Apple Pay落地中国,未来能否抢占移动支付市场?

万赟

美国休斯敦大学维多利亚分校,德克萨斯州维多利亚 77901

2016年2月18日,Apple Pay正式登陆中国。由于阿里巴巴和腾讯这两大移动支付平台具有市场先入优势,很多业界人士对Apple Pay在中国的市场发展前景并不看好。但不可否认的是Apple Pay的安全性和方便性更具有优势,而且它在很大程度上解决了用户信息被盗风险及消费隐私泄露问题。本文介绍Apple Pay的前期策划、相关技术、存储方式、支付流程及市场前瞻。

2016年2月18日Apple Pay正式登陆中国(图1)。由于阿里巴巴和腾讯这两大移动支付平台具有市场先入优势,很多业界人士对Apple Pay在中国的市场发展前景并不看好,但不可否认的是Apple Pay的安全性和方便性更具有优势,而且它在很大程度上解决了用户信息被盗风险及消费隐私泄露问题。另外银联以及各大银行期望通过Apple Pay与阿里巴巴以及腾讯等电商移动支付平台进行竞争,这会间接帮助Apple Pay提高市场份额。

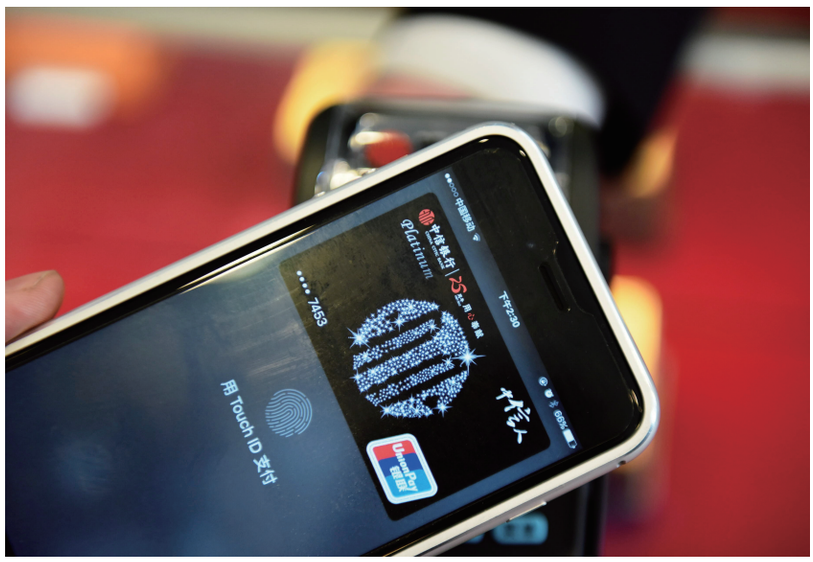

图1 2016年2月18日,一名顾客在浙江杭州一商家具有"银联云闪付"功能的POS终端上进行"Apple Pay"(图片来源:新华网,龙巍 摄)

抽样调查显示从2014年11月在北美通过iPhone 6上市到2015年10月,Apple Pay在北美市场的普及率从9%稳步上升到16.6%。目前iPhone 5/5s仍然是主流苹果手机,随着iPhone 6/6s份额的不断上升,可以预计Apple Pay在中国的普及率会继续增加。

苹果公司在向一个新领域推出第一代产品时往往采取稳扎稳打、一步到位的策略,本文通过分析苹果支付的设计细节来说明为什么它很可能会像指纹ID一样快速推动其他手机制造商提供类似的解决方案,奠定移动支付领域的新标准。

1 前期筹划

Apple Pay的筹划阶段至少可以追溯到2008年。2008年9月苹果公司向美国专利局提交一份名为《点对点网络金融交易的设备和方法》的专利申请。申请提出用智能手机的近场通信(NFC)芯片与支付终端进行支付信息交换的产品原型,并采取用摄像头捕捉

收稿日期:2016-04-28

作者简介:万赟,副教授,研究方向为电子商务和互联网应用,电子信箱:WanY@uhv.edu

引用格式:万赟. Apple Pay落地中国,未来能否抢占移动支付市场?[J]. 科技导报, 2016, 34(9): 55-58; doi:10.3981/j.issn.1000-7857.2016.09.007

