铁路计算机应用
RAILWAY COMPUTER APPLICATION

铁路设计企业管理信息化系统网络安全关键技术研究

刘　峰，韩　寓

Key technologies for network security of railway design enterprise management information system

LIU Feng and HAN Yu

引用本文:
刘峰, 韩寓. 铁路设计企业管理信息化系统网络安全关键技术研究[J]. 铁路计算机应用, 2023, 32(11): 68-72.
LIU Feng, HAN Yu. Key technologies for network security of railway design enterprise management information system[J]. Railway Computer Application, 2023, 32(11): 68-72.

在线阅读 View online: http://tljsjyy.xml-journal.net/2023/I11/68

文章编号：1005-8451（2023）11-0068-05

铁路设计企业管理信息化系统网络安全关键技术研究

刘　峰，韩　寓
（中国铁路设计集团有限公司，天津　300308）

摘　要：针对企业管理信息化系统建设项目，通过风险评估方法全面地剖析存在的内、外部安全风险，以网络安全等级保护（简称：等级保护）2.0 中“一个中心、三重防护”框架为指导，设计网络安全防御技术体系。在 Web 应用安全、数据安全、威胁自动化响应等方面开展关键技术研究，落实 Web 应用安全防护技术、集中数据监测与审计技术、综合威胁分析及响应技术，满足等级保护和攻防实战要求。该安全防御技术体系已在某铁路设计企业得到应用，有效提升了企业管理信息化系统纵深防御能力。

关键词：网络安全等级保护；Web 应用安全；数据安全；威胁分析；安全编排自动化响应（SOAR）

中图分类号：U29 : F530.6 : TP393　**文献标识码：**A　**DOI：**10.3969/j.issn.1005-8451.2023.11.14

Key technologies for network security of railway design enterprise management information system

LIU Feng, HAN Yu
(China Railway Design Group Co. Ltd., Tianjin　300308, China)

Abstract: This paper focused on the construction project of enterprise management information system, comprehensively analyzed the existing internal and external security risks through risk assessment methods, and designed a network security defense technology system guided by the "one center, three layers of protection" framework in classified protection 2.0 of cybersecurity. The paper conducted key technology research in areas such as Web application security, data security, and threat automation response, implemented Web application security protection technology, centralized data monitoring and auditing technology, comprehensive threat analysis and response technology, and met the requirements of level protection and offensive and defensive combat. This network security defense technology system has been applied in a railway design enterprise, effectively enhances the depth defense and active defense capabilities of the enterprise management information system.

Keywords: classified protection of cybersecurity; Web application security; data security; threat analysis; Security Orchestration Automation and Response (SOAR)

近年来，铁路设计企业转型升级稳步推进，从发展战略上对企业管理信息化、移动办公提出了更高的要求。因此，企业大力开展管理信息化系统升级建设工作，打破信息孤岛，将分散的管理信息化系统进行集成重构，打造信息集成平台，实现企业流程和业务数据有机结合。

管理信息化系统集成重构，通过服务总线、数据集成等技术，打通了各管理业务数据壁垒，畅通了服务流程，提升了企业的管理质量和效率。然而，异构应用集成和数据整合使得业务系统内部结构变得复杂，各业务系统间建立了密集的调用关系；办公业务信息化建设也增加了企业互联网的暴露面，导致系统内、外部安全风险增加。传统网络的边界安全存在局限性，迫切需要建立更加精准、完善的安全防护体系。

本文围绕铁路设计企业管理信息化系统建设项目，提出了网络安全防御技术体系，并在 Web 安全、数据安全、威胁分析及自动化响应方面落地应用，切实提高了信息系统整体安全性。

