doi:10.3969/j.issn.1000-436x.2014.z2.018

商业银行移动支付安全研究

陈曦[1,2]，田有亮[3]，马卓[4]，马建峰[4]

(1. 招商银行总行 博士后科研工作站，广东 深圳 518067；2. 招商银行总行 信息技术部，广东 深圳 518067;
3. 贵州大学 理学院，贵州 贵阳 550025；4. 西安电子科技大学 计算机学院，陕西 西安 710071)

摘 要：移动支付无疑是目前互联网金融领域最为引人关注的焦点。然而，用户在享受移动支付方便快捷服务的同时，却面临着严峻的安全问题：手机木马、隐私泄露等事件层出不穷，大量具有完整攻击行为的金融支付类病毒，可在远程/近场支付过程中对用户的账户、密码、验证码等信息进行直接窃取。安全性问题已经严重阻碍了移动支付市场的进一步发展。针对上述问题，以金融机构的角度，全面梳理移动支付中的安全问题，包括移动终端安全、支付安全（包括近场支付、远程支付）、网络安全、业务交互逻辑安全等。此外，对学术界与产业界中相关安全关键技术的研究现状进行了分析与归纳。最终，基于上述阶段性的研究成果，给出移动支付安全体系设计架构与规划建议，指引未来商业银行在移动金融领域的信息安全研究重点与方向。

关键词：移动支付；终端安全；近场支付；漏洞挖掘；风险评估

中图分类号：TP393 **文献标识码**：A **文章编号**：1000-436X(2014)Z2-0131-09

Research on security of mobile payment for commercial bank

CHEN Xi[1,2], TIAN You-liang[3], MA Zhuo[4], MA Jian-feng[4]

(1. Department of Post-Doctoral Research Center, China Merchants Bank, Shenzhen 518067, China;
2. Department of Information Technology, China Merchants Bank, Shenzhen 518057, China;
3. School of Science, Guizhou University, Guiyang 550025, China;
4. School of Computer Science and Technology, Xidian University, Xi'an 710071, China)

Abstract: There is no doubt that mobile payment is the spotlight in Internet finance now. Although users can enjoy quick and convenient services, they have to face with more severe security problems at the same time: the attack incidents, such as cellphone Trojan and privacy leaks emerge endlessly. Lots of viruses which are designed for attacking financial payments can steal users' personal information including account, password and verification code in the proceedings of remote payment and near field communication. Security issues have already seriously impeded the further development of the mobile payment market. To solve the above problems, discusses the security issues in mobile terminals, payments, network and interactive logic of banking business from financial institutions' perspective was discussed systematically. In addition, current status of relevant security key technologies are summarized from academic research community and industry fields. Finally, based on related research achievements, the design of system architecture and suggestions for mobile payment security are proposed, which can guide the future development of commercial bank.

Key words: mobile payment; terminal security; near field communication; vulnerability mining; risk assessment

收稿日期：2014-06-18

基金项目：国家科技部重大专项基金资助项目（2011ZX03005-002）；国家自然科学基金资助项目（61363068, 60872041, 61072066, 61100233）；中央高校基本科研业务基金资助项目（JY10000903001, JY10000901034）；中国银行业监督管理委员银行业信息科技风险管理课题

Foundation Items: The Major National S&T Program (2011ZX03005-002); The National Natural Science Foundation of China (61363068, 60872041, 61072066, 61100233); Fundamental Research Funds for the Central Universities (JY10000903001, JY10000901034); China Banking Regulatory Committee's Banking Information Technology Risk Management Project

1 引言

我国商业银行信息化建设经过多年的发展，IT 技术已经成为银行高效运作的基础平台与核心竞争力。而随着移动互联网金融时代的到来，手机银行、微信银行等新渠道与新业务快速普及与发展，其利用移动互联网与手持设备（包括手机、平板电脑等），将银行的柜面业务延伸到移动终端，实现个人金融业务和企业金融业务的自助服务。移动支付的发展不仅可以帮助银行摆脱对网点的依赖，还可提高客户粘合度、拓展新客户、延伸新业务。此外，加快移动支付体系的建设、抢占移动入口，将帮助银行在面对移动运营商、第三方支付、电子商务企业时，占据支付价值链的上游。然而，消费者对移动金融服务的安全性仍然缺乏信任。据调查分析，消费者对移动支付最关心的三大问题依次是交易的安全性、私密性与易用性。因此，在移动社交网络、大数据时代的今天，尽快提升移动安全技术，完善移动支付、手机银行等金融服务，建立安全便捷的移动支付业务模式，是银行业急需部署的工作。

目前，移动支付主要分为远程支付（手机银行、手机支付宝）和近场支付（NFC）2 种。其中，远程支付可看作互联网支付业务的延伸；而近场支付则借助于近场通信和智能卡技术，可支持银行卡、公共事业等多种应用方式。无论是早期的短信支付、STK 支付，还是近期的 NFC 支付、Square、Google Wallet、二维码支付、微信支付等，移动支付产业链的各方都在通过技术与业务创新，使客户可以随时、随地、便捷地完成支付。移动支付可实现第三方账户、银行账户（借记卡、信用卡）、移动支付专用账户等多账户于一体，用户通过移动终端实现在线远程支付与线下近场支付。相对于常规金融支付工具，移动支付的用户粘性更强、携带更为方便、支付更加便利，线上线下的服务场景也更加丰富。而央行的扶持性政策，包括促进不同服务主体互联互通、推动区域手机支付试点，降低移动支付服务市场准入门槛、允许多方参与主体提供支付服务等，更让移动支付驶入了发展的快车道。相对于第三方支付、电信运营商等，银行在有效客户群体、营销渠道、用户粘性、业务资源、品牌效应方面的优势越来越小。在金融支付历史性大变局的今天，商业银行需尽早争夺移动支付入口,完善近场支付（小额钱包）与远程支付（绑定银行卡）体系，发展创新性支付业务模式。

