第 61 卷　第 3 期
2008 年 5 月
武汉大学学报（哲学社会科学版）
Wuhan University Journal（Philosophy & Social Sciences）
Vol. 61. No. 3
May 2008. 409～414

移动银行的信息安全及防范对策

聂　进　胡现玲

[摘　要] 移动银行是商业银行借助现代信息技术和无线通信技术，向客户提供金融信息和交易服务的新型金融服务方式，是当代金融业发展的新趋势。与网上银行相比，移动银行作为一种实体银行的虚拟环境更加安全。由于其涉及了更多的无线通信和其他相关技术，其潜在的信息安全问题也更加复杂。根据信息安全原则，针对移动银行信息安全问题，应进行加密技术、身份认证、数字签名、WPKI 技术等移动安全技术进行防范。

[关 键 词] 移动银行；信息安全；加密技术
[中图分类号] G350　[文献标识码] A　[文章编号] 1672-7320(2008)03-0409-06

移动通信技术的成熟和广泛商业化为移动银行的发展提供了通信技术基础，而功能强大、价格便宜的移动通信设备的普及为移动银行的兴起和发展创造了有利条件。移动银行与网络银行一样，可以为我们提供账户查询、资金转账、在线炒股等各种银行服务，不受时间和空间的限制；同时，在我们紧急需要服务（如查询最近的 ATM 位置）时移动银行可以利用定位系统及时提供服务[1]（第 81 页）。与网络银行相比，移动银行能为客户提供更为方便、快速、即时、高效、个性化的服务[2]（第 229 页），这也是移动银行逐步被人们接受的魅力所在。

与网上银行相比，移动银行具有更高的安全性。这是由于移动银行网络基本上是封闭的，其数据通信采用端到端的加密技术和高强度加密协议；同时，还采用了数字签名机制和手机与银行卡的绑定机制，而且移动设备具备非常强大的内置认证特征和标准的安全设施；与多人共用 PC 机不同，手机是私人所属物，所有这些因素共同确保了移动银行的安全。

由于移动银行是基于无线通讯网络，数据传输过程属于开放的，而且相对于有线终端，移动终端具有系统资源有限、处理能力低、存储能力小等特点[2]（第 228-238 页），再加上银行经营资金业务的特点，致使移动银行容易成为非法入侵和恶意攻击的对象，存在随时遭受攻击的风险。因此，移动银行作为一种实体银行的虚拟工作环境，其交易不仅有与传统银行相类似的安全问题，而且由于它所独有的移动性、虚拟性和即时性等特点，其潜在的安全问题比传统银行及网络银行更加复杂。据国外的研究调查表明，安全问题是移动银行不能有效推广应用的最大障碍[3]（第 392 页）。因此，如果银行要在这个新的领域占有一席之地，必须关注移动银行所面临的信息安全问题。

一、移动银行的信息安全问题

（一）移动银行系统的组成

移动银行是依托移动通信网络（如 GSM、GPRS、3G 等），使用手机、PDA 等移动通信终端设备，通过基于 STK 技术的短信、WAP、BREW 等多种技术模式来办理银行相关业务（如银行转账、自助缴费等）的虚拟银行，是货币电子化与移动通信业务相结合的一种电子商务。

收稿日期：2008-01-05
作者简介：聂　进，武汉大学信息管理学院副教授；湖北 武汉 430072。
胡现玲，武汉大学信息管理学院硕士生。

移动银行系统,就我国的应用情况而言,一般是以用户随身携带的移动设备为终端,借助移动运营商的服务平台,通过用户和银行签定金融服务协议,为用户和银行打造一个以客户服务为中心,集各种银行服务资源(网上银行、ATM 等)为一体的、综合运用多种通信技术与渠道的新一代金融服务平台。其中,移动设备、移动运营商通过无线通信网络连接,而移动运营商与银行系统之间通过互联网或金融专用网进行连接(如图 1 所示)。

