铁路车站客票预售票系统网络安全问题的探讨

黄红 曾云平 许宏丽 (北方交通大学计算中心 100044)

摘要:本文就影响车站售票系统不安全因素进行了分析,着重对网络结构、信息处理、数据库、网络安全管理等提出了一系列安全措施,以保证车站售票系统的安全运行。

关键词:安全 局域网 车站售票系统

车站售票系统网络是整个客票系统网络的基础,根据车站的大小及客运量的多少,网络的规模也相差甚远。大的车站售票窗口可多达 40 个以上,并且还与市内的售票点相连接,日售票量很大;而较小的车站,只有几个售票窗口,日售票量较少。根据网络需求和应用负载等情况,车站售票系统的网络以局域网为主,辅之以必要的远程网,用以连接站内较远的售票点或市内售票点。车站售票系统是与旅客接触最直接的窗口,所以它的安全也是很重要的。

一、威胁车站售票系统安全因素

1. 威胁局域网安全因素

通信线路上由于电磁信号辐射,造成接受信息混乱发生死机现象。对通信介质的攻击,包括被动方式攻击(搭线窃听)和主动攻击方式(无线电仿冒),通过联接上网一个未授权的工作站而进行的网络攻击。攻击的方式可能有:窃听网上登录信息和数据;监视 LAN 上流量及与远程主机的会话。在合法工作站上进行非法使用,如截获合法用户 logoff 指令,继续与主机会话;冒充一个主机 logon,从而窃取其他用户的 ID 和口令,非法对局域网上资源进行删除修改。在局域网上,如果没有完善的访问控制,冒充合法用户对资源进行访问是比较容易的。局域网与其他网络联网时,即使各成员网能安全运行,联网后也可能发生相互侵害的后果。网络病毒也会对局域网造成严重的威胁。

局域网用户缺乏安全操作常识,局域网提供商的安全允诺不能全部实现,造成了局域网环境威胁。局域网的每一组成部分都需要保护,包括服务器、工作站与局域网的连接部件、局域网与局域网及外部世界的连接部件、线路及线路接续区等。

2. 车站售票系统本身的安全问题

对于车站售票系统来讲最重要的是要保障客票座席数据库的数据的安全,它是客票发售和预定系统的最基本的数据,所以要保证它的完整性和一致性。这包括保证车站售票系统电源设备的安全,服务器和磁盘系统的安全是保证整个客票系统安全的基础,实行异地售票要保证数据通信网络的安全,对车站售票系统加密也是保护信息最有效的方法之一,确保车站与车站局域网之间信息的安全,建立在自然灾害情况下的安全措施,建立系统安全运行与管理措施,以及杜绝伪造软纸车票给铁路经济和旅客造成的危害等。

要保证存根数据的安全。因为售票存根数据的"重放"和篡改对财务和审计造成主要的威胁。例如,铁路免票乘车证存根"重放"可能导致正常票款的流失,篡改本站发票的异地始发车车票存根,将导致车站内的清算纠纷。以上问题若无公正技术解决方法,将会导致真正责任者对所犯罪行的抵赖。此外由于存储介质损坏或失败也会造成存储数据出错或丢失。比如用磁盘长期存储售票存根,就面临此威胁。

二、车站售票系统的安全措施

车站售票系统采用局域网结构,所以它的安全措施可以采用加密装置、加密软件、访问控制和验证等方法。由于车站售票系统选择配置不同,它所受到的威胁也不一样,实现的方法也有所差别。车站售票系统所用的操作系统和数据库的环境是一样的,使用 unix 操作系统和 SYBASE 数据库环境。车站售票系统安全可靠的使用要考虑以下几个方面:

1. 场地、电源系统的安全

硬件系统的安装场地必须符合国家及铁道部的有关

© 中国科学院软件研究所 http://www.c-s-a.org.cn

标准，必须设置防火、防雷设备。电源系统应备有双路供电系统和可靠的 UPS 设备。

2. 网络构造

网络的构造不同对局域网的安全有着重大的影响，如在建造网络时，采用环形拓扑，那么任何一个节点的故障，就会影响整个网络的安全性、可靠性，同时每个报文都要通过中间节点转发，数据的安全性也没有保障。考虑到车站售票系统的应用范围，要求的安全可靠程度，所以车站售票系统禁止采用环形拓扑结构，这样避免由于一个节点故障影响整个售票系统。车站售票系统采用以太网技术，它使用总线拓扑结构，即 CSMA/CD 方法。

