第 5 章

电子商务安全技术

电子商务作为一种新兴的商业模式，得到越来越多的关注。任何事情都具有两面性，在人们享受着 Internet 的开放性的同时，也面临着日益严重的安全性问题，因此人们提出了各种增强电子商务安全性的手段。本章着重讨论信息安全性相关的各种技术以及病毒防治的基本知识。

本章学习目标：

(1) 安全性基本概念。
(2) 安全协议(SSL 协议、SET 协议)。
(3) 安全问题及其解决方案。
(4) 信息加密技术与应用。
(5) 数字签名与应用。
(6) 身份认证与识别。
(7) WWW 安全技术。
(8) 防火墙技术。
(9) 计算机犯罪的类型与防范。
(10) 计算机病毒的防范与查杀。

5.1 电子商务所面临的安全问题

5.1.1 Internet 的安全隐患

Internet 的安全隐患主要表现在以下

几个方面：

(1) 开放性。正如前面提到的，开放性和资源共享是 Internet 最大的特点，也是优点。但它的问题却不容忽视。因为，当轻易而方便地访问到别人的计算机时，就应该想到，如果不采取任何安全措施，别人也可以同样轻易而方便地访问你的计算机。到现在为止，Internet 还没有一个主控机构。这样，保护 Internet 联网用户的安全就只有靠用户自身的安全意识了。

(2) 传输协议。Internet 采用 TCP/IP 传输协议。这种协议本身并没有采取任何措施来保护传输内容不被窃取。

(3) 操作系统。由于组成 Internet 的主机上的操作系统存在漏洞，使得每一个连入 Internet 的主机都可能因面临黑客的攻击出现安全问题.

(4) 信息电子化。与传统的书面信函相比，电子化信息的固有弱点就是缺乏可信度，因为电子信息是否正确完整是很难由信息本身鉴别的。而且在 Internet 上传递电子信息，存在着难以确认信息的发出者以及信息是否被正确无误地传递给接收方的问题。

5.1.2　电子商务面临的安全问题

1. 信息泄露

在电子商务中表现为商业机密的泄露，主要包括两个方面：

(1) 交易双方进行交易的内容被第三方窃取。

(2) 交易一方提供给另一方使用的文件被第三方非法使用。

2. 篡改

在电子商务中表现为商业信息的真实性和完整性的问题。电子的交易信息在网络上传输过程中，可能被他人非法的修改、删除或重放(指只能使用一次的信息被多次使用)，这样就使信息失去了真实性和完整性。

3. 身份识别

这涉及电子商务中的两个问题。

(1) 如果不进行身份识别，第三方就有可能假冒交易一方的身份，以破坏交易、败坏被假冒一方的信誉或盗取被假冒一方的交易成果等。进行身份识别后，交易双方就可防止“相互猜疑”的情况。

(2)“不可抵赖”性。交易双方对自己的行为应负有一定的责任，信息发送者和接收者都不能对此予以否认。进行身份识别后，如果出现抵赖情况，就有了反驳的依据。

4. 信息破坏

这也涉及两方面内容。

(1) 网络传输的可靠性。网络的硬件或软件可能会出现问题而导致交易信息传递的丢失与谬误。

(2) 恶意破坏。计算机网络本身容易遭到一些恶意程序的破坏，而使电子商务信息遭到破坏。如：

① 计算机病毒。一种通过修改其他程序而把自身或其变种不断复制的程序，即会“传

染”的程序。

② 计算机蠕虫。一种通过网络将自身从一个节点发送到另一个节点并启动的程序，而这种程序通常都带有破坏性的指令。

③ 特洛伊木马。一种执行超出程序定义之外的程序。例如，一个编译程序除了完成编译功能外，还把用户的源程序偷偷地复制下来。

④ 逻辑炸弹。一种当运行环境满足某种特定条件时执行特殊功能的程序。

根据上面的讨论，可以看出，上面所说的“计算机病毒”的概念是狭义的。事实上，把具有以上特征的程序统称为“计算机病毒”。计算机病毒是计算机界的一大公害。对于利用计算机进行交易的电子商务参与者而言，计算机病毒也是他们不得不防的，因为病毒的爆发势必会造成巨大的经济损失。