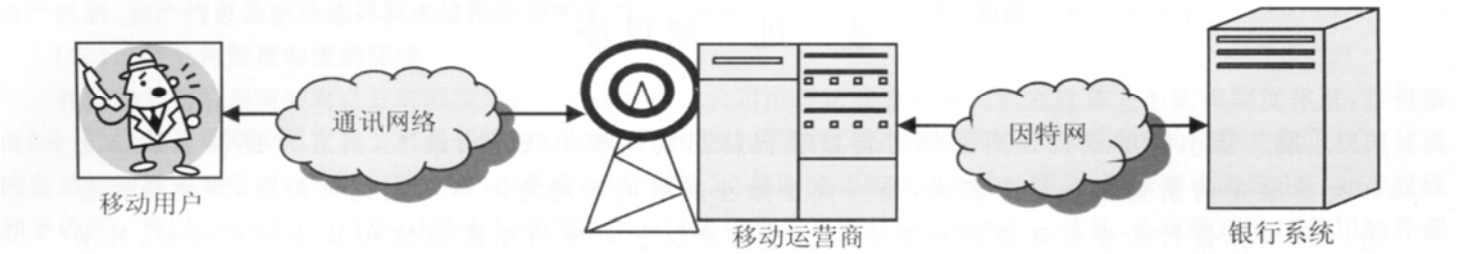

图 1 移动银行系统的构成

移动银行系统整合了多种无线通信渠道,综合了各种技术模式的优点,具有良好的可拓展性,为提供个性化、以客户为中心的崭新的金融服务模式奠定了良好的技术基础。我国已实施移动银行业务的各个银行都在竭力综合利用多方位的移动服务渠道和各种技术模式(如表 1 所示),尽可能使自己所提供的服务方便安全、无用户接入壁垒、覆盖范围广、实用性强,以便开发更多的客户资源。

表 1 中国的移动银行的技术模式

银行名称	技术模式
中国银行	基于 STK 卡的短信方式
中国建设银行	BREW 和 WAP
中国交通银行	WAP
中国招商银行	WAP2.0 和基于 STK 卡的短信方式
中国工商银行	基于 STK 卡的短信方式,短信有特定的格式
华夏银行	手机支持 USSD 协议
兴业银行	WAP 和 KJAVA

资料来源:作者根据中国各大银行网站所公布的移动银行技术模式进行综合绘制(2007 年 12 月)

(二)移动银行的信息安全问题

与电话银行、网上银行相比,移动银行的安全性是相对较高的。但移动银行并非固若金汤,毕竟许多安全性相对比较好的加密技术和认证措施因移动设备运算和存储能力所限而不能利用,并且移动银行经营资金的特点也会使它成为非法入侵和恶意攻击的对象,存在随时遭受攻击的风险。

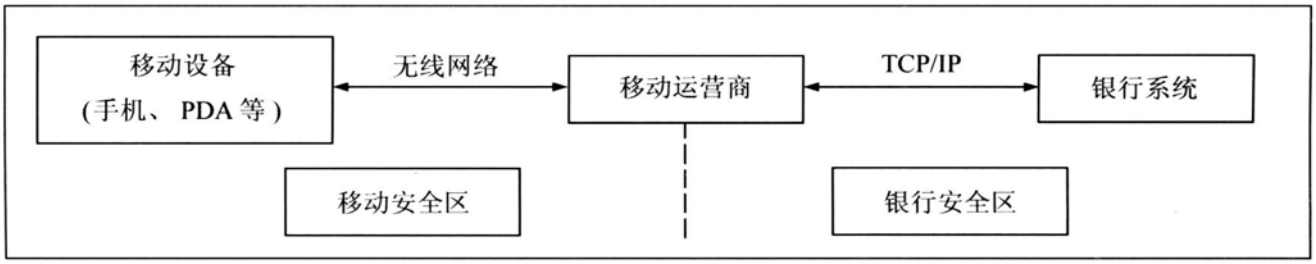

图 2 移动银行的安全区域

与网络银行在终端设备和银行应用系统间只有一个安全区域相比,移动银行将面临双安全区域[4](第 31-32 页):一是在用户和移动运营商之间,二是在运营商和银行之间(如图 2 所示)。其中,在运营商和银行系统这个安全区域面临着与网络银行相似的信息安全问题,如网络入侵、病毒攻击等,但在用户和移动运营商之间,由于涉及到无线通讯网络的应用和移动设备自身的特点,使得移动银行在信息安全

