移动支付安全性分析及技术保障研究

随着我国电子商务的广泛应用，人们使用的支付方式早已不局限于现金本身，而扩大到银行卡、网上银行、电话银行等多种方式。目前，随着我国移动电话的广泛使用，基于移动终端的应用愈加广泛，在这种移动通讯工具上应运而生产生了更便利的移动支付功能，人们可以利用手机登录互联网进行远程购物消费，可以在便利店、商场、超市等进行现场刷卡消费[1-3]。然而，作为一种新兴的电子支付方式，移动支付拥有传统支付方式无法比拟的优势，但是其安全性也更多引起人们的关注。由于目前发生移动支付行为是基于手机号上绑定的银行卡、信用卡以及与商家之间完成，或者基于手机 SIM 卡与 POS 机近距离完成，故此，类似于密码破解、信息复制、病毒感染等都有可能对移动支付造成重大的损失。因此，我们有必要对移动支付的安全性进行分析，并通过技术手段来进行解决[3-5]。

1 移动支付概念及分类

1.1 概念辨析

目前，在日常生活中围绕移动支付涉及众多新型支付词语众多，包括移动支付、手机支付、移动钱包、手机钱包、移动银行、手机银行等，它们之间相互联系又互有不同。

所谓移动支付也称为手机支付，就是允许用户使用其移动终端(通常是手机)对所消费的商品或服务进行账务支付的一种服务方式。单位或个人通过移动设备、互联网或者近距离传感直接或间接向银行金融机构发送支付指令，产生货币支付与资金转移行为，从而实现了移动支付功能。移动支付将终端设备、互联网、应用提供商以及金融机构相融合，为用户提供货币支付、缴费等金融业务。所谓移动钱包也称为手机钱包，是指中国移动开发的基于无线射频识别技术(RFID)的小额电子钱包业务。用户办理该业务后，即可利用手机在中国移动合作的商户进行 POS 机刷卡消费。手机钱包(移动钱包)是用于中国移动用户移动电子商务交易支付的中间帐户，可更好地满足银行对小额移动电子商务结算处理的需求，满足商户对小额商品交易管理的需求，方便用户使用。用户开通手机钱包业务后，就能有一个与手机号码绑定的消费账户，账户直接就是手机号码，往这个账户上充值[7]，就像是给手机内置了钞票，在商家消费的时候，在专用的 POS 刷卡机前晃晃手机就能结账，也可以上网或发短信进行远程购物，此外，这个业务也可以用于企业的门禁系统和企业内部消费，如食堂用餐、内部消费等。

所谓移动银行也称为手机银行，是利用移动通信网络及终端办理相关银行业务的简称。手机银行是由手机、GSM 短信中心和银行系统构成。在手机银行的操作过程中，用户通过 SIM 卡上的菜单对银行发出指令后，SIM 卡根据用户指令生成规定格式的短信并加密，然后指示手机向 GSM 网络发出短信，GSM 短信系统收到短信后，按相应的应用或地址传给相应的银行系统，银行对短信进行预处理，再把指令转换成主机系统格式，银行主机处理用户的请求，并把结果返回给银行接口系统，接口系统将处理的结果转换成短信格式，短信中心将短信发给用户。

我们通过对三组概念的比较可以发现，移动支付(手机支付)是一个整体概念，用户通过移动设备、互联网或近距离传感进行移动业务处理。移动钱包(手机钱包)更倾向于小额电子钱包业务，它的主要消费方式就是在POS刷卡机前刷卡进行现场支付。移动银行(手机银行)主要是办理相关银行业务，也就是说用户使用手机进行银行业务操作时，实际上是和银行发生相关业务往来，比如说查询账单、银行转账等。

1.2 方式分类

根据移动支付在电子商务中的应用，我们认为移动支付可以按业务种类分为以下几种方式：

1)SMS(Short Message Service，短消息业务)，终端用户通过发送短消息的形式请求服务内容，从用户的话费中扣除费用，通常只适合于小额支付，如：利用短信支付服务进行铃声下载等。

