Internet Banking Transactions' Technical Risk and its Prevention

Feng ZHANG
School of Management, Beijing Union University, Beijing, China
Email: gltzhangfeng@buu.edu.cn

Abstract: The number of Internet Banking users has grown continuously in china, while an active Internet Banking user-degree increase rapidly, but the security of Internet Banking continues to be the focus of the community. Internet technology continues to upgrade and "hacker" means used to attack constantly renovate, that makes the occurrence possibility of Internet Bank's technical risk is growing. This paper focuses on analyzing the technical risk in the process of Internet Banking transactions, and puts forward the targeted preventive countermeasures and suggestions.

Keywords: internet banking; online trading; technical risk

网络银行交易技术风险及其防范

张　峰
北京联合大学管理学院，北京，中国，100101
Email: gltzhangfeng@buu.edu.cn

摘　要：中国网络银行用户数量持续增长，同时，用户使用网银的活跃度也在迅速提升，但网银安全仍是社会各界关注的焦点。网络技术的不断升级和“黑客”攻击手段的不断翻新，使得网络银行发生技术风险的可能性越来越大。本文着重分析了网络银行交易层面的技术风险，并针对性地提出了防范对策建议。

关键词：网络银行；网上交易；技术风险

1 引言

网络银行是银行利用互联网技术，通过网络向银行客户提供开户、销户、转账、投资理财等服务项目的总称。网络银行作为一种实体银行的虚拟工作环境，其风险范畴要比实体银行更大。其中，技术风险是网络银行风险的核心内容，是指因技术方面的缺陷使银行系统遭受“黑客”袭击，以及客户误操作或银行员工的违规行为导致网站和客户利益受到损害，甚至面临倒闭的危险。网络技术的不断升级和“黑客”攻击手段的不断翻新，使得网络银行发生技术风险的可能性越来越大，而且远远高于其他各种风险。因此，技术性风险应该是网络银行关注的首要风险。

郇凤悦（2009）对网络银行的技术风险进行了比较系统的分析，根据网上银行业务的流程和环节，把网络银行技术风险分为三大类：系统与信息层面的技术风险、网络层面的技术风险、交易层面的技术风险。本文重点分析交易层面的技术风险及其防范对策。

2 我国网络银行业务发展概况

2.1 网银用户持续增长

据《2009 年中国网上银行调查报告》显示：尽管受到全球金融危机的冲击，中国网上银行总体上依然保持了向上发展的态势。2009 年，在行业主管部门、各商业银行以及中国金融认证中心(China Financial Certification Authority，简称 CFCA)相关机构的大力推动下，个人网银市场逆市而上，展现了强劲的发展势头。数据显示：2009 年，全国城镇人口中，个人网银用户的比例为 20.9%，比 2008 年增长了 2%。其中活动用户占 76.7%，呆滞用户占 23.3%；未来一年的潜在用户比例为 13.9%。同时，分析发现，其中 35-44 岁的“社会核心”人群和女性市场网银用户增幅较大，网银正进一步渗透到各类人群中。企业网银方面，2009

年，全国企业网银用户的比例为 40.5%，比 2008 年略有下降，其主要源于受金融危机冲击较大的，百万元以下规模中小型企业的网银用户比例比 2008 年下降了 4%，而这部分企业在总体企业数量中占到了 50%以上。尽管如此，企业网银交易用户比例为 70.3%，比 2008 年上升了 5.9%。

