银行网络系统安全策略

中国建设银行深圳市分行　李建平

计算机网络的不断发展，加快了银行电子化建设的进程，同时也带来了许多安全问题。本文提出了银行计算机网络系统的安全问题，分析了不安全因素对网络资源构成危害的途径与可能性，讨论了其安全需求、安全对策和安全技术，最后阐述了银行计算机网络系统的安全管理手段。

问题的提出与分析

由于互联网络的开放性和通信协议的安全缺陷，以及在网络环境中数据存储和对其访问与处理的分布性特点，网上传输的数据很容易受到破坏、窃取、篡改、转移和丢失，对网络服务的干扰等。这些潜在危害通常是由对网络的攻击所引起，其手段有：身份窃取（Identity Interception）、假冒（Masquerading）、数据窃取（Data Interception）、否认（Repudiation）、错误路由（Misrouting）、拒绝服务（Denial of Service）和业务量分析（Traffic Analysis）等。此外，用户在操作和管理上的失误，同样会对网络安全构成危害。

网络的安全性定义为：

①保证网络服务的可用性，即要求网络向客户有选择和不受时空限制地提供其所需要的网络服务；

②保证网上信息资源的完整性、可用性和有限的传播范围。因此，网络资源的安全性应具有以下特点：

(1)保证数据信息的完整性，即不能非法更改信息的原始数据。

(2)保证数据信息的可用性，即客户在时空上的任何一点，只要需要，信息必须是随时可用的。

(3)保证数据信息的隐私性，即对信息的非法访问应加以拒绝。

(4)保证数据信息的可靠性，即确保信息来自可靠的信源。

综上所述，计算机网络安全应该包括物理安全和逻辑安全两大部分。物理安全是指网络系统的设备和相关设施受到物理保护，免于被破坏、被丢失等；逻辑安全包括信息完整性、保密性和可用性。

1. 网络中关键设备的可靠性

包括各类计算机设备（如服务器、工作站等）、网络通信设备（如路由器、交换机、智能集中器、调制解调器等）和传输媒体，其可靠性是计算机网络安全和可靠运行的基础。

2. 网络操作系统的可靠性

网络操作系统是网络的灵魂，实现网络系统协同工作，对网络系统资源进行统一管理，对用户对系统的存取访问进行控制。一般来说，对计算机网络的入侵都要突破网络操作系统才能达到。因此，网络操作系统的可靠性对网络的安全十分关键。

3. 数据库系统的可靠性

确保信息安全是计算机信息系统的核心。银行界已全部采用了数据库系统，其中存有各种大量数据，如果遭到破坏，损失是难以估量的。因此就对银行系统所使用数据库的可靠性提出了更高的要求。

4. 网络计算机病毒的威胁

计算机病毒会破坏文件系统和系统软件，尤其是在网络环境中，其传播速度更快、扩散更广。一旦病毒侵入，会导致网络效率急剧下降，系统资源遭到破坏，甚至造成整个网络系统的瘫痪。

银行网络系统的安全功能

银行电子化网络系统中传输的是资金和帐务信息，电子转帐业务的迅速发展，使银行网络终将成为非法入侵者的主要攻击目标。如果不能解决网络通信中存在的安全问题，那么就难以真正实现电子货币、无纸贸易、电子信贷和网络银行等业务。

在进行银行网络的安全设计时，首先要确定网络的安全方针，选择网络的安全功能和安全措施。安全方针是网络安全的目标，安全功能是达到安全目标所需具备的功能和规定，安全措施则是实现安全功能的具体技术机制、方法和设施。目前，采用开放系统互联OSI（Open System

Interconnection)模型的安全体系结构作为网络安全设计的依据，其安全目标就是网络的可用性、完整性和保密性的具体化。

对此，ISO制定的网络安全体系结构针对网络系统存在的潜在危害提出了以下网络安全功能：

(1)对等实体认证。网络中任何两个开放系统主机(Host)在同等分层上建立联接或在数据传输过程中，对对方实体的合法性进行判断以防假冒。对等实体可以是用户与用户、进程与进程，或它们的组合即客户与服务器、服务器与服务器。

(2)访问控制服务。对一个实体访问另一个实体或其功能、服务和能力的限制，即资源只能被对该资源拥有访问权限的实体所访问。

(3)数据保密性。不得擅自将处于联机的数据、文件或数据库、网络传输中的保密信息给非授权人员。其目的是保护网络上传输的信息及Host之间交换的数据，防止数据信息的泄露和破坏。

