文章编号：1005-8451（2013）03-0001-04

铁路客运服务系统信息安全测试方法研究

姚洪磊[1]，李红建[2]，张　彦[1]，周泽岩[1]，祝咏升[1]
（1.中国铁道科学研究院　电子计算技术研究所，北京　100081；
2.沪汉蓉铁路湖北有限责任公司　技术装备部，武汉　430000）

摘　要：铁路客运服务系统是铁路信息系统建设中的一个重要组成部分，目前客运服务系统已实现互联网售票、电子支付等对外服务，铁路客运服务系统安全保障平台已成为保障客服信息系统安全的重要手段。本文从应用安全、网络安全、主机安全和数据安全4个方面对铁路客运服务系统安全保障平台开展测试，研究其在铁路客运服务系统联调联试中的应用，提出了一套针对现有安全保障平台的信息安全测评方法和内容。

关键词：铁路客运服务系统安全保障平台；信息安全测评体系；联调联试
中图分类号：U293：TP391　**文献标识码：**A

Research on method of information security test for Railway Passenger Service System

YAO Honglei[1], LI Hongjian[2], ZHANG Yan[1], ZHOU Zeyan[1], ZHU Yongsheng[1]
(1.Institute of Computing Technologies, China Academy of Railway Sciences, Beijing　100081, China ;
2.Equipment Department, Hubei Hu-Han-Rong Railway Limited Liability Company, Wuhan　430000, China)

Abstract: Railway Passenger Service System was an important component element in Railway Information System. Right now, Internet ticketing, electronic payment had been implemented in Passenger Service System, security threats was gradually increased. Security safeguard platform was the important method for protecting Railway Passenger Transport Service System. In this paper, four aspects such as application security test, network security test, host security test, and data security test would be carried out on the System of railway passenger service security safeguard platform, their application would also be researched in combined test of Railway Passenger Service System, an information security testing method was proposed refer to the security safeguard platform in use.

Key words: railway passenger service security safeguard platform; Information Security Safeguard Testing System; combined test

目前，铁路客票系统已实现了互联网售票、电子支付等服务[1~2]，随着系统开放，其受外部攻击、病毒感染的安全威胁也逐步增大，铁路信息系统安全建设变得尤为重要。在国内其它行业及机构信息系统安全测评研究和相关标准规范的基础上[3~7]，本文通过开展铁路信息系统安全控制测评及整体测评研究，排查系统安全隐患和薄弱环节，提出有针对性的抵御威胁的防护对策和整改措施，发掘系统中存在的安全隐患和防护漏洞，评估铁路客运服务系统的安全防护措施与所定安全等级间存在的差距，提供基础安全保障并推动铁路信息系统安全等级保护工作。

1　系统组成与部署现状

1.1　系统组成

铁路客运服务系统主要包括票务系统和旅客服务系统。

铁路客运服务系统信息安全保障平台由安全管理设备和分布式防护设备组成，通过专用的安全通信协议，安全管理设备实现对分布式设备的控制和管理，其中安全管理设备由密码服务、安全认证、安全通信设施等构成；分布式设备主要由防火墙、网闸、防病毒、入侵检测系统（IDS）以及安全代理等组成。

收稿日期：2012-07-18
基金项目：中国铁道科学研究院基金项目（1052DZ1301）。
作者简介：姚洪磊，助理研究员；李红建，高级工程师。

1.2 安全部署现状

铁路票务系统安全建设依托所属铁路局既有客票系统安全管理平台，通过在车站客票网络不同安全域部署安全访问控制系统、安全隔离系统、管控器、安全管理服务终端等，实现和所属铁路局安全平台的通信，对客票的售票终端、安全设备等信息资产进行安全接入认证、授权管理、安全审计，提供基础安全保障，杜绝未经授权的访问和蓄意攻击。