收稿日期：2023-07-31
作者简介：刘　峰，工程师；韩　寓，高级工程师。

1　安全防御技术体系

管理信息化系统建设过程中须严格遵照网络安全等级保护（简称：等级保护）相关要求[1]，并落实网路安全攻防实战演练的防御经验，降低管理信息化系统自身安全隐患，有效抵御外部威胁。管理信息化系统的安全风险主要分为系统安全隐患及外部安全威胁[2-4]，系统安全隐患主要源于该类系统在设计建设过程中存在的问题，包括信息资产漏洞（供应链安全隐患）、系统互联网暴露面大、系统运行时数据监测不到位，审计不全面等；外部安全威胁来自外部的各种恶意攻击，主要包括 Web 后台探测扫描、Web 权限控制及系统间横向渗透等。

针对上述安全风险，根据等级保护 2.0 中“一个中心，三重防护”的总体思路，建立企业管理信息化系统网路安全防御技术体系[5]，如图 1 所示。以安全管理中心为核心、以计算环境安全为基础、以区域边界安全和通信网络安全为支撑，实现事前精细化防护、事中快速识别响应和事后可审计溯源的安全闭环管理。

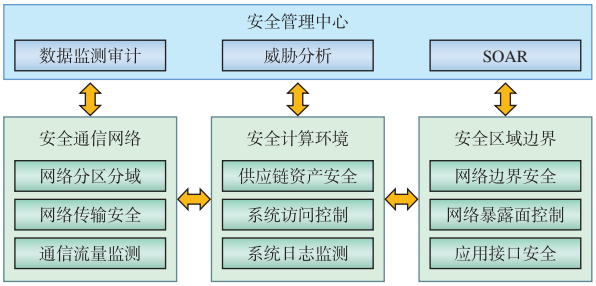

图1　管理信息化系统网络安全防御技术体系

（1）安全管理中心：是企业信息安全事件管理的核心平台，该平台集中汇聚企业网络各种信息资产、各类安全系统的日志数据，以及原始网络流量数据，实现全面数据监测及审计；基于大数据分析技术进行威胁建模分析，对触发安全规则的攻击威胁按预先编排的脚本，调动对应网络区域的安全设备执行主动防御，实现信息安全事件从事前、事中到事后的自动化闭环管理[6-8]。

（2）安全通信网络：指承载管理信息化系统的网络通信环境安全，通过网络区域隔离、网络传输加密及网络通信流量审计等方面实现通信网络安全。

（3）安全计算环境：指管理信息化系统的软、硬件资产运行安全，通过解决供应链资产漏洞、消除 Web 安全隐患、系统运行日志审计，实现计算环境安全。

（4）安全区域边界：指管理信息化系统服务端与客户端、管理信息化系统与第三方系统、管理信息化系统内部组件之间的信息安全边界，通过网络边界安全防护技术、Web 应用暴露面控制及应用程序接口（API，Application Programming Interface）安全控制，实现区域边界安全。

2　网络安全关键技术

本文通过 Web 应用安全防护、集中数据监测与审计、综合威胁分析及响应等关键技术，实现管理信息化系统网络安全防御技术体系的落地。

2.1　Web 应用安全防护技术

管理信息化系统应用安全网关集中对外发布服务。应用安全网关主要具备 7 层负载均衡和 Web 应用防护体系功能，基于应用安全网关的 SSL（Secure Sockets Layer）证书卸载技术和超文本传输协议（HTTP，Hyper Text Transfer Protocol）请求头部安全校验技术，加强应用暴露面管控，建成 Web 应用级安全区域边界。

2.1.1　SSL 证书集中卸载

管理信息化系统通过 HTTPS 协议对外提供服务，为实现 HTTPS 流量集中管控，使用应用安全网关 SSL 证书卸载技术，统一代理各应用、与用户建立 HTTPS 连接。用户与应用安全网关建立 HTTPS 连接、应用安全网关与管理信息化系统各应用建立 HTTP 连接，如图 2 所示。

