

Regarding our Country's Network Bank Information Security Question Comprehensive Topology Analysis

Lingling ZENG, Jun LI

Wuhan University of Technology, Wuhan, China

Email: zeng_1129@yahoo.com.cn

Abstract: Internet banking is the use of Internet digital communications technology to Internet as a trading platform and service channels, on-line for the public to provide clearing and credit services, commercial banks or financial institutions, Internet banking has become a new banking model. Internet banking has a low transaction cost, fast and convenient transmission of information without time and space constraints, but there are also a number of Internet banking security risk. This article describes the network of banks in relation to the basic content, but also from information security-related aspect of some research carried out in conjunction with the chart illustrates. To ensure the security of Internet banking transactions, on one hand banks are required to establish strict security measures and procedures, on the other hand, consumers have to master the proper and safe use of Internet banking methods. The article finally made a case study, given the summary. As long as the necessary security protection strategy, a reasonable choice of network security products, online banking will be able to achieve the safety requirements to enable consumers to bring confidence to enjoy the convenience of online banking and efficient service.

Keywords: internet Banking; security technology; security; information security

对于我国网络银行信息安全问题综合拓扑分析

曾玲玲, 李 俊

武汉理工大学, 武汉市, 中国, 430000

Email: zeng_1129@yahoo.com.cn

【摘要】 网络银行是采用 Internet 数字通信技术,以 Internet 作为交易平台和服务渠道,在线为公众提供结算、信贷服务的商业银行或金融机构,网络银行已成为一种新型的银行模式。网络银行具有交易成本低、信息传递快捷方便、不受时间空间限制等优点,但是网络银行也存在诸多安全隐患。本文介绍了网络银行有关基本内容,也从信息安全相关方面进行了一些探讨并结合图表进行了说明。要确保网络银行交易的安全,一方面银行要建立严密的安全防护措施体系,另一方面消费者也要掌握正确安全地使用网络银行的方法。文章最后做了实例分析,给出有关总结。只要采取必要的安全防护策略,合理地选择网络安全产品,就能实现网上银行的安全要求,使广大消费者放心地享用网上银行带来的便捷、高效的服务。

【关键词】 网络银行; 安全技术; 安全措施; 信息安全

1 网上银行概述

目前金融业正进入一个竞争的新时代,成本的大幅增加和竞争的日益加剧,迫使银行业寻求一种新型的成本低、自动化程度高的服务方式与途径。到 21 世纪,银行业的目标是在任何时候(Anytime)、任何地方(Anywhere)、以任何方式(Anyhow)为客户提供服务,我们称之为 AAA 银行。专家估计,零售银行的未来

是虚拟银行,即建立在计算机通信技术基础之上的银行,在虚拟银行中,客户能够在任何时间、地点通过自动化服务渠道及统一的方式获得银行服务。^[2,3]

随着 Internet 在全世界范围的爆炸性扩展,Internet 银行在虚拟银行中的地位也日渐趋增。推动 Internet 银行技术大幅度发展的因素有很多,最根本的原因还是银行所面临的日益加剧的竞争压力,想在将来生存和盈利,必须在既能充分满足客户需求又能大幅降低

成本的新型服务渠道上投资, Internet 是目前最好的选择。

2 网络银行的本质与优势

网络银行, 有人叫网上银行(Internet Banking), 有人叫电子银行(Electronic Banking)或虚拟银行, 也有人叫在线银行(Online Banking)。根据美国联邦储备机构的定义: 网络银行是利用互联网作为其产品、服务和信息的业务渠道, 向其零售和公司客户提供服务的银行。^[4]

网络银行是银行业务在网络上的延伸, 是信息技术在世纪之交贡献给金融电子化领域的最新创意。网上银行依托迅猛发展的计算机和计算机网络与通信技术, 利用渗透到全球每个角落的 Internet, 把银行的业务直接在 Internet 上推出。新式的网上银行几乎囊括了现有银行金融业的全部业务, 代表了整个银行金融业未来的发展方向。

