闪付卡重放攻击研究与 PBOC3.0 协议漏洞分析

闫 萌,邹俊伟,刘亚辉,冯 钒,朱 翀
(北京邮电大学 电子工程学院 通信与网络研究中心,北京 100876)

摘 要:基于 NFC(near field communication,近场通信)技术的闪付服务,即中国银联所推出的小额免密支付服务,在丰富人们生活的同时,也使得用户的个人信息和财产安全面临着威胁。对此,从闪付服务中可能的隐私泄漏点-闪付卡出发,设计了一个针对其进行重放攻击的模型,以及进行攻击所需的基于 PBOC3.0 协议的通信协议。在此基础上利用 PC 机及附属设备搭建环境,对闪付卡与收单方间合法通信过程进行了监听,并利用监听过程中所截留的数据,模拟了闪付卡扣款流程,实现了重放攻击。此外,通过对截留的通信数据的分析,并结合对 PBOC3.0 协议的研究,找到了 PBOC3.0 协议的漏洞。最后提出了针对闪付卡重放攻击的对抗措施,以及 PBOC3.0 协议的改进措施。

关键词:近场通信;闪付卡;PBOC3.0;重放攻击
中图分类号:TP39 **文献标识码**:A **文章编号**:1673-629X(2018)04-0148-04
doi:10.3969/j.issn.1673-629X.2018.04.031

Replay Attack Research on 'Quickpass' Card and Analysis on Weakness of PBOC3.0 Protocol

YAN Meng,ZOU Jun-wei,LIU Ya-hui,FENG Fan,ZHU Chong
(Communications and Networks Center,School of Electronic Engineering,Beijing University of Posts and Communications,Beijing 100876,China)

Abstract:'Quickpass',a service based on NFC (near field communication) which allows free pay under small amount of money launched by China Unionpay,has riched people's life,but also makes the users' personal information and property security under dreadful threats. For this,focused on one weak point of 'Quickpass',the 'Quickpass' card,we design a model for replay attack and its corresponding communication protocol based on PBOC3.0 protocol. With PC and its attached application we monitor the communication process between 'Quickpass' card and POS,and then describe a simulation of replay attack to Quickpass card with successful deduction. Through analysis of data caught and PBOC3.0 protocol,we have found the vulnerability of PBOC3.0. In the end,we put forward the measures against replay attack to 'Quickpass' card and improving PBOC3.0.

Key words:near field communication;'Quickpass' card;PBOC3.0;replay attack

0 引 言

近年来,越来越多的企业开始采用非接触式智能卡代替手输密码、磁条卡或纸质票卡,如公交卡、大学学生卡等。非接触式支付也随之越来越普及[1]。闪付(quick pass),是中国银联金融 IC 卡的非接触式支付产品应用,是一种新兴支付方式,可以使银行卡持有人进行快速的小额支付,而无需输入用户名和密码。这种支付方式在当今快节奏的生活中很受欢迎,但同时闪付技术也逐渐面临着安全威胁,大量用户的敏感信息面临着泄露的风险。由于闪付技术是以 NFC(near field communication,近场通信)技术为支撑,因此,针对 NFC 通信可能使用的攻击方式(如窃听、数据损坏、中继攻击、重放攻击等)都需要警惕[2]。

基于 NFC 技术的电子钱包应用 Google wallet,已被研究人员破解[3-4]。而其他支持 NFC 技术的手机,也有研究人员对其进行了破解,并找到了手机安全模块的漏洞[5-6]。以上相关信息表明,NFC 支付的安全漏洞,越来越成为攻击者的目标。对此,文中针对闪付技术中个人隐私可能的泄露点,及针对含有'QuickPass'标识的银联芯片卡(简称'闪付卡')的可能攻击方式,重放攻击,展开讨论。

