第三章电子商务安全技术

3.1电子商务安全要求

3.1.1 电子商务所面临的安全问题

电子商务的安全隐患可分为如下几类:

（1）信息的截获和窃取。

（2）信息的篡改。

（3）信息的假冒。

（4）交易抵赖。

3.1.2 电子商务安全需求

（1）机密性。

（2）完整性。

（3）认证性。

（4）不可抵赖性。

（5）有效性。

3.1.3 电子商务安全内容

电子商务安全从整体上可分为两大部分：计算机网络安全和商务交易安全。

计算机网络安全的内容包括：计算机网络设备安全、计算机网络系统安全、数据库安全等。其特征是针对计算机网络本身可能存在的安全问题，实施网络安全增强方案，以保证计算机网络自身的安全性为目标。

商务交易安全则紧紧围绕传统商务在互联网络上应用时产生的各种安全问题，在计算机网络安全的基础上，如何保障电子商务过程的顺利进行。即实现电子商务的保密性、完整性、可鉴别性、不可伪造性和不可抵赖性。

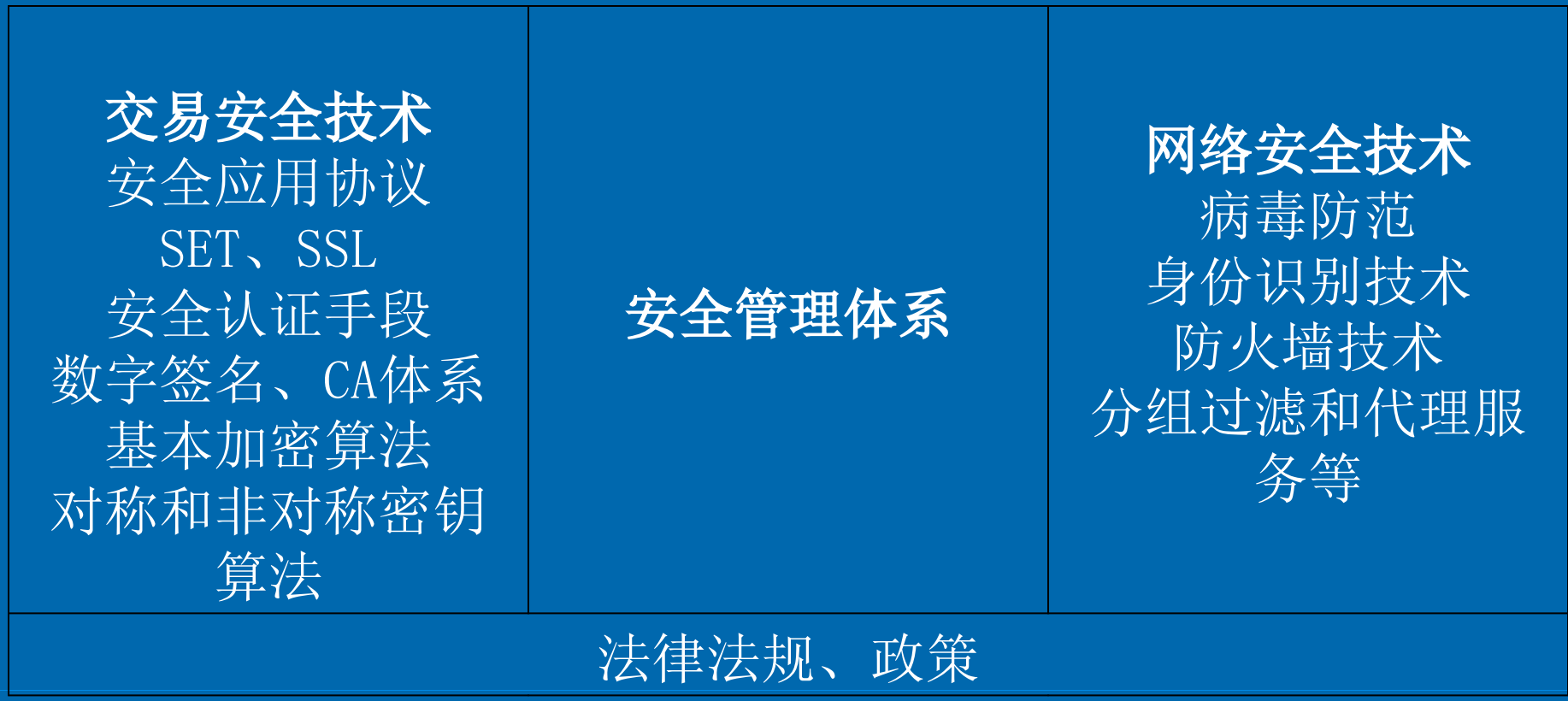

图3.1电子商务安全构架

3.2 计算机网络安全技术

3.2.1 计算机网络的潜在安全隐患

电子商务的网络环境包括Intarnet、Extranet和Internet三种结构组成的网络环境。

企业内部计算机系统面临的风险典型的有：

- 没有好的备份系统导致数据丢失；
- 有外来磁盘携带的病毒攻击计算机系统；
- 业务人员的误操作；
- 删除了不该删除的数据，且无法恢复；
- 系统硬件、通信网络或软件本身出故障；
- 意外事故对系统的破坏；
- 人为蓄意破坏

如果企业的内部网连接上Internet，则Internet本身的不安全性对企业内部的信息系统带来的潜在风险主要有：

- 外部非法用户潜入系统胡作非为，甚至破坏系统；
- 数据丢失，机密信息泄漏；
- 互联网本身固有的风险的影响；
- 网络病毒的攻击

从纯技术角度上来看，存在着五个方面的薄弱性。

- 缺乏安全防护设备（没有安装防火墙）；
- 不足的安全配置与管理系统；
- 通信协议上的基本安全问题；
- 基于WWW、FTP上的应用软件问题；
- 不完善的服务程序。

3.2.2 计算机网络安全体系

一个全方位的计算机网络安全体系结构包括网络的物理安全、访问控制安全、系统安全、用户安全、信息加密、安全传输和管理安全等在实施网络安全防范措施时要考虑以下几点：

