信息时代的网络银行系统

孙江海 （交通银行上海分行电脑处）

一、网络银行概念

网络银行是随着国际互连网络 INTERNET 的普及而发展起来的一种高科技的银行业务手段。简单地说，网络银行就是一套信息系统，它可以使银行和客户通过计算机互连网络连接起来，并在网络上实现银行的业务操作。

INTERNET 网络银行可以向客户提供银行现有绝大部分业务的服务，并且根据银行的需求，可以方便地增加或者改变网络银行系统的功能和业务。

网络银行系统的业务功能可以按照银行的业务需求和安全需求而分为不同的部分。

实际上，网络银行可以提供所有银行业务中的非现金业务服务，并且可以随着银行业务的扩展而不断增加功能。

二、网络银行的优越性

网络银行作为一种高科技的银行业务手段，与传统的银行服务体系相比，具有众多明显的优点：

1.银行服务效率大大提高

客户通过网络银行系统进行银行业务，每一笔业务的操作均通过客户的计算机与银行之间自动进行。与传统的柜台服务方式相比，有很多优点。首先，客户进行银行业务的等待时间大大减少，操作简便易行，方便了客户；其次，网络银行的建立分流了一批拥有计算机的客户，缓解了现有银行营业所的营业压力，并且减少银行业务中间环节；另外，网络银行系统的建立，使银行可以容易地实现全天 24 小时服务，大范围远地连网服务，实时交易服务等，从而大幅度地提高银行的服务效率。

2.银行的相对投入大大减少

网络银行系统可以通过 INTERNET 与大量客户同时进行银行业务，可以大大提高银行的业务能力。建立一套网络银行系统的投资比新建一个传统的营业所少很多，但是建立网络银行系统所获得的收益却远大于建立一个传统的营业所。所以，与传统的方式相比，建立网络银行系统会使银行的相对投入会大大减少，提高了银行投资的收益。

3.拓展银行新兴业务的良好基础

网络银行系统不仅是现有银行服务的重要手段，而且为银行在未来拓展新兴业务建立了良好的基础。网络银行系统是一套完整的，安全的，基于 INTERNET 技术的分布式多平台计算机信息网络平台。有了这套系统平台，就可以方便地与其他网络交易，网络金融系统连接，并发展出许多新兴的银行业务，例如：

(1)网络商场。网络商场是一种基于 INTERNET 的网上服务机制，为上网者提供购物服务。开有网络银行帐户的客户可以通过 WWW 浏览器访问网络商场的 Web 主页，浏览挑选商品，并通过网络银行进行转帐付款，网络商场随即向客户发货，实现了快捷方便的购物途径。

网络商场的付款操作需要银行介入，如果建立了网络银行系统，银行就可以方便地与网络商场连接，支持网络商场的付款功能。

(2)网络缴费。银行可以在网络银行系统的基础上，与邮电，工商，电力，税务，交通等各个部门联合开展网络缴费的服务，使上网的企业和个人客户方便地通过网络银行系统缴纳各种费用。

(3)电子钱包。电子钱包是网络银行系统另一种的业务项目。客户只需要在自己的计算机上安装 IC 卡读写器，就可以通过网络，将帐户上的存款(一定限额以内)下载到自己的 IC 卡中。客户可以在许多小额支付的场合方便地使用电子钱包进行消费，例如公用电话，公共交通购票，公园门票，自动购物机等等。客户可以随时通过网络向电子钱包中添加现金。

(4)网络证券交易。网络证券交易是网络银行系统一个非常重要的业务方向。银行通过网络银行系统与证券交易所的交易系统连接，向客户提供在线的证券交易服务。客户可以在用 WWW 浏览器访问网络证券交易服务的主页，实时地进行证券交易，客户的资金流动由网络银行系统来完成。客户将得到一种简单，可见，快速，安全的证券交易服务。

