一种基于 WEB 方式的企业电子银行系统的安全设计方案

A Safety Design of Enterprise Electron Bank Based Upon WEB Model

蒙宁瑜
Meng Ningyu

(中国建设银行广西区分行科技处 南宁 530022)
(Department of Science and Technology, Guangxi Branch, China Construction Bank, Nanning, 530022)

摘要 简述企业电子银行系统的特点、结构和工作方式，分析企业电子银行系统存在的安全隐患，并针对这些安全隐患，从系统网络设计、网络配置、应用软件的安全设计及内部管理机制等方面提出一种基于 WEB 方式的企业电子银行系统的安全设计方案。

关键词 电子银行 安全隐患 安全设计

中图法分类号 TP 393.08; F 830.4

Abstract The feature, system architecture and process about Enterprise Electronic Bank (EEB) were explained. By analysis of safety hidden danger of EEB, a safety design based upon Web model is developed for EEB in consideration of network design, network configulation, safety design and byelaw of software application and bylaw, etc.

Key words electronic bank, safety hidden danger, safety design

企业电子银行是通过利用网络通讯技术结合计算机安全防范技术等现代化的处理手段，将企业的计算机与银行的计算机业务系统相连接，实现企业自助金融服务的虚拟银行，它基于 WWW 技术的 BROWSE/SERVER 模式，借助安全硬件设备（如 IC 卡等），可以为客户提供多种金融产品，使企业的财务人员不用到银行就能办理如同城转帐、异地汇兑、银行汇票（本票）申请、发放工资、委托收款、贷款申请、贷款本息归还和预约提现、语言、预约上门收款等业务，将银行的服务延伸到企业，从而有效的提高企业的办事效率和银行的服务质量。

由于企业电子银行服务牵涉到银行的资金安全，因此，如何确保数据的安全是企业电子银行系统需要考虑的重要内容，作者就企业电子银行系统的安全问题结合工作实践，提出一种基于 WEB 方式的企业电子银行系统的安全设计方案。

2000-12-25 收稿，2001-03-23 修回。

1 企业电子银行潜在的安全隐患

一个典型的企业电子银行系统一般采用基于 WEB 技术的 BROWSE/SERVER 模式，其网络整体结构如图 1 所示。

此种方案需路由器（含 Modem）、防火墙、Web 服务器、企业电子银行前置服务器，利用通用浏览器方式，安全依靠 SSL 数据通讯保密方式和安全服务器提供的安全服务，网络隔离依靠防火墙，客户接入通讯协议采用 TCP/IP。Web 服务器运行在 Windows NT Server 操作系统上，WebServer 采用 IIS (Internet Information Server) 信息服务器，与企业银行业务主机的接口采用 ASP 和 CGI。企业银行业务主机运行在 SCO Open Server 平台上。从系统的体系结构和应用流程可以看出，企业银行潜在的安全漏洞主要出在：(1) 不合法用户的登录；(2) 通讯过程中数据的被窃和篡改；(3) 转帐交易的抵赖；(4) 银行网站受到攻击；(5) 应用软件系统的安全性；(6) 管理的安全性。