然而，随着智能手机的普及，各类病毒木马和恶意软件横行，移动支付的安全问题日益严重。传统的信息安全问题主要从身份认证与通信加密 2 个方面来解决，但面对越来越多的病毒与黑客攻击，用户终端环境的薄弱性使厂商提供的安防方案大打折扣。针对 NFC 近场支付等新技术的新型攻击手段，也使传统的安全方案无法适应。移动金融的本质是资金的转移，支付核心是账户、支付介质是移动终端。因此，移动金融安全首先需要从移动终端安全、移动支付安全、业务流程安全多个角度进行全方位的考量。特别对于 NFC 近场支付技术，其安全性仍要回归 NFC 三大功能：卡模拟、读写、点对点交互。在这 3 种通信模式中，近场支付可能遭到的攻击包括窃听、数据篡改、中间人攻击等。在窃听攻击方面，目前已出现通过 NFC 手机获取非接触卡的非加密信息，进行伪卡交易的案例；而在数据篡改攻击方面，也已出现了通过应用破解篡改地铁卡余额的案例；相对于以上 2 种攻击，针对 NFC 的中间人攻击则更加多样。

利率市场化、金融自由化，银行坐享丰厚利差的时代即将逝去。同业竞争的日趋加剧与声势浩大的移动互联网金融浪潮，也使商业银行必须做出改变以迎接挑战。央行曾指出，作为一种新的金融模式，互联网金融的风险主要集中在信息安全和风险管控等方面。而移动支付作为互联网金融的入口，其安全是首要问题。独立市场调研公司 TNS 近期的调查结果显示，93%的中国消费者表示，支付是否安全是影响其考虑使用移动支付服务的重要因素。信息的机密性、真实性、支付终端的安全性、移动支付各环节的法律保障健全性，也成为移动支付能否快速推广的重要因素，需要产业链各方联手共同提高移动支付的安全性。因此，只有建立一套系统、全面、动态的商业银行移动支付安全体系，提升对移动信息技术风险的防范能力和对经营管理的安全保障能力，才能在移动互联网时代，真正提升商业银行的核心竞争能力，促进商业银行企业战略目标的实现。

2 背景

纵观历史，随着人类社会经济与科学技术的进步，支付工具经历了实物支付、信用支付、电子支付等多个阶段。而在移动通信技术与互联网技术飞

速发展的今天，迈入了移动支付时代。移动支付联盟(mobile payment forum)[1]给出了这样的定义：“移动支付，就是通过无线连接，使用一种移动通信设备作为电子支付工具使付款人向收款人进行支付的一种电子转移方式”。移动支付业务最早出现在20 世纪 90 年代初期的美国，在传入日本、韩国等东亚地区后迅速发展，如移动信用卡、移动钱包等概念的正式商用都出现在日韩等地，而 NNTT DOCOMO、SK TELECOM 等公司目前仍然是移动支付领域领跑者。而我国在移动支付发展初期，主要由电信运营商主导，通过短信 SMS 服务来为用户提供手机代扣费的方式进行移动消费。由于 SMS 信息量少、无法实现交互通信，这一阶段市场发展十分缓慢；而随着移动智能终端的不断普及、3G/4G 网络覆盖区域的逐步扩大，用户可以更快捷、方便地实时处理数据，移动支付进入了快速发展期，并出现了银行、电信运营商、第三方支付三足鼎立的局面，手机钱包、异度支付、壹钱包等创新性产品层出不穷跟。目前在市场层面，相关报告[2,3]显示 2013 年中国仅第三方移动支付市场交易规模就达 12 197.4 亿元，同比增长 707%，商业模式日益清晰；在政策层面，央行近期组建了互联网金融问题研究小组，对移动金融的重视程度正在大幅提高；而在技术层面，原有银联主导 13.56 MHz 和中移动主导 2.4G 移动支付标准之争已取得统一。此外，中国人民银行与中国银联就中国金融移动支付出台了多项技术规范，涵盖了应用安全、智能卡卡片安全、数据短信转换平台规范、可信服务管理系统规范等。标准统一意味着电信运营商与金融机构将更好地开展合作，实现受理环境的互联互通。因此，随着各方条件的成熟，预测未来移动支付市场将继续呈现爆发式的增长。

而与此同时，移动支付安全问题层出不穷。据艾瑞咨询的报告[4]显示，2013 年移动端新增恶意软件 691 639 个，是 2012 年的 5 倍，其中窃取用户隐私行为占比 49.6%。在系统层面，MasterKey 漏洞、Android 锁屏漏洞、WebView 漏洞等对用户的安全造成了很大的影响。特别国内的伪淘宝病毒，在窃取用户支付宝帐号密码的同时，还会将支付验证码转发到指定手机。而手机银行 Zitmo 等木马，通过截获上传银行短信交易码（mTAN 代码）的方式在全球范围内已经造成了接近 36 亿欧元的经济损失。该类具有完整行为的金融支付类病毒的出现，引发人们对手机支付安全的广泛关注。相关统计表明，针对 Android 系统的攻击在移动终端的安全威胁中占比最高。2013 年 Android 应用市场提交的软件中，恶意应用占比竟达 5.6%。同时，国内第三方市场的混乱也进一步造成了 APP 重打包攻击、权限提升攻击、注入式攻击的泛滥[5,6]，攻击者可利用程序漏洞或系统组件接口，实现对支付程序进程通信的监听，以及内存数据的截取。

