

面向现场模式的NFC智能手机移动支付安全研究

赵洪坡

南昌理工学院 江西南昌 330044

摘要: 移动支付的使用方法多种多样,但是,在面向一般用户的微型支付方面,利用NFC技术来实现移动支付具有天然的优越性,并与智能手机的使用相结合;它使“手机卡”和“钱包”成为一体,推动了“智能化”的发展。在此基础上,提出了一种适用于手机的安全支付方法。这对大部分的手机用户来说,都是一件很有价值的事情。在NFC技术架构和安全支付的特性基础上,对已有的移动支付系统进行了深入的研究,最后对移动支付的安全应用解决方案和安全性进行了探讨。

关键词: 移动支付; NFC; 支付安全

Research on NFC smart phone mobile payment security for field mode

Hongpo Zhao

Nanchang Institute of Technology Nanchang, Jiangxi 330044

Abstract: There are various methods for using mobile payments. However, when it comes to micro payments for general users, utilizing NFC (Near Field Communication) technology for mobile payments has inherent advantages and can be combined with the use of smartphones. It integrates the “phone card” and “wallet,” promoting the development of “smart” capabilities. Building upon this, a secure payment method suitable for mobile phones is proposed, which is of significant value to the majority of smartphone users. Based on the architecture of NFC technology and the characteristics of secure payments, in-depth research is conducted on existing mobile payment systems. Finally, the paper discusses security application solutions and the security aspects of mobile payments.

Keywords: mobile payment; NFC; Payment security

引言:

随着移动银行、微信支付、移动钱包等服务的推广和使用,越来越多的新兴服务开始出现。手机支付业务已深入到人民群众的日常生活中。手机支付的迅速发展,不断改善的网络基础结构。艾瑞顾问公司的一项研究表明,手机网络技术与电商行业正处于快速发展阶段。我国2013年移动互联网市场规模达到1059.8亿元。预期到2017年,该产品的市场份额将达到4个百分点。翻了5倍,也就是将近6万亿人民币。在这当中,随着互联网用户数量的增加,智能电话的数量也在迅速增加。移动购物、移动营销、移动营销都同时为移动付款的扩大打下了坚实的基础。手机上网市场正步入快速增长的正轨,

手机付款的时代来临了。

人们可以利用带有近场通信技术的移动电话,通过移动电话来购票。利用自己的手机,可以在网络上进行各种在线交易,也可以在银行卡上进行快速付款。商业旅行、行程安排、住宿安排等,只要用移动电话,就能很容易地完成付款。换言之,近距离通信技术在将来的应用将大大增加,还给手机支付带来了新的发展空间。

一、NFC的移动支付基本原理

在手机上网时代,手机成为人们日常生活中最常用的支付方式之一。当前,移动支付有两种形式:一种是利用手机网络实现的远距离支付,另一种是利用NFC技术实现的近距离支付。像手机支付宝,微信支付这样的支付方式,都是以网络为基础的远距离支付技术,随着远距离支付技术的发展,其交易规模和使用人数也在持续增长。其中,以苹果包为代表的近距离支付技术发展,

2022年度江西省教育厅科学技术项目编号: GJJ2202715.

项目名称: NFC移动支付在智能手机中的应用与前景分析。

是当前一个热门领域。

近场通信(NFC)是采用无线电频率(RFID)技术实现的一种短程、无接触、无干扰的通讯方式,其通讯范围通常不超过10厘米,具有106 kbps、212 kbps和424 kbps等特点,被广泛用于手机等移动终端。当前,NFC技术正在逐步地在手持设备中普及,用户可以使用NFC支付,在进行消费或者购买商品的时候,可以使用手机等手持设备来进行支付,可实现近场联机支付,也可以进行离机支付。在离机支付时,NFC支付技术不需要使用移动网络,采用RF装置与POS终端进行通信,实现付款,加快付款速率,降低网络传输成本。

NFC支付技术是基于RFID的非接触性无线电波技术而发展出来的一项互联技术,它兼具了RFID多种形式的优势,与RFID的区别就是NFC有三种工作模式:模拟卡、阅读器、点对点。卡模拟模式是将具备NFC支付功能的手机模拟为非接触式的IC卡,只要将手机靠近POS机,就可以通过无线射频技术实现支付。阅读器模式是一种手机付款装置,它拥有IC卡读取、NFC贴纸、电子招贴画等多种功能,用户可以通过手机查看特定的交易内容。所谓“点对点”,就是指在具备近场通信能力的各种电子装置间,通过这种方式,可以实现各种类型、各种功能的装置间的信息交流。

