近场通信技术的安全研究进展与发展趋势

张玉清[1),3)] 王志强[2),3)] 刘奇旭[1)] 娄嘉鹏[2)] 姚 栋[2)]

[1)](中国科学院大学国家计算机网络入侵防范中心 北京 101408)

[2)](北京电子科技学院 北京 100070)

[3)](西安电子科技大学综合业务网理论及关键技术国家重点实验室 西安 710071)

摘 要 随着移动互联网和移动支付的发展,NFC 技术因其天然的安全特性和便利性,成为运营商、银行、厂商等热捧的对象.由于涉及到移动支付和敏感信息的传输,该技术也受到安全研究人员和攻击者的广泛关注.虽然国内外安全专家和学者对 NFC 安全问题已进行了一定的研究,但目前还没有详细和全面介绍最新安全研究成果的论文.为解决此问题,该文分析和总结了国内外最新的研究成果,并对 NFC 安全问题未来的研究方向进行了展望.首先,介绍了 NFC 技术的基本特性、通信过程、协议栈、工作模式等,分析了该技术面临的安全威胁,包括通信安全、安全漏洞、安全元件、恶意软件、网络钓鱼等内容.然后,通过分析相关研究工作,总结了 NFC 技术的安全研究现状.最后,从安全威胁的角度,对未来的研究方向进行展望,在安全信道、漏洞挖掘、安全元件、恶意软件检测、恶意内容检测、移动支付等方面分析了研究内容和研究方法.

关键词 近场通信技术;安全威胁;研究进展;发展趋势;网络安全;信息安全;网络空间安全

中图法分类号 TP309 **DOI 号** 10.11897/SP.J.1016.2016.01190

Research Progress and Trends on the Security of Near Field Communication

ZHANG Yu-Qing[1),3)] WANG Zhi-Qiang[2),3)] LIU Qi-Xu[1)] LOU Jia-Peng[2)] YAO Dong[2)]

[1)](*National Computer Network Intrusion Protection Center, University of Chinese Academy of Sciences, Beijing* 101408)

[2)](*Beijing Electronic Science and Technology Institute, Beijing* 100070)

[3)](*State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an* 710071)

Abstract With the development of mobile internet and mobile payment, NFC (Near Field Communication) attracts service providers, banks and manufacturers' attention because its natural safety properties and convenience. For the reason that NFC involves mobile payment and sensitivity information transmission, it has also gained security researchers and attackers' increasing attention. Although many work on NFC security has been studied currently by experts and scholars at home and abroad, there is no a thorough and detailed analysis on current research progress and development trends of NFC security. To solve this problem, the paper analyzes and summarizes the latest overseas and domestic research results, and prospects a further research on NFC security. First, the paper introduces NFC's basic features, communication process, protocol stack, operation mode and so on, analyzes security threats faced by NFC, including communication security, security vulnerabilities, secure element, malware, phishing and so forth. Second, the paper summarizes the research status and progress of NFC security by analyzing the related research work. Finally, from the point of view of security threats, the future research directions

收稿日期:2015-01-30;在线出版日期:2015-11-13.本课题得到国家自然科学基金(61303239,61272481,61572460)、国家发展和改革委员会 2011 年信息安全专项项目(发改办高技[2012]1424)资助.**张玉清**,男,1966 年生,教授,博士生导师,主要研究领域为密码学、信息安全和网络安全.E-mail:zhangyq@ucas.ac.cn.**王志强**,男,1985 年生,博士,主要研究方向为系统安全、网络安全.**刘奇旭**,男,1984 年生,博士,讲师,主要研究方向为漏洞挖掘、漏洞评估、应急响应.**娄嘉鹏**,男,1977 年生,硕士,主要研究方向为系统安全、网络安全.**姚 栋**,男,1975 年生,硕士,主要研究方向为信息安全.

cover research contents and methods about secure channels, vulnerability discovering, secure element, malware detecting, malicious content detecting, mobile payment and so on.

Keywords　near field communication; security threat; research progress; development trends; network security; information security; cyberspace security

1　引　言

NFC(Near Field Communication)技术是一种近距离的双向高频无线通信技术,能够在移动终端、智能标签(Tag)等设备间进行非接触式数据交换[1-3].NFC 技术具有通信距离短、一次只和一台设备连接、硬件安全模块加密等特点,具有较好的保密性和安全性.

由于 NFC 技术天然的保密性和安全性,所以该技术受到移动支付厂商、运营商、银行等的重视和推广.当前主流的移动支付[4]包括运营商计费、手机外设支付[5]、NFC 支付[6-7]、图像识别支付[8]、条形码/二维码支付[9-12]、生物特征识别支付[13-15]、超声波支付[16]等支付方式.运营商计费是指用户通过短信等方式对支付的行为进行授权,运营商处理用户的支付行为并从用户的账户中扣除相应的费用.例如,用户通过短信代码购买网络流量,运营商根据价格从用户的手机号账户中扣除流量费用.该支付方式的支付过程比较简单和直接,是移动支付最初的支付方式,但其支付范围和扣费方式具有一定的局限性,且安全性较差.手机外设支付是指通过插入手机音频、基座等接口的硬件设备读取银行卡获取账号信息,并完成支付的过程.比较典型的支付例子包括 Square、拉卡拉、盒子支付等.该支付方式通过硬件读取银行卡信息,安全性比较高,应用的范围比较广,局限性较小,但该方式需要用户和商家配置读卡的硬件设备,增大了支付的硬件成本.NFC 支付是指通过移动终端的 NFC 模块读取银行卡获取账户信息来完成支付的过程.该支付方式具有良好的保密性和安全性,且当 NFC 手机没电时也能完成支付.因此,该方式是目前比较受推崇的一种支付手段.图像识别支付是指通过图像识别技术扫描银行卡等卡片信息来获取用户的账号信息完成支付的过程.该支付方式受识别过程的环境影响较大,且无法保证卡片的安全性和真实性,具有很大的安全隐患.条形码/二维码支付是指通过移动终端扫描条形码/二维码获取商品信息,并通过银行卡、电子钱包等手段完成支付的过程.该支付方式可以与手机外设支付、NFC 支付、图像识别支付等结合,共同完成支付过程.该支付方式易于实现,支付便捷,但容易受到虚假或恶意条形码/二维码的攻击,安全性较差.生物特征识别支付是指以人脸、虹膜、指纹等生物特征作为安全校验手段,来完成支付的过程.生物特征具有唯一性,能够保证支付过程的安全性,但某些人、群体的生物特征难成像,识别困难,且容易受到"复制生物特征"的安全威胁.例如,通过整容手术可实现相似的面部特征,通过复制指纹痕迹可重现用户指纹等.超声波支付是指通过手机客户端发出超声波,终端设备获取声波并转化为支付交易号,进而通过订单支付完成交易的过程.该支付方式需要依赖网络信号的质量,这是超声波支付的先天缺点,使得用户体验大打折扣,且需要增加一定的硬件成本.以上简单介绍了几种主流的移动支付手段,从安全性、硬件成本、用户体验等方面综合分析,NFC 支付是未来最有前景的支付手段之一.

随着物联网和电子商务的发展,NFC 技术被迅速推广并应用于移动终端等支持 NFC 技术的设备上.根据研究公司 IHS Technology 的统计报告①,在 2013 年的智能手机市场上,配备 NFC 功能的智能手机出货量从 2012 年的 1.2 亿台上升到 2.75 亿台,增幅达到 128%.根据 IHS 的统计报告,2014 年 NFC 智能手机出货量在 2013 年的基础上增长 50%多,达到 4.44 亿台;总体而言,到 2018 年,该类智能手机出货量将在 2013 年的基础上增长 325%,达到 12 亿台.这些数据从侧面反映了 NFC 技术在移动领域逐渐被推广和应用.

虽然 NFC 技术具有天然的保密性和安全性,但其安全性仍受到很多威胁和挑战.2012 年 2 月,zvelo 公司发现一个谷歌电子钱包 NFC 支付系统的漏洞,通过该漏洞可暴力获取 PIN 码盗刷用户的信用卡,这个漏洞需要 Root 权限且未设置锁屏密码②.随后,The Smartphone Champ 又发现了不需

① NFC-Enabled Cellphone Shipments to Soar Fourfold in Next Five Years [EB/OL]. http://press.ihs.com/press-release/design-supply-chain/nfc-enabled-cellphone-shipments-soar-fourfold-next-five-years, 2015,1,9

② Google Wallet Security: PIN Exposure Vulnerability [EB/OL]. https://zve lo.com/google-wallet-security-pin-exposure-vulnerability/, 2015,1,9

Root 权限即可获取 PIN 码的漏洞,通过在设置菜单清空数据即可设置新的 PIN 码①. 2012 年 7 月,在 Blackhat 大会上,Accuvant 实验室首席顾问 Miller 利用 Android 操作系统的 NFC 漏洞,读取并自动开启网址下载恶意软件,来入侵移动设备[17]. 同年 9 月,Intrepidus 公司的 Corey Benninger 和 Max Sobell 在 EUSecWest 会议②上利用 NFC 支付漏洞实现零花费的刷卡,该漏洞波及波士顿、费城、芝加哥等多个城市的地铁系统. 2014 年,"NFC 手机能够轻松读取银行卡信息"的新闻迅速传播,引发了人们对 NFC 技术的担忧③. 虽然读取的银行卡信息不能影响银行卡的交易安全,但在一定程度上造成了个人信息的泄露.

随着 NFC 技术的推广和应用,尤其在移动支付领域,NFC 安全问题越来越受关注,国内外已经逐步开始对 NFC 安全问题进行深入的研究. 不管从理论还是实践的角度,国内外学者提出了各种攻击向量、防御措施和解决方案,取得了很多研究成果. 然而,目前还没有详细而全面介绍这些最新研究成果的综述论文. 为了深入理解 NFC 技术的原理、面临的安全威胁、防御方案及未来安全研究发展趋势,并掌握国内外研究的新动向,阐述和总结 NFC 技术及安全研究的发展趋势具有重要的意义.

本文第 2 节介绍 NFC 协议栈和工作模式技术;第 3 节介绍 NFC 技术面临的安全威胁;第 4 节介绍 NFC 安全研究现状;第 5 节分析未来的研究方向;最后是结束语.

2 NFC 协议栈和工作模式

2.1 通信过程和基本设备

为了更好地描述 NFC 协议栈和工作模式,首先简单介绍下 NFC 的通信过程和基本设备. NFC 通信是指 NFC 设备之间或 NFC 设备与 NFC 标签之间的数据传输[18]. 其中,NFC 设备是指 NFC 通信的读写设备和操作对象,可作为通信的发起者(Initiator)或目标(Target)④,包括 NFC 读写器和 NFC 电子标签. NFC 读写器包括 NFC 控制器(NFC Controller)、主控制器(Host Controller)、安全元件(Secure Element)和天线,如图 1 所示. NFC 控制器,也称 NFC 芯片,负责将数字信号转换为射频信号,并通过 13.56 MHz 天线发送;同时负责接收射频信号,并将其转换为数字信号,与主控制器和安全元件进行通信. 主控制器,负责实现对 NFC 控制器的控制和操作以及与安全元件之间通过私有接口进行数据交互. 安全元件,用于存储敏感数据,例如密钥、余额等,通过 NFC 控制器与外界设备进行通信,保证数据存储和交易过程的安全性. 天线,通过无线接口与 NFC 控制器进行通信,实现 13.56 MHz 射频信号的发射与接收. 此外,NFC 电子标签是存储数据的 IC 卡,能够被 NFC 读写设备读取,可作为通信的目标(Target).

