文章编号：1005-8451（2008）01-0031-04

北京地铁5号线乘客信息系统安全体系的设计与实现

蔡晓蕾[1]，朱胜利[2]，陈玉峰[3]，王 浩[1]
（1.中国铁道科学研究院 电子计算技术研究所，北京 100081；
2.北京市轨道交通建设管理有限公司 科技部，北京 100037；
3.北京神州数码有限公司，北京 100085）

摘 要：介绍北京地铁5号线乘客信息系统安全保障体系的设计目标和设计原则，根据北京地铁5号线乘客信息系统的需求和实际情况，对系统部署的安全体系架构和实现方案进行详细论述。

关键词：乘客信息系统；信息安全；网络安全；地铁
中图分类号：U231.92-39 **文献标识码**：A

Design and implementation of Safety Structure of Passenger Information System for Beijing 5th Urban Railway

CAI Xiao-lei[1], ZHU Sheng-li[2], CHEN Yu-feng[3], WANG Hao[1]
(1.Institute of Computing Technologies, China Academy of Railway Sciences, Beijing 100081,China;
2.Beijing Urban Railway Construct Manage Ltd., Beijing 100037, China;
3.Digital-China Ltd., Beijing 100085, China)

Abstract: The object and principle of safety structure design of Passenger Information System for Beijing 5th Urban Railway were described. Based on the demands and facts of the System, the safety configuration and implementation way were proposed in detail.

Key words: Passenger Information System (PIS); information safety; safety of network; urban railway

北京地铁5号线南起宋家庄，北至天通苑北，正线线路全长约27.6 km。全线设23座车站，其中16座为地下站，7座为地面站或高架站。北京地铁5号线乘客信息系统依托多媒体网络技术，通过布设从线路控制中心到各车站的有线网络以及隧道区间内的无线局域网络，可以实现控制中心到车站及车厢的文字、图像和视频信息的实时双向传输。乘客信息系统是一个大型的信息系统，应着重加强网络安全和应用系统安全建设，针对可能遇到的各种安全威胁和风险，采取行之有效的安全措施，保障系统中信息的保密性、完整性和可用性。

1 乘客信息系统安全保障体系设计目标

1.1 互连接口处的网络访问控制与隔离

与其他专业之间的网络连接使用高强度安全设备进行隔离。网络之间通过防火墙进行网络隔离与网络级访问控制。此外，在各专业之间进行信息交换时，还应进行高强度的网络访问控制，严格限制用户的访问资源范围。

1.2 移动接入系统的访问控制

对于内部移动用户和移动列车，应保证具有防止非法用户（节点）进入网络、抗攻击和抗信息在传输过程中被窃取、失密等安全功能。

1.3 网络防病毒

采用网络防病毒系统与单机防病毒软件相结合的方式，构建起一套完整的防病毒体系。

1.4 对重要信息数据及其相关重点服务器的保护

在物理环境安全、安全运营管理和数据安全保密等方面采取有效的技术手段，保证重要信息的安全。如在关键的服务器上配备主机入侵检测系统、主机脆弱性扫描系统、设置合理的备份和恢复系统、以及完善的机房监控和管理系统等。

1.5 实现多级的访问控制

对网络中的计算机进行基于地址的粗粒度访问控制或基于用户及文件的细粒度访问控制。访问控制措施对内部和外部访问者同样有效。

1.6 建立网络安全评估体系

收稿日期：2007-08-01
作者简介：蔡晓蕾，在读硕士研究生；朱胜利，工程师。

采用网络安全分析系统，定期评估网络的安全性，以便及时发现网络或系统漏洞，并制订提高网络安全强度的策略。

1.7 完善安全管理机制

建立完善的安全管理机构及安全管理制度，实现安全管理培训制度化，制定有效措施保证系统安全措施的执行，强化安全管理。

2 乘客信息系统安全保障体系设计原则

2.1 可实施性原则

安全体系中的网络风险分析以及网络安全需求分析都是从可实施的角度出发的，按照体系的指导，可以直接把目前已有的安全技术、安全产品、安全措施、网络设施建设、直至管理规范都规划到某个安全层次中去。因此，安全体系不是一个学术化的理论体系，而是一个用于指导实际工作的可实施的体系。

