

doi: 10.3969/j.issn.1672-6073.2019.05.022

NFC 技术在 AFC 系统中的 安全研究

陶 克¹, 程玉柱²

(1. 福州地铁集团有限公司, 福州 350009; 2. 长沙民政职业技术学院软件学院, 长沙 410004)

摘 要: 介绍 NFC 技术在地铁票务中的典型应用。NFC 技术在天然保密性、双向鉴权和对原 AFC 系统改动少等方面具有一定的优势, 但其同时在通信、设备、软件和所在环境方面也具有一定的安全隐患。分析 NFC 在内部传输、软硬件及环境方面的安全威胁, 提出手机端软件技术改进方法和后台使用数据风险监控三级预警方法, 采用双重安全机制以规避安全威胁, 确保 NFC 技术在地铁应用中的收益安全, 尽可能地避免收益漏洞。

关键词: 信息安全; NFC; AFC; 手机支付

中图分类号: U231

文献标志码: A

文章编号: 1672-6073(2019)05-0133-05

Security of NFC Technology in AFC System

TAO Ke¹, CHENG Yuzhu²(1. Fuzhou Metro Group Co., Ltd., Fuzhou 350009;
2. Software School, Changsha Social Work College, Changsha 410004)

Abstract: This paper introduces a remarkable application of near-field communication (NFC) technology in subway ticketing. NFC technology has certain advantages in natural security, bidirectional authentication, and causes less change to the original automated fare collection (AFC) system. However, it has some security risks in communication, equipment, software, and environment. This paper analyzes the security threats of NFC in the aspects of internal transmission, software/hardware, and environment, and proposes an improvement method in software technology and a three level warning method for data risk monitoring in the background, and uses double security mechanism to avoid security threats while ensuring that NFC technology gains revenue in subway applications and avoids loss of revenue.

Keywords: information safety; NFC; AFC; mobile payment

随着“互联网+”与传统行业地铁票务的深度融合, 推动了票务经济形态的不断更新, 给传统自动售检票系统提供了创新、改革、前进的空间。地铁发卡权的获得, 手机票的完美实现, 让电子票卡做加法, 实体票卡做减法, 在方便用户出行的同时减少了地铁公司整体的运营开支^[1]。在地铁已实现了 NFC 技术应

用的全流程: 空中发卡、充值(含实体卡)、支付、查询、锁卡/解锁等功能。虽然 NFC 技术具有天然的保密性, 双向鉴权和数据加密等安全手段, 是二维码单向通信、容易被复制、信息量有限所无法比拟的。但 NFC 技术安全性也受到人们的高度重视, 其安全性仍受到诸多因素的威胁和挑战。

1 NFC 技术在地铁的应用

NFC 技术(near field communication, 近距离通信技术)在地铁进行线下支付时不需要启动相关 App, 也无需在联网的环境中, 只需在靠近读卡器的读写区域内进行相应密钥验证和 TAC(交易验证码)计算即可完成交易。NFC 在手机上使用支持模拟卡、模拟读卡

收稿日期: 2018-05-31 修回日期: 2018-06-26

第一作者: 陶克, 男, 工学博士, 高级工程师, 从事智能交通、信息安全的研究, keke100@hotmail.com

通信作者: 程玉柱, 男, 工学博士, 副教授, 从事信息安全的研究, vogue21ct@qq.com

基金项目: 湖南省教育厅科学研究项目(17B022)

器和点对点3种基本模式^[2]。这3种基本模式可以用于地铁不同的场景,而模拟卡和模拟读卡器模式可以与AFC系统中刷卡和充值业务完美结合。

1.1 读卡器模式(reader/writer mode)

在NFC技术的读卡器模式中,NFC设备主要被用于非接触式读取,发送固定频率磁场给电子钱包写入特定的信息,此时的读卡器模式主要完成对电子钱包信息的读写,而且以这种方式工作的NFC设备可实现主从模式之间的通信^[3]。通过该模式在联网环境中获取充值密钥和TAC计算机制,可以应用于地铁手机票卡或地铁发行的实体卡进行读写充值操作。

1.2 非接触卡模拟模式(card emulation mode)

NFC设备仿真卡的模式是将NFC设备等同采用传统射频识别技术的IC卡,可以完成现有IC卡的工作,此时的NFC设备具有了智能卡的所有功能,可以在短距离内实现安全加密的非接触式信息交换^[4]。与传统射频技术IC卡不同的是,该非接触卡模拟卡模式可在基本无源感知方式下完成,当NFC芯片作为被读应用时,功耗非常小,并且是瞬间读取,在刚自动关机不能打电话情况下也能读取。