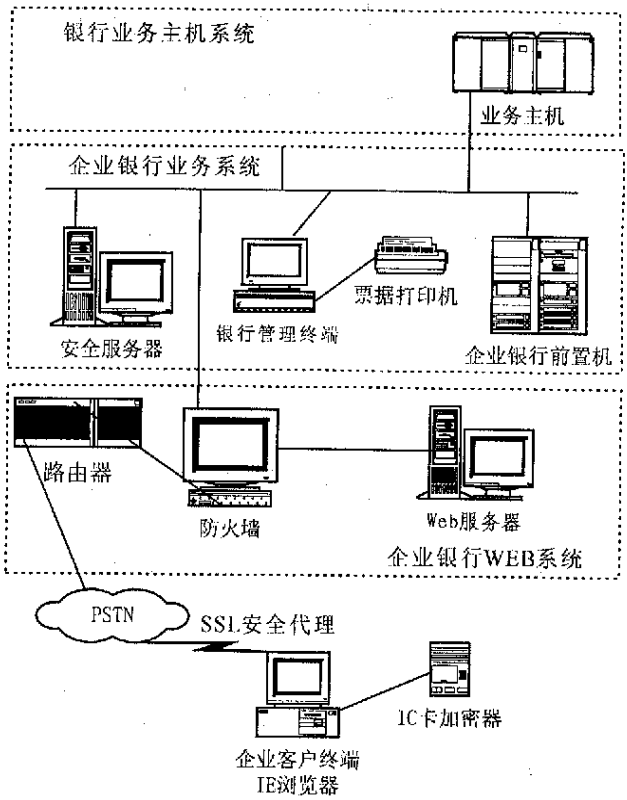

图 1 企业电子银行系统的网络结构

2 企业电子银行系统的安全对策

针对企业电子银行潜在的安全隐患，可以采取以下几个方面的措施来确保企业电子银行系统的安全。

2.1 网络设计

由于系统通过公用通信线路进行数据传输，数据的安全性和保密性受到严重的威胁，因此，在网络设计上可采用一些防范措施：(1) 采用通信服务器（前置机）。通过引入通信服务器，作为 WEB SERVER 与银行业务主机之间进行数据交换的中介，业务系统将要输出的数据放置在通信服务器中，由它向外输出，外部输入的数据经由通信服务器进入内部的业务系统。由于将数据库和业务系统封闭在系统内部，增加了系统的安全性。(2) 采用网段分离技术。把系统前置机、WEB SERVER 与业务主机设计在不同的网段，不同网段间可以通过配置使之不能直接互访，从而减少银行业务系统被正面攻击的机会。通过虚拟网技术，网络管理员可以在网络控制台上对网段做任意划分。

2.2 网络配置

网段分离和通信服务器起作用，还需要网络配置来具体实施和保证，如用于实现网段分

离的虚网配置。为进一步保证系统安全，还要在网络配置中对防火墙和路由等方面做特殊考虑。

2.2.1　*路由器*

路由配置避免入侵者绕过通信服务器而直接访问数据库等内部资源。

2.2.2　*防火墙*

防火墙避免入侵者借助公开网段访问内部网段。路由器通常都具有过滤型防火墙功能。这一功能通俗地说就是由路由器过滤掉非正常 IP 包，把大量的非法访问隔离在路由器之外。过滤的主要依据在源、目的 IP 地址和网络访问所使用的 TCP 或 UDP 端口。几乎所有的应用都有其固定的 TCP 或 UDP 端口，通过对端口的限制，可以限定网络中运行的应用（如可以封掉 telnet，ftp 等功能）。

过滤防火墙检查所有送往银行的数据包的源地址和目的地址，滤除不指向银行网络服务的数据包，同时清除那些具有银行内部网络地址的外部数据包，防止外部用户试图伪装成内部信息访问银行内部网络。HTTPS 是外部数据和银行内部网络的唯一通道。

2.2.3　*网络服务程序的配置*

任何非法的入侵最终都需要通过被入侵主机上的服务程序来实现，关闭被入侵主机上一些没有必要运行的程序（如主机等价性、用户等价性及其他一些登录服务、数据传输服务），入侵必然无效。这也是保证系统安全的一个相当彻底的措施。

2.3　应用软件的安全设计

在应用系统的安全设计上，应该考虑以下几个方面的内容。

2.3.1　*安全的身份认证*

企业电子银行使用 SSL (Secure Sockets Layer) 结合公钥密码体系来进行客户和服务器的身份认证。

SSL 是由 Netscape 公司开发的一套 Internet 数据安全协议，SSL 协议位于 TCP/IP 协议与各种应用层协议之间，为数据通讯提供安全支持，见图 2。