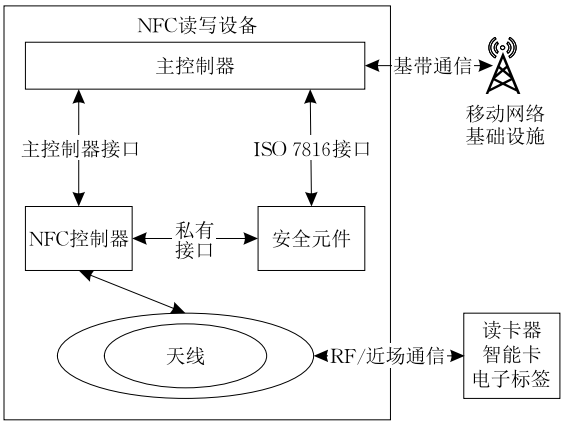

图 1 NFC 通信架构[7,19]

2.2 协议栈

NFC 是在 RFID 的基础上演变而来的,其协议规范也是基于 RFID 的众多标准制定和扩展的,可分为物理层(Physical Layer)、数据链路层(Data Link Layer)、协议层(Protocol Layer)和应用层(Application Layer)[17].

物理层,是 NFC 协议参考模型的最底层,它包括物理通信媒介及其物理特性,该层主要的作用是产生并检测磁场以便发送和接收携带数据的信号,为上层提供一个通信媒介以及它们的机械、电气、功能和规程特性. 例如邻近集成电路卡(Proximity Integrated Circuit Card,PICC)特性、天线、交变磁场、工作频率、输出功率等. 物理层的协议主要有 ISO 14443 A-1/ISO 18092、ISO 14443 B-1、Felica JIS X6319-4/ISO 18092⑤ 等,其中 NFC A、NFC B 和 NFC F 是

① Google Wallet Security Vulnerability Demonstrated[EB/OL]. http://www.youtube.com/watch?v=Rh1ytHrhj2E, 2015, 1, 9

② NFC for Free Rides and Rooms (on your phone)[EB/OL]. http://media.risky.biz/EUSecWest-SoBenn-Transit2012-Preview.pdf, 2015, 1, 9

③ NFC 手机真的可以轻松读取银行卡信息吗?[EB/OL]. http://www.zhihu.com/question/24106690, 2015, 1, 9

④ Introduction to NFC [EB/OL]. http://www.adafruit.com/datasheets/Introduction_to_NFC_v1_0_en.pdf, 2015, 1, 9

⑤ Near Field Communication-Interface and Protocol (NFCIP-1)[EB/OL]. http://www.ecma-international.org/publications/files/ECMA-ST/Ecma-340.pdf, 2015, 1, 9

指 NFC Tag 的 3 种协议，分别代表遵循 ISO 14443 Type A、ISO 14443 Type B 和 ISO 18092(JIS X 6319-4)标准的协议，三者的主要区别在于所关注的调制方式、编码方案和协议初始化程序不同.

数据链路层可分为两层：媒体接入控制层(Media Access Control)和逻辑链路控制层(Logical Link Control). 媒体接入控制层，主要负责控制与连接物理层的物理介质，描述了工作频率、磁场强度、不同设备之间的通信信号调制和解调等特性，代表协议主要有 ISO 14443 A-2/ISO 18092、ISO 14443 B-2、Felica JIS X6319-4/ISO 18092 等. 逻辑链路控制层，主要定义了磁场内轮询、帧格式、命令的请求和应答、冲突检测机制、通信链路初始化等，与 LLC 层一起控制协议层与物理层之间的通信，代表协议主要有 ISO 14443 A-3/ISO 18092、ISO 14443 B-3、Felica JIS X6319-4/ISO 18092 等.

协议层，该层类似于 OSI 七层模型中的传输层，负责非接触环境下数据的半双工数据块的传输. 代表协议有 Topaz、MIFARE、MIFARE Ultralight、ISO 14443 A-4、ISO 14443 B-4、LLCP 等，这些协议定义了近耦合磁场环境下的数据发送、接收等命令格式和数据传输流程. 协议层是在数据通信过程中真正传输和发送数据的层，通信载荷可以是任意格式的数据，载荷数据一般由应用层协议定义.

应用层为 NFC 协议参考模型的顶层，用于为用户提供各种应用服务. 该层协议主要指 NFC 数据交换格式(NFC Data Exchange Format，NDEF)协议，其定义了用户数据交换的各类报文，例如 URI、TEXT、Smart Poster 等类型报文.

2.3　工作模式

NFC 工作模式是指 NFC 设备之间的通信方式和操作过程，文献[1,7,18]也称之为通信模式或操作模式(参见前页脚注⑤). 这里把通信模式和工作模式看成按照不同参照划分的种类，按照通信的发起者划分，工作模式可分为主动模式(Activie mode)和被动模式(Passive mode)①. 在主动模式下，通信双方均产生 RF 场；在被动模式下，只有通信发起者产生 RF 场. 在主动模式下，发起者和目标设备均产生 RF 场，并使用各自的 RF 场传输数据. 发起者按照选定的传输速度进行通信，目标设备按相同的速度应答. 发起者可以选择 106 kbps、212 kbps 或 424 kbps 其中一种传输速度，目标设备必须按照相同的速度将数据传回发起者；在被动模式下，发起者按照选定的传输速度发起通信，目标设备以加载调制的方式响应发起者命令，按照相同的传输速度应答. 从产生 RF 场的角度看，发起者是主动的，目标设备是被动的. 因此，单纯的从产生 RF 场的角度来区别发起者和目标设备是不合适的，因为在主动模式下两者均产生 RF 场，应该从通信的发起者来区分发起者和目标设备.

按照通信的对象划分，可分为点对点模式(P2P mode)、读卡器模式(Reader/Writer mode)和卡模拟模式(Card Emulation mode)②. 点对点模式能够在两个具备 NFC 功能的设备之间实现数据点对点传输，如共享音乐、传输图片等. 在此模式下，发起者发起通信，与目标设备建立链接进行数据传输. 发起者首先产生 RF 场初始化 NFCIP-1 通信，目标设备则响应发起者所发出的命令，并选择由发起者所发出的或是自行产生的 RF 场进行通信. NFCIP-1 是 NFC 技术的基础，其定义了电感耦合设备在频率 13.56 MHz 下的通信模式，并规定了 RF 接口的调制、编码、传输速度、帧格式以及初始化等. 在读卡器模式下，NFC 设备作为读卡器，使用 13.56 MHz 载波振幅调制与 NFC 标签(Tag)进行通信，载波的振幅变化导致 Tag 感应线圈的电压随之改变，Tag 使用简单的解码电路对信号进行解码. Tag 与读卡器的通信，采用负载调制的方法来实现，通过 Tag 线圈的负载是通过改变并联电容的开关实现的. 卡模拟模式，相当于采用 RFID 技术的 IC 卡，NFC 设备可以代替信用卡、公交卡、门禁卡等 IC 卡. 在该模式下，充当 IC 卡的 NFC 设备不用产生 RF 场来供电，其属于被动组件，RF 场由读卡器产生. 当宿主设备没有电时，例如手机，充当 IC 卡的 NFC 设备仍可以正常工作，这是该模式最大的优点.

3　面临的安全威胁

随着移动互联网和移动支付的发展，NFC 技术和 NFC 移动终端以及应用被迅速推广和普及. 2014 年，中国人民银行因安全问题叫停二维码支付，鼓励银行拓展 NFC 手机支付应用，中国银联和三大运营商斥巨资开发 NFC 支付软件和硬件③. 在政府和法规政策的支持下，NFC 技术的发展如火如荼，基于

① PN512[EB/OL]. http://www.cn.nxp.com/documents/data_sheet/PN512.pdf, 2015,1,9

② ISO14443[EB/OL]. http://www.openpcd.org/ISO14443, 2015,1,9

③ 2014 年国内 NFC 市场发展状况看点[EB/OL]. http://www.yktchina.com/ZT/nfc2014/index.html, 2015,1,9

NFC 技术的应用，尤其在移动支付方面，在不断推广和流行. 由于 NFC 系统和应用可能包含敏感的个人隐私、支付信息等，其安全性更加重要. 如图 2，NFC 安全威胁从整体上可分为终端安全威胁、系统安全威胁、应用安全威胁和通信安全威胁. 终端安全威胁包括终端丢失、设备损坏、SIM 卡克隆、电磁辐射窃听、芯片安全等. 终端丢失将可能直接造成用户信息被窃取，是终端安全面临的最大的安全风险. 此外，设备损坏将导致信息不可用，SIM 卡克隆能够通过复制手机 SIM 卡获取用户信息，电磁辐射窃听可获取手机通信的信息，智能芯片可被植入恶意程序来获取用户信息等. 系统安全威胁包括系统漏洞、恶意软件、系统 API 滥用、权限滥用、系统后门等. 智能终端操作系统存在大量安全漏洞或后门，系统 API 和权限存在被滥用的风险，且恶意软件也能危及系统的安全，这些因素将危及 NFC 依赖的智能操作系统安全. 应用安全威胁包括应用漏洞、逆向工程、重打包、恶意软件等. 应用程序开发者良莠不齐，应用存在大量安全漏洞；由于对安全重视不足，通过逆向工程技术或重打包，能够获取应用程序的源代码、用户信息，并植入恶意程序，严重危害了应用程序的安全. 通信安全包括窃听、数据破坏、中间人攻击、拒绝服务攻击等，通过监听数据、修改数据、重放数据等导致通信中断、信息泄露、金钱损失等严重的后果.

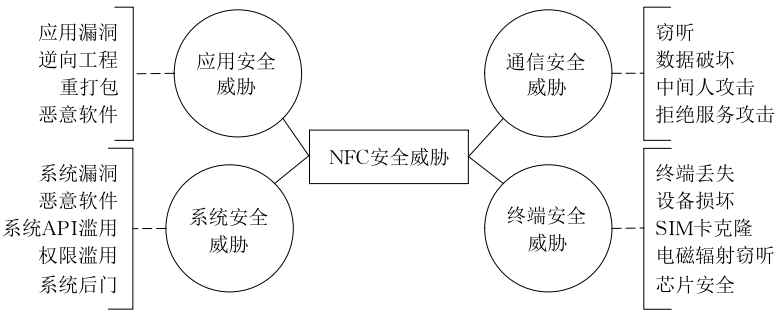

图 2 NFC 安全威胁

以上从 4 个方面概述了 NFC 面临的安全威胁，下面将针对重要的安全威胁或安全部件详细阐述安全威胁和相关解决方法，包括通信安全、安全漏洞、安全元件、恶意软件、网络钓鱼等. 下面将具体介绍这些安全威胁.

