肖和阳　卢嫣　编著

电子商务安全技术

DIANZI SHANGWU ANQUAN JISHU

国防科技大学出版社

电子商务安全技术

肖和阳　卢　嫣　编著

国防科技大学出版社
·长沙·

内 容 简 介

本书主要是围绕保障电子商务活动的安全性进行展开，这些保障措施包括网络安全技术、信息加密技术和电子支付安全技术。

本书适合作高等院校电子商务本专科专业学生、MBA 专业学生、经济管理类专业硕士生及本科高年级学生的教材；也适合企业各部门管理人员、信息技术人员使用；还可作为相应层次电子商务培训班的教材。

图书在版编目(CIP)数据

电子商务安全技术/肖和阳，卢嫣编著．—长沙：国防科技大学版社，2005.3
ISBN 7-81099-163-9

Ⅰ．电… Ⅱ．①肖…②卢… Ⅲ．电子商务—安全技术 Ⅳ．F713.36

中国版本图书馆 CIP 数据核字(2005)第 011068 号

国防科技大学出版社出版发行
电话：(0731)4572640 邮政编码：410073
E-mail：gfkdcbs@public.cs.hn.cn
责任编辑：唐卫葳 责任校对：徐 飞
新华书店总店北京发行所经销
长沙精美彩色印刷厂印装
*
开本：787×1092 1/16 印张：15.5 字数：368 千
2005 年 3 月第 1 版第 1 次印刷 印数：1-2000 册
ISBN 7-81099-163-9/F·16
定价：22.00 元

前 言

电子商务是基于计算机、软件以及通信网络基础上的经济活动。它以Internet作为通信手段，使得人们可以在计算机信息网络上建立自己企业的形象，宣传自己的产品和服务，同时可以进行电子交易和资金结算。电子商务的实际应用时间并不长，但以其高效率、低支付、高收益和全球性的特点，很快得到企业和政府的重视，发展十分迅速。我国加入WTO后，电子商务在我国的应用将会更加快速地发展，以便与世界贸易接轨。因此，电子商务的发展前景极其诱人。

然而，事物的发展都存在其两面性，电子商务一方面给我们带来便利，但同时也有一部分人利用网络和协议的一些缺陷进行各种犯罪活动。我们知道，电子商务是基于计算机互联网的交易行为，网络必须保证大量的经济信息能够安全地在网上传送，资金能够安全地在网上划拨。但是，由于Internet是一个开放的系统，网上传送的信息可能被破坏、被窃听或被篡改，甚至交易一方可能事后反悔，不承认签订的电子合同。因此，我们必须保证信息的传送是安全的，信息本身是安全的，网上交易是安全的。

本书主要围绕保障电子商务活动的安全性进行展开，这些保障措施包括网络安全技术、信息加密技术和电子支付安全技术。全书共分为九章，第一章电子商务安全性概述，第二章密码学基础，第三章电子商务的认证，第四章安全套接层(SSL)协议，第五章SET协议及其安全性分析，第六章常见的电子商务网络攻击与防范技术，第七章端口扫描技术，第八章安全电子支付，第九章常见的安全电子商务系统。

各章内容简介如下：第一章是电子商务安全性概述，主要介绍了电子商务安全威胁、电子商务安全体系结构；第二章密码学基础，主要介绍了古典密码学、对称加密模型、非对称密钥密码系统、数字签名；第三章电子商务的认证，主要介绍了身份证明与认证体系、证书与认证机构、公开密钥基础设施PKI、北京认证中心；第四章主要介绍了安全套接层(SSL)协议、规范及相关技术；第

五章介绍了 SET 协议的由来、SET 协议、一个基于 SET 的交易、SET 协议的安全性分析、SSL 协议与 SET 协议的比较；第六章常见的电子商务网络攻击与防范技术，主要介绍了黑客、特洛伊木马、虚拟专用网 VPN 技术、防火墙技术；第七章端口扫描技术，主要介绍了扫描器的基本概念、流光扫描器；第八章安全电子支付，主要介绍了电子支票、微机支付系统机制、第九章主要介绍了常见的安全电子商务系统、网站安全策略、网上商城、安全网络银行系统。

本书由肖和阳主编，第 1、3、6 章由肖和阳和卢嫣共同编写，第 2、4、5、7 章由肖和阳编写，第 8、9 章由卢嫣编写。

本书适合于电子商务专业和计算机专业的高年级学生使用，同时也适用于网络工程师、网络管理人员以及对计算机网络安全技术感兴趣的广大网络爱好者。

由于电子商务技术和应用涉及的范围广、内容多、技术更新快，加之编者学识、资料和编写时间所限，书中肯定存在疏漏和不妥之处，敬请广大读者和专家批评指正。

编　者

2004 年 12 月 26 日于湖南涉外经济学院

目　录

第一章　电子商务安全性概述

随着互联网的发展，电子商务已经逐渐成为人们进行商务活动的新模式，越来越多的人通过互联网进行商务活动。电子商务的发展前景十分诱人，而其安全问题也变得越来越突出，如何建立一个安全、便捷的电子商务应用环境，对信息提供足够的保护，已经成为商家和用户都十分关心的话题。