5.2 电子商务认证技术

信息认证是安全性很重要的一个方面。信息认证的目的有两个：一是确认信息的发送者的身份。二是验证信息的完整性，即确认信息在传送或存储过程中未被篡改过。

认证是为了防止有人对系统进行主动攻击（如窜改）的一种重要技术。与认证有关的技术包括数字签名技术、身份识别技术和信息的完整性校验技术等。

5.2.1 数字签名技术

为了鉴别文件或书信的真伪，传统的做法是，要求相关人员在文件或书信上亲笔签名或印章，包括商业合同、银行提单、日常书信等。签名起到认证、核准和生效的作用。随着信息时代的来临，人们希望通过数字通信网络迅速传递贸易合同，这就出现了合同真实性认证的问题，数字或电子签名就应运而生了。

数字签名技术是将摘要用发送者的私钥加密，与原文一起传送给接收者。接收者只有用发送者的公钥才能解密被加密的摘要，然后用 Hash 函数对收到的原文产生一个摘要，与解密的摘要对比，如果相同，则说明收到的信息是完整的，在传输过程中没有被修改，否则，就是被修改过，不是原信息。同时，也证明发送者发送了信息，防止了发送者的抵赖。

数字签名必须保证以下三点：

（1）接收者能够核实发送者对报文的签名。

（2）发送者事后不能抵赖对报文的签名。

（3）接收者不能伪造对报文的签名。

使用公钥密码技术就可以实现数字签名。发送方 A 用其不公开的解密密钥 Akd 对报文 M 进行运算，将结果 D(M,Akd)传给接收方 B。B 用已知的加密密钥对接收到的内容进行运算，得出结果 E(D(M,Akd),Ake) = M。因为除了 A 以外没有人能拥有 A 的解密密钥，所以除了 A 以外就没有人能产生密文 D(M,Akd)。这样，就表示报文 M 被电子签名了。

如果 A 抵赖曾发报文给 B，B 就可将 M 及 D(M,Akd)出示给第三方（仲裁方）。仲裁方可以很容易地用密钥 Ake 验证 A 确实发送消息 M 给 B，从而使 A 无法抵赖。反过来，如果

B 将 M 伪造成 M′，则 B 不能在仲裁方面前出示 D(M′，Akd)，从而证明了 B 伪造了报文。可见数字签名也同时起到了验证信息完整性的作用。

由这个过程可以看出，以上处理仅是对报文进行了数字签名，并没有对报文进行加密。因为任何一个截获到 D(M，Akd)的人都可以利用公开的加密密钥得到原始报文 M。所以，在这种传输系统中，通常会使用两套密钥，一套用于数字签名，另一套用于加密。

目前已有大量的数字签名算法，比如 RSA 数字签名算法、ElGamal 数字签名算法、Fiat-Shamir 数字签名算法、Schnorr 数字签名算法、美国的数字签名标准/算法(DSS/DSA)和椭圆曲线数字签名算法等。

5.2.2　身份识别技术

通过电子网络开展电子商务，身份识别问题是一个不得不解决的问题。一方面，只有合法用户才可以使用网络资源，所以网络资源管理要求识别用户的身份。另一方面，传统的交易方式交易双方可以面对面地谈判交涉，很容易识别对方的身份。而通过电子网络交易却不同，交易双方并不见面，通过普通的电子传输信息很难确认对方的身份。因此，电子商务中的身份识别问题显得尤为突出。只有采取一定的措施使商家可以确认对方身份，商家才能放心地开展电子商务。当然，这其中也需要一个仲裁机构，以便在发生纠纷时，进行仲裁。因为存在身份识别技术，有关当事人就无法抵赖自己的行为，从而使仲裁更为有理有据。在电子商务中，身份识别技术的实现往往要采用密码技术(尤其是公钥密码技术)设计出安全性高的识别协议。

身份识别的常用方法主要有两种，一种是使用口令的方式；另一种是使用标记的方式。

1. 口令方式

口令是应用最广的一种身份识别方式，如现代通信网的接入协议等。通行字一般是长度为 5～8 的字符串，由数字、字母、特殊字符、控制字符等组成。

1) 口令选择一般应满足的几个原则

口令的选择一般应满足以下几个原则：

(1) 容易记忆。

(2) 不易猜中。

(3) 不易分析。

第一条是针对用户本人而言的，另两条则是针对想非法侵入系统的人。可以看出，第一条原则与另两条原则之间却有着一定的矛盾性。因为容易记忆的东西往往是用户比较熟悉的，如亲友的生日、姓名、家里的电话号码等。这些虽然容易记忆，但也同时是容易猜中的。而且用户很喜欢只用小写字母或数字作为口令，这就给穷举破译口令带来了方便。所以口令的选择一定要慎重，而且应该定期更换。在满足以上条件的前提下，口令的长度应该尽量长，因为越长的口令越不容易被破译。