- 要加强主机本身的安全，做好安全配置，及时安装安全补丁程序，减少漏洞；
- 要用各种系统漏洞检测软件定期对网络系统进行扫描分析，找出可能存在的安全隐患，并及时加以修补；
- 从路由器到用户各级建立完善的访问控制措施，安装防火墙，加强授权管理和认证；
- 利用RAID5等数据存储技术加强数据备份和恢复措施；
- 对敏感的设备和数据要建立必要的物理或逻辑隔离措施；

•对在公共网络上传输的敏感信息要进行数据加密；
•安装防病毒软件，加强内部网的整体防病毒措施；
•建立详细的安全审计日志，以便检测并跟踪入侵攻击等。

3.2.3 常用的计算机网络安全技术

目前,常用的计算机网络安全技术主要有病毒防范技术、身份认证技术、防火墙技术和虚拟专用网VPN技术等。

1.病毒防范技术

为了防范病毒,可以采用以下措施:

（1）安装防病毒软件，加强内部网的整体防病毒措施；

（2）加强数据备份和恢复措施；

（3）对敏感的设备和数据要建立必要的物理或逻辑隔离措施等。

2.身份识别技术

身份识别技术是计算机网络安全技术的重要组成部分之一。它的目的是证实被认证对象是否属实和是否有效。其基本思想是通过验证被认证对象的属性来达到确认被认证对象是否真实有效的目的。被认证对象的属性可以是口令、问题解答或者像指纹、声音等生理特征，常用的身份认证技术有口令、标记法和生物特征法。

（1）口令

传统的认证技术主要采用基于口令的认证方法。当被认证对象要求访问提供服务的系统时，提供服务的认证方要求被认证对象的口令，认证方收到口令后，将其与系统中存储的用户口令进行比较，以确认被认证对象是否为合法访问者。

（2）标记方法

标记是个人持有物，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，所以智能卡取代磁卡是很必要的。智能卡的原理是在卡内安装电脑芯片以取代原来的磁介质，这样就克服了磁介质的缺陷，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。

（3）生物特征法

生物特征法是基于物理特征或行为特征自动识别人员的一种方法，其优点是严格依据人的物理特征并且不依赖任何能被拷贝的文件或可被破解的口令，所以它是数字证书或智能卡未来的选择。