铁路旅客服务系统主要完成旅客服务相关业务，解决各子系统之间信息交互过程中的安全问题，通过部署安全产品及设备，建立一套合理的、全方位、多层次安全防护体系，有效抵御各种病毒和混合威胁的攻击，保证旅客服务系统的安全运营。

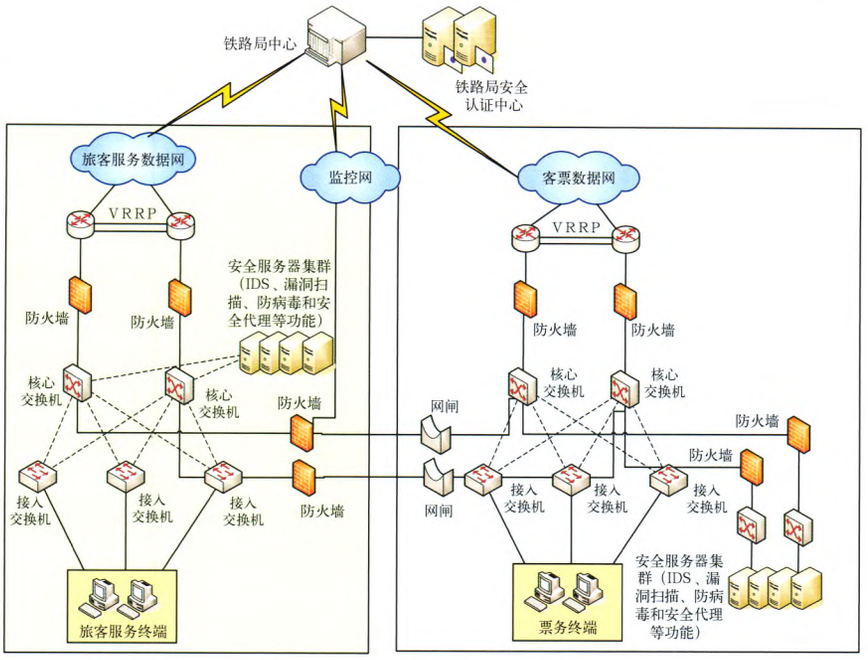

图1 客运服务系统安全保障平台部署示意图

通过部署物理隔离网闸，实现票务网络和旅客服务网络安全域的划分，并进行数据流向访问控制，在实现物理隔离的基础上提供与旅客服务系统的数据交换，保证票务系统的安全独立运营。两个网络之间只允许售票信息通过授权进行数据传递，拒绝其它网络信息通过隔离网闸及防火墙到达对方网络。在防火墙上进行细粒度的访问控制，禁止非授权用户访问网络。

票务网络、旅客服务网络与铁路局中心网络互联边界分别部署防火墙，实现对进出数据的访问控制，防止来自上级网络区域的网络攻击和越权访问，同时可以拦截车站内部的一些非法访问及攻击行为。铁路客运服务系统安全保障平台总体网络结构如图 1 所示[8]。

2 测试内容

根据《铁路客运服务系统安全保障平台设计方案》中系统功能设计，对铁路客运服务系统信息安全展开网络安全测试、主机安全测试、应用安全测试和数据安全测试，如图 2 所示。