1.3 点对点模式(peer to peer mode)

NFC技术在点对点模式下将通过两个近距离的NFC设备之间建立快速通信连接,即可进行简单的数据交换,如发送图片、同步设备文件等,最远距离为10 cm,传输速度和建立通信时间都比蓝牙和红外快,这种通信可以是双向或者是单向^[5]。

2 NFC技术在地铁中应用的优点

1) NFC手机使用模拟卡模式如CPU卡双向通信,实现手机票卡在地铁的应用,且无需在闸机前打开App软件就能过闸。使用App能在线进行空中发卡、充值、查询最近乘车和充值交易记录^[6]。完全实现了手机票卡的一体化,显示出NFC技术的优越性,又能可视化地在手机上查询票卡交易的明细和余额,比App展现二维码单向通信过闸更快捷、高效。

2) NFC手机模拟读卡器模式可以通过App,实现在线获取相应密钥和TAC计算机制进行空中发卡和充值(含本手机卡和地铁发行实体卡),而节省去各站点排队办理业务的时间。

3) NFC手机票卡的增加,可以直接按照地铁方票卡结构进行设计和扩充应用,使用13.56 MHz频率通信AFC系统不需要增加任何硬件,对原有系统改变最

少,只增加新票卡种类参数或原票卡种类中规划号段区分,增加系统报表展示和清分系统少量区分修改。

4) NFC手机支付系统与原有AFC系统对接时,不影响地铁既有AFC系统的运行安全,不对既有的票卡发行、制作规则造成影响。NFC手机票卡相对独立的发卡系统,不需要对既有发卡系统进行改造。

5) NFC手机票卡的配发是电信运营商或厂家负责,与地铁系统中已有的票卡配发方式剥离,不会对现有票务规则带来冲击。地铁运营方完全不需要参与手机票卡的采购、配发过程,只需在清分系统内增加相应票卡业务处理方式,并不需要牵涉到其他单位或部门回收等业务,对现有地铁票务运作体系不造成任何影响,将减少诸多中间环节和客观因素影响,可直接实现量产。

3 NFC的安全性分析

由于手机归属权在用户手中,而且NFC系统和应用包含敏感的个人隐私、存储密钥、支付信息等,其安全性非常重要。图1显示了NFC的安全威胁源,其主要包括通信安全、硬件设备安全、软件系统安全和环境安全4个部分。

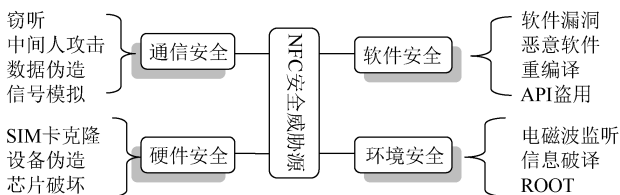


图1 NFC安全威胁源

Fig. 1 NFC security threat source

3.1 通信安全

当NFC手机在进行刷卡支付和充值的时候,设备将在仿真卡或读写器的模式下工作,NFC设备间将进行一系列通信和验证,而且IC卡信息传入到NFC射频器期间,都可以窃听NFC手机支付的无线通信接口,因为在两个设备建立通信之后,有可能电子钱包内部的数据在交互过程中不是一直处于密文状态,这导致数据在该层交互时有被盗取的可能,从而形成数据泄露^[7]。

还有一种可能是通过中间人方式采取第三方会话,伪造数据利用NFC的接口,采取信号模拟对NFC手机支付通信设备之间数据进行模拟,直至接收到反馈或应答的可用数据,导致数据被窃取。其主要威胁是数据信息传输过程中的干扰,从而导致真实数据的

泄露。

3.2 硬件设备安全

在 NFC 手机支付中 SE(secure element, 安全元件)安全芯片对电子钱包信息的保护发挥着至关重要的作用,是存储密钥、敏感数据、加密运算等操作的安全芯片。现阶段 SE 安全芯片设置有 3 种模式:为手机中的设置在 SD 卡中的 SWP-SD(singlewire protocol, 单线连接方案)模式、设置在 SIM 卡中 SWP-SIM 模式和手机全终端模式^[8]。人为故意更新、置换或删除 SE 模块,以及对安全密钥、机密隐私信息模块损坏和替换 SE 模块的完整性问题。

特别在使用 SWP-SD 模式外部 SE 模块的 NFC 解决方案中,恶意对承载 NFC 手机支付应用中电子钱包使用的 SE 模块安全进行逐步替换。一旦成功替换已验证 SE 模块,有可能导致身份冒用以及各种未经授权的侵权行为,盗取用户的系统关键数据或个人唯一标识,最终导致未经授权的 NFC 手机支付实现^[9]。

