轨道交通自动售票机系统的信息安全防护技术研究

易新林
重庆轨道交通运营有限公司　重庆　400000

摘　要：轨道交通自动售票机系统信息安全防护技术是保障轨道交通运营安全的关键。研究聚焦系统架构脆弱性，分析硬件、软件、网络层安全威胁，提出动态加密、隐私保护、量子密钥分发、零信任网络架构等防护技术，并结合AI异常检测、区块链审计日志存储等手段，构建多层次防御体系，有效抵御数据窃取、系统控制权夺取等攻击，提升系统抗风险能力。

关键词：轨道交通；自动售票机系统；信息安全；防护技术

引言：随着轨道交通智能化、网络化发展，自动售票机系统作为票务交易核心终端，面临数据泄露、恶意攻击等安全挑战。其涉及支付信息处理、票务数据传输及设备远程运维等关键环节，一旦遭受攻击将直接影响运营秩序与乘客财产安全。然而，现有防护体系多依赖传统技术，难以应对新型复合威胁。因此，研究轨道交通自动售票机系统的信息安全防护技术，构建多层次、动态化的安全防御体系具有重要的现实意义。

1 轨道交通自动售票机系统安全威胁分析

1.1 系统架构与脆弱性

（1）硬件层，工控机、读卡器、支付终端作为系统核心硬件，存在广泛物理攻击面。工控机接口缺乏有效防护，易被植入外接设备读取内部数据；读卡器易遭受侧信道攻击，泄露卡片加密信息；支付终端若未做防拆解设计，可能被篡改内部电路，窃取支付密码、银行卡信息等敏感数据。（2）软件层，系统多采用定制化操作系统，虽简化了功能，但漏洞更新不及时，易被攻击者利用；中间件配置常存在默认密码、权限过高问题，攻击者可通过配置缺陷突破软件防护，获取系统操作权限。（3）网络层，车地通信依赖LTE/5G技术，无线传输过程中存在信号拦截、篡改风险；内部专网未严格划分权限，设备接入缺乏有效校验，易遭受中间人攻击，窃取或篡改设备间传输的票务、支付数据[1]。

1.2 典型攻击场景建模

（1）支付信息窃取，攻击者通过侧信道攻击分析支付终端的电流、电磁信号，破解加密算法；或通过内存数据提取技术，获取终端临时存储的银行卡号、支付密码等敏感信息，造成用户财产损失。（2）系统控制权夺取，攻击者篡改设备固件，植入恶意程序，绕过系统验证；或通过恶意代码注入，利用软件漏洞夺取工控机控制权，进而操控整个售票机系统，篡改票务数据、植入虚假支付界面。（3）服务可用性破坏，攻击者发起DDoS攻击，占用系统网络带宽与计算资源，导致售票机无法响应用户操作；或篡改系统核心业务数据，造成票务紊乱、交易失败，中断轨道交通售票服务。

1.3 安全需求分析

（1）功能性需求，核心是保障数据保密性、完整性、可用性。保密性要求对支付信息、用户数据进行加密存储与传输，防止泄露；完整性要求建立数据校验机制，抵御数据篡改；可用性要求提升系统抗攻击能力，避免服务中断，保障用户正常购票。（2）合规性需求，需严格遵循PCIDSS支付卡行业规范，规范支付终端配置、数据存储与传输流程，保障支付安全；同时符合GDPR数据保护要求，明确用户数据收集、使用范围，建立数据泄露应急机制，保护用户隐私权益。

2 轨道交通自动售票机系统的信息安全防护关键技术研究

2.1 数据安全防护技术

（1）动态加密机制，采用国密SM4算法应用于票务数据传输全过程，替代传统加密算法提升防护等级。该算法支持128位密钥加密，具备高效性与抗破解性，可根据票务数据类型（如购票信息、支付凭证、订单记录）动态调整加密密钥，避免固定密钥泄露带来的风险。在数据传输时，先对票务明文进行分段加密，搭配时间戳生成唯一加密标识，接收端通过对应密钥与标识校验解密，确保数据在车地、机网传输过程中不被窃取、篡改，适配轨道交通高频数据交互场景[2]。（2）隐私保护技术，将差分隐私技术应用于乘客行为分析实践，在保障数据分析价值的同时保护用户隐私。通过向乘客行为数据（如购票时间、线路选择、支付方式）中添加微小扰动噪声，模糊单个用户的具体行为特征，避免攻击者通过数据分析溯源定位个人。同时设置合理的隐私预算，平衡数据可

