第59卷 第3期
2006年5月

武汉大学学报(人文科学版)
Wuhan University Journal (Humanity Sciences)

Vol. 59. No. 3
May 2006. 373 ~ 377

网上银行安全及相应对策探讨

聂 进,雷 雪
(武汉大学 信息管理学院,湖北 武汉 430072)

[作者简介] 聂 进(1964-),女,湖北武汉人,武汉大学信息管理学院副教授,主要从事电子商务、网络金融研究;雷 雪(1982-),女,河南南阳人,武汉大学信息管理学院硕士生,主要从事网络银行安全与管理研究。

[摘 要] 安全问题的解决是网上银行正常运营的核心,也是金融机构和用户最为关注的问题。从技术层面、管理层面、法律层面和用户层面看,我国网上银行安全现状及存在着一些问题,应采取相应的对策:1. 加强网上银行的网络安全体系建设;2. 完善银行管理制度并健全相关法律法规;3. 增强用户的安全防范意识。

[关 键 词] 网上银行;安全;对策
[中图分类号] G203 [文献标识码] A [文章编号] 1671-881X(2006)03-0373-05

随着现代信息技术的飞速发展,网上银行作为一种全新的适应当前电子通讯技术发展需求的银行形式正在蓬勃兴起。安全问题与网上银行相伴而生。计算机病毒、黑客攻击及网络欺诈是威胁当前网上银行安全运行的重要隐患,网上银行欺诈事件是国际上增长最快的安全事件之一,在几乎所有发展中国家均呈上升趋势[1](第7-11页)。比尔·盖茨曾经预言:"传统商业银行是要在21世纪灭绝的一群恐龙",而网上银行的安全隐患证明该预言未免过于乐观。在现有的技术水平下,网上银行面临远远高于传统银行的交易和操作风险。

我国网上银行呈阶段性跳跃式发展趋势。到目前为止,境内开展实质性网上银行业务的有60多家银行的分支机构,这将成为商业银行为高端用户提供服务的主要方式。但因技术的不足,管理水平落后,法律法规不健全以及用户安全防范意识不够,网上银行的安全现状不容乐观。相关调查结果显示,47.5%的用户选择网上银行网站时最看重的因素是"交易安全性";在网上购物支付方法中,汇款、网上支付和货到付款的比例分别为33.4%、41.5%和24.7%[2];61.2%的网民因"担心交易安全问题"而不使用网上支付[3]。可见,网上银行的安全可靠性是用户首要考虑和关心的内容,它在一定程度上影响了网民电子支付手段的运用,从而制约了电子商务的发展[4]。由于互联网自身的安全性特点,对信誉至上的银行业来说存在着极大的风险。因此,网络安全是影响网上银行发展的第一要素。

一、我国网上银行安全现状及存在问题分析

(一)技术层面分析

网上银行是传统银行业务在互联网上的实现和拓展,技术实现上是一个Browser/Server结构的复杂Web应用程序集。其安全性问题主要包括以下几个方面:网上银行体系结构安全问题、网上银行应用系统安全问题、用户端安全问题和网络通讯中数据传输安全问题。

收稿日期:2006-01-13

1. 网上银行体系结构安全分析。应用系统的体系结构决定了系统的安全性、灵活性、伸缩性与可维护性,从总体上限定了系统所能达到的安全级别。网上银行的业务特征决定了它对系统安全的要求比其他 Web 应用程序更为严格和苛刻,其体系结构的设计关系重大。国内银行可预测的安全风险主要包括外部安全和内部安全两大类:外部安全问题以病毒和黑客入侵为主;内部安全问题主要是指银行内部人员利用网络漏洞进行非法操作,这方面的案件屡见不鲜。目前,国内银行有实力单独开发体系结构的为数尚少,大部分银行都是采用技术外包的形式,由专门的软件公司负责网上银行系统的开发和维护。一旦有事故发生,银行工作人员必须求助于软件公司的技术支持,这不仅给网上银行系统安全问题的处理造成障碍,而且给银行自身留下了安全隐患。

2. 网上银行应用系统安全分析。网上银行应用系统安全主要是指网络、Web 服务器、主机和数据库安全等方面。网络安全是指通过 SSL 或 SET 等加密通讯技术,保证只有授权许可的通信才能在客户机和服务器之间建立连接,且传输中的数据不能被读取或更改;Web 服务器安全主要依赖防火墙对可疑数据包进行过滤,防止病毒及黑客的侵入;主机安全包括反病毒、系统安全检测、入侵检测和审计分析等;数据库安全指要具备必须的针对突发事件的应急措施,如数据的备份和恢复等等。我国各大银行对内部网络建设比较重视,许多大型软件公司都致力于网络安全解决方案的研究,使网络的安全问题有了很大改善。但是,技术的进步使安全防范更加严密的同时,也使破解技术随之逐步提高,病毒和黑客层出不穷。目前,我国银行业因运用系统设计存在不足,如定制化软件没有解决相互间通信的安全问题,软件程序的复杂性和编程方法的多样性使软件系统中很容易有意无意地留下一些不易被发现的安全漏洞等,导致黑客有机可乘,形成一系列安全隐患。