方面有以下几方面的特点：

1.信息的泄露、丢失和被篡改。由于移动银行需要通过无线网络来传递信息[5]（第 247 页），无线网络利用无线电波进行传播，与有线网络的传播媒介大部分处于地下等一些相对比较安全的场所相比，当前的无线网络技术几乎没有提供控制覆盖区域的手段和方法，当然也就无法对无线介质进行控制。因此，攻击者可能通过搭接、在电磁波辐射范围内安装接受装置等方式，截获在移动通信网络上传输的机密信息，删除、修改、添加或重发某些重要信息，干扰合法用户的正常使用。

2.信息的不完整性。由于移动设备的移动性以及传输信道的不稳定性等特点[6]（第 43 页），容易造成通信数据的不完整。当客户的手机从无线信号良好的地区进入覆盖不好的地区时，或者受到其他信号干扰时，往往会发生信息延迟或通讯失败，这样易造成交易数据的不完整或数据丢失[7]（第 3-4 页）。除此之外，移动设备的电量不足，也会导致正在进行的银行业务因发生中断而造成交易数据的不完整性。

3.拒绝服务攻击。攻击者占领短信网关或者利用网关漏洞向手机发送大量短信，进行短信拒绝服务攻击。通过特定装置持续对移动银行服务系统进行干扰，改变其正常的服务流程，或执行无关程序使系统响应速度减慢甚至瘫痪，或者对移动设备进行通信干扰，使合法用户无法正常进入移动银行系统或不能得到响应的服务。

4.病毒攻击。尽管目前所发现的手机病毒主要限于破坏手机功能、损耗手机电量、清除手机中的记录信息等，但其对移动银行的潜在威胁要远大于网络银行[5]（第 245-246 页）。这是由于移动终端所携带的病毒不仅可以感染无线网络的终端操作系统，还可以感染固定网络的终端操作系统（如“韦拉斯科”可同时在手机 Symbian 操作系统和电脑 windows 系统上运行）；其次，受移动设备的运算能力所限，杀毒软件目前很难使用；再者，很多无线网络都没有防毒措施。近日，俄罗斯发现了首例可以通过手机网络传播的计算机病毒。这种病毒可以感染运行 Symbian 操作系统的手机，还能通过蓝牙技术传播，即手机中毒后会启动蓝牙功能将病毒打包成为安全文件传到临近其它已打开蓝牙功能的手机上。因此，如不能对病毒进行有效防范，其重要数据将会被破坏，进而给移动设备和客户的切身利益带来威胁。

二、移动银行的信息安全技术防范对策

从以上移动银行信息安全问题的分析中可以看出，移动银行与网络银行在信息安全问题方面有很大差别，移动银行面临的安全问题更加复杂。因此，我们不能将网络银行的安全策略简单地移植到移动银行系统中，而应该在借鉴网络银行信息安全的基础上，根据移动银行自身的特点来引入新的安全技术和措施以保障移动银行的安全。有关移动银行安全措施与对策主要有以下几点：

（一）用更好的加密技术来实现数据保密性

加密技术是保证移动银行系统安全所采用的最基本的安全措施，通过对信息加密可以达到保证传输信息的机密性、完整性和确定性，防止信息被篡改、伪造和假冒，进而满足移动银行对保密性和安全性的需求。尽管目前一些安全机制已在手机以及无线通信网络的设计中被考虑到了，并且所使用的无线传输的基础结构如 GSM 也采用了加密技术。但是，就移动银行应用而言，这些加密技术和传输层安全机制对银行这种时常涉及机密和敏感信息（如 PIN 和银行登录密码）的保护力度是不够的。当前许多安全性相对比较好的加密和认证措施都需要客户端有比较强大的运算能力和存储能力来支撑，在网络银行的客户端是运算能力非常强大的 PC 机，可以使用这些复杂的加密和认证技术来确保安全，而移动银行的终端设备处理能力低，这就限制了复杂加密认证技术的应用，从而带来安全隐患。

