文章编号：1005-8451（2015）02-0005-04

铁路信息系统安全体系研究

张 彦

（中国铁道科学研究院 电子计算技术研究所，北京 100081）

摘 要：分析中国铁路信息系统的安全现状和面临的信息安全威胁，提出铁路信息安全系统的顶层建设构思，构建基于铁路安全管理中心和PKI/CA认证中心支持下的安全应用环境子系统、区域边界防护子系统、通信网络防护子系统三重防护技术体系，以客票系统为例检验该体系的适用性。

关键词: 信息系统；安全体系；适用性

中图分类号：U29-39 **文献标识码：**A

Security system of China Railway Information System

ZHANG Yan

(Institute of Computing Technologies, China Academy of Railway Sciences, Beijing 100081, China)

Abstract: This article analyzed the security of China Railway Information System, proposed a top level concept for the construction of the Railway Information Security System, three-layered protection architecture which was consisted of the subsystem of secure application environment, the subsystem of boundary protection, and the subsystem of communication network protection. The System was based on the support of railway security management center and the PKI/CA(Public Key Infrastructure/Certificate Authority) certificate authority. The TRS(Ticketing and Reservation System) was taken as an example to test the applicability.

Key words: Information System; security system; applicability

中国铁路信息系统按照《铁路信息化总体规划》思路建设。根据该规划，铁路信息系统分为运输组织、客货营销和经营管理3大应用领域[1]，其中，按照四级安全等级保护建设的重大信息系统集中在运输组织和客货营销，其他重要信息系统按三级安全等级保护建设，次要的信息系统按二级安全等级保护建设。如何按照信息安全等级保护思路构建铁路信息系统安全体系，是本文的论述重点。

1 铁路信息系统安全现状分析

1.1 铁路信息系统分类

由于中国铁路设置了铁路总公司、铁路局、站段3层机构，铁路总公司是宏观管理机构，铁路局是业务管理机构，站段是业务执行机构，应用类信息系统需要考虑3层不同机构之间的业务关联关系。

就系统应用宽泛程度而言，铁路信息系统大致分为3类：第1类是全路性的大型应用系统，部署在铁路总公司、铁路局、站段3级管理与业务部门中，铁路行业使用的大多数信息系统属于这一类应用，如铁路客票系统、列车调度与指挥系统等；第2类是局部的中型应用系统，如铁路运输清算系统，按业务要求部署在铁道总公司和铁路局两级管理机构中；第3类是独立的应用系统，如车号识别系统等只在编组站、分界站等处应用。

1.2 安全措施

中国铁路信息系统目前采用的信息安全措施大致有3种：（1）采用独立的专用网络，如客票网、调度网等，不同的网络服务于不同的业务，网络间提供信息交互服务；（2）部分系统建立了对外的统一信息安全支撑平台，用于防患来自外部网络的攻击；（3）部分系统建立了内部的安全保障平台，在有信息交互的网络边界部署外部访问控制器、内部访问控制器、隔离网闸、防火墙、入侵检测等安全设备。

1.3 安全现状

随着社会的发展，铁路的业务已突破封闭式专网运营模式，向互联网方向渗透。如近年来客运的互联网售票服务，货运的大客户服务等，无不需要通过互联网这一便捷的网络通道，使人们足不出户

收稿日期：2014-10-08
作者简介：张 彦，研究员。

就能购买火车票、托运货物等，在给千家万户带来方便的同时，也给铁路信息系统的安全带来严重挑战，铁路靠传统的专网抵挡外部入侵的措施已不能满足信息系统安全形势的发展需要，须要从顶层考虑，建立一套自顶向下的、完整的安全体系和策略，为各级各类应用系统提供安全保障。

2　信息系统安全体系总体设计

2.1　信息安全体系的顶层构思

从上述分析可知，铁路信息系统量多且规模大，多网并建，各系统之间纵横交错，因此，铁路信息系统的安全体系建设不因只考虑单一系统、单一网络的安全，也不因只涉及单一管理层面的安全，而应自顶向下全盘统筹，贯穿铁路信息系统的各个层面。具体的说就是：按照 GB/T22239-2008《信息安全技术－信息系统安全等级保护基本要求》中提出的物理安全、主机安全、网络安全、应用安全及数据安全 5 个方面的技术要求，以“信息共享、设施共用、纵深防护、主动防御、内外兼防”为原则，构建铁路总公司、铁路局、站段各级信息系统的“二个中心、三重防护”安全体系架构，合理划分安全域，强化网络边界和应用环境安全。

