地铁车辆乘客信息系统的网络安全分析与优化策略

葛亮

南京地铁运营有限责任公司

DOI: 10.12238/ems.v6i10.9351

[摘要] 随着城市化进程的加快, 地铁作为城市交通的重要组成部分, 其乘客信息系统也日益复杂。本文探讨了地铁车辆乘客信息系统中的网络安全问题, 并提出了相应的解决措施, 以期提高系统的安全性和稳定性。

[关键词] 地铁车辆; 乘客信息系统; 网络安全

Network Security Analysis and Optimization Strategy of Subway Vehicle Passenger Information System

Ge Liang

Nanjing Metro Operation Co., Ltd

[Abstract] With the acceleration of urbanization, as an important component of urban transportation, the subway's passenger information system is becoming increasingly complex. This article explores the network security issues in the passenger information system of subway vehicles and proposes corresponding solutions to improve the security and stability of the system.

[Keywords] subway vehicles; Passenger information system; network security

一、地铁车辆乘客信息系统

地铁车辆乘客信息系统 (Passenger Information System, PIS) 是地铁运营中的关键组成部分, 旨在为乘客提供实时信息和服务。该系统通常包括车载显示屏、车站显示屏、语音播报系统和移动应用程序等多个子系统。其主要功能是发布列车运行信息、到站提醒、紧急通知等, 以提高乘客的出行体验和安全性。此外, PIS 还可以与其他地铁系统 (如票务系统、监控系统) 进行集成, 形成一个综合的信息服务平台。PIS 不仅提升了地铁运营的效率, 还增强了信息的透明度和及时性。然而, 随着信息技术的发展, PIS 面临着越

来越严峻的网络安全挑战, 必须采取有效的措施来保护系统的安全和稳定运行。

二、地铁车辆乘客信息系统网络安全的含义

PIS 系统网络安全是指通过各种技术和管理手段, 保障 PIS 及其数据免受恶意攻击、破坏和未授权访问, 从而确保信息的机密性、完整性和可用性。具体来说, PIS 网络安全涵盖以下几个方面:

首先, 保护信息的机密性, 即防止未经授权的访问和泄露。对于 PIS 而言, 乘客个人信息、实时运行数据等均需严格保护, 避免因信息泄露而引发隐私问题或运营安全隐患。

其次, 确保信息的完整性, 防止数据被篡改或破坏。PIS 中的信息必须准确无误, 例如列车时刻、运行状态和紧急通知等, 一旦这些信息被恶意篡改, 可能导致乘客误导, 甚至引发安全事故。

第三, 保障信息的可用性, 即确保系统在需要时能够正常运作。PIS 需要在高峰时段、紧急情况下始终保持高效运行, 任何形式的网络攻击导致系统瘫痪或信息传输中断, 都将严重影响地铁运营和乘客安全。

最后, PIS 网络安全还包括防范各种网络威胁, 如病毒、恶意软件、拒绝服务攻击等。通过防火墙、入侵检测系统、加密技术等多层次防护手段, 建立一个安全可靠的网络环境。

三、网络安全的主要问题

1. 地铁乘客信息系统中的网络通信问题

地铁乘客信息系统依赖于网络通信来传递实时数据和指令, 包括列车位置、运行状态和乘客公告等。网络通信问题主要表现为数据传输过程中的安全隐患。例如, 网络通信容易受到各种攻击, 如数据截获、中间人攻击和拒绝服务攻击。黑客可以通过窃听网络数据包, 获取敏感信息, 或者通过篡改数据包内容, 导致乘客信息失真。网络通信的不稳定性也是一个问题, 尤其是在地铁环境中, 地下隧道和高铁速度会导致信号强度波动, 影响数据传输的可靠性。此外, 不同子系统之间的通信协议和数据格式差异, 也可能导致数据传输错误和信息丢失, 进而影响系统的正常运行。为了保证地铁乘客信息系统的稳定性, 必须重视网络通信中的这些安全隐患。

2. 地铁乘客信息系统中的通信传输协议问题

通信传输协议是地铁乘客信息系统中各个子系统进行数据交换的基础。然而, 许多现有的传输协议存在安全漏洞, 容易被攻击者利用。例如, 一些协议缺乏加密措施, 导致数据在传输过程中容易被截获和篡改。部分协议的身份认证机

制不完善, 使得非法访问和数据篡改的风险增加。另外, 不同厂商和系统之间使用的通信协议不统一, 增加了兼容性问题和安全管理的复杂性。例如, 某些旧版协议在设计时没有考虑到现代网络安全威胁, 无法抵御当前复杂的网络攻击手段。此外, 通信协议的更新和升级通常需要较长的时间和较大的成本, 这使得地铁乘客信息系统容易长期处于安全风险之中。通信传输协议的安全性直接影响着地铁乘客信息系统的整体可靠性和数据安全性, 必须给予高度重视。