从整体上来讲，电子商务的活动大致包括以下三个方面：

(1) 电子商务信息必须通过计算机网络进行传输；

(2) 在网络上传输的信息需要进行加密；

(3) 进行商务活动的双方必须得到某种身份认证，以保证交易的安全性。

1.1　电子商务安全问题的引出

电子商务的安全性体现在网络安全、信息加密技术以及交易的安全上，电子商务交易安全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，保障电子商务过程的顺利进行。计算机网络安全与商务交易安全实际上是密不可分的，两者相辅相成，缺一不可。没有计算机网络安全作为基础，商务交易安全就犹如空中楼阁，无从谈起；没有商务交易安全保障，即使计算机网络本身再安全，仍然无法达到电子商务所特有的安全要求。

随着电子商务在全球范围内的迅猛发展，电子商务中的网络安全问题日渐突出。根据中国互联网络信息中心(CNNIC)发布的"中国互联网络发展状况统计报告(2000/1)"，在电子商务方面，52.26%的用户最关心的是交易的安全可靠性。由此可见，电子商务中的网络安全问题是实现电子商务的关键之所在。

1983 年 10 月 24 日，美国著名的计算机安全专家、AT&T 贝尔实验室的计算机科学家 Rober Morris 在美国众议院科学技术会议运输、航空、材料专业委员会上作了关于计算机安全重要性的报告。从此，计算机安全成了国际上研究的热点。随着互联网络技术的发展，网络安全成了新的安全研究热点。网络安全就是如何保证网络上存储和传输的信息的安全性。

由于在互联网设计之初，只考虑其方便性、开放性，使得互联网络非常脆弱，极易受到黑客的攻击或有组织的群体的入侵，也会由于系统内部人员的不规范使用或不满雇员的恶意破坏，使得网络信息系统遭到破坏，信息泄露。

1.1.1 电子商务安全威胁类别

目前,从技术方面,一般的电子商务系统都面临着以下几种安全隐患:

1. 信息的截获和窃取

如果没有采用加密措施或加密强度不够,攻击者可能通过互联网、公共电话网、搭线、电磁波辐射范围内安装截收装置或在数据包通过的网关和路由器上截获数据等方式,获取输出的机密信息,或通过对信息流量、流向、通信频度和长度等参数的分析,推导出有用信息,如消费者的银行账号、密码等。

2. 信息的篡改

当攻击者熟悉了网络信息格式以后,通过各种方法和手段对网络传输的信息进行修改,并发往目的地,从而破坏信息的完整性。这种破坏手段主要有以下三个方面:

- 插入。在信息中插入一些内容,使得接收方读不懂或接收错误的信息。
- 篡改。改变信息流的次序,更改信息的内容,如更改资金划拨方向等。
- 删除。删除某个消息或消息的某些部分。

3. 信息的假冒

当攻击者掌握了网络信息数据规律或解密了商务信息以后,可以假冒合法用户或发送假冒信息来欺骗其他用户,主要有以下两种方式:

- 伪造电子邮件。虚开网站或电子商店,给网上用户发电子邮件,收定货单;伪造大量用户,发电子邮件,穷尽商家服务器的资源,使合法用户不能正常访问网络资源,使有严格时间要求的服务不能及时得到响应等。
- 假冒他人身份。如冒充领导发布指示、调阅机密文件;冒充他人消费、栽赃;冒充主机欺骗合法主机及合法用户;冒充网络控制程序,套取或修改使用权限、保密字、密钥等信息;接管合法用户,欺骗系统,占用合法用户的资源。

4. 交易抵赖

交易抵赖包括多个方面,如发信者事后否认曾经发送过某条信息或内容;收信者事后否认曾经收到过某条消息或内容,商家卖出的商品因价格差异而不承认原有的交易。在现实生活中经常发生的恶意抵赖同样会在网络上发生。

因此,在电子商务活动中,必须采取多种措施,保证电子商务的有效性、保密性、完整性、可鉴别性、不可伪造性和不可否认性。这些也是电子商务的安全要素。

从电子商务交易各方来划分,可分为对商家和消费者的威胁:

1. 对商家的威胁

电子商务中安全性差,可能对商家产生巨大的威胁,如中央系统安全性被破坏,入侵者假冒成合法用户来改变用户数据(如商品送达地址)、解除用户定单或生成虚假定单;竞争者检索商品递送状况,不诚实的竞争者以他人的名义来订购商品,从而了解有关商品的递送状况和货物的库存情况;客户资料被竞争者获悉;被他人假冒而损害公司的信誉;不诚实的人建立与销售者服务器名字相同的另一个 WWW 服务器来假冒销售者;消费者提交定单后不付款;虚假定单;获取他人的机密数据,当某人想要了解另一个人在销售商处