3. 多级访问控制

多级访问控制在局域网内，数据和流量必须加以控制，否则用户和数据为争用户访问权限产生混乱，数据就会产生碰撞，引起信息丢失或网络挂起等现象。为了避免上述现象发生，必须严格使用网络协议。

4. 通信安全措施

对抗电磁信号侦听，电缆加屏幕层或用金属管道，使较常规电缆难以塔线窃听；使用光纤消除电磁辐射；对敏感区域进行物理保护。

对抗非法工作站的接入：最有效的方法是使用工作站 ID，工作站网卡中存有标识自身的唯一 ID 号，LAN 操作系统在用户登录时能自动识别并进行认证。

对合法工作站的非法访问：主要通过访问控制机制，这种机制可以逻辑实现或物理实现。

5. 网络可靠性

网络可靠性的目标是建立一个具有软硬件容错功能的数据传输系统，为了保证客户/服务器结构中远程数据访问和通信，通信网上要求有足够的动态备份路由。关键部分的网络设备应达到动态备份要求。一般站点，网络设备也应采取一主一备的配置，故障时网络系统的切换不应超过 30 秒钟。为了保证安全，车站售票系统的服务器均采用双主机热备份，RAID 磁盘阵列，磁盘双工等容错技术。

大城市内车站售票量大，一般在市内均设有铁路售票处或地方代售点。可以采用铁路专线或租用共用数据通信线路(DDN)方式和电话后备份方式，将这些售票处或代售点直接连到车站局域网路由器，以保证通道更可靠安全。

在这个过程中，路由器提供最高程度的冗余码和容错能力。在网络终结时，实施阻塞控制，以确保信息包在互连网中没有关键性错误而引起超时。路由器是大型车站售票系统与远程售票处连接必不可少的通信设备。

6. 访问控制

访问控制要在操作系统、网络和应用软件三级采取安全保护措施。在操作系统级，用户在开机时要输入用户名和口令，如果口令不符，不准启动系统。用户上网后，也要对输入口令进行验证，网络系统查看它是否是网上的合法用户，若不是则拒绝上网。进入系统后若要访问系统资源，在应用级中必须核对用户权限，看此用户是否有权访问其资源，如访问权限与系统设置不符，则拒绝访问。访问控制中文件应受保护，为保护数据使用的安全，对数据库的存取、修改要设置权限，严防非法用户的侵入或超级操作。

7. 信息加密

车站售票系统是客票发售和预订的重要部分，数量多，分布范围广，主要完成售票、订票、退票、财务结算等功能，同时处理来自地区售票中心的下载信息。这些信息是客票预售系统的基本数据，所以要保证这些重要数据的安全。

对于车站客票预售系统，实行加密措施也是保护信息的最有效的方法之一。加密的重点应是数据加密，对财务、统计等重要数据进行加密，采用加密装置或加密软件包方式。加密方法包括数据加密、敏感信息加密、通信线路上的数据加密等。通信数据加密方法有两种，一种是链路加密，即点对点加密；另一种加密是端端加密。以下是对几种加密方法进行比较。

链路加密：在通信网络中，每两个节点之间采用一对加密与解密设备。作用于 OSI 数据模型的数据链路层，信息在一条物理链路上进行加密和解密。此类系统中，加密盒置于线路的两端，这样可确保传送数据的可靠性和完整性。它的特点是独立于提供商，能保护网上的控制信息，密钥管理简单，但是数据与通信控制信息必须在中继节点解密变为明文，并经过再加密才流到下一个节点，因此通信节点必须安全、可靠。缺点是浪费设备，降低传输效率。

端端加密：即用户对用户加密。数据在整个传输过程中都可以保持保密形式。作用于 OSI 数据模型的第 4～7 层，其优点是花费少，效率高。对于采用分组交换的通信网来说，通信控制必须以明文方式传输，所以它依赖于网络协议，安全性不很高。

应用加密：作用于 OSI 数据模型的第 7 层。其优点是花费少，效率高；缺点是加密算法和密钥驻留于应用

© 中国科学院软件研究所 http://www.c-s-a.org.cn

层，易于失密。

使用终端认证设备将各个终端唯一编码，利于主机识别软件及硬件系统。只有带有正确的网络接口卡(NIC)标识符的设备才允许登录。

使用消息认证设备用于保证传送消息的完整性。它们通常用于更加注重消息不被更改的应用领域。一般采用基于 DES 或 RSA 的加密算法。

8. 座席数据库的安全

座席数据库是客票发售和预订系统的核心动态数据库，能否准确地生成与维护是计算机售票成败的关键。座席数据库的生成维护、修改要由专人负责，对座席数据库进行修改后，要经过认真确认后再存储，避免造成座席数据库错误，以保证数据的一致性。