2) 口令管理与识别过程

口令的管理方式也是一个重要问题。如果用户的口令都存储在一个文件中，那么一旦这个文件暴露，非法用户就可获得口令。这个问题可以用单向函数来解决，即计算机存储并不存储口令，只存储口令的单项函数。其识别过程如下：

(1) 用户将口令传送给计算机。

(2) 计算机完成口令单向函数值的计算。

(3) 计算机把单向函数值和机器存储的值比较。

这样非法侵入者想获得合法用户口令就不会太容易了。

2. 标记方式

标记(token)是一种个人持有物,它的作用类似于钥匙,用于启动电子设备。标记上记录着用于机器识别的个人信息。常用的标记多采用磁介质,而磁介质却有不少缺陷。磁介质最大的问题就是易受环境影响,而且也易被修改和转录。所以,以智能卡取代磁卡是很有必要的。智能卡的原理是在卡内安装计算机芯片以取代原来的磁介质,这样就克服了磁卡的缺陷,使身份识别更有效、安全。但智能卡仅仅为身份识别提供了一个硬件基础,要想得到安全的识别,还需要与安全协议配套使用。

5.2.3 认证机构

由上文可知,数字签名技术是利用公钥加密技术来验证网上传送信息的真实性。但这存在着一个严重的问题,那就是,任何人都可以生成一对密钥。那么,怎样才能保证一对密钥只属于一个人呢? 这就需要一个权威机构对密钥进行有效的管理,颁发证书证明密钥的有效性,将公开密钥同某一个实体(消费者、商户、银行)联系在一起。这种机构就称为认证机构(Certificate Authority,CA)。

1. 认证机构的职能

认证机构是一个权威机构,专门验证交易双方的身份。认证机构的核心职能是发放和管理用户的数字证书,它接受个人、商家、银行等参与交易的实体申请数字证书,核实情况,批准申请或拒绝申请,并颁发数字证书。此外,认证机构还具有管理证书的职能。

认证机构的管理功能包括以下几个方面:

(1) 证书的检索。数字证书包括有效证书和已撤销证书。用户在验证发送方数字签名时,需要查验发送方的数字证书。这就需要检索有效证书库。另一方面,证书可能在其有效期限内被认证机构撤销,所以,用户也需要检索已撤销证书库。

(2) 证书的撤销。在证书的有效期已到,用户的身份变化,用户的密钥遭到破坏或被非法使用等情况下,认证机构就应撤销原有的证书。

(3) 证书数据库的备份。

(4) 有效地保护证书和密钥服务器的安全。

认证机构在整个电子商务环境中出于至关重要的位置,它是整个信任链的起点。认证机构是开展电子商务的基础,如果认证机构不安全或发放的证书不具权威性,那么网上电子交易就根本无从谈起。

2. 数字证书定义及内容

数字证书(digital ID)又叫数字凭证、数字标识,它包含证书持有者的有关信息,以标识他们的身份。数字证书包括的内容有证书持有者的姓名、证书持有者的公钥、公钥的有效期、颁发数字证书的单位、颁发数字证书单位的数字签名和数字证书的序列号。

3. 数字证书的类型

认证机构发放的证书分为两类：SSL 证书和 SET 证书。一般来说，SSL（安全套接层）证书是服务于银行对企业或企业对企业的电子商务活动的；SET（安全电子交易）证书则服务于持卡消费、网上购物。虽然它们都是用于识别身份和数字签名的证书，但它们的信任体系完全不同，而且所符合的标准也不一样。简单地说，SSL 证书的作用是通过公开密钥证明持证人的身份。SET 证书的作用则是通过公开密钥证明持证人在指定银行确实拥有该信用卡账号，同时也证明了持证人的身份。

4. 数字证书的申请

用户想获得证书时，首先要向认证机构提出申请，说明自己的身份。认证机构在证实用户的身份后，向用户发出相应的数字证书。认证机构发放证书时要遵循一定的原则，如要保证自己发出的证书的序列号各不相同，两个不同的实体所获得的证书的主题内容应该相异，不同主题内容的证书所包含的公开密钥相异。