的信誉时，他以另一人的名字向销售商订购昂贵的端口，然后观察销售商的行动，假如销售商认可该定单，则说明被观察者的信誉高，否则，则说明被观察者的信誉不高。

2. 对消费者的威胁

入侵者可以通过多种方式和手段来构成对消费者的威胁。如虚假定单，一个假冒者可能会以客户的名字来订购商品，而且有可能收到商品，而此时客户却被要求付款或返还商品；付款后不能收到商品，在要求客户付款后，销售商中的内部人员不将定单和钱转发给执行部门，因而使客户不能收到商品；机密丧失，客户有可能将秘密的个人数据或自己的身份数据（如 PIN、口令等）发送给冒充销售商的机构，这些信息也可能会在传递过程中被窃听；拒绝服务，攻击者可能向销售商的服务器发送大量的虚假定单来穷竭它的资源，从而使用户不能得到正常的服务。

1.1.2　电子商务安全威胁现状

当前电子商务所面临的网络安全现状不容乐观。和那些不从事在线商务的公司比起来，从事电子商务的公司网站遭遇黑客非法入侵的可能性要高出 57%。而据国内的统计资料显示，约有 64%的公司信息系统受到黑客的危害性攻击，其中金融业占总数的 57%。

从 2000 年 2 月 7 日至 2 月 9 日，短短 3 天时间内，美国几大主要网上站点遭受不明身份黑客地攻击，其中包括著名的电子商务网站 eBay 和 Amazon。在黑客开始所谓“拒绝服务”（Denial of Service）式的攻击后，亚马逊（Amazon）站点容纳顾客的能力急剧下降。数分钟后访客数量只有平时同一时段访客数量的 1.5%，大约一小时后亚马逊网站才恢复正常。Buy.com 的一台服务器在两三个小时内速度减慢，而 E-TRADE 则瘫痪了 3 个小时。据统计，3 天来黑客袭击各大网站所造成的直接或间接的经济损失高达数十亿美元。

在计算机犯罪和网络侵权方面，无论是数量、手段，还是性质、规模，已经到了令人咋舌的地步。据有关方面统计，目前美国每年由于网络安全问题而遭受的经济损失超过 170 亿美元，德国、英国也均在数十亿美元以上，法国为 100 亿法郎，日本、新加坡问题也很严重。在国际刑法界列举的现代社会新型犯罪排行榜上，计算机犯罪已名列榜首。2003 年，CSI/FBI 调查所接触的 524 个组织中，有 56%的客户遇到过电脑安全事件，其中 38%遇到 1～5 起、16%以上遇到 11 起以上。因与互联网连接而成为频繁攻击点的组织连续 3 年不断增加；遭受拒绝服务攻击（DoS）的网站则从 2000 年的 27%上升到 2003 年的 42%。调查显示，521 个接受调查的组织中 96%有网站，其中 30%提供电子商务服务，这些网站在 2003 年一年中有 20%发现未经许可入侵或误用网站的现象。更令人不安的是，有 33%的组织说他们不知道自己的网站是否受到过损害。据统计，全球平均每 20 秒就发生 1 次网上入侵事件，黑客一旦找到系统的薄弱环节，所有用户均会遭殃。

最近，美国赛门铁克计算机安全公司发布了半年一次的“互联网安全威胁报告”，全面回顾了互联网安全领域存在的主要问题。在全球范围内，管理型服务威胁以及间谍软件引起了赛门铁克的高度关注。

赛门铁克指出，在全球 180 个国家和地区有两万台服务监视器和公司从运行反间谍软件的 1.2 亿个客户、服务器和网关上收集恶意代码数据。在报告中，赛门铁克指出互联

网主要有下列五类威胁：

一是 Windows 漏洞的修补很不完善。赛门铁克称，在过去六个月中，宣布漏洞和出现相关攻击代码的平均时间为 5.8 天。攻击代码能大面积地搜寻漏洞并迅速地利用漏洞。比如，Witty 蠕虫出现在漏洞发现后的两天内。

二是远程控制网络的现象快速增加，这从 2003 年底的 2000 台电脑猛增到 2004 年 6 月的 3 万台。通过对目标电脑的非授权远程控制，不法分子可以发动拒绝服务攻击。赛门铁克公司称，远程网络控制和漏洞结合使用造成了极为严重的威胁。一旦发现漏洞，用户应及时进行网络升级，这样就可以找到补救的办法。