2.2 可管理性原则

制订安全体系时应建立一个动态的、可控的安全体系结构，管理人员不需要掌握具体的安全技术，而是在一套合理的安全规范的指导下，就可以管理网络的安全。这样，可以有效地对安全设备和安全技术进行利用与管理，使得整个网络的安全性是可控的。

2.3 安全完备性原则

安全是一个多层面的问题，同样，安全体系也是一个多层次的结构。以安全的层次理论模型为基础，从安全层次出发，进行详细的安全分析，再从每一个层次中分离出若干子系统，完整地将网络的总体安全因素都考虑在内，可以保证基本不会遗漏大的安全问题和安全隐患。

2.4 可扩展性原则

随着网络的扩展，其网络结构和应用结构也会日趋复杂。北京地铁5号线乘客信息系统安全体系考虑到了这一点，安全体系的可扩充性结构为以后的网络扩展和业务扩充都预留了接口，只要在安全防护体系的指导下，系统的实施都可以采取更新的技术、更换更高档次的产品、或进行拓扑的扩充来对安全功能进行扩展和延续。

2.5 专业性原则

北京地铁5号线乘客信息系统安全体系所涉及的所有网络安全的概念、系统定义和体系思想，都是参考目前国内、国际有关网络安全的专业规范制定，均符合相关的安全标准，这样可以确保本安全体系的技术深度和专业性。

3 乘客信息系统安全保障体系架构

北京地铁5号线乘客信息系统对安全的需求是全方位的和整体的，相应的安全体系也是分层次的，不同层次反映不同的安全问题。根据北京地铁5号线乘客信息系统的应用现状情况和网络的结构，将安全体系划分为5层：物理层安全、系统层安全、网络层安全、应用层安全以及安全管理。如图1。

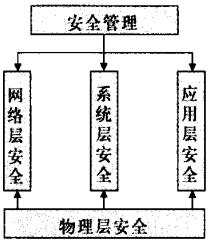

图1 安全体系层次结构

3.1 物理环境的安全性（物理层安全）

包括通信线路的安全，物理设备的安全，机房的安全等。物理层的安全主要体现在通信线路的可靠性（线路备份、网管软件和传输介质）；软硬件设备安全性（替换设备、拆卸设备、增加设备）；设备的备份；防灾害能力，防干扰能力；设备的运行环境（温度、湿度、烟尘）；不间断电源保障，等等。

3.2 操作系统的安全性（系统层安全）

这一层次的安全问题来自网络内使用的操作系统：Windows 2000/XP/2003等。系统层的安全性问题表现在3方面：（1）操作系统本身的缺陷带来的不安全因素，主要包括身份认证、访问控制和系统漏洞等；（2）操作系统的安全配置问题；（3）病毒对操作系统的威胁。

3.3 网络的安全性（网络层安全）

该层次的安全问题主要体现在网络信息的安全性。包括网络层身份认证，网络资源的访问控制，数据传输的保密与完整性，远程接入的安全，域名系统的安全，路由系统的安全，入侵检测的手段，网络设施防病毒等。

3.4 应用的安全性（应用层安全）

该层次的安全考虑提供服务所采用的应用软件

和数据的安全性，包括：广告制作、媒体发布系统等。此外，还包括病毒对系统的威胁。

3.5 管理的安全性（管理层安全）

安全管理包括安全技术和设备的管理，安全管理制度，部门与人员的组织规则等。管理的制度化程度极大地影响着整个网络的安全，严格的安全管理制度、明确的部门安全职责划分和合理的人员角色定义都可以在很大程度上降低其他层次的安全漏洞。