3.1 通信安全

通信安全是 NFC 技术面临的比较传统的安全威胁，主要分为窃听、数据破坏、数据复制、中间人攻击等[7,17-23].

窃听是指攻击者在 NFC 通信过程中使用特殊设备捕捉通信数据的过程. 在 NFC 非支付的通信过程中，链路层通讯一般不加密，攻击者可以轻易获取 NFC 标签中的内容. 尽管 NFC 技术的通信距离不超过 20 cm，但这种特性并不能阻止其被窃听，通过利用定制的特种天线[24-25]或者增强的信号接收器等就可以扩大近场通信的距离，进而截获通信数据，且窃听者不必完全截获就能够还原通信内容. 如果 NFC 标签存在于身份证、护照等包含个人敏感信息的 IC 卡中，遭遇窃听将导致个人隐私的泄露.

数据破坏是指攻击者通过发送预先构造的数据来干扰或者阻塞正常通信信道进而实现破坏正常通信数据的目的. 该过程不需要破解通信数据，仅需要使用大功率的设备发送干扰数据就可导致目标 NFC 设备拒绝服务. 例如，在 NFC 支付系统，票务系统等应用中，将导致 NFC 终端无法提供服务或者产生错误的交易.

数据篡改主要是指利用特殊设备更改或者使用预先构造的恶意 NFC 标签替换有效的标签. 由于很多标签应用设置了逻辑保护，不允许修改内容，例如，商品标签是用来描述商品价格、用途、支付数据等内容的，商场或者超市一般均会设置写保护. 但是，当前便宜的读写设备和特殊的 IC 卡将使得更改、复制或者替换标签内容成为现实，攻击者可以把篡改的标签贴到商品上，顾客将按照修改后的标签进行支付，最终将导致用户和商家的利益受损.

在 NFC 的通信过程中，中间人攻击是指 NFC 通信双方的通信数据被攻击者截获，攻击者利用截获的信息在特定的位置加以篡改以达到其攻击的目的. 中间人攻击包含了数据窃听、篡改以及数据的转发，虽然中间人攻击在真实环境中会因通信距离、通信模式等遭到较大限制，但该攻击仍然会对 NFC 通信，尤其是 NFC 支付带来很大的威胁.

为了确保 NFC 技术的通信安全，最有效的方法就是建立安全信道[20]，通过密钥共享和加密传输等手段来保证数据的完整性、保密性[26-27]. 安全信道能够防止窃听、数据篡改等，保证通信设备之间数据传

输的机密性、完整性和真实性. 对于中间人攻击，建议采用主动通信模式，且主动通信者应该主动监听任何攻击者发出的干扰磁场.

3.2 安全漏洞

安全漏洞(Security Vulnerability，SV)[28-29]是研究安全问题的生命线，是网络和信息安全的核心问题. 它是指信息系统在设计、实现或者运行管理过程中存在的缺陷或不足，从而使攻击者能够在未授权的情况下利用这些缺陷破坏系统的安全. 网络攻击和防御的核心就是安全漏洞，攻击者能够通过安全漏洞攻击软硬件目标，访问未授权的资源或者破坏目标系统等. 提前发现并修补 NFC 安全漏洞是 NFC 系统和应用安全的重要保障.

关于 NFC 技术，已知且细节公开的漏洞总结如下：

CVE-2008-5825①：手机 Nokia 6131(固件为05.12)的智能海报应用遇到包含空格(0x20)、回车(0x0D)或点(0x2E)字符的 URI 记录时，无法正常显示该记录. 攻击者通过构造包含以上畸形数据的 URI 记录，可以诱导用户访问恶意网站、拨打收费的电话或发送购买彩铃的短信.

CVE-2008-5826②：通过把 NDEF 记录的载荷长度、NDEF URI 电话记录的长度字段或 NDEF URI 短信记录的长度字段设置为一个大值并写入标签，会导致手机 Nokia 6131(固件为 05.12)在触碰该类标签时崩溃.

CVE-2008-5827③：手机Nokia 6131(固件为05.12)在下载完 JAR 文件时会自动安装软件，远程攻击者可以利用此特性构造 URI 记录执行任意代码.

Bugtraq ID 68470④：Android 及定制 ROM 系统存在一个拒绝服务漏洞，当 NFC 手机在触碰包含蓝牙配对报文时，导致 NFC 服务崩溃. 该漏洞是由蓝牙配对报文中畸形的本地名字段长度造成，畸形的长度值为 0b0000 0000 或 0b1XXX XXXX(X 代表 0 或 1)时.

E 乐充公交卡支付漏洞⑤：e 乐充公交卡是调用支付宝接口为北京市政交通一卡通进行支付的软件. 该软件存在一个逻辑漏洞，通过二次利用支付宝的支付结果再次充值，将导致 e 乐充公交卡应用发生异常，退还第一次支付的充值金额，实现零元充值.

安全漏洞是 NFC 支付和应用的最大威胁之一，有效挖掘 NFC 的漏洞，提出相应的修复措施和建议，是保证 NFC 安全的重要手段之一.

3.3 安全元件

安全元件(Secure Element，SE)，是存储密钥、敏感数据、加密运算等操作的安全芯片. 由于 NFC 最重要的应用就是移动支付功能，SE 则是保证支付安全的核心硬件，故其安全性不容忽视.

目前包含 SE 的 NFC 终端类型可分成 3 类：单线协议(Single Wire Protocol，NFC-SWP)方案、全终端方案、MicroSD 方案[30]，如图 3 所示. 3 种方案是根据 SE 的存在位置划分的，NFC-SWP 方案中 SE 是放置在 SIM 卡中，全终端方案中是把 SE 安置在终端上，MicroSD 方案中使用包含 SE 的独立外置MicroSD卡插入终端上. 其中 NFC-SWP 方案是目前比较流行的方案，并逐步得到推广.

从图 3 可以看出，不管是哪种方案，SE 是 NFC 支付和敏感数据通信的重要安全保障，在设计过程中均需要考虑 SE 面临的安全威胁及相应的安全措施. 例如，SE 与 NFC 控制器之间、SE 与操作系统之间的访问 API 以及访问控制权限等，一旦发生权限越界或者其他威胁安全的操作，将导致 SE 中的敏感信息泄露或金钱损失等.

3.4 恶意软件

恶意软件(Malware)[31-40]是指在未明确提示用户或未经用户许可的情况下，在用户计算机或其他终端上安装运行，侵犯用户合法权益的软件⑥. 针对 NFC 技术来说，恶意软件的恶意行为一般包括内容劫持、广告弹出、窃取用户支付信息、恶意扣费、恶意卸载、恶意捆绑或者其他侵犯用户知情权和选择权的行为.

随着智能手机的普及和流行，恶意软件逐渐开始从传统的 PC 平台扩散到移动平台. 根据 F-Secure 实验室和 Sophos 实验室的研究报告⑦⑧，与 PC 平台相比，移动平台恶意软件的数量几乎可以忽略. 但由于移动操作系统存在的漏洞和薄弱的安全设计，尤

① Vulnerability Summary for CVE-2008-5825[EB/OL]. http://web. nvd. nist. gov/view/vuln/detail?vulnId=CVE-2008-5825, 2015,1,9

② Vulnerability Summary for CVE-2008-5826[EB/OL]. http://web. nvd. ni st. gov/view/vuln/detail?vulnId=CVE-2008-5826, 2015,1,9

③ Vulnerability Summary for CVE-2008-5827[EB/OL]. http://web. nvd. nist. gov/view/vuln/detail?vulnId=CVE-2008-5827,2015,1,9

④ Google Android NFC Bluetooth Simple Pairing Message Denial of Service Vulnerability[EB/OL]. http://www. securityfocus. com/bid/68470, 201 5,1,9

⑤ e 乐充公交卡充值支付漏洞[EB/OL]. http://www. wooyun. org/bugs/wooyun-2010-059796, 2015,1,9

⑥ "恶意软件定义"细则[EB/OL]. http://www. isc. org. cn/hdzt/feyrj/listinfo- 4196. html, 2015,1,9

⑦ Mobile Threat Report Q1 2014[EB/OL]. http://www. f-secure. com/static/doc/labs_global/Research/Mobile_Threat_Report_Q1_2014_print. pdf, 2015,1,9

⑧ Sophos Labs. Security Threat Report 2014[EB/OL]. http://www. sophos. com/en-us/medialibrary/PDFs/other/sophos-security-threat-report-2014. pdf, 2015,1,9

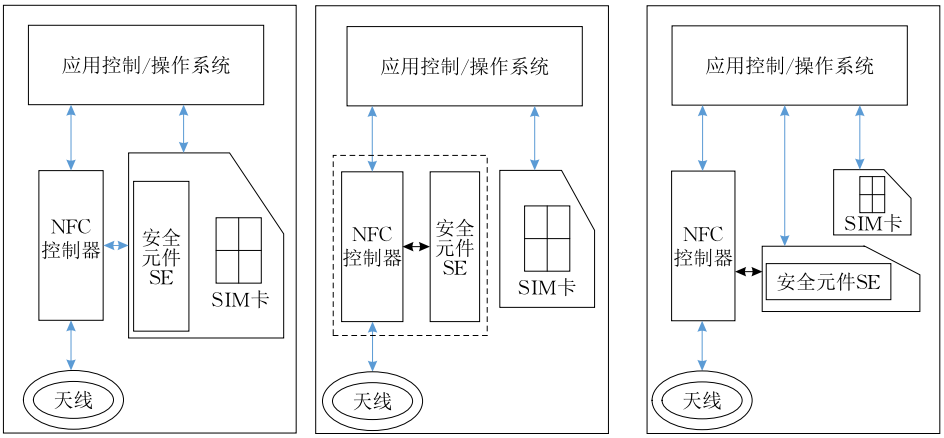

图 3 包含 SE 的 NFC 终端类型[30]

其是开源的 Android 操作系统,且移动终端设备包含更多的隐私信息等,导致移动操作系统平台成为恶意软件新的温床. 根据网秦公司最新的研究报告①,2014 年第一季度手机恶意软件同比增长 63.9%,被感染的智能手机同比增长 71.5%. 根据 360 互联网安全中心发布的《中国移动支付安全报告》②,具有 NFC 支付功能的支付宝钱包占移动支付下载量近 6 成,而其他 NFC 相关应用,如 NFC 快拍、e 乐充、云飞等,下载量达到几十万次. 一旦攻击者通过捆绑恶意的应用程序诱骗用户下载 NFC 恶意支付应用,用户的手机将成为攻击者的"取款机". 2014 年 11 月,AVL 安全研究团队③发现一款利用 NFC 手机攻击交通卡的恶意软件,通过将该款恶意软件安装在一个 NFC 手机上,攻击者手持该 NFC 手机轻轻靠近圣地亚哥交通卡(bip!-card),就可以任意篡改卡中的余额. 由于 NFC 支付和 NFC 应用的推广和普及,针对 NFC 技术的恶意软件检测就成为了保证 NFC 支付安全的关键研究方向之一.

