等保2.0时代城市轨道交通信号系统网络安全防护新思路

王　晔,陈丽娟,衣　然
(中国电子信息产业集团有限公司第六研究所,北京 100083)

摘　要:随着网络安全法的深入贯彻和实施,等级保护制度已成为新时期国家网络安全的基本制度,等级保护2.0的出台,网络安全保护对象实现了对云计算、大数据、物联网、移动互联网、工业控制系统的全覆盖。结合等级保护2.0新标准要求以及城市轨道交通信号系统网络安全的建设需求,依照"一个中心,三重防御"核心思想,提出城市轨道交通信号系统网络安全防护新思路。

关键词:城市轨道交通;信号系统;网络安全;等级保护2.0
中图分类号:TP391　　**文献标识码**:A　　DOI:10.19358/j.issn.2096-5133.2020.03.001
引用格式:王晔,陈丽娟,衣然.等保2.0时代城市轨道交通信号系统网络安全防护新思路[J].信息技术与网络安全,2020,39(3):1-5.

A new idea on network security protection of urban rail transit signal system in the era of classified protection 2.0

Wang Ye,Chen LiJuan, Yi Ran
(The 6th Research Institute of China Electronics Corporation,Beijing 100083,China)

Abstract:With the in-depth implementation of the network security law,hierarchical protection system has become the basic system of national network security in the new era. With the classified protection 2.0,network security protection objects have realized the full coverage of cloud computing, big data, Internet of Things, mobile Internet, industrial control system. Combined with the requirements of the new standard of classified protection 2.0 and the construction requirements of network security of urban rail transit signal system, this paper puts forward a new idea of network security protection of urban rail transit signal system according to the core idea of "one center,triple defence".

Key words: urban rail transit;signal system;network safety;classified protection 2.0

0 引言

随着《中华人民共和国网络安全法》的正式实施,我国正式进入网络安全建设新时代。其中明确提到:"国家对公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域,以及其他一旦遭到破坏,丧失功能或者数据泄露,可能严重危害国家安全、国计民生、公共利益的关键信息基础设施,实行重点保护"[1]。

城市轨道交通信号系统作为关键信息基础设施之一,是否能够持续安全运行,直接关系到广大乘客的生命安全和社会运行秩序,一旦遭到破坏,后果不堪设想。目前信号系统网络安全并未受到高度重视,即便进行了网络安全防护建设,但是业务现场仍处于传统的被动的安全防护阶段,主要采用"封、堵、查、杀"的方式筑起安全防线。面对新形势下有目的性的新型网络攻击,必须调整安全建设思路,在网络和信息系统安全防护被攻击之前,构建主动防御体系,保障城市轨道交通信息基础设施的运行安全。

1　安全需求分析

1.1　系统网络结构

信号系统按访问对象划分为三大安全区域,包括控制中心、设备集中站(含车辆段、停车场)、非设备集中站,其中业务系统包括列车自动监控子系统(ATS)、列车自动防护子系统(ATP)、列车自动驾驶子系统(ATO)、数据通信子系统(DCS)、联锁子系统(CI)、维护子系统(MSS)等多个子系统。各子系统通过信息交换网络构成闭环系统,实现地面控制

与车上控制结合、现地控制与中央控制结合,构成一个集行车指挥、运行调整以及列车驾驶自动化等功能为一体的列车自动控制系统。按照信号系统实际业务需求,目前信号系统的等级保护只覆盖到ATS 子系统和维护网子系统。信号系统网络结构示意图,如图 1 所示。