3.3 软件系统安全

在 NFC 手机系统上捆绑恶意程序,将对用户的交易内容劫持、软件捆绑、监视用户支付流、恶意跳转等来侵犯用户隐私,剥夺用户选择权和知情权;也可在用户不知情的情况下,向已被认证过的会话中 SE 模块使用一些有问题的根证书,将产生错误的信任关系,从而到达控制的目的。

软件系统破坏或者入侵关键就是系统漏洞,扫描软件系统漏洞找出攻击目标,从而达到从后门进入系统或者访问未授权的资源等。提前发现并修补 NFC 安全漏洞是系统和应用安全的重要保障,而且 NFC 新技术方面软件存在有安全漏洞经验不足,通过逆向工程技术或重打包,找出漏洞能够获取应用程序的安全数据、用户信息,并植入恶意程序,严重危害到整体软件程序的安全^[10]。

3.4 环境安全

当 NFC 手机使用读写器功能的射频通信链路时将可面临被窃听,ISO/IEC 18092 标准规定了 NFC 数据链路是无线方式。因此基于开放环境下的无线数据传输将有被盗取的可能,将威胁到用户 ID、支付信息等非常敏感的内容。

用户可以对手机进行 Root 操作,通过 Root 后可以访问手机中所有储存的信息,包括各种支付凭证等的关键信息,这也让恶意软件有了获取敏感数据的渠

道,而且可以被恶意用户使用获取的信息去进行伪卡交易。

4 NFC 手机支付安全问题解决方案

NFC 手机支付安全问题可以采取两个方面进行控制:前端技术预防和后台数据风险监控预警。前端技术预防方法将着重从 NFC 手机的技术环节入手,通过采取密文、身份验证、访问控制等一系列必要技术手段和方法去除安全威胁。因 NFC 手机在用户手中,很难进行全面的把控,所以有必要采取后台数据风险监控预警,处理地铁各场景交易过程中上传的交易数据,并进行全流程分析监控。

4.1 对于前端技术预防方案

1) 安全模块采取的保障机制。针对手机 SE 安全模块,可以使用访问控制机制,如个人密码的错误次数限制和数字签名的周期生命控制;对于密钥的恢复和备份条件,防止密钥失效或遗失后加密程序无法正常使用;硬件系统需采取完整性监控以防止运行时替换发生;所有传输和存储过程中采取密文形式;严禁下载无签名、无验证来源方的软件并运行;避免数据重放使用,所有交易记录都须打上时间戳。在 SWP-SIM 模式中,使用 SIM 卡的自毁保护机制,在 3 次密钥不正确将“烧卡”,使得该模式下 SIM 信息不可复制。

2) 基带处理器的安全机制。采取具有 NFC 功能的手机,在基带处理器中能与 SE 交互的 API 函数接口,以及基带处理器为 NFC 相关应用提供运行环境,然而有些应用程序可在没有用户知晓的情况下就被调用了。而且基带能与安全模块相互认证,提供人机界面以及 SIM 卡的传输和应用程序之间调用接口。因此,在手机的不同安全域中,使用不同可信度的应用程序;严格划分不同的安全域提高其安全性能。

3) NFC 芯片的安全机制。NFC 电子钱包在生成时将写入一个唯一 ID,并限制该 ID 不可被复制,使用加密算法利用 ID 值计算出一个密文,并将其存储在电子钱包的特定区域,当 NFC 设备每次进行通信时,将校验匹配对该密文的值,区分电子钱包的真伪,实现 NFC 技术的安全通信。也让用户能自主开关 NFC 模块功能,以防止 NFC 芯片被他人随意读取。

4) 使用交易验证安全机制。针对 NFC 手机所产生的所有充值(含对实体卡)或者消费交易记录,都根据地铁密钥组中分散因子统一鉴权,再利用其 TAC 计算机制,每条交易记录传回 AFC 系统后进行统一校验,保证每条交易不可篡改、不可伪造。交易文件在

传输中也使用校验机制,保证文件在传输中的完整性。交易文件格式可使用地铁现有交易文件格式,对原有系统影响减少到最低。

5) 建立安全应用场景。NFC 手机在软件使用时对其安全性进行检查,对于已经 Root 的手机,提示安全风险并限制最高金额,控制其风险;对于空中充值应用,必须采取在线验证机制充值,保证安全可控。

