• 电子商务系列教材 •

电子商务安全

（第二版）

主　编◎张　波　刘　鹤
副主编◎杜　鹏　孟祥瑞

華東理工大學出版社
EAST CHINA UNIVERSITY OF SCIENCE AND TECHNOLOGY PRESS

电子商务系列教材

电子商务安全

（第二版）

张　波　刘　鹤　主　编

杜　鹏　孟祥瑞　副主编

華東理工大學出版社
EAST CHINA UNIVERSITY OF SCIENCE AND TECHNOLOGY PRESS

图书在版编目(CIP)数据

电子商务安全/张波，刘鹤主编. —2 版. —上海：华东理工大学出版社，2009.11
（电子商务系列教材）
ISBN 978-7-5628-2653-8

Ⅰ.电... Ⅱ.①张...②刘... Ⅲ.电子商务—安全技术—高等学校—教材 Ⅳ.F713.36

中国版本图书馆 CIP 数据核字(2009)第 189189 号

电子商务系列教材

电子商务安全(第二版)

.....

主　　编 / 张　波　刘　鹤
责任编辑 / 李国平
责任校对 / 李　晔
封面设计 / 陆丽君
出版发行 / 华东理工大学出版社
社　址：上海市梅陇路 130 号，200237
电　话：(021)64250306(营销部)　(021)64252174(编辑室)
传　真：(021)64252707
网　址：press.ecust.edu.cn
印　　刷 / 常熟华顺印刷有限公司
开　　本 / 787 mm×1092 mm　1/16
印　　张 / 18.75
字　　数 / 449 千字
版　　次 / 2006 年 8 月第 1 版
　　2009 年 11 月第 2 版
印　　次 / 2009 年 11 月第 1 次
印　　数 / 4051—8050 册
书　　号 / ISBN 978-7-5628-2653-8/F·218
定　　价 / 29.00 元

内 容 摘 要

本书共分 10 章，分别介绍了电子商务安全的基础知识、密码技术、密钥管理与数字证书技术、数字签名与身份认证技术、Internet 基础设施安全（如 DNS 安全、IPSec 安全、VPN 安全、E-mail 安全、Web 安全等）、网络安全防护技术、防火墙技术、数据库系统安全技术、计算机病毒及其防治技术等，最后阐述了电子商务安全评估与管理方面的内容。

本书可作为高等院校电子商务专业、信息管理与信息系统专业、管理类专业、计算机类专业等相关本专科专业学生的教材，也可作为电子商务从业人员以及相关从业人员的参考书。

前　言

随着计算机技术、网络技术和通讯技术的飞速发展，基于 Internet 的电子商务越来越受到社会各行各业的高度重视，成为越来越多的人们关注的焦点。但是，在电子商务的具体实施过程中，安全问题却始终是制约或阻碍进一步推进电子商务的瓶颈之一。开展电子商务（如网上支付）活动时，在 Internet 上需要传输消费者和商家的一些机密信息，如消费者信用卡信息、商家的客户信息和订购信息等，而这些信息一直是网络非法入侵者或黑客的攻击目标。如何保证电子商务安全、保证数据的完整性和交易的可靠性、不可否认性等，已经成为电子商务发展必须要解决的关键问题，对这些问题的担心也是导致很多消费者不愿意进行网上购物或网上支付的最主要原因。

各种网络安全事故和故障的发生，使越来越多的人特别是专家们意识到，人们普遍对电子商务安全意识的淡薄和安全人才的缺乏是网络出现安全漏洞的一个非常重要的原因。因此，出现了一批与电子商务安全相关的新兴职业，如电子保安、电子商务律师、电子商务司法人员、电子商务法官、电子商务安全警察、电子商务安全员、电子商务安全策划等等。勿庸置疑，电子商务安全知识及其应用技术已经成为电子商务从业人员必须了解和具备的重要知识与能力，也成为众多学者、研究开发人员、政府人员和管理人员关注的目标。