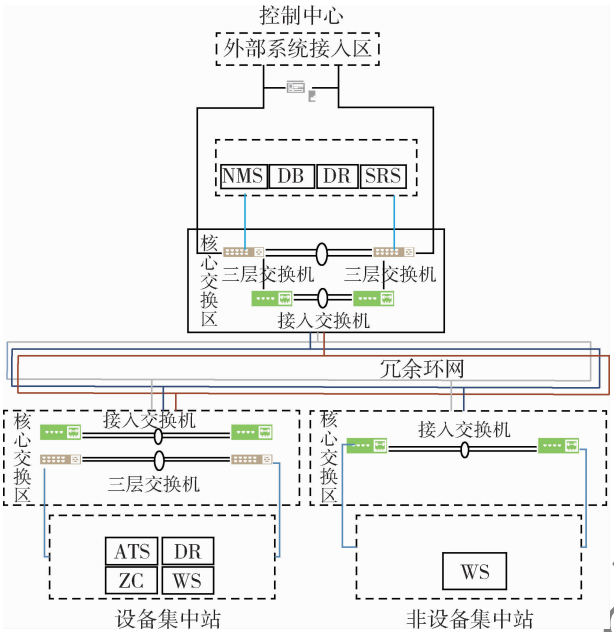

图 1　信号系统网络结构示意图

1.2　安全防护现状

目前,既有信号系统的安全防护大部分仅限于采用了传统防火墙、防病毒等初级的防护措施。传统防火墙主要进行两个网络之间的逻辑区域隔离控制,主要访问控制、安全域管理等功能,但是传统防火墙一般未装载工业协议解析模块,不能理解支持工业控制协议,传统防火墙的架构也不太适应工业网络实时性和生产环境的要求。终端主机防护通过安装防病毒软件来实现,但是防病毒软件需要定期升级最新的病毒库,工业控制系统网络环境下不能保证病毒库实时更新。

新建信号系统参照等级保护 1.0 的标准做了比较完善的安全防护工作,主要体现边界防护、安全检测、安全审计等方面。

(1)对信号系统与外部接口的网络边界部署工业防火墙,工业防火墙除了传统防火墙具备的访问控制、安全域管理等功能外,还增加了针对工业协议的深度解析模块,可以做到对信号系统应用层协议内容的解析,防止应用层协议被篡改或破坏。另外信号系统的核心交换机一般都进行了 VLAN 划分[2],将服务器、工作站、安全设备划分在不同的 VLAN 中,降低了网络被攻击后的风险。

(2)对关键主机和服务器的配置进行加固、补丁管理、漏洞修复等措施,部分通过部署白名单防病毒软件对恶意代码和恶意程序运行进行有效阻止。

(3)在核心区域交换机镜像口旁路部署入侵检测系统。对各级交换系统间的通信流量进行分析,检测病毒、蠕虫、木马、间谍软件、可疑代码、扫描等网络威胁攻击,一旦发现攻击及时上报。

(4)通过部署日志审计系统,对信号系统网络中的安全设备和主机、网络设备、安全设备日志信息集中审计分析。

1.3　风险分析

信号系统现有的这些传统的安全防护手段虽然可以抵御大多数常见类型的威胁和攻击,但存在着局限性,有一定的安全风险隐患。

(1)缺少整体的安全体系规划,部署的安全产品各司其职,关联程度不高,仅能进行单点或单一层面的防护,防护体系呈现扁平化的结构,没有构建统一的安全防护体系,这就是安全产品堆砌很多,但是防护能力依然欠缺的原因。

(2)防护手段主要作用于攻击或威胁发生后,属于静态监测、被动防御,对于未知威胁和新型网络攻击却很难发挥作用。

(3)信号系统的安全风险状态不能预测,缺少工控系统安全态势感知能力,无法从资产、脆弱性、威胁等多个视角全面分析安全态势。

(4)安全管理方面,运营人员安全意识不足,信息安全技术水平较低,需要信息安全管理能力的提升。

2　安全防护新思路

信号系统的网络安全防护在做好顶层设计构建安全防护体系的基础上,重点在等保 2.0 新增要求项上展开安全防护新思路,主要体现在新型网络攻击防护,预知安全态势,以及组建专业的安全管理团队,提高安全防护保障能力等方面。

2.1　顶层安全设计

构建信号系统网络安全防护体系需要从信号系统业务流程及系统安全需求分析为基础,保证信号系统所有用户访问、操作都经过授权,保证信号系统运行环境安全可靠,保证各种安全机制不被旁路,因此必须以可信计算为基础,以细粒度的访问

控制为核心,遵循“一个中心、三重防护”的原则构建信号系统网络安全纵深防护体系[3-4]。

“一个中心、三重防御”是指以安全管理中心为核心,构建以安全计算环境为基础、安全区域边界和安全通信网络为保障的信息安全整体防护体系。信号系统安全防护体系如图 2 所示。

