文章编号：1005-8451（2020）08-0006-05

基于自适应安全的铁路网络安全框架设计研究

王启东
（中国国家铁路集团有限公司 科技和信息化部，北京 100844）

摘 要：介绍自适应安全框架的定义与特征，结合新形势下的铁路信息系统网络安全保障需求，从基础结构安全、纵深防御、主动防御、联防联治4个方面，提出基于自适应安全的铁路网络安全框架设计思路，并围绕该框架形成风险纵深安全防御、数据纵深安全检测、自动化快速响应、安全情报预警4个重点研究方向，通过体系化的建设模式，提升铁路网络安全防御自适应能力。

关键词：自适应；铁路网络安全框架；防御；检测；响应；预测
中图分类号：U29 : TP393 **文献标识码：**A

Railway network security framework based on adaptive security

WANG Qidong
(Department of Science, Technology and Information Technology, China Railway, Beijing 100844, China)

Abstract: This paper introduced the definition and characteristics of adaptive security framework. Combined with the requirements of railway information system network security under the new situation, from four aspects of infrastructure security, defense in depth, active defense, joint defense and joint governance, the paper proposed the design idea of railway network security framework based on adaptive security, and formed four key research directions of risk in-depth security defense, data in-depth security detection, automatic rapid response and security information early warning around the framework. Through the systematic construction mode, it can be improved the adaptive ability of railway network security defense.

Keywords: adaptive; railway network security framework; defense; detection; respond; predict

铁路网络安全保障体系经过多年建设，初步构建了以外部服务网、内部服务网和安全生产网为层次的纵深防御体系。目前，随着5G、大数据、工业互联网等新技术迅速发展和在铁路信息化建设中的逐步应用，铁路信息系统面临的网络安全威胁已经由互联网攻击、病毒、木马植入等传统攻击方式，转变为事件型、零日漏洞攻击、高频度APT（Advanced Persistent Threat）攻击、黑产形式的大规模数据窃取等威胁行为。以外部网络安全设备为核心的防御体系已经无法满足当前形式下应对网络安全威胁的需要，亟需以实现叠加演进的安全能力为目标，构建体系化、实战化的网络安全保障体系，构成动态、主动的铁路网络安全防御体系。建立能够适应大规模新型网络安全威胁的自适应网络安全保障体系，将会是未来铁路网络安全工作的重点思考方向之一。

收稿日期：2020-03-30
基金项目：中国铁路总公司科技研究开发计划课题（P2018S006）
作者简介：王启东，正高级工程师。

本文介绍自适应安全框架的定义与特征，结合新形势下的铁路信息系统网络安全保障需求，提出基于自适应安全的铁路网络安全框架设计思路，并基于该框架提出了4个应用研究方向。

1 自适应安全框架概述

1.1 自适应安全框架定义

自适应安全框架是2014年由IT研究与顾问咨询公司Gartner提出的面向下一代的安全体系框架之一[1]，以应对云计算、物联网、大数据、移动互联（简称：云物大移）等环境下所面临的安全风险。自适应安全框架按照防御、检测、响应、预测4个维度，把庞大而复杂的网络安全防御工作作为一个持续演进、循环的过程，强调对网络进行细粒度、多角度的监测与响应，对安全威胁进行持续化的实时动态分析。自适应安全框架和经典的PDR（Protection-Detection-Response）网络安全模型相比，在保护、检测和响应领域均有重合的设计思想，而在预测领域，基于对

历史风险和安全现状的分析，突出了对风险不断适应和循环改进的过程，这也是自适应安全框架中具有突破意义的设计理念，尤其在高级持续性攻击防御中，例如对抗 APT 攻击、DDos（Distributed Denial of service）攻击、0Day 攻击，自适应网络安全框架将体现重要优势。

1.2　自适应安全框架的关键能力

自适应安全框架模型如图 1 所示，以持续监控和分析为核心，包含防御、检测、响应和预测 4 部分循环内容 [2]。该框架假设系统始终处在安全风险的环境中，不同于以事件驱动的 PDR 模型，在一定程度上弱化了防御手段的重要性与有效性，通过检测和响应环节的持续监控与分析，强调对未知威胁的预测和感知，自动适应不断变化的网络环境，优化自身安全防御机制。