信用卡图像、识别姓名和卡号等关键支付信息等功能。这份专利勾画出Apple Pay最初的框架设想。

2 近场通信:Apple Pay第一技术要素

专利里提到的近场通信是Apple Pay的第一个技术要素。近场通信是射频识别(RFID)技术的一个应用子集。第二次世界大战期间德英交战双方需要通过雷达识别是敌人还是自己的飞机。德军发现自己飞机返回时如果在空中翻滚的话,反射回的雷达信号会有所不同,于是用这种方法进行区别。英国军方则在飞机上安装了转发器,当接收到自己的雷达信号时转发器会反射回特定信号或者直接发送回应信号给雷达。这种雷达识别技术后来转为民用,形成了无源和有源两类射频识别技术。2008年,中国开始陆续采用的电子地铁车票就是使用射频识别技术,让用户可以以非接触方式刷票进入。近场通信技术也可以分成主动(有源)和被动(无源)两种模式,主要区分在于主动通信时发起和目标设备都产生各自的射频场,而被动模式下目标设备不产生射频场,使用负载调制以相同的速度将数据传回发起设备。近场通信与其他射频识别技术相比具有传输距离短(最远10 cm)但是带宽高、能耗低、适合保密数据交换的特点,所以成为Apple Pay的首选。除了近场通信,当时能够提出用手机摄像头捕捉和识别用户姓名、卡号等关键支付信息也体现出苹果公司在提高用户体验方面的用心。

在启动Apple Pay的项目后,遵循乔布斯的一贯作风,苹果公司通过收购创业公司,猎取专业人才以及连续提交各种相关专利方式来快速搭建支付系统框架。就像当初推出iPod和iTune时与各大唱片公司进行谈判合作一样,在后面的6年时间里,Apple Pay的项目团队除了完善软硬件的挑选、搭配和设计外,还与运通、维萨、万事达、摩根大通等信用卡公司和主要银行用不同方式尝试最佳的移动支付模式,进行了大量合作调研工作(注:2010年维萨卡和一家从事近场通信技术的小公司为当时尚未配备近场通信芯片和功能的iPhone 3G和iPhone 3GS提供带NFC功能的手机外壳。用户的iPhone使用该机套后就可以实现近距离移动支付。维萨卡则和苹果公司分享了用户反馈)。

经过几年的摸索和数据收集,苹果公司在2012年5月向美国专利局提交了更详细的设计细节的专利申请,并在同年9月推出Apple Pay的前身(Passbook)。Passbook可以让用户在苹果手机中存储优惠券、登机牌、活动门票、回馈卡或其他类型的通过二维码和条形码来展示移动支付凭证,Passbook还具有按位置和时间触发相关凭证的功能。每个凭证可以最多包含10个位置,每个位置被编写为GPS坐标(经度,纬度和海拔高度)或iBeacon UUID。苹果手机可以根据用户所在位置和时间判断相关的凭证来提醒和显示给用户。不过Passbook还没有处理信用卡的功能,因为Apple Pay还需要通过信用卡公司以及银行的配合才能实现整个支付框架的关键部分,这就是卡号替代(tokenization),而这一功能的成功实施和普及将不仅显著提高用户支付信息的安全性,还会成为移动支付发展历史上一个重要的分水岭。

3 卡号替代技术:移动支付发展史上分水岭

在移动支付领域,支付信息的提交和确认是整个移动支付的关键环节。因为无论采用何种传输方式,只要支付信息从手机传送到支付终端,就有可能被黑客截取而产生安全隐患(注:黑客截取支付信息的方式多种多样,比如近几年频频发生信用卡在北美被盗用后一个小时内在亚洲市场刷爆的案例,就是黑客在商店的支付终端秘密安装了读卡设备的缘故)。要避免这类风险,最理想的方式是避免传输实际支付信息,转为用替代卡号来达到同样目的。所谓替代卡号简单来说就是信用卡公司为用户信用卡的真实卡号生成一个对应的替代数字卡号,用户可以用这个替代数字卡号进行支付,信用卡公司通过这个替代卡号来找到对应的真实卡号后确认支付。当然替代卡号只是整个支付信息的核心部分。要让信用卡公司成功识别替代卡号,还需要用户提供其他信息,比如与替代卡号相关的手机信息、用户身份及交易信息等。

替代卡号技术在金融信息安全领域的应用最早出现在2005年,但是随后几年,配套技术的落后和计算机在生成替代卡号的随机性方面的一些局限使这项技术一度停滞不前。苹果公司能够从众多潜在的安全技术里面挑选替代卡号做为支付核心技术是因为苹果手机是第一个能够为替代卡号提供相应的软硬件配套系统的移动设备,而苹果公司也是第一个说服所有信用卡公司和大银行支持这一框架的公司。从这一点来看,库克沿用了当年乔布斯说服各大唱片公司以及后来的各大出版商先后推出数字音乐(iTune)和图书(iBook)平台的相同策略,这就是一流的技术实现加上一流的跨界联合。