保障电子商务安全是实施电子商务的关键环节，在推进电子商务进一步发展的过程中起着举足轻重、不可低估的作用。电子商务的安全问题是一个庞大的系统性工程，必须在具体实施过程中采取综合防范的思路，从技术、管理、政策、法律法规等诸多方面提供一套完备的安全解决方案，如此才能为交易和支付活动提供富有保障的商务安全环境。

本着普及电子商务安全知识及其应用技术，推进我国电子商务的发展，增进与国内外同行之间交流的目的，以及为高等院校电子商务及其相关专业提供一本适用教材或参考书籍，或者为相关的社会从业人员提供一本自学自习的参考用书的想法，我们编写了这本书，希望我们对电子商务安全问题的探讨能对我国电子商务的发展起到一定的作用，并为我国电子商务人才的培养贡献一点绵薄之力。

本书最大的特点在于立足电子商务的安全问题，系统全面地阐述了电子商务方方面面的安全知识和应用技术，使读者对电子商务安全有一个完整性的认识。本书系统性强、内容新颖、实用性和可操作性强、图例丰富，对于复杂的概念、过程、原理等都配有图解，非常便于讲解和自学。此外，每章结尾都配有思考题，便于教学和启发思维。

本书由张波(安徽理工大学),刘鹤(四川师范大学文理学院)主编;杜鹏(华中师范大学汉口分校),孟祥瑞(安徽理工大学)副主编。张波编写了第1章,第2章,第7章,第8章;刘鹤,张波编写了第3章,第4章;杜鹏,张波编写了第5章,第6章;陈洋(江苏大学)编写了第9章,第10章。雷轶、程元栋、沈长霞、曹营、李铁锋、杨忠连等也参与了本书的部分编写或对编写提供了帮助。

本书在编写过程中,参考了大量国内外相关的书籍、杂志和资料。正是这些书籍、杂志和资料的作者的智慧结晶使我们深受启发,才能最终完成本书的编写工作,在此,我们谨向这些作者表示诚挚的谢意!

本书内容涉及面较广,但因编者水平有限和篇幅的限制,许多相关知识和技术未能介绍或介绍得不够全面,疏漏之处在所难免,恳请读者批评指正。作者编有本书的电子课件,有需求者请联系。E-mail: gpli@ecust.edu.cn.

编　者

2009.8

目　录

第1章　电子商务安全概述

电子商务(Electronic Commerce)是指政府、企业和个人利用现代电子计算机与网络技术来实现商业交换和行政管理的全过程;它是一种基于互联网,以交易双方为主体,以银行电子支付结算为手段,以客户数据为依托的全新商务模式。电子商务的参与者包括企业、消费者和中介机构等。它的本质是建立一种全社会的"网络计算环境"或"数字化神经系统",以实现资源在国民经济和大众生活中的全方位应用。

随着 Internet 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 Internet 进行商务活动。电子商务的发展给人们的工作和生活带来了新的尝试和便利,前景十分诱人,也为人们带来了无限商机。但许多商业机构对是否采用电子商务仍持观望态度,主要原因是对网上运作的安全问题存有疑虑。在竞争激烈的市场环境下,电子商务的一些信息可能属于商业机密。一旦信息失窃,企业的损失将不可估量。因此,在运用电子商务模式进行贸易的过程中,安全问题就成为电子商务最核心的问题,也是电子商务得以顺利推行的保障。它包括有效保障通信网络,信息系统的安全,确保信息的真实性、保密性、完整性、不可否认性和不可更改性等。

本章主要介绍电子商务安全概念的核心内涵,以及当前电子商务的安全环境,即面临的威胁、安全要素、安全技术、安全体系结构和安全相关标准等。

1.1　电子商务安全概况

近年来,网络技术和电子商务迅猛发展,人们的网络活动剧增,网络安全问题也因此成为人们一直关注的话题。电子商务安全的重要性已不言而喻。尽管政府以及一些企业已意识到这个问题,但因为一直缺乏一个安全保护的完整概念,所以很多人在安全认知上仅限于对防火墙的了解,而防火墙只是安全保护的一个方面,绝不等于全部,这也正是实施了防火墙的网络仍有漏洞的原因所在。