自世界第一家网上虚拟银行——安全第一网络银行(SFNB)1995 年 10 月开业以来, 各国的银行纷纷把业务搬上互联网。1997 年开始中国银行、招商银行都推出了网络银行业务。网络银行具有无可比拟的优势, 它给金融业带来了前所未有的发展和繁荣, 同时也给世界银行业的发展带来了新的金融风险。

与传统银行相比, 网络银行是在开放的网络系统中以先进的数字流转技术来完成信息传输, 采用数字化的方式进行款项支付和资金结算的, 优势主要有:

1) 交易速度快。网络银行的客户足不出户, 只要轻轻点击鼠标, 瞬间就可以办理银行提供的各项相关服务。

2) 经营成本低、交易成本低。传统银行拓展业务依靠简单地增设营业网点, 需要大量的房屋、设备、资金、人力等资源的投入, 而网络银行投入少量的资金、设备、人力, 就可以将银行业务拓展大的领域范围。

从一个实际调查的例子, 可以看出 Internet 银行的巨大潜力。据美国权威机构调查和预测, 各种服务渠道的平均每项交易成本情况如下表 1:

我们看到使用 Internet 的交易成本最低。

3) 任何时间(Anytime)、任何地点(Anywhere)、任何方式(Any way)。网络银行不仅可以为用户提供全年 365 天、每天 24 小时的全天候服务, 而且可以跨越地域障碍, 为用户提供基本的对私、对公等网上支付服

务, 更可充分利用 Internet 提供理财助理、财务分析、个性化服务、目标营销、客户关系管理等特色。

Table 1. The average cost of each transaction in various service channels

表 1. 各种服务渠道的平均每项交易成本

服务渠道	每项交易成本(美元)
分支机构	1.08
电话	0.54
ATM	0.27
利用银行软件的个人 PC	0.15
Internet	0.01-0.03

3 网络银行的发展现状

国内除了中国建设银行外, 招商银行、中国银行、中国工商银行等国有商业银行都已经推出了网络银行业务。中国网络银行业务起步比较晚, 与西方发达国家比, 有近二十年的差距, 产品功能还是比较缺乏的, 具有差异性的产品更是很少看到。就目前而言, 客户使用最多的还只是一些网络银行的基本服务, 比如账户查询、在线转账和在线支付等, 少数群体会去接触网上证券、网上购物和企业银行等较高级别的网络银行服务。我国网络银行建设近些年发展速度还是很快的, 图 1 和图 2 中是近几年调查的 10 个经济发达的城市中, 个人和企业使用网上银行的情况。

可看出我国网络银行业有了重大发展。现在我国网上银行呈现以下特征: 1) 设立网站或开展交易性网上银行业务的银行数量增加。2) 网上银行业务量在迅速增加。3) 网上银行业务种类、服务品种迅速增多。