3.5 网络钓鱼

网络钓鱼[41-42]是指攻击者通过构造恶意的内容,并通过欺诈、利益诱惑和其他社会工程学手段使得用户去访问或读取恶意内容,并进行敏感信息交换、支付等操作,最终导致用户隐私泄露或利益损失④. 例如,攻击者伪造一个智能海报标签,其中包含一个恶意的网址,用户由于无法识别智能海报的真伪,一旦触碰该标签,可能打开钓鱼网站或者其他恶意网址,造成财产损失.

除了以上针对 NFC 技术的安全威胁,还包括硬件安全威胁、接入网络安全威胁、云安全威胁等等,这里不具体介绍了.

以上从通信安全、安全漏洞、安全元件、恶意软件、网络钓鱼等方面介绍了 NFC 技术面临的安全威胁. 针对这些安全威胁,研究人员已经做了大量的研究,下节将介绍 NFC 安全研究的现状.

4 NFC 安全研究现状

由于 NFC 技术的迅速发展,其安全性受到越来越多的威胁和挑战. 在工业界和学术界,研究人员针对 NFC 安全技术已经做了大量的研究,并取得了一定的进展,下面将按照时间顺序依次介绍相关研究进展.

Haselsteiner 等人[20]从非接触式 Token、票据/微支付、配对 3 个应用场景分析了 NFC 面临的威胁,包括数据劫持/破坏/修改、中间人攻击等,并提出了安全通道、能量检测等防御措施,且针对安全通道措施提出一个 NFC 秘钥认证机制.

Mulliner[22]提出一种支持 NFC 的移动手机安全测试方法,通过对 NFC 子系统和 NFC 接口控制的软件组件进行测试,发现了大量未知漏洞,其中一些可以被用来标签内容欺骗,即通过插入一些空白,导致用户打开网络钓鱼等恶意网址或 APP,进而导致隐私泄露等,还可制作 NFC 蠕虫以及构造畸形 NDEF 数据包进行 DoS 攻击. 该方法采用手工构造测试用例进行测试,无法实现自动化,耗费大量人力

① 2014 年第一季度网秦全球手机安全报告[EB/OL]. http://s1.nq.com/file/cnnq/download/2014Q1.pdf, 2015,1,9
② 中国移动支付安全报告[EB/OL]. http://aqvs9knlja.l5.yunpan.cn/lk/Q4UgpLKMLV9Xq, 2015,1,9
③ NFC 手机:攻破交通卡[EB/OL]. http://blog.avlyun.com/2014/11/1668/nfc-phone-fee-consumption/, 2015,1,9
④ Phishing[EB/OL]. http://en.wikipedia.org/wiki/Phishing, 2015,1,9

和时间，效率低下.

Van Damme 等人[23]提出了一个针对 NFC 的安全保护系统，并在 Nokia6313/2 上开发了一个 NFC 应用支付程序，其中使用了基于 PKI(Public Key Infrastructure)的安全协议加密，最后对结果进行评估. 该方案是从防御的角度对 NFC 支付安全进行研究，通过加密手段会造成一定的时间开销.

Jara 等人[21]认为 RFID 是一种局限于身份认证的解决方案，扩展到 NFC 上就会产生安全问题，因为 NFC 涉及到身份认证、支付等问题，他们首先使用公钥密码算法 RSA 评估了 NFC 设备(Google Nexus One、PDA Acer N30 等)执行非对称加密方案的能力. 根据数据载荷和等待时间指标，分别使用不同的密钥长度和信息长度进行评估. 最后，他们提出了使用非对称加密方案例如 RSA 交换共享密钥、再使用对称密钥算法例如 AES 传输数据的混合安全方案. 该方案的缺点是密钥长度太长以及生成证书的时间过长.

贾凡等人[7]采用威胁建模的方法分析了 NFC 支付的流程以及各个模块之间的数据流图，确定整个支付系统的入口和要保护的数据，并分析了潜在的安全威胁和攻击场景，最后从安全技术及使用过程两个方面提出相应的威胁对付策略. 该方案从理论的角度分析 NFC 支付安全和相关措施，需要一定的评估和验证.

Miller[17]使用基于生成和变异策略结合的 Fuzzing 技术对协议层和应用层测试，利用 Sulley 完成变异测试，同时使用 logcat 进行监控异常，发现了大量的漏洞. 该方法虽然采用基于生成和变异结合的方法构造测试用例，但针对具体报文时却采用单一的策略构造测试用例，此外，针对目标异常的监控手段也比较单一.

Ghag 从 NFC 的角度上分析了谷歌电子钱包受到的威胁并评估了谷歌钱包的安全措施[6]，他的工作是基于现有的移动支付解决方案，包括嵌入式的解决方案、基于 SIM 卡的解决方案和基于安全存储卡的解决方案. 该文献也是仅仅从理论的角度进行分析和评估.

Wiedermann[43]提出一个基于 Fuzzing 技术的漏洞挖掘架构，并开发一个测试工具 Fuzzing-to-go，针对 Android NFC API 和 NFC APP 进行测试，使用 Sulley 生成测试用例，利用 Intent 发送报文，对 7 个应用进行测试，发现了一些 DoS 漏洞. 该方法采用 Sulley 的进程监控方式，对智能手机的监控效果不好，且监控手段比较单一，不能提供详细的 logcat 异常日志；同时，该方法对 Android 系统和 API 版本依赖性强，可移植性差.

Gummeson 等人[44]提出一种基于硬件的 NFC 防护方案，他设计并开发了小型无源的“补丁”EnGarde，可嵌入手机后壳，用于拦截 NFC 恶意交互，包括拦截恶意操作、智能拦截黑名单中的行为事件等. 该方法是从防护的角度对 NFC 安全进行研究，同时该方案需要增加一定的硬件成本.

Roland 针对 Android 平台的两种场景设计了安全元件 Secure Element 模拟器[45]，包括 Android 模拟器和 Android 手机. 该模拟器可以用来测试和调试 Java Card 语言编写的 applet 程序，应用程序开发者可以使用 SE 模拟器取代真实的 SE 模块，极大简化和降低了 SE 应用程序开发的复杂度和开销.

王志强等人[46]针对 Android 系统和 Windows Phone 系统等移动终端平台、NFC 第三方应用程序进行了系统和全面的测试，采用 ACS ACR122U 模拟标签，通过进程操作模拟“触碰”操作，实现了自动化的漏洞挖掘，并发现了蓝牙自动打开、Wifi 自动打开、第三方应用程序解析等大量未知的漏洞.

文献[6-7,20-21]从安全信道、身份认证、安全支付等方向研究 NFC 的数据传输安全，是从积极防御的角度进行研究，提出的方案停留在理论层面，有待实践的检验. 文献[22]从手工的角度进行测试，效率比较低下. 文献[23]实现了一个支付方案，对未来 NFC 支付的发展具有一定的借鉴意义，需要考虑加密算法的安全性和时间开销. 文献[17,43,46]均是从漏洞挖掘的角度去分析 NFC 的安全，均实现了自动化的测试，但文献[17,43]中的协议测试用例构造策略比较粗糙，且仅针对 Android 平台有效.

从整体上看，NFC 的研究工作可分为攻击和防御两个部分. 从攻击的角度，NFC 的研究工作侧重于挖掘和检测 NFC 技术相关的应用程序、支付系统等中的安全漏洞或者安全隐患，并针对这些安全漏洞或安全隐患提出相应的攻击方案，最后提出漏洞修复和安全防御措施. 此类研究工作以文献[17,22,43,46]为代表，这些文献使用 Fuzzing 测试等技术挖掘 NFC 相关应用程序的安全漏洞，按照漏洞挖掘、漏洞利用、漏洞修复的过程研究 NFC 技术相关的应用安全状况. 该类研究工作研究的对象是已有的 NFC 应用程序、系统等，具有一定的滞后性. 因此，该类研究工作的特点是“先攻击后防御”，即在发

现 NFC 安全漏洞和利用漏洞造成的损失或影响后，根据攻击的机理针对特定的漏洞、设计缺陷等提出相应的修复措施和防御方案. 从防御的角度，NFC 研究工作侧重于使用加解密算法、密钥共享、签名算法、恶意内容检测算法等研究具体的软件和硬件防御系统设计、防御措施等，该类研究工作以文献[20-21, 23-44]为代表. 加解密和密钥共享算法用于保证 NFC 通信过程中的数据安全，防止数据和信息泄露；签名算法用于防止数据被篡改、重放等，确保数据的完整性；恶意内容检测算法用于防止通过 NFC 方式传入恶意内容和数据，确保 NFC 应用程序等的可用性和安全性. 防御角度的研究工作，是从秘密性、完整性、可用性 3 个角度为 NFC 通信过程提供安全保证. 该类研究工作的特点就是“超前性”，即在 NFC 系统、应用程序等的设计和开发阶段，就积极地加入安全防御措施，这部分工作是未来软件开发和安全研究工作的发展方向和趋势.

以上是 NFC 技术安全研究主要进展的介绍和整体分析. 随着移动支付和 NFC 手机的普及和推广，针对 NFC 技术的安全威胁和挑战还将不断出现，需要安全人员继续从攻击和防御的角度研究 NFC 相关的安全技术，为 NFC 应用和支付等提供安全保障.

5 未来的研究方向

通过调研 NFC 安全的研究现状和分析 NFC 技术面临的安全威胁，将 NFC 安全研究工作分为 5 个部分：硬件安全、移动操作系统安全、应用程序安全、数据安全、支付安全，如图 4 所示.