2.1 应用安全测试

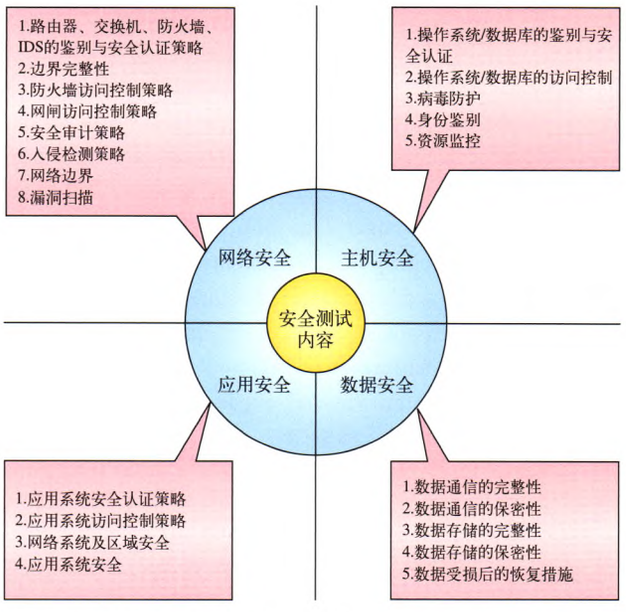

图2 铁路客运服务系统信息安全测试体系结构示意图

对客运服务应用系统的安全测试主要从鉴别与安全认证、访问控制、网络系统及区域安全、应用系统安全几个方面进行测试，如表 1 所示。

2.2 网络安全测试

对客运服务网络安全测试主要从鉴别与安全认证、访问控制、安全审计、入侵检测、网络边界、漏洞扫描几个方面进行测试，如表 2 所示。

2.3 主机安全测试

对客运服务主机安全测试主要从鉴别与安全认证、访问控制、病毒防护、身份鉴别、资源监

表1 应用安全测试

测试项	测试内容
鉴别与安全认证	是否有专用的登录控制模块对登录用户身份标识和鉴别
	是否有用户身份的鉴别信息复杂度要求
	是否用户身份标识唯一，保证系统中不存在重复用户
	是否提供登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施
访问控制	是否有专用的访问控制模块对用户的权限进行管理
	是否根据管理员用户的角色分配权限，实现管理用户的权限分离，仅授予管理用户所需的最小权限
	是否实现由授权主体配置访问控制策略，并严格限制默认账户的访问权限
网络系统及区域安全	远程用户以及系统访问客运服务系统是否通过防火墙的VPN加密技术
	远程连入方式采用的加密方式
	是否对连入客运服务系统的用户数量进行了限制
应用系统安全	是否采用PKI技术进行身份认证
	是否提供权限管理模块，实现对资源的访问控制
	访问控制的覆盖是否包括访问资源相关的主体，客体及它们的操作
	是否严格限制默认用户的访问权限
	是否授予不同用户为完成各自承担任务所需的最小权限
	是否在关键业务的通信过程采用了加密和签名处理

表3 主机安全测试

测试项	测试内容
鉴别与安全认证	是否采用登陆的身份鉴别和认证机制
	是否对管理员的登陆地址应进行限制
	是否管理身份标识唯一，保证系统中不存在重复用户
	是否有用户身份的鉴别信息复杂度要求
	是否提供登录失败处理功能，如采取结束会话、限制非法登录次数和自动退出等措施
访问控制	是否启用访问控制功能，依据安全策略控制用户对资源的访问
	是否根据管理用户的角色分配权限，实现管理用户的权限分离，仅授予管理用户所需的最小权限
	是否实现操作系统和数据库系统特权用户的权限分离
病毒防护	是否采取对恶意代码的防范措施
	是否保持恶意代码库的升级和检测系统的更新
身份鉴别	是否通过终端部署USB key及安全代理，实现对用户以及设备提供代理认证服务
	是否通过USB key，对访问用户的权限进行了控制，控制策略有哪些
资源监控	是否对主机产生的日志进行统一收集和审计分析
	是否实现对应用服务器进行统一监视，包括动态监视设备的CPU、硬盘、内存、网络等资源的使用情况
	是否实现对网络设备及安全设备进行统一监视，包括动态监视设备的CPU、硬盘、内存、网络等资源的使用情况