图1　Gartner自适应安全框架模型

（1）安全防御层面，主要包括加固和隔离、攻击转移和事故预防能力，设计目标在于通过多种成熟的安全防护手段，减少对系统暴露面的攻击。

（2）安全检测层面，主要包括事故检测、风险确认和优先排序、事故隔离能力，设计目标在于检测分析可能绕过安全预防机制的潜在入侵行为，并根据风险进行安全评估、确认和排序，一旦入侵行为被识别，立即进行系统隔离，防止威胁进一步扩散。

（3）安全响应方面，主要包括调查取证、设计建模、修复改善能力，设计目标在于为修复系统和预防新攻击，通过完整的事件调查取证、追踪溯源，重新调整相应的防护策略和控制措施。

（4）安全预测方面，主要包括主动评估风险、预测攻击、安全基线能力，设计目标在于面对不断变化的业务需求和安全威胁，基于态势感知、情报预警等关联分析技术，不断修改、完善安全基线，实现主动风险评估和威胁预测。

2　铁路网络安全内外部风险因素分析

基于纵深防御的国铁企业网络安全框架已建立多年，随着云物大移等信息技术的广泛应用，铁路网络安全框架亟需转型升级，以适应新形势下网络安全保护的需要。目前，铁路网络安全技术防护手段方面缺乏对攻击的快速识别和快速响应能力，难以应对更多、更复杂的未知安全威胁。

（1）当前，国铁企业统建系统总体上按照中国国家铁路集团有限公司（简称：国铁集团）、铁路局集团有限公司（简称:铁路局）、站段三级架构构建 [3]，按照信息系统不同类型进行横向隔离，网络安全防护对象复杂分散，防护手段以防火墙、防病毒、入侵检测等传统安全防护设备为主，各类网络安全设备和系统防护策略执行力度不统一，网络安全防护工作逐渐呈现出“碎片化”现象，网络安全整体发展缺乏实战化的全局洞察和预警能力。

（2）国内外规模性大、破坏性强的网络攻击事件急剧上升，面对愈加严峻的有组织、有目的的网络攻击形势和突发威胁，能够快速触发响应措施，迅速、弹性恢复业务运转的能力尚为不足 [4]，缺乏对事件告警、情报预警、威胁线索等各个方面的闭环管理机制，对网络安全事件的响应速度和预防水平亟待加强。

（3）铁路互联网售票系统和互联网货运系统积累了大量公民个人信息和客户货主信息，针对铁路业务系统内部个人隐私数据的安全防护与风险预警能力有待加强，尤其在云计算与大数据广泛应用后，应用系统和数据高度集中，大规模数据泄露风险增加。

（4）新技术应用带来新的安全隐患，适应新技术应用的能力尚为不足。云物大移等信息技术已在铁路系统内广泛应用，在提升业务竞争力的同时，也给铁路网络安全防护工作带来新挑战。对于业务规模大、应用系统复杂程度高的铁路系统而言，网络安全复杂度和工作量将成倍增长，而传统防护手段

对新技术应用的适应能力尚显不足。

3 设计思路

以应对新形势下网络安全威胁、优化自身安全防御机制为目标，结合铁路网络安全内外部风险因素分析，提出基于自适应安全的铁路网络安全框架，如图 2 所示。该框架是以构建叠加演进型的网络安全能力建设为目的，以提高安全威胁主动检测和网络安全风险动态感知为手段，开展国铁企业基础结构安全、纵深防御能力、主动防御能力、联防联治能力建设 [5-6]。