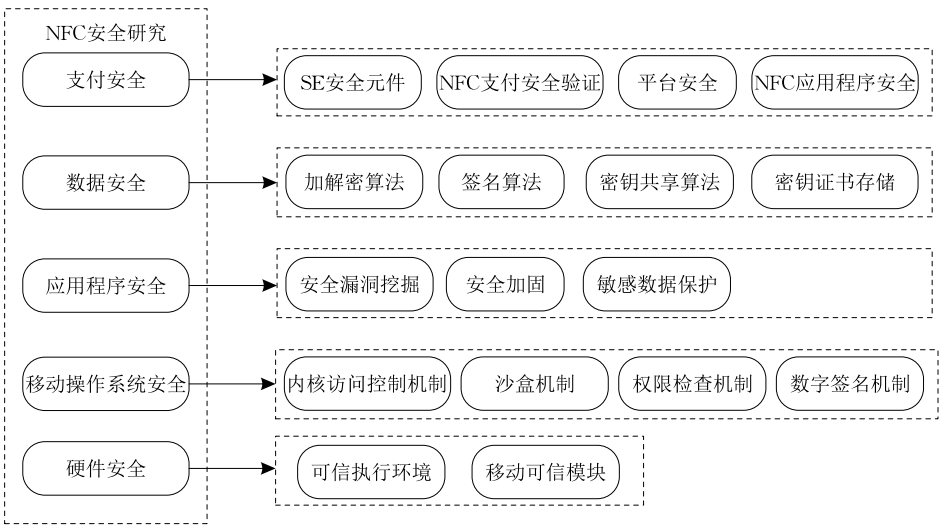

图 4 NFC 安全研究工作

硬件安全通过可信执行环境(Trusted Execution Environment，TEE)和移动可信模块(Mobile Trusted Module，MTM)来实现. TEE 是 GP(Global Platform)组织设计的一种安全区域①，位于智能电话的主处理器中，确保敏感数据存储、处理及保护等操作处于一个可信环境中. 它为授权的安全软件(Trusted Applications)提供安全的运行环境，并对安全软件的数据与资源实施机密性、完整性及访问控制等安全保护. MTM② 是 TCG(Trusted Computing Group)组织设计的用于移动设备的安全组件，支持安全启动、安全的根密钥及免疫数据保护等. TEE 和 MTM 是 GP 和 TCG 组织从硬件级别针对移动平台设备提出的安全解决方案，目前很多硬件厂商均提出了自己的可信计算体系结构，但这些体系结构大都依赖于被动的硬件设备或者没有可信的操作系统支持，导致信任链的源头存在安全风险，因此并不能保证系统运行时计算环境的可信. 如何设计完整的可信计算平台体系结构是目前需要解决的核心问题之一[47]. 在可信计算的关键技术中，信任链扩展也是需要解决的问题之一，它的思想是以底层硬件为基础通过层层度量和认证的方式构建从系统启动到操作系统运行的可信计算环境. 由于可信计算平台基于不可信的硬件设备上，不仅为可信平台带

① Trusted Execution Environment [EB/OL]. http://www.trustedcomputing group. org/media_room/news/253, 2015, 4, 27

② Mobile Trusted Module [EB/OL]. http://www. trustedcomputinggroup. org/resources/mobile_trusted_module_20_use_cases, 2015, 4, 27

来不安全因素，还将借助信任链的传递导致风险扩散[47]. 因此，需要针对信任链的扩展技术进行深入的研究. 此外，系统运行时刻的完整性度量也是可信计算需要解决的难题. 以上就是可信计算面临的主要问题和研究内容，实现安全可信的移动平台[48-49]是在硬件级别保证上层安全的基础.

移动操作系统安全，以 Android 系统为例，一般包括内核访问控制机制、沙盒机制、权限检查机制、数字签名机制等[50]. 访问控制机制包括身份认证和授权[51]，身份认证解决的是口令认证 ，即“你是谁”问题，授权解决的是“你能干什么”问题. 设计安全的访问控制策略，能消除隐蔽信道带来的安全风险，是保证移动操作系统安全的核心技术之一. 沙盒(sandbox)机制[52-53]是为了实现不同应用程序和进程之间的相互隔离，保证应用程序无法访问没有授权的系统资源或其他应用程序的资源. Android 系统使用 Dalvik 虚拟机和 Linux 的文件访问控制来实现沙盒机制，任何应用程序如果想要访问系统资源或者其他应用程序的资源必须在自己的 manifest 文件中进行声明权限或者共享 uid. 权限检查机制是 Android 系统中一个重要的安全机制[54]，任何一个应用程序在使用 Android 受限资源(网络、短信、蓝牙、通讯录、照片等)之前都必须提前向 Android 系统提出申请，等待 Android 系统批准后应用程序方可访问和使用相应的资源. 数字签名机制[50]是指所有安装到 Android 系统中的应用程序都必须拥有一个数字证书，此数字证书用于标识应用程序的作者和应用程序之间的信任关系. 只有当应用程序的数字签名与声明此权限的应用程序所用数字签名相同时，Android 系统才会授权. 以上是 Android 系统主要的安全机制，不同操作系统的安全机制并不完全相同，需要具体分析和研究. 如何设计安全的保护机制，是保证移动操作系统安全的重要研究内容.

应用程序安全研究包括安全漏洞挖掘、安全加固、敏感数据保护等. 安全漏洞挖掘是从攻击的角度寻找应用程序的漏洞，并提出相应的修复措施和解决方案. 安全加固是保障应用程序安全的主要技术之一，是指通过对应用程序加密、混淆、加壳等，防止应用程序被执行反编译、二次打包、插入恶意代码等恶意操作，保护应用程序的源代码和知识产权. 敏感数据保护，指应用程序包含的数据库、口令、账号等敏感信息的存储和保护，防止被越权读取和修改等恶意操作，常用的方法包括加密、身份认证等. 应用程序安全研究的目标就是保护敏感数据和应用程序源代码，修复存在的安全漏洞，防止“跟踪/调试/窃听”等逆向技术. 关键和具体的研究技术将在后面深入介绍.

数据安全，涉及数据的加解密算法、签名算法、密钥共享算法、密钥证书存储等研究内容. 如何设计安全的加解密算法，防止数据被未授权读写；如何设计安全的签名算法，防止数据伪造和抵赖；如何共享密钥和存储密钥证书，保证加解密过程的安全. 解决这些问题，是保证敏感数据安全存储和传输的关键. 此外，建立安全的数据传输通道是保证数据安全传输的关键技术，后面将具体介绍安全通道.

支付安全是属于 NFC 技术应用层面的安全. 基于 NFC 技术的支付安全研究工作包括安全元件 SE 的安全、NFC 支付安全验证、平台安全、NFC 应用程序安全等. SE 是移动支付的核心组件，研究 SE 自身和相关的安全问题是移动支付安全的核心问题. NFC 支付安全验证涉及签名验证、支付口令验证等算法，这是整个近场支付的关键阶段. 平台安全，是指从移动支付的角度研究支付平台的安全体系设计，该部分可参考图 4 中硬件安全部分. NFC 应用程序安全，是指从 NFC 技术的角度分析相关应用程序的安全问题，可参考图 4 中应用程序安全部分.

以上从硬件安全、移动操作系统安全、应用程序安全、数据安全、NFC 支付安全等五个部分概述了 NFC 安全研究工作涉及的内容. 根据 NFC 面临的安全威胁和研究现状，下面将选择核心和关键的技术或问题具体介绍 NFC 技术相关的研究内容和研究方向，包括安全信道、漏洞挖掘、安全元件、恶意软件、恶意内容检测、移动支付等相关研究内容.

5.1　安全信道

安全信道[7,17-23,55-56]是抵抗嗅探、篡改、伪造、中间人攻击的重要手段，是从积极防御的角度保证 NFC 的通信安全. 如何建立一个有效的安全通道，是确保 NFC 技术在数据传输过程中的安全所面临的重要研究问题.

安全的通信信道具有两个特点：保密性和完整性. 保密性是指确保数据内容的安全，不会被窃听者查看到，该特性一般采用加密和解密来实现. 加解密算法分为对称和非对称算法，对称算法效率高，缺点是密钥共享需要建立专门的信道；非对称算法能够提供方便和安全的密钥管理，并具有数字签名的功能. 两类算法的选择需要根据具体算法的强度、效率和系统的性能等方面综合考虑. 完整性是指安全信道在传输过程中没有受到恶意的或者意外的修改.

完整性一般通过散列函数、消息认证码、加密等方法来鉴别. 散列函数①,又称哈希函数、杂凑函数,是指把任意长的输入消息串变化成固定长的输出串的一种函数,其中固定长的输出串称为该消息的杂凑值. 消息认证码②,又称为带密钥的消息认证码,是基于密钥和消息认证码获得的一个值,用于数据认证和完整性校验. 加密,是指把明文加密后以密文作为数据认证符. 建立一个安全信道,就要考虑以上两个特性,选择合适的加密和完整性校验算法,确保数据的通信安全.

5.2 漏洞挖掘

漏洞挖掘针对的是移动操作系统、系统 NFC 处理模块和第三方应用程序,通过检测其中的安全漏洞,提前修复这些漏洞,是从主动攻击的角度保证 NFC 技术在通信过程中的数据安全. 下面将具体介绍针对 NFC 技术的主要漏洞挖掘方法.

5.2.1 手工测试

手工测试(manual testing),就是由测试人员手工构造测试用例,并逐个将其输入到被测目标,观察目标的响应,是最原始的漏洞挖掘方法[57]. 手工测试一般适用于时间资源不足、技术水平不足以及无法自动化的场合,可以最大程度地发挥人的主观能动性,设计出最真实的用户情况,容易识别出显而易见的缺陷和难以发现的缺陷,尤其是业务逻辑类的问题. 手工测试的效果完全依赖于测试人员的业务知识、计算机操作能力、测试经验等,没有规律可循,不可重复使用,无法移植,不适用于大规模测试.

在 NFC 相关漏洞挖掘的过程中,手工测试具有非常重要的作用. 由于部分 NFC 协议规范是收费的或者自定义的,例如 Wifi 简单配置协议规范需要收费 99 美元,NFC 标签助手使用了自定义的控制屏幕亮度、铃声等报文,导致构造的测试用例效率比较低. 使用手工分析和测试的方法可以最大限度发挥人的主观能动性,分析并推断出协议报文的格式,提高测试用例的有效性. 手工测试是漏洞挖掘初期经常采用的一种方法.

5.2.2 Fuzzing 测试

Fuzzing 测试,也称为 Fuzz 测试或模糊测试,是指通过向被测目标输入大量的畸形数据并监测异常来发现漏洞的一种自动化测试技术[43,58-60].

Fuzzing 测试过程一般分为 6 个阶段,分别为识别目标、识别输入、生成测试用例、执行测试用例、监视异常、确定可利用性[58].

(1)识别目标. 确定被测试的目标程序,包括识别目标应用程序中具体的文件、库、使用的协议等. 主要是指确定被测的 NFC 协议和被测的目标,例如测试 NDEF 协议和 Android 系统的 NFC 类.

(2)识别输入. 确定输入变量,包括数据包、文件、环境变量、端口号等所有发送到目标程序的数据,这对于测试用例的构造是至关重要的. 如果没有输入,Fuzzing 测试无法继续进行,几乎所有的安全漏洞均是由特定的输入变量触发的. 针对 NFC 技术,输入变量一般是指数据包以及测试过程中需要设置的环境参数.

(3)生成测试用例. 测试用例,是指根据确定的输入变量生成的输入数据. 测试用例生成,是 Fuzzing 测试最关键的一个阶段,直接影响到测试结果的好坏. 通过分析 NFC 论坛官方文档,获取各类 NDEF 报文的格式,使用半有效的数据生成 NFC 各种协议报文的一个或多个测试字段,其他字段使用正常数据填充,进而生成各类测试用例.

(4)执行测试用例. 执行是指把生成的测试用例输入到目标程序,包括发送数据包给目标应用程序、打开一个文件、发起一个目标进程等,其中数据包、文件为测试用例. 针对 NFC 的协议,执行测试用例的环境搭配如图 5 所示. 图中使用的设备 ACR 122U 模拟虚拟的标签,在 Ubuntu 系统下向虚拟标签中写入测试用例,然后把 NFC 手机放到 ACR 122U 上,利用进程操控模拟“触碰”标签的过程,实现自动化的执行测试用例. 其中 ACR 122U 也可使用其他设备代替.