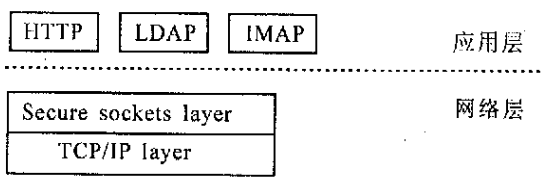

图 2　SSL 协议的设置位置

SSL 协议可分为两层：(1) SSL 记录协议 (SSL Record Protocol)：它建立在可靠的传输协议（如 TCP）之上，为高层协议提供数据封装、压缩、加密等基本功能的支持。(2) SSL 握手协议 (SSL Handshake Protocol)：它建立在 SSL 记录协议之上，用于在实际的数据传输开始前，通讯双方进行身份认证、协商加密算法、交换加密密钥等。

公钥密码体系是不对称加密算法体系，在公钥密码体系中，银行向客户发放配对使用的公开密钥和私有密钥，公开密钥对外公布，私有密钥仅供特定用户使用。使用公开密钥加密的信息只能使用某一特定私有密钥解密。由此，参与交易的双方，通过公开密钥和私有密钥配对使用能在进行交易处理前确认对方身份。客户能够确保他是将信息传送给银行而不是怀有恶意的第三方。同时，银行能确保他收到的信息是来自授权的合法用户，而不是一个正寻找途径侵入银行的入侵者。

银行的身份证机构向每位客户发放一份公钥证书，证书指示用户的公钥与用户的身份紧密联系。开始交易前，客户利用浏览器的 SSL 加密功能，向银行发送一份安全认证请求消息，银行发送一份包含银行公钥的身份证消息作为应答。浏览器验证银行身份，然后使用银行公

钥加密，产生一份包含客户公钥的应答消息发给银行，银行使用银行私钥解密此信息，并使用客户公钥加密信息应答客户。这样，客户和银行相互认证了对方身份详见图3，浏览器用银行公钥加密产生一个随机的会话钥，或对称钥。银行使用其私钥解密该对称钥，对称钥将用来加密当前会话中所有需要在网上传送的数据。对称密钥在客户与银行的每一次通信中都是唯一的，由此减少了任何外部人员进入干扰破坏交易的风险。