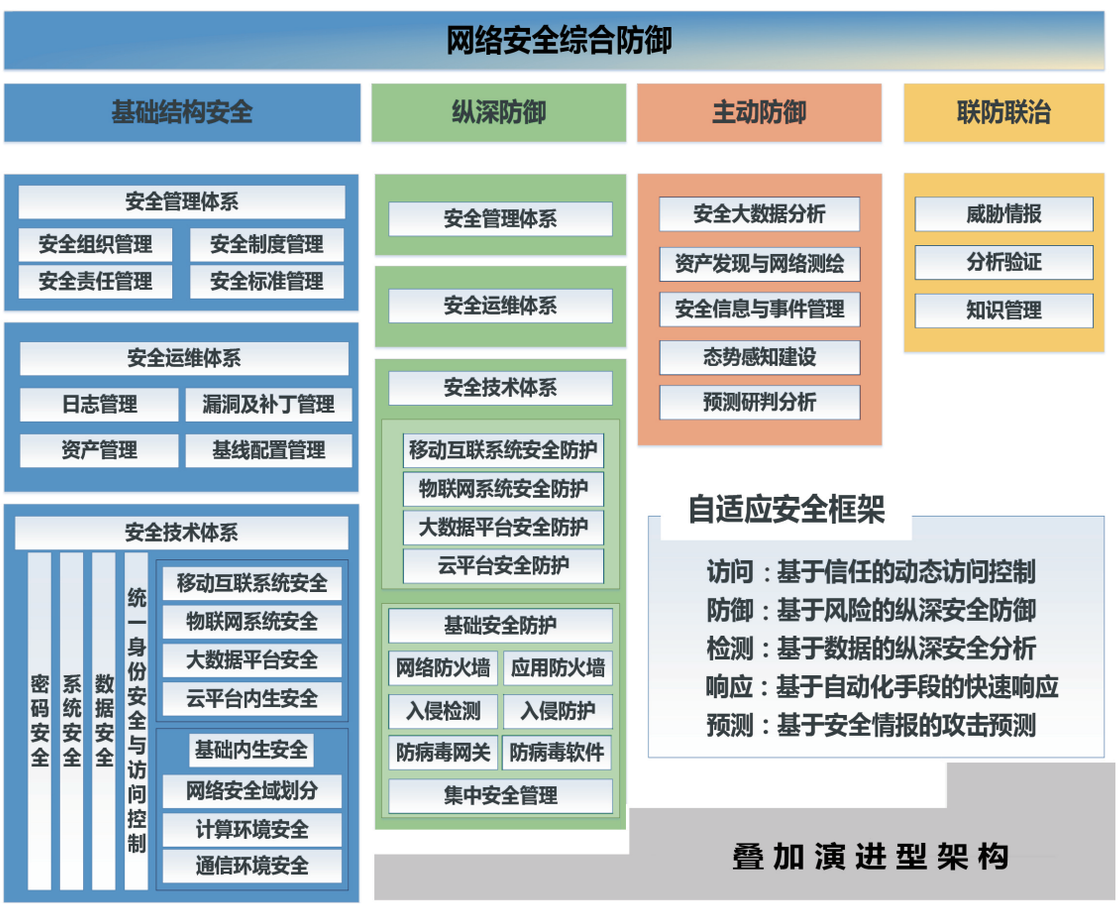

图2 基于自适应安全的铁路网络安全框架

3.1 基础结构安全能力建设

是指国铁企业原有传统网络安全相关工作，具体包括网络安全组织管理、安全制度管理、网络分区分域、系统安全、数据安全、应用开发安全、漏洞与补丁管理、云平台内生安全、大数据平台安全等。基础结构安全作为铁路网络安全根基性的保障工作，是投入成本高、重视度高、长期性重复的工作，是一切网络安全工作的前提。

3.2 纵深防御安全能力建设

是指国铁企业内部为落实网络安全工作，部署在网络、主机、应用等基础架构层面上的静态、被动、外挂式的安全防护设备和系统 [7]，依靠安全防护设备内置的安全策略监控、抵御内外部安全威胁，是国铁企业网络安全防护体系中的重要环节。具体包括纵深防护体系设计、网络边界防护、终端安全、局域网安全等。

3.3 主动防御安全能力建设

主动防御安全能力是指强调网络安全防护工作的积极、主动、动态能力，包括网络安全日志汇聚、安全事件分析、安全编排与自动化、系统内部威胁防控等。国铁企业推行网络安全监控指挥中心后，依托态势感知平台、集中安全管理平台、网络安全监控指挥信息平台等技术平台，规范网络安全监控、攻防演练、事件响应处置流程，强化安全事件的分析、研判和响应处置。

3.4 联防联治能力建设

是指对国铁企业内部网络威胁的识别、理解和预见性的安全能力。基于国铁企业基础安全、纵深防御安全和主动防御能力建设与保障工作，通过扩大威胁视野，使铁路网络安全工作由各自为战转向联合行动，具体包括情报收集、情报生产、情报使用、情报共享等 [8]。

上述网络安全框架设计体现了以网络安全能力为导向的设计思路，构建安全与信息化“深度融合、全面覆盖”的自适应安全体系，逐步提高国铁企业网络安全成熟度。

4　设计实现

4.1　基于风险的纵深安全防御

以健全铁路网络安全基础防御能力为目标，遵循纵深防御理念，基于传统安全防护手段与策略，以等级保护合规建设为基础，综合运用云物大移等信息技术，规划铁路网络安全技术架构，构建覆盖安全通信网络、安全区域边界、安全计算环境等全方位的技术蓝图。在安全工具和技术平台的更新升级、安全技术策略的统筹优化方面，确保安全基线和安全技术规范在铁路应用开发、科研管理、生产运营等工作中有效贯彻落实。