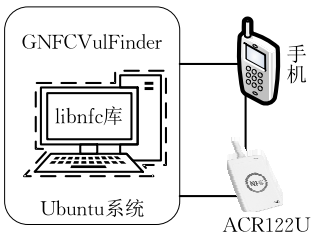

图 5 执行测试用例

(5)监视异常. 该步骤是 Fuzzing 测试必不可少的阶段,也是经常被安全研究人员忽视的步骤. 如果没有异常监控,在自动化测试过程中仅靠肉眼观察是无法确定触发异常的模糊数据,而且还会导致安全漏洞的漏报. 一般使用监控进程的 CPU 利用率、监控被测目标的日志等方法检测异常. 例如,在

① Hash function [EB/OL]. http://en.wikipedia.org/wiki/Hash_function, 2015,1,9

② Message authentication code[EB/OL]. http://en.wikipedia.org/wiki/Messa ge_authentication_code, 2015,1,9

Android 目标平台下，logcat 就是一个有效的日志监控工具.

(6) 确定可利用性. 针对发现的异常，一般需要确定异常是否可以利用，这个过程需要人工的参与，但该过程不是必需的.

根据 Fuzzing 测试的 6 个过程，可以发现该技术具有一些天生的缺点，即无法发现某些类型的漏洞. 这些漏洞包括访问控制缺陷、设计逻辑不良、后门、多阶段安全漏洞[58]等. 因为 Fuzzing 测试并不是完全智能的，无法理解目标应用程序的设计逻辑，因此无法检测逻辑类型的漏洞.

5.2.3　程序分析

程序分析技术包括静态程序分析技术和动态程序分析技术.

静态程序分析，也称静态应用程序安全检测(Static Application Security Testing，SAST)，是指在不运行计算机程序的条件下，通过词法分析、语法分析、语义分析、控制流分析、污点分析等技术[61-63]对程序代码进行扫描，验证代码是否满足规范性、安全性等指标的一种代码分析技术. 该技术需要使用人工指定或者自动推断的方法设定安全代码应该遵循的程序规范，然后使用代码分析技术进行语义分析，从而挖掘违背程序规范的行为，即漏洞[64]. 该技术拥有应用程序的全部源代码，因此可以完全遍历程序，代码覆盖率可以达到 100%. 由于任何关于程序分析的问题都是不可判定的[65-66]，不存在任何一种机械化的方法能够证明程序的完全正确性. 因此，静态程序分析技术不可避免地存在漏报和误报.

针对 NFC 应用程序，静态程序分析的方法如图 6 所示. 首先，通过直接获取、静态反编译、逆向工程等手段获得 NFC 应用程序的源代码或二进制代码. 其次，通过词法分析和语法分析等手段把源代码转换成中间代码，并利用流分析获取数据流和控制流. 再次，针对安全漏洞进行分析和建模，并对中间代码、数据流和控制流进行漏洞挖掘. 最后，分析检测出的漏洞，输出结果.

动态程序分析一般通过插桩技术分析程序的异常行为. 插桩技术[67]是指在保证被测程序逻辑完整性的基础上在程序的关键位置插入一些“桩”，即加入一些测试代码，然后执行插桩后的程序，通过“桩”的执行获取程序的控制流和数据流信息，进而分析程序的异常行为. 由于该技术需要插入冗余代码“桩”，因此大大增加了程序运行分析的时间开销，这是动态程序分析面临的一个严峻问题. 同时，“桩”仅

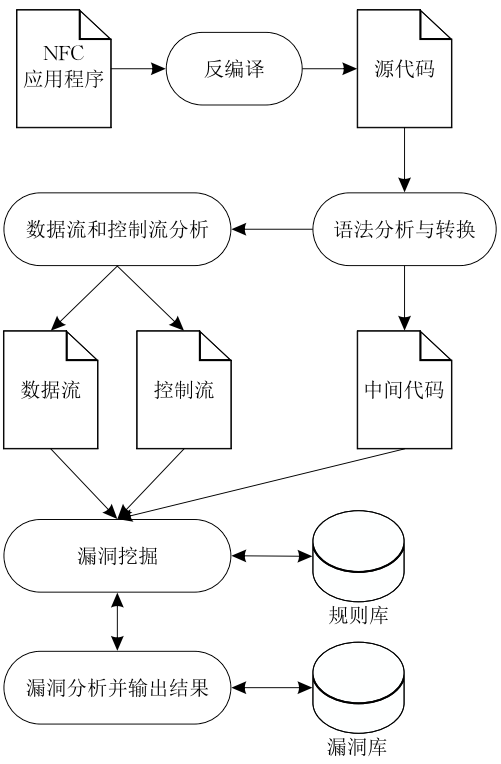

图 6　静态程序分析过程

在关键位置被插入，无法保证代码的完全覆盖. 和静态程序分析一样，动态程序分析同样存在漏报和误报的问题.

针对 NFC 应用程序，动态程序分析常常根据 Android 系统的关键 API 进行监控和插桩，例如蓝牙、wifi、sms 等. 首先，针对漏洞进行建模，确定漏洞的规则和描述. 其次，对关键 API 进行插桩，并获取 NFC 应用程序的系统调用序列. 最后，使用漏洞规则匹配的方法，针对获取的序列进行漏洞检测.

5.2.4　二进制代码审核

由于大部分 NFC 应用程序并不是开源的，甚至采取加密、方法名混淆、第三方 so 库等多种方式对 APK 文件进行加固，很难获取程序的源代码. 为了理解程序具体功能的操作细节，研究人员一般采取分析程序编译后的汇编指令的方法，即使用代码逆向工程(Reverse Code Engineering，RCE)[68-71]. 在汇编代码层次上进行安全评估而不是在源代码层次上进行安全评估，这种安全评估一般称为二进制审核[58](binary auditing).

针对 Android 系统平台，二进制代码审核获取的是反编译后的二进制代码，即 smali 代码. 但由于反编译技术的限制，在反编译的过程中会导致大量的变量信息丢失，包括变量类型和函数参数类型等，这样获得的二进制代码较难理解，甚至会存在逻辑

错误.因此,该技术对研究人员的技术要求很高,且一般存在比较高的漏报率和误报率,自动化效率比较低.

5.3 安全元件

安全元件 SE 是 NFC 支付的核心部件,其控制权也受到了移动运营商、银联等的竞争和抢占,如何确保 SE 的安全是 NFC 支付研究面临的关键问题之一.

SE 是一个安全芯片,敏感数据处理、加密运算等业务均需要单独的安全芯片处理,例如公交刷卡、银行卡支付、余额等.除了 SE 本身的数据处理事务外,SE 还向客户端开放了访问 SE 的接口,以实现余额查询、空中充值等功能.

针对 SE 的功能和安全特性,具体的研究点包括:内部加密算法的设计及其安全性、SE 访问控制策略的安全设计、APP 访问 SE 的 API 安全性等.加密算法是确保事务处理安全的重要手段,算法设计原则是在没有解密密钥的情况下通信或者其他事务处理过程中的数据在有效期内无法被破解.SE 访问控制策略是控制客户端应用对 SE 的访问操作权限,对 SE 访问的控制和授权是确保 SE 安全的重要手段之一.APP 访问 SE 的 API 安全性是指客户端应用程序访问 SE 的 API 是否安全,API 安全与否主要在于参数、数据等输入变量是否会导致信息泄露、越权访问、拒绝服务等危害 SE 安全的结果.需要注意的是,客户端通过应用处理器访问 SE 的接口芯片,由于 SE 的位置不同,接口芯片也会不同,例如 NFC-SWP 终端类型,SE 集成在 SIM 卡中.

5.4 恶意软件检测

随着智能手机的普及和流行,恶意软件开始向手机平台蔓延,包括安卓系统(Android)、苹果手机系统(IOS)、微软手机系统(Windows Phone)等手机操作系统平台.同时,由于移动支付和 NFC 技术的发展和普及,移动智能操作系统和 NFC 技术存在的漏洞或针对 NFC 模块的恶意软件逐渐开始出现.例如,节 3.4 中 AVL 团队发现的一款利用 NFC 手机攻击交通卡的恶意软件.

为了保证 NFC 数据传输和移动支付的安全,移动恶意软件的检测研究势在必行.在工业界,安全厂商大部分采用和 Windows 平台相同的检测方法,主要使用基于特征码的方法检测恶意软件,这种方法检测精度高,误报率比较低,但不能检测的特征库外的恶意软件[38].此外,恶意软件的变种行为相似,但特征签名不同,导致此类检测方法不能抵抗混淆、加壳等攻击[72].恶意软件及其变种数量非常大,需要创建大量的特征签名添加到特征库,这会增加检测的时间开销[40],降低恶意软件检测系统的性能.在学术界,研究人员基于静态特征、动态行为等作为恶意软件检测的依据,包括权限、系统调用、能量、时间开销、组件、消息传递等特征,然后使用相似度算法、数据挖掘或机器学习算法检测恶意软件[73-79].恶意软件检测评价最重要的指标就是漏报率和误报率,如何降低误报并减少漏报仍将是未来恶意软件检测面临的关键问题.

5.5 恶意内容检测

随着移动互联网和移动支付的发展,智能手机、平板电脑、路由器等移动智能终端设备逐渐开始内置 NFC 模块,NFC 技术在提供了便利的同时,也给智能终端设备带来了安全隐患.

从安全威胁入口的角度分析,NFC 技术给移动互联网带来了新的安全威胁入口.通过 NFC 模块,手机、平板电脑、智能家居设备等终端可以从外部 NFC 标签和其他 NFC 终端设备接收各种数据,包括短信、电话、智能海报、支付信息、功能设置等数据.然而,接收数据的终端设备往往忽略从 NFC 模块获取的数据的安全检测,或者对这些数据的检测和过滤较少.例如,在触碰智能海报或者包含 URL 的 NFC 标签时,具有 NFC 功能的 Android 手机会自动打开网址,不进行任何的安全检测或人工交互;在通过 NFC 标签进行拨打电话时,NFC 手机没有检测电话号码的正常与否,直接进行拨号,这将导致"@¥%&\…"等畸形的数据串能够突破拨号键盘的限制.

根据 NFC 入口安全的威胁分析,针对入口内容的检测和过滤,有必要进行深入的研究和开发.由于通过 NFC 传输的数据种类众多,需要根据具体的传输内容研究具体的安全检测方法,并把相应的检测方法应用到 NFC 应用程序的开发工作上.例如,针对包含 URL 的标签内容或者 P2P 传输的数据,需要在接收端开发相应的恶意网址检测模块,减少钓鱼网站、恶意软件网址、利用特定漏洞构造的恶意网址等带来的安全威胁.

5.6 移动支付

移动支付是 NFC 技术得以大力推广的一个重要原因,反之,正是由于 NFC 技术天然的安全特性使其成为移动支付的重要媒介.在 NFC 技术的应用方面,移动支付的存在形式分为两类:圈存和电子钱包.