2.2 网银用户活跃度迅速提升

在网银用户量进一步攀升的同时，用户使用网银的活跃度也在迅速提升：2009 年活动个人用户人均每月使用网银 5.6 次，2008 年为 5 次；交易用户平均每月使用次数更高，为 5.9 次，也高于 2008 年的 5.5 次。企业用户方面，月使用频率则更高：2009 年，平均每家活动用户使用网银的次数从 10.3 次增长到 11.3 次。企业网银对于柜台业务的替代比率达到了 50.7%。在活跃度提升的背后，是用户对于网银功能的进一步了解和更多的尝试。2009 年使用各项网银功能的个人用户比例均比 2008 年增加，特别是网上支付、转账汇款、信用卡还款和个人贷款 4 项功能，增幅非常明显。企业用户方面，账户查询、转账汇款则是他们使用比例最高的两项企业网银功能。活跃度的提升以及对网银功能的更多尝试表明，对于很多网银用户来说，使用网银正在由对新鲜事物的浅尝辄止转变为日常生活和企业运营的必须，网银普及正向纵深发展。

2.3 网银安全仍需重视

网银高速增长的同时，安全性一直是各界关注的焦点。《2009 年中国网上银行调查报告》显示，2009 年，个人用户对于网银安全的信心已经提升，3/4 以上潜在用户认为网银是“安全”的。其信心来源主要集中在以下几点：一是自我防范意识和能力的增强；二是对银行实力和对银行的信任；三是对网银安全技术手段和安全措施有一定的了解；四是亲朋好友的使用经历及口碑。与此相对应，导致非潜在用户认为网银不安全的首要原因则是不了解网银安全技术手段，其次是担心黑客/木马病毒盗取账户资金。如何帮助用户提升自我防范意识以及掌握必要的安全防范手段仍然是未来一段时间内网银普及推广工作的重点。

3 网络银行交易层面技术风险的内容

詹德新等（2007）将网上银行交易风险归纳为三方面：客户端交易凭证的保管及使用、金融机构服务端信息设备与系统的安全防护、交易讯息经由因特网传输过程是否遭受外来黑客的干扰或截听。郇凤悦（2009）将网络银行交易层面的技术风险分为密码盗窃风险、客户误操作风险和银行员工的技术风险三大类。本文按照网络银行交易主体及业务流程将网络银行交易层面的技术风险归纳如下：

3.1 客户端存在的安全隐患

客户在网上交易过程中的无意识、疏忽大意和误操作会给银行和自己带来损失。如：客户使用电子银行前并未充分了解各项权利义务及操作方式，就会产生客户操作风险；客户在没有安全防护措施的场合使用个人信息容易造成信息泄露和权益受损；客户没有授权的交易可能会给银行造成经济损失；客户缺乏安全防范意识将认证磁盘随意放置，致遭不法分子复制盗用进而盗领存款；客户本身利用电子银行进行非法的洗钱活动；不法分子仿冒银行网站，借此骗取客户基本资料，损及金融机构商誉等。

3.2 金融机构服务端存在的安全隐患

1）金融机构未定期修补系统程序或未及时升级版本、未扫描异常更新或复制的系统文件、系统安控参数设定不完整，致使黑客利用缓冲区溢出漏洞、植入木马程序取得特权使用者密码或附加植入计算机病毒以瘫痪主机及防火墙系统，或附加木马程序进行数据窃取及破坏，或利用系统安控设定不周延以进行数据窃取及破坏。

2）金融机构对使用者的数据文件未制订系统安全管理规范、未限制使用文件修改工具、职务分工不当或未落实，违反牵制原则，导致不法分子或金融机构内部人员窃取未隐藏的使用者数据文件，并采用字典攻击法推测出使用者密码，进而篡改数据库或文件内容。

3）金融机构未确实有效地监督厂商人员维护系统、未与厂商洽订保密契约、未建立内部安全措施，致入侵者将IP、防火墙规则等重要数据拷贝至储存媒体或印成纸张携出办公室、或利用e-mail、ftp、http将数据利用拨接方式绕过防火墙传送，以攻击银行内部主机。

4）柜台整体交易流程不符合牵制原则，中心产制及核发电子凭证、软件、密码函不符牵制及机密性，致客户数据、电子凭证、软件、密码信函遭窃取；对重要电子凭证、基码及密码保管不当，导致不法分子借此窃取客户数据、重要电子凭证、基码、软件及密码以从事不法活动。

978-1-935068-12-9 © 2010 SciRes.