基于风险的网络安全防御技术体系如图 3 所示，在纵深防御能力建设方面，按照网络安全等级保护 2.0 要求，优化网络安全基础性防护措施，强化通信网络、区域边界、计算环境安全防护。在此基础上，利用安全态势感知、异常行为深度检测、威胁情报预警、资产深度数据防护等规划，加强主动防御能力建设。

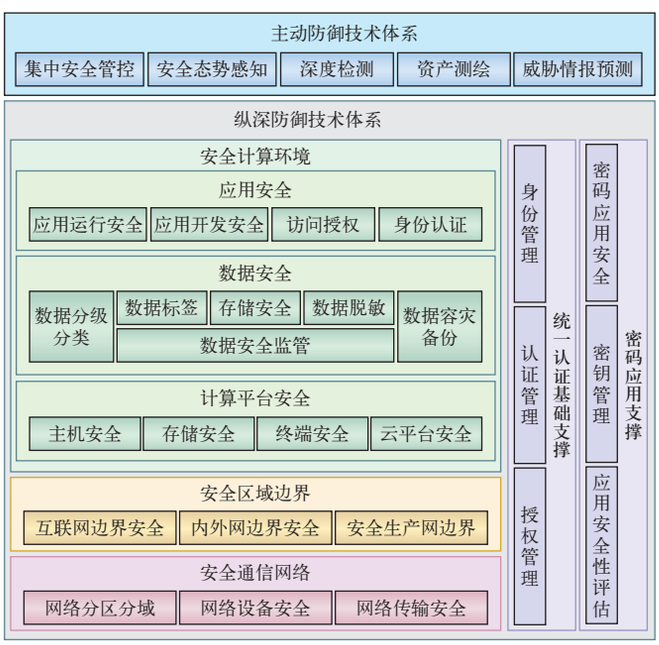

图3　网络安全防御技术体系

4.2　基于数据的纵深安全检测

以提高铁路网络安全主动监管能力为目标，围绕铁路系统核心资产、内部风险脆弱点，依托渗透测试、风险评估、等级保护等手段，组织漏洞分析排查和补丁修复。通过对铁路系统内部终端设备、应用系统、网络设备、存储系统、操作系统、数据库等信息化资产的深度分析，对每个纵深层所产生的数据进行分析研判、信任评估，将不同纵深的数据进行融合关联分析，不断减少对威胁的检测时间，完善检测规则。基于数据的纵深安全检测技术构成如图 4 所示。

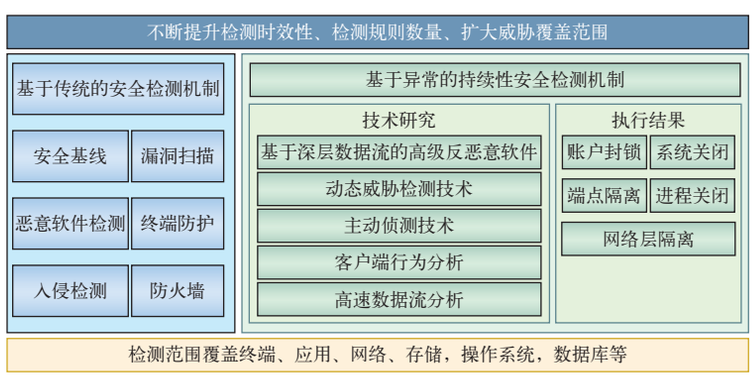

图4　基于数据的纵深安全检测技术构成

4.3　基于自动化手段的快速响应

以加强铁路网络安全持续响应能力为目标[9]，推进信息系统运维调度和应急指挥中心，强化对安全事件的调查取证和追踪溯源能力。建立安全事件问题整改追踪平台，通过集约管理实现安全事件的敏捷运营及快速处置，形成安全响应联动机制，优化防护策略和控制措施，减少事件响应时间，不断提升防护强度，网络安全自动化响应流程如图 5 所示。