圈存就是用户从银行等单位的个人账户中把金钱存入 IC 卡上，它是增加 IC 卡中电子现金余额的过程. 圈存到 IC 卡上的资金大多是在特定的消费环境下进行刷卡消费的. 例如，在校园里，一卡通一般与银行的个人账户进行关联和绑定，学生可以通过自助终端设备把银行中的金钱圈存到一卡通中，用于校园消费. 在 NFC 技术推广的阶段，北京亿阳汇智通科技股份有限公司开发的 e 乐充应用程序或写卡器即可把银行、支付宝等个人账户的金钱充值到北京市政交通一卡通中. 通过 NFC 手机直接给一卡通充值，不仅使得充值更加灵活和方便，还大大减少了人力和物力. 从工作模式的角度，圈存属于 NFC 的读卡器模式，NFC 手机或其他终端充当智能读卡器和写卡器.

电子钱包是指装入电子现金、电子信用卡、电子借记卡、电子零钱等电子货币，集多种功能于一体的电子货币支付方式[80-81]. 由于 NFC 技术天然的安全特性，使得基于该技术的电子钱包受到银行和电信运营商等的青睐，并开始逐渐推广，例如和包、翼支付、沃支付等. 目前 NFC-SWP 方案是国内最流行的电子钱包解决方案，即把 SE 和手机号码卡合并，例如中国电信的 RFID-UIM 卡、中国移动的 NFC-SIM 卡、中国联通的 RF-SIM 卡等. 该类电子钱包采用的安全方法主要包括数据加密、数字签名、安全支付口令等方法，这些方法能够基本保证支付交易的安全进行.

由于涉及到资金交易，基于 NFC 技术的移动支付受到了研究人员和攻击者的关注. 2014 年 5 月，e 乐充应用程序爆出支付漏洞，可免费给公交卡充值. 该漏洞通过 hook 方式获取支付成功的 pay 返回值，并再次通过 hook 手段把支付撤销时的返回值替换为获取的 pay 返回值，导致支付金额退回到支付宝账户，最终实现免费充值的目的. 同年 10 月，北京地铁收费系统被爆存在设计缺陷，攻击者使用 NFC 手机能够随意修改单程地铁票卡的金额. 该漏洞存在于地铁票卡中不安全的签名算法，可被轻易破解.

从安全研究的角度分析，NFC 移动支付应用面临的安全风险主要来自于 NFC 支付类客户端、操作系统、NFC 手机卡、数据通信、恶意软件、安全单元等. NFC 支付类客户端面临的安全威胁主要指应用程序存在的安全风险，例如密码明文传输和本地保存、应用程序设计缺陷等等. 操作系统存在的安全风险主要是指系统安全漏洞，该类漏洞可导致系统提权、敏感信息泄露、系统功能打开等后果. NFC 手机卡由 SE 和手机卡组成，该方式也是目前最流行的 NFC 支付方式，安全风险主要来自 SE，具体请参考 5.3 节. 在支付过程中，通信的数据一旦被嗅探、破解、修改，将可能造成支付金额的损失，其危害比非支付类应用的数据泄露更严重. 为了保证支付过程中的数据通信安全，最好的方法是建立安全通道，具体请参考 5.1 节. 恶意软件是 Android 系统等移动操作系统最大的安全威胁之一，也是 NFC 支付面临的安全威胁之一，例如山寨的 NFC 支付软件、包含恶意代码的 NFC 支付软件等，该类恶意软件的分析和检测是保障 NFC 支付安全的重要手段之一，具体介绍参考 5.4 节.

6　结束语

随着移动互联网和移动支付的发展，NFC 技术由于其天然的安全特性和便利性，成为运营商、银行、软件开发者等热捧的对象. 同时，NFC 技术也受到安全研究人员和攻击者的关注. 虽然国内外安全研究人员已经逐步开始对 NFC 安全问题进行了一定的研究，但目前还没有详细和全面介绍 NFC 安全研究进展的论文. 本文首先从基本特性、通信过程、协议栈、工作模式等方面介绍了 NFC 技术，并分析了该技术面临的安全威胁，包括通信安全、安全漏洞、安全元件、恶意软件、网络钓鱼等内容. 然后，通过分析相关参考文献，对 NFC 技术的安全研究现状进行分析和总结. 最后，从安全信道、漏洞挖掘、安全元件、恶意软件检测、恶意内容检测、移动支付等方面对 NFC 技术的研究内容进行分析，并展望未来的研究方向和方法.

致　谢　感谢所有对本文研究给予支持和帮助的人!

参　考　文　献

[1] Coskun V, Ozdenizci B, Ok K. A survey on Near Field Communication (NFC) technology. Wireless Personal Communications, 2013, 71(3): 2259-2294

[2] Markantonakis K, Mayes K. Secure Smart Embedded Devices, Platforms and Applications. New York: Springer, 2013

[3] Patauner C, Witschnig H, Rinner D, et al. High speed RFID/NFC at the frequency of 13.56MHz//Proceedings of the 1st International EURASIP Workshop on RFID Technology. Vienna, Austria, 2007

[4] Karnouskos S. Mobile payment: A journey through existing procedures and standardization initiatives. IEEE Communications Society Surveys and Tutorials, 2004, 6(4): 44-66

[5] Frisby W, Moench B, Recht B, et al. Security analysis of smartphone point-of-sale systems//Proceedings of the USENIX Conference on Offensive Technologies. California, USA, 2012: 22-33

[6] Ghag O, Hegde S. A comprehensive study of Google wallet as an NFC application. International Journal of Computer Applications, 2012, 58(16): 37-42

[7] Jia Fan, Tong Xin. Threat modeling for mobile payments using NFC phones. Journal of Tsinghua University (Science and Technology), 2013, 52(10): 1460-1464(in Chinese)
(贾凡, 佟鑫. NFC手机支付系统的安全威胁建模. 清华大学学报(自然科学版), 2013, 52(10): 1460-1464)

[8] Mattes D. Image Processing for Credit Card Validation. California: Jumia Inc., Technical Report: US20140052636, 2013

[9] Liu Y, Yang J, Liu M. Recognition of QR code with mobile phones//Proceedings of the 47th International Conference on Decision and Control. Cancun, Mexico, 2008: 203-206

[10] Lee J, Cho C-H, Jun M-S. Secure quick response-payment (QR-Pay) system using mobile device//Proceedings of the 13th International Conference on Advanced Communication Technology. Gangwon-do, South Korea, 2011: 1424-1427

[11] Finzgar L, Trebar M. Use of NFC and QR code identification in an electronic ticket system for public transport//Proceedings of the 19th International Conference on Telecommunications and Computer Networks. Split, Croatia, 2011: 1-6

[12] Gao J Z, Prakash L, Jagatesan R. Understanding 2D-barcode technology and applications in M-commerce-design and implementation of a 2D barcode processing solution//Proceedings of the 31st Annual International Computer Software and Applications Conference. Beijing, China, 2007: 49-56

[13] Jain A K, Ross A, Prabhakar S. An introduction to biometric recognition. IEEE Transactions on Circuits and Systems for Video Technology, 2004, 14(1): 4-20

[14] Prabhakar S, Pankanti S, Jain A K. Biometric recognition: Security and privacy concerns. IEEE Security & Privacy, 2003, 1(2): 33-42

[15] Delac K, Grgic M. A survey of biometric recognition methods //Proceedings of the 46th International Symposium on Electronics in Marine. Zadar. Croatia, 2004: 184-193

[16] Lee O. Sound-based mobile payment system//Proceedings of the International Conference on Web Services. California, USA, 2004: 820-821

[17] Miller C. Exploring the NFC attack surface//Blackhat. Las Vegas, USA, 2012

[18] Fischer J. NFC in cell phones: The new paradigm for an interactive world. IEEE Communications Magazine, 2009, 47(6): 22-28

[19] Madlmayr G, Langer J, Kantner C, et al. NFC devices: Security and privacy//Proceedings of the 3rd International Conference on Availability, Reliability and Security. Barcelona, Spain, 2008: 642-647

[20] Haselsteiner E, Breitfuß K. Security in near field communication (NFC)//Proceedings of the Workshop on RFID Security. Graz, Austria, 2006: 12-14

[21] Jara A J, Alcolea A F, Zamora M A, et al. Evaluation of the security capabilities on NFC-powered devices//Proceedings of the European Workshop on Smart Objects: Systems, Technologies and Applications (RFID Sys Tech). Ciudad, Spain, 2010: 1-9

[22] Mulliner C. Vulnerability analysis and attacks on NFC-enabled mobile phones//Proceedings of the International Conference on Availability, Reliability and Security. Fukuoka, Japan, 2009: 695-700

[23] Van Damme G, Wouters K, Preneel B. Practical experiences with NFC security on mobile ohones//Proceedings of the RFID Security. Leuven, Belgium, 2009

[24] Diakos T P, Briffa J A, Brown T W, et al. Eavesdropping near-field contactless payments: A quantitative analysis. The Journal of Engineering, 2013, 1(1): 180-186

[25] Brown T W, Diakos T, Briffa J A. Evaluating the eavesdropping range of varying magnetic field strengths in NFC standards//Proceedings of the 7th European Conference on Antennas and Propagation. Gothenburg, Sweden, 2013: 3525-3528

[26] Ellis J H. The possibility of secure non-secret digital encryption. England: UK Communications Electronics Security Group, Report: 1, 1970

[27] Merkle R C. Secure communications over insecure channels. Communications of the ACM, 1978, 21(4): 294-299

[28] Bishop M, Bailey D. A critical analysis of vulnerability taxonomies. California: University of California Technical Report: 1, 1996

[29] Shirey R. Internet security glossary. Massachusetts: BBN Technologies, Technical Report RFC 2828, 2000

[30] Yuan Qi. Technology solution and standards development for mobile payment. Information and Communications Technologies, 2012(6): 43-38(in Chinese)
(袁琦. 移动支付技术方案与标准进展. 信息通信技术, 2012(6): 34-38)

[31] Apel M, Bockermann C, Meier M. Measuring similarity of malware behavior//Proceedings of the 34th Conference on Local Computer Networks. Zurich, Switzerland, 2009: 891-898

[32] Aycock J. Computer Viruses and Malware. New York: Springer, 2006

[33] Bazrafshan Z, Hashemi H, Fard S M H, et al. A survey on heuristic malware detection techniques//Proceedings of the 5th Conference on Information and Knowledge Technology (IKT). Shiraz, Iran, 2013: 113-120

[34] Cesare S, Xiang Y. Classification of malware using structured control flow//Proceedings of the 8th Australasian Symposium on Parallel and Distributed Computing. Brisbane, Australia, 2010: 61-70

[35] Christodorescu M, Jha S, Seshia S A, et al. Semantics-aware malware detection//Proceedings of the IEEE Symposium on Security and Privacy. Oakland, America, 2005: 32-46

[36] Felt A P, Finifter M, Chin E, et al. A survey of mobile malware in the wild//Proceedings of the 1st ACM Workshop on Security and Privacy in Smartphones and Mobile Devices. Chicago, America, 2011: 3-14

[37] Jacob G, Debar H, Filiol E. Behavioral detection of malware: From a survey towards an established taxonomy. Journal in Vomputer Virology, 2008, 4(3): 251-266