NFC的通讯方式有两种,一种是无源通讯,另一种是有源通讯。被动通信指的是:NFC终端产生一个无线电频率,另外一方可以利用这个无线电频率来获得能量,并将信息调制与磁场产生装置进行交流,这是在卡模拟模式和读写模式中经常使用的一种通信方式。而主动通信指的是,在进行数据交换的过程中,可以通过数据来获得数据。这就对数据交换的双方都是有源性的设备提出了需求,与此同时,在数据传输的过程中,还会有一些数据传输过程,多用于点对点的通讯方式。

二、基于NFC技术的手机支付面临的问题

尽管近距离通信技术有很多优点,其技术也很先进。但是,也有值得关注的安全问题。手机上的数据安全问题由来已久。从手机网络技术和电子商务开始,手机的电子付款也开始出现。在移动支付的发展中,安全一直是各方最关注的问题,伴随着移动支付使用人数的增加,它的安全缺陷也在不断地暴露出来。针对移动支付的特点,新型病毒与新型科技骗局层出不穷,其受到的威胁也很特殊。包含下列要素:

- 1.资料的保密性,当使用者传送资料时,若未做保密性处理,那么未经许可的攻击就会被拦截,并且会窃取合法使用者的私密资料,比如使用者的银行账号,1:3的付款方式等等。

- 2.资料整合。确保真实的信息在完整且无损坏的状态下从发送方到达合法的接收方,以避免在买方与支付

处理平台之间传输的信息遭到篡改、插入、删除等破坏。

- 3.非抵赖的资料。保证在买方和卖方之间进行的一切信息都是以无法否认的记录为基础的。避免买方和卖方对其所发出或所收到的讯息做出否认。手机支付的普及。同时,由于无线网络技术和无线网络的特殊性,使得无线网络中存在着大量的信息被窃听和篡改等安全隐患。

所谓的“偷听”,就是不法的攻击者使用类似于“监视器”这样的技术手段,在两终端间进行近距离的信息传送,而传送的信息并未进行任何加密运算。这样,只要传输的资料被加密,攻击者就可以轻易地从非法的监听器中获知传输的资讯。这并不代表着绝对的安全。在加密器所选取的密码键比较短时。这样的话,攻击方很有可能会猜到密码,密文很容易就被破解了。即便传输的资料是经过加密的。同样也是危险的。尤其是在NFC无接触的卡片方式下。因为NFC装置在这种情况下是不工作的。如果是这样的话,他传输的信息很有可能会被偷走。

三、基于NFC的移动支付安全解决方案

在此基础上,本文提出了一种新的移动通讯系统。由于用于实现移动支付的协议也在持续更新,这篇文章就将重点研究其中的一种点对点的近距离通信技术(NFC)在移动支付的应用过程 and 安全性。针对目前NFC手机付款的安全性问题,给出了一种行之有效的、切实可行的方法,构建了一套以近场通信为基础的手机支付的安全性体系。

移动支付处理系统的主体包括四个方面:使用者(即消费者)、商家、移动支付处理中心和银行。他们每个人都有自己的责任。银行的功能是对顾客和商户的账户进行转账,帮助顾客和商户完成手机支付的顺畅转账。顾客和商户是手机支付流程中最重要的角色。每一方都要成为一家银行的用户,与其签订了手机付款的协议。

凭证服务器会按照验证服务器所发布的验证凭证进行验证,为客户和商户间的银行账户进行有关业务的转账。所以手机付款的加工中心,除与使用者的终端机及商户的联结外。同时也要求与众多的金融组织进行协作。对于每一个参与者来说,在一个以NFC技术为基础的手机支付程序中,可以实施一个跨线的手机现金支付业务。手机付款的办理和商户的身份都经过了合法的认证,然后就可以放心使用。当使用者的NFC手机在手机支付中心登记完毕后。使用NFC装置的标识与使用者的银行账户相关的特点,可以随时进行数据和信息的传输,实现了以近距离通信为基础的手机支付系统。NFC安全性的移动支付流程可以由两个步骤组成:一个是对用户进行身份验证,另一个是对用户进行交易。

- 1.用户将其验证要求以密码的方式向手机支付处理器发出,处理器经过特定的方式进行验证,当前较为成熟的方法是采用Kerberos认证技术,通过验证服务器对用户的身份进行验证。手机付款系统会把确认的凭证发

给商户，商户经确认后即可完成付款，反之则取消付款。

2. 在通过了身份验证的合法性后，选择了该商户的货物，并向该商户发出了采购指示信息。之后，由商户将顾客的购买指示以及有关的信息交给了移动支付处理中心，而移动支付处理中心将购买信息发送到了顾客的手机上，要求顾客对其进行确认，如果顾客始终没有得到顾客确认的答复信息，那么就会被终止。在用户确定了所购买的信息无误后，将其发送到商户，商户将此信息传递到移动支付处理中心，从而要求用户进行移动支付。在接到处理中心的支付通知之后，消费者利用自己的移动终端，将自己的开户银行卡账号、密码等支付信息，发送到移动支付处理中心，然后由其向其开户的支付服务提供商（银行）进行兑换支付。在银行兑换支付之后，移动支付处理中心便会告知商户支付交易完成，可以交付货物，并将相应的交易和支付记录保存下来，方便消费者进行查询。到此，手机付款的整个流程就完成了。