媒体在报道Apple Pay时没有过多渲染使用替代卡号的意义,但这项技术却是移动支付发展历史上的一个分水岭。从技术角度看,在此之前移动支付技术的发展重点在如何用各种加密和防火墙技术保护手机、服务器及传输过程中的支付信息;采用替代卡号方式技术后,这方面的压力将全面降低,因为即便黑客拿到信用卡号的替代号码也无法使用它。可以预见如果未来移动支付全面采用这一技术,将导致一大批为先前方式提供各种加密服务的公司失去市场,甚至信用卡公司本身的一部分收入(比如向商家收取的数据安全费用)结构也将做出调整。

为深入研究替代卡号的用户体验效果,苹果公司从2013年开始先后与运通、万事达和维萨卡三家信用卡公司合作,秘密展开用不同的用户试验项目。这些项目不但对媒体保密,甚至对

项目参与者也保密。维萨卡公司750名参与匿名替代卡号项目的成员一直到年底都不知道是跟哪一家公司合作。2013年7月苹果公司与摩根大通、美洲银行、富国银行在内的主要发卡银行的卡号替代系统搭建工作。摩根大通在其总部设置了秘密项目室,300多个项目参与人员中只有1/3的参与人员知道合作对方是苹果公司,其他人则一直到苹果公司在产品发布会上宣布苹果支付上线后才知道。

前面说到替代卡号消除了传输真实卡号的风险,但是需要软硬件的配合。这就涉及到Apple Pay里的另一个关键部件安全芯片(Secure Element)。Apple Pay用它解决信息存储风险。

4 信息存储:移动端存储与云端存储相结合

移动支付的信息存储设计一般有两种方式。一种是把支付信息存储在移动端,另一种是将其存储在云端。

在第一种方式里一般使用安全芯片来存储支付信息。这类芯片内部包含一个类似于CPU的微控制器,可以直接在芯片内部对支付信息进行加密和解密,避免黑客通过更改外部软件造成泄密。除了将信息和信息处理一起内置外,安全芯片还具有防止反编译和硬件侵入功能,比如当察觉到芯片的物理参数发生不正常改变后自动将敏感数据清零,甚至在断电情况下也可以进行,最大限度避免内藏数据的泄露。这种移动端存储技术在苹果支付采用之前,已经被应用到硬盘和操作系统加密上,比如微软公司的BitLocker驱动器加密就是采用类似的概念。用户通过设置在计算机主板上的加密芯片来加密整个硬盘数据,避免硬盘丢失造成的数据泄露。不过由于硬件成本原因,微软操作系统通常采取的是通过在硬盘上划分出一个加密分区来存储密钥和加密解密程序,然后借此实现对整个硬盘的加密。

不过不少业界人士认为无论何种方式,将数据存储在移动端不安全,于是有了第二种方式,也就是将信息放在云端专门用来保存支付信息的服务器上。如果采用这种方式,服务器一般用特别严密的手段维护,安全级别与信用卡公司的替代卡号服务器类似。支付信息的读取必须通过好几种认证方式产生一致的结果才能进行,比如每一笔交易产生的动态密码和替代卡号能够在服务器端成功解密并对应,移动端用户提供的指纹或密码通过验证,甚至还需要云端服务器对整个读取需求的风险评估达到一定分数等。只有所有条件都满足,支付信息才能被读取出来。

这两种方法各有利弊。第一种方式的好处是不需要联网就可以进行安全控制,第二种方式相对来说更安全。Apple Pay则采取了两者结合的方案。要想让手机中存储的虚拟信用卡像真实的信用卡一样好使,就需要在没有网络连接的情况下也可以实现支付功能,也就意味着支付信息必须以某种方式存储在手机上,所以苹果支付在手机中加入了安全芯片。为了提高安全性,该芯片镶嵌在近场通信芯片模块里,独立于手机上的任何其它部件。另一方面,存储在手机上的是替代卡号,所以支付过程中信息的验证是按照第二种方式进行的,也就是说通过移动端的指纹ID和密码验证后,替代卡号和交易动态密码等信息通过商家的支付终端被传送到远程替代卡号服务器,后者给出真实卡号后才能完成授权支付。

下面介绍Apple Pay如何将前面提到的这些设计原理以及要素融合在一起形成其支付流程的。

5 支付流程

苹果支付的主要流程分为提交新卡和交易支付两部分。

当用户需要通过相机提交新的信用卡信息时,苹果手机把识别出的信用卡号以及其他支付信息加密后直接传递到苹果服务器,不在手机上保留。苹果公司接收并解密传递过来的支付信息后,将该信息连同其他用户信息(比如用户在iTune上的交易历史,手机号码、型号及操作系统,甚至是用户提交信息的地理位置等)一起加密提交给信用卡发卡机构(银行或者信用卡公司)的服务器(注:使用信用卡支付需要向商家提供的一般包括用户姓名,主账户号码(PAN,俗称信用卡号),卡的有效期和信用卡验证码(CVV)。其中验证码是通过卡号、有效期和服务约束代码生成的3位或4位数字。支付卡安全标准(PCI-DSS)中明确规定,商家不得储存用户的验证码。因为如果保存的验证码万一连同其他保存的支付信息被黑客获得,凭借这些信息,任何人都可以进行无卡消费)。