5）银行的操作人员、软件人员等通过某些技术手段和本身拥有的权限,对账户进行修改,进行盗用客户资金或者套取银行利息等违规行为。这种手段具有极大的隐蔽性,给银行带来的损失也是巨大的。

3.3 网络漏洞引发交易风险

1）网上银行主机与中心主机间数据的传送加密不够，导致不法分子或金融机构内部人员窃取以明码方式传送于网上银行主机及中心主机间的客户网上银行交易密码，或篡改转账交易数据封包。

2）Internet/Extranet/modems未严禁开放主机拨接功能；未订定系统安全策略、未利用网址转换(NAT)技术隐藏内部终端/服务主机的IP地址；未严禁透过Internet联机维护主机数据；未利用防火墙反诈骗及反攻击技术防止各种入侵手段；未利用网上扫瞄等网上侦测工具程序扫描异常网段，导致不法分子、金融机构内部人员或黑客透过拨接直接进入主机或利用维护主机系统的特定网页，进入主机修改数据及开放不必要的服务功能。

4 网络银行交易技术风险的防范

针对上述网络银行交易层面技术风险的隐患，相关主体可以有针对性地采取如下风险防范对策。

4.1 客户自身增强风险防范意识并进行规范化操作

客户在开通网上交易功能并进行网上交易之前，应该全面了解相关权利义务、操作流程和正确的操作方法，采取必要的保密技术和手段，时刻警惕不法分子通过“网络钓鱼”、木马病毒等手段盗取银行账户信息。金融机构应提供客户网上银行业务或服务的详细操作说明文件，对客户权益、信息安全及隐密性等注意事项，应以书面且较醒目的方式告知客户注意。鼓励客户使用网上银行“专业版”,它是一种基于PKI的证书机制，能够做到网上真实身份的认证和抗否认的数字签名，及数据的完整性和保密性。

4.2 金融机构加强自身系统和内控制度建设

4.2.1 强化网络银行信息设备安全管理

1）电子转账、交易性指示等金融交易讯息或电子文件传输，应确认符合来源辨识性、讯息隐密性、完整性、不可重复性、不可否认传输讯息等设计，应用程序设计应避免产生缓冲区溢位系统漏洞，以免遭人利用附加不当指令窃取数据。

2）网关(Gateway)系统建置或变更通讯等转换内容，应建立符合内控原则的控管程序；对异常进出网关的事件应留存记录备查；对重大异常状况应建立警示机制及追踪管理措施。

3）信息部门负责网上银行信息系统软、硬设备维护的职务应有适当分工，其建置与变更应妥善控管，并留存可供追踪查核的审核日志。

4）加强计算机机房门禁，涉及储存客户数据的设备应严加控管。有关私密金钥、凭证资料或乱码基码及各项相关隐密性数据，在产生、变更、储存时均应加强控管及符合内控原则；金钥长度应符合主管机关的规定。

5）对联外网站与内部网上或计算机系统间的路径应加以控管；对未经防火墙的远程访问应予过滤及管制；对未经授权或违规的异常存取或进出网站情形，应设计侦测、警示及追踪的机制，并设有防范网页遭窜改的控管措施。

4.2.2 强化系统可用性管理

金融机构应制定故障预防(如病毒防范、侦测、警示等)程序、系统备援及系统复原等措施，并定期演练、检讨、改善。

4.2.3 督促金融机构加强内部控制职能，充实审计部门科技力量

可以调整或分配部分科技人员到稽核部门，也可以加强对审计人员科技培训工作，使商业银行内部控制制度覆盖整个业务流程，防止内部工作人员违规操作或恶意犯罪。

4.2.4 加快相关立法工作

确定数字证书、数字签名、电子证据、电子合同的法律效力，同时应规定银行负责维护电子数据的真实性、完整性，并长期保存，严禁篡改、伪造、销毁交易记录、客户资料、系统日志等电子数据。这些电子数据既可作为法律依据，也利于税务、审计、监管部门及执法机构的必要检查。考虑到电子技术的快速发展，立法应具有一定的前瞻性，避免频繁改动，处处被动。要尽快制定相关的技术标准和规范，对网络银行业务使用的硬件、软碎产品，认证、加密、安全传输技术，信息包格式、用户接口标准等各方面制定全面、可行的标准，为网络银行业务的持续发展创造有利条件。