为了降低加密所需的计算强度，同时又保证较高的安全性，目前移动设备开始利用对称加密算法 AES 和非对称加密算法 ECC 这两种加密技术，即以 AES 为“内核”，ECC 为“外壳”，对于无线通讯传输的数据可用 AES 加密，而加密用的密钥则用 ECC 加密传送，此种方法既保证了数据安全又提高了加密和解密的速度。这是由于 AEC 和 ECC 都是目前最安全的加密技术[8]（第 20-21 页），现有的攻击方法都不能实现对其有效的攻击。当攻击者选择攻击密文，则需要直接攻击 128 位的 AES，这在现有的技

术条件下是极其困难的;若选择攻击ECC的会话密钥,则又面临棘手的ECDLP数字难题,且会话密钥只使用一次,此后不会再有效,即使得到密钥也没有多大的使用价值。除此之外,这种混合算法的密钥管理量非常小,减小密钥的管理量,也就提高了安全性。

(二)系统和数据完整性

针对移动终端在通信过程中所造成交易数据的不完整性,移动通讯系统应该提供相应的机制,用来防止这种数据不完整性的发生。其中载波通道、手机终端、网关、服务器等设备时时面对恶意手机病毒以及其他恶意攻击的威胁。因此,手机银行系统应当配备适当的安全措施,如防火墙、入侵检测系统和快速恢复机制保证数据安全。完整性机制应当能够对系统、文件编码进行完整性检测,用以保证手机银行系统的完整性,在数据传输过程中,数据不完整或传输失败的情况都应当及时记录分析,以便找到系统中的漏洞。

(三)身份认证

身份认证是移动银行的第一道重要防线,是其它安全机制的基础。在开放式的网络环境中,只有实现了有效的身份认证,才能保证访问控制、安全审计、入侵防范等安全机制的有效实施。实现身份认证主要通过以下几种形式[9](第48-49页):实体所知道的东西,如口令、密钥等;实体所拥有的东西,如智能卡、网络钥匙等;实体所具有的某种特征,如人的指纹、声音等特征。目前,在我国的移动银行业务中使用比较多的是STK卡(如中国银行、工商银行、招商银行等),客户和银行通过签订协议将客户身份信息与手机号码进行唯一绑定,加上登录密码的验证与控制,通过建立客户身份信息、手机号码、登录密码三重保护机制对客户进行身份认证。但是,将手机号码和银行登录密码作为身份标识其安全性并不是很高,并且不受法律保护。银行登录密码属于静态密码,虽简单易记,但移动设备的移动性和易丢失等特点使客户在开放的环境中登录移动银行时容易遭受肩窥攻击、穷举攻击和字典攻击等[9](第68页)。韩国作为世界移动银行的开拓者,已研发了基于WIPI移动平台的动态认证系统DAS4M[9](第71-73页),DAS4M通过在移动设备屏幕上随机显示字符表,然后利用置换根据口令在随机显示的字符表中所处的位置来选择在移动设备键盘中所对应的数字来实现的。尽管这种系统给使用者带来不便,但能很好的防止肩窥攻击和词典攻击。因此,我们也可以借韩国之鉴将目前网络银行所使用的动态密码及其它技术应用到移动银行,来确保移动银行的安全。

生物认证以人体具有的惟一的、可靠的、终生稳定的生物特征作为认证依据,从理论上说,生物特征几乎无法被造假和冒用,因此它具有其它的认证技术不可比拟的安全性和可靠性。声纹、虹膜、视网膜、脸部特征识别,都是以非接触方式进行,易于被用户接受。但目前多数仍处于研究实验或小范围应用阶段,由于识别设备成本高、对识别正确率没有确切结论、采取的特征会由于某些因素呈现不稳定性等原因,该技术目前尚不成熟,未进入推广阶段。