5. 认证机构的层次结构

认证机构有着严格的层次结构。按照 SET 协议的要求，认证机构（CA）的体系结构，如图 5-1 所示。

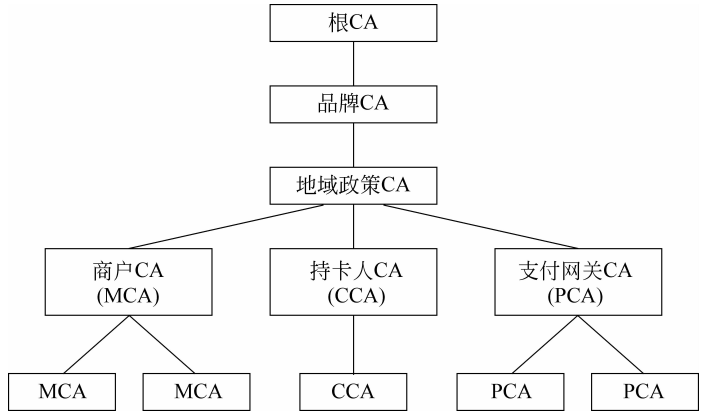

图 5-1　SET 认证机构体系

根 CA（root CA）是离线的并且是被严格保护的。仅在发布新的品牌 CA（brand CA）时才被访问。

品牌 CA 发布地域政策 CA（geopolitical CA）、持卡人 CA（cardholder CA）、商户 CA（merchant CA）和支付网关 CA（payment Gateway CA）的证书，并负责维护及分发其签字的证书和电子商务文字建议书。

地域政策 CA 是考虑到地域或政策的因素而设置的，是可选的。

持卡人 CA 负责生成并向持卡人分发证书。

商户 CA 负责发放商户证书。

支付网关 CA 为支付网关（银行）发放证书。

5.2.4 信息完整性

信息的完整性要靠信息认证来实现，信息认证是信息的合法接收者对消息的真伪进行判定的技术。信息认证的内容包括：

(1) 信息的来源。

(2) 信息的完整性。

(3) 信息的序号和时间。

使用数字签名技术和身份识别技术可以鉴别信息发送者的身份，也就是明确了信息的来源。正像前面分析的那样，数字签名技术可以证实文件的真伪，而身份识别技术可以证实发送人身份的真伪。

信息序号和时间的认证主要是为了阻止信息的重放攻击。常用的方法有消息的流水作业号、链接认证符、随机数认证法和时间戳等。

信息内容的认证即完整性检验常用的方法是：信息发送者在信息中加入一个鉴别码并经加密后发送给接收者检验(有时只加密鉴别码)。接收者利用约定的算法对解密后的信息进行运算，将得到的鉴别码与收到的鉴别码进行比较，若二者相等，则接收；否则拒绝接收。目前实现这一功能的方法有两种：一是采用消息认证码(MAC)，二是采用窜改检测码(MDC)。

5.3 电子商务的其他安全技术

5.3.1 加密技术

1. 基本概念

加密技术是实现信息保密性的一种重要手段，目的是为了防止合法接收者之外的人获取信息系统中的机密信息。所谓信息加密技术就是采用数学方法对原始信息(通常称为“明文”)进行再组织，使得加密后在网络上公开传输的内容对于非法接收者来说成为无意义的文字(加密后的信息通常称为“密文”)。而对于合法的接收者，因为其掌握正确的密钥，可以通过解密过程得到原始数据(即“明文”)。由此可见，在加密和解密的过程中，都要涉及信息、算法和密钥这三项内容。

信息包括明文和密文。算法是加密或解密的过程采用的数学方法，包括加密算法和解密算法。密钥是在加密或解密的过程中需要的一串数字，包括加密密钥和解密密钥。下面通过一个例子来理解加密、解密、算法和密钥的概念。

例如，将 26 个字母 a、b、c……x、y、z 的自然顺序保持不变，但使它们与 d、e、f……z、a、b、c 分别对应，即相差 3 个字母的顺序。这条规则就是加密算法，其中的 3 为密钥。如果原始信息即明文是 good night，则按照这个加密算法和密钥加密后的密文是 jrrgqljkw。不知道算法和密钥的人，是不能将这条密文还原成 good night 的。

从这个例子可以看出，算法和密钥在加密和解密过程中缺一不可。在实际的加密过程中，一般加密算法是不变的，目前存在的加密算法也是非常有限的，但是密钥是变化的。一条信息的加密传递的过程如图 5-2 所示，其中，M 代表信息，T 代表算法，K 代表密钥。