4.3 不断完善网络系统安全

4.3.1 完善入侵监控系统,加强漏洞扫描

入侵检测是一种主动安全防护措施。在网上银行的各个关键位置和关键服务器中布置入侵监控系统,用于保护关键应用的服务器,实时监视可疑的连接和非法访问的闯入,并对各种入侵立即进行反应,如断开网络开关等,从而提供对内部攻击、外部攻击和误操作的实时保护。同时,加强对安全漏洞的扫描。对网上银行各个主机和网络设备存在的安全漏洞进行定期的检查,及时发现漏洞和安全隐患并进行修补,以此加强系统安全。

4.3.2 提升加密技术,保证数据通讯安全

为保障信息传输的安全性,银行在定期备份重要数据或采用影像技术提高数据完整性的同时,采用合适的加密技术,以确认网上银行的业务用户身份和授权,保证网上交易数据传输的保密性、真实性,保证通过网络传输信息的完整性和交易的不可否认性,防止内部信息在网上被拦截和窃取。例如,使用SSL协议和SET协议进行交易数据的加密传输,也可以利用加密算法如RSA算法,对传输的数据进行加密。

4.3.3 加强身份鉴别机制

在网络银行系统中,采用双重身份认证,即基本身份认证(用户名及密码)和附加身份认证(动态口令与数字证书)的方式,杜绝不法分子通过窃取客户密码盗窃资金,保障网上银行安全。

4.3.4 利用防火墙等技术,避免网络黑客和病毒的攻击

利用防火墙的访问控制、审计功能、地址翻译、AT(网络地址转移)技术、AAA(身份认证、授权、审计)等功能,在银行系统的计算机网络与公网的连接处以及网上银行的边界配置硬件防火墙,对进出网络的数据检查和控制,隔离银行内部网络的外在安全威胁。此外,还要及时更新杀毒软件版本,注意病毒流行动向,形成一套完整的网络系统病毒防御体系。

References (参考文献)

[1] Xun Fengyue. Internet banking technical risk research based on security[J]. Guangdong Vocational College of Finance Journal, 2009 (2) :41-44.
郇凤悦.基于安全视角的网络银行的技术风险研究[J].广东财经职业学院学报，2009（2）：41-44.

[2] Zan Dexin, Gong Lin, Yang Bitian. Online banking transaction risk and countermeasures [J]. Network security technology and applications, 2007 (6) :68-70.
詹德新,龚麟,杨碧天.网上银行交易风险及防范措施[J].网络安全技术与应用,2007（6）：68-70.

[3] Li Hongxia. China's Internet banking technology risk and its control [J]. Financial Theory and Practice, 2005 (9) :79-80.
李红霞.我国网络银行技术风险及其监管[J].金融理论与实践,2005(9)：79-80.

[4] Zhang Chuanliang. On the Internet banking technical risk and prevention [J]. Information Exploration, 2007 (12) :75-77.
张传良.论网上银行的技术风险与防范[J].情报探索,2007(12)：75-77.

[5] TengXun Finance. CFCA released 2009 China Online Banking Report [EB / OL]. Http://finance.qq.com/a/20091203/006967.htm ,2009-12-03.
腾迅理财.CFCA 发布 2009 中国网上银行调查报告［EB/OL］.http://finance.qq.com/a/20091203/006967.htm,2009-12-03.