三是即使是拥有杰出的 IT 人才、IT 管理财富 100 强公司，也存在蠕虫扩散的威胁。赛门铁克调查发现，财富 100 强公司中大约有 40%的公司控制的 IP 地址会导致蠕虫病毒的攻击。这表明，尽管公司已采取了措施，但他们的系统仍会被蠕虫感染。

四是针对电子商务的攻击行为增长迅速。2003 年，针对电子商务的攻击行为只有 4%，而 2004 年这种攻击行为增长了四倍，达到了 16%。

五是网站应用业务仍很不安全，有价值的机密的人力资料信息、商务服务以及财会应用方面的漏洞很容易导致网站攻击现象的发生，而这种攻击不会危及服务器的安全。赛门铁克估计，2004 年上半年发现的安全漏洞中有 39%和网站应用漏洞相关，有 82%的网站应用漏洞很容易被利用。

对发展中的中国来说，开展电子商务，网络安全和商务安全尤为重要。一方面，国内几乎所有的计算机主机、网络交换机、路由器和网络操作系统都来自国外；另一方面，由于美国政府对计算机和网络安全技术的出口限制，使得进入我国的电子商务和网络安全产品（包括 Web 浏览器、Web 服务器、防火墙和路由器等软硬件）均只能提供较短密钥长度的弱加密算法。

因此，从长远来看，为保证我国电子商务的正常发展，对电子商务中的安全技术进行研究，发展自主的电子商务安全技术是重中之重。

目前，在网络安全问题上还存在不少知识盲区和制约因素。网络是新生事物，许多人一接触就忙着用于学习、工作和娱乐等，对网络信息的安全性无暇顾及，安全意识相当淡薄，对网络信息不安全的事实认识不足。与此同时，网络经营者和机构用户注重的是网络效应，对安全领域的投入和管理远远不能满足安全防范的要求。总体上看，网络信息安全处于被动的封堵漏洞状态，从上到下普遍存在侥幸心理，没有形成主动防范、积极应对的全民意识，更无法从根本上提高网络监测、防护、响应、恢复和抗击能力。近年来，国家和各级职能部门在信息安全方面已做了大量努力，但就范围、影响和效果来讲，迄今所采取的信息安全保护措施和有关计划还不能从根本上解决目前的被动局面，整个信息安全系统在迅速反应、快速行动和预警防范等主要方面，缺少方向感、敏感度和应对能力。

1.2　电子商务安全体系结构

电子商务是多种技术的集合体，包括获得数据（如共享数据库、电子公告牌），处理数据（如认证、加密）、交换数据（如 EDI、电子邮件）等等。

1.2.1　电子商务体系结构

随着网络技术的发展，真正意义上的、完善的电子商务应可提供网上交易和管理等全过程的服务。概括起来讲，电子商务的服务功能主要体现在如下几个方面：网上广告宣传服务、网上咨询和交易洽谈服务、网上产品订购服务、网上货币支付服务、电子账户管理服务、网上商品传递及查询服务、用户意见征询服务以及交易活动管理服务等。而电子商务的安全性问题不像人们所想象的那样仅限于用户数据库信息管理的安全性和网上货币支付服务的安全性问题，而是贯穿了如图 1－1 所示的电子商务活动的全过程中。

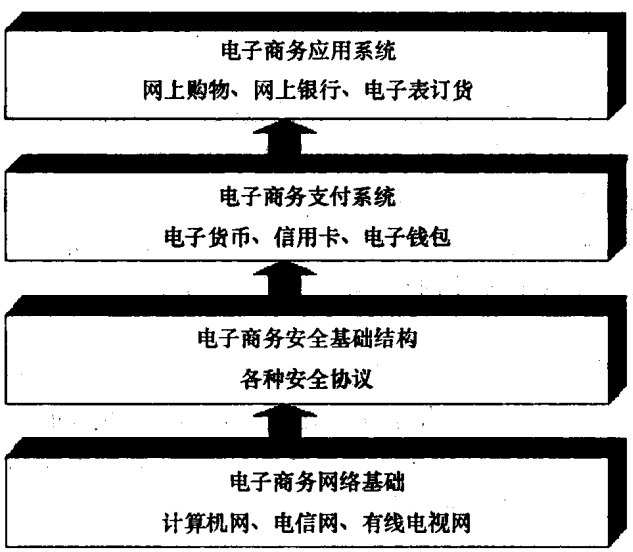

图 1－1　电子商务体系结构示意图

1.2.2　电子商务安全体系结构

电子商务需要一个完整的电子商务技术体系作为基础。概括起来，电子商务的基础结构包括以下四个方面内容：电子商务网络基础、电子商务安全基础结构、电子商务支付系统和电子商务业务系统。电子商务的安全体系结构便是基于以上各层系统建立起来的，电子商务的安全体系结构如图 1－2 所示。

在此安全体系之上可建立电子商务的支付体系和各种业务应用系统，有关基本加密