面对上述种种威胁，商业银行应从终端安全、支付安全多个角度，对移动支付环境下存在的安全问题进行挖掘，并针对其中重点安全问题，包括手机银行客户端加固、远程近场安全支付融合等，给出相应的技术解决方案；并在金融机构的角度，根据上述安全技术研发成果与安全要素评估模型，最终形成企业级的移动支付安全体系架构设计方案，其中，具体包括移动支付信息安全系统建设规划、业务运营安全策略、信息安全规章制度、风险评估方法等，从而为商业银行移动支付的快速发展保驾护航。以下，将从终端安全、支付安全、网络安全、业务安全 4 个方面，对其中的关键安全问题进行详细的分析与阐述。

3　移动终端安全

3.1　关键安全问题

近些年，手机银行与第三方支付客户端的安全事故频发。智能手机的开放环境导致了安全问题难以杜绝，其中 Android 平台的恶意病毒与木马更是远超其他移动操作系统。因此，移动终端作为移动支付的源头与核心，其安全性至关重要。因此，将从硬件、操作系统、应用系统、信息资产等多个角度开展研究工作。对商业银行移动客户端设计方案进行代码漏洞挖掘、逆向工程分析、完整性分析以及可验证安全的评估，并考虑在客户端内嵌入支付安全管理模块，为手机银行等应用提供支付安全基础服务，实现移动支付终端的加固与完善。如图 1 所示，具体可细分为以下几个方面。

1) 硬件级安全：研究可信执行环境(TEE, trusted execution environment)与移动可信模块(MTM, mobile trusted modules)的安全体系架构。针对商业银行等金融机构，提出可支撑移动支付、数字版权等业务的安全解决方案。

2) 操作系统安全：研究主流移动终端操作系统（Android、IOS）的安全机制，包括系统沙箱机制、

签名机制、用户 ID 机制、数据访问与权限申明等安全机制。

3) 应用程序安全：设计系统化的移动应用程序安全漏洞静态分析与动态分析方法，包括 APP 代码安全、完整性校验、防跟踪/调试/窃听（逆向工程）、敏感信息保护、身份安全。此外，研究交易过程安全设计模型，保证交易流程的逻辑安全。

4) 信息资产安全：研究移动终端数据安全保护机制，具体包括密钥、证书、系统数据和用户数据等信息资产的安全保护与管理。

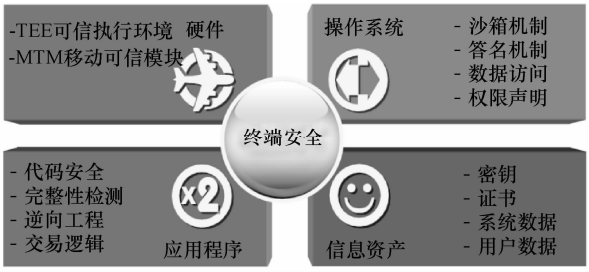


图 1 移动终端安全

3.2 研究现状

在终端安全层面，目前业界主要从硬件安全与软件安全 2 个方面展开。然而，商业银行作为金融机构，能够开展的硬件研发工作较为有限。而在软件安全方面，相关研究工作主要集中在安全威胁高发区的 Android 系统。而权限管理与沙箱机制作为 Android 安全的核心[7]，目前是学术界与产业界研究的热点。在权限安全方面， Enck 等[8]提出了基于 Permission 申请的轻量级恶意应用程序识别方法，其利用 Kirin 认证服务来实现 Permission 安全规则与应用程序特征的比对；Chin 等[9]研究了 Android 应用间的消息传递，针对消息的发送者和接收者不可信任的情况，提出了应用间组合攻击模型；David 等[10]采用统计学的(SOM, self-organizing map)算法，对基于 Permission 的安全模型进行了详细的分析与讨论；Felt 等[11]设计 Stowaway 自动检测工具，通过扫描反编译后得到的应用程序代码，将需调用的 API 集与权限集进行映射，并与程序应用配置文件中所解析出的声明权限集相比较，以确定该程序是否存在权限过度申请情况；Shin 等[12]则给出了形式化的 Permission 的授权管理控制模型；张中文等[13]利用访问控制模型对 Permission 机制工作场景进行了抽象，分析了 Permission 机制的安全问题，发现了一个可以绕过权限管理，主动提升应用程序访问权限的漏洞；Chan 等[14]提出了 DroidChecker 工具，利用过程间控制流程图搜索和静态检查，实现对权限组合攻击的检测，但该方案不支持动态注册组件，因此，存在较高的漏报率与误报率。

而在沙箱机制方面，由于 Dalvik 虚拟机中运行的进程必须依托内核层 Linux 进程而存在，因此 Android 系统使用 Linux 文件访问控制与 Dalvik 虚拟机来实现其沙箱机制。Enck 等[15]提出 TaintDroid 跟踪系统，其扩展 Android 虚拟机对隐私数据进行着色，可有效地监控并发现程序运行实例对隐私数据的滥用情况，但 TaintDroid 并未提供针对隐私泄露的阻断方案；Zhou 等[16]设计了 TISSA 隐私保护系统，通过权限的手动配置实现对隐私数据的细粒度控制；Luo 等[17]则对 Android 特定组件的安全进行研究，其指出 WebView 组件的调用将导致客户端可信计算基的瓦解，并且浏览器的沙箱保护机制也将被打破，Luo 在文献[17]中给出了 WebView 的攻击模型以及解决方案。