图2　应用安全网关 SSL 证书集中卸载

SSL 证书集中卸载，为应用安全网关实施 HTTP 请求头部安全校验提供基础，同时也为流量安

全分析创造条件。通过镜像采集应用集中发布平台解密后的 HTTP 流量，可开展威胁分析，避免镜像 HTTPS 加密流量无法分析问题。

2.1.2 HTTP 请求头部安全校验

基于前期信息资产调研结果，对管理信息化系统实施 HTTP 请求头安全校验，能够有效地缩减应用暴露面。HTTP 请求头部校验技术主要包括统一资源标识符（URI，Uniform Resource Identifier）校验、用户代理（UA，User-Agent）校验和跨域请求源校验 3 种安全机制，具体应用如下。

（1）统一资源定位符（URL，Uniform Resource Locator）校验：通过应用安全网关严格限制对互联网暴露 URI，仅允许白名单内的 URI 请求调度到指定应用服务器上。如图 3 所示，基于 URI 校验技术能够屏蔽掉网站后台、中间件后台等维护入口，同时实现同一个传输控制协议（TCP，Transmission Control Protocol）端口上发布多个应用系统，避免不同厂商子系统占用不同 TCP 端口，增加暴露面。

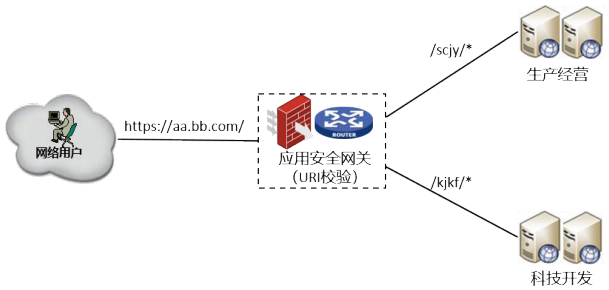

图3 应用安全网关 SSL 证书集中卸载

（2）UA 字段校验：UA 字段携带了客户端工具的标识信息（如浏览器类型和版本、浏览器渲染引擎、浏览器语言等），服务端根据 UA 字段采取相应响应方式。应用安全网关对请求报文头 UA 做白名单过滤，仅允许管理信息化系统移动端 App 特定 UA 标识通过，实现对客户端工具的合法性校验，进一步控制应用暴露面。

（3）跨域请求校验：为防止某些敏感 URL（如用户认证 API 接口）被恶意请求，应用安全网关针对敏感 URL 实施跨域请求校验，仅允许通过指定网址或指定标识符跳转访问。根据不同请求场景校验的 HTTP 头部字段不同：对 PC 端浏览器发出的敏感 URL 请求，应用安全网关校验 Referer 字段是否为管理信息化系统网址；对移动端 App 发出的敏感 URL 请求，则校验 X-Requested-With 字段是否为 App 特定标识（管理信息化系统移动端 App 上使用 Ajax 请求）。跨域请求源校验策略要求 HTTP 请求头必须携带指定校验字段（Referer 或 X-Requested-With）且字段值必须在白名单内，若条件不满足则中断 TCP 连接。实施跨域请求源校验，能够防止暴露于互联网的敏感 URL 被恶意请求。

2.2 集中数据监测与审计技术

管理信息化系统的安全数据主要包括系统日志数据和流量数据，对客户端采集、Syslog 转发、流量镜像等技术实现集中数据监测和审计。

2.2.1 客户端和 Syslog 的系统日志采集

管理信息化系统日志数据包括系统级日志、网络安全系统日志。

（1）系统级日志（包括应用、中间件、数据库、操作系统）采集主要通过服务器部署日志采集客户端，统一收集并转发。其中，应用日志主要采集用户登录日志、用户操作行为日志，要求在开发阶段明确日志格式，至少包含时间、账户名、真实源 IP 地址、行为等必要信息，用于事后取证；中间件日志主要采集 Web 请求日志，用于网络扫描威胁分析；数据库采集数据查询操作审计记录，用于 SQL 注入攻击的事后取证；操作系统日志主要采集用户、进程、文件、命令等关键行为。

（2）网络安全系统日志采集主要基于 Syslog 协议转发。企业数据中心既有的网络防火墙、Web 应用防火墙（WAF，Web Application Firewall）、网络检测和响应系统（NDR，Network Detection and Response）、端点检测和响应系统（EDR，Endpoint Detection and Response）、蜜罐系统产生的安全告警日志，是辅助威胁判定的重要依据。

