文章编号：2095-2163(2020)03-0367-04 中图分类号：TP393.08 文献标志码：A

NFC 移动支付的安全威胁和安全技术研究

张梦飞
（哈尔滨工业大学 计算机科学与技术学院，哈尔滨 150001）

摘 要：随着移动互联网的发展，尤其是智能手机的普及，NFC 移动支付逐渐成为一种主流的移动支付方式。但是由于 NFC 技术还不完善，所以还存在很多的安全威胁，严重制约着 NFC 移动支付的发展。为了保障 NFC 移动支付的数据安全和用户的隐私，本文提出了使用数据加密、随机数、书籍签名等几种安全技术，并分析了这些安全技术在应对安全威胁方面的有效性。相信通过这些安全技术的应用的使用，有助于构建一个更加安全的 NFC 移动支付系统。

关键词：NFC；移动支付；安全威胁；数据加密；安全技术

Research on security threat and security technology of NFC mobile payment

ZHANG Mengfei
（School of Computer Science and Technology, Harbin Institute of Technology, Harbin 150001, China）

【Abstract】 With the development of mobile Internet, especially the popularity of smart phones, NFC mobile payment has gradually become a mainstream mobile payment method. However, due to the imperfect NFC technology, there are still many security threats, which seriously restricts the development of NFC mobile payment. In order to protect the data security of NFC mobile payment and the privacy of users, this paper proposes several security technologies such as data encryption, random number and book signature, and analyzes the effectiveness of these security technologies in dealing with security threats. It is believed that the use of these security technology applications will help to build a more secure NFC mobile payment system.

【Key words】 NFC; mobile payment; security threat; data encryption; security technology

0 引 言

随着无线通信技术和移动互联网技术的发展，尤其是智能手机的普及，移动支付正在迎来空前的多样化的发展。按照支付所依托的技术条件又可以分为 2 种支付方式，即：远程支付和 NFC 近场支付。以现在移动支付的发展状况来看，目前技术最成熟，应用最广泛的还是基于远程的支付方式，其中以通过 QR 码技术实现的微信、支付宝支付为代表，已经在生活的众多场景中投付使用。但是基于 NFC 的移动支付由于其安全性更好，操作更方便等优点，目前已经在公共交通、餐饮、零售等行业取得了很大的应用进展。

根据艾瑞咨询公司发布的《中国移动 NFC 支付行业研究报告》[1] 显示，在 2017 年中国使用 NFC 移动支付的金额规模达到了 48.9 亿元，而仅在 2018 年第一季度，这一数字就已经达到了 28.9 亿元。

1 NFC 移动支付基本原理

1.1 NFC 工作基本原理

NFC 的概念是在 2004 年 3 月由飞利浦半导体、诺基亚和索尼三家公司共同参与研制开发。是通过无线射频识别（RFID）和互联技术的融合而产生的新技术，是一种工作在较短距离的无线通信技术标准。通过在单一芯片上集成了感应式读卡器、感应式卡片和点对点通信的功能，运行工作频率为 13.56 MHz，能在大约 10 cm 范围内建立设备之间的连接，传输速率可为 106 Kbit/s、212 Kbit/s、424 Kbit/s，未来可提高到 848 Kbit/s 以上。

NFC 终端有 3 种工作模式：

（1）读/写模式：NFC 终端作为一个读卡器，可以读写银行卡、支持 NFC 的标签以及工作在卡模拟模式下的其他 NFC 设备。

（2）卡模拟模式：将 NFC 终端模拟成一个非接触的智能卡，当卡模拟模式下的终端靠近读卡器终端时，可以像普通的卡片一样实现相应的功能。

（3）点对点模式下：2 个支持 NFC 功能的终端通过进行点对点通信来完成信息传输。

NFC 标准的制定，主要有飞利浦、诺基亚、索尼牵头组建的 NFC 的标准化组织 NFC Forum（NFC 论坛），欧洲计算机制造商协会 ECMA，和国际标准化组织 ISO 这三家。先后演化出 ISO1443、ISO18092、ISO15698、ISO 21481[2-3] 等标准。