(4)数据完整性。这是网络安全中最首要和最基本的要求，是指在系统中存储或在网络中传输的数据不遭受任何形式的插入、删除、修改和重发，保证合法用户读取、接收和使用该数据。

(5)信息流安全服务。防止在有用信息的空隙之间插入有害信息，避免出现非授权的活动和破坏。其目的是保证信息流所含内容及其在流动方向上的安全保密。

(6)信源确认。信源确认用于确保在网上访问所获得的数据信息来自合法的信源。

(7)不可抵赖性。指报文的收／发方不能否认收／发过该报文的一种安全需求，如果一方否认，公证机制将根据不可抵赖性机制予以裁决，为数据接收者／发送方同时提供数据源／数据接收的证据，使发送方／接收方无法否认发送／收到过报文及其内容。

此外，还应具有可用性(保证网络具有指定最低限度的连续工作能力，包括对降低性能、影响连续工作的因素进行检测与报告、在设施故障时提供充分的恢复能力，如切换、自动调节等)和可审计性(即指在网络系统中的每一项操作都会留下痕迹，记录下该项操作的各种属性，保留必要的时限以备审查，防止操作者否认)。

为了保证以上安全功能的实现，ISO制定的网络安全体系结构规定了以下八种安全机制：

①数据加密机制是数据信息保护中最基本的方法，通过加密把数据变换成不可读的格式，防止在传输过程中被篡改、删除和替换。

②数字签名是采用一种算法对通过网络传输的信息实现签名的技术，其目的是防止通信的任何一方对自己的行为否认，并防止有人冒充用户对收到的文件加以篡改，或伪造对方发送的信息等。

③访问控制是控制不同用户的访问权限，包括对网络系统、主机、数据库系统和文件系统的访问权限等，并将非法访问事件实时报告给审计跟踪系统，从而产生报警或形成审计记录。

④数据完整性机制。实体之间的信息交换是以一种数据单元的形式进行传输，所以既要对单元数据加密，还要保证数据单元序列的完整性。数据单元序列的完整性要求数据编号连续和时间标记正确，以防止篡改、假冒、丢失、重发或加入数据。

⑤鉴别交换机制是以互换信息的方式来确定实体身份的，用于鉴别交换的技术有：口令、密码技术以及采用用户的特征或所有权(如利用指纹或身份卡进行识别)。

⑥ 业务流量填充机制是在信息传输的间隙连续不断地发出伪随机序列，使非法者在网上窃听数据时无法判断其可用性，并防止其对信息的流量和流向进行分析。

⑦ 路由控制机制是使信息发送方选择特殊的安全路由，因为通信的两节点间可能有多条路线，但并非所有路线都是安全可靠的。

⑧ 公证机制的目的是通过公证机构解决信息传输中的责任问题，因此通信双方必须各自向双方都信任的公证机构发送必要的信息，由公证机构保存，以备以后发生纠纷时进行仲裁。以上安全功能与安全机制并非一一对应，一种安全功能可采取一种或多种安全机制来实现，其间关系如表1。

表 1

安全功能 \ 安全机制	加密	数字签名	访问控制	数据完整性	鉴别交换	业务量填充	路由控制	公证
对等实体认证	Y	Y	N	N	Y	Y	N	N
访问控制	N	N	Y	N	N	N	N	N
数据保密	Y	N	N	N	N	N	Y	N
数据完整性	Y	N	N	N	N	Y	N	N
信息流安全服务	Y	Y	N	Y	N	N	N	N
信源确认	Y	Y	N	N	N	N	N	N
不可抵赖性	N	Y	N	Y	N	N	N	Y

银行网络安全的设计与实现

OSI将网络划分为七个不同的层次：物理层、数据链路层、网络层、传输层、会话层、表示层和应用层。其中

前四个层次对应网络的低层，后三个层次对应网络的高层，现在的传输和路由设备一般都工作在网络的低层上。在OSI网络模型中，一种安全功能由某一特定层有选择地提供，即安全功能由相应安全机制来支持，因此安全功能与网络分层的关系由表2说明。