2.2.2 基于 SDN 和 NFV 的流量采集

管理信息化系统流量数据主要包括用户与系统间的南北向流量和系统内部不同组件间的东西向流量。基于企业数据中心云计算网络技术，包括软件定义网络技术（SDN，Software-Defined Network）和

网络功能虚拟化技术（NFV，Network Function Virtualization），实现在一张物理网络之上构建多张虚拟网络及虚拟防火墙。通过网络分区隔离，原本同网段内东西向流量转变为跨网段间南北向流量，为管理信息化系统内部互访流量镜像采集分析创造条件。

鉴于各虚拟防火墙与虚拟网络均构筑在物理网络之上，仅需要将镜像采集点设置在物理交换机与防火墙之间即可采集所有分区互访流量。此外，采用隧道封装远程交换端口镜像（ERSPAN，Encapsulated Remote Switch Port Analyzer）技术解决虚拟网络分区内东西向流量采集。ERSPAN 基于通用路由封装（GRE，Generic Routing Encapsulation）技术和本地流量镜像技术，在底层网络可达基础上构建端到端 GRE 虚拟网络隧道，将目标网络内部流量跨 3 层远程传输到流量分析设备上，实现对管理信息化系统的东西向流量采集，如图 4 所示。

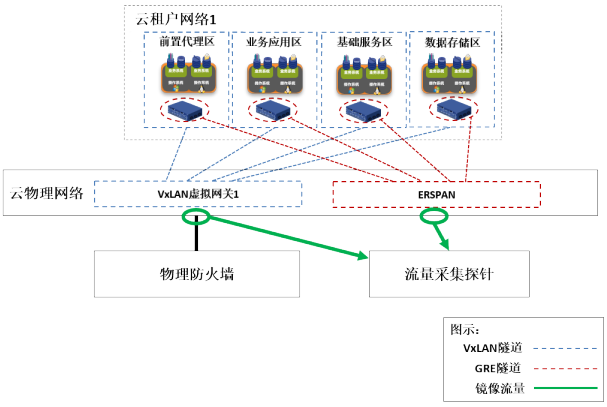

图4　系统全流量采集

2.3　综合威胁分析与响应技术

综合威胁分析与响应技术基于管理信息化系统网络流量和日志监测数据，通过安全编排自动化响应（SOAR，Security Orchestration Automation Response）技术，主动且快速控制威胁风险，其技术架构主要包括威胁感知层、威胁分析层及威胁处置层，如图 5 所示。综合威胁分析与响应技术的实施主要包括基础环境建设、威胁模型建立和威胁防御策略形成，重点针对管理信息化系统的服务总线模块面临的横向威胁开展防护。

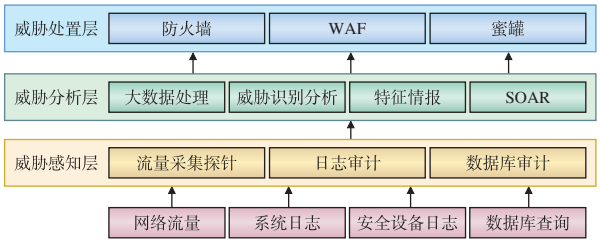

图5　综合威胁分析与响应技术架构

2.3.1　基础环境建设

基础环境建设内容主要包括威胁感知层和威胁处置层建设。

威胁感知层主要基于集中数据监测和审计技术，将管理信息化系统南北向与东西向的网络流量、系统运行日志、安全设备日志、数据库审计日志进行全面采集，其信息采集深度与广度决定了威胁研判的准确性。

威胁处置层通过 SOAR 技术与企业网内各分区、各层级安全防御系统（如防火墙、WAF、蜜罐）建立联动，对分析明确的威胁行为，调动对应区域安全防御系统快速封锁攻击源，实现精准防护。处置层的可控制安全防御设备数量决定了威胁防御的时效性。