2000 年 2 月 7—9 日这三天,美国许多著名的网站先后遭到互联网历史上最严重的计算机黑客攻击,在美国社会引起了强烈震动。

黑客 3 天来的袭击,造成的直接和间接经济损失达 10 亿美元。2 月 7 日,除了免费电子邮件等三个站点未受影响外,雅虎的大部分网络服务陷于瘫痪。雅虎是当时全球第二大搜索引擎网站,每天被浏览页次达 465 亿次,其股市价值达 930 亿美元。8 日上午,先是当天股市的网络销售公司的购买网站死机,再是网上电子拍卖网站电子港湾、网上书店及商品销售的亚马逊网站告急。电子港湾的注册用户达 1 000 万,是每月浏览达 15 亿次的网上拍

卖网站。8 日下午商品买卖一度被停止数小时。当晚，美国有线电视新闻网宣布，其网站因负荷超载，从下午 7 时至 8 时 45 分信息传送被阻断。2 月 9 日，电子商务网站再度遭殃，电子交易网站在股市开市前遭到持续 1 小时的攻击，信息技术公司的科技新闻网站 ZDNet 约有 70%的内容被中断 2 小时，上网者无法接触到包括网站新闻和产品浏览等内容的信息。

美国联邦计算机案件处理中心主任大卫·加诺说："全美至少有数百台计算机受到袭击。所幸的是，黑客并未进入这些网络内部窃取业务和客户资料。如此众多的大型网站，特别是新兴的电子商务网站，在短短的 3 天内连续遭到黑客攻击，这在因特网历史上还是第一次。"有关专家称，此事将进一步引起人们对网络安全和电子商务风险的关注。

电子商务的安全问题是一个涉及范围极广的社会问题，希望有越来越多的企业和个人加入到关心电子商务安全的行列中来，一起为创造电子商务安全环境，开创崭新电子商务时代出力献策！

1.1.1 电子商务安全概念与特点

电子商务的一个重要技术特征是利用 IT 技术来传输和处理商业信息，因此，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为目标。

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，保障电子交易和电子支付等电子商务的顺利进行，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等。

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。

电子商务安全以网络安全为基础，但是，电子商务安全与网络安全又是有区别的。首先，网络不可能绝对安全，在这种情况下，还需要运行安全的电子商务；其次，即使网络绝对安全，也不能保障电子商务的安全。电子商务安全除了基础要求之外，还有特殊要求。

从安全等级来说，从下至上有计算机密码安全、局域网安全、互联网安全和信息安全之分，而电子商务安全属于信息安全的范畴，涉及信息的机密性、完整性、认证性等方面。这几个安全概念之间的关系如图 1-1 所示。同时，电子商务安全又有它自身的特殊性，即以电子交易安全和电子支付安全为核心，有更复杂的机密性概念和更严格的身份认证功能，对不可拒绝性有新的要求，需要有法律依据性和货币直接流通性特点，还需要网络设有的其他服务（如数字时间戳服务）等。

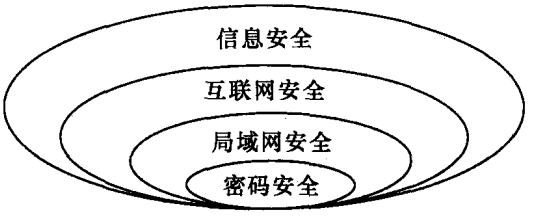

图 1-1 安全概念基本关系示意图

电子商务安全具有如下四大特性。

(1) 电子商务安全是一个系统概念

电子商务安全问题不仅仅是个技术性的问题，更重要的是管理问题，而且它还与社会道德、行业管理以及人们的行为模式等紧密地联系在一起。

(2) 电子商务安全是相对的

就像房子的窗户上只有一块玻璃一样，一般说来是安全的，但是如果用石头去砸，那就不安全了，但我们不会因为石头能砸碎玻璃而去怀疑玻璃的安全性，因为大家都有一个普遍的认识：玻璃是不能砸的，有了窗玻璃就可以保证房子的安全。同样，不能追求一个永远也攻不破的安全系统，安全与管理始终是联系在一起的。也就是说，安全是相对的，而不是绝对的，要想网站永远不受攻击，不出安全问题是不可能的。