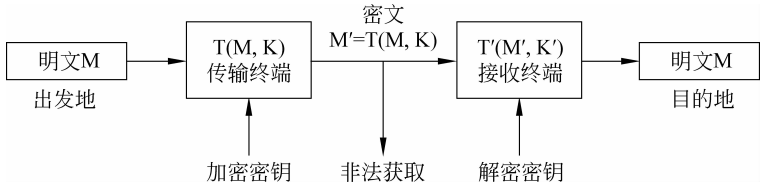

图 5-2　信息加密传递过程

由此可见，尽管在网上传递的信息有可能被非法接收者捕获，但仍是比较安全的。因为想在没有密钥和解密算法的前提下，恢复明文，或者读懂密文，是非常困难的。具体有多困难，就要看加密算法的复杂程度以及密钥的长度了。

这样就出现了两门学问：密码编码学和密码分析学。这两门学问合起来就称为密码学。密码编码学是为了设计出安全的密码体制，防止被破译；而密码分析学则是研究如何破译密文，即在未知密钥的情况下，从密文推出明文或密钥的技术。密码学正是在这种破译和反破译的过程中发展起来的。

2. 密码体制分类

按加密密钥和解密密钥是否相同，可将现有的加密体制分为两种：单钥加密体制和双钥加密体制。使用单钥加密体制的加密技术称为对称密钥加密，使用双钥加密体制的加密技术称为非对称密钥加密。下面分别介绍对称密钥加密和非对称密钥加密。

1）对称密钥加密

对称密钥加密(Secret Key Encryption)也称为专用密钥加密，即发送和接收数据的双方必须使用相同的密钥对明文进行加密和解密运算。对称密钥加密如图 5-3 所示。

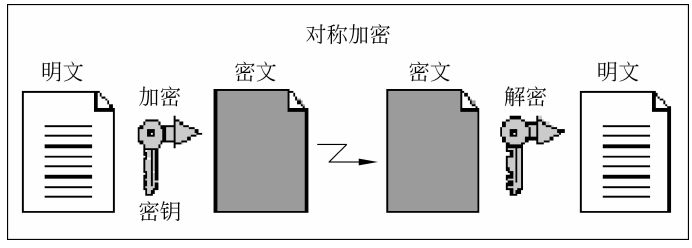

图 5-3　对称密钥加密

使用对称密钥加密可以简化加密的处理，每个交易参与方都不必彼此研究和交换专用的加密算法，而是采用相同的加密算法并只交换共享的专用密钥。如果进行交易的交易参与方能够确保专用密钥在密钥交换阶段未曾泄露，那么交易信息的保密性和完整性就可以通过对称密钥加密算法加密信息和随信息一起发送的报文摘要来实现。

在对称密钥体制中，加密和解密双方使用相同的密钥，其优点是具有很高的保密强度。但对称密钥必须按照安全途径进行传递，双方虽然在通信时加了密，比较保险，但是，密钥却要事先约定或通过信使传递。如果通过信使传递，一方面可能会导致失密；另一方面，在高度自动化的大型计算机网络中，用信使传递密钥显然是不合适的。如果事先约定密钥，则进行网络通信的每个人都要保留其他所有人的密钥，当某一参与方有 n 个交易关系，那

么他就要维护 n 个专用密钥（即每把密钥对应一交易参与方）。这就给密钥的管理和更新带来了困难，密钥管理成为影响系统安全的关键性因素。此外，对称加密方式存在的另一个问题是无法鉴别交易参与者的身份，难以解决数字签名验证等问题。对称密钥加密存在着以下问题：

（1）密钥使用一段时间后就要更换，加密方需经过某种秘密渠道把密钥传给解密方，而密钥在此过程中可能会泄露。

（2）网络通信时，如果网内用户都使用相同的密钥，就失去了保密的意义；但如果网内任意两个用户通信都使用互不相同的密钥，密钥量太大，难于管理。

（3）无法满足互不相识的人进行私人谈话的保密性需求。

（4）难以解决数字签名验证的问题。

2）非对称密钥加密

非对称密钥加密（Public Key Encryption）也称为公开密钥加密，由美国斯坦福大学赫尔曼教授于 1977 年提出。它主要指每个人都有一对唯一对应的密钥：公开密钥（公钥）和私人密钥（私钥），公钥对外公开，私钥由个人秘密保存；用其中一把密钥来加密，就只能用另一把密钥来解密。非对称密钥加密如图 5-4 所示。