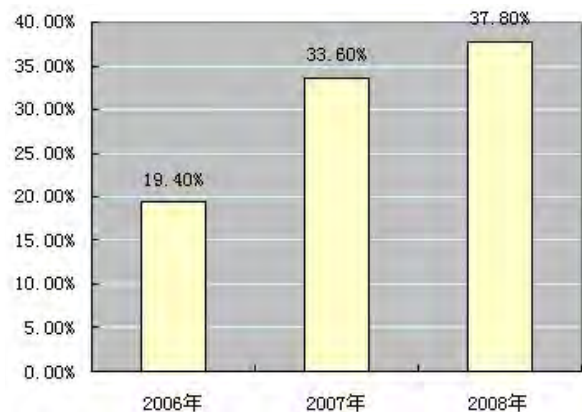


Figure 1. Individual using online banking situation

图 1. 个人使用网上银行情况

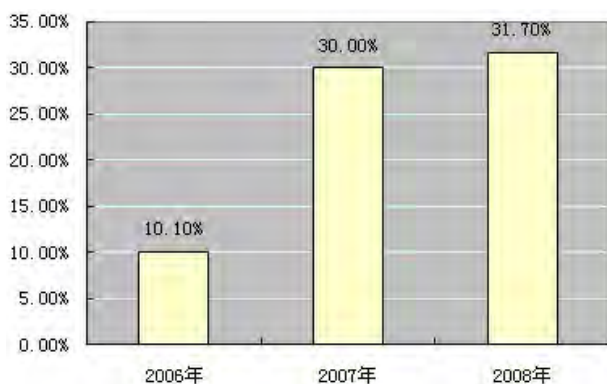


Figure 2. Enterprises using online banking situation

图 2. 企业使用网上银行情况

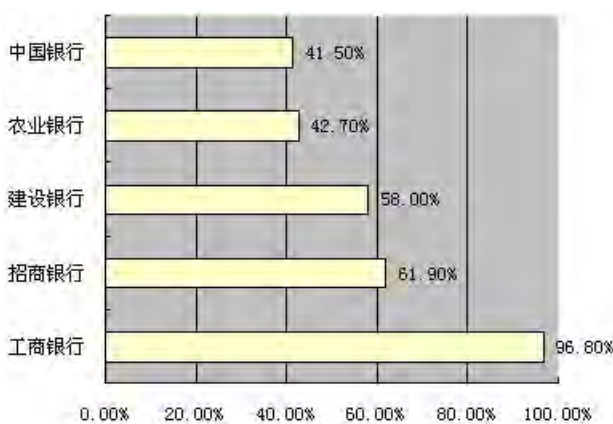


Figure 3. Famousness prong of online banking in the user

图 3. 各商业银行网上银行在用户中的知名度

4) 银行日益重视业务经营中的品牌战略。5) 外资银行开始进入网上银行领域。但我国目前尚未出现完全依赖或主要依赖信息网络开展业务的纯虚拟银行，由此看出，中国的网上银行业务发展任重道远。

4 网上银行服务的主要内容

网上银行服务是根据市场需求而发展的，在目前主要有三个层次的应用：

1) 网络营销

这是一个较容易实现的方面，开展网络营销，直接利用互联网提供网上银行信息服务，同时开发现有网络同互联网的兼容技术和安全措施。

2) 电子商务服务

银行利用广域网、互联网技术，充分与电子商务

主办企业合作，介入其清算业务及信用业务，全面介入电子商务，使银行成为未来商业的先行者。目前电子商务已进入实际操作阶段，安全第一网络银行为消费者提供的网上购物系统，只须在网络银行申请一个帐户，存入一定金额，就能在网上选购商品。选定后按照指示输入信用卡密码和支付金额，交易就完成。

3) 网上银行服务

金融企业充分利用现有成功的网络技术与多媒体技术，谋求低成本、高质量的现代商业银行服务，改善传统业务的营运成本、风险度等。在原有系统业务基础上，在网上进行业务创新，使客户能够办理包括储蓄、转帐、信用卡、信贷、证券交易、跟踪收支、现金分析和财政状况分析等在内的各项事务。

5 网上银行的信息安全性分析

5.1 网络银行安全体系的基本内涵

与传统银行相比，网络银行多了由网络技术带来的风险，这与金融网络系统要求稳定性、可靠性、安全性是密切相关的。考虑到网络银行所处的互联网环境和本身业务的特殊性，安全性最为关键，核心就是信息安全。信息安全一般是指网络信息的保密性、完整性、真实性、可用性和不可抵赖性。

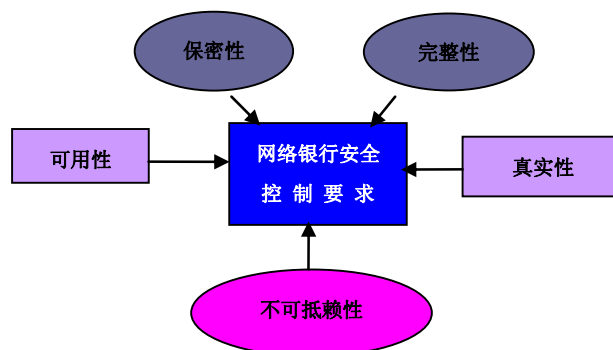


Figure 4. Schematic diagram of information security issues

图 4. 信息安全问题示意图

为了解决网上购物、交易和结算中的安全问题，需要有一个权威的第三方身份认证机构或称CA(Certification Authority)中心，来证明客户身份的真实性。除了CA之外，通常还需要使用加密技术对网上交易的信息进行加密。大致从以下三方面分步进行讨论：