三、网络银行的安全风险

在 INTERNET 这种公众网络上开展银行业务，保证用户和银行机密信息的安全性是至关重要的。对于 INTERNET 上的安全威胁，主要有以下几种：

1. 对用户身份的仿冒

用户身份仿冒是最常见的一种网络攻击方式，传统的对策一般是靠用户的登录密码来对用户身份进行认证，但用户的密码在登录时是以明文的方式在网络上进行传输的，很容易被攻击者在网络上截获，进而可以对用户的身份进行仿冒，使身份认证机制被攻破。在这种情况下，身份认证的可靠性就变得至关重要。

2. 对网络上信息的监听

攻击者在网络的传输链路上，通过物理或逻辑的手段，对数据进行非法的截获与监听，从而得到用户或服务方的敏感的信息。

为了保证信息的保密性，必须对网络中传输的敏感信息进行加密保护。

3. 对网络上信息的篡改

攻击者有可能对网络上的信息进行截获并且篡改其内容（增加、截去或改写）。这就对数据传输的完整性提出了要求。

4. 对发出的信息予以否认

某些用户可能对自己发出的信息进行恶意的否认，例如否认自己发出的转帐信息等。所以，必须保证信息的不可抵赖性。

5. 对信息进行重发

除了以上情况之外，还存在"信息重发"的攻击方式，既攻击者截获网络上的密文信息后，并不将其破译，而是把这些数据包再次向银行的服务器发送，以实现恶意的目的。所以，系统必须保证信息的唯一性，即能够区分出重发的信息。

四、"网上银行"系统

为了满足国内银行业在互连网上开展网络银行业务的需求，交通银行上海分行与信安世纪公司专门合作开发了一套以安全技术为核心的网络银行产品："网上银行"系统，包括：

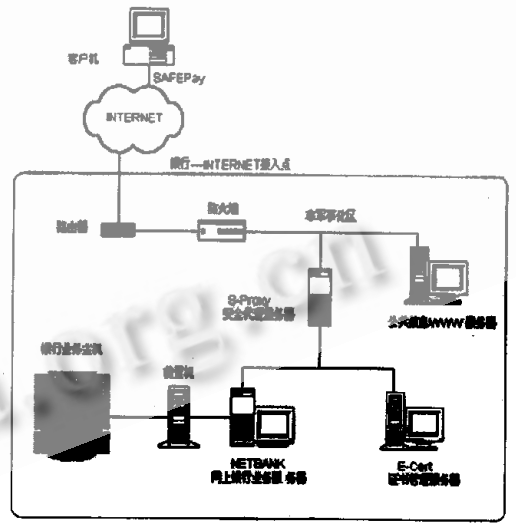
·证书系统（E－Cert）。证书系统提供用户电子证书的产生、发放、管理、回收等功能。电子证书（Certificate）是用户在 Internet 安全系统中的身份证件，用于用户的身份认证和数字签名。证书系统对用户证书进行集中的离线管理，拥有自己独立的数据库系统和图形管理界面。证书系统安装在服务方的 CA 服务器中。

·服务方安全代理 S－Proxy。服务方安全代理系统 S－Proxy 为整个网络银行系统构架了一个安全服务的平台，主要有服务方数据的加密、解密，对客户的身份认证、数字签名校验、数据完整性校验、ACL 管理、审计记录等。

·客户端安全代理 SAFEPay。客户端安全代理为客户端提供完整的安全保障，包括客户端信息的加密、解密、数字签名、数据完整性校验、与 Web 服务器的通信等。

·银行业务系统开发工具包（NetBank）。NetBank 是一个基于普遍符合 INTERNET 标准的一套例程，利用它可以很方便简洁地开发各项银行业务。

下图是典型的网上银行系统配置示意图：



网上银行系统典型配置示意图

在客户一方，通过 INTERNET 和服务方（银行）连接，客户的计算机中装有通用的 WWW 浏览器和"客户端安全代理"SAFEPay 软件。需要更高安全级别的客户还可以选择使用 IC 卡的方式，这就需要增加一台 IC 卡读写器。客户通过浏览器发出的交易请求被 SAFEPay 签名并且加密以后，通过 INTERNET 发送给银行。