4 乘客信息系统安全保障体系的实现

根据北京地铁5号线乘客信息系统应用的实际环境，重点从网络体系、应用体系以及管理体系进行安全部署，保证系统安全保障体系的实现。

4.1 网络体系安全部署方案

4.1.1 外部网络接口安全部署方案

（1）控制中心采用2台服务器主备方式运行，避免主机单点故障；

（2）每台服务器与内部网络连接均配置双网卡，连接到两台不同的交换机，避免控制中心内部网络单点故障；

（3）外部接口采用2条线路分别接到2台防火墙，2台防火墙分别连接2台服务器，避免外部线路单点故障；

（4）与其他专业连接均采用防火墙过滤，防止外部攻击，保证网络安全；

（5）2台服务器均安装瑞星防病毒软件，定期更新病毒库，保证系统软件安全；

（6）2台服务器以串口的模式连接外部线路，关闭不需要的服务。

4.1.2 内部无线网络安全部署方案

（1）设置复杂的SSID，隐藏并禁止WLAN向外广播SSID，避免无恶意用户的侵入；

（2）设定MAC绑定认证，禁止未经绑定的MAC地址设备访问网络；

（3）采取WPA-PSK认证，确保用户接入的合法性，WPA-PSK认证的通用密钥长度在8 bit~63 bit之间选择，可设置复杂的密钥；

（4）采取WPA-TKIP对无线传输数据进行加密，由于TKIP采用的是动态密钥管理机制，保证了无线传输很难被攻破；

（5）启用WLAN的防火墙和WIP策略，检测并过滤已知的无线恶意攻击。

4.1.3 内部有线网络安全部署方案

有线网络包含了不同的层次，因此，安全性必须贯穿于各个层次，北京地铁5号线乘客信息系统的有线网络从下面几个方面进行部署。

（1）交换网络设备本身的安全强化：交换网络设备本身的安全性隐患包含设备缺省的配置、Dos攻击和网络蠕虫等。这些安全隐患都为网络攻击提供方便之门。应通过交换机设备自身的强化来保护设备的安全。北京地铁5号线乘客信息系统选用了阿尔卡特OmniSwitch系列交换机，该系列交换机设备可以通过缺省的安全性和拒绝服务Dos攻击防御、网络蠕虫攻击等措施进行设备本身的安全强化。

（2）部署交换网络设备管理的安全性，通过对OmniSwitch交换机进行网络分权管理、交换机访问的认证、安全的Socket层、SNMPv3以及自动退出等部署，从而实现设备管理的安全性。

（3）部署交换网络设备网络访问属性的安全性，对OmniSwitch交换机的网络访问属性进行访问控制列表和VLAN绑定。

（4）部署防火墙和入侵检测系统：配置防火墙是保证网间访问安全的一个核心措施，但是防火墙只具备静态的访问控制能力，而且缺少足够的深度协议分析和内容检测能力。因此，在5号线乘客信息系统中部署入侵检测系统，对各种网络攻击行为进行实时深度检测，构建深度动态防御体系。根据北京地铁5号线乘客信息系统的网络结构和应用模式，在控制中心选用华为3Com公司的SecEngine D500部署入侵检测系统。

（5）部署漏洞扫描系统：漏洞扫描是对系统脆弱性的分析评估，能够检查、分析网络范围内的设备、网络服务、操作系统和数据库系统等系统的安全性，从而为提高网络安全的等级提供决策的支持。北京地铁5号线乘客信息系统选择在控制中心配置绿盟科技的RSAS远程安全检测系统，通过该项部署，可及时发现网络漏洞并在网络攻击者扫描和利用之前予以修补，从而提高网络的安全性。

4.2 应用体系安全部署方案

（1）建立访问控制。通过对特定网关、网段和服务建立的访问控制体系，将绝大多数攻击阻止在到达攻击目标之前。通过安全边界产品，严格控制不同安全等级间的访问，保证数据由安全级别较高的专业生产系统向安全级别较低的管理系统等流动