收稿日期:2017-04-24 **修回日期**:2017-08-24 **网络出版时间**:2017-12-05
基金项目:国家自然科学基金(61471067)
作者简介:闫 萌(1993-),女,硕士研究生,研究方向为信息安全与智能卡;邹俊伟,讲师,研究方向为智能卡技术、信息安全与物联网。

网络出版地址:http://kns.cnki.net/kcms/detail/61.1450.TP.20171205.1433.094.html

1　NFC 技术概述及 NFC 支付

随着通信技术和金融业的高速发展,NFC 技术开始逐渐为人所熟知。它由 RFID 技术(radio frequency identification,非接触式射频识别技术)演变而来,是一种用于短距离内的高频无线电通信技术。应用了 NFC 技术的芯片卡如公交卡、校园一卡通以及带 NFC 功能的银行卡等可在短距离内识别兼容设备,进行数据交换,有一定的智能性。由于很多大范围系统都会使用 NFC 芯片卡,故针对 NFC 芯片卡的各类标准也应运而生。

EMV 标准是全球统一的对于支持 NFC 技术的银行卡,也针对非接触式智能卡,以及与其进行交互所需要的终端所制定的标准。“闪付”是中国银联的非接触式支付产品及应用,支持由 EMV 标准结合国情改进而来的 PBOC3.0 标准,其最大特征就是小额免密支付。因契合人们对快捷、高效支付的需求,银联“闪付”作为一种新兴支付方式发展迅猛。截至 2014 年一季度末,全国支持闪付服务的 NFC 终端已有近 300 万台。

随着闪付技术的高速发展,其安全问题也日益受到关注。由于闪付技术小额免密的特点,大部分闪付卡在接触式电子现金以及非接触 PBOC 环境下,都不需进行动态验证就可完成交易。文献[1,7-8]对 EMV 规范体系的安全性进行了探讨,并指出 EMV 规范的安全性和可能存在的漏洞。此外,也有许多研究者指出,NFC 技术易遭受窃听、数据损坏、中继攻击、重放攻击等的威胁[2],并提出了一些解决方案,如电磁屏蔽等[6]。

重放攻击是文中研究的重点。所谓重放攻击,就是攻击者通过窃听或者其他方式获得一个目的主机已接收过的包,并将其重新发送给对方,来达到欺骗对方的目的,主要用于身份认证过程。这种攻击方式可以绕过复杂的加解密过程,因而难于防范。文中基于 PBOC 规范规定的交互指令以及所设计的重放攻击模型,使用 PN532 模拟中间阅读器和中间标签,造成合法通信的假象,从而截取 NFC 阅读器读取闪付卡与收单方之间的通信数据。针对电子现金的消费功能,进行模拟攻击。

2　重放攻击模型及通信协议设计

2.1　重放攻击模型设计

构建的重放攻击模型如图 1 所示。reader 与主机和 ecard 共同构成攻击方,启用 NFC 技术与闪付卡进行 APDU 指令交互,对闪付卡与收单方合法通信进行监听并截留通信数据。卡片认为 reader 即是与其进行合法通信的收单方,与其进行数据交换。由终端发送指令给攻击者借此获得闪付卡与收单方之间通信的合法 APDU,再将监听到的 APDU 写成脚本,由主机假扮合法收单方欺骗闪付卡,与之进行通信。在该研究中,收单方即指支持闪付功能的 POS(point of sale,销售终端)终端。

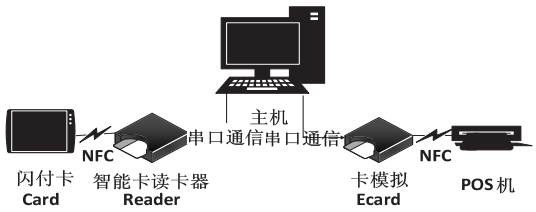

图 1　重放攻击模型

在该模型中,设计以 PC 机作为主机,reader 端由 Arduino uno 芯片组和 NFC-shield 组成,ecard 由一个 Arduino 操纵的 PN532 模块充当。系统由 PC 机在相关程序的支撑下,reader 和 ecard 端探测智能卡设备并进行转发。所接收到的数据,也即闪付卡与收单方之间进行交互的 APDU 显示在 PC 机屏幕上。