1) 网络银行安全性的技术层面^[5]

主要从系统安全层次中的信息、安全软件、安全硬件、安全物理环境入手,分析国内外网络银行在安全技术方面所采用的标准、交易手段及支付体系的安全技术等,银行需全面的网上电子支付作支持,电子货币或网络货币是最高级的支付工具。

2) 政策、法律及规范

按中央银行与商业银行的职能分工,我国网上银行系统可分为两个层次的系统,下层系统是商业银行为广大客户提供支付服务的金融服务系统,是金融服务、信息管理的重点,主要是商业银行与客户之间的资金往来和结算系统的运作,网上银行安全性的技术层面的分析主要停留在这一层;上层系统是中央银行为商业银行提供支付服务,并执行中央银行货币政策职能,对国民经济实施宏观调控的系统,是完成商业银行之间支付和中央银行与商业银行之间支付活动的最终资金清算与结算系统,国家有关网上银行安全性的政策法规建设也主要通过这一层反映出来。

3) 职业道德(人为因素)

在安全方面一定不能忽视人的因素,银行信息系统中由于人为因素造成系统不安全的情况已有发生,计算机犯罪时间短、破坏性大且后果严重,我国目前尚无一部完整的惩治计算机犯罪的专用法律,往往给不法分子提供可乘之机。加强安全管理、职工教育、职工技术培训等显得日益重要。

5.2 网上银行安全性基本要求

安全技术的突破,电子结算、网上购物、网上银行等一批银行新业务正迅猛的发展。Internet 带来了机遇和利润,Internet 上也充满了黑客、间谍等入侵者。要想从事 Internet 商务,就必须抵挡住黑客们的攻击,这对银行网络的安全性提出了更高的要求。

第一,我国商业银行在系统网络安全上存在的问题。我国的商业银行计算机系统发展水平较低,从网络上来看,网络营运封闭,专网运行,比较安全,但不适合现代网上银行业务;网络保护力度不够,进入小型机的控制也只有路由器,而无防火墙对数据包的合法性进行确认。在系统网络安全上存在的问题主要有以下几个方面:1) 口令保护不严 2) 用户权限分配紊乱 3) 不安全 TCP 工具的使用 4) 对数据包加密程度不高 5) 对交易实体的合法性缺乏更严格的认证。我们的银行网络系统在安全上存在太多的漏洞,必须加强银行内部网络和系统的安全。

第二,网上银行安全性要求。网上银行交易的关键是如何更安全可靠,网上交易要解决交易双方的确认、数据源的不可否认性、数据接收方的不可否认性、数据完整性、数据包的机密性和防重传性等主要问题。怎样才能确认合法身份,如何确保各种账户和资料在保存和传输中不被窃取或更改,以及如何阻止非法侵入银行主机和核心数据系统是重点问题。

5.3 网上银行安全交易手段

近年流行的多个安全电子交易协议或标准中,均采纳了一些常用的安全电子交易的方法和手段。典型的方法和手段有以下几种:

1) 密码技术

采用密码技术对信息加密,是最常用的安全交易手段。在电子商务中获得广泛应用的加密技术有以下两种:(a)公共密钥和私用密钥(public key and private key);(b)数字摘要(digital digest)

2) 数字签名(digital signature)

采用数字签名,能确认以下两点:信息是由签名者发送的;信息自签发后到收到为止未曾作过任何修改。数字签名采用了双重加密的方法来实现防伪、防赖。其原理为:

(a) 发送文件用 SHA 编码加密产生 128bit 的数字摘要。

(b) 发送方用自己的私用密钥对摘要再加密,这就形成了数字签名。

(c) 原文和加密的摘要同时传给对方。

(d) 接收方用发送方的公共密钥对摘要解密,同时对收到的文件用编码加密产生又一摘要。

(e) 加密后的摘要和收到的文件在接收方重新加密产生的摘要相互对如两者一致,则说明传送过程中信息没有被破坏或篡改过。否则不然。(如下图 5)