的单向性；

（2）检查安全漏洞。通过对安全漏洞的周期检查，即使攻击可到达攻击目标，也可使绝大多数攻击无效；

（3）攻击监控。通过对特定网段和服务建立的攻击监控体系，可实时检测出绝大多数攻击，并采取相应的行动（如断开网络连接、记录攻击过程和跟踪攻击源等）；

（4）加密通讯。主动的加密通讯，可使攻击者不能了解和修改敏感信息；

（5）认证。防止攻击者假冒合法用户；

（6）进行备份和恢复。在攻击造成损失时，尽快地恢复数据和系统服务；

（7）设置多层防御。攻击者在突破第1道防线后，延缓或阻断其到达攻击目标；

（8）隐藏内部信息，使攻击者不能了解系统内的基本情况；

（9）设立安全监控中心，为信息系统提供安全体系管理、监控以及紧急情况服务。

4.3 管理体系安全部署方案

安全管理在系统的安全保密中占有非常重要的地位，即使有了完善的安全保密技术措施，如果管理的力度不够，也会造成严重的安全隐患。因此，系统的安全方案应特别强调不能忽视安全保密管理，并提供安全保密管理的具体措施。

4.3.1 安全管理机构

为了增强安全保密管理，必须建立安全保密管理机构。要有职能部门负责各个部门的计算机安全保密管理。由相关领导主管计算机安全工作。安全保密管理网络覆盖各个相关部门。安全组织机构要制定安全规划和应急方案。针对风险和威胁采取主动和被动相结合的防治措施。安全组织机构要制定信息保护策略，确定需要保护的数据的范围、密级或保护等级，根据需要和客观条件确定存取控制方法和加密手段。

4.3.2 安全管理制度

应提出明确的安全保密管理制度。安全保密管理制度包括：场地与设施安全管理；出入控制管理；设备管理；存储介质管理；相关信息管理；口令管理；数据备份管理；计算机病毒防护管理；安全审计管理；应急措施等方面。

4.3.3 系统安全管理

依据系统的安全保密策略建立不同等级的安全管理信息库。这些安全信息可以是数据表格形式、文档形式、嵌在系统软件或硬件中的数据库或规则等。系统安全管理要求保障管理协议和传送管理信息通道的安全，防止潜在的各种安全威胁和破坏。特别是两个安全保密管理应用软件之间的通信更应该保证其安全性。

4.3.4 安全事件处理

需要对网络进行大量的风险分析和安全分析，比如，明确资源状况、资源弱点、预测事件发生的可能性、事件损失的评估、保险安排、故障控制、安全计划等一系列工作。安全事件处理管理要确定安全事件报告的界限和远距离报告的途径以及处理内容等。

4.3.5 安全审计管理

包括记录和远距离收集安全事件、启用和终止被选安全审计记录数据、跟踪调查安全事件和形成安全审计报告等。安全审计数据应防止被任意调用、修改和破坏。

4.3.6 安全恢复管理

对安全事故制订明确的安全恢复计划、规程和操作细则，提出完备的安全恢复报告。必要的备份措施是成功恢复的关键。备份包括：通信中心备份、线路备份、设备备份、软件备份和文档资料备份等。安全主管部门应建立安全恢复文档资料。

4.3.7 人员管理

做好人员审查、人员培训和人员考核工作。

5 结束语

北京地铁5号线乘客信息系统是一个架构在有线和无线网络体系之上的大型多媒体视频信息系统，且与其他专业存在着大量接口，安全保障体系的设计和实现对系统成功实施起着关键性作用。在系统设计、实施过程中应重视对网络、应用和管理各方面的安全部署，从而确保系统能够安全、稳定和可靠地运行。

参考文献：

[1] 艾寿民. 网络安全技术探析[J]. 商场现代化，2007（4）.

[2] 李雪梅. 工业系统信息安全管理体系的构建[J]. 微计算机信息，2007（3）.

[3] 王 皓. 网络信息安全获取与传输系统研究与实现[J]. 四川大学学报，2007（1）.