四、网络安全应对措施

1. 建立健全网络分析系统, 强化技术手段管控

地铁乘客信息系统需要一个全面的网络分析系统来监控和分析网络流量。网络分析系统通过实时监测数据流动, 发现异常行为和潜在威胁。系统可以利用大数据分析和机器学习算法, 识别复杂的攻击模式和行为特征。引入高级的入侵检测系统 (IDS) 和入侵防御系统 (IPS), 可以有效拦截和响应网络攻击。防火墙和 VPN (虚拟专用网络) 也是网络安全的重要技术手段, 它们可以保护数据传输的安全性和完整性。通过定期进行漏洞扫描和渗透测试, 能够及时发现并修补系统中的安全漏洞。网络分析系统的建立和技术手段的强化, 为地铁乘客信息系统提供了坚实的安全保障。

2. 设置网络边界, 确保系统安全

地铁乘客信息系统的网络安全依赖于明确的网络边界设置。通过在网络边界部署防火墙, 可以有效地控制和过滤进入系统的流量。防火墙能够阻止未授权的访问, 防止外部攻击者入侵内部网络。划分网络区域也是一种有效的安全措施, 将不同的子系统和应用程序隔离, 减少安全事件的影响范围。使用隔离技术, 如虚拟局域网 (VLAN) 和网络分段, 能够进一步细化网络边界的管理。外部连接和远程访问也需要严格控制, 通过 VPN 和双因素认证等手段, 保证访问者的身份验证和数据传输的安全性。网络边界的设置和管理, 为地铁乘

客信息系统提供了多层次的保护,降低了安全风险。

3. 实施操作权限分级,提高入侵检测能力

操作权限分级是防止内部安全威胁的有效策略。通过对不同角色和用户赋予不同的操作权限,可以减少因误操作或恶意行为导致的安全事件。系统管理员可以设置严格的权限控制策略,确保只有经过授权的用户才能访问特定数据和功能。结合入侵检测系统(IDS),能够实时监控用户行为,识别异常操作并及时报警。日志记录和审计也是关键手段,系统会详细记录用户的操作历史,便于事后追查和分析。通过定期审查权限设置和用户活动,可以及时调整权限分级策略,防止权限滥用。操作权限分级和入侵检测的结合,构建了一个动态防御体系,有效提高了地铁乘客信息系统的安全性。

4. 完善系统检测体系,强化日常操作管理

地铁乘客信息系统的安全依赖于一个全面且有效的系统检测体系。这个体系包括定期的安全检查、漏洞评估和系统更新。通过引入自动化监控工具,可以持续监控系统的运行状态,及时发现和响应安全威胁。自动化工具能够识别异常活动,如异常登录尝试或异常数据流量,帮助管理员快速采取应对措施。定期进行漏洞扫描和渗透测试,是检测系统潜在安全风险的重要手段。通过模拟攻击,发现系统中的安全漏洞,并及时修补,防止恶意攻击者利用这些漏洞。此外,制定详细的操作规程和应急预案,可以有效指导日常操作和紧急情况下的处理步骤。操作规程应包括系统维护、更新和备份的具体流程,确保系统在正常运行中保持高水平的安全性。应急预案则应明确突发事件的应对措施,减少安全事件对系统的影响。加强日常操作管理,通过培训和教育,增强员工的安全意识和操作技能,也是维护系统安全的重要措施。

5. 引入第三方评估,夯实系统管理培训

第三方评估可以为地铁乘客信息系统提供独立的安全审计和专业建议。引入独立的安全评估机构,能够全面审查系

统的安全措施,发现内部人员可能忽视的安全漏洞。这些机构拥有丰富的经验和先进的技术手段,能够提供客观的评估报告和改进建议。评估报告不仅有助于了解当前系统的安全状况,还可以作为改进安全策略的依据。此外,第三方评估有助于提高系统的可信度,向公众和相关监管机构展示对网络安全的重视。系统管理培训则是增强内部人员安全意识和技能的关键措施。通过定期举办安全培训课程,更新员工对最新安全威胁和防护措施的认知,提升整体防护水平。培训内容应包括网络安全基本知识、应急响应技能和操作规程,确保所有人员都具备必要的安全操作能力。结合实际案例和模拟演练,增强员工应对真实安全事件的能力。引入第三方评估和加强系统管理培训,能够构建一个全面、动态的安全防护体系,为地铁乘客信息系统的安全运行提供有力保障。

五、结语

本文探讨了地铁乘客信息系统的网络安全问题,并提出了一系列应对措施。地铁乘客信息系统的网络安全不仅涉及网络通信和传输协议问题,还包括完善的检测体系和日常操作管理。我们建议通过建立健全的网络分析系统,设置明确的网络边界,以及实施操作权限分级等方法来增强系统的安全性。此外,引入第三方评估和强化系统管理培训,可以进一步提高安全防护水平。笔者认为,只有通过多层次的综合措施,才能有效保障地铁乘客信息系统的安全和稳定运行,为乘客提供可靠的出行服务。

[参考文献]

- [1]高蕾,王声柱,李虹江,等.地铁网络安全管理的有效性探究[J].智能城市,2022,8(04):59-61.
- [2]周品荣,戴海燕.轨道交通网络安全管理中心与综合监控系统融合的网络安全监控与协同联动研究[J].城市轨道交通研究,2023,26(10):206-210.