9. 存根数据

存根数据是售票业务的记录信息，它不仅反映售票工作的实际情况，而且是统计分析财务结算的依据，所以存根数据应具有较高的保密性。因此对存根数据的保存，要采用纠错编码、定期转储等措施来防止因存储介质损坏造成的数据出错或丢失。存根数据生成后要禁止作任何的修改和变更，对它的查询也要受到控制，以保护它的完整性和安全性。

由于售票系统中的存根数据是财务部门最原始数据，它是实施财务收入核查、财务清算与审计的基础，所以，必须对售票存根等重要的数据实施“数据签名”来保证财务与审计的安全性。

10. 计算机病毒的防御

车站售票窗口对座席数据访问是随机的，具有很强的实时性。由于计算机直接面对用户，而且操作系统比较简单，更容易被病毒感染。因此对计算机病毒的预防和消除是非常重要的。计算机病毒的入侵途径是从局域网的 Client 感染到 Server 上，首先要防的是工作站的入口。有盘工作站软件由两部分组成，一是防病毒部分，利用智能病毒防御技术对所有病毒进行防御；二是杀病毒部分，利用快速扫描查毒技术，可以消除所有引导型病毒和已知的文件型(包括各种)病毒，它包含了国内流行的绝大部分病毒，并率先实现清除第三代变种病毒。无盘工作站增加防病毒部分，无盘工作站虽然没有硬盘和软驱，但它同样有内存，当无盘工作站上运行服务器上带病毒程序时，病毒会驻留在该无盘站内存中。反过来，它会传染服务器上的其他文件，造成网络上病毒的迅速传播。在无盘站引导时先驻留防病毒程序，就可防止无盘站运行病毒程序，避免恶性循环。

11. 网络文档

做好网络文档工作，也是对网络安全的必要保护。从网络健康角度来讲，有必要强调网络文档的重要性。如果网络有了很好的档案，就会大大减少网络维护和故障处理时间。应建立网络布线文档，如建立网络拓扑图、网络功能图，建立网络全部站点列表、用户名、协议地址(IP、IPX)等。还应建立网络系统文档，如服务器网络硬件文档和服务器网络软件文档、网络全部网卡文档、全部网络设备文档等。

12. 网络安全管理

在车站售票系统局域网中，为了保证网络能安全、可靠地运行，必须要有网络管理。它的主要任务是对网络资源、网络性能和密钥进行管理，对访问进行控制，对网络进行监视。网络管理应负责对该网的构造和性能进行管理，用户不能随意改变网络的拓朴结构。如果网络采取加密措施，还要对密钥进行管理。

局域网安全管理的一般控制原则：对服务器访问只能通过控制台，工作站间不得自行联网，同一时刻一个用户只能登录一台工作站，禁止使用网上流量监视器，工作站自动挂起，会话清除，键盘封锁，交易跟踪等。

口令控制：规定最大长度和最小长度，字符多样化，建立及维护一个软字库，鉴别口令字，经常更换口令等。

审计日志：应记录不成功的 logon 企图，未授权的访问或操作企图，网络挂起，脱离联接及其他规定的动作。应具备自动审计日志检查功能。审计文件应加密等。

磁盘使用：公用目录应只读，并限制访问。对重要数据库磁盘要有双份，以防止磁盘突然故障。

数据备份：是 LAN 可用性的保证。除镜象磁盘中的数据库备份外，基础数据的维护库与运行库互为备份，存根信息的车站数据库与地区数据库互为备份。基础数据每天维护后拷贝到磁带上，作为一天的历史信息。

物理安全：限制通信访问的用户、数据、传输类型、日期和时间。

为增强售票系统的安全，要制定相应的安全方针和安全策略，对新增加网络用户、增进网络资源时要有正规的程序。

铁路客票发售和预定系统是高新技术的集成，是一项非常复杂的系统集成。本文仅就车站售票系统的网络安全问题提出了一些参考措施，但还需要在实际应用中得到调整和完善，为中国铁路客票系统的顺利实施打下基础。

(来稿时间：1997 年 9 月)

© 中国科学院软件研究所 http://www.c-s-a.org.cn