,具有更大的危害性和隐蔽性。此种连接方式可以通过双向关闭 MODEM,即主机房和网点同时关闭 MODEM 来防范非营业时间或下班后非法访问业务前置机的问题。

2.2 采用终端服务器方式连接终端

图 2 给出了采用终端服务器方式连接终端的示意图,网点终端通过终端服务器与业务前置机连接。

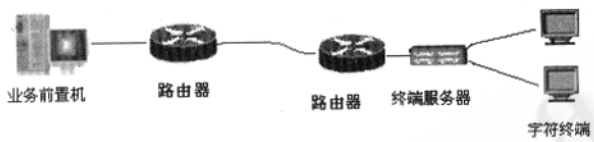

图 2 终端服务器方式连接

在图 2 中,终端与终端服务器之间用 RS232 连接,终端服务器一般安装在营业网点,终端服务器与业务前置机之间通过 TCP/IP 通信,前置机安装有服务程序作为服务端,终端服务器作为客户端。此种连接的方式存在假冒终端服务器风险,因为对终端没有提供完备的认证机制,如果没有有效的安全防护,非法终端的入侵点将扩大,增加了防范的难度,而且不能通过简单的关闭 MODEM 来控制非营业时间的非法访问。

2.3 网络终端直接与前置机相连

图 3 网络终端直接与前置机相连

图 3 是网点网络终端通过 TCP/IP 直接与业务前置机进行通信的示意图。网点的网络终端直接利用 telnet 功能登录业务前置机操作业务。网络终端相当于一台无盘工作站,仅具有网络功能。由于网络终端没有提供完备的认证机制,这种连接方式比前两种连接方式更容易被假冒,因为只要一台 PC 机和终端配套的外设就可以假冒网络终端。

3 业务终端安全防护技术与对策

3.1 研究现状分析

为确保银行业务系统的安全,增强其作业的可靠度和可信度,许多公司和各家银行对银行业务的终端安全做了许多研究,开发了一些安全产品。相关专业人士也正积极探索一些有效的防护对策。

针对"多用户卡 + 多路复用器"方式,一些公司推出了终端加密设备,其实现方式是在主机房的多用户卡和多路复用器之间串接加解密设备,在网点端的多路复用器和终端之间串接加解密设备,他们之间按照设定方式互相认证[2]。这种技术可以有效防止搭线窃听或中途窃取数据,同时也可以避免非法终端的接入。

为了解决终端设备的认证问题,目前主要研究并推出了两类身份认证方式,即 IC 卡方式身份认证和指纹方式进行身份认证。其中一种 IC 卡方式身份认证是只在终端上加入 IC 卡认证设备,操作者在登录时,首先必须插入个人的 IC 卡,否则即使密码正确,也不能够进入系统[3]。因此,只要妥善保管了个人的 IC 卡,就可以确信自己的身份是不能被窃取的。另一种 IC 卡方式身份认证是在原先业务前置机的多用户卡出口处和终端连接处分别放置 IC 卡控制器——置于终端的 IC 卡终端控制器和置于业务前置机多用户卡通信出口的 IC 卡主机控制器。IC 卡控制器被透明地连接在原有业务系统中,由此增加了多重身份认证(包括产品序列号认证、终端柜员 IC 卡口令认证、IC 卡控制器终端线路认证)、加密/解密和双重 Login 日志等安全功能,增强了业务系统安全性,能够有效防范金融犯罪。指纹方式进行身份认证是在终端上加入指纹仪,操作者在登录时,首先在指纹仪按下个人的拇指,将此时采集的指纹与指纹数据服务器中的指纹核对(事先采集),如果核对一致即允许进入系统,否则即使密码正确,也不能够进入系统。由于每个人的活体指纹是不同的,且无法复制,因此,可以确保个人身份不被窃取。

以上的研究和应用极大地加强了银行业务终端的安全,可以有效防止搭线窃听和非法终端的访问,但也存在以下问题:

(1) 随着各家银行网点网络的改造,网点与上一级的连接基本上通过 TCP/IP 方式,多路复用器方式连接除特殊地点外已经被置于网点的终端服务器和网络终端所代替,因此多用户卡与多路复用器之间串接加密设备方式无法满足其他连接方式的安全需要。

(2) 简单易行 IC 卡认证、CA 认证、指纹认证都需要 IC 卡读写器或指纹仪等专用终端认证设备的配合,在增加设备投入、加大维护工作的同时,应用范围也受到很大限制。

(3) 缺少对终端合法工作时间的控制,存在利用合法终端在非工作时间作案的可能性。

3.2 基于银行系统的业务终端安全防护技术

要确保银行业务前置机的安全,必须对终端的访问进行控制,防止非营业时间和非授权终端的访问。为此我们可以研究业务终端的防伪技术和业务终端的访问控制技术,从网点终端和业务前置机二个方面同时做终端访问的认证、访问