3.防火墙技术

（1）基本概念

防火墙是一种将内部网和公众网如Internet分开的方法。它能限制被保护的网络与互联网络之间，或者与其他网络之间进行的信息存取、传递操作。防火墙可以作为不同网络或网络安全域之间信息的出入口，能根据企业的安全策略控制出入网络的信息流，且本身具有较强的抗攻击能力。它是提供信息安全服务，实现网络和信息安全的基础设施。

防火墙是在内部网与外部网之间实施安全防范的系统，可被认为是一种访问控制机制基于两种准则进行设计；

一切未被允许的就是禁止的。基于该准则，防火墙应封锁所有信息流，然后对希望提供的服务逐项开放。这种方法可以创造十分安全的环境，但用户使用的方便性、服务范围受到限制。

一切未被禁止的就是允许的。基于该准则，防火墙转发所有信息流，然后逐项屏蔽有害的服务。这种方法构成了更为灵活的应用环境，可为用户提供更多的服务。但在日益增多的网络服务面前，网管人员的疲于奔命可能很难提供可靠的安全保护。

（2）防火墙的功能

•保护数据的完整性。可依靠设定用户的权限和文件保护来控制用户访问敏感性信息，可以限制一个特定用户能够访问信息的数量和种类；

•保护网络的有效性。有效性是指一个合法用户如何快速、简便地访问网络的资源；

•保护数据的机密性。加密敏感数据。

利用防火墙可以提供安全决策的集中控制点，使所有进出网络的信息都通过这个惟一的检查点，形成信息进出网络的一道关口；可以针对不同的用户对网络的不同需求，强制实施复杂的安全策略，起到“交通警察”的作用；可以对用户的操作和信息进行记录和审计，分析网络侵袭和攻击，并及时发出报警信息；可以防止机密信息的扩散以及信息间谍的潜入，可保护内部网络敏感资源和重要的个人信息；可以减少网络的脆弱性。但是防火墙也有一些缺点，它不能防止来自内部变节者（恶意的知情者）和不经心的用户带来的威胁；无法防范通过防火墙之外的其他途径的攻击；不能防止传送已感染病毒的软件或文件所带来的病毒；无法防止数据驱动型的攻击，数据驱动型的数据从表面上看是无害的数据被邮寄到或拷贝到Internet主机上，但一旦执行就开始攻击。

（3）防火墙的实现技术

防火墙系统的实现技术主要分为分组过滤（Packet Filer）和代理服务（Proxy service）两种。

分组过滤技术是一种简单、有效的安全控制技术，它通过在网络间相互连接的设备上加载允许、禁止来自某些特定的源地址、目的地址、TCP端口号等规则，对通过设备的数据包进行检查，限制数据包进出内部网络。分组过滤技术的最大优点是对用户透明，传输性能高。但由于安全控制层次在网络层、传输层，安全控制的力度也只限于源地址、目的地址和端口号，因而只能进行较为初步的安全控制，对于恶意的拥塞攻击、内存覆盖攻击或病毒等高层次的攻击手段，则无能为力。

代理服务是运行于内部网络与外部网络之间的主机之上的一种应用。当用户需要访问代理服务器另一侧主机时，对符合安全规则的连接，代理服务器会代替主机响应，并重新向主机发出一个相同的请求。当此连接请求等到回应并建立起连接之后，内部主机同外部主机之间的通信将通过代理程序将相应连接映射来实现。对于用户而言，似乎是直接与外部网络相连的，代理服务器对用户透明。由于代理机制完全阻断了内部网络与外部网络的直接联系，保证了内部网络拓扑结构等重要信息被限制在代理网关内侧，不会外泄，从而减少了黑客攻击时所需的必要信息。同时，内部网络到外部的服务连接也可以受到监控，代理服务程序可以将所有通过它的连接作出日志记录，以便对安全漏洞检查和收集相关的信息。

代理服务器的应用也受到诸多限制。首先是当一项新的应用加入时，如果代理服务程序不予支持，则此应用不能使用。其次，它只能抵御经由防火墙的攻击，不能防止内部应用软件所携带的数据和病毒或其他方式的袭击，也不能对内部计算机系统未授权的物理袭击提供安全保证。

