手机银行业务的安全问题研究

方泽南，刘卫刚，余光卓
(深圳桑达电子集团有限公司，广东 深圳 518031)

摘 要：随着移动互联时代的来临，手机银行业务迎来了前所未有的发展机遇，对手机银行安全性的担忧也在不断升温。概述了手机银行业务的发展趋势，分析了现有手机银行的风险防范措施及存在的不足，提出了基于安全加密金融卡的安全解决方案，对手机银行业务的发展以及国家金融安全稳定具有重要意义。

关键词：手机银行；身份认证；信息安全
中图分类号：TP309 **文献标识码**：A **文章编号**：1674-7720(2013)24-0004-03

Research on the security of mobile banking business

Fang Zenan, Liu Weigang, Yu Guangzhuo
(Shenzhen SED Electronics Group Co., Ltd., Shenzhen 518031, China)

Abstract: With the coming of age of mobile Internet, mobile banking has ushered in unprecedented opportunities for development, security concerns are also on the rise. This article provides an overview on the developing trends of mobile banking, analyses existing risk-controlling measures and their flaw, and proposes a new security solution based on T-card certification. It's significantly important for the mobile banking, as well as national financial security and stability.

Key words: mobile banking; identity authentication; information security

随着计算机技术与移动技术日益完善的结合，新型的移动智能通信终端的概念影响到了社会各个领域和阶层。随着智能终端的迅速普及，移动电子商务和移动金融业务高速发展，成为当今广义互联网领域炙手可热的话题。

由于手机银行业务大部分是基于手机号码上绑定的银行卡、信用卡来完成的，通过对敏感数据的盗取来操控被盗者账户的案例时有发生；病毒感染、信息截获、密码破解等都对手机银行业务造成巨大的安全隐患和经济损失。本文针对手机银行的安全性进行分析，并提出一种全新的安全方案。

1 手机银行业务的发展

手机银行是继网上银行之后出现的一种新的银行服务方式，在具备网络银行全网互联和高速数据交换等优势的同时，又突出了手机随时随地的移动性与便携性，从而为银行客户提供个性化、综合性的服务，并减轻银行柜面压力，因此迅速受到银行的青睐。伴随着中国移动互联网时代的来临以及智能手机终端的普及，未来商业银行必将围绕手机银行推出更多的增值业务。

由于蕴含的巨大的商机，移动支付业务吸引了全球众多知名商业银行和移动运营商的积极参与，从全球范围看，逐步形成了日韩领先、欧美跟进、中国追赶的局面。

截止 2012 年底，我国的手机银行用户达到 9 800 万，手机银行资金处理规模已达到 8 000 亿元。预计到 2015 年，中国手机银行用户将超过 3 亿，资金处理规模可以突破 9 万亿。

2 手机银行业务面临的安全威胁

手机银行虽然使用越来越广泛、越来越便捷，但是与网上银行一样面临着不同的风险。手机银行作为一种实体银行的虚拟环境，不仅有传统银行所具有的风险，而且由于它具有即时性、虚拟化等特点，风险要远远高于传统银行。目前，我国手机银行业务存在下列的安全风险。

2.1 核心系统的技术风险

手机银行业务的开展都需要核心技术平台来支持，因此银行必须设定特定的技术解决方案来支撑。如果设计方案存在漏洞，那将会给银行带来一定的风险。同时各商业银行都是通过客户端进行手机银行业务，网络与设备出现问题、病毒侵入以及突发事件都会给手机银行

业务带来风险。银行安全措施做的不到位，一旦计算机病毒侵入往往会造成主机系统崩溃、数据丢失等严重后果；或者系统遭黑客侵入，对手机银行的客户信息进行窃取和修改，这不仅会给客户造成不小的经济损失，同时银行在声誉上和经济上也会受到伤害[1]。

2.2 手机操作系统的恶意入侵

智能手机是搭载手机银行客户端软件的终端设备，它所面临的威胁直接影响到手机银行和移动支付的安全，智能手机技术的发展，使得智能手机的使用得到普及，截止 2012 年年底，iOS 与 Android 系统几乎占据了智能手机市场全部份额，Android 系统为 68.8%，iOS 系统为 18.8%。

由于 Android 操作系统的开放性特点，市场上针对 Android 平台的恶意程序、病毒、木马等远超其他操作系统，Android 系统的恶意代码占比达到 98.96%[2]。