2)WAP(Wireless Application Protocol,无线应用通讯),终端用户通过访问WAP站点，进行简单的金融业务，用户可通过手机上网进行远程操作，如：在互联网上进行购物及缴话费、水费、电费、燃气费等。

3)USSD(Unstructured Supplementary Service Data，非结构化补充数据业务)，是一种基于GSM网络的新型交互式数据业务，如证券交易、移动银行业务等。

4)NFC(Near Field Communication，短距离通讯)，是一种短距离的无线连接技术，用户可以使用“手机钱包”在合作商户POS机上现场刷“机”消费，比如说：在便利店、商场、超市等场所进行现场刷卡消费。

2 移动支付国内外发展现状

2.1 国外发展现状

美国三大移动通信运营商AT&T、T-mobile和Verizon无线于2010年11月合资成立了移动支付公司ISIS。该公司计划于2012年在盐湖城进行试点，利用移动支付功能完成盐湖城零售商的销售结算，并为犹他州交通管理局提供一种移动车票支付方式。公司设想把盐湖城以及其他城市变成消费者无需随身携带钱包，使用手机取代现金和信用卡消费的地方。日前，Aite Group发布的2010~2013年美国账单支付渠道和方式的预测数据显示，未来三年，移动支付将增长377%，成为美国人日常账单支付中增长最快的渠道，网上支付、借记卡支付、电话支付也将分别增长18%、4%、1%。

欧盟从2007年底开始重视移动支付功能，英国的信用卡发行商Barclaycard、诺基亚和VisaEurope等合作推出手机钱包业务，主要用于乘坐公共交通工具、买报纸时的小额支付。截止2011年3月，欧洲五国(英国、法国、西班牙、德国、意大利)市场上，总共有2000万手机用户，其中8.5%的手机用户开通了手机移动支付功能。

日本的手机钱包已经拓展到大额支付，甚至包括了消费信贷和股票投资业务。日本移动支付市场发展的首要推动者是NTT DoCoMo。早在1999年，NTT DoCoMo即推出i-mode手机互联网服务，并获得巨大成功。为发展移动信用卡业务，NTT DoCoMo于2005年4月同三井住友金融集团(SMFG)及其旗下的三井住友卡及三井住友银行公司结成战略联盟，并斥资980亿日元开展移动支付功能开发。

在韩国，目前70%的电子支付(即超过10亿美元的交易额)都是由移动支付完成的。通过与运营商合作，几乎所有的韩国零售银行都提供手机银行业务。现在，每个月有超过30万人在购买新手机时会选择具备特殊记忆卡的插槽，用以储存银行交易资料，并进行交易时的信息加密。

2.2 国内发展现状

在我国，移动支付产业属于新兴产业。截止2010年底，我国手机用户达7.4个亿，开通移动支付功能用户达1.92亿，实现交易6268.5万笔，支付金额共170.4亿元。并且，目前已开展了多个SIMpass试点应用示范工程，包括湖南移动、重庆移动、厦门移动、广东移动、南京移动等。其中，湖南移动2009年下半年开始进行SIMpass试点工作，目前主要应用包括湖南移动办公大楼门禁，食堂用餐，美容美发消费及停车场缴费。重庆移动在小额支付领域方面构建起了全国最成熟的现场手机小额支付商业环境。截至2009年8月，重庆RFID现场移动支付用户数已达到50万户，商户数达到4000家，铺设POS机5500余台，每月消费额超过500万元，用户充值金额超过300万元。厦门移动已经采购两万张双界面SIM卡用于公交一卡通的应用，目前已经发放500张卡片，使用效果良好。并且，厦门移动与厦门e通卡及建行正洽谈移动支付平台的建设。广东移动已经确定搭建基于双界面SIM卡的移动支付平台，主要应用在广州的地铁项目。并且，广东移动已将SIMpass用于大楼门禁、食堂用餐等，员工充分体验这项技术带来的便利。南京移动全新推出的“智汇移动手机一卡通”业务，将惠及全市700万的移动用户，市民可以利用移动支付完成公交车、地铁、出租车消费交易，甚至是去超市购物，到加油站加油等。