(3) 电子商务安全是有代价的

无论是现在国外的 BtoB 还是 BtoC，都要考虑到安全的代价和成本问题。如果只注重速度，就必定要以牺牲安全来作为代价；如果要考虑到安全，速度就得慢一点。当然这与电子商务的具体应用有关，如果不直接牵涉到支付等敏感问题，对安全的要求就可以低一些；如果牵涉到支付问题，对安全的要求就要高一些，所以安全是有成本和代价的。作为一个经营者，应该综合考虑这些因素；作为安全技术的提供者，在研发技术时也要考虑到这些因素。

(4) 电子商务安全是发展的、动态的

今天安全，但明天不一定安全，因为网络的攻防是此消彼长、道高一尺魔高一丈的事情。尤其是安全技术，它的敏感性、竞争性以及对抗性很强，需要不断地检查、评估和调整相应的安全策略。没有一劳永逸的安全，也没有一蹴而就的安全。

1.1.2　电子商务面临的安全威胁

要了解电子商务的安全威胁，需要考察从客户机到电子商务服务器的整个过程。在考察“电子商务链”上每个逻辑链条时，必须包括客户机、在通信信道上传输的消息、万维网(WWW)和电子商务服务器(包括服务器端所有的硬件)等。

1. 对客户机的安全威胁

在实时的、动态的、可交互的 WWW 内容出现前，网页是静态的。静态页面是用 WWW 标准页面描述语言 HTML 编制的，其作用只是显示内容并提供到其他页面的链接。为增加页面的生动性以及客户机与服务器之间的交互能力，同时也为了分担服务器端的负载，动态网页技术得以广泛应用，相应地安全状态也就发生了变化。此外，一些其他的相关技术也成为威胁客户机安全的不确定性因素，如被恶意利用也会招致不良后果。

(1) 动态内容

动态内容是指在页面上嵌入一段对用户透明的程序，它可产生一些动态的效果，例如显示动态图像、下载和播放音乐或实现基于 WWW 的电子表格程序、客户机中的表单数据提交等交互操作。动态内容扩展了 HTML 的功能，使页面更为生动活泼，同时，动态内容还将原来要在服务器上完成的某些辅助性处理任务转给在多数情况下处于闲置状态的客户机来完成，均衡了服务器的负载。

动态内容有多种形式，最著名的动态内容形式包括 JavaScript 和 VBScript、Java

Applet 和 ActiveX 控件等。这些程序经常被企图破坏客户机的人伪装成无害的内容，一旦触发运行，就会对客户机带来安全威胁。这种隐藏在程序或页面里而掩盖其真实目的的程序被统称为特洛伊木马。它可窃听计算机上的保密信息，并将这些信息传给它的远程 WWW 服务器，从而构成保密性侵害。而且，特洛伊木马还可改变或删除客户机上的信息，构成完整性和不可拒绝性侵害。

(2) 相关技术或机制

能够威胁到客户机安全的因素，除了动态内容，还包括其他一些相关技术或机制。这些技术或机制和动态内容相呼应，使得其对客户机的安全威胁势态扩大，或者后果更加严重。

① cookie

cookie 的存在也使得客户机更加容易泄露用户的秘密。通过 WWW 页面潜入的恶意代码可使通常存放在 cookie 里的信用卡号、用户名和口令等敏感信息暴露。cookie 的设计目的是解决需要记忆关于顾客订单信息或用户名与口令等问题。因为因特网是无状态的，它不能记忆从一个页面到另一个页面间的响应。但这也给有些恶意的动态内容提供了可乘之机。

② 邮件通讯簿

使用客户端邮件收发软件的用户通常在电子邮件通讯簿上存放联系人的信息，一些计算机病毒可以成功地检测到这些内容，并把病毒发给这些联系人。

③ 信息隐蔽

一般情况下，计算机文件中都有冗余的或能为其他信息所替代的无关信息。后者一般驻留在背景中，使人无法看到。信息隐蔽是指隐藏在另一段信息中的信息，它提供将加密的文件隐藏在另一个文件中的保护方式，粗心的观察者看不到其中含有的重要信息。