3. 客户端安全分析。传统的身份识别方法通常是靠用户名和密码对用户的身份进行认证。综合来看,我国网上银行客户端的安全设置主要存在以下两方面的隐患:一是传统的网页输入控件(INPUT)不具备安全保护特性,恶意程序能够很容易捕获键盘输入字符从而获取用户的输入信息;二是恶意程序可以对某个账号以暴力方式获取密码。

表 1 我国主要网上银行客户端的安全设置

客户端	招商银行	工商银行	农业银行	建设银行	中国银行	交通银行
账号输入域	安全控件	普通控件	普通控件	普通控件	普通控件	普通控件
密码输入域	安全控件	安全控件	普通控件 软键盘	普通控件 软键盘	普通控件 软键盘	安全控件
验证码	有	有	有	有	无	有

注:以上数据主要针对个人网银普通版

由上可见,我国网上银行客户端的安全设置普遍存在不足,用户常成为受攻击的目标,被恶意代码窃取账号、密码甚至文件公钥证书等,致使用户不能随意使用网吧等公共场所的终端处理网上银行业务,无法真正实现网上银行随时、随地、安全的服务要求。此外,有相当一部分银行的个人网上银行没有提供数字证书储存介质,这样很难保证网上转账支付活动的安全,成为隐患。综上所述,客户端的安全防护乃是目前整个网上银行体系最薄弱的环节。

4. 网络通讯中数据传输安全分析。目前,在数据传输过程中为了保障信息的安全、准确和完整性,有两种流行的传输协议:SSL 和 SET。SSL(Security Sockets Layer)即安全套接层协议,可以保证信息传输的机密和完整性,但不能保证信息的不可抵赖性,而且多方认证也十分困难;SET (Secure Electronic Transaction)即安全电子交易协议,设计比较严格,安全性高,它能保证信息传输的机密、真实、完整和交易的不可否认性,但本身比较复杂,不易于实施。现在我国在支付安全系统方面,仅中国银行在个人支付方面采用 SET 协议进行安全控制,其他银行,如招商银行采用 SSL 技术双重安全机制,建设银行采用给用户发放认证卡的方式,中国银行在对企业认证方面也是采用简易的 SSL 协议等。鉴于 SSL 的缺陷,多数银行采用 SSL 协议加数字签名的方式来保证信息的不可抵赖性,一定程度上确保

了数据的安全传输。

(二)管理与法律角度分析

我国网上银行的技术安全管理尚不完善。开办网上银行时, 有相当一部分银行交易的软硬件管理检测制度未经权威机构或专家检验评估; 一些银行为了加快发展, 甚至对涉及核心技术与信息的软件也是从第三方购买, 或由其他公司开发、维护和管理, 潜在的安全风险很大[5](第 117-119 页)。此外, 尽管网上交易和结算的安全要求目前都有实现技术, 但相应的管理还存在诸多不足: 比如 CA(电子认证)中心建设呈无序状态, 国内各 CA 中心签发的证书所采用的技术标准和管理规范存在差异, 不能实现跨行认证和跨行交易, 给用户带来了诸多不便, 不利于安全防护措施的实施[6](第 105-112 页)。

我国有关网上银行的立法和制度建设与发达国家相比较存在着差距, 网上银行安全运行所需要的法制环境不健全。(1)不断发展的信息技术为在未经许可的情况下广泛收集和采用客户详细的个人信息提供了可能。我国对网上银行中诸如账号、E-mail 之类的个人隐私资料缺乏法律保护, 造成网上个人资料频繁泄露。(2)计算机犯罪已给众多的网络银行用户带来了经济损失, 而我国有关惩罚利用计算机犯罪的法律尚不健全, 很难适应网上银行迅速发展的需求; 此外网上欺诈所致的网络银行事故的责任界定不明确, 易出现银行和用户"扯皮"现象[7]。(3)2005 年 4 月实施的《电子签名法》为数字证书的使用提供了技术和法律保障, 而我国各网上银行系统实施的认证措施离《电子签名法》的要求尚有距离, 尤其是 CA 中心建设的准入规则还未出台, 致使其贯彻和实施不易。