2.3 针对手机银行客户端的攻击

智能手机操作系统并不像 PC 操作系统拥有有效安全保护机制，给手机银行终端软件带来了极大的安全威胁。这些威胁中，主要来自于窃取用户信息和盗用用户身份，此类比例在逐年增高。要弄清如何防范对手机的攻击，首先要了解攻击手段：

(1)程序代码攻击威胁

程序代码攻击泛指病毒、蠕虫、间谍程序与恶意程序等攻击，这些如同被植入的后门程序，会造成系统当机、资料被窃取或无法执行等情况。可通过软件逆向工程、二次打包等方式进行攻击。

(2)钓鱼、中间人攻击

钓鱼、中间人攻击是非法用户盗取合法用户的身份鉴别资料或证书时所采取的攻击行为，若不使用证书，一般身份鉴别资料（如账号与密码），即可轻易遭受攻击，采用证书还必须知道合法使用者私钥，以减少被攻击成功的机会。

(3)窃听攻击

目前窃听攻击的方式众多，如窃取敏感数据、篡改交易关键数据等，是最普遍的一种攻击手段，通过被植入的恶意程序或后门木马程序进行恶意监听和内存数据截取攻击；要预防此类的攻击唯有加强传输端加密算法的设计，采用可信赖的证书机制防止此类攻击。

(4)使用者身份真实性威胁

当移动用户使用手机进行资料查询或网络交易时，都有可能遭受到资料被攻击者窃取，则攻击者将以窃取的资料，通过恶意攻击程序不断地攻击，若移动用户登录的网站或移动设备中没有可以识别使用者身份的安全机制，即会产生安全性的威胁。

(5)资料机密性威胁

资料要具有机密性，最简单的就是采用加密方式。使用手机再传递交易信息时，必须在手机端先将资料加密后再传送至服务器端，或者使用具有 SSL 功能的浏览器，保护资料传输的安全性。若采用安全防护机制，发生传输安全问题时，手机端内存资料与传输中的信息由于已经加密，攻击者无法解开加密资料，减少了移动用户资料遗失的风险。

(6)传输安全性威胁

传输安全性攻击泛指信息传递中，被偷听、窃取、重送与伪造，市面上已经有不少可执行重复攻击的程序，若手机端出现安全性的漏洞，攻击者将会有机可乘。应随时修补移动系统产生的安全漏洞，防止手机遭受传输安全性攻击，而传送的资料一定要经过加密[3]。

以上的威胁手段会造成用户的卡号、账号、密码等敏感数据的泄露。不法分子利用这些数据，通过钓鱼、监听、利用程序、系统漏洞等手段伪冒交易，伪造资金转账、消费，窃取用户账户的资金，给用户以及银行造成巨大的损失，必须采取相应的安全解决方案进行防范[4]。

3 现有的安全技术措施

手机银行依赖智能手机及移动互联网。手机银行或支付客户端的安全加密是解决此类安全问题的必要手段。常用的方法有身份识别技术、数据的完整性和保密性技术。

3.1 身份识别

身份鉴别即验证移动用户信息，移动用户在取得用户证书后，由证书取得的公钥来检验身份与签章的正确性，经由身份验证程序方能取得连接到手机银行服务端的通行码，才能取得相应的服务权限。

目前各大商业银行都对手机银行采取了客户身份信息和手机号码绑定的方式进行安全防范，当客户输入密码和个人身份信息时，数据立即被加密编码，同时保证机密信息传输的单向性。在这过程中，若客户输入信息错误，或者线路出现故障，系统立即终止交易并返回到登录页面再进行身份鉴定。为了保证手机银行的操作过程是按客户意愿进行的，手机银行系统另行设计了客户二次确认机制，防止信息被窃取。

3.2 数据的完整性和保密性

手机银行业务是客户利用手机以及相连接的无线网络来完成业务操作的，一旦客户的手机网络信号不好时，往往会导致信息延迟和数据的不完整。因此，移动通信系统中提供相应的机制来应对这种事情的发生。同时建立相应的安全机制，使用证书的公开密钥系统，经由加密与数字签名来保证数据资料的完整性以及机密性。

手机银行整个系统采用端对端的加密数据传送方式来保证数据的保密性。交易数据在传送之前，手机端和手机银行服务平台建立一个安全通道，如果客户提供的帐号密码和验证信息正确，客户与服务器才能建立连接，客户才能进行交易，这样客户的敏感和机密信息得到保护。这些手段和措施在一定程度上保证了手机银行业务的安全性[5]。