2.2　模型通信协议设计

模型中所设计的通信协议包括两个部分:请求和响应。模型中每个部分中间的数据交互都要遵循这个协议,有请求必有回应。协议中数据的格式符合银联 PBOC3.0 协议。

请求报文是收单方向闪付卡所发送的报文,格式见图 2,由一个 4 字节长的必备头与其后的一个变长的条件体组成。请求报文发送的数据长度用 Lc(命令数据域的长度)表示,期望返回的数据字节数用 Le(期望数据长度)表示。当 Le 存在且值为 0 时,表示要求可能的最大字节数(≤256)。在应用选择中给出的读记录(READ RECORD)命令、选择(SELECT)命令中,Le 应该等于“00”[9]。

CLA	INS	P1	P2	Lc	Data	Le
必备头				条件体		

图 2　请求报文格式

响应报文是闪付卡回应收单方请求所发送的报文,格式见图 3,由一个变长的条件体及其后两字节长的尾部组成。SW1、SW2 是响应报文的结尾,表示请求报文的处理状态。在处理成功时,SW1、SW2 为固定值 9 000[1]。

Data	SW1	SW2
条件体	必备尾	

图 3　响应报文格式

3　闪付卡安全漏洞分析

通过对招商银行及农业银行闪付卡的监听,得到了用户在交易过程中需要提供的各种身份数据,接下

来将借此探究 PBOC3.0 协议的漏洞以及对闪付卡实施重放攻击的可能性。在合法通信的过程中,所有数据报文的格式都遵循 PBOC3.0 规范。

由于卡内大部分记录读取权限为自由[1],攻击者可任意对包含用户敏感信息的闪付卡内的数据进行读取。终端机通过发送 APDU 指令读取信息,第一条和第二条 APDU 完成了闪付卡的初始化和选择应用的过程,第三条指令开始卡片进入脱机状态,即预扣款状态。农行和招行的前三条 APDU 格式基本相同。第四条指令开始读记录,至最后一条指令完成,卡片会完成扣款流程。

由于本次模拟攻击中使用的两个银行的闪付卡都没有对终端的合法性进行验证,在模拟攻击中,采用了攻击者编写脚本假扮收单方欺骗闪付卡的方式进行攻击,并且模拟消费成功。

综上所述,通过对符合 PBOC3.0 协议的闪付卡通信过程的监听,发现了 PBOC3.0 协议的两个漏洞:

(1)在身份认证过程中,PBOC3.0 协议并未强制规定由闪付卡对合法性进行认证,闪付卡有可能与未经授权的终端完成通信。因此利用一台 PC 机编写程序,就可以欺骗闪付卡,令其以为自己在进行合法交易。

(2)在监听过程中,用户的许多敏感信息被明文传输。下一部分将展示提取到的一些用户敏感信息。并且已有团队的研究表明:通过读文件指令 00B2020C00,就可以获取包含如标签为 9F61 的持卡人证件号,标签为 5F20 的持卡人姓名等敏感信息[1]。需要提及的一点是,由于 PBOC3.0 协议对闪付卡中存储的用户个人敏感信息内容没有强制规定,卡片中的信息完全由发卡行决定。因此,在芯片卡广泛发行的情况下,用户信息可能会遭到泄露。