2.2　安全体系总体设计思路

“两个中心”是指覆盖整个铁路信息系统的安全管理中心和为铁路信息系统进行统一身份认证的 PKI/CA 认证中心，“三重防护”是指通信网络防护、区域边界防护和安全应用环境保护 [2]。

“两个中心支撑下的三重防护体系”是从系统的整体安全角度考虑，兼顾系统各安全区域间、各安全层面间的关联性，形成以安全管理中心进行统一管理、统一监控、统一审计、综合分析的集中管理平台，以 PKI/CA 认证中心为铁路行业统一身份认证平台，以通信网络防护、区域边界防护和安全应用环境保护三重协同防护的纵深防御体系。如图 1 所示。

2.2.1　安全管理中心

安全管理中心是技术架构的核心，实现对通信网络防护子系统、区域边界防护子系统和安全应用环境子系统的统一管控。该中心是对三重防护体系的有效支撑，分别在铁路总公司和铁路局部署，各层次之间有数据交互。安全管理中心由系统管理子系统、安全管理子系统和审计管理子系统组成，分别对应“三权分立”模式的系统管理员、安全管理员和审计管理员。

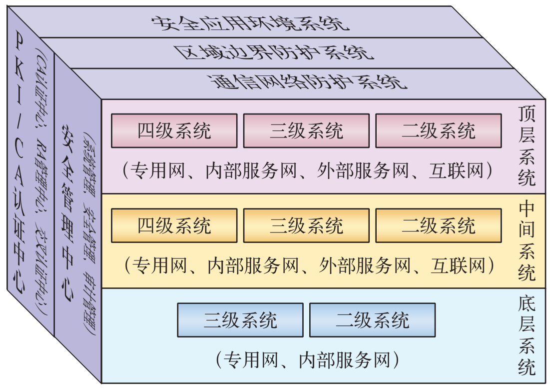

图1　安全技术体系架构图

2.2.2　铁路PKI/CA认证中心

铁路 PKI/CA 认证中心为铁路行业统一的身份认证系统，可以奠定铁路行业网络信任体系基础，有效解决应用系统的身份认证问题，使之具备高强度的身份认证和责任认定机制，为应用系统的权限管理和单点登录提供支撑平台和服务。该系统分别部署于铁路总公司和铁路局，铁路总公司 PKI/CA 认证中心包括 CA 认证中心、RA 管理中心和交叉认证中心，铁路局根据实际情况可以考虑建设 CA 认证中心和 RA 管理中心 [3]。

2.2.3　通信网络防护系统

网络通信包括铁路客票网、调度网、生产网、内部服务网、外部服务网等不同专网之间的通信，以及专网与互联网之间的通信。不同的专网之间部署通信网络防护系统并实现安全通道功能，专网与互联网之间以及四级系统与其他系统之间部署强隔离系统和外部访问控制系统，其他网络之间部署内部网络控制系统和防火墙等安全设备，防止内部发生安全泄漏事件。

2.2.4　区域边界防护系统

区域边界防护分为纵向区域边界防护和横向区域边界防护。纵向边界是铁路总公司中心对铁路局中心、铁路局中心对车站及相邻铁路局之间的边界，在构建纵向边界防护策略时，主要考虑边界完整性保护、外部非法接入、内部用户非法外联、强制访

问控制机制等。横向边界是指二、三、四级信息系统间的安全域边界，按照“二级系统统一成域，三级、四级系统独立分域”的划分原则构建。

2.2.5 安全应用环境子系统

安全应用环境系统针对二、三、四级各类应用系统部署服务器、终端等不同环境下的安全防护策略。服务器可采取的安全策略包括身份鉴别、标记管理、强制访问控制、安全审计和系统可信安全机制等。终端的安全采用基于安全操作系统的安全防护机制，可采用访问控制软件与终端软件完整性检查、操作系统安全加固等措施。

3 安全体系在铁路客票系统中的应用

3.1 需求分析

分析铁路客票系统的整体架构和网络构成，可以从以下几方面给出客票系统的安全需求：

（1）设备安全需要：核心数据库服务器、应用服务器、接口服务器、交易前置服务器的安全，车站售票窗口、代理售票窗口、TVM、管理机等各类接入终端的安全；（2）网络安全需求：客票网、内部服务网、外部服务网、互联网的接入安全；（3）纵向边界安全需求：铁路总公司客票中心系统、地区客票中心系统、车站系统边界的安全；（4）横向边界安全需求：客票核心系统、客户服务中心网站、电子支付平台、运输清算等系统、旅客服务系统进行数据交换的安全；（5）数据安全需求：票库、存根、常用客户等重要数据的存储和传输安全；（6）人员安全需求：内部操作人员进入系统的安全认证、外部用户通过互联网进入12306网站的安全认证、系统管理员进入后台系统的安全认证等。