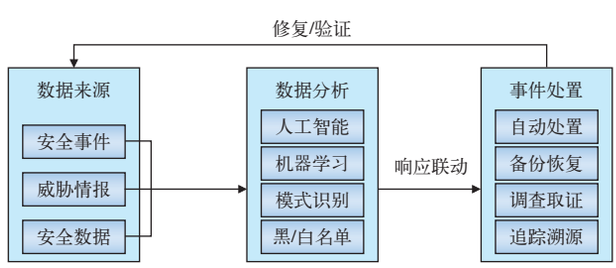

图5　网络安全自动化响应流程示意

4.4　基于安全情报的威胁防控

以深化铁路网络安全主动防御能力为目标，依托信息沟通渠道和通报机制，借助大数据分析、可视化等技术，加快推进安全态势平台、安全情报分

析平台建设[10-11]。围绕终端设备、服务器、业务系统的内在安全要求，持续优化铁路网络安全基线系统能力，逐渐实现对未知、新型攻击的预测与研判，增强对铁路系统内部潜在威胁的识别、理解和预见性的安全能力。通过对网络流量、系统日志、用户行为、文件内容等方面的深度检测，构建铁路内部威胁安全管控机制，对多种安全威胁数据进行自动化挖掘和网络威胁情报关联分析，实现网络安全态势感知和安全威胁的精准预测。

网络安全威胁预警流程如图 6 所示，包含感知、理解和预测 3 个层次的信息处理。感知层用于获取网络环境中的重要数据和安全信息；理解层用于整合、分析感知层的数据和信息，定性或定量地评估网络环境的安全级别与可能面临的安全威胁；预测层基于评估结果，预测网络发展趋势，辅助决策，防止大规模网络安全事件的发生。

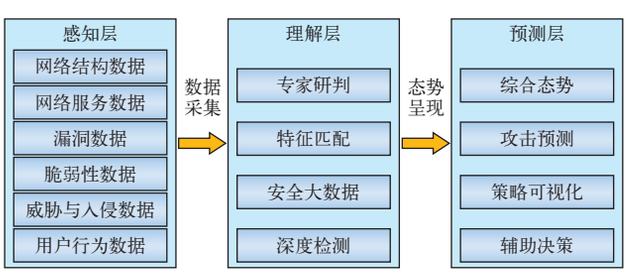

图6 网络安全威胁预警流程

5 结束语

基于自适应安全的铁路网络安全框架给出了以能力为导向的网络安全规划思路，能够避免传统模型下网络安全产品的堆叠，将局部整改模式转变为体系化规划建设模式。本文介绍的规划思路还需要长远的验证过程，同时也要匹配铁路网络安全工作过程中的现状问题，不断适应网络安全的快速发展，确保安全能力能在铁路系统内有效集成，全面提升铁路网络安全保障能力。

参考文献

[1] Peter Firstbrook, Neil MacDonald.Top Security and Risk Management Trends [R]. Stamford, USA: Gartner Research Report, 2020, 2.

[2] Peter Firstbrook, Neil MacDonald. Best Practices for Detecting and Mitigating Advanced Persistent Threats[R].Stamford, USA: Gartner Research Report, 2015, 4.

[3] 张文塔 . 铁路网络安全管理体系的建设与实施 [C]// 第十三届中国智能交通年会学术委员会 . 第十三届中国智能交通年会大会论文集 . 北京：电子工业出版社，2018.

[4] 张继春 . 网络安全面临的风险挑战与战略应对 [J]. 前线，2017（5）：18-23.

[5] 聂　君，李　燕，何扬军 . 企业安全建设指南：金融行业安全架构与技术实践 [M]. 北京：机械工业出版社，2019：17-31.

[6] 周志洪，韩　敏，赵明明，等 . 面向等级保护的网上国网纵深防御体系顶层架构设计 [J]. 计算机工程与应用，2018，54（S2）：111-116.

[7] 杨增宇 . 新时期网络安全工作顶层设计研究 [J]. 中国金融电脑，2020（1）：79-81.

[8] 陈　钟，孟宏伟，关　志 . 未来互联网体系结构中的内生安全研究 [J]. 信息安全学报，2016，1（2）：36-45.

[9] 刘　洋 . 铁路信息系统平台集中安全运维综合监管系统设计 [J]. 铁路计算机应用，2018，27（11）：35-39.

[10] 秦智超，岳兆娟，田　辉 . 应急管理网络信息体系中的内生安全机制设计 [J]. 中国电子科学研究院学报，2019，14（12）：1233-1241.

[11] 李建华 . 网络空间威胁情报感知、共享与分析技术综述 [J]. 网络与信息安全学报，2016，2（2）：16-29.

责任编辑　王　浩