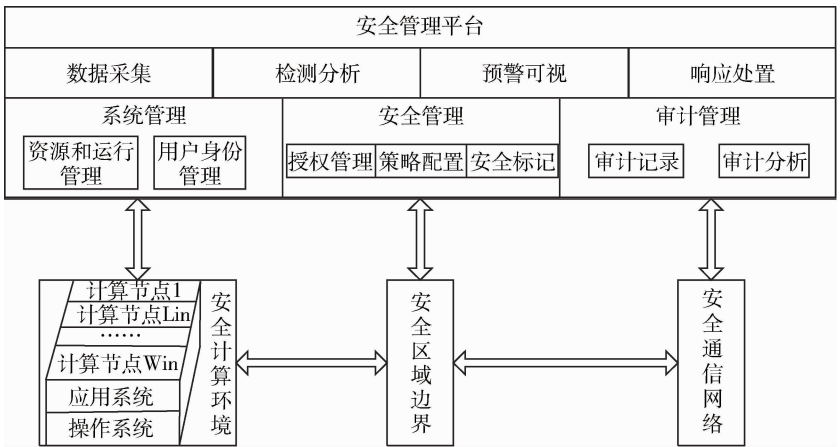

图 2 信号系统安全防护体系

安全管理中心是一个集合的概念,核心是实现所有安全机制的统一集中管理,是三层防护体系的控制中枢。安全管理中心由安全管理平台实现,基本功能包括系统管理、安全管理、审计管理,同时建立全局统一可控的态势感知平台,共同为信号系统的安全可靠运行提供重要支撑。

安全管理平台采用“三权分立”,权利最小化原则。系统管理主要功能是对信号系统的整体运行情况进行管控,确保系统稳定高效运行。对计算环境内的工作站、服务器等主机类设备,路由器、交换机等网络设备,安全设备以及网络流量和用户行为进行监测,对管理人员以及用户身份进行集中管理和授权等;安全管理主要功能是对信号系统安全策略实行统一配置、参数设置,安全标记,对设备的安全性和可用性实时监控,设置告警阈值;审计管理用于采集和处理整个信号系统中各个节点的审计信息,包括终端用户的登录、文件的读写、入侵日志、网络访问行为等,通过对审计信息的关联分析,分析出信号系统可能存在的安全风险。

安全计算环境是信号系统安全的核心和基础,是授权和访问控制的源头。一方面计算环境安全通过主机、服务器操作系统、应用系统和数据库自身的安全服务机制,保障应用业务处理全过程的安全。另一方面设置以强制访问控制为主体的系统安全机制,通过对用户行为的控制,来防止非授权用户访问和授权用户越权访问,同时限制终端设备相关端口的使用。

安全区域边界是信号系统与外部系统进行数据交互的区域,安全区域边界重点对进入和流出计算环境的信息实施控制和保护,允许安全策略内的信息流经过边界。为满足访问控制、边界完整性检查、入侵防范等基本安全要求,一般在关键网络节点处,部署工控网关类设备、入侵检测类设备等进行安全防护。

安全通信网络是计算环境之间实现信息传输功能的载体,信号系统通信网络主要是安全区域之间的网络通道,安全通信网络需要确保用户信息传输过程中不被窃听、篡改和破坏,需要对通信流量实时监控,对异常流量和操作及时告警和记录。

2.2 应对新型网络攻击

随着针对工控系统的新型网络攻击的出现,如 APT 攻击、勒索软件、远程木马、网络蠕虫、邮件钓鱼等,信号系统虽然采用了一些网络安全防护措施,但仍面临着网络信息安全的严峻考验。其中 APT 攻击是信号系统面临的最大威胁,这种攻击通常采用 0day 漏洞,攻击目标明确,持续时间很长,很难被发现和进行防御。

因此采用有效的技术应对新型网络攻击,成为信号系统安全防护的重要部分。在《GBT22239-2019 信息安全技术网络安全等级保护基本要求》以及《GBT28448-2019 信息安全技术网络安全等级保护测评要求》中也明确提出要求,应采取技术措施

对网络行为进行分析,实现对网络攻击特别是新型网络攻击行为的分析,应部署抗 APT 攻击系统、网络回溯系统和威胁情报检测系统或相关组件,并验证是否对网络行为进行分析,实现对网络攻击特别是未知的新型网络攻击的检测和分析[5-6]。

结合信号系统的网络架构以及业务特点,结合现有的防护手段,可以通过建立信号系统运行白环境来应对新型网络攻击[7]。

(1)信号系统区域边界层面的防护,首先确定系统的区域边界,信号系统的区域边界比较清晰,一般是与综合监控系统(ISCS)、乘客信息系统(PIS)、广播系统(PA)等外部系统互联互通。在信号系统的区域边界处部署工业防火墙,在对信号系统应用层通信协议深度解析的基础上,利用特有的白名单访问控制机制,实现信号系统边界最小授权管理控制,保证只有可信任的设备才可以接入,与业务相关的访问才可以连接。