3.2 安全风险分析

铁路客票系统面临的安全风险主要有：

（1）来自外部的安全威胁：通过互联网等外部网络非法接入，对客票系统进行恶意破坏、病毒扩散、DDos攻击、资源滥用等。（2）来自内部的安全风险：内部人员越权、跨区域登录服务器或核心数据库，篡改存根、财务统计数据、票库等重要数据源，非法锁定票源，插入有病毒的移动介质传播病毒，对安全管理员、系统管理员、数据库管理员缺乏有效的监督和审核措施等。（3）互联系统间的接口安全：客票系统、12306网站、电子支付、旅客服务、运输清算等系统之间通过数据交换接口进行非法操作，造成网络拥堵，发布带病毒的接口数据造成病毒传播等。（4）断电、断网、空调失效、机房漏水等环境因素造成系统运行中断等。

3.3 安全方案

根据对铁路客票系统安全需求及安全风险的分析，本方案拟以铁路客票系统为中心，将与其有关联

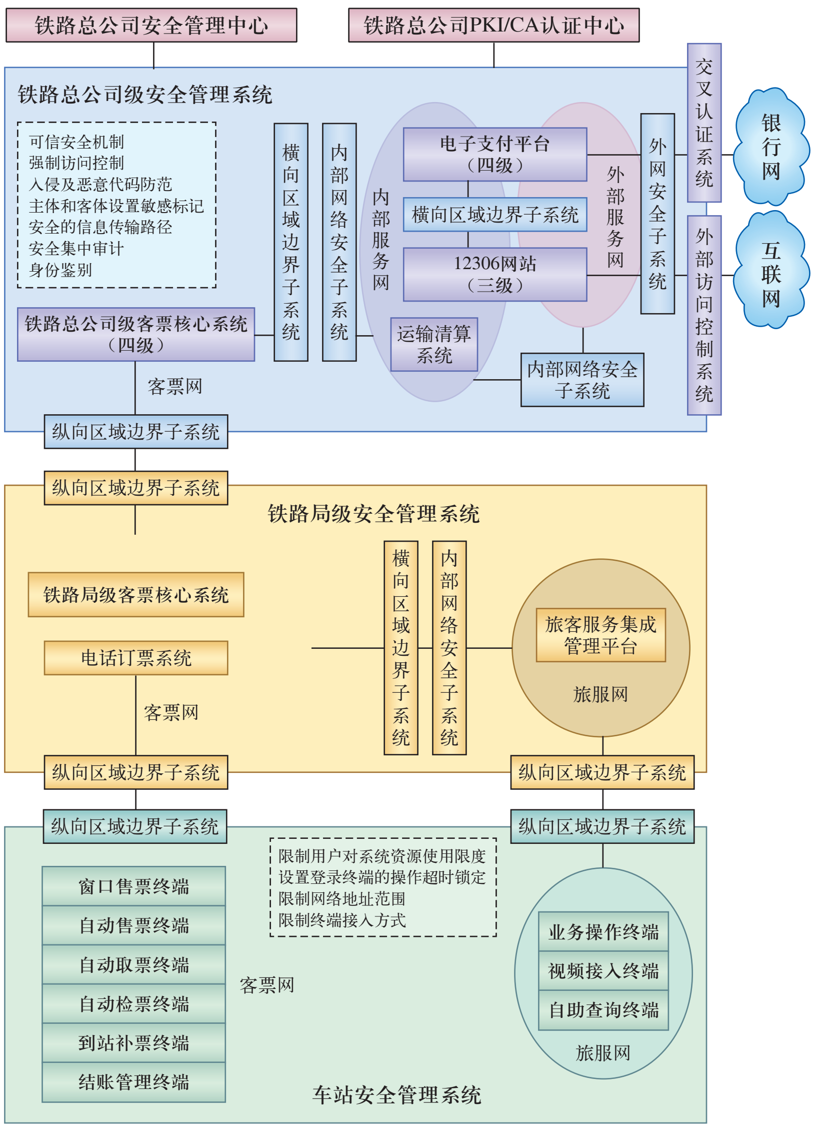

图2 铁路客票系统安全结构图

（下转P16）