文章编号：1005-8451（2015）02-0033-05

互联网环境下铁路信息安全等级保护设计方案研究

姚洪磊，史　宏
（中国铁道科学研究院　电子计算技术研究所，北京　100081）

摘　要：信息安全是铁路信息系统建设的一个重要问题，目前我国铁路缺少统一、标准化的信息安全等级保护解决方案，伴随互联网发展，铁路出现一批面向互联网提供服务的信息系统，该类信息系统的上线应用，生产系统不可避免与外网互联，信息安全受到威胁日益加大。本文提出了互联网接入管理中心支持下的安全计算环境子系统、安全区域边界子系统、安全通信网络子系统保护三重防护技术体系结构，形成纵深防御体系。基于该体系并结合互联网信息系统的特点，对安全方案设计开展了研究，可为相关部门采取相应的防护技术和管理措施提供理论依据和参考。

关键词：互联网信息系统；信息安全等级保护；设计方案
中图分类号：U29-39　　**文献标识码：**A

Proposal of railway information security level protection on Internet

YAO Honglei, SHI Hong
(Institute of Computing Technologies, China Academy of Railway Sciences, Beijing 100081, China)

Abstract: Information security was an important issue for the construction of Railway Information System. There was a lack of standardized solutions for information security level protection in railway industry. With the development of Internet, a number of service-oriented information systems on the Internet were developed, manufacturing system was connected with internet inescapability and the security threat was increased. Treble Defense-in-depth System supported by security management center was proposed in the paper which was consisted of safe compute environment, border protection and communication network protection. Combined with the characteristics of Information Systems on Internet, security program was designed in this paper. The proposed program could provide references for relevant departments.

Key words: Information System on Internet; information security level protection; design proposal

经过几十年的发展，铁路信息系统现已成为涵盖各专业不同业务的庞大信息系统体系，该体系中除运行于铁路内部网络的信息系统外，部分信息系统由于业务需要，需面向互联网提供服务，如铁路互联网售票系统[1]、铁路电子商务系统[2]、大客户服务系统[3]等，由于实现与外网的互联，信息系统存在各种类型的安全隐患和潜在的危险，黑客及怀有恶意的人员将可能利用这些安全隐患对内部网络进行攻击，造成严重后果。

自我国开展信息安全等级保护工作以来，相关学者已经对各类信息系统信息安全等级保护体系的设计开展了大量的研究[4~7]。针对铁路行业特点，本文提出互联网接入管理中心支持下的安全计算环境、安全区域边界和安全通信网络子系统为主要防护手段的三重防护技术体系结构，形成纵深防御体系，同时基于该体系并结合面向互联网提供服务信息系统的特点，对安全设计方案开展了研究。

收稿日期：2014-10-08
作者简介：姚洪磊，助理研究员；史　宏，研究员。

1　安全风险分析

1.1　非法访问

互联网用户或其他网络区域用户试图访问铁路总公司或各铁路局客服中心网站所开放服务之外的信息和服务，导致网站面临非法内联和外联的安全威胁，特别面临着恶意攻击导致系统瘫痪的安全风险。

1.2　外部非法入侵和攻击

铁路部分应用系统外部终端可以通过 ADSL 拨

号、无线网实现访问。但随着接入点的不断增多，系统极易遭受来自外部和内部的非法入侵和攻击。

1.3 计算机病毒、蠕虫及恶意代码的攻击

铁路通信网未与互联网连接前，所面临的恶意代码攻击主要来自光盘、软盘、移动存储终端等外部介质的恶意代码，与互联网连接后，通过 E-mail、文件下载、网页浏览等方式，计算机病毒可以直接经外网、无线网入侵铁路内部信息系统。

1.4 高峰期巨大访问量的安全风险

铁路部分信息系统如铁路客户服务中心等面向大量用户的服务网站，均面临高峰期巨大访问量，造成系统满负荷而拒绝响应和网络瘫痪，软件可靠性问题导致的系统瘫痪等安全问题。

2 安全需求分析

（1）铁路客户服务中心、铁路电子支付平台等与互联网直接连接的服务网站，需要强化身份鉴别、自主和强制访问控制，防止非法内联和非法外联，特别需要防范恶意攻击导致系统瘫痪的安全风险。

（2）当铁路内部网与外部网进行信息交换时，需要在系统边界处实现系统间有效地隔离并严格控制信息的出入。

（3）针对需要通过互联网实现交易的交易平台，需要强化内部安全和交易的真实性，需要防范内部使用人员有意或无意非法授权访问和越权操作，防止用户对交易行为的否认，造成交易的真实性无法确认。