2. 对通信信道的安全威胁

因特网是将客户机和电子商务服务器连接起来的电子通道。安全威胁的第二个环节就是将客户机连到服务器上的传输信道，即因特网。

虽然因特网起源于军事网络，但美国国防部高级研究项目中心建造网络的主要目的不是为了安全传输，而是为防止一个或多个通信线路被切断即提供冗余传输。因特网发展到今天，其不安全状态与最初相比并没有多大改观。在因特网上传输的信息，从起始节点经由若干中间节点到目标节点之间的路径是随机选择的。在同一起始节点和目标节点之间发送信息时，每次所用的路径也都是不同的，所以根本无法控制信息的传输路径，也不知道信息包曾到过哪里，因而无法保证信息传输时所通过的每台计算机都是安全的和无恶意的。如果信息包在传递途中被任意一个中间节点窃取、篡改甚至删除，那么客户所遭受的损失将是无法弥补的。

(1) 搭线窃听

开展电子商务的一个很大的安全威胁就是敏感信息或个人真实信息被窃。在因特网上，有种叫做“嗅探器”的特殊软件能够记录下通过某个网关或路由器的信息。它类似于在电话线上搭线并录下一段对话。嗅探器可以截获并阅读电子邮件信息，也可记录敏感信息或个人真实信息，或者用来攻击相邻的网络，并且能够做到不留痕迹。

(2) IP 欺骗

所谓 IP 欺骗，就是伪装成合法主机的 IP 地址与目标主机建立连接关系。通过这种欺骗方法可以把某个服务器的访问者引到一个虚假网站，或者假冒合法用户主机的名进入目标服务器。

当用户主机与目标服务器之间建立了 TCP 连接后，通过双方信息包的不断交互取得用户主机或服务器的信息。入侵者猜测出信息包的序列号，就能够向用户主机或服务器发出伪造的、看上去是来自合法主机的数据包，构成对完整性的威胁。

此外，用户主机与服务器之间建立网络连接时经常需要某种形式的认证，发生在应用层上的认证是不透明的，如进行 FTP 或 Telnet 连接时需要用户输入密码和账号。IP 地址欺骗可以针对非应用层的、通常是自发的、无需用户参与的认证，从而达到非法入侵的目的。

(3) IP 源端路由选择

IP 数据包在因特网上传输达到最终目的主机之前通常要经过许多路由器。路由器动态决定了 IP 数据包的传输路线。允许源端路由选择就是允许 IP 数据包向经过的路由器声明达到目标主机所希望经过的路由。

入侵者利用 IP 数据包源端路由选择避开那些包含过滤路由器、防火墙以及其他安全检查机制的路由，就可以访问在正常情况下所不能访问的主机。另外，如果目标主机的访问控制机制是认证源主机的 IP 地址，入侵者使用 IP 源端路由选择就可以有效地通过目标主机的认证。

(4) 目标扫描

入侵者在确定扫描目标系统后，利用一些扫描程序和安全分析工具，如 ISS 扫描器、SATAN 等，寻求该系统的安全漏洞或弱点，并试图找到安全性最弱的主机作为入侵的对象。如果目标主机的管理员系统配置不当，或者未能及时发现并更新针对产品或系统安全漏洞的补丁程序，就极易被攻破薄弱主机，继而造成对与本机建立了访问链接和信任关系的其他网络计算机被攻破的连锁反应，最终威胁到整个系统。

3. 对服务器的安全威胁

客户机、因特网和服务器的电子商务链上第三个环节是服务器。企业借助各种服务器软件设置自己的 WWW 服务器、FTP 服务器、E-mail 服务器等。对企图破坏或非法获取信息的人来说，服务器有很多弱点可被利用。攻击的入口有 WWW 服务器及其软件、数据库和数据库服务器以及通用网关接口 CGI(Common Gateway Interface)程序或其他工具程序。