在服务方，银行通过自己的路由器接入 INTER-

NET,路由器直接与防火墙相连,防火墙在网络层进行包过滤,并分离内外网段。防火墙后的网段(非军事化区)上连接了 S-Proxy 和公共信息 WWW 服务器。S-Proxy 在应用层实现可靠的安全保障,包括加、解密,签名、认证等等。S-Proxy 后面受保护的内部网段上连接 NETBANK、E-Cert 等服务器。经过 S-Proxy 解密并认证的交易信息发送到 NETBANK 服务器,经过 NETBANK 处理、检验信息来源的合法性后传送给银行业务主机进行处理。E-Cert 则负责发放所有用户的证书,并对证书进行管理和审计。

为了保证整个网络银行系统的安全,其中采用了以下安全技术:

1.身份鉴别机制

在 INTERNET 网上银行系统中,用户的身份认证采用"非对称密码体制"的加密机制、数字签名机制和用户登录密码的多重保证。服务方(银行)对用户的数字签名信息和登录密码进行检验,全部通过以后,才对此用户的身份予以承认,确保了身份认证的安全可靠。

2.数据加密机制

INTERNET 网上银行系统采用了对敏感数据流进行加密传输的方式,一旦用户登录并通过身份认证以后,用户和服务方之间在网络上传输的所有数据全部用会话密钥加密,直到用户退出系统为止,而且每次会话所使用的加密密钥都是随机产生的。这样,攻击者就不可能从网络上的数据流中得到任何有用的信息。

3.数据完整性机制

INTERNET 网上银行系统采用了基于"HASH 算法"和"非对称密码体制"的方法对数据传输的完整性进行保护。具体做法是,对敏感的信息先用"HASH 算法"制作"数字文摘",再用非对称加密算法进行"数字签名"。一旦数据信息遭到任何形式的篡改,篡改后所生成的"数字文摘"必然与由"数字签名"解密后得到的原始"数字文摘"不符,所以就可以立即检验出原始的数据信息已经被他人篡改,这样就确保了数据的完整性不被破坏。

4.数字签名机制

INTERNET 网上银行系统中,每一笔金融交易都回附带有发出方的数字签名,这主要有两个目的。

第一,银行根据交易信息的数字签名来确认交易发出方身份的合法性。如果用户的数字签名错误,则银行不予受理。这样,就实现了交易的认证要求。

第二,用户每次业务操作的信息均由用户的私钥进行数字签名。因为用户的私钥只有用户自己才拥有,所以信息的数字签名就如同用户实际的签名和印鉴一样,可以作为确定用户操作的证据,交易发出者不能对自己的数字签名进行否认,保证了银行的利益不受损害。这样,就实现了交易的抗否认要求。

5.防重发机制

由于用户发出的操作具有时间上的唯一性,即同一用户不可能在完全相同的一个时刻,同时发出一个以上的业务操作,所以 INTERNET 网上银行系统采用了"时间戳"的方法来保证每一次操作信息的唯一性。在每个用户发出的操作数据包中,加入当前系统的时间信息,时间信息和业务信息一同进行数字签名。由于每次业务操作的时间信息各不相同,所以即使用户进行多次完全相同的业务操作,也会得到各不相同的数字签名。这样,就可以对每次的业务操作进行区分,保证了信息的唯一性。

6.审计机制

INTERNET 网上银行系统中,对用户每次登录、退出及用户的每次交易都会产生一个完整的审计信息,并记录到审计数据库中备案。这样,就方便了日后的查询、核对等工作。

交通银行上海分行互联网络银行服务系统使用户在家中、办公室、宾馆或全世界任何地方,只需一台普通的个人电脑和取得入网手段就能获得全天候的实时银行服务。目前我们为企业和个人用户提供公共金融信息查询、帐户信息查询、支付转帐及外汇买卖等服务。

随着业务需求的增加,将不断地有新地业务加入互联网络银行系统中去,以便为用户提供更高质量地服务。

(来稿时间:1999 年 5 月)