3 移动支付中的安全问题

3.1 移动支付中安全问题现状

我们在分析了目前移动支付国内外使用现状后，提出移动支付中可能隐藏的安全问题如下：

1)普通手机通常没有加密技术，在支付过程中往往会造成信息泄露，这已成为移动支付发展的一大难题。用户在使用手机进行支付时，未进行加密等安全措施保护，而黑客们通过钓鱼网站或木马程序就可以窃取用户信息，将被移动支付功能进行非法复制，从而造成用户的损失。

2)对参与交易各方的身份识别，手机支付须解决的一大问题就是商家和消费者合法身份的确认。由于移动支付将银行、商家紧密联系，涉及现金转帐的往来，如何解决合法身份认证就显得尤为重要。

3)用户信用体系有待进一步建设和完善，通常一些小额支付业务可以通过扣除手机话费的方式进行付费交易，于是就可能产生手机话费透支、恶意拖欠等现象。同时，由于我国手机号管理不够完善，许多手机号购买时尚未采取实名制管理，由此可能造成恶意透支现象发生。

4)手机丢失会给移动支付用户带来损失。由于手机的便捷携带，也使得手机在日常生活中会出现频繁丢失的情况，而移动支付通常是手机卡与银行卡、信用卡相关联，由此可能造成用户在丢失手机后自己的移动支付帐户被他人冒用的风险。

图 1 显示了移动支付的系统结构，移动支付是由银行、商家、移动支付服务提供商、认证中心、用户等多元素组成，该系统还与移动网络运营商，移动网络内容服务商，信用卡服务等其他机构产生业务往来，这样一个庞大而复杂的移动支付产业链，其安全问题不仅只涉及其技术本身的安全防范，还会考虑到和其他系统之间的信息的安全传递。

3.2 移动支付安全特性

我们在考虑了移动支付面临的安全问题后，认为移动支付系统需要具备下列特性：

1)交易双方身份的认证：移动支付功能应可以确认交易双方的身份。

2)资料信息的私密性：交易必须保持其不可侵犯性，经由网络送出以及接受的信息应是不能被任何闯入者读取、修改或拦截的。黑客入侵电脑系统前往往利用网络窥视、并事先收集使用者在登入系统时输入的账号、密码及使用者姓名等重要信息，再冒名侵入系统。

3)资料信息的一致性、完整性：移动支付交易必须保证交易不被破坏或干扰，电子交易的内容在用户端和服务器间的传递过程需要确认没有被改变，也就是信息在交易的处理过程中不能被任意加入、删除或修改。

4)不可否认性：移动支付必须是防止发送方或接收方抵赖所传输的消息的一种安全服务。也就是说，当接收方接收到一条消息后，能够提供足够的证据向第三方证明这条消息的确来自某个发送方，而使得发送方不能抵赖发送过这条消息。同理，当发送一条消息时，发送方也有足够的证据证明某个接收方的确已经收到这条消息。

4 移动支付安全技术分析

我们通过对移动支付安全问题的分析，认为可以通过无线公钥基础设施(WPK I)、WAP 安全、身份认证等方式来确保移动支付的安全性。

4.1 无线公钥基础设施(WPKI)

WPKI (Wireless PKI)是有线 PKI 的一种扩展，它将互联网电子商务中 PKI 的安全机制引入到移动支付交易过程中。WPKI 通过采用公钥基础设施以及证书管理策略，有效地建立了安全有效的无线网络通信环境。WPKI 以 WAP 的安全机制为基础，通过管理实体间关系、

密钥和证书等来增强移动支付的安全性。WPKI 作为安全基础设施平台，一切基于身份验证的应用都需要 WPKI 技术的支持，它可与 WTLS、TCP/IP 相结合，实现身份认证、私钥签名等功能。WPKI 的主要组件包括：终端用户实体应用程序(EE)、PKI 门户(PKI Portal)、认证中心(CA)、目录服务(PKI Directory)、WAP 网关以及服务器等设备，WPKI 的基本工作原理如图 2 所示：