(2)在网络关键节点部署基于"白名单"技术的深度检测系统,通过对采集的 ATS 网、维护网所有通信流量机器智能学习,建立信号系统正常通信流量模型,实时监测异常流量并告警,保证只有可信任的流量才能在信号系统网络中传输。

(3)在终端主机部署白名单架构的安全防护软件,防护软件扫描信号系统主机的进程,对经过确认的可执行程序生成一个唯一的特征码,特征码集合起来形成特征库,即白名单。只有白名单内的可执行程序才可以运行,其他进程都被阻止,从根本上扼制恶意代码的运行。

2.3 感知未来安全态势

习近平总书记在 419 座谈会上提出:"要树立正确的网络安全观,加快构建关键信息基础设施安全保障体系,全天候全方位感知网络安全态势,增强网络安全防御能力和威慑能力"。随着网络安全法、等级保护 2.0 等政策标准的出台,对未来安全态势的感知被提升到了战略高度,安全态势感知技术应需迅速崛起。态势感知的最终目的是能够基于环境动态地、整体地识别安全风险,依靠大数据的支撑,从整个系统视角发现识别安全威胁,进而理解分析预警,最终响应处置落地。

信号系统在安全管理中心三大功能的基础上,强化安全态势感知,通过安全态势感知平台建设,实现对所有安全设备的安全事件的统一收集、关联分析达到安全态势感知,宏观展现系统的安全态势。安全管理中心的安全态势感知功能主要由信号系统防护、检测、审计系统共同实现,通过对信号系统的安全信息进行统一持续监测,对采集的数据进行深度分析和信息挖掘,发现面临的信息安全威胁态势,对正在发生的及将来的威胁进行"客观、准确、及时、直观"的集中展示与告警,为安全风险威胁提供分析手段,为安全保障措施提供客观的决策依据。

在信号系统中,安全态势感知网络相当于人体的神经系统;工业防火墙、深度检测系统、安全审计系统等安全设备以及服务器、网络设备作为态势感知信息来源的基础,相当于神经元;安全分析相当于神经中枢——大脑,每个安全事件的处理过程就相当于神经传导和处理过程[8]。信号系统的态势感知目标就是要为信号系统 IT 资源及其业务系统穿上一件保护外套,部署一套全方位的态势感知网络。态势感知网络示意图如图 3 所示。

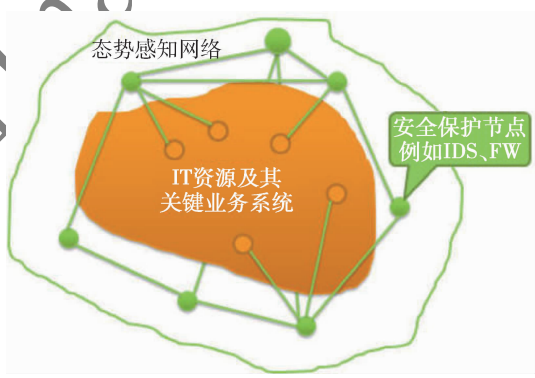

图 3 态势感知网络示意图

传统的态势感知仅是通过采集安全设备的审计信息和扫描结果进行总结归纳,以图表的形式展示出来,主要针对已知网络攻击行为进行监测和评估,评估结果单一,也没有实现网络安全态势感知的预测功能。如今,态势感知需要采集多个维度信息源的数据,采用数据分析技术识别海量数据中有用的信息,通过机器学习、威胁情报分析等自动生成分析模型,由已知威胁来推演未知威胁,对未来安全趋势进行风险预警和协同防御。态势感知框架[9-10]如图 4 所示。