(三)从用户角度分析

用户的安全意识是影响网上银行安全的不可忽视的重要因素。VISA 卡国际组织发布的调查结果显示, 有 85%的网上银行事故是由于用户操作失误造成的。我国网络银行用户安全意识普遍较弱, 如对假冒站点的辨别能力不足, 对使用网上银行时如何保护自己的账户隐私、确保交易安全等方面的了解和重视程度不够等。虽然多数网上银行已经能够提供数字证书的使用, 但事实上大部分用户对数字证书的认识模糊, 且鉴于数字证书存储介质需收取一定费用, 所以部分用户不愿购买。而银行技术手段对此却无能为力。

二、加快网上银行安全运行的对策

(一)加强网上银行的网络安全体系建设

可靠的系统体系结构是建立网上银行安全体系的基础。当前一般采用分层方法进行网上银行应用程序的开发, 即逻辑角度应能明确区分 Web 应用层、数据通信层与数据源层, 确保各个层面安全策略的独立性; 从开发角度要能区分客户端、应用层与数据服务层三大部分, 这样有助于细化安全风险, 易于在威胁发生时迅速分析原因, 及时控制和排除威胁。此外, 银行内部要充分发挥科技人才资源优势, 调动其主动性, 在外包公司的辅助配合下开发信息系统, 一定程度上可减少安全隐患。

在提高应用系统的安全方面, 可采用设置多重防火墙、增加过滤路由器、建立加密的通讯网关服务器等方案, 有效地实现内外网的隔离与访问控制; 完善身份鉴别机制、访问控制机制、角色管理机制、防止重发机制和审计机制等, 保证交易安全; 采用国际先进的网络安全检测软件, 24 小时实时安全监控, 及时发现并修正系统可能存在的弱点和漏洞, 定期对网络系统进行安全性分析; 建立详细的安全审计日志, 充分使用网络监控设备或实时入侵检测设备, 对进出各级局域网的常见操作进行实时检查、监控、报警和阻断, 来防止针对网络的攻击与犯罪行为; 银行要对可能引起系统中断或故障的各种原因进行评估, 事先制订出相应的灾难恢复计划。

在加强客户端的安全防护方面, 可使用网络银行专用的用户端输入控件(如 ActiveX)取代传统网页控件, 来防止恶意程序捕获普通键盘事件, 获取用户敏感信息; 同时可通过附加输入随机验证码来预防恶意程序的暴力攻击。此外, 各网上银行应采用先进的加密认证技术, 为用户提供安全可靠的数字证

书,并提供相应的类似智能卡或 USB—Key 等更为安全的数字证书储存介质。当然,若能将基于虹膜认证、指纹认证的生物特征身份认证技术与数字证书结合起来就可以更好地解决客户端的安全问题。

在网络通信环节中,要有效地防范任何来自系统内部或外部对通信数据的非法截取、篡改和窥视,采用严格的数据加密技术来保障通信的安全性。SET 可维护在任何开放网络上的个人金融资料的安全性,是目前公认的网上交易国际安全标准。我国应积极采用安全性较高的 SET 协议。

(二)完善与改进网络银行的管理体制与法规建设

网络银行安全主要来自于技术方面、管理方面和法律制度方面,而加强管理体制的建设将有助于从根本上防范和杜绝技术与管理方面的安全漏洞的产生。人是金融业发展中的决定因素,安全的技术必须和安全的高质量的管理相结合才能发挥作用,在网络银行建设与发展过程中应该有一系列安全管理制度,用于规范操作人员的行为和网络系统的管理,这些规章制度应当包括:网络系统人员的设置与职责的确定和划分,机房出入制度,网络系统日常操作维护规范,安全扫描/临控工具的使用规定,系统的应急处理措施、安全审计制度等。

建立综合的全国网络金融监管监控信息系统,向发达国家借鉴经验实施金融信息系统的总体规划,成立专门的部门对监管信息系统的基本业务、关键技术、系统的框架结构、所应当遵循的标准、监管数据的采集、监管信息的管理等进行系统科学的规划。国家应对银行业加强监管,尤其是对网络银行业务的市场准入进行严格控制;网上银行要建立起一套保护、监测、反应为一体的动态自适应的金融监控和预警体系,以提高对自身安全漏洞和内外部攻击行为的监测、控制、管理和实时处理能力。国家可以成立专业"黑客"咨询和"防黑"系统集成公司,由他们负责根据各个网站的不同情况来量体裁衣,制定与各网站相适应的"防黑"策略和技术。各大银行使用数字证书或电子签名方式进行用户身份认证和交易授权的,均应采用中国权威、公正的第三方安全认证机构提供的电子认证服务。这将有利于强化公众信心,保障网上支付的安全。