(四)数字签名

数据签名技术在身份认证和操作不可否认性等方面具有重要的作用。数据签名技术能够保证[11](第219-233页):信息除发送方和接受方外不被其他人窃取;信息在传输过程中不被篡改;接受方能够确认发送方身份;发送方对于自己的信息不能抵赖。数字签名采用了公开密钥密码体制,即利用一对相互匹配的不对称密钥实现加密和解密,同时用于签名和核准签名。客户在每次业务操作过程中,可以利用不对称密钥体制的私人密钥对相关信息进行数字签名,因为用户的私人密码只有用户自己才有,所有信息的数字签名就如同用户实际的签名和印签一样,可以作为用户操作的证据。目前,得到大多数人认可的数字签名技术是基于大整数因子分解问题的RSA算法和基于椭圆曲线上离散对数计算问题的ECC算法。我国移动银行应用较多的是STK卡技术中的数字签名,即在STK卡中嵌入基于非对称密钥体系的RSA密钥,结合Hash函数来实现数字签名,但RSA在运算速度和安全性方面不如ECC,而将ECC用于数字签名更适合于移动银行。这是因为[10](第54-73页):ECC安全性能更高、计算量小和处理速度快、存储空间占用小、带宽要求低;而RSA比较复杂,运算量大,加密速度慢。根据David Clark实

验比较，一个 RAS 加密算法，典型密钥长度为 1024 位，其安全性能与一个 160 位的 ECC 加密算法相同，ECC 以较小的计算量便能完成相同的工作量，较适合移动设备。ECC 已被应用于电子商务、电子政务等领域中，相信不久也将应用到移动银行安全技术中。

（五）**WPKI** 技术

WPKI（Wireless Public Key Infrastructure）技术是无线公开密钥体制为了适应无线网络认证和加密的需要而逐渐发展起来的，该技术是将互联网电子商务中 PKI（Public Key Infrastructure）安全机制引入到无线网络环境中的一套遵循既定标准的密钥及证书管理平台体系（如图 3 所示）。但 WPKI 不是一个全新的 PKI 标准[5]（第 252 页），它采用了优化的 ECC 椭圆曲线加密和压缩的 X.509 数字证书，它同样采用证书管理公钥，通过第三方的可信任机构——认证中心（CA）验证用户的身份，有效建立安全和值得信赖的无线网络环境，以保证数据传输的安全性、数据的完整性、用户的身份认证、交易的不可抵赖性等信息的安全。

其中，WPKI 是在 PKI 基础上进行了优化[11]（第 2505-2507 页），WPKI 为了减少公钥证书存储空间，就在证书的储存上引入大小约为 100B 的椭圆曲线密码机制，能用占较小内存的密钥，使得证书尺寸缩小，同时 WPKI 对 IETF PKIX 证书格式中的一些字段尺寸做了限制，由于 WPKI 是 PKIX 的子集，保证了这些 PKI 标准的相互操作的可能性。

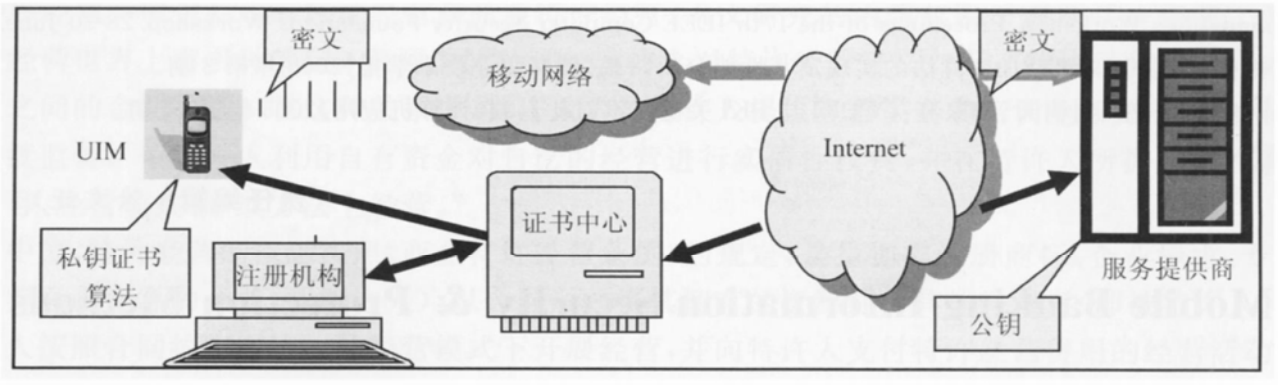

图 3　**WPKI** 安全体系总体架构图

WPKI 采用基于 ECC 算法的公钥体制，利用一对互相匹配的密钥（公钥和私钥）进行加密、解密，当发送一份文件时，发送方使用接收方的数字证书中提供的公钥对数据进行加密，接收方则使用自己的私钥解密，这样信息就可以安全无误地到达目的地。通过使用 WPKI 技术，能够保证数据传输的机密性、完整性、身份真实性以及交易的不可抵赖性，消除了用户在交易中的风险。随着 WPKI 相关技术的不断发展和完善，将进一步降低 WPKI 证书的数据长度和处理难度，并且实现 WPKI 与标准 PKI 之间的互通性，为移动银行的发展创造更好的安全保障。