4 重放攻击实施结果

应用图 1 所示的模型,对招商银行和中国农业银行发行的闪付卡与收单方的合法通信进行了监听,并尝试利用截留的数据包进行重放攻击。

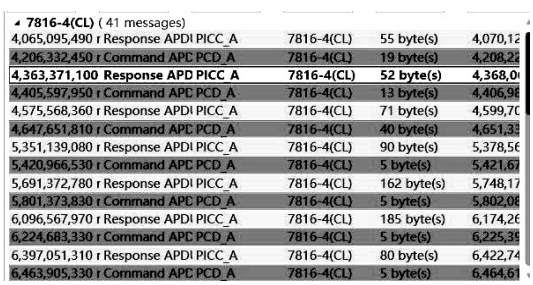

图 4 对招行闪付卡进行攻击的过程

图 4 是对招行的闪付卡进行重放攻击过程中 APDU 及其返回值的记录。其中“Command APDU”是主机模拟收单方发送给卡片的 APDU,即请求报文;而“Response APDU”是卡片返回值,也就是响应报文。表 1 列出了其中一条交互报文中几个重要标签及其解析结果,其中包含了闪付卡卡片号码和持卡人的姓名等隐私数据。

表 1 招行信用卡返回响应解析

标签	定义	数据
82	应用交互特征	7C00
9F36	应用交易计数器	000C
57	2 磁道等效数据	6217＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊
9F10	发卡行应用数据	A02000010000000000AE846452
9F26	应用密文	1B02E06C1394C710
5F34	应用主账号序列号	01
9F6C	卡片交易属性	0000
9F5D	脱机可用余额	000000000000
5F20	持卡人姓名	60＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊

在模拟攻击中,利用主机监听并截留的交互数据,实现了将监听到的 APDU 写成脚本形式来模拟收单方,自动发送,并成功实现卡内电子现金的消费。实际上因为银行后台数据库中并未记录该笔消费,在结算时恢复了卡内脱机现金数目。但在此次模拟中成功欺骗了卡片,令其以为自己在与合法的收单方通信,从而成功完成了卡内电子现金的消费。选择这种攻击方式是由于收单方在通信中对闪付卡的合法性进行了验证,持卡人验证方法由卡内数据标签为 8E 的数据决定。而闪付卡在通信中,对于收单方的认证过程相对简单,使得欺骗能够成功实现。

但同时,两个银行的闪付卡的 82 标签(应用交互特征)值均为 7C00,即都采用了 DDA(动态数据验证)和 SDA(静态数据验证)两种身份验证方式[10-13]。SDA,即静态数据验证的签名是在卡发行时就定好的,SDA 加密过程中所用的私钥是发卡行的私钥,因此,只采用 SDA 验证方式的卡片,被人取得静态数据后,可能被复制。而 DDA 每次用来签名加密所用的私钥是 IC 卡私钥。由于 DDA 中需要卡片私钥的参与,而卡片私钥是无法被读取的,所以闪付卡不会被完整复制,可以有效抵御伪卡[14]。

5 对抗措施分析

闪付卡由于其对小额支付的速度要求,必然牺牲一定的安全性。第三、四节展示并分析了招行闪付卡与主机间的 APDU 报文交互过程,并指出了重放攻击的可能性及 PBOC3.0 协议存在的漏洞。针对发现的漏洞,主要从两方面提出对抗措施:敏感信息的加密存储和增加闪付卡对收单方的认证过程。

(1)增加闪付卡对收单方的认证过程[15]。对于本次攻击中所发现的,收单方缺乏身份认证,攻击者假

扮收单方与闪付卡进行交易的情况,建议 PBOC3.0 协议中增加闪付卡对收单方的认证过程。如学习 SSL 通信体制,由闪付卡生成随机密钥 key,此 key 用发卡行 RSA 公钥加密后发送到收单方端,再由收单方用私钥解密得到密钥 key,通过该随机密钥 key 对收单方的合法性进行认证。但这种方法有可能会加大通信时间代价。

(2)信息加密存储。对于监听过程中发现的用户信息泄漏问题,虽然这些信息并不能直接导致用户资金被盗,但仍是一个安全隐患。因此建议 PBOC3.0 协议强制避免敏感信息的明文存储。可行的措施是:将明文读取的用户敏感信息如持卡人姓名等,经过公钥密码体制加密后,存储进卡内相应位置,在需要时由收单方后台(如银行)关联。