发卡机构验证确认接收到的信息后,会允许这张信用卡被加载到该用户的Apple Pay账户,同时会为这张信用卡生成两条重要的支付信息,一条是前面提到的与该手机联系在一起的信用卡的替代卡号(意味着只有从这个手机提交的支付申请才会被批准),这里替代卡号的数位长度和对应的信用卡号一致;另一条是每次用户使用该信用卡在手机上进行支付时用来生成一次性动态交易密码的密钥。替代卡号和密钥被加密传回给苹果公司服务器后,将被直接存储到手机的安全芯片里。

值得关注的是因为在存储过程中替代号码和密钥是以加密的形式从发卡机构的服务器直接存储到用户手机的安全芯片里,所以除了发卡银行外,包括苹果公司在内的其他个体没有解密钥匙,无法将其解密,这样既保证了只有发卡银行可以解密确认交易的真实性和有效性,又在一定程度上减轻了苹果公司的风险责任。

当信用卡被添加到Apple Pay后,用户就可以使用苹果手机进行支付操作了。支付时用户将手机头部靠近支付终端,手机前端检测到支付终端信号时就会唤醒苹果支付程序,显示常用的信用卡等待用户用指纹触摸ID或者是输入手机密码确认。确认后,安全芯片内部的微控制器会用前面提到的银行提供的密钥生成一个一次性的动态交易密码,将该密码和替代卡号以及其他

相关信息一起提交给商家的支付终端。支付终端将这些信息提交给信用卡公司,后者通过一系列解密和验证确认后完成支付过程。

6 市场前瞻

准确地讲Apple Pay并没有和目前北美及中国的主要移动支付平台进入正面竞争,它是以一个交易工具的形式进入这一市场,为信用卡公司提供了一个移动支付在技术层面的解决方案,但是毋庸置疑,这一解决方案为信用卡公司和互联网移动支付平台进行竞争提供了重要的技术保障。

对银行和其他信用卡金融机构来说,中国市场的移动支付主要竞争对手是阿里巴巴的支付宝和腾讯微信支付。凭借各自庞大的用户群和互联网技术优势,这两个平台在短短几年内迅速占据移动支付市场。2015年开始,阿里巴巴投入巨资全面拓展线下各种商家的终端支付市场,直接威胁到银行信用卡市场。

与Apple Pay不同的是,以支付宝、微信支付为代表的移动支付是阿里巴巴和腾讯等互联网巨头垄断网络电子零售的最后一步。在这之前这些互联网电商已经掌握了用户各种消费习惯和信息,存储了用户的不同信用卡支付信息,移动平台是用来取代银行和信贷机构的消费信用角色,从而彻底垄断电商交易的所有环节。如果这种垄断形成规模,再凭借人工智能的强大分析能力,一家公司就可以通过信贷利率伸缩和动态产品展示等手段轻易地控制一个普通消费者的消费空间和能力,在自身利润最大化的同时造成对普通消费者利益的伤害(比如一家医疗保险公司如果掌握了每一个居民的健康状况,就可以通过提高保费的方式将有健康问题的申请人拒之门外,减少自己的医疗费用支出,违背了医疗保险的初衷)。

而银联和各大银行为代表的传统信用卡机构对这两大平台的技术优势和灵活支付手段产生的市场竞争几乎没有还手之力,只能通过行政干预和政策歧视等手段延缓这一趋势。Apple Pay则为这些机构提供了扳回一局的机会。

尽管国内消费者对消费隐私的敏感性还不强,随着个人金融和信贷产业的不断扩大及个人信用分数系统的不断成熟,会有越来越多的用户意识到支付信息的泄露所造成的危害以及个人消费隐私的重要性。而目前移动支付市场只有Apple Pay为这方面提供了全面的保障。

如果Apple Pay的市场覆盖率进一步扩大,以Android系统为基础的智能手机也跟随采用类似的解决方案,有理由相信银行业能够借机推出有竞争力的移动端金融理财产品,这两者的合作将会全面遏制支付宝和微信支付在市场占有率上的进一步发展,消费者的个人权益也将得到一定保障。

(责任编辑 刘志远)