4.2 后台数据风险预警机制

根据地铁业务数据特点,将实时监控分析各终端设备上传的每笔交易数据入库情况,分析交易数据并进行分析监控预警,如图2所示。以票卡的逻辑卡号为主关键字,根据各终端上传入库的票卡交易数据中逻辑卡号,实时比对入库数据中逻辑卡号交易记录中记录的余额字段,以每笔出站交易的余额是递减,且不超过线网最高票价为正常交易数据。

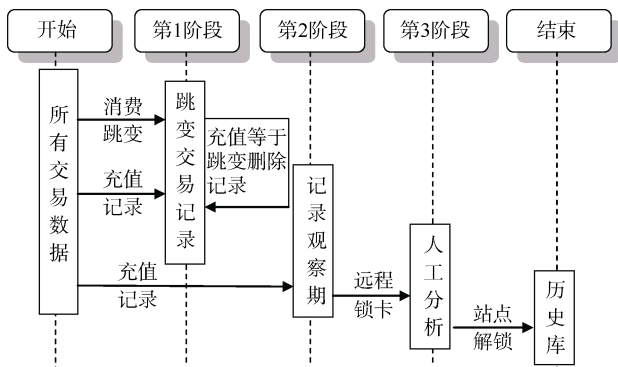


图2 数据分析监控预警

Fig. 2 Data analysis monitoring and warning

第1阶段预警:当发现比对数据有反向跳变(增长)时,将该条交易记录列入第1阶段预警表进行记录,并检查在递减的最后一笔交易,至跳变(增长)记录时间段中是否有该票卡的充值记录。当查询有充值记录时,而且上传入库累计充值记录等于跳变(增长)值时,删除第1预警阶段该票卡记录;如果充值记录不等于跳变(增长)值时,该票卡记录计入第2阶段预警表。

第2阶段预警:预警表数据根据地铁公司 AFC 设备检修或维护周期,设置一段时间观察期,实时查询上传入库充值记录;若在观察期内查询到有递减的最后一笔交易,至跳变(增长)记录时间段中的充值记录累计值,等于跳变(增长)值时,删除第1和第2阶段该票卡记录;若在观察期内未能查询到充值记录等于跳变(增长)值,则该票卡记录计入第3阶段预警表。

第3阶段预警:预警表的数据将作为人工分析

的重点,如果一个票卡有多条记录在第3阶段预警表里,将进行远程锁手机票卡行为,待持手机用户去地铁站点(或指定点)进行解锁,解锁后预警表记录移入历史表备查。对于该阶段用户因有多次余额增加,将进行重点分析盯控,防范有可能风险的出现和漏洞的补查。

5 结语

综上所述,随着“互联网+”票务新时代的来临,NFC 凭借自身具有的良好应用功能,克服了传统的 AFC 系统购票模式暴露出的单程票流失率高,终端设备纸币、硬币模块贵及故障率高,零币要求多等诸多问题,但新型技术引进也带来了一定业务的安全风险,因此提升前端管理和技术手段、后台数据分析以及地铁自身对应提高风险监控能力,必将成为 AFC 系统发展的新研究方向。

参考文献

- [1] 梁云杰. 基于 NFC 技术的一种安全手机支付方案研究[J]. 河南科技学院学报(自然科学版), 2017, 44(6): 63-68.
LIANG Yunjie. The scheme of safe mobile payment based on NFC technology[J]. Journal of Henan institute of science and technology (natural sciences edition), 2017, 44(6): 63-68.
- [2] VEDAT Coskun, BUSRA Ozdenizci, KEREM Ok. A survey on near field communication (NFC) technology[J]. Wireless personal communications, 2013, 71(3): 2259-2294.
- [3] 王志强, 刘奇旭, 张玉清. Android 平台 NFC 应用漏洞挖掘技术研究[J]. 通信学报, 2014, 35(Z2): 117-123.
WANG Zhiqiang, LIU Qixu, ZHANG Yuqing. Research of discovering vulnerabilities of NFC applications on Android platform[J]. Journal on communications, 2014, 35(Z2): 117-123.
- [4] NE Tabet, MA Ayu. Analyzing the security of NFC based payment systems[J]. International conference on informatics & computing, 2017: 169-174.
- [5] 杨妍玲. 基于 NFC 技术的手机移动支付安全应用研究[J]. 现代计算机(专业版), 2015(20): 56-60.
YANG Yanling. Research on the application of mobile payment security based on NFC technology[J]. Modern computer, 2015(20): 56-60.
- [6] 张亚飞, 张博, 贺文娜, 等. 基于 TEE 的 NFC 卡模拟安全方案研究[J]. 北京电子科技学院学报, 2014, 22(4): 48-53.