此外，对于重打包攻击，目前有效的检测方法包括静态分析法与动态分析法，其中静态分析包括差异分析、特征匹配、权限检测、函数检测、类别检测等。而动态分析法包括文件读写监控、网络连接监控、自定义行为匹配等。其中，Zhou [18]设计了 DroidMOSS 应用相似度度量系统，通过对 6 个第三方市场的测试比对，其发现市场中 5%~13%的应用为重打包应用。然而，该系统只对 APP 中的 Java 代码进行分析，而忽略了其中的 Native 代码（占比 5%左右）；Timothy 等[19]分析了 76 480 个 Android 市场中的应用（其中 35 423 个 Google Play 应用，41 057 个第三方市场应用），发现其中存在大量通过重打包伪装成正常应用的恶意病毒。针对该问题，Timothy 等设计了 AppIntegrity 验证协议，可有效提高 Android 市场对重打包恶意病毒的识别率；在文献[20]中，Jung 等对韩国国内 Android 市场中 7 家不同银行的手机银行客户端进行了抗重打包攻击测试，结果 7 家银行无一幸免：研究人员通过重打包方法对正常的网银客户端 APP 进行篡改后放入 Android 市场，若用户下载恶意 APP 并通过其进行转账操作，将会在不知情的情况下将资金转入攻击者指定的账户。在这个重打包攻击过程中，实施攻击的研究人员不需要获取用户任何的公钥证书、账户密码等信息，便可完成攻击；Zhou 等[21]提出了一种高效的水印机制，并给出了 AppInk 工具。

利用该工具，可有效地抵抗利用开源工具 Proguard 与 ADAM 实施的重打包攻击；然而，手机病毒繁杂多样、难以进行系统化分析，Guillermo 等[22]针对上述问题设计了基于文本挖掘与信息检索的 DENDROID 系统，其利用向量空间模型对文本挖掘建模过程进行重塑，从而实现对病毒样本的划分与归类。

4　移动支付安全

4.1　关键安全问题

基于 NFC 技术，实现基于 SE 安全元件的近场远程融合支付方案，保证个人化数据的安全性与 SE 多应用的安全性，确保其可抵抗针对 NFC 近场支付的中间人攻击、窃听攻击、篡改攻击，建立 SE 到 TSM 系统的“端到端”安全方案，是支付安全的重点方向。具体研究工作如下。

1) GP 安全规范：GP（global platform）规范定义了多应用卡的安全机制和管理机制，如图 2 所示，包括控制指令、应用下载参数、卡应用管理机制等。深入研究 GP 安全架构，包括 APDU 安全通信协议、安全通道与安全域管理，保证移动支付的多应用安全通信。

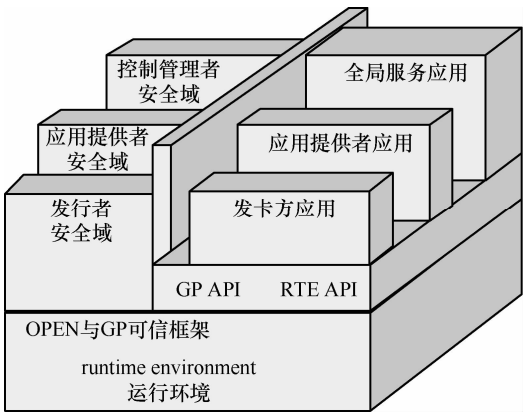


图 2　GP 安全规范

2) TSM 公共服务平台：TSM 是承担 SE 载体管理与多应用管理的实体，是联系运营商、账户管理机构、应用发行机构以及最终用户的桥梁，是保证 SE 及应用安全的基础。因此，深入研究 TSM 公共服务平台的接入管理（保证接入结构的合法性）、应用路由（保证应用的合法性）、身份验证（保证终端的合法性）机制。

3) SE 安全元件：SE（secure element）是移动支付的核心单元，是移动支付应用承载体，同时也是移动支付电子认证证书的载体。研究 SE 检测、SE 发行、SE 匹配流程，避免 SE 在实名认证与应用所有人身份匹配流程漏洞所引发的安全支付威胁。

4) 近场支付安全验证：研究 SDA 静态签名验证、DDA 动态验证、CDA 复合验证等支付验证方法，保证 POS 机与卡片进行脱机验证时的交易安全。

4.2　研究现状

NFC 近场支付技术近年来发展迅速。作为一种短距离无线通信技术，由于其方便易用，成本低廉，被广泛集成于新型手机的通信模块，用来实现手机近场支付、多媒体互联等应用。NFC 设备具有 3 种不同的工作模式[23]：读卡器模式、智能卡模式、点对点模式，其采用无线射频信号实现数据的读写与身份认证。然而，与远程支付类似，NFC 同样面临着各式各样的安全威胁。具体来讲，包括以下 4 类[24,25]：窃听、数据篡改、中间人攻击、钓鱼攻击。在窃听攻击方面，Hancke[26]给出了一个实验性的攻击过程，利用低功耗设备获取了目标对象的 ISO 14443 令牌信息；Caney[27]则设计了简易的 Android 窃听程序，并利用 Google Nexus S 手机实现了对 PNC Visa payWave 借记卡与 Clipper 交通卡中用户个人隐私信息 PII 的盗取；Thomas P[28]则在超市通过购物篮内隐藏的天线，实现了对非接触银行卡片的信息盗取；在数据篡改攻击方面，Allah [29]指出由于在链路层缺少安全保护，攻击者可以随意修改交易数据，并给出了数据篡改攻击的攻击模型；而 NFC 最大的潜在威胁是中间人攻击，在文献[30]中 Roland 等在真实环境下，实现了对 Google Wallet 的中间人攻击：在被攻击人手机端安装中继软件，利用系统权限提升漏洞实现对安全元件（SE）的访问，截获移动支付过程中的 APDU 指令信息；除此以外，在钓鱼攻击方面，Charlie Miller[31]在 2012 年的 Black Hat 大会上展示了如何通过近距离无线通信技术对 Android 智能手机进行攻击，其利用 NFC 代码解析上存在的漏洞实现手机对恶意网址的访问，从而最终在无交互问询的情况下控制用户手机。