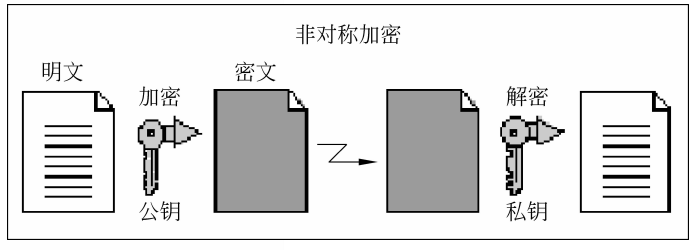

图 5-4　非对称密钥加密

在电子商务交易过程中，商家可以公开其公钥，而保留其私钥；客户可以用商家的公钥对发送的信息进行加密，安全地传送到商家，然后由商家用自己的私钥进行解密。公开密钥加密技术解决了密钥的发布和管理问题，是目前商业密码的核心。使用公开密钥技术，进行数据通信的双方可以安全地确认对方身份，提供通信双方身份的可鉴别性。非对称密钥加密具有以下优点：

（1）密钥分配简单。

（2）密钥的保存量少。

（3）可以满足互不相识的人之间进行私人谈话时的保密性需求。

（4）可以完成数字签名和数字鉴别。

（5）公钥密码体制大都是分组密码，一般不再按明文的加密模式对其进行分类。

公钥密钥解决了专用密钥出现的问题，而且，公钥加密算法不需要联机密钥服务器，密钥分配协议简单，所以极大地简化了密钥管理。但是公钥算法要比私钥算法慢很多，所以在实际应用中，通常使用公钥密码体制交换密钥，而利用私钥密码体制传递正文。除了加密功能外，公钥系统还可以提供数字签名。

3. 报文摘要算法

报文摘要算法(Message Digest Algorithms)采用单向 Hash 算法对需要加密的明文进行摘要,而产生的具有固定长度的单向散列值。其中,散列函数(hash functions)是一个将不同长度的报文转换成一个数字串(即报文摘要)的公式,该函数不需要密钥,公式决定了报文摘要的长度。报文摘要算法和非对称密钥加密一起,可以提供数字签名。报文摘要算法主要有安全散列标准和 MD 系列标准。

1) 安全散列算法

安全散列算法(Secure Hash Algorithm,SHA)是一种报文摘要算法,它产生 160 位的散列值。SHA 已经被美国政府核准作为标准,即 FIPS 180-1 Secure Hash Standard (SHS),FIPS 规定必须用 SHA 实施数字签名算法。在产生与证实数字签名过程中用到的 Hash 函数也有相应的标准做出规定。

2) MD2、MD4 和 MD5

MD2、MD4 和 MD5(MD Standards for Message Digest)是由 RSA 数据安全公司创始人 Ron Rivest 发明的报文摘要算法,由 Ron Rivest 设计。该编码法采用单向 Hash 函数将需加密的明文"摘要"成一串 128 位的密文,这一串密文亦称为数字指纹(finger print),它有固定的长度,且不同的明文摘要成密文,其结果总是不同的,而同样的明文其摘要必定一致。这样这串摘要便可成为验证明文是否是"真身"的"指纹"了。其中 MD2 最慢,MD4 最快,MD5 是 MD4 的一个变种。

4. 加密技术存在的问题

密码学界流传着这样一句名言:加密技术本身都是很强的,但是它们的实现却往往很差。人们需要的是一个贯彻了加密体制的、针对企业环境开发的、标准的加密系统。现在加密的标准很多,固然是有了更多的选择余地,但同时也带来了兼容性的问题。由于缺乏一个安全交易的通用标准,所以不同的商家可能会采用不同的标准。

针对这个问题,产生了安全套接层(SSL)技术。安全套接层技术是由 Netscape 公司于 1994 年提出的,目的是提供 Internet 上的安全通信服务。安全套接层技术支持 DES、RC2 和 RC4 等加密算法。虽然安全套接层安全服务比较强大,但由于加密技术一是国家控制的技术,安全套接层加密技术的出口自然受到美国国家安全局的限制。目前美国可以使用 128 位的安全套接层技术,但出口的算法的密钥一般只能达到 40 位,它的安全性显然比 128 位的密钥算法差得多。好在近来美国对这方面的限制有所放松,允许出口较尖端的技术应用于银行系统。这对于整个世界银行系统的安全性是很有好处的。但就我国而言,开发自己的高强度加密技术还是很有必要的,因为只有把加密技术牢牢地把握在自己手中,才能够比较主动地把握各类信息的安全性。

5.3.2　防火墙技术

1. 基本概念

防火墙(firewall)原是汽车上的一个装置,它用来隔离引擎和乘客,在引擎爆炸时可以保护乘客的安全。在计算机界,防火墙是指一种逻辑装置,用来保护内部的网络不受来自