NFC 三种工作模式和支持的标准格式如图 1 所示。

作者简介：张梦飞（1990- ），男，硕士研究生，主要研究方向：NFC 移动支付。

收稿日期：2019-06-12

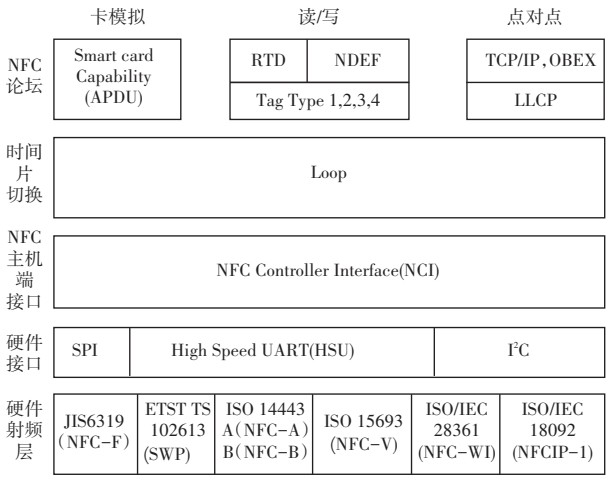

图 1 NFC 技术标准和工作模式

Fig. 1 NFC technical standards and working modes

NFC 通信模式按照是否产生射频场和提供能量可以分为 NFC 被动通信和 NFC 主动通信两种模式[3]。文中将展开研究论述如下。

(1)被动通信模式。被动通信是指在整个通信过程中,能量源由发起方提供,而目标方不产生能量,而是从发起方 RF(射频)场获得能量,并且使用耦合的方式,以相同的速率将数据回传给发起方。这里的目标方可以是有源设备如卡模拟模式下的智能手机等,也可以是诸如 NFC 标签、银行卡等无源设备。

(2)主动通信模式。主动通信模式是指发起方和目标方在传输数据时都要提供能量。当发起方发送数据时,将产生自己的能量场,而接收方则以侦听模式接收发起方的数据。当发起方发送完数据后,将关闭自己的能量场并调整为侦听模式,等待接收方发送数据。反之,接收方在进行数据应答时要和发起方采取同样的策略。

1.2 NFC 移动支付基本流程

NFC 移动支付即近场支付,是一种非接触式的支付方式, NFC 移动支付的系统架构[4]如图 2 所示。由图 2 可知,该系统中各部分的功能设计可阐释分述如下。

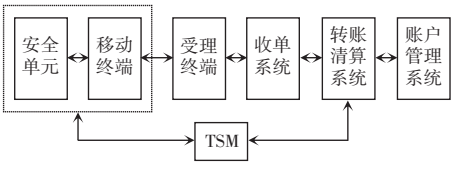

图 2 NFC 移动支付系统架构

Fig. 2 NFC mobile payment system architecture

(1)移动终端:指在移动支付过程中,用户所使用的移动支付终端设备,一般为支持 NFC 功能的智能手机。

(2)受理终端:通常是指参与移动支付交易的商家使用的终端设备如 POS 机等。

(3)收单系统:一般负责产生和转发交易信息,收集、整理和提交结算数据等。

(4)转账清算系统:指实现账务的转接和结算功能的系统。

(5)账户管理系统:指提供资金管理和账务结算的系统,如银行等。

(6)TSM:第三方可信服务平台,如支付宝、手机钱包等,可以实现移动支付安全管理。

(7)安全单元:用于存储安全敏感的数据或者用户的隐私数据等,如交易的关键数据,用户的银行卡信息等,确保敏感数据和用户隐私的安全性和交易的不可否认性。安全单元以 SIM 卡、SD 卡或单芯片的形式存在。