3) 数字时间戳(digital time—stamp)

在电子交易中,需对交易文件的日期和对间信息采取安全措施,而数字时间戳服务(DTS:digital time stamp service)就能提供电子文件发表时间的安全保护。它是网上安全服务项目,由专门的机构提供。时间戳(time—stamp)是一个经加密后形成的凭证文档,它包括:时间戳的文件的摘要;DTS 收到文件的日期和时间;DTS 的数字签名。

4) 数字凭证(digital certificate, digital ID)

数字凭证是用电子手段来证实一个用户的身份和

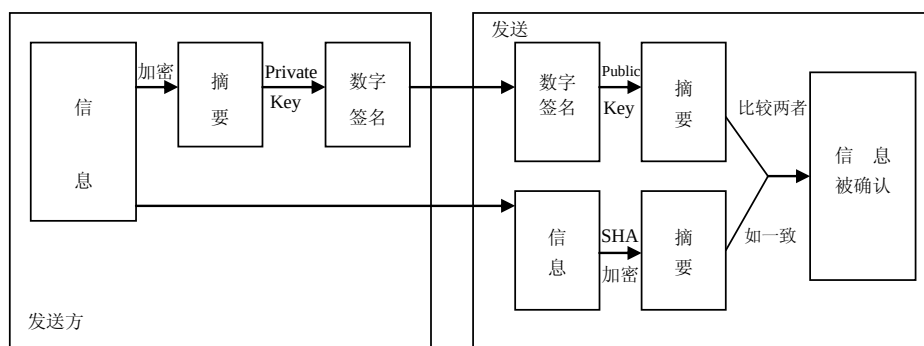


Figure 5. The process of digital signature

图 5. 数字签名的过程

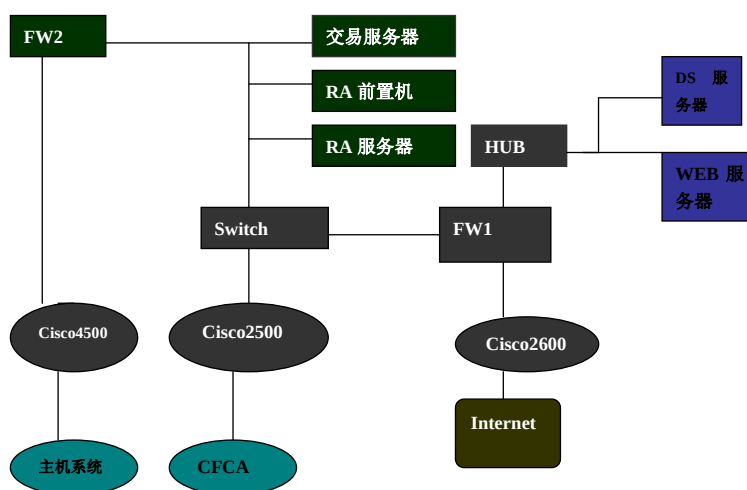


Figure 6. A domestic commercial bank online banking topology

图 6. 国内某商业银行网上银行拓扑图

对网络资源的访问的权限。内部格式是由 CCITTX.509 国际标准所规定的，包含凭证拥有者的姓名；凭证拥有者的公共密钥；公共密钥的有效期；颁发数字凭证的单位；数字凭证的序列号；颁发数字凭证单位的数字签名。

数字凭证类型有个人凭证(Personal Digital ID)；企业(服务器)凭证(Server ID)；软件(开发者)凭证(Developer ID)。前二类是常用的凭证，第三类用于较特殊的场合，大部分认证中心提供前两类凭证，能提供各类凭证的认证中心并不普遍。

5) 认证中心(CA:Certification Authority)

在电子交易中，无论是数字时间戳服务(DTS)还是数字凭证(Digital ID)的发放都不是靠交易的双方自己能完成的，需要有一个具有权威性和公正性的第三方来完成。认证中心就是承担网上安全电子交易认证