首先,态势感知需要有大数据的支撑,应具有主动采集能力。数据来源包括信号系统资产信息、拓扑信息、系统性能和运行状态信息、各种设备告警、警报、事件、日志等原数据。

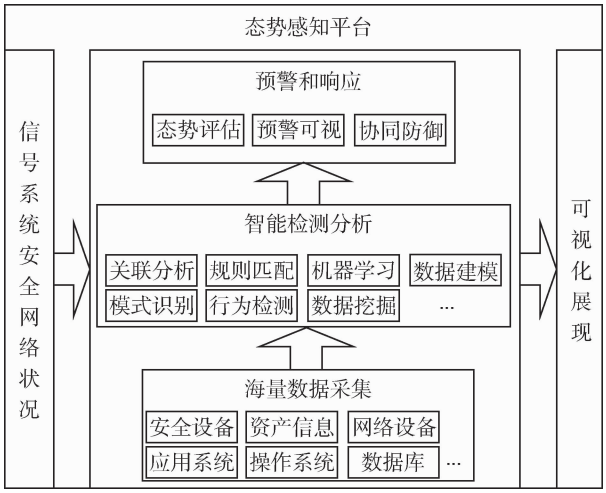

图 4　态势感知框架

其次,通过智能化检测分析,从海量数据中分析出有效的安全问题,如威胁、脆弱性等。智能分析不仅仅是匹配静态特征库进行安全威胁分析,要基于流量特征、行为分析建模、机器学习、数据关联等进行深度智能数据分析,从而具有解决未知威胁的能力。

最后,智能分析结果送入预警与响应模块,一方面借助态势可视化进行预警展示,另一方面,送入流程处理模块进行流程化响应与安全风险运维,做到及时、高效响应处置。

2.4　组建安全管理团队

"三分技术,七分管理",技术是安全防护的必要手段,人是安全防护的核心和尺度。信号系统运营人员普遍存在安全意识不高,安全知识缺乏,安全能力不足的问题。面对日益严峻的网络安全现状,需要组建专业的安全管理团队来提供网络安全保障服务。安全管理团队可以由信号系统运营单位自己组建,也可通过专业的第三方安全团队来提供安全管理。安全管理团队在做好基本安全管理工作的同时,还需加强以下管理工作:

(1)做好系统风险监测、预警通报工作,及时向有关部门通报可能影响系统的重大漏洞和风险。

(2)做好应急预案,定期开展应急演练,在演练过程中通过发现现存的网络安全问题,找到安全防护体系的短板,及时弥补持续优化,提升安全防护能力。同时通过演练提高面对突发网络攻击的应急响应和应急处置能力[11]。

(3)负责突发安全事件的响应和处置,攻击过程的分析和处理,以及事件的调查与溯源,做好事后的总结工作。

3　结论

随着信息化的发展,网络安全形势越来越严峻,尤其是 APT 等新型攻击方式层出不穷,信号系统传统的防御措施已经无法应对新型网络攻击。等级保护 2.0 时代信号系统安全防护要在现有的传统安全防护基础上,结合等级保护新增要求项,做好安全防护顶层设计。以"一个中心、三重防御"为核心思想,构建一个事前态势感知、事中响应防护、事后追踪溯源的主动安全防御体系,全面提升信号系统网络安全感知能力和防护能力。

参考文献

[1] 中华人民共和国网络安全法[S]. 2017-06-01.
[2] 李莉,杨帆. VLAN 技术在地铁信号系统数据通信网中的应用[J]. 铁路通信信号工程技术,2014,11(6):64-67.
[3] GB/T 22239-2019. 信息安全技术网络安全等级保护基本要求[S]. 2019.
[4] 姜立群,刘畅,井柯. 城市轨道交通 CBTC 信号系统网络安全方案[J]. 自动化博览,2018:56-59.
[5] GB/T 25070-2019. 信息安全技术网络安全等级保护安全设计技术要求[S]. 2019.
[6] GB/T 28448-2019. 信息安全技术网络安全等级保护测评要求[S]. 2019.
[7] 威努特工业控制系统网络安全"白环境"解决方案[EB/OL]. [2019-12-31]. https://wenku. baidu. com/view/e152e889fab069dc 502201aa. html.
[8] 赵龙. 威努特:构建工控系统威胁预警和安全态势感知能力[J]. 智能制造,2017:13-16.
[9] 罗珍珍. 铁路信号系统信息安全态势评估方法研究[D]. 北京:北京交通大学,2018.
[10] 陶源,黄涛,张墨涵,等. 网络安全态势感知关键技术研究及发展趋势分析[J]. 信息网络安全,2018(8):79-85.
[11] 工业和信息化部. 工业控制系统信息安全防护指南[Z]. 2016-10-17.

(收稿日期:2019-12-31)

作者简介:

王晔(1986 -),女,硕士,网络安全等级测评师,主要研究方向:工控信息安全。

陈丽娟(1990 -),女,本科,网络安全等级测评师,主要研究方向:工控信息安全。

衣然(1988 -),男,硕士,网络安全等级测评师,主要研究方向:工控信息安全。

版权声明