NFC 移动支付的在线交易流程如图 3 所示,详细步骤具体如下。

步骤 1 用户将移动终端放置于受理终端无线射频场中,受理终端向安全单元发送命令,以获取发起交易所需的数据信息。

步骤 2 安全单元响应由受理终端发起的交易命令,并将处理结果返回受理终端。

步骤 3 客户端提示用户本次交易的结果(此步骤可选)。

步骤 4 受理终端向收单系统发起交易请求,收单系统请求账户管理系统获取交易结果。

步骤 5 收单系统向受理终端返回交易结果,然后受理终端就可以显示交易结果。

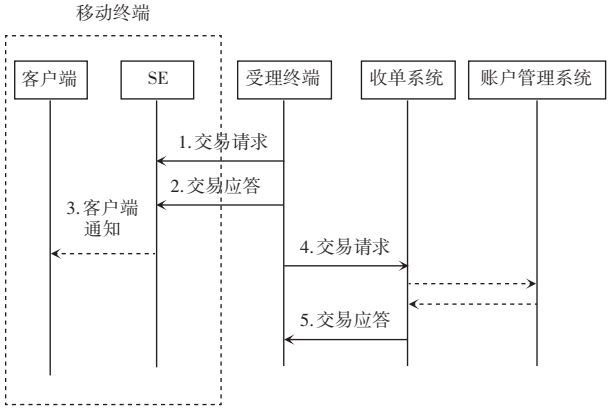

图 3 NFC 移动支付交易流程

Fig. 3 NFC mobile payment transaction process

2 NFC 移动支付的安全威胁

研究中,目前对于 NFC 移动支付中面临的安全威胁给出了探讨总述如下。

(1)窃听。窃听是指在 NFC 移动支付交易期间,攻击者用特殊手段获取交易数据或者是卡片信息,并对其进行分析,导致用户隐私信息泄露。虽然 NFC 是近距离通信,但是由于其射频场是开放的,因此就给居心不良者提供了攻击可能,攻击者可能通过一些特殊装备获得设备正在传输的信息。由于现在 NFC 技术并没有对数据加密提出要求,而且很多情况下数据的传输都是以明文传递的,这就极大地增加了数据被窃听的风险。

(2)重放攻击。重放攻击主要是发生在消息被攻击者窃听之后的下一轮会话中。当攻击者通过窃听获得了通信双方的交互信息之后,就把窃听到的数据原封不动地重新发送给接收方。由于重放的信息是双方约定的合法的信息,因此往往能达到欺骗接收方的目的,这样就破坏了双方的身份认证,影响了认证的准确性给系统造成了额外的负担。

(3)消息篡改。消息篡改是指攻击者再截获发送方发送的数据之后,然后对数据进行篡改发送给消息原本的接收方。数据篡改的形式有:插入无效数据、删除关键数据以及对数据的恶意修改,如在支付过程中攻击者对双方的交易信息或者银行账号进行修改,使得双方无法达成交易或者产生错误的交易,从而造成被攻击的财产损失。

(4)中间人攻击。中间人攻击[5]分为 2 种方式。第一种能够是在双方传输数据的过程中发生的中间人攻击。在第三方攻击者获取到了交易双方中的任一方的合法身份标识信息之后,就可以通过身份信息伪装成合法终端骗取另一方的信任,完成与另一方的信息交互。第二种是通过恶意程序的攻击。具体表现为攻击者利用恶意应用,应用协议数据单元(APDU)命令向安全单元调用数据请求,当安全单元响应之后,恶意应用程序就把得到的回应信息转发给第三方攻击者,这样攻击者就获得了交易的敏感信息。

(5)交易抵赖。交易抵赖是指参加交易的双方参与者,拒绝承认参与过交易行为,以此来逃避交易过程中产生的资金转移,达到逃避支付的目的,但是对交易的另一方却造成了财产损失。

(6)拒绝服务。拒绝服务(DOS 攻击)主要可以通过 2 种形式实现。一种是通过硬件实现,攻击者采用额外的硬件通过不停地读取交易方的标签或者强制让交易方不停地读取自己的标签,造成交易的一方无法和对方取得交互,从而达到破坏交易的目的。另一种是通过软件层面实现。攻击者通过向交易一方发送超大规模的数据量,造成交易者不得不耗费大量资源来处理这些数据,从而占用了大量的资源,而没有办法响应另一方的请求信息,以此达到破坏交易的目的。