对应于OSI模型的不同层次，可以采用的安全机制是不同的，而且不同层次的地位也不尽相同，以下作一分析：

(1)物理层规定了网络设备的接口，在这里采用的安全技术是有限的，主要是业务量填充和加密技术。在现代密码学产生之前，加密主要在物理层进行，但现在已很少在物理层上进行加密处理，因为代价太高，而且难以控制。

表 2

安全功能 \ 协议层	物理层	链路层	网络层	传输层	会话层	表示层	应用层
对等实体认证	N	N	Y	Y	N	Y	Y
访问控制	N	N	Y	Y	N	Y	Y
数据保密	Y	Y	Y	Y	N	Y	Y
数据完整性	N	N	Y	Y	N	N	Y
信息流安全服务	Y	N	Y	N	Y	N	Y
信源确认	N	N	Y	Y	N	Y	Y
不可抵赖性	N	N	N	N	N	Y	Y

(2)数据链路层可以采用加密技术，由于不同的链路层协议的帧格式都有区别，所以在加密时必须区别不同的链路层协议。

(3)网络层可采用众多的安全技术，如加密、授权访问控制、数字签名、路由选择控制、业务量填充和数据完整性，也正是该层完全体现了网络的特点。网络互连、网路控制和网络管理等功能主要在该层实现，因此网络层是实施安全技术的主要层次之一。

(4)传输层加密是对端到端之间传送的数据信息进行保护，并为用户提供连续的安全服务，当传送的信息通过中间节点时仍保持密文形式，只有到达目的节点端口才被解密还原成明文。该层除不能采用业务量填充技术之外，其他可以采用的技术与网络层相同。由于传输层的协议较少，因此对该层的关注远不如网络层。

(5)会话层的确切定义到目前为止仍是模糊不清的，经常与表示层和应用层合二为一，因此一般不在会话层进行安全处理。

(6)表示层是对信息的不同格式进行转换，而加密也是一种格式转换。不同的是前者把信息从一种可读的格式变成另一种可读的格式，后者则把信息从可读的变成不可读的。表示层在实际应用中往往与应用层难以区分。虽然在该层能提供安全机制，但完全由表示层独立提供的只有加密一种，其他的都要依赖于应用层的合作。

(7)应用层：应用层可实施所有的安全技术。

在网络安全的技术防范中，数据加密交换是其中最基本的安全技术。网络中的数据加密除了选择加密算法和密钥以外，两个主要问题是实现加密网络协议层以及密钥的管理分配。

数据加密可以在OSI协议参考模型的多个层上实现。通常在网络层以下的加密称为全链路加密，网络层以上的加密称为端间加密。链路加密是目前最常用的加密方法，通常用硬件在物理层上实现，用户没有选择的余地，也不必了解加密技术的细节，一旦在一条线路上采用链路加密，往往需要在全网内部都采用链路加密。端间加密则由用户选择，包括选择加密与否，选择对哪些数据加密，甚至采用什么加密算法。端间加密一般由软件完成，在网络高层进行加密，不需要考虑网络低层的线路、调制解调器、接口与传输码，但是用户的联机加密软件必须与网络通信协议结合。端间加密也可以由硬件完成。在实际中可以根据需要同时采用链路加密和端间加密两种方法。

从技术角度讲，目前流行有三种数据加密算法：对称密钥加密算法、非对称密钥加密算法和不可逆加密算法。广泛采用的DES（Data Encryption Standard）是一种对称加密，数据发送方用一个密钥对数据进行转换，生成密文，接收方则需要用同样的密钥解密，生成明文。对称加密要求数据收发双方必须拥有同一密钥，因此存在两个问题：一是如何保证收发双方间密钥的安全性，二是对称加密要求用户与每一个通信伙伴间分别保存一对系统密钥。非对称密钥加密算法要求数据发送方用接收方提供的一个公共密钥加密数据，而接收方用一个与之相应的私有密钥解密。由于公共密钥无需保密，且被所有数据发送方所共知，因而很好地解决了对称加密中存在的两个问题。但是非对称密钥加密算法的性能较差，限制了其广泛使用。在实际问题中，非对称密钥加密算法很少单独使用，而是经常与对称密钥加密算法同时混合使用。通常收发的实际信息采用对称加密，而用非对称加密技术加密对称加密密钥、数字签名和检验等。不可逆加密算法不需要密钥加密，而且经过加密的数据无法还原，只有输入与原文相同的数据才能得到相同的密文，其计算量通常相当大，只适合于对少数数据进行加密，如口令等。■