（4）针对基于互联网面向社会的客户服务类网站，需要强化主机系统的可用性，在采用总公司、地区中心设置数据库服务器，车站不设置数据库服务器后，特别需要防范高峰期增加的巨大访问量引起的系统超负荷运行，该问题导致系统拒绝响应和网络瘫痪。

3 设计方案

3.1 总体技术框架

以一个网络结构分为铁路总公司、地区和车站三层结构并面向互联网提供服务的信息系统为例，其逻辑结构可以分为铁路总公司级安全域、地区级安全域和车站级安全域，3 个级别的安全域安全目标一致，其安全保护的重点和强度有所不同。地区中心为例的安全系统技术框架如图 1 所示。

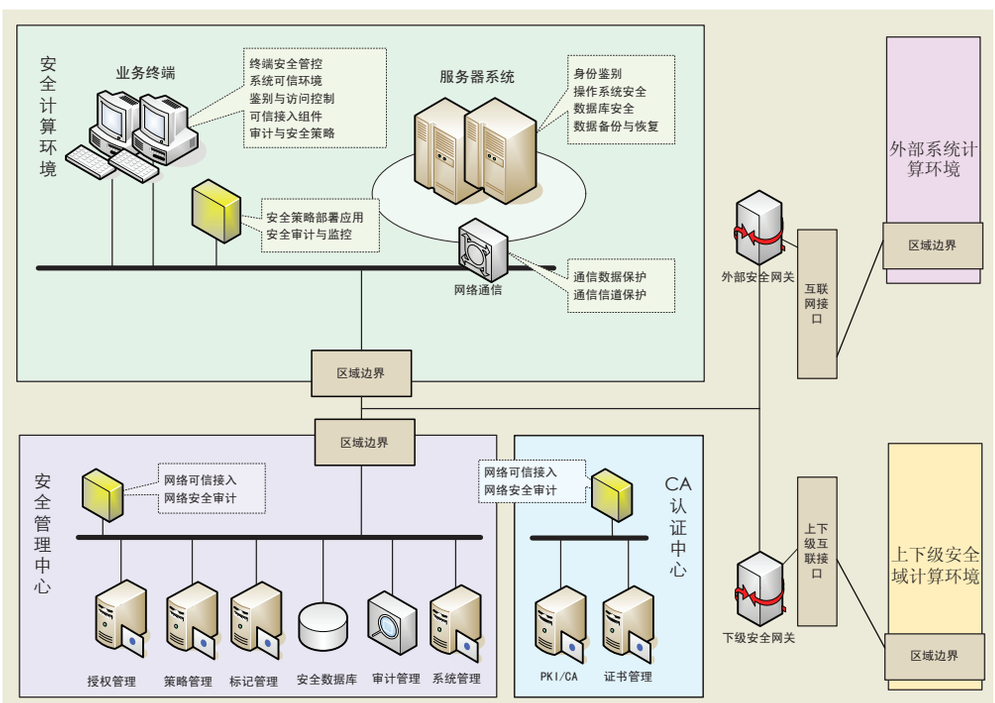

图1　安全系统总体框架

3.2 安全管理中心

安全管理平台实现对铁路信息安全系统进行统一、集中的监管，保障系统运行安全，监控和保护信息处理过程的安全。安全管理平台对分布在网络环境的各种安全机制和服务进行集中管理与控制，是安全策略部署和控制中心，其部署的安全策略是各安全部件和各安全保障层面的纽带，安全管理中心组成结构图如图 2 所示。