服务，签发数字证书，确认用户身份的服务机构。通常是企业性的服务机构，主要受理数字凭证的申请、签发及对数字凭证的管理，认证中心依据认证操作规定来实施服务操作。

上述五个方面是安全电子交易的常用手段，常常结合在一起使用，从而构成网上银行安全交易的体系。

6 实例研究

对照国内某商业银行网上银行建设情况，从其技术层面构建、制度规范建设、从业人员职业道德等进行分析。

6.1 技术层面构建

从网上银行系统的信息安全、软件安全、硬件安全、环境安全入手，根据网络银行的结构图，网上支付所采用的标准、协议、制度等进行分析。网络拓扑结构：

解释:

- 1) 后台主机: IBMRS/6000 H70, 操作系统: AIX4.3.2, 数据库: INFORMIX7.31 (for AIX)
- 2) 交易服务器: HP LH3000, 操作系统: SCO OPENSERVR 5.05, 数据库: INFORMIX 7.31(for UNIX)
- 3) WEB 服务器: IBM F50
- 4) FireWall (FW): 天融信硬件防火墙
- 5) 交换机(Switch)大多为 CISCO, 有少量为 IBM; 路由器(HUB)为 DLINK、3COM 等。

银行整个网络呈树型结构, 树型结构是和银行的数据流向相符的。总行是整个网络的汇接点, 也是网络资源的中心, 主机系统就在总行, 分行间的数据要经过总行转发 (如图 7 网络结构图)。

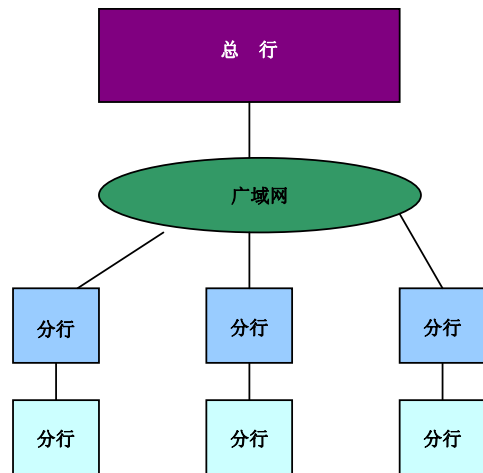


Figure 7. Network structure

图 7. 网络结构图

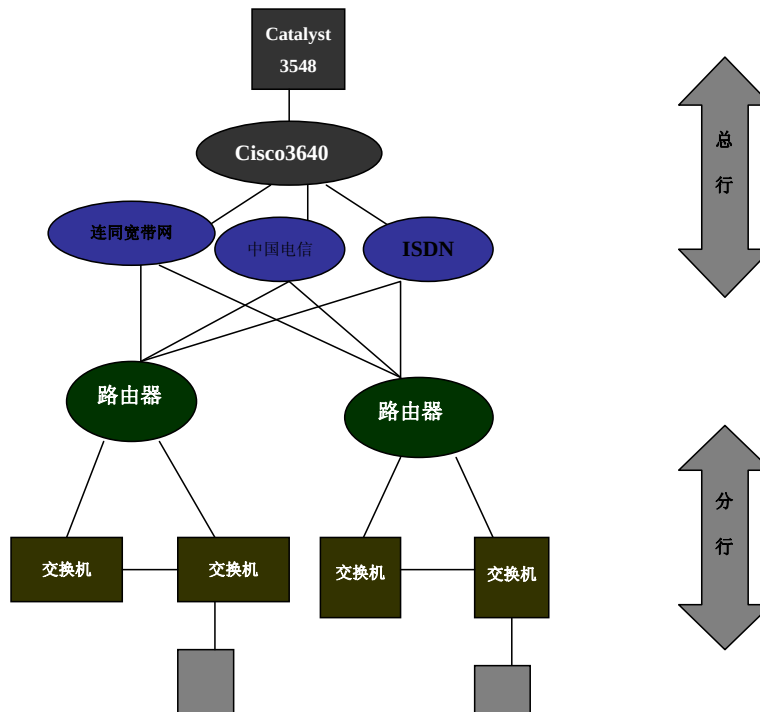


Figure 8. Schematic diagram of the new network transformation program

图 8. 新网络改造方案示意图

系统广域网通信因距离远, 中间环节多, 是通信中最不可靠的一部分。同时广域网资源也是昂贵的、故障恢复不控制在银行手中的部分, 广域网上要有足够的冗余通信手段以保证通信的可靠性。