2.3.2　横向威胁识别模型建立

威胁识别模型建设基于威胁分析层的大数据分析，通过提取原始流量或日志中的安全特征，根据不同威胁情况将安全特征进行组合建立威胁识别模型。

针对管理信息化系统服务总线的横向威胁识别，内置威胁模型，如 ARP 扫描、端口扫描、口令爆破等，可识别基础的横向威胁；服务总线 API 接口规范抽取安全特征，建立定制化的横向威胁模型。

应用场景：服务总线平台会校验访问 API 接口请求报文的合法性，即请求报文的 HTTP 头部须携带预先注册的请求方身份标识（ClienId）及目的操作（OperationCode）。对于未携带指定字段、或者指定字段的值与注册信息不一致则判定为非法请求，服务总线会返回特定错误码。如图 6 所示，在请求中伪造 ClientId 值，服务总线校验为非法请求并返回 XML 格式错误码“1008”。

将 ClientId 和 OperationCode 字段及服务总线非

图6　服务总线对非法请求返回错误码

法请求错误码作为安全特征，三者进行关联即得到针对服务总线 API 接口的横向威胁模型。

2.3.3　威胁防御策略形成

根据不同业务安全需求场景，以统计、关联等形式应用威胁模型并基于 SOAR 建立联动处置规则，最终形成面向实际业务安全场景的威胁防御策略。

应用场景：基于服务总线平台 API 接口横向威胁模型，采取频率统计方法判定攻击威胁，即在指定时间段内多次匹配该威胁模型则认定服务总线遭受横向渗透攻击，进而，基于态势感知平台 SOAR 实施自动化联动防御。威胁防御策略的应用，实现了威胁从发现到处置在 1 min 内完成，提高安全威胁处置时效性，在当今攻防实战中具有很高实用价值。

3　结束语

铁路设计企业将网络安全充分融入到企业管理信息化系统建设项目中，为网络安全与信息化深度融合打下良好基础。基于等级保护 2.0 中 “一个中心，三重防护” 安全框架，建立网络安全防御技术体系。该安全防御技术体系已在某铁路设计企业得到应用，有效提升了企业管理信息化系统纵深防御能力。对信息系统安全建设有一定借鉴意义。

未来，还须继续完善网络安全体系，依托等级保护定级、安全风险量化分级、数据分类分级等措施，形成网络安全分级防护策略，并建设安全分级防护基础设施环境，进一步提高企业网络安全管理水平。

参考文献

[1] 国家市场监督管理总局，中国国家标准化管理委员会. 信息安全技术 网络安全等级保护基本要求：GB/T 22239-2019[S]. 北京：中国标准出版社，2019.

[2] 魏长水，姚洪磊. 铁路信息系统网络安全风险评估指标体系研究 [J]. 铁路计算机应用，2020，29（8）：33-37.

[3] 张　彦，马延妮，司　群. 基于等级保护思想的网络安全风险评估关键技术研究 [J]. 铁路计算机应用，2020，29（8）：28-32.

[4] 沈　路. 铁路信息系统安全风险评估研究 [J]. 铁路计算机应用，2011，20（6）：22-25.

[5] 陈　勋，张德栋，赵英明，等. 基于等级保护 2.0 的中小型企业网络安全建设研究 [J]. 铁路计算机应用，2021，30（8）：46-51.

[6] 刘　峰，韩　寓. 铁路设计企业安全态势感知技术研究与实践 [J]. 铁路计算机应用，2021，30（11）：68-72.

[7] 高　鹏，陈智雨，闫龙川，等. 面向零信任环境的新一代电力数据安全防护技术 [J]. 电力信息与通信技术，2021，19（2）：7-14.

[8] 熊栋宇，黄　魏. 城市轨道交通生产系统网络安全设计方案研究 [J]. 城市轨道交通研究，2021，24（3）：81-86，91.

责任编辑　徐侃春