3.3 安全计算环境

3.3.1 用户身份鉴别增强

针对一个面向互联网提供服务的 Web 系统，所有互联网客户均可以访问，客户服务中心外网的用

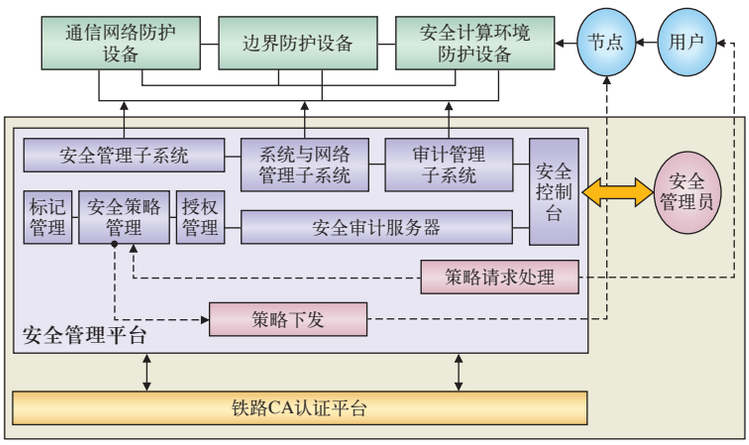

图2　安全管理中心组成结构图

户主要包括互联网客户及相关管理员。对这两种用户在应采用不同的认证机制，身份鉴别均可通过既有铁路 PKI/CA 认证中心实现，系统管理员认证需提供专有认证插件。

3.3.2　访问控制增强

基于互联网的服务客户服务网站（以下简称服务网站）应与安全管理中心紧密配合，实现统一的安全访问控制策略。安全管理中心为服务网站提供统一的认证、授权、安全目录、用户管理等服务，并与安全代理系统紧密整合，为网站的内、外网信息交换提供代理证书认证、权限检查、代理安全访问等服务。

3.3.3　应用层安全审计增强

基于互联网信息系统应用层的审计主要是服务网站外网及内网应用，对应用层的审计主要通过审计接口实现，应用层的审计机制如图 3 所示。

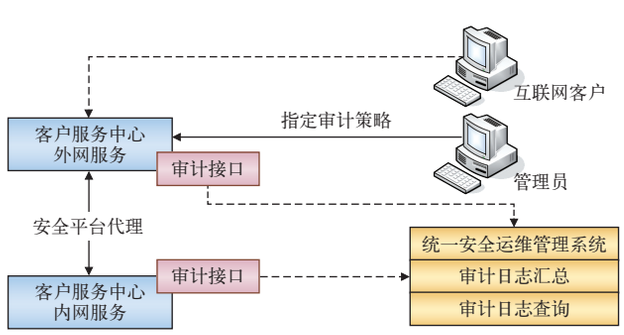

图3　应用层安全审计机制图

3.3.4　Web应用安全扫描

由于面向互联网提供服务的信息系统是一个 Web 应用，将通过 Web 应用安全扫描技术实现 Web 应用的可信执行。Web 应用安全扫描系统通过黑盒和白盒扫描相结合的方法。

3.3.5　主机综合入侵防护

在核心服务器上部署主机综合防护系统，提供数据库服务的可信执行保护。采用多种检测防护手段，如入侵防范与阻断、基于控制台的网络攻击防范等。

3.3.6　网页防篡改及防盗链

客户服务中心外网 Web 服务器需要有效的防篡改、防盗链机制，通过网页防篡改、防盗链系统实现。

3.3.7　CDN方式对高峰期访问分流

针对面向互联网提供服务的信息系统，在高峰期可采用内容分发网络（CDN，Content Distribution Network）方式进行访问分流。CDN 分流策略可以避开互联网上有可能影响数据传输速度和稳定性的瓶颈和环节，使内容传输的更快、更稳定。

3.4　安全区域边界

3.4.1　数据隔离和控制操作

（1）确保物理和逻辑边界接口得到充分保护，禁止非法外联和非法接入，确保合法信息能进出边界和接口。（2）确保在边界和通过远程 VPN 访问进行数据交换的数据得到保护，确保受保护边界内的系统和网络维持可用性。(3)保护边界内的系统和数据，防止外部攻击或破坏。（4）为通过边界发送和接收信息提供强认证访问控制，基于边界控制策略，有选择地允许重要信息跨边界流动。

3.4.2　安全加固

外网接入边界的安全防护由外网安全互联平台实现，由安全接入设备、安全隔离与信息交换设备、互联网接入安全管理中心组成，实现保密性检查和完整性检查。检查所有由内网流向外网的信息，禁止破坏系统完整性的信息进入，该平台可逻辑扩展，远程安全终端可通过 VPN 实现可信接入，安全平台体系结构如图 4 所示。