控几个方面进行测试，如表3所示。

2.4 数据安全测试

对客运服务主机安全测试主要从数据通信完整性、数据通信保密性、数据存储完整性、数据存储保密性几个方面进行测试，如表4所示。

表2 网络安全测试

测试项	测试内容
鉴别与安全认证	是否采用登陆的身份鉴别和认证机制。
	是否对管理员的登陆IP地址应进行限制
	是否管理身份标识唯一，保证系统中不存在重复用户
	是否有用户身份的鉴别信息复杂度要求
	是否提供登录失败处理功能，如采取结束会话、限制非法登录次数和自动退出等措施
访问控制	是否能够对非授权设备私自联到网络的行为进行检查，准确定出位置，并对其进行有效阻断
	是否在网络边界部署访问控制设备，并启用访问控制功能
	防火墙是否根据会话状态信息对数据流进行控制
	防火墙是否对进出网络的内容进行过滤，实现协议级的命令控制
	防火墙是否决定允许或拒绝用户对受控系统进行资源访问，控制粒度为单个用户
	网闸是否在内网边界部署，并启用访问控制策略
安全审计	是否对网络系统中的网络设备运行状况、网络流量、用户行为进行记录
	审计记录是否包括事件的日期和时间、用户、事件类型、事件是否成功等信息
	是否能够对记录的数据进行分析，生成审计报表
	应用系统审计，覆盖到每个用户的安全审计，对应用系统的重要安全事件进行审计
入侵检测	网络边界处是否部署入侵检测系统
	是否能够监视攻击行为：端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲溢出攻击、IP碎片攻击和网络蠕虫攻击等
	当检测到攻击行为时，记录攻击源IP、攻击类型、攻击目的、攻击时间，在发生严重入侵事件时应提供告警
网络边界	在系统的核心区域和非核心区域是否部署防火墙
	防火墙访问控制策略是否对用户和端口进行了控制
	网络边界处是否部署网闸
	网站的用户访问控制策略及数据交换的访问控制策略
漏洞扫描	是否有网络安全漏洞扫描设备
	是否定期采取措施对主机和网络设备进行安全漏洞扫描
	是否定期采取措施对应用系统进行安全性评估
	是否对系统内主机和网络设备的安全配置进行安全检查

3 测试方法

3.1 测试手段

（1）访谈。测试人员依据测试案例，通过与系统实施人员进行有目的性、有针对性的询问和交流，以帮助测试人员了解并分析系统的安全防护手段的合理性。

（2）手工检查。测试人员通过直接访问指定网络设备及安全设备，输入有效的查询命令，从而验证访谈结果的真实性，同时分析查询结果，评估系统的安全防护策略是否合理并正确生效。

（3）工具测试。测试人员使用专业的安全测

表4　数据安全测试

测试项	测试内容
数据通信完整性	是否配备检测鉴别信息和重要业务数据在传输过程中完整性受到破坏的功能
	鉴别信息和重要业务数据在传输过程中是否有完整性保证，具体措施有哪些
数据通信保密性	网络设备的管理数据、鉴别信息和重要业务数据采用加密或其他有效措施实现存储保密性
	主要网络设备操作系统，查看其管理数据、鉴别信息和重要业务数据是否采用加密或其他有效措施实现传输和存储保密性
数据存储完整性	系统的鉴别信息和重要业务数据在存储过程中是否有完整性保证，具体措施有哪些
	是否配备检测验证鉴别信息和重要业务数据在存储过程中完整性受到破坏的功能并恢复措施
数据存储保密性	用户鉴别信息和重要业务数据是否采用加密或其他有效措施实现传输加密

评工具，使测评对象产生特定的行为，查看和分析测试结果是否满足设计要求；通过模拟系统的内部及外部攻击，验证系统的安全防护手段是否有效。

3.2 测试点部署

（1）测试点

服务器：应用服务器、数据库服务器等；网络设备：路由器、交换机等网络设备；安全设备：防火墙、网闸等网络设备。

（2）工具接入点

配置核查工具接入点：测试网络可达的防火墙、路由器、交换机、主机等的安全配置项是否符合安全保障平台设计方案要求；漏洞扫描工具接入点：测试网络可达的防火墙、路由器、交换机、主机等设备是否存在安全漏洞；协议分析仪接入点：测试应用系统的数据传输的机密性和完整性；客户端/服务端仿真攻击工具接入点：从应用系统客户端到服务端的整个网络进行仿真攻击测试。测试点布置图如图3所示。