3　应对安全威胁的安全技术

(1)公钥私钥密码体系。公钥私钥密码体系是通过某一种加密算法得到一个公钥和一个私钥,其中公钥是密钥对中公开的部分,任何人都可以看到,私钥则是不公开的部分,只有拥有者自己知道。公钥通常用于会话数据加密、数字签名验证等,公钥加密的信息可以用相应的私钥解密的数据。而私钥加密的数据,就必须使用公钥才能解密。

采用这种技术对 NFC 的设备信息、交易数据、银行卡信息进行加密,由于攻击者不知道私钥,所以就可以有效应对窃听、消息篡改等攻击手段,实现数据的安全传输和数据的保密性。

(2)数字签名。数字签名,是将普通签章的数字化,数字签名就代表了签名者的身份。其特性是制造签名非常容易,但仿冒签名就非常困难。数字签名可以与被签署的信息结合起来,且没有办法从信息上移除。数字签名包含 2 个算法:其一是签署算法,使用私钥对信息或者信息的哈希值进行处理来产生签名;其二是验证算法,使用公钥来验证经过签名的数据的真实性。

采用数字签名技术,可以有效验证 NFC 支付系统各个参与者的身份,由于签名的不可仿冒性,从而可以避免中间人攻击,又可以认证交易证的身份使交易行为不可抵赖。

(3)随机数技术。在 NFC 支付的消息传递过程中,除了传递交易相关的数据之外,还可以在每一次数据传递中还要额外增加一个或者多个实时变化的随机数,每一个角色都按照自己制定的规则生成随机数,在收到交易数据时可以对比数据中的随机数是否是自己生成的。

采用随机数技术,一方面可以保证数据的安全性,使攻击者即使窃取到了消息,也无法对消息进行伪造,从而避免了消息篡改。又由于随机数是实时可变的,因此使得攻击者没有办法进行重放攻击。

(4)匿名化。在客户进行交易的时候,使用的是自己的假名或者是虚拟 ID,而客户的真实身份信息,只有银行或者可信认证平台知道。用户的假名和真实身份之间没有任何必然联系。用户在交易系统中使用假名进行交易,而在结算时银行会验证假名的真实性并根据假名计算用户的真实身份信息。

即使攻击者得到了用户的假名,也不知道客户的真实身份,所以也无法通过银行验证。

通过匿名化技术保护了用户的隐私和用户的账户安全。保证了系统的整体的安全性和身份的不可伪造性。

(5)组签名。在组签名系统中,任何组的合法成员都可以代表组生成匿名的签名,并且验证者可以使用组公钥来检查组签名的有效性[6]。验证者可以验证签名是否由组成员签名,但不能知道谁签署了该消息以为客户提供匿名,并且也不能链接同一客户的不同交易以提供不可链接性。小组管理者可以通过签名来验证签名者的身份,因此签名者不能否认自己的签名。通过组签名既保证了组成员的匿名性,又保证了可追溯性,合法用户可以通过其匿名性得到保护,可追溯性可以对用户的非法行为进行跟踪。

采用组签名策略可以有效防止身份冒用,从而避免中间人攻击、数据篡改等。也保证了系统的整体的安全性和交易的不可抵赖性。

(6)AES 和 ECC 混合加密算法。首先,在数据传输过程中采用 AES 算法对 NFC 移动支付中的数据进行加密,然后用 ECC 算法对 AES 算法的密钥进行加密管理;其次在解密时,先通过对 ECC 算法的解密得到 AES 算法的密钥,然后通过得到的 AES 密钥再对数据进行解密[7]。这样不仅保证了数据传输的安全可靠,同时也兼顾了加密和解密的速度。