4.虚拟专用网技术（Virtual Private Network，VPN）

虚拟专用网是用于Internet电子交易的一种专用网络，它可以在两个系统之间建立安全的通道，非常适合电子数据交换（EDI）。在虚拟专用网中交易双方比较熟悉，而且彼此之间的数据通信量很大。只要交易双方取得一致，在虚拟专用网中就可以使用比较复杂的专用加密和认证技术，这样就可以大大提高电子商务的安全性。VPN可以支持数据、语音及图像业务，其优点是经济、便于管理、方便快捷地适应变化，但也存在安全性低，容易受到攻击等问题。

3.3交易安全技术

3.3.1加密技术

1.对称密钥加密体制

2.非对称密钥加密体制

3.3.2 认证技术

1.常用的安全认证技术

(1)数字摘要

(2)数字信封

(3)数字签名

(4)数字时间戳

(5)数字证书

2.安全认证机构

3.3.3安全认证协议

1.安全套接层SSL协议

2.安全电子交易SET协议

3.3.4公钥基础设施

3.3.1加密技术

采用加密技术对信息进行加密,是最常见的安全手段。加密技术是一种主动的信息安全防范措施，其原理是利用一定的加密算法，将明文转换成为无意义的密文，阻止非法用户理解原始数据，从而确保数据的保密性。明文变成密文的过程称为加密，由密文还原为明文的过程称为解密，加密和解密的规则称为算法。在加密和解密的过程中，由加密者和解密者使用的加解密可变参数叫做密钥。

目前，在电子商务中，获得广泛应用的两种加密技术是对称密钥加密体制（私钥加密体制）和非对称密钥加密体制（公钥加密体制）。它们的主要区别在于所使用的加密和解密的密码是否相同。

1.对称密钥加密体制

对称密钥加密，又称私钥加密，即信息的发送方和接收方用一个密钥去加密加密和解密数据。对称加密技术的最大优势是加/解密速度快，适合于对大数据量进行加密，但密钥管理困难。

对称加密比较典型的算法有DES（数据加密标准)算法及其变形Triple DES(三重DES），GDES（广义DES）；欧洲的IDEA；日本的FEALN、RC5等。DES标准由美国国家标准局提出，主要应用于银行业的电子资金转账（EFT）领域。

2.非对称密钥加密体制

非对称密钥加密系统，又称公钥密钥加密，它需要使用一对密钥来分别完成加密和解密操作，一个公开发布，称为公开密钥（Public-Key)；另一个由用户自己秘密保存，称为私有密钥（Private-Key）。信息发送者用公开密钥去加密，而信息接收者则用私有密钥去解密。公钥机制灵活，但加密和解密速度却比对称密钥加密慢得多。

在非对称加密体系中，密钥被分解为一对（即一把公开密钥或加密密钥和一把专用密钥或解密密钥）。这对密钥中的任何一把都可作为公开密钥（加密密钥）通过非保密方式向他人公开，而另一把则作为专用密钥（解密密钥）加以保存。

非对称加密算法的关键是寻找对应的公钥和私钥，并运用某种数学方法使得加密过程是一个不可逆过程，即用公钥加密的信息只能是用与该公钥配对的私有密钥才能解密，反之亦然。常用的算法有RSA、ElGamal等。

特性	对称	非对称
密钥的数目	单一密钥	密钥是成对的
密钥种类	密钥是秘密的	一个私有、一个公开
密钥管理	简单不好管理	需要数字证书及可靠第三者
相对速度	非常快	慢
用途	用来做大量资料的加密	用来做加密小文件或对信息签字等不太严格保密的应用

表4.1 对称与非对称加密体制对比

为了充分利用公钥密码和私钥密码算法的优点，克服其缺点，解决每次传送更换密钥的问题，提出混合密码系统，即所谓的电子信封（envelope)技术。发送者自动生成对称密钥，用对称密钥加密发送的信息，将生成的密文连同用接收方的公钥加密后的对称密钥一起传送出去。收信者用其秘密密钥解密被加密的密钥来得到对称密钥，并用它来解密密文。这样保证每次传送都可由发送方选定不同密钥进行，更好地保证了数据通信的安全性。