用性与隐私保护强度，既可为轨道交通运营调度提供数据支撑，又防止乘客隐私信息泄露，符合数据保护相关规范要求。

2.2 通信安全防护技术

（1）量子密钥分发（QKD）在车地通信中的可行性研究，QKD基于量子力学原理，可生成理论上绝对安全的加密密钥，解决传统密钥分发易被拦截破解的问题。结合轨道交通车地通信LTE/5G传输场景，优化QKD节点部署，简化密钥协商流程，降低设备部署成本与能耗，适配车载终端、售票机构件的小型化需求。通过实验验证QKD在高速移动、信号干扰环境下的密钥生成速率与稳定性，论证其在车地票务数据、控制指令传输中的可行性，提升车地通信抗攻击能力。（2）基于SDP（软件定义边界）的零信任网络架构设计，打破传统网络“内外网隔离”的防护理念，遵循“永不信任、始终验证”原则。通过SDP技术封装自动售票机系统网络边界，对所有接入网络的设备（工控机、支付终端、服务器）进行身份认证与权限管控，仅授权设备可访问核心资源。动态分配访问权限，根据设备安全状态、用户操作场景实时调整，限制非法设备接入与权限滥用，防范中间人攻击、内网渗透等风险，保障内部专网通信安全。

2.3 系统安全加固技术

（1）可信执行环境（TEE）在支付模块的部署方案，将支付模块核心功能（密码输入、支付加密、数据校验）部署于TEE中，构建与系统主操作系统隔离的可信执行空间。TEE具备硬件级安全防护能力，可抵御恶意代码注入、内存读取等攻击，确保支付密码、银行卡信息等敏感数据在独立环境中处理与存储，不被外界窃取篡改。优化TEE与主系统的交互接口，保障支付流程流畅性，同时定期更新TEE固件，修复安全漏洞，提升支付模块安全性。（2）基于AI的异常行为检测，采用LSTM神经网络分析设备日志，实现对自动售票机系统异常行为的实时检测与预警。收集工控机运行日志、支付终端操作日志、网络传输日志等数据，通过LSTM神经网络训练异常检测模型，精准识别正常操作模式。当检测到固件篡改、恶意代码注入、异常数据传输等行为时，立即触发预警信号，并阻断异常操作，同时记录异常日志，为后续溯源提供支撑，提升系统对未知攻击的应对能力[3]。

2.4 应急响应与恢复技术

（1）区块链技术在审计日志不可篡改存储中的应用，将系统审计日志（操作记录、攻击痕迹、数据变更记录）上传至区块链网络，利用区块链去中心化、不可篡改、可追溯的特性，确保审计日志不被篡改、伪造。每个节点同步存储日志数据，即使部分节点遭受攻击，也可通过其他节点恢复完整日志，为攻击溯源、责任认定提供可靠依据，同时满足合规性审计要求。（2）自动化攻击溯源系统设计，结合SOAR（安全编排自动化与响应）技术，整合日志分析、漏洞扫描、威胁情报等功能，构建自动化攻击溯源系统。当系统遭受攻击时，SOAR技术自动触发应急响应流程，收集攻击相关数据，通过关联分析定位攻击源头、攻击路径与攻击手段，同时自动执行阻断、隔离等应急操作。生成详细的溯源报告，为后续系统加固提供指导，缩短应急响应时间，提升攻击处置效率[4]。

3 轨道交通自动售票机系统的信息安全防护体系设计与实现

3.1 总体架构设计

结合轨道交通自动售票机系统的架构特点与安全需求，构建基于分层防御模型的总体安全架构，实现从终端到云端的全流程、多层次防护，保障系统全生命周期安全稳定运行。分层防御模型涵盖三个核心层级，各层级协同联动、各司其职：终端安全层聚焦自动售票机本身，包括工控机、支付终端、读卡器等核心设备，通过硬件加固、软件防护实现终端自身安全；网络传输层针对车地通信、内部专网传输，采用加密传输、访问控制等技术，防范数据窃取、篡改与中间人攻击；云平台管理层负责统筹终端设备、网络资源的安全管控，实现日志审计、异常预警、应急调度等功能，形成“终端防御-网络隔离-云端管控”的闭环防护体系。

3.2 核心模块实现

（1）安全启动机制，基于UEFI Secure Boot技术实现固件验证，替代传统BIOS启动模式，从系统启动源头保障安全。在自动售票机工控机启动过程中，UEFI固件会对引导程序、操作系统内核、设备驱动等进行完整性校验，仅允许通过数字签名验证的合法程序运行，拒绝恶意篡改的固件与程序启动。同时，预留合法签名更新接口，定期更新固件签名列表，及时适配系统升级需求，有效防范固件篡改、恶意代码注入等攻击，确保系统启动过程安全可控。（2）动态令牌认证，将TOTP算法应用于运维人员登录认证，解决传统静态密码认证易泄露、易破解的问题，保障运维操作安全。运维人员登录售票机管理系统时，除输入账号密码外，还需通过专用认证设备生成动态令牌，令牌基于TOTP算法，结合时间戳与密钥实时生成，每30秒更新一次，且仅单次有效。系统后台同步验证令牌有效性，双重认证通过后方可授予运维权限，同时根据运维人员岗位分配最小权限，限制操作范围，防范越权操作与非法登录，保障系统运维安全[5]。