在新的网络改造方案中, 在广域网部分, 每个分行到总行都有两条主线路, 一条是租用中国电信的

Frame Relay, 另一条是租用联通公司的宽带网线路。租用不同服务商提供的线路可提高线路的可靠性。另有一条 ISDN 拨号备份线路, 线路的带宽根据分行规模的大小, 在 64K-384K 之间, 拨号备份线路的速率可达到 128K。(如下图 8 所示)

两条主线路互为备份又负载均衡。拨号备份线路平

时不启动，只有两条主线路同时断掉时或主线路带宽不够时才拨号。

路由器通过局域网，与以太网交换机相连，路由器上备两个快速以太网端口，同时连到交换机系统上，可以达到热备份的效果。路由器的两个局域网端口分别与两台交换机相连。

6.2 技术层面安全性方面的考虑

重点考虑以下几点：

1) 各分行金融业务应用和办公自动化系统分开，可利用 Catalyst3548 交换机 VLAN 的功能，将不同的业务分在不同的 VLAN 里面。借助 Cisco3662 支持 VLAN Routing 的功能，将这些 VLAN 通过快速以太网口连接起来，在路由器上使用 ACCESS-LIST 定义安全策略，实现不同应用之间的安全。

2) 动态路由协议之间使用安全认证。OSPF 动态路由协议要求路由器在交换 LSP(链接状态包)之前，首先要建立相邻关系，建立相邻关系时定义身份鉴别，只有通过鉴别的路由器能建立起相邻关系，避免非法的路由攻击。

3) 1SDN 远程拨号相对不安全，要单独处理。远程拨号备份，使用 PPP CHAP 验证，PPP CHAP 在线路上不容易被攻破。远程拨号应用，还可使用集中化管理的远程访问认证服务器 Cisco Secure。所有的拨号连接或虚终端的连接都要通过该服务器进行验证、鉴别、授权、计帐。它能记录用户登录的起始及终止时间，这些是银行用于审计的重要数据。同时 Cisco Secure 能根据用户名限制用户的登录时间段，根据用户名还可进行授权，不同用户有不同的登陆权限。

4) 分行及分行以下的数据在进入骨干网之前，要经过路由器上的 ACCESS-LIST 或硬件防火墙的过滤，一方面防止未经授权的数据进入总行，带来安全方面的不利因素；另一方面使骨干上的路由器节省下 CPU 能力用于快速的数据转发，实现复杂的动态路由处理及路由策略处理。

5) 采用 PKI 加密方式，使用 SET 协议的支付网关，为国内该行发行的信用卡和借记卡用户提供网上安全支付手段，客户端需要下载软件。确保网上支付安全，须对接入用户的合法性进行认证授权，由国家统一的中国金融认证中心进行 CA 认证。

6.3 规范制度及人为因素安全方面的控制

主要是国家及中国人民银行制定实施，该行在安

全制度及人员的规范也作了细致的工作：1) 安全组织管理机制。成立电子化生产系统安全防范工作小组，负责全行的电子化生产系统安全保密和风险防范工作。2) 制度建设和执行情况。制定了一系列的《运行管理实施细则》，《安全防范实施细则》，《安全保密实施细则》等等，各项管理工作均落实到人，使管理工作制度化、规范化，提高了计算机系统的可靠性。业务数据维护均由申请部门按规定填表提交申请，并交相关部门和领导审批，维护时实行双人互相监督机制，将过程和结果记录，强化运行管理制度的执行，提高了系统数据维护的实效性和安全性。

