安全小课堂第七十四期【NFC支付安全】

京东安全应急响应中心 2017-09-22

NFC技术能给我们的生活带来极大的便利，能够用于乘车、购物、交换信息、刷门禁卡，可以说它能够应用到我们生活的方方面面，那么NFC技术安全吗？JSRC **安全小课堂第七十四期**，邀请两位老师分享NFC支付安全技术,同时感谢白帽子们的精彩讨论。

什么是NFC支付?

京安小妹

NFC是一种移动支付方式，与二维码扫码支付的区别在于，NFC是一种高频无线通信技术，不需要使用移动网络。应用NFC技术的手机相当于把手机变成了支付终端，可以直接刷机支付。比如我们现在常见的手机钱包，可以直接手机贴到公交、地铁的刷卡器上进行支付。以及我们现在核发的芯片银行卡，普遍带有QuickPass的标志，有这个标志可以直接将卡片贴到对应POS机上进行支付，这里面也是NFC支付的技术。另外一个大家都知道，公交卡，饭卡，这些也都用的是NFC支付的技术，所以NFC支付实际上在我们生活里可以说是无处不在。

讲师： 单好奇、sweeper

NFC支付的工作原理?

京安小妹

NFC支付技术即NFC（Near Field Communication缩写，近距离无线通讯技术）。这个技术由非接触式射频识别（RFID）演变而来，由飞利浦半导体（现恩智浦半导体）、诺基亚和索尼共同研制开发，其基础是RFID及互连技术。近场通信（Near Field Communication,NFC）是一种短距高频的无线电技术，在13.56MHz频率运行于20厘米距离内。其传输速度有106 Kbit/秒、212 Kbit/秒或者424 Kbit/秒三种。近场通信已通过成为ISO/IEC IS 18092国际标准、ECMA-340标准与ETSI TS 102 190标准。大家常见的高频门禁卡和大学食堂饭卡通常也遵循一样的通信标准，只不过具体传输的数据类型是肯定不一样的。我们目前常见的NFC支付协议标准一般都是走在ISO14443A上。

讲师： 单好奇、sweeper

NFC支付存在的安全隐患问题?

京安小妹

就像我们刚才提到的公交卡啦，大学饭卡啊之类的，如果是Mifare系列的卡片，基本都可以做到卡片加密区密钥的破解，只需要用ACR122U或者Proxmark 3这种NFC的硬件攻击设备，破解出对应的卡片密钥。拿到密钥之后，一般分两种攻击方式，一种是直接复制出来一样的卡片，里面的金额也一样，所以可以点无数次炒饭；另一种呢，就是读出来消费前的数据，消费之后再读一次，找到哪些区块有数据变化，这些基本上就是代表着卡片余额，有密钥就可以直接改卡内金额啦！
Mifare早期的算法有漏洞，可以做到知道一个密钥推算出所有扇区对应的密钥，每个扇区的密钥是可以做到单独设置。但是很多卡的全部扇区里会有几个用的是FFFFFFFFF这类默认密钥，就可以直接算出来所有的密钥。现在Mifare的卡算法做了升级，没有那么好算，但是处于成本考虑，国内用的很多这种卡，比如酒店的，用的还都是早先的卡。对于常见的Mifare卡，有个比较简单的教程，由奇虎360 T7 redrain编写：
http://ohroot.com/drops/drops/RFID%E5%85%A5%E5%9D%91%E5%88%9D%E6%8E%A2%E2%80%94%E2%80%94Mifare%20Classic%20card%E7%A0%B4%E8%A7%A3%EF%BC%88%E4%B8%80%EF%BC%89.html
虽然咱现在的银行卡也都是NFC闪付，遵循的也是ISO14443A协议，但是实际交换的数据内容都是自行加密的，走PBOC交易协议，对于这种类型的攻击，就很难了。
NFC攻击分为几种呢，一般分为两种，一种是密钥破解攻击，这种就是复制卡居多，另外一种是针对银行卡的透传攻击，不需要知道加密的具体内容，只需要把数据传过去，因为这个加密协议实在是破解不了。