此外,为了对抗通信过程中的监听,从而对抗重放攻击,也有研究人员提出了一些措施:如采取位置距离绑定,即通过比对节点间的位置来检测其相互距离的办法[16];或者通过在 APDU 报文中加入时间戳,并丢弃传输时间过长的报文的方式,来确保通信始终在近场距离内;以及通过电磁屏蔽的办法防止监听[1-2]。

6　结束语

文中设计了重放攻击的模型以及攻击所需的通信协议,并利用 PC 机及附属设备实现了对招商银行和中国农业银行发行的闪付卡与收单方之间通信的监听。并利用监听中拦截的数据,编写程序实现了模拟攻击。同时基于监听中所拦截的 APDU 交互报文,对其进行分析,找出 PBOC3.0 协议存在的弱点,并提出改进方案。而对于改进方案的可行性,将在以后的研究中继续探索。

参考文献:

[1] 杨　卿,黄　琳. 无线电安全攻防大揭秘[M]. 北京:电子工业出版社,2016.

[2] 罗勤文,邹俊伟,张晓莹. 基于近场移动支付的中继攻击与 PBOC 协议安全漏洞分析[D/OL]. 2014. http://www.paper.edu.cn/html/releasepaper/2014/07/203/.

[3] ROLAND M,LANGER J,SCHARINGER J. Practical attack scenarios on secure element-enabled mobile devices[C]// Proceedings of 4th international workshop on near field communication. Washington,DC,USA:IEEE Computer Society,2012:19-24.

[4] ROLAND M,LANGER J,SCHARINGER J. Applying relay attacks to Google Wallet[J]//Proceedings of the 5th international workshop on near field communication. Washington,DC,USA:IEEE Computer Society,2013:1-6.

[5] CHA B,KIM J. Design of NFC based micro-payment to support MD authentication and privacy for trade safety in NFC applications[C]//Proceedings of seventh international conference on complex,intelligent,and software intensive systems. Washington,DC,USA:IEEE Computer Society,2013:710-713.

[6] MULLINER C. Vulnerability analysis and attacks on NFC-enabled mobile phones[C]//Forth international conference on availability,reliability and security. [s. l.]:[s. n.],2009:695-700.

[7] 刘　淳,范晓红,张其善. EMV 规范的安全框架分析[J]. 遥测遥控,2006,27(2):68-72.

[8] 刘　淳,张其善. EMV 规范中的密钥管理[J]. 遥测遥控,2006,27(1):67-70.

[9] Technology Department. China financial integrated circuit (IC) card specifications (PBOC 3.0)[J]. 中国标准化:英文版,2013,60(3):84-87.

[10] 杜　磊,李增局,彭　乾,等. 金融 IC 卡规范脱机动态数据认证的漏洞研究[J]. 计算机工程与科学,2016,38(10):2070-2076.

[11] 朱建新,朱立国. 基于 EMV 标准的金融 IC 卡安全框架设计与实现[J]. 微计算机信息,2007,23(30):65-67.

[12] 张向军,陈克非. 基于 PBOC 智能卡的匿名可分电子货币协议[J]. 计算机应用,2009,29(7):1785-1789.

[13] 彭　乾,李增局,史汝辉. EMV 应用密文的差分错误注入分析[J]. 网络与信息安全学报,2016,2(4):64-72.

[14] BOND M,CHOUDARY O,MURDOCH S J,et al. Chip and skim:cloning EMV cards with the pre-play attack[C]// IEEE symposium on security and privacy. Washington,DC,USA:IEEE Computer Society,2014:49-64.

[15] 郎春华,王小海,赵云峰. 中国金融 IC 卡规范对 EMV 的支持性研究[J]. 浙江大学学报:理学版,2007,34(1):46-49.

[16] BOUKERCHE A,OLIVEIRA H A B F,NAKAMURA E F,et al. Secure localization algorithms for wireless sensor networks[J]. IEEE Communications Magazine,2008,46(4):96-101.