时间的控制等工作，以确保业务系统安全。

（1）业务终端的防伪技术。尽管可以采用 IC 卡身份认证或指纹身份认证来确保终端访问安全，但是 IC 卡认证、CA 认证、指纹认证都需要专用终端认证设备的配合，在增加设备投入、加大维护工作的同时，应用 范围受到很大限制，同时也改变了原有的使用习惯。将原有静态密码认证方式为动态密码认证可以在不改变原有使用习惯、不增加网点连接设备的情况下确保业务终端的安全。其具体思路是：主机房设置动态密码（令牌）认证服务器，给每个柜员发放一个令牌以产生动态密码，该令牌每 60 秒产生一个一次性不可预知的密码，与用户静态口令密码共同使用，每次登录业务系统都要对用户进行有效认证，保护业务系统的身份认证服务器安全软件检查密码并授权。这种认证方式不管对哪一种终端连接方式都适用。其特点是以变取胜、简单易行，该系统相对独立，接口简单，易与现有的应用系统连接，对正在运行的应用系统仅需做极小改动。采用专用认证服务器进行认证，保障现有应用系统的完整性，保护系统资源，其逻辑结构参见图 4。

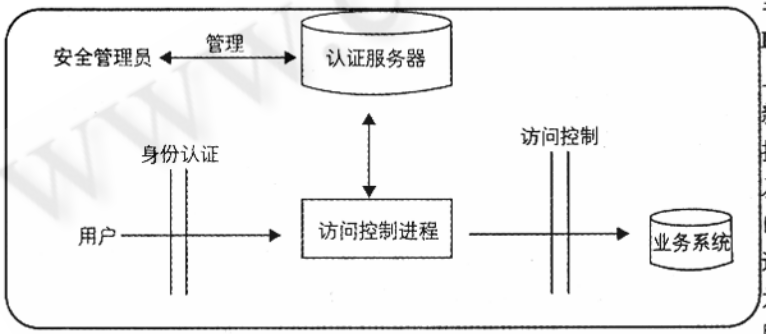

图 4　业务终端的防伪逻辑图

（2）业务终端访问控制技术。为了生产系统的安全，可以通过同时使用二种安全控制方式实现。

第一，根据工作时间，在服务器端编制服务程序 start，控制终端访问的时间，具体的思路是对每一个网点的每一台终端，根据工作时间，用文本文件列出控制的开关机时间（分上午、中午、下午、晚上、节假日）（用 2 个文件：工作日、非工作日），如与设定计划不符，即系统报非营业时间，如需延长必须经过手续由主机房操作员通过菜单修改，以防止犯罪分子在非工作时间利用偷盗的柜员卡和密码虚存资金。对于终端服务器和网络终端可以在前置机侧做 IP 地址和 MAC 地址捆绑校验，防止非法连接。为了防止非法登录，所有终端全部工作在哑终端方式，连接后终端上出现的画面不是 login 而是选择菜单，进而进入工作画面。之所以要使用哑终端，是因为在明终端模式下，登录的用户名输入是命令行方式，非法入侵者可以用试探法找出存在漏洞的用户名，潜入系统。具体实现为：

① 把所有终端设为哑终端，启动 start 时，从参数文件读出每个终端允许登录的用户和允许使用的时间，然后在终端上显示用户登录选择菜单，即综合业务、人行天地对接等菜单选项；

② 操作员选中要登录的菜单项后，程序检查是否在合法的时间段内，检查通过则根据/etc/passwd 文件检查该用户名，设置用户环境，并直接运行该用户的应用程序（在/etc/passwd 中指定）；

③ 配合后台监控进程（某 tty 终端合法的使用时间一到，即把 start 进程杀死，此 tty 终端就无法使用了），实现对终端使用的安全控制。程序设置了三个参数文件：

- config. txt – –终端登录控制文件，start 启动时读入；
- config. tmp – –终端登录控制临时文件，格式同上。当用户终端需临时增加用户或延长营业时间时，设置此文件，设置后即起作用，start 不需重启；
- user. txt – –系统用户名的中文对照，用于菜单显示。

第二，在路由器或交换机上做访问列表的控制，以防止非法设备连入网络中。网络中常说的 ACL 是 Cisco IOS 所提供的一种访问控制技术，初期仅在路由器上支持，近些年来已经扩展到三层交换机，部分最新的二层交换机如 2950 之类也开始提供 ACL 的支持。ACL 使用包过滤技术，在路由器上读取第三层及第四层包头中的信息如源地址、目的地址、源端口、目的端口等，根据预先定义好的规则对包进行过滤，从而达到访问控制的目的。网络中的节点分为资源节点和用户节点两大类，其中资源节点提供服务或数据，用户节点访问资源节点所提供的服务与数据。ACL 的主要功能就是一方面保护资源节点，阻止非法用户对资源节点的访问，另一方面限制特定的用户节点所能具备的访问权限。

4　结束语

本文在分析银行业务终端安全隐患的基础上，提出了业务终端的安全防护对策，并对业务终端的安全访问给出了设计方案。目前该方案已经在某市工商银行系统得到应用，对防止内部人员作案，提高系统安全性提供了有效的手段。

参考文献

1　陈卫东，加强和完善信息系统的安全管理。URL http://www. zgjrj. com/jsbz/new_page_1. htm

2　工商银行技术保障部，强化计算机安全管理 促进银行电子化建设健康发展，中国金融电脑，2000(2)。

3　IC 卡终端身份认证系统 URL http://www. ctiforum. com/factory/xinyada/xiyada01_0414. htm.