讲师： 单好奇、sweeper

NFC支付防御手段有哪些呢？

京安小妹

防御手段一般分为被动式和主动式。主动式的代表就是360安全卡套，安全卡套里面有特殊的涂层，大家都知道NFC实际上是无线电技术，所以做了这一个屏蔽层，利用了法拉第笼原理，就可以做到阻断读卡信号了。除了卡套还有一种防护手段，就是去主动地产生白噪声信号，这样就做到了干扰正常的卡和读卡器之间的交互，可以做到防护钱包里所有带有NFC功能的卡片。我们的这个设备也叫做360卡防，如果有兴趣可以点进http://unicorn.360.cn/kafang/
看一下。可以做到防护钱包里所有带有NFC功能的卡片，包括银行卡，护照，和身份证。

：

讲师： 单好奇、sweeper

NFC分高频低频，125Khz和13.56Mhz有不同的适用场景，前者在门禁系统中多，后者在支付系统中多，针对这两个分别有什么比较有效的攻击手段?

京安小妹

讲的东西，都是在13.56Mhz这个频率上的，其实还有一种用的更多的，就是125Khz的。125KHz在很多小区的门禁系统里用的到，对于125Khz，分两个主要的大类，一个是普通的em410x，t5577芯片卡之类的，这种很容易复制，小区门口大爷十块钱给你克隆一张，还有一种就是HID卡，这种走ISO15639协议，自带加密，比Mifare类非接触式卡安全的多。对于普通意义上的125Khz小区门禁卡，常见的低频卡，上面会有ID，有了这个ID，我们就直接可以复制出来一张一模一样的卡开你家小区楼门，我们的针对性攻击设备，比如HackID Pro和HackID Plus，可以做到模拟、爆破、读取所有常见低频类ID卡。关于详细介绍大家也可以看看我们在i春秋上的解说，
https://www.ichunqiu.com/course/54933
比如我们刚才做的这个破解低频卡的小设备，我们举个例子，比如你拿到了某公司清洁工的门禁卡，读取出来他的ID卡号，就可以模拟出来一张一样的卡了，但是肯定进不了总裁办公室，一般情况下公司的所有门禁卡都是连号的，所以你可以用我们的设备枚举ID卡号，达到提升权限的目的了。
高频的NFC，一般以破解密钥、克隆卡片为主，工具主要是ACR122U和Proxmark 3这类设备为主，另外就是透传类破解工具，比如我们做的HackNFC；低频的NFC，一般以直接复制克隆和暴力破解为主，因为低频的NFC由于传输速率的问题，有价值的一般只有ID部分，所以无法承载更多的数据交互和计算性质的功能。

下面给大家一些比较有用的参考链接：
NFC 透传攻击
https://conference.hitb.org/hitbsecconf2015ams/wp-content/uploads/2014/12/WHITEPAPER-Relay-Attacks-in-EMV-Contactless-Cards.pdf
EMV银行卡协议攻击
https://cybercamp.es/cybercamp2015/sites/default/files/contenidos/material/slides_cybercamp-15.pdf
Mifare卡片攻击
https://www.blackhat.com/docs/sp-14/materials/arsenal/sp-14-Almeida-Hacking-MIFARE-Classic-Cards-Slides.pdf

：

讲师： 单好奇、sweeper

本期JSRC 安全小课堂到此结束。更多内容请期待下期安全小课堂如果还有你希望出现在安全小课堂内容暂时未出现，也欢迎留言告诉我们。

安全小课堂的往期内容开通了自助查询，回复“安全小课堂”或者点击阅读原文进行查看。

最后，广告时间，京东安全招人，安全开发、运营、风控、安全研究等多个职位虚位以待，招聘内容具体信息请扫描二维码了解。

简历请发送：cv-security@jd.com

微信公众号：jsrc_team

新浪官方微博：京东安全应急响应中心