面对上述安全威胁，学术界与产业界研究人员做出了很多努力。针对窃听攻击，Hasoo[32]通过引入伪标识与 PDU 数据单元，给出了一种有效的 NFC 用户隐私保护协议；Park[33]基于 NTRU(N-th degree truncated polynomial ring)，设计了零知识证明与环签名方案，实现了 NFC 设备间的匿名身份认证与通信，保护了用户支付交易信息的安全性；而针对

中间人攻击，文献[34]基于双设备交互认证，给出了可证安全的 NFC 身份验证方案，认证过程分为注册、认证、密钥协商 3 个部分。该方案在杜绝中间人威胁的同时，保护了用户隐私；Gummeson[35]则针对 NFC 的卡模拟、读卡器以及点对点 3 种通信模式下的非授权交互，提出了 EnGarde 安全防火墙方案，实现对恶意通信的阻断与拦截。然而，该方案并未给出防火墙安全策略的制定规则，并需要对 NFC 设备硬件进行一定的改动，因而难以在目前的 NFC 终端中实施与推广。

5 移动网络安全

1) 接入网络安全：研究 3G、4G 移动网络以及 WLAN 的网络安全策略、认证与密钥协商协议（AKA）等，分析移动终端在远程支付过程中潜在网络威胁攻击，完善移动应用程序的安全保护措施，保证安全接入。

2) 云安全：如图 3 所示，一方面，可参考并研究 Bell ID 的云 SE 与 Google Wallet 云服务[36]，针对移动支付，设计创新性的云安全产品；另一方面，针对云计算安全中的可搜索加密[37]、同态密码学开展预研工作，为下一步的移动金融体系的云部署打下基础。

6 移动业务安全

研究近场支付与远程支付相结合的支付模式，考虑金融机构和非金融支付机构互联互通、银行和运营商资源共享，打通产业链（包括移动金融终端的研发及生产、移动金融公共服务平台的建设及维护、交易内容管理平台）各方的壁垒。实现移动支付产业的良性发展，是未来移动支付的必由之路。

为用户提供一站式、个性化的服务，为企业用户提供定制化的服务，是未来移动金融的发展趋势。而在移动环境中，如何保证用户数据的机密与用户信息的隐私保护是需要重点关注的问题之一。

如图 4 所示，移动金融的快速发展，必将产生海量的零碎、即时数据（大量的小额支付与转汇帐）。银行所拥有的有效实体客户信息，结合移动金融大数据，能实现更精准的客户营销。而大数据作为银行未来的核心资本之一，其安全性显得尤为重要与关键。因此，研究行内数据库风险管理系统，保证数据资源机密性的同时，实现数据资源访问的可控性与可追溯性。

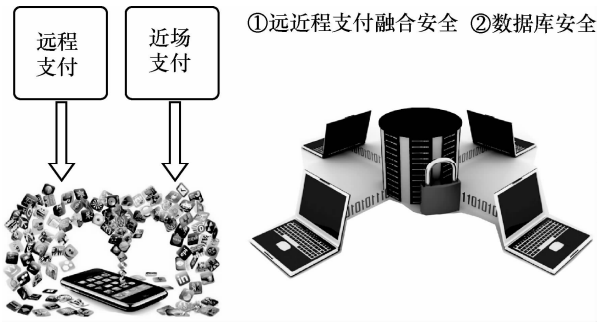


图 4 移动业务创新安全

云计算作为一种全新的业务模式，其所具有的独特能力正可以帮助国内银行推动营销模式的改变，并实现跨行业合作、提升服务能力、改善运营效率。目前，IBM 与中国工商银行联合发布了《从云计算到基于云的业务模式——国内银行未来创新机会》白皮书。如何利用混合型或共享的云架构