3.4.2.1　边界访问控制

主要由安全接入设备完成，采用基于 PKI 身份证书验证的接入控制，实现基于端口的网络可信接入控制。

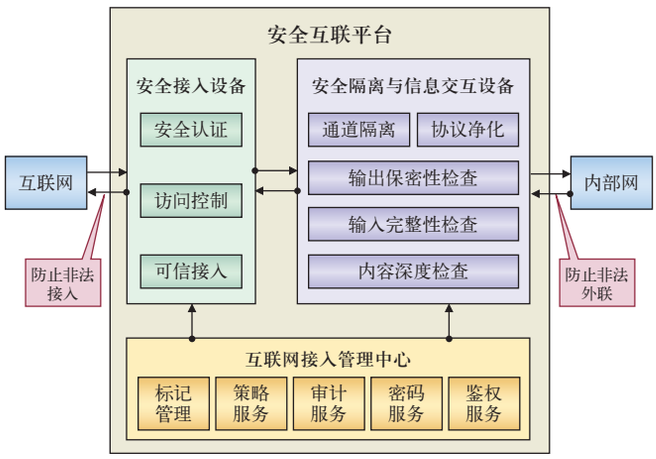

图4 安全互联平台体系结构图

（1）身份和标识鉴别：a. 对接入用户实现认证；b. 对管理员实现认证，c. 对接入服务器和终端进行标识和安全认证 。（2）对访问内网的用户设备进行鉴权。

3.4.2.2 边界内容深度过滤

主要由安全隔离和信息交换设备完成，采用强制访问控制和深度过滤策略，包含采用 ISO 七层强制访问控制的安全隔离设备，对内网中标记允许传输到外网的数据进行强制访问控制策略过滤，对外网传输到内网的数据进行内容过滤和完整性检查，包含：

（1）通道隔离：外网与内网两个网络之间的链路层连接，通信层连接、网络层连接和应用层连接的安全隔离。（2）协议净化：以 TCP/IP 剥离技术来完成数据的交换，并根据有外网信息系统业务的特定协议实现强制访问控制。（3）数据内容：数据采用加密，签字等安全机制进行安全通信。

3.4.2.3 外部边界强制访问控制

（1）外部交易服务器与外网安全互联平台进行安全认证，通过后，才允许下一步操作；（2）所有访问的交易数据通过节点认证设备的签字，并加上安全标签；（3）安全互联平台收到交易数据，进行验签，不通过则阻断；（4）安全互联平台进行安全检查，解析交易数据的标记信息，安全隔离与信息交换设备，验证通过，则允许通过，否则，阻断该交易。

3.4.2.4 边界安全审计和完整性保护

由安全接入设备，安全隔离与信息交换设备、安全审计部件等在安全管理中心管控下共同完成。

（1）对内网传出的信息进行保密性检查、并对访问内网的用户进行完整性检查；（2）对互联网传入的信息进行完整性检查，建立外部接入系统的白名单机制，可以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、跟踪攻击源等）；（3）安全审计组件，通过采集网络设施的性能、故障、运行状态信息、业务应用的运行状态信息（如日志、运行事件等）和安全状态信息，并执行关联分析，事件分析和综合分析，发现异常的行为，包含未授权的身份、登录密码的多次错误和隐蔽信道等。

3.5 安全通信网络

通信网络安全主要包括铁路总公司中心到铁路局中心、铁路局中心到车站不同区域之间的通信路径的安全可靠。不同的安全域之间部署安全通信网络系统并实现安全通道的相应功能；区域系统内部不同系统之间部署强隔离系统，保障数据的完整性、机密性。针对与互联网连接的信息系统，通信网络安全包含互联网安全互联和内网安全互联，其中与互联网的安全互联是本节着重讨论的内容。

3.5.1 互联网安全互联

互联网安全互联是以各系统自身安全防护为基础，辅以相关网络安全互联机制，包含 VPN、安全通信等，为不同安全等级系统之间的数据传输与交换提供安全保障，实现数据传输的机密性、完整性、抗抵赖性和可追溯性。互联网安全互联逻辑结构图如图 5 所示。