7 总结

网上银行系统是相当先进的，经过近年来的发展，大家都意识到安全性建设对于网上银行这样开放性系统的重要性，在系统的建设中也加大投入来构筑安全防线。目前国内由于网络技术的限制、管理制度不健全、人员的素质有待提高，实现一个高度安全对客户有较高要求的系统，难免会带来一定的困难。^[6,7]

建设有中国特色的网上银行，要适应国情与民情，从本文的论述来看，至少应做好以下几个方面的工作：

1) 网上银行是一个全球互通、联系紧密的整体，网络及主机系统都应采取可持续运行技术，一旦出现故障，能自动切换到备份系统或不停机更换故障设备，以保证系统的不间断运行，维护整个网上银行的通畅运行。

2) 中国的商业银行在其电子支付系统中普遍选择了国际中流行的 SSL 和 SET 两种。选择 SSL 的致命之处在于浏览器所能够支持的密钥长度很容易被攻破。选择 SET 需要用户安装特殊的软件，并且因为网络带宽等原因，速度问题比较突出。宽带网的建成可以有效地解决这一问题，我国网上支付基本是基于银行卡方式，建议国内的商业银行倾向于选择 SET 协议，安全性比较高。

3) 中国随着网上银行应用和发展，数据安全已变得愈来愈重要。由于受美国政府出口管理条例的限制，大多数 Web 浏览器和服务器的国际版本只支持 40 位以下的弱加密算法，对于传输重要金融数据是远远不够的，国内网上银行的发展迫切需要具有自主知识产权的安全增强软件。

4) 建立必要的法律框架。网上银行和客户之间必须明确和遵守的法律义务和责任，我国这方面的法律法规还不完善，必须有一套健全的安全管理制度来规

范人的行为，还应当有一套安全稽核的方法进行事后监督以便及时发现问题。

网上银行在国际上作为一种银行服务发展趋势已不可逆转，我国的网上银行需要在体制、安全技术、管理等诸多问题中不断总结经验，取长补短，不断发展和创新，这样我国的网上银行必将迎来美好的前景。

References (参考文献)

- [1] Huangxu. On the current Bank e-Security Management. Hainan Finance, 2008(4).
黄旭，浅议当前银行电子化安全管理，海南金融，2008(4).
- [2] Yang Gaolin. Introduction to Internet Banking Marketing[M]. China Financial Publishing House, 2007.
杨高林，网络银行营销概论[M]，中国金融出版社，2007.
- [3] Zhang Changhui. New developments in electronic banking. Electronics and Automation, 2008(9).
张长惠，银行电子化的新发展，电子与自动化，2008(9).
- [4] Huang Xiaowu. Internet Banking[M]. Wuhan: Wuhan Press, 2008.
黄孝武，网络银行[M]，武汉：武汉出版社，2008.
- [5] Liu hao. China's Internet banking security problem-solving approach. Modern Finance, 2007.2.
刘昊，我国网络银行安全问题解决途径，现代金融，2007.2.
- [6] Wang yinggou. Thinking of building China's Internet Banking. Modern Finance, 2009.7.
王莹构，构建中国网络银行业的思考，现代财经，2009.7.
- [7] David Chappell. Understanding BizTalk Server 2007[R]. Microsoft Corporation, 2008(11): 12-15.
- [8] Elliotte Rusty Harold, W Scott Means. XML in a Nutshell [M]. 2nd Edition. Sebastopol O'Reilly & Associates, 2007.
- [9] David Wagner, Bruce Schneier. Analysis of the SSL 3.0 protocol. The Second USENIX Workshop on Electronic Commerce Proceedings, USENIX Press, November 2008.
- [10] Henry Engler. "The Future of Banking" [J]. American Economic Review, 2007.
- [11] Joseph A. DiVanna, "Redefining Financial Services" [J]. Journal of Economic Perspectives, 2009.
- [12] Jifu Wang: Strategic Challenge, Strategic Responses, and Strategies: Study of Chinese State-owned Enterprises, Dissertation of Auburn University, 2007(8): 12-14.
- [13] Sherif M.H., Serhrouchni A., Gaid A.Y. et al. SET and SSL: electronic payments on the Internet. Computers and Communications, 2008(7): 353-358.