[38] Natani P, Vidyarthi D. An overview of detection techniques for metamorphic malware//Proceedings of the Intelligent Computing, Networking, and Informatics. Raipur, India, 2014: 637-643

[39] Treadwell S, Zhou M. A heuristic approach for detection of obfuscated malware//Proceedings of the IEEE International Conference on Intelligence and Security Informatics. Texas, America, 2009: 291-299

[40] Zhao Z, Wang J, Bai J. Malware detection method based on the control-flow construct feature of software. IET Information Security, 2014, 8(1): 18-24

[41] Ramzan Z. Phishing attacks and countermeasures. Handbook of Information and Communication Security. New York, USA: Springer, 2010: 433-448

[42] Van Der Merwe A, Loock M, Dabrowski M. Characteristics and responsibilities involved in a Phishing attack//Proceedings of the 4th International Symposium on Information and Communication Technologies. Dublin, Ireland, 2005: 249-254

[43] Wiedermann N. Fuzzing-To-Go: A Test Framework for Android Devices[Ph. D. dissertation]. Technische Universität München, München, 2012

[44] Gummeson J, Priyantha B, Ganesan D, et al. EnGarde: Protecting the mobile phone from malicious NFC interactions//Proceedings of the 11th Annual International Conference on Mobile Systems, Applications, and Services. Taipei, China, 2013: 445-458

[45] Roland M. Debugging and rapid prototyping of NFC secure element applications. Mobile Computing, Applications, and Services, 2014: 298-313

[46] Wang Zhi-Qiang, Liu Qi-Xu, Zhang Yu-Qing. A research of discovering vulnerabilities of NFC applications on Android platform. Journal on Communications, 2014(Z2): 117-223 (in Chinese)
(王志强，刘奇旭，张玉清. Android 平台 NFC 应用漏洞挖掘技术研究. 通信学报，2014(Z2)：117-223)

[47] Zhu Lu. Researches on Some Key Techniques of Trusted Computing Architecture[Ph.D. dissertation]. Wuhan University, Wuhan, 2010(in Chinese)
(祝璐. 可信计算体系结构中的若干关健技术研究[博士学位论文]. 武汉大学，武汉，2010)

[48] Zhang X, Aciicmez O, Seifert J-P. A trusted mobile phone reference architecturevia secure kernel//Proceedings of the 2007 ACM Workshop on Scalable Trusted Computing. Virginia, USA, 2007: 7-14

[49] Kim M, Ju H, Kim Y, et al. Design and implementation of mobile trusted module for trusted mobile computing. IEEE Transactions on Consumer Electronics, 2010, 56(1): 134-140

[50] Enck W, Ongtang M, Mcdaniel P. Understanding Android security. IEEE Security & Privacy, 2009(1): 50-57

[51] Stamp M. Information Security: Principles and Practice. Beijing: Tsinghua University Press, 2013(in Chinese)
(斯坦普. 信息安全原理与实践. 北京：清华大学出版社，2013)

[52] Blasing T, Batyuk L, Schmidt A-D, et al. An Android application sandbox system for suspicious software detection//Proceedings of the 5th International Conference on Malicious and Unwanted Software (MALWARE). Nancy, France, 2010: 55-62

[53] Spreitzenbarth M, Freiling F, Echtler F, et al. Mobile-sandbox: Having a deeper look into Android applications//Proceedings of the 28th Annual ACM Symposium on Applied Computing. Coimbra, Portugal, 2013: 1808-1815

[54] Felt A P, Wang H J, Moshchuk A, et al. Permission re-delegation: Attacks and defenses//Proceedings of the 20th USENIX Security Symposium. Berkeley, USA, 2011: 19-31

[55] Canetti R. Universally composable signature, certification, and authentication//Proceedings of the Computer Security Foundations Workshop. California, USA, 2004: 219-233

[56] Nagao W, Manabe Y, Okamoto T. A Universally Composable Secure Channel Based on the KEM-DEM Framework, Theory of Cryptography. New York: Springer, 2005

[57] Whittaker J A. Exploratory Software Testing. Beijing: Tsinghua University Press, 2009(in Chinese)
(惠特克. 探索式软件测试. 北京：清华大学出版社，2009)

[58] Sutton M, Greene A, Amini P. Fuzzing: Brute Force Vulnerability Discovery. Boston: Pearson Education, 2007

[59] Zhu X, Wu Z, Atwood J W. A new fuzzing method using multi data samples combination. Journal of Computers, 2011, 6(5): 881-888

[60] Wu Zhi-Yong, Xia Jian-Jun, Sun Le-Chang, et al. Survey of multi-dimensional Fuzzing technology. Application Research of Computer, 2010, 27(8): 2810-2813(in Chinese)
(吴志勇，夏建军，孙乐昌等. 多维 Fuzzing 技术综述. 计算机应用研究，2010，27(8)：2810-2813)

[61] Wichmann B, Canning A, Marsh D, et al. Industrial perspective on static analysis. Software Engineering Journal, 1995, 10(2): 69-75

[62] Livshits B. Improving Software Security with Precise Static and Runtime Analysis [Ph. D. dissertation]. Stanford University, California, 2006

[63] Bumbulis P, Cowan D D. RE2C: A more versatile scanner generator. ACM Letters on Programming Languages and Systems (LOPLAS), 1993, 2(1-4): 70-84

[64] Kong Ying. Static Detection of Web Vulnerabilities[Ph. D. dissertation]. University of Chinese Academy of Sciences, Beijing, 2012(in Chinese)
(孔莹. 基于代码分析技术的 Web 漏洞挖掘[博士学位论文]. 中国科学院研究生院, 北京, 2012)

[65] Hopcroft J E. Introduction to Automata Theory, Languages, and Computation. New Jersey: Addison Wesley, 1979: 185-192

[66] Rice H G. Classes of recursively enumerable sets and their decision problems. Transactions of the American Mathematical Society, 1953, 74(3): 358-366

[67] Huang J. Detection of data flow anomaly through program instrumentation. IEEE Transactions on Software Engineering, 1979, 5(3): 226-236

[68] Cui W, Kannan J, Wang H J. Discoverer: Automatic protocol reverse engineering from network traces//Proceedings of the USENIX Security. Boston, USA, 2007: 199-212

[69] Cui W, Peinado M, Chen K, et al. Tupni: Automatic reverse engineering of input formats//Proceedings of the 15th ACM Conference on Computer and Communications Security. Virginia, USA, 2008: 391-402

[70] Hall P A. Software Reuse and Reverse Engineering in Practice. London: Chapman & Hall, Ltd., 1992

[71] Comparetti P M, Wondracek G, Kruegel C, et al. Prospex: Protocol specification extraction//Proceedings of the 30th IEEE Symposium on Security and Privacy. Washington, USA, 2009: 110-125

[72] Santos I, Brezo F, Ugarte-Pedrero X, et al. Opcode sequences as representation of executables for data-mining-based unknown malware detection. Information Sciences, 2013, 231: 64-82

[73] Bose A, Hu X, Shin K G, et al. Behavioral detection of malware on mobile handsets//Proceedings of the 6th International Conference on Mobile Systems, Applications, and Services. Colorado, USA, 2008: 225-238

[74] Burguera I, Zurutuza U, Nadjm-Tehrani S. Crowdroid: Behavior-based malware detection system for Android//Proceedings of the 1st ACM Workshop on Security and Privacy in Smartphones and Mobile Devices. Chicago, USA, 2011: 15-26

[75] Kim H, Smith J, Shin K G. Detecting energy-greedy anomalies and mobile malware variants//Proceedings of the 6th International Conference on Mobile Systems, Applications, and Services. Breckenridge, USA, 2008: 239-252

[76] Schmidt A-D, Bye R, Schmidt H-G, et al. Static analysis of executables for collaborative malware detection on Android//Proceedings of the 9th IEEE International Conference on Communications. Dresden, Germany, 2009: 1-5

[77] Wu D-J, Mao C-H, Wei T-E, et al. Droidmat: Android malware detection through manifest and API calls tracing//Proceedings of the 7th Asia Joint Conference on Information Security (Asia JCIS). Tokyo, Japan, 2012: 62-69

[78] Xie L, Zhang X, Seifert J-P, et al. pBMDS: A behavior-based malware detection system for cellphone devices//Proceedings of the 3rd ACM Conference on Wireless Network Security. New Jersey, USA, 2010: 37-48

[79] Shabtai A, Fledel Y, Elovici Y. Automated static code analysis for classifying Android applications using machine learning//Proceedings of the International Conference on Computational Intelligence and Security (CIS). Nanning, China, 2010: 329-333

[80] Finkelstein L D, Gutman J, Puhl L, et al. Electronic wallet. Motorola: Illinois, Technical Report US5221838, 1993

[81] Sasaki O, Matsuse T, Takayama H, et al. Electronic ticket, electronic wallet, and information terminal. Osaka: Osamu Matsushita Electric Ind. Co. Ltd, Technical Report: US 7392226, 2008

ZHANG Yu-Qing, born in 1966, professor, Ph. D. supervisor. His research interests include cryptography, information security and network security.

WANG Zhi-Qiang, born in 1985, Ph. D. His current research interests includes system security and network security.

LIU Qi-Xu, born in 1984, Ph. D., lecturer. His current research interests include vulnerability discovering, vulnerability assessment and emergency response.

LOU Jia-Peng, born in 1977, M. S. His current research interests includes system security and network security.

YAO Dong, born in 1975, M. S. His current research interests focus on information security.

Background

As NFC(Near Field Communication) is becoming more and more popular with banks, mobile operators and manufacturers, its security has also attracted security researcher and attackers due to its wide application perspective. The attacks

aimed at NFC payment and other NFC-related applications have also emerged one after another for the reason that NFC involves mobile payment and sensitivity information transmission. Researchers in academia and industry have done lots of work on enhancing the security of NFC from all kinds of aspects. However, there is no a thorough and detailed analysis on current research progress and development trends of NFC security. To solve this problem, the paper analyzes and summarizes the latest research results, and prospect a further research on NFC security in the future. The paper firstly introduces NFC's basic features, communication process, protocol stack, operation mode and so on, analyzes security threats faced by NFC. Then, the research status and progress of NFC security are summarized by analyzing the related research work. Finally, from the point of view of security threats, the future research directions cover research contents and methods on secure channels, vulnerability discovering, secure element, malware detecting, malicious content detecting, mobile payment and so on.

We have done a series of studies on NFC security from the point of vulnerability discovering, and lots of vulnerabilities on Windows Phone OS, Android OS, other customized OSs based on Android, NFC payment and other applications. The vulnerabilities cover DoS(denial of service), opening wifi, bluetooth or other capability leaks, causing a mobile phone screen black and so on. Furthermore, we give some suggestions and measures for fixing these vulnerabilities. Based on above research work and related work of experts and scholars at home and abroad, we analyzes and summarizes the latest research results, and prospect a further research on NFC security.

This research was supported by the National Natural Science Foundations of China (61303239, 61272481, 61572460) and Reform Commission Special Notice of Information Security ([2012]1424).