3.5.1.1 安全接入

通过接入设备的安全互联部件实现，基于 IP 等级标记信息实施网络访问控制，IP 等级标记包含指明等级级别的 ID、发起连接主体标记等相关信息。

互联网接入：解析外部连接 IP 等级标记信息并分析主体信息，与外部边界的安全管理中心联动确定能否接入。如可接入，需要分配接入主体访问内网的权限和访问控制规则。

安全互联 / 外部安全管理：包含接入、接出通信网络访问控制策略，基于等级标记的安全互联协议配置，安全管理员的认证等。

3.5.1.2 安全接出

通过安全隔离设备，解析内部连接 IP 等级标记

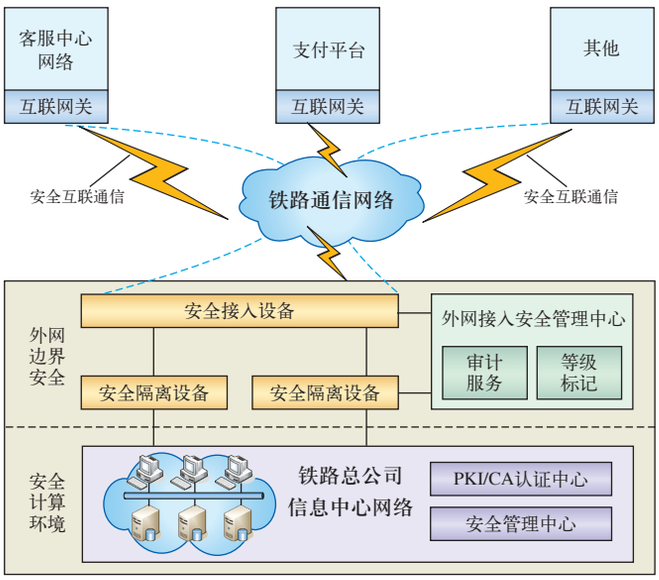

图5　互联网安全互联逻辑结构

信息并分析主体信息，与安全管理中心联动确定能否接出。

3.5.1.3　安全互联通信与安全互联协议

符合安全等级要求，避免不同等级信息系统间信息交互时高敏感度信息流向低敏感度实体、低完整性保护系统中的主体操作高完整性保护系统中的客体，实现安全互联。

3.5.2　外网终端接入

3.5.2.1　远程访问虚拟网

Access VPN 适用于铁路内部出差人员远程移动办公的情况。铁路管理层利用 Access VPN 可以随时随地接入内部资源，访问业务系统，了解生产运营信息，进行审批和指挥调度；技术人员可以远程移动办理业务和处理工作流，进行远程维护；列车中的乘务人员可以与地面进行无线信息交互，应对突发事件，查询客运信息，维护乘车秩序。

3.5.2.2　企业内部虚拟网

Intranet VPN 利用 Internet 线路保证网络的互联性，而利用隧道、加密等 VPN 特性保证信息在 Intranet VPN 上安全传输。铁路行业机构庞大，办公环境复杂，有些办公地点不适合铺设永久性的电缆，在这种情况，Intranet VPN 可以作为一种建设成本低并且应用安全的组网方案。

3.5.2.3　企业扩展虚拟网

Extranet VPN 通过一个使用专用连接的共享基础设施，将客户、合作伙伴连接到铁路内部网。Extranet VPN 结构的主要好处是，能容易地对外部网进行部署和管理，外部网的连接可以使用与部署内部网和远端访问 VPN 相同的架构和协议进行部署。Extranet VPN 可用于在铁路与大客户之间通过特定的加密隧道建立互联网络，由于无需特别的专线租用，成本可大幅降低。

4　结束语

本文结合信息安全技术和铁路信息系统网络的特点，在对互联网安全风险进行分析的基础上，提出了互联网接入管理中心支持下的三重防护设计方案。其中，安全管理中心统一对各安全防护子系统进行管理；安全计算环境子系统为互联网信息系统提供安全运行的计算环境；安全区域边界子系统针对外网对信息系统可能造成的威胁、内部网络间的数据交换产生的安全威胁进行防护；安全通信网络子系统对数据传输的机密性和完整性进行保护。对铁路行业面向互联网提供服务的信息系统的建设和改造提供一定参考。

参考文献：

[1] 王明哲，张振利，徐　彦，等．铁路互联网售票系统的研究与实现 [J]. 电力信息化，2012，21（4）：23-25.

[2] 郭大亮，范清芬．电子商务的信息安全技术与管理研究 [J]. 信息安全与通信保密，2012（4）：70-75.

[3] 郭玉华，陈治亚．基于客户生命周期的铁路大客户细分与发展模型 [J]. 铁道科学与工程学报，2011，8（2）：86-91.

[4] 沈昌祥．高安全级信息系统等级保护建设整改技术框架 [J]. 中国人民公安大学学报：自然科学版，2009（1）：1-4.

[5] 姚洪磊，张　彦，祝咏升，等．铁路信息安全体系的提出及在互联网售票系统中的应用 [J]. 北京交通大学学报，2012，36（5）：105-111.

[6] 孙祥鹏，廖华春．水利网络与信息安全防护体系研究 [J]. 甘肃水利水电技术，2011，47（1）：35-37.

[7] 王令朝．创建铁路信息安全管理及其标准体系的探讨 [J]. 铁道技术监督，2010，38（7）：1-5.

责任编辑　徐侃春