(1) WWW 服务器

WWW 服务器软件是用来响应 HTTP 请求并传送 HTML 格式的页面的，其主要设计目标是支持 WWW 服务和方便使用。通常该类软件比较复杂，包含错误代码的概率也较高，因此含有许多已知的和未知的安全漏洞。这些漏洞经常被攻击者利用，加之系统管理员的一些不当管理行为，极易造成系统的瘫痪或信息的泄露等严重后果。

(2) 数据库服务器

电子商务系统用数据库存储用户数据，并可从 WWW 服务器所连的数据库中检索产品信息。数据库除存储产品信息外，还可能保存有价值的信息或隐私信息，如果这些信息被更改或泄露将会给公司带来无法弥补的损失。

现在多数大型数据库都使用基于用户名和口令的权限安全措施，一旦用户获准访问数据库，就可查看数据库中相关内容。而有些数据库没有以安全方式存储用户名与口令，或没有对数据库进行安全保护，仅仅依赖 WWW 服务器的安全措施。如果有人得到用户的认证信息，他就能伪装成合法的数据库用户来下载保密的信息。

此外，隐藏在数据库系统里的恶意程序可将数据权限降级，把敏感信息发到未保护的区域。这样，所有用户都可访问这些信息，其中当然包括那些潜在的侵入者。

(3) CGI

通用网关接口 CGI 可实现从 WWW 服务器到另一个程序(如数据库程序)的信息传输。CGI 和接收它所传输数据的程序为网页提供了动态内容。同 WWW 服务器一样，CGI 脚本是能以高权限运行的程序，并且运行起来不受 Java 运行程序安全的限制，如果滥用就会带来安全威胁。因此，恶意的 CGI 程序能自由访问系统资源，使系统失效、调用删除文件的系统程序或查看顾客的保密信息。

(4) ASP

活动服务器页面 ASP(Active Server Pages)是微软推出的工具软件，可以在服务器端运行脚本语言 VbScript 和 JavaScript 编写的程序。ASP 简单实用、灵活而强大，可实现与客户端交互信息和数据库访问等操作。但 ASP 也存在安全漏洞，通过 ASP 可以入侵 WWW 服务器，窃取服务器上的文件，捕获 Web 数据库等系统的用户口令，删除服务器上的文件，直到造成系统损坏。

(5) 邮件炸弹

邮件炸弹是将大量的消息发给同一个电子邮件地址，目标电子邮件地址收到的大量邮件超出了所允许的邮件区域限制，导致邮件系统堵塞或失效。邮件炸弹通常会导致邮件服务器拒绝服务。

(6) 溢出攻击

通过客户机传输给 WWW 服务器或直接驻留在服务器上的 Java 或 C++程序需要经常使用缓存。缓存中存放了从文件或数据库中读取的数据，是数据进出的临时存放区域。但是向缓存发送数据的程序如果出错，就会导致数据或指令替代了内存指定区域外的内容，即缓存溢出。缓存溢出的后果就是，程序运行遇到意外然后死机，从而破坏服务器的“不可拒绝性”。因特网蠕虫病毒就是这样的程序，它引起的溢出会消耗掉所有系统资源，直到主机停止运行。

另一种溢出攻击就是将指令写在关键的内存位置上，使侵入的程序在完成了覆盖缓存内容后进入系统保留区。保留区内存储着关键性信息，如 CPU 寄存器的内容和控制权移交前程序的计算状态。当控制权返还给原程序时，保留区的内容就会重新载入 CPU 寄存器，将控制权交给程序的下一条指令。但在攻击发生时，控制权将返还给攻击程序，而不是让出控制权的原程序。WWW 服务器通过载入记录攻击程序地址的内部寄存器来恢复运行。恢复运行的攻击程序将会获得很高的超级用户权限，这就使每个程序都可能被侵入的程序泄密或破坏。

(7) 口令破译

用户所选的口令不当或者攻击者使用一些工具软件，也会构成安全威胁。有的用户所选的口令非常简单或者规律性很强，极易被猜出。再者是有人通过使用字典攻击程序，按电