3.3 仿真实验环境搭建

（1）测试床设计，模拟AFC系统真实业务场景搭建实验测试床，还原自动售票机全业务流程。测试床包含模拟工控机、仿真支付终端、读卡器等硬件设备，搭建模拟车地通信的LTE/5G传输环境与内部专网，部署云平台管理节点，模拟票务购买、支付交易、数据传输、运维管理等真实业务操作，确保测试场景与实际应用高度一致，为后续防护效果测试提供可靠环境支撑。（2）攻击工具链构建，基于Metasploit框架进行定制化开发，构建适配自动售票机系统的攻击工具链。针对系统可能面临的固件篡改、恶意代码注入、中间人攻击等典型威胁，定制攻击模块与脚本，优化攻击流程，提升攻击工具的针对性与有效性。通过该工具链模拟各类恶意攻击，测试防护体系的防御能力与应急响应效率，为防护体系的优化完善提供数据支撑。

4 轨道交通自动售票机系统信息安全防护体系的实验验证与效果评估

4.1 测试环境与工具

（1）硬件环境，搭建由工控机、智能票务终端、模拟支付网关组成的硬件测试平台。工控机选用轨道交通专用型号，匹配自动售票机实际配置；智能票务终端模拟售票、支付全流程操作；模拟支付网关还原真实支付链路，用于测试支付信息传输的安全性与稳定性，整体硬件配置与现场AFC系统保持一致。（2）软件环境，工控机与票务终端安装定制化Linux发行版，精简冗余功能、关闭无用端口，适配售票机轻量化运行需求；部署Wireshark抓包分析工具，实时捕获网络传输数据，用于检测数据加密效果与攻击行为痕迹；同时搭配漏洞扫描、性能监测工具，辅助完成防护效果与性能影响测试。

4.2 防护效果验证

（1）抗中间人攻击测试，聚焦TLS1.3协议性能对比，分别测试采用TLS1.3与传统TLS1.2协议在数据传输中的抗攻击能力，记录攻击拦截成功率、数据传输完整性。实验表明，TLS1.3协议可有效抵御中间人窃听、篡改攻击，拦截成功率达100%，且传输延迟更低，适配车地高频数据交互场景。（2）恶意代码检测率，对比传统签名检测与AI行为分析两种方式的恶意代码检测效果，选取常见恶意代码样本进行测试。结果显示，传统签名检测率仅为78%，而AI行为分析检测率提升至99%，可有效识别未知恶意代码，防护效果更优。

4.3 性能影响分析

（1）加密算法对交易响应时间的影响，开展＜200ms阈值测试，分别测试启用SM4动态加密与未启用加密时的交易响应时间。实验显示，启用加密算法后，平均交易响应时间为156ms，远低于200ms阈值，不会影响用户购票体验。（2）异常检测模块的资源占用率，监测AI异常检测模块运行时的CPU、内存占用情况，测试结果显示，模块运行时CPU占用率平均为3.2%，内存占用率平均为2.8%，均低于5%的预设阈值，不会造成系统资源冗余消耗，保障系统稳定运行。

结束语

轨道交通自动售票机系统信息安全防护研究，通过剖析系统安全威胁，针对性提出数据动态加密、量子通信、AI异常检测等创新防护技术，构建起涵盖终端、网络、云端的立体化防护体系。实验验证表明，该体系可有效抵御各类攻击，保障数据安全与系统稳定运行。未来，需持续跟进技术发展，优化防护策略，为轨道交通智能化运营筑牢安全基石。

参考文献

[1]王明.轨道交通通信网络安全防护技术研究[J].交通科技与经济,2023,(4):56-60.

[2]李华,张强.基于加密技术的轨道交通通信网络安全策略[J].铁道通信信号,2022,(2):45-48.

[3]王成涛.城市轨道交通的车站自动售检票系统分析[J].电子技术,2022,51(04):50-51.

[4]杨承东,刘洋.智慧城轨自动售检票系统的技术发展趋势[J].都市快轨交通,2021,34(01):52-56.

[5]何靓俊,虞腾飞,唐微曙.基于城市轨道交通的云数据中心信息安全研究[J].中国高新科技,2023,(11):121-123.