WPKI 基本工作原理为[10]：

1)用户向 RA 提交证书申请；

2)R A 对用户的申请进行审查，审查合格后将申请交给 CA；CA 为用户生成一对密钥并制作证书，将证书交给 RA；

3)CA 同时将证书发布到证书目录中，供有线网络用户查询；

4)R A 保存用户的证书，针对每一份证书产生一个证书 URL，将该 URL 发送给移动终端用户；

5)同时有线网络服务器下载证书列表备用；

6)移动终端向 WAP 网关发送文档、签名及证书 URL 建立安全 WTLS/TLS 连接；

7)WAP 网关与有线网络服务器建立 TLS/SSL 连接；

8)移动终端和有线网络服务器实现安全信息传送。

4.2 WAP 协议安全方式

我们可以通过 WAP 协议方式来解决移动支付交易协议的安全问题，WAP 的安全性主要由 WTLS/ TLS、以及 WMLScript SignText 来实现。

1)WTLS/ TLS。无线安全传输层 WTLS(WirelessTransport Layer Security)是根据工业标准 TLS Protocol 制定的安全协定，是设计使用在传输层之上的安全层。WTLS 的功能类似全球资讯网站所用的 SSL 加密传输技术，可以确保资料在传输的过程中经过编码、加密处理，以避免黑客在资料传输过程中窃取保密性资料。WTLS 被设计在两个通信应用之间提供私密性、资料一致性和身份认证服务。WTL S 支持不同的安全等级，每一个等级都牵涉到不同的握手(Hand-shake)需求，较高等级的安全性可能需要较复杂的握手程序及较大的频宽。WTLS 支持不同的加密机制，并依据密钥的长度划分不同的安全等级[11]。

2)WMLScript SignText。使用者可以通过输入一些文字决定接受或拒绝开发者写入的应用。WAP 浏览器提供一个 WMLScript 功能，Crypto.signText 用来要求使用者输入一些字串。当呼叫 SignText 方法时，显示使用者输入的字串，要求使用者确认。例如，当使用者接受

时，必须输入 PIN 码。资料签署后，签章和资料会传回服务器，服务器在取得数位签章后验证使用者身份。

4.3 身份认证方式

在移动支付中，最关键的问题是使用者的身份认证，我们提出以下五种方式可以提供不同安全程度的认证：

1)移动电话号码采用实名制管理；

2)移动支付加入固定的密码；

3)移动支付过程中采用共用一副密钥，并开展对称式加密进行数据交换；

4)移动支付中可采用动态密码管理的方式，密码采用唯一性管理；

5)移动支付中可运用移动 PKI 做身份认证，如 WIM。

在实际操作中，将根据不同的因素和安全需求决定不同的身份认证方式。小额移动支付认证可以采用移动电话号码和固定密码认证，大额移动支付认证可以采用固定的密码和动态密码来提高安全性。并且，以 WIM 为基础的移动 PKI 认证方式可以同时满足以上两项要求，进而可以完成更多的移动支付功能。

5 结束语

随着手机的普遍使用，用户通过手机来完成移动支付更加普及。人们不但可以通过移动支付在互联网上进行购物、处理日常消费、处理银行相关业务，还可以利用手机钱包在 POS 机上进行近距离刷卡消费，大大方便了人们的生活。但是，移动支付的安全问题不容忽视。我国在研究移动支付安全技术方面，可以采用统一标准规范，完善交易流程、加密与电子认证、在线支付、信用管理、供应链管理、系统集成等关键技术，逐步制订移动电子商务业务和技术规范，加快制定和完善行业相关业务规范和标准，并加大安全芯片、SIM 卡、智能读卡设备等研发力度，共同来推进移动支付的产业化应用。（编选：中国电子商务研究中心）