通过混合加密可以更加有效地保证数据在传输过程中的安全,有效应对窃听、消息篡改等威胁。

(7)HMAC 消息认证技术。HMAC 消息认证技术的基本原理是:发送方和接收方在进行消息传送之前要事先确定一个 Hash 函数,这个 Hash 函数主要用来计算传输信息的摘要值。发送方首先利用会话的密钥,从摘要值中计算出认证码,然后再将包括认证码在内的全部信息发送给接收方。接收方在收到发送方发来的数据之后,首先根据约定好的散列函数获取到摘要值,再通过密钥解密出发送发来的认证码,然后判断收到的认证码和密钥解密出来的摘要值是否一致。如若一致,则说明数据在传输过程中没有被攻击认证有效。否则,这说明消息被攻击,认证无效。HMAC 消息认证技术保证了身份的认证性。

4 结束语

目前,手机已经像钱包一样与人形影不离,甚至使用的频率比钱包还要多[8]。NFC 移动支付是将 NFC 技术应用到移动支付交易流程中的技术手段。NFC 移动支付中的安全威胁主要存在于 NFC 设备之间的交互中。本文主要介绍了 NFC 的基本工作原理,NFC 移动支付的主要流程,列举了 NFC 移动支付过程中主要存在的安全威胁,并提出了采用公钥密钥加密、随机数、匿名化、群组签名、AES 和 ECC 混合加密算法等应对安全威胁的安全技术,并分析了安全技术切实的可能性。如果将这些安全技术,应用到完整的交易系统中,则能够形成一个安全的 NFC 移动支付系统。

参考文献

[1] 上海艾瑞市场咨询有限公司. 艾瑞咨询系列研究报告(2018 年第 6 期)[R]. 北京:上海艾瑞市场咨询有限公司,2018.

[2] 杨军. NFC 技术的应用、标准进展及测试[J]. 现代电信科技,2009,39(10):1.

[3] 王三元, 程代伟. NFC 技术发展与应用[J]. 北京电子科技学院学报, 2016,24(4):44.

[4]王淼. NFC 技术原理与应用[M]. 北京:化学工业出版社,2014.

[5]贾凡, 佟鑫. NFC 手机支付系统的安全威胁建模[J]. 清华大学学报(自然科学版),2012(10):1460.

[6] ATENIESE G, CAMENISCH J, JOYE M, et al. A practical and provably secure coalition-resistant group signature scheme[C]// The 20th Annual International Cryptology Conference. Santa Barbara, CA, USA:dblp, 2000: 255.

[7] 缪昌照,徐俊武. AES 与 ECC 混合加密算法研究[J]. 软件导刊,2016,15(11):63.

[8] 张素娜, 贾利军, 张怀武, 等. NFC 手机研究进展[J]. 通信技术, 2012, 45(12):134.

(上接第 366 页)

[2] 李月,陆杰华. 我国老年人社会参与:内涵、现状及挑战[J]. 人口与计划生育,2018(11):14.

[3] 丁志宏. 社会参与对农村高龄老人健康的影响研究[J]. 兰州学刊,2018(12):179.

[4] 刘颂. 老年社会参与对心理健康影响探析[J]. 南京人口管理干部学院学报,2007(4):39.

[5] 郑晓冬,方向明. 社会活动参与对老年人健康的影响—基于 CHARLS 2011 数据的考察[J]. 哈尔滨工业大学学报(社会科学版),2017,19(2):16.

[6] 张莉,崔臻晖. 休闲活动对我国老年人认知功能的影响[J]. 心理科学,2017,40(2):380.

[7] 张祥晶. 积极老龄化战略下老年人政治参与状况及影响因素[J]. 中国老年学杂志,2018,38(20):5082.

[8] 谢云婷. 社会参与对老年人身心健康的影响—以南京市为例[J]. 现代交际,2018(9):79.

[9] 薛新东. 社会参与对我国中老年人认知功能的影响[J]. 中国卫生政策研究,2018,11(5):1.

[10]秦秋红. 我国农村女性空巢老人社区养老面临的问题及其解决[J]. 陕西师范大学学报(哲学社会科学版),2018,47(5):25.

[11]孙学娇. 城市空巢老人社会参与研究[D]. 淄博:山东理工大学,2010.