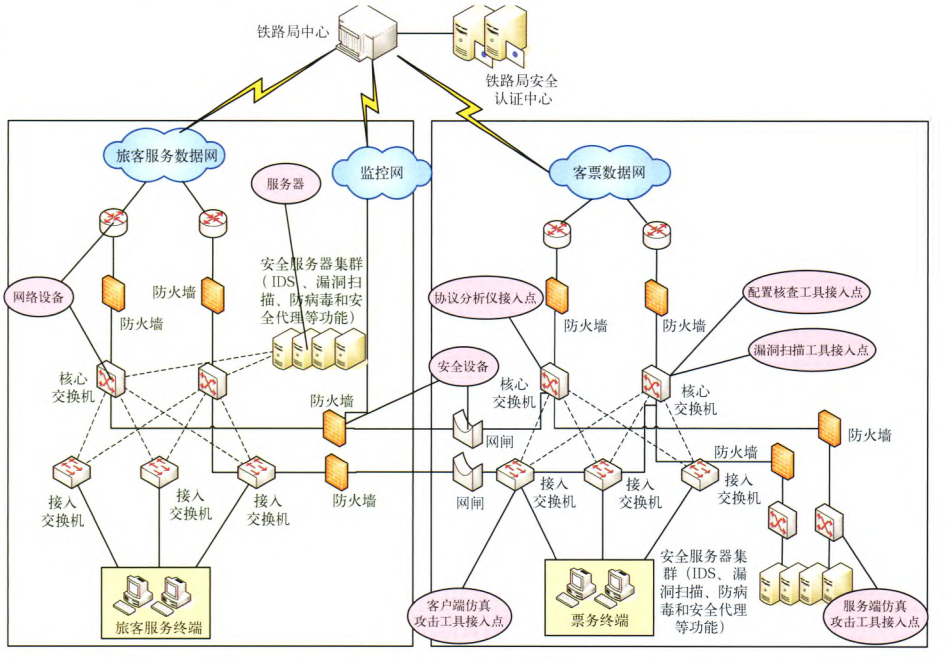

图3　测试点部署示意图

4　结束语

本文针对铁路信息安全保障平台的设计方案和部署现状，提出了一套安全保障平台的测评体系，涉及应用安全、网络安全、主机安全和数据安全4个层面，综合运用访谈、手工检查和工具检查等手段对各层面的安全防护系统和设备安全开展测试，为建立铁路信息安全测评体系提供了依据。

参考文献：

[1] 深圳市永达电子股份有限公司．永达安全管理控制平台（SOC）和铁路客票安全系统建设方案 [J]. 信息网络安全，2010（10）：89 - 90.

[2] 张文塔．铁路客户服务中心方案及关键技术研究 [J]. 铁路计算机应用，2009，20（5）：18 - 21.

[3] 江常青，邹　琪，林家骏．信息系统安全测试框架 [J]. 计算机工程，2008，34（2）：130 -132.

[4] 王　平，靳智超，王　浩．EPA工业控制网络安全测试系统设计与实现 [J]. 计算机测量与控制，2009，17（11）：2153 -2155.

[5] 贺　红，徐宝文，袁胜忠．对应用软件进行安全测试的对手模式及其应用 [J] 计算机科学，2009，33（9）：266 -269.

[6] GB/T 20274-2006 信息系统安全保障评估框架 [S]. 北京：中国标准出版社，2006.

[7] 信息安全风险评估规范 [S]. 北京：国家信息中心，2006.

[8] 中国铁道科学研究院．京沪高速铁路客票系统总体技术方案 [Z]. 北京：中国铁道科学研究院，2011.

责任编辑　陈　蓉