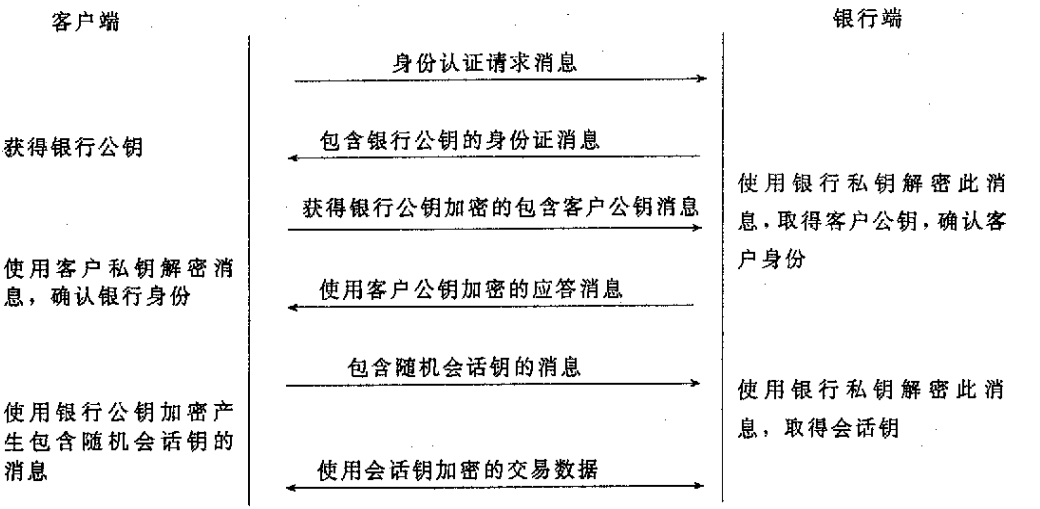

图3 企业银行与客户的身份认证过程

2.3.2 安全的交易处理过程

在应用层上，设计一个安全服务系统，从应用层提供全面的安全交易服务，包括：(1) 鉴别与认证。包括终端系统与中心服务器之间的鉴别和中心服务器对终端用户的认证和鉴别。(2) 完整性控制。对网络中传输的报文进行MAC认证，这是银行的业务系统通常采用的安全机制。在主机数据库系统中，对一些关键数据表如客户帐户数据表、交易流水数据表、操作员登记表等，增加DAC域段，该域段的值一般是由本数据表中的关键域段如帐号、余额、密码、支取方式、帐户状态等通过一定的算法计算得到。这样，在每次对这些数据表的记录进行访问时，都进行DAC计算并校验；或当用专门的校验过程进行检查时，可以及时发现被非正常改变的数据记录，保证数据记录的完整性。(3) 信息保密。根据应用的需要，对客户口令、用户PIN以及其他希望加密的信息(包括文件)，由安全服务系统进行加密后传输或存放。(4) 数字签名。安全服务系统可以根据业务的需要，对关键或敏感交易作数字签名，实现不可否认性。(5) 访问控制。不同的用户具有不同的权限，根据权限要求设置不同的功能调用和数据访问控制，以强制控制方式，由安全服务系统实施控制。(6) 跟踪与审计。对所有的交易过程进行跟踪，并安全地保存，提供给审计人员根据其设定的审计范围与规则进行审计。

2.3.3 安全的密钥管理

密钥是加密算法中的可变部分，同时数据的安全性在很大的程度上依赖于对密钥的保护，而不能仅仅寄希望于对算法和硬件本身采取某种保护。密码体制可以公开，密码设备可以丢失，但密钥丢失或出错，不但合法用户不能提取信息，而且可能使非法用户窃取信息。因此，密钥的安全管理应作为应用设计的一个重点之一。

企业电子银行系统对密钥的管理应采用集中的管理方式，由中心（银行端）集中负责密钥的生成、分发。在企业电子银行客户端，有身份认证密钥和数据加密密钥，包括一组非对称密钥和一个交易密钥以及系统认证密钥，都保存在 IC 卡中。非对称密钥中用于数字签名的私钥是不变的，而用于数据加密的交易密钥是一次一密，每次由客户端产生并用于 DES 算法的加密密钥，结合 IC 卡中的 TRI—DES 加密算法加密传输数据。在企业电子银行系统银行端，有系统主密钥、密钥加密密钥和数据加密密钥。数据加密密钥有每个客户的临时交易密钥、客户身份认证公有密钥、客户重要数据加密密钥等；密钥加密密钥是用于加密保存数据加密密钥的密钥；系统主密钥是用于加密密钥并启动系统。系统主密钥、密钥加密密钥保存在 IC 卡中，其他的数据加密密钥则以密文形式和客户访问控制等重要信息一起存放在数据库中。

2.3.4　数据库安全管理

对数据加密密钥库和重要数据库采用如下方法保护：(1) 确保数据库的完整性与可靠性。通过单向函数的密码算法对数据加密，以确保数据的完整性。(2) 数据库的有效性。(3) 数据库的保密性。(4) 数据库的可审计性和存取控制。(5) 用户身份鉴别。

2.4　完善内部安全管理机制

银行需要制定相应的规章管理制度，如企业与银行签定的银企合作协议书、企业电子银行重要机具管理制度、企业电子银行后台管理办法等，确保不出现人为的安全漏洞。另外，还应加强对数据资料管理、监督检查，以保证数据资料能正常恢复；要定期对计算机处理的数据结果进行核查，发现问题及时分析处理。

3　结语

企业电子银行的安全问题是一个系统性、综合性的问题，建设时不能孤立考虑，只有层层设防，安全问题才能得到有效解决。同时，与其他技术一样，入侵者的手段也在不断提高。在安全防范方面没有一个一劳永逸的措施，只有通过不断地改进和完善安全手段，加强管理，才能尽可能保证不出现漏洞，保证系统的正常运转，保证银行资金的安全。

参考文献

1　Bruce Schneier (美). 应用密码学协议、算法与 C 源程序. 吴世忠，祝世雄，张文政等译. 北京：机械工业出版社，2000.

2　李庆霞，葛传滨. 计算机网络安全及对策. 中国金融电脑，1999，6：57～59.

（责任编辑：邓大玉）