尽管移动银行也存在着信息安全问题，但瑕不掩瑜。由于移动银行能够真正为客户提供超越时空的“3A（anywhere、anywhen、anyway）”、更具个性化和更具安全性的服务，同时它也是一种身份的象征，相信随着移动通信技术的发展以及移动终端设备功能的完善，移动银行将会像网络银行一样逐步被人们认可和接受。

移动银行若能和银行已有服务渠道进行有机的整合，并充分发挥无线互联网和手机这种灵巧终端的优势，开发出独特的产品或服务（如定制服务等），必将能发挥更大的作用，体现更有力的竞争优势。从某种意义上说，移动银行的投入属于银行远期发展战略部署的范畴，不能用是否能马上赢利来衡量其存在的价值，因此，中国的银行应该及早行动迎来移动银行的春天。

[参 考 文 献]

[1] Tiwari Rajnish, &Stephan Buse, Cornelius Herstatt. 2006."Customer on the Move: Strategic Implication of Mobile Banking for Banks and Financial Enterprises,"*E-Commerce Technology*, The 8th IEEE.

[2] Schwiderski-Grosche, S. & H. Knospe. 2002. "Secure Mobile Commerce," *Electronics & Communication Engineering Journal* (5).

[3] Brown I, &Z.Cajee, D. Dzvies . 2003."Cell Phone Banking: Predictors of Adoption in South African Exploratory Study,"*International Journal of Information Management* (5).

[4] 李 伟、吴庆华、廖卫国:《WPKI移动银行安全技术模式研究》,载《湖北工学院学报》2004年第5期。

[5] 袁雨飞、王有为等:《移动商务》,北京:清华大学出版社2006版。

[6] 胡爱群:《无线通信网络的安全问题及对策》,载《电信科学》2003年第12期。

[7] Pousttchi, K. & M. Schurig. 2004. "Assessment of Today's Mobile Banking Applications from the View of Customer Requirements,"*System Sciences* (5-8Jan).

[8] 张 勇、刑长征:《AES和ECC相结合的数据加密技术的研究》,载《计算机安全》2007年第7期。

[9] 张 丽、赵 洋:《身份认证技术的研究与安全性分析》,载《计算机与现代化》2007年第50期。

[10] Lee, SangJun &SeungBae Park. 2005."Mobile Password System for Enhancing Usability-Guaranteed Security in Mobile Phone Banking,"*Lecture Notes in Computer Science*.

[11] Canetti, R. 2004. Universally Composabie Signature, Certification, and Authentication. Computer Security Foundations Workshop. Procedings of the 17th IEEE Computer Security Foundations Workshop. 28-30 June.

[12] 王彬丽、李志华:《ECC加密算法的实现及其性能分析》,载《邯郸职业技术学报》2005年第3期。

[13] 路 纲、佘 堃、周明天、刘家芬:《WPKI与PKI关键技术对比》,载《计算机应用》2005年第11期。

(责任编辑 涂文迁)

Mobile Banking Information Security & Protection Methods

Nie Jin, Hu Xianling

(School of Information Management, Wuhan University, Wuhan 430072, Hubei, China)

Abstract: With the help of modern information technology and wireless communication technologies, mobile banking as a new type of financial services carrier can provide more efficient and effective financial services customers. Meanwhile it is the new trend of the financial industry development. Compare with Internet banking, mobile banking as virtual environment is more secure and friendly to user. The implementation of wireless communication technologies, creates more complicated information security problems for mobile banking mobile banking. Based on the principles of information security, this paper presented issues of information security on mobile banking and discussed the security protection methods such as: Encryption technology, identity authentication, digital signature, WPKI technology, etc.

Key words: mobile banking; information security; encryption technology