- ZHANG Yafei, ZHANG Bo, HE Wenna, et al. Research on TEE-based security scheme for NFC card emulation[J]. Journal of Beijing electronic science and technology institute, 2014, 22(4): 48-53.
- [7] 王影. 基于 NFC 的移动支付安全技术研究[D]. 广州: 广东工业大学, 2016.
- WANG Ying. Research of mobile payment security based on NFC[D]. Guangdong University of Technology, 2016.
- [8] 吴宇婷, 刘瑛祺. 基于 NFC 技术的移动支付系统实现方案[J]. 铁路计算机应用, 2017, 26(8): 43-46.
- WU Yuting, LIU Yingqi. Implementation scheme of mobile payment system based on NFC technology[J]. Railway computer application, 2017, 26(8): 43-46.
- [9] KAI Fan, PANFEI Song, et al. NFC secure payment and verification scheme with CS E-ticket[J]. Security and communication networks, 2017, 4796373: 1-4796373: 9.
- [10] M Al-Tamimi, A Al-Haj. Online security protocol for NFC mobile payment applications[J]. International conference on information technology, 2017: 827-832.
- (编辑: 王艳菊)

(上接第 116 页)

参考文献

- [1] 张钰梅. 城市轨道交通路网客流拥挤传播特性及疏解策略研究[D]. 北京: 北京交通大学, 2015.
- [2] 张仁鑫. 盾构管片拼装质量可视化检测技术研究[D]. 武汉: 华中科技大学, 2013.
- [3] 郭铜. 地铁隧道盾构法施工质量控制重点及措施[J]. 科技视界, 2015(1): 163.
- [4] 李云丽. 盾构隧道施工过程中管片结构受力特征研究[D]. 北京: 北京交通大学, 2008.
- [5] 丁烈云, 周诚, 周迎, 等. 一种基于图像识别的管片拼装质量的智能检测系统及其检测方法: CN102589443 A[D]. 2012-07-18.
- [6] MO HH, CHEN JS. Study on inner force and dislocation of segments caused by shield machine attitude[J]. Tunnelling & underground space technology, 2008, 23(3): 281-291.
- [7] WANG Z, WANG L, LI L, et al. Failure mechanism of tunnel lining joints and bolts with uneven longitudinal ground settlement[J]. Tunnelling & underground space technology, 2014, 40(1): 300-308.
- [8] 刘云广. 基于地面三维激光扫描技术的变形监测数据处理[D]. 北京: 北京建筑大学, 2013.
- [9] SEO D J, CHOO J. Development of cross section management system in tunnel using terrestrial laser scanning technique. 2008.
- [10] HAN JY, GUO J, JIANG YS. Monitoring tunnel profile by means of multi-epoch dispersed 3-D LiDAR point clouds[J]. Tunnelling & underground space technology, 2013, 33(1): 186-192.
- [11] GOSLIGA RV, LINDENBERGH R, PFEIFER N. Deformation analysis of a bored tunnel by means of terrestrial laser scanning[J]. IASPRS, 2006, 167-172.
- [12] STIROS S, KONTOGIANNI V. Mean deformation tensor and mean deformation ellipse of an excavated tunnel section[J]. International journal of rock mechanics & mining sciences, 2009, 46(8): 1306-1314.
- [13] 官云兰, 程效军, 张明, 等. 三维激光扫描数据配准方法[J]. 工程勘察, 2008(1): 53-57.
- [14] XIAO C, MIAO Y, LIU S, et al. A dynamic balanced flow for filtering point-sampled geometry[J]. The visual computer, 2006, 22(3): 210-219.
- [15] FLEISHMAN S, COHEN-Or D. Robust moving least-squares fitting with sharp features[J]. Acm transactions on graphics, 2005, 24(3): 544-552.
- [16] DEY TK, SUN J. An adaptive MLS surface for reconstruction with guarantees[C]. Eurographics symposium on geometry processing, 2005: 43.
- [17] LIPMAN Y, COHEN-Or D, LEVIN D. Data-dependent MLS for faithful surface approximation[C]. Eurographics Symposium on Geometry Processing, 2007: 59-67.
- [18] 张巧英, 陈浩, 朱爽. 密度聚类算法在连续分布点云去噪中的应用[J]. 地理空间信息, 2011, 9(6): 101-104.
- [19] 琚俏俏, 程效军, 徐工. 基于椭圆拟合的隧道点云去噪方法. 工程勘察, 2014(9): 69-72.
- (编辑: 郝京红)