我国《电子签名法》于 2005 年 4 月 1 日通过,标志着我国法律体系正式迈进网络时代,是我国电子商务立法史上的一个里程碑。由于信息技术的迅猛发展变化,电子商务发展日新月异,立法滞后不单是网络银行而且是整个电子商务发展的瓶颈和障碍。从立法的角度来看,需要健全明确的适应网络经济的公民个人隐私权、企业商业秘密和金融信息保护的法律法规。网上银行应适应新形势,以《电子签名法》为依托,完善《票据法》中的相关条款,制定网上支付新规则[8]。针对随着计算机网络发展而出现的新情况、新问题,要不断修订和完善我国《刑法》中有关计算机犯罪的法律条款;此外,需加强相关法律的宣传和教育,增强用户遵守网络安全协议的法律意识。加强网上银行的前瞻性研究,在借鉴国外相应的立法经验的基础上,密切关注网上银行的最新发展动态及其对整个金融业的影响,研究、制定有关法律、法规,逐步建立适合我国国情的网上银行法律框架,确保网上银行的安全运行。

(三)增强用户的安全防范意识

从用户角度来讲,一方面应养成良好的操作习惯:登陆网络银行时应尽量避免使用搜索引擎或网络实名;密码设置上应使用复杂密码机制;定期查看交易记录,随时掌握账户变动情况;警惕电子邮件链接等。另一方面,应采取数字证书这种有效的安全保障措施,明确认识其使用、保管及法律意义。

从银行角度来讲,要提供完备的安全防范手册,尽量在其网页的醒目位置对用户使用网上银行时如何保护自己的账务隐私、确保交易安全等方面进行明确的提示,加强对客户安全使用网上银行的培训和教育。如 2005 年 11 月,中国金融认证中心在网上银行信息安全知识公益宣传活动中,向公众演示了数字证书的安全性及使用流程,积极宣传数字证书的可靠性能及重要作用,起到了很好的教育效果。

安全问题不仅关系到网上银行发展的前景,同时也决定电子商务发展的进程。解决好网上银行安全问题、推动电子商务快速发展时不待我。但做好网上银行的安全工作并非银行一家之责,而是一个社会系统工程,需各方面的协作与努力。根据美国互联网用户行为研究专业机构 Pew Internet &

American Life 在 2004 年 11 月份的调查, 占美国 44%的互联网用户使用网上银行服务, 根据中国互联网络信息中心发布于 2005 年 1 月份的《中国互联网络发展状况统计报告》, 到 2004 年 12 月底, 中国互联网用户中有 5.1%将网络银行作为常用的网络服务之一, 由此可见, 我国网上银行的发展还有漫长的路要走。随着网上银行安全体系的完善、相关管理制度的加强、对应法律法规的健全、国民安全意识的增强, 将会有更好的网上银行运行环境, 网上银行在我国一定会得到健康快速发展。

[参　考　文　献]

[1] Anna Granova, JHP Eloff. Online banking and identity theft: who carries the risk[J]. Computer Fraud & Security, 2004 (11).

[2] 中国互联网络发展状况统计报告[R]. http://www.cnnic.net.cn/download/2005/2005011801.pdf, 2005-01-08.

[3] 2005 年中国网上支付简版报告[R]. http://www.iresearch.com.cn/html/Online_Payment/detail_free_id_20636.html, 2005-08-27.

[4] 网银安全制约电子商务[EB/OL]. http://www.enet.com.cn/city/inforcenter/A20050124385092.html, 2005-01-24.

[5] 李兴智, 丁凌波. 网上银行理论与实务[M]. 北京: 清华大学出版社, 2003.

[6] 谭荣华, 刘瀚波, 王　丹. 我国网上银行安全认证体系架构的理性选择[J]. 金融研究, 2003, (12).

[7] 杨　谷, 张碧涌. 网上银行安全问题探讨[EB/OL]. http://finance.sina.com.cn/roll/20030321/1623323557.shtml, 2005-01-27.

[8] 《电子签名法》对我国网上银行的影响及对策[EB/OL]. http://news.xinhuanet.com/dzswdh/2005-04/05/content_2787079.htm, 2005-04-05.

(责任编辑　涂文迁)

Strategies for the Security of Online Banking

NIE Jin, LEI Xue

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

Biographies: NIE jin (1964-), female, Associate professor, School of Information Management, Wuhan University, majoring in E-commerce; LEI Xue (1982-), female, Graduate, School of Information Management, Wuhan University, majoring in banking security and management.

Abstract: Security is the primary concern for the online banking, as well as for the financial system and consumers. Based on an in-depth analysis of technology, administration, legislation and consumers involved, we present here an up-to-date report on the security status of online banking in China. The existing security problems are thoroughly investigated and the following solutions are proposed: 1. Strengthening the security system of online banking. 2. Optimizing the management system of banks. Improving legal regulation and enforcement of the law. 3. Educating consumers to protect their information on the net.

Key words: online banking; security; solution