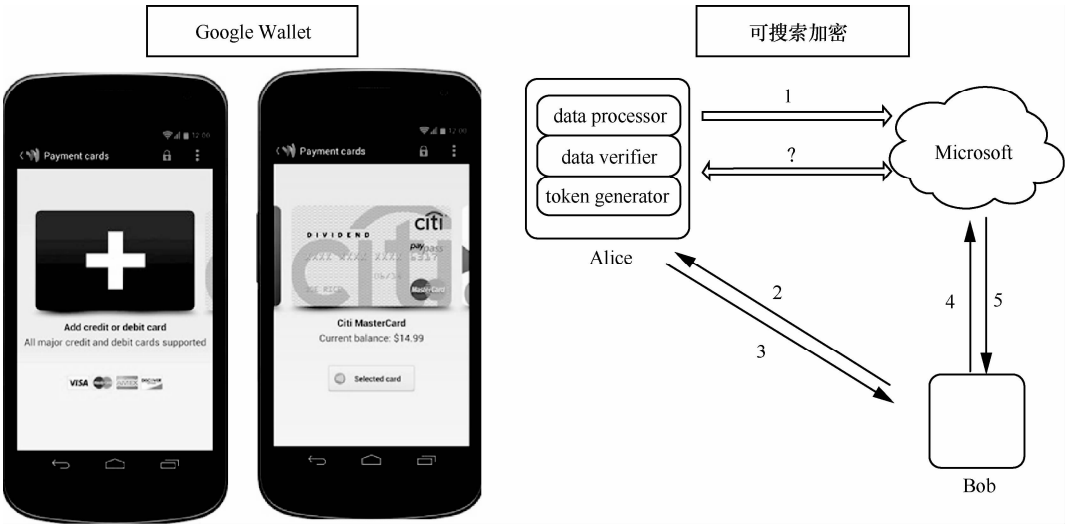


图 3 移动网络安全

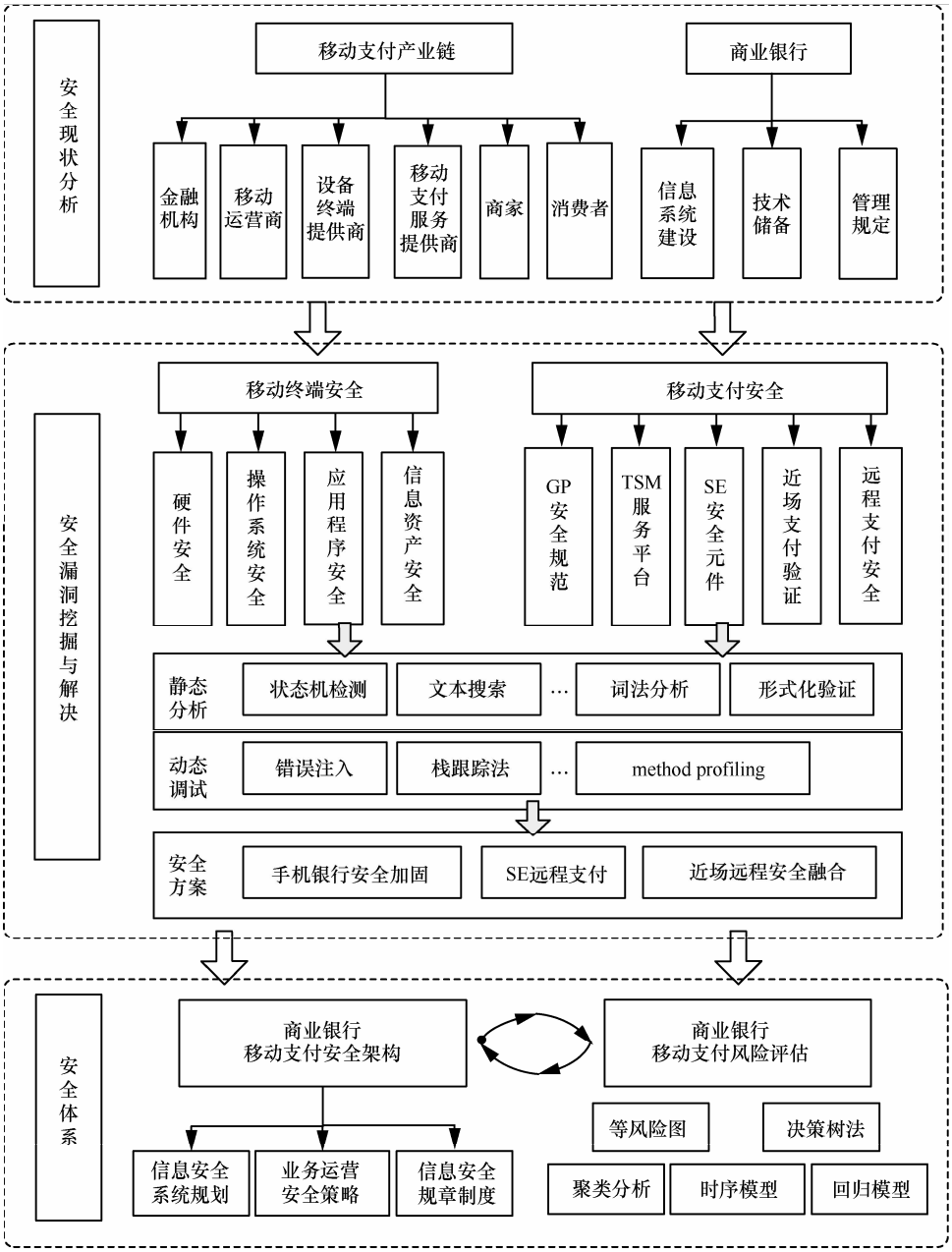


图 5　移动支付安全体系

实现移动金融信息系统的灵活性、可扩展性以及按需定制可用性的同时，保证移动支付系统以及敏感金融数据的安全性与可控性，是商业银行未来研究方向之一。

4　安全体系设计

从国内的研究现状来看，在终端安全层面，目前已经在权限保护等方面取得一些理论成果，但大多可实施性较差，未形成有效技术方案与产品。Android 恶意应用检测、动态分析等技术的研究起步较晚，多数仍停留在使用特征码匹配的阶段，不仅需要在服务器端维护海量的恶意特征码数据库，也无法对未知恶意应用及时响应和防范；而对于 NFC 近场支付，利用非接触卡伪卡交易等多样化的攻击方式使研究人员难以用传统的安全手段进行防御。特别对于手机银行加固方案、远程近场支付融合等最为迫切移动安全需求，并没有形成面向金融客户的系统解决方案。网络安全与业务安全的研究工作也都较为零散。

笔者认为，目前商业银行亟需加强移动支付体

系建设工作，应形成企业安全发展规范与顶层设计架构。具体来讲，应从安全现状分析、安全漏洞挖掘与解决、安全体系设计三大步骤，来逐步推进自身的移动安全建设。

安全现状分析：首先，需要分析和把握国内外移动支付产业的概念、特点、分类、基本要素，并详细研究产业链各个环节中存在的安全威胁与隐患，包括金融机构、移动运营商、设备终端提供商、支付服务提供商、商家、消费者。另一方面，从技术储备与管理架构两方面对自身的安全体系进行评估。