在以上的流程中，以信息传输安全的思想为基础，参与者必须是经过身份认证机制识别的合法用户，消费者使用NFC技术，在手机终端和商户NFC设备之间，可以进行近距离的重要信息交换，利用3G移动网络，在用户的手机终端和移动支付处理中心的服务器之间，可以

进行数据加密传输，从而增强了用户的信息安全性。在整体的移动支付体系中，近场通信技术不仅可以使使用者成为一张方便的付款卡片，而且还可以让使用者通过商店的近场通信装置进行非接触式的信息交流。在整个消费过程中，可以将用户的快捷消费和商家的便利收取都展现出来，让每个人在日常生活中都可以随时获得便利的服务，同时还可以与移动运营商和银行一起，更好地扩展其业务范围，这也是NFC被广泛接受的原因。

在各个实体进行信息交流的过程中，网络是数据信息交互传递的桥梁，快速的数据传输速度和安全可靠的网络质量是实现移动支付不可或缺的要害。目前，NFC的整体支持环境可谓是一应俱全。具有近距离通信功能的智能电话终端不断涌现，相应的标准也不断制定。伴随着移动互联技术的不断发展，现在用户的移动终端，比如安卓系统的智能手机都拥有NFC功能，并且智能终端支持的移动网络也可以实现移动支付。

四、面向现场模的NFC的移动支付用户验证方法

在利用NFC进行信息移动支付时，必须要对用户的身份进行认证，确认其信息的合法与否，判断其是否具备服务权限，这是一个对其进行认证的过程。以下是当前常见的身份验证方法：

表1 常见身份认证方式

| 身份认证方式 | 安全性特点 | 环境需求 | 缺点 |
|--------|---------------------------|---------------|--------------------------|
| 用户密码 | 密码窃取安全性低 | 方便 | 安全性低 |
| 数字证书 | 采用非对称密码保证信息的完整性、不可抵赖性、保密性 | 方便用户将密钥导入终端 | 成本高，维护成本高 |
| 短信动态验证 | 可变动态指令，安全性高 | 需要用手机短信接受动态口令 | 网络环境不好或者服务器访问量过大时无法接受指令。 |
| 智能IC认证 | 安全性高 | 采用硬件加密 | 成本较高，需要专门的硬件设备 |
| 指纹验证 | 具有唯一性 | 需要设备支持 | 需遴选设备和软件，成本较高。 |

NFC手机与POS机进行交易时，首先要对手机的身份进行认证。在此流程中，若使用设定好的会话密钥来对互动信息进行加密，在进行身份验证的时候，要对使用者的身份信息加以保护，这样就能确保资讯互动的安全性，保障使用者的资讯安全性。

五、结束语

本文提出了一种利用NFC近场通信技术来实现移动支付的安全机制，可以确保在支付的过程中，移动用户的信息传递的安全性，从而提高传输的整体效率和安全性，有效降低整个信息传递过程中系统的功耗，解决在传统的移动支付过程中，存在的连接时间长、操作复杂、系统功耗大等问题，基本满足了用户信息安全传递的需要。然而，NFC在手机付款方面的发展仍是一个比较敏感的问题，也是一个长期而艰巨的任务。要进行主动的协作，这不但要有技术厂家的持续开发，还要有移动运营商对移动支付网

络的大力推进，还要有手机制造商对其所生产的手机NFC功能装备进行改进。银行等金融机构要与NFC技术的移动支付保持紧密的合作关系，并要建立起相应的配套基础设施。对于那些使用NFC手机进行移动支付的用户来说，他们要增强自己的安全意识，要主动地去面对各种可能的威胁，不让自己的NFC手机遗失或被盗。同时，也应加强对其的规范与规范，加强对其的规范。NFC近场通信技术有望在未来的几年内占据主导地位，并在未来占据主导地位。

参考文献：

- [1] 庞贝宁, 庞秀平. NFC移动支付安全问题探究[J]. 合作经济与科技, 2019, (04): 72-73.
- [2] 欧阳秉炎. NFC技术在移动支付中的应用[J]. 广东通信技术, 2020, (06): 67-69.
- [3] 韩子康, 陈金鹰, 徐曾萍. 基于NFC的移动支付系统探究[J]. 信息化建设, 2018, (10): 81.