4 风险及其防范

目前银行针对上述身份认证及其配套的保密措施仅仅以用户账号、密码口令、交易码作为用户身份的有效性检验，当这些信息被非法窃取时，业务运行的安全性将受到很大的挑战。

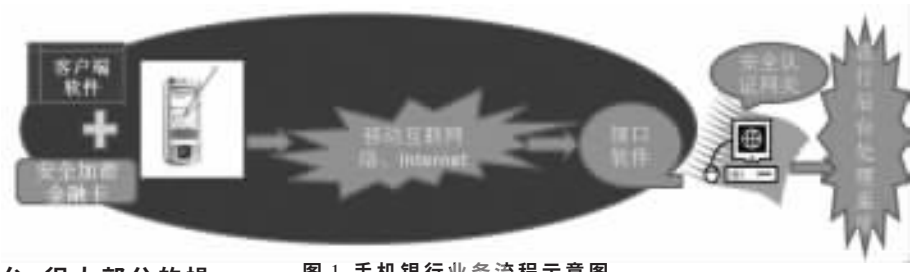

图 1 手机银行业务流程示意图

手机银行业务以手机作为操作平台，很大部分的操作系统是开放性的。大部分客户对操作系统本身不熟悉、不关注，给不法分子有可乘之机。由于客户端软件原则上是由银行发布并更新的，一般不会受到用户的注意和怀疑。用户在手机客户端输入真实的客户资料(身份证、账号、密码等)很可能被木马截取并通过短信、邮件秘密发送到预先设定的手机或者邮箱。手机银行业务的安全防范体系会变得非常脆弱，由于身份证、账户、密码等信息的泄露导致的资产损失风险也大大增加。

借鉴网上银行的技术方案，提出手机银行的安全防范解决方案：在现有的交易体系和流程中，增加安全加密金融卡的身份认证方式(见图 1)。安全加密金融卡的物理和电器性能与标准的 T(micro SD)卡一样，可以直接插入大多数智能手机。金融卡内置单片机或智能卡芯片，可以存储用户的密钥或数字证书，利用卡内的密码算法实现对用户身份的认证。运行时，首先对硬件金融卡进行认证，合法的用户才被允许进一步操作。这样，即使手机被放置了木马，非法用户如果没有得到金融卡及其相应密码，也无法登录网上银行开展业务，也就不容易截取用户的私密信息。安全加密金融卡的功能和工作原理与计算机网络中的 U 盾相同，能大大提高手机银行的业务安全，并且其具备以下优点：(1)安全有效，已经在计算机网上银行的实践中得到证明；(2)有计算机网上银行的先例，很容易被银行和用户理解和接受；(3)参照计算机网上银行的系统架构和实施办法，这种方案很容易规划设计和实施。

现有手机银行的业务存在安全防范的薄弱环节，本文提出了一种利用安全加密金融卡保证手机银行业务安全的有效且实用的解决方案。该方案保证手机银行在客户端是可信的、安全的。由于安全加密金融卡或者 U 盾是由一组集成电路(控制芯片+存储单元等)构成的，就象手机的 SIM 卡，也存在能够被硬拷贝的可能。如果安全加密金融卡或者 U 盾被硬拷贝，手机或者网上银行业务的安全性将会受到威胁[6]。因此需要一种针对客户端身份信息和证书硬拷贝的安全解决方案，这在本人其他论文中将会详细阐述。

参考文献

[1] 张纪. 手机银行风险分析与安全策略[J].海金融，2006(2):76-77.
[2] 张忠永.从国际经验看中国手机银行发展 [J].银行家，2013(4):127-128.
[3] 刘以研，白璐.信息技术条件下的手机银行安全问题研究[J].情报科学，2012,30(4):609-612.
[4] 徐杰. 电子银行安全评估方法探讨[J]. 中国金融电脑，2012(11):50-54.
[5] 柯海清，冯启明.数据加密技术及网络应用[J].武汉理工大学学报(交通科学与工程版),2002，26(6)：818-821.
[6] 方泽南.具有加密功能的移动存储器[P].专利 200820212055.9，2009.

(收稿日期：2013-09-12)

作者简介：
方泽南，男，1965 年生，博士，高级工程师，主要研究方向：保密存储、移动支付与信息安全。