安全漏洞挖掘与解决：综合运用多种研究方法，对商业银行移动支付领域的潜在安全威胁进行分析与漏洞挖掘，包括对手机银行等移动客户端进行静态分析与动态调试，从文件访问控制、权限控制、组件封装、进程间通信等多个角度寻找其安全隐患。另一方面，针对 NFC 近场支付开展测试性攻击，分析其抵抗窃听攻击、中间人攻击的安全属性。此外，研究近场支付与远程支付的支付模式，梳理金融机构和非金融支付机构互联互通方式，评估移动支付业务的交易流程是否存在相应的逻辑安全问题。最终，对终端系统漏洞进行抽象与分类，其包括访问验证错误、缓存区错误、输入验证错误、边界条件错误与条件竞争错误等。并利用状态机检测、形式化验证、词法分析等方法，对手机银行加固、远近场支付融合等重点难点技术问题进行深入的研究，给出商业银行可实施的系统设计与技术解决方案。

安全体系设计，总结前期安全理论分析与威胁漏洞的挖掘成果，提出适应自身发展的商业银行移动支付安全架构。首先，分别从移动终端安全（包括硬件安全、操作系统安全、应用程序安全、信息资产安全）、移动支付安全等多个角度出发，总结前期的安全技术解决方案，部署云安全、移动用户隐私保护等问题的预研工，进而形成商业银行移动安全体系建设发展规划。此外，综合化考虑商业银行的移动支付业务流程中的关键安全要素，利用决策树法、时序模型、回归模型等定量分析方法，构建动态的移动支付安全评估模型，并制定移动支付业务安全运营策略与信息安全规章制度。

商业银行移动支付安全体系规划图如图 5 所示。

5 结束语

信息安全问题是移动社交网络、大数据时代商业银行必须持续关注的重点问题。随着商业模式的日益清晰、智能手机的普及以及 4G 网络的大面积覆盖，预计 2016 年中国移动支付市场交易规模将突破万亿。银行银联、移动运营商、互联网公司、第三方支付公司都在积极推进移动支付业务，而安全性对于移动支付始终是一个最为关键的问题。因此，商业银行应该转变思维方式，拥抱互联网金融。通过不断的技术创新，保证移动终端、移动支付与移动通信的机密性与有效性，逐步实现安全可靠的 3A 支付（anytime、anywhere、anyhow）。

参考文献：

[1] MÜLLER-VEERSE F. Mobile Commerce Report[R]. Technical Report, Durlacher Research Ltd, 1999.

[2] 艾瑞咨询. 2012-2013 年中国移动支付用户调研报告简版[EB/OL]. www.iresearch.com.cn, 2013.
iResearch. 2012-2013 China Mobile Payment User Behavior Report[EB/OL]. http://www.iresearch.com.cn, 2013.

[3] 艾瑞咨询. 2013 年中国第三方移动支付数据报告[EB/OL]. http://www. iresearch.com.cn, 2014.
iResearch. 2013 China Third-party Payment Platforms Data Report[EB/OL]. http://www.iresearch.com.cn, 2014.

[4] 艾瑞咨询. 2013 年中国移动安全数据报告[EB/OL]. http://www. iresearch. com.cn, 2014.
iResearch. 2013 China Mobile Security Report[EB/OL]. http://www.iresearch. com. cn, 2014.

[5] ENCK W, ONGTANG M, MCDANIEL P. Understanding android security[J]. Security & Privacy, 2009, 7(1): 50-57.

[6] ENCK W, OCTEAU D, MCDANIEL P, *et al*. A study of android application security[A]. USENIX Security Symposium[C]. 2011.

[7] DAVI L, DMITRIENKO A, SADEGHI A R, *et al*. Privilege Escalation Attacks on Android[M]. Information Security. Springer Berlin Heidelberg, 2011.346-360.

[8] ENCK W, ONGTANG M, MCDANIEL P. On lightweight mobile phone application certification[A]. Proceedings of the 16th ACM Conference on Computer and Communications Security[C]. 2009. 235-245.

[9] CHIN E, FELT A, P, GREENWOOD K, *et al*. Analyzing inter-application communication in android[A]. Proceedings of the 9m International Conference on Mobile System, Applications and Services[C]. 2011.

[10] BARRERA D, KAYACIK H G, VAN OORSCHOT P C, *et al*. A methodology for empirical analysis of permission-based security models and its application to android[A]. Proceedings of the 17th ACM Conference on Computer and Communications Security[C]. 2010. 73-84.

[11] FELT A P, CHIN E, HANNA S, *et al*. Android permissions demystified[A]. Proceedings of the 18th ACM Conference on Computer and Communications Security[C]. 2011.627-638.

[12] SHIN W, KIYOMOTO S, FUKUSHIMA K, *et al*. A formal model to analyze the permission authorization and enforcement in the Android framework[A]. 2010 IEEE Second International Conference on Social

Computing (SocialCom)[C]. 2010.944-951.

[13] 张中文, 雷灵光, 王跃武. Android Permission 机制的实现与安全分析[J]. 信息网络安全, 2012, (8): 3-6.
ZHANG Z W, LEI L G, WANG Y W. Studying the implementation and security of the permission mechanism in Android[J]. Netinfo Security, 2012, (8): 3-6.

[14] CHAN P P F, HUI L C K, YIU S M. Droidchecker: analyzing android applications for capability leak[A]. Proceedings of the fifth ACM conference on Security and Privacy in Wireless and Mobile Networks[C]. 2012.125-136.

[15] ENCK W, GILBERT P, CHUN B, *et al*. TaintDroid: an information-flow tracking system for realtime privacy monitoring on smartphones[A]. Proceedings of the 9m USENIX Symposium on Operating Systems Design and Implementation[C]. 2010.

[16] ZHOU Y J, ZHANG X W, JIANG X X, *et al*. Taming information-stealing smartphone applications on android[A]. TRUST[C]. 2011. 93-107.

[17] LUO T B, HAO H, DU W L, *et al*. Attacks on Web view in the android system[A]. Proceedings of the Annual Computer Security Application Conference[C]. 2011.

[18] ZHOU W, ZHOU Y, JIANG X, *et al*. Detecting repackaged smartphone applications in third-party android marketplaces[A]. Proceedings of the Second ACM Conference on Data and Application Security and Privacy[C]. 2012.317-326.

[19] VIDAS T, CHRISTIN N. Sweetening android lemon markets: measuring and combating malware in application marketplaces[A]. Proceedings of the Third ACM Conference on Data and Application Security and Privacy[C]. 2013.197-208.

[20] JUNG J H, KIM J Y, LEE H C, *et al*. Repackaging attack on Android banking applications and its countermeasures[J]. Wireless Personal Communications, 2013.1-17.

[21] ZHOU W, ZHANG X, JIANG X. AppInk: watermarking Android APPS for repackaging deterrence[A]. Proceedings of the 8th ACM SIGSAC Symposium on Information, Computer and Communications Security[C]. 2013.1-12.

[22] SUAREZ-TANGIL G, TAPIADOR J E, PERIS-LOPEZ P, *et al*. Dendroid: a text mining approach to analyzing and classifying code structures in Android malware families[J]. Expert Systems with Applications, 2014, 41(4): 1104-1117.

[23] MADLMAYR G, LANGER J, KANTNER C, *et al*. NFC devices: security and privacy[A]. Availability, Reliability and Security, 2008[C]. ARES 08, Third International Conference on IEEE, 2008.642-647.

[24] HASELSTEINER E, BREITFUB K. Security in near field communication (NFC)[A]. Workshop on RFID Security RFIDSec[C]. 2006.

[25] MULLINER C. Vulnerability analysis and attacks on NFC-enabled mobile phones[A]. Availability, Reliability and Security ARES'09[C]. 2009.695-700.

[26] HANCKE G P. Practical eavesdropping and skimming attacks on high-frequency RFID tokens[J]. Journal of Computer Security, 2011, 19(2): 259-288.

[27] CANEY R, DORROS C, KENNEDY S, *et al*. Mobile Pickpocketing: Exfiltration of Sensitive Data through NFC-enabled Mobile Devices[R].Technical Report, CMU-cyLab-13-015, Carnegie Mellon University, 2013.

[28] DIAKOS T P, BRIFFA J A, BROWN T W C, *et al*. Eavesdropping near-field contactless payments: a quantitative analysis [J]. The Journal of Engineering, 2013, 1(1).

[29] ALLAH A, MOSTAFA M. Strengths and weaknesses of near field communication (NFC) technology[J]. Global Journal of Computer Science and Technology, 2011, 11(3).

[30] ROLAND M. Applying Recent Secure Element Relay Attack Scenarios to the Real World: Google Wallet Relay Attack[R]. arXiv preprint arXiv:1209.0875, 2012.

[31] Charlie Miller. Exploring the nfc attack surface[EB/OL]. http://media.blackhat.com, 2012.

[32] EUN H, LEE H, OH H. Conditional privacy preserving security protocol for NFC applications[J]. Consumer Electronics, IEEE Transactions on, 2013, 59(1): 153-160.

[33] PARK S W, LEE I Y. Anonymous authentication scheme based on NTRU for the protection of payment information in NFC mobile environment[J]. Journal of Information Processing Systems, 2013, 9(3).

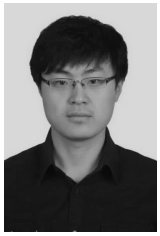
[34] LEE Y S, KIM E, JUNG M S. A NFC based authentication method for defence of the man in the middle attack[A] .Proceeding of the 3 rd International Conference on Computer Science and Information Technology (ICCSIT'2013)[C].2013.4-5.

[35] GUMMESON J J, PRIYANTHA B, GANESAN D, *et al*. EnGarde: Protecting the mobile phone from malicious NFC interactions[A]. Proceeding of the 11th Annual International Conference on Mobile Systems, Applications, and Services[C]. 2013.445-458.

[36] DYKES R. Cloud based electronic wallet: U.S. Patent Application 13/468,686[P]. 2012-5-10.

[37] KAMARA S, LAUTER K. Cryptographic Cloud Storage[M]. Financial Cryptography and Data Security, Springer Berlin Heidelberg, 2010.136-149.

作者简介：



陈曦（1984-），男，浙江绍兴人，博士，招商银行总行博士后，主要研究方向为移动支付安全、逆向分析、安全协议等。

田有亮（1982-），男，贵州盘县人，中国科学院信息工程研究所信息安全国家重点实验室博士后，贵州大学副教授，中国计算机学会、中国密码学会、ACM 会员，主要研究方向为博弈论、安全协议分析及分布式密码体制等。

马卓（1980-），男，陕西西安人，西安电子科技大学副教授，中国计算机学会、ACM、中国密码学会会员，主要研究方向为可信计算、网络安全等。

马建峰（1963-），男，陕西西安人，西安电子科技大学教授、博士生导师，主要研究方向为密码学、计算机网络与信息安全。