高等学校计算机科学与技术教材

电子商务安全
(第2版)

COMPUTER Science and Technology

□ 祝凌曦　编著

- 原理与技术的完美结合
- 教学与科研的最新成果
- 语言精练，实例丰富
- 可操作性强，实用性突出

清华大学出版社　●　北京交通大学出版社

高等学校计算机科学与技术教材

电子商务安全

（第2版）

祝凌曦　编著

清华大学出版社
北京交通大学出版社
·北京·

内 容 简 介

本书是作者长期从事电子商务安全课程教学成果的总结。本书系统地介绍了在电子商务交易过程中所涉及的安全问题，以及针对这些安全问题的主要安全标准及防范措施。

全书分为10章。第1章绪论，主要介绍中国电子商务的安全现状，同时分析制约电子商务广泛普及的瓶颈因素；第2章密码学及公钥基础设施的基本理论基础；第3章讲述PKI体系与功能应用；第4章介绍认证机构CA及其具体应用；第5章对数字签名及其应用进行介绍；第6章介绍了安全电子交易协议SET的主要内容；第7章讲述了安全套接层协议SSL的主要内容；第8章主要介绍网络银行及其相关的安全内容；第9章介绍目前流行的移动支付的主要内容及其安全风险和防范对策；第10章对第三方支付系统的安全进行了概要的阐述。

本书通俗易懂，除了基本的理论讲解之外，更多的是由具体的流程介绍构成，具备很强的可操作性，可作为高等院校电子商务专业高年级本科生的教材，也可以作为对电子商务在应用中的安全感兴趣的工程人员、技术人员的参考用书。

图书在版编目(CIP)数据

电子商务安全/祝凌曦编著. —2版. —北京：北京交通大学出版社：清华大学出版社，2014.10
（高等学校计算机科学与技术教材）
ISBN 978-7-5121-2078-5

Ⅰ.①电… Ⅱ.①祝… Ⅲ.①电子商务-安全技术-高等学校-教材 Ⅳ.①F713.36

中国版本图书馆CIP数据核字（2014）第201273号

责任编辑：谭文芳
出版发行：清华大学出版社　邮编：100084　电话：010-62776969
　　北京交通大学出版社　邮编：100044　电话：010-51686414
印 刷 者：北京时代华都印刷有限公司
经　　销：全国新华书店
开　　本：185×260　印张：17.75　字数：452千字
版　　次：2014年10月第2版　2014年10月第1次印刷
书　　号：ISBN 978-7-5121-2078-5/F·1414
印　　数：1~3 000册　定价：35.00元

第 2 版前言

《电子商务安全》是我出版的第一本书及教材，其中付出了太多的心血与辛苦。印象中，为编写这本教材，之前足足准备了三年时间，从开始编写到初稿完成也用了近一年的时间。那时候，每天除了教学外，其他时间基本都用在书稿的编写和整理上，希望能用自己的努力，向读者展现一个较全面的电子商务安全领域，毕竟那时电子商务在我国刚刚起步，电子商务这门学科也刚刚起步，很多概念和方向都不是很明晰。

幸运的是，这本教材的编写得到了学校和教育部的认可，被列入了教育部高等教育“十一五”规划教材建设项目，并且在 2006 年出版之后，得到了读者的认可，多次的印刷，第 1 版的发行量远远超过了我的预期。

转眼，教材第 1 版出版至今已经 8 年。自 2009 年以来，电子商务在我国的发展日新月异，出现了很多新的变化，以前很不清晰的地方，也逐渐变得清晰。同时，在近几年电子商务安全课程的教学中，也发现了一些以前没有注意到的问题和缺少的知识点。本书责任编辑谭文芳也多次提出应对这本书进行修订，这也使我感到有必要更新内容，让读者了解电子商务安全的最新进展，于是，就有了现在呈现在读者面前的第 2 版。

在本书第 2 版的编写过程中，对全书的结构和内容进行了重新的组织，对第 1 版的每一章都作了修改、补充或内容上的更新，每章增加了引导案例和拓展阅读。由于近年来，电子商务方面的书籍大量涌现，在第 2 版的编写中，尽量不重复已有中文书籍中的内容。第 2 版的编写宗旨就是不求内容的精深，但求简单、直观，可以让读者更为清楚的了解电子商务安全领域中应该了解的内容。

在此，非常感谢责任编辑谭文芳对本书出版的热情支持与多方面的协助，与这样能力卓著、认真负责的编辑共事是一个作者的幸运，没有她的督促与支持，就没有本书的再版。

在本书第 2 版的编写过程中，也得到了凌媛、申睿、冯欢、唐瑞、王琛、黄滢颖、康艳萍、周秀婷等的帮助。其中，凌媛对全书的主要内容进行了整理，唐瑞参与编写了第 9 章，申睿对第 1 章的数据进行了更新，冯欢参与编写了第 10 章。在此对以上朋友表示感谢。另外，也要感谢这么多年来我所教过的电子商务专业的学生们，在和你们相处的过程中，我也受益匪浅。

还要感谢我的父母，没有他们的培养，就没有今天我的一切。特别感谢我的妻子和岳母，是她们承担了家里所有的家务，使我有足够的时间来完成教学、科研和写作。

最后，将本书献给我的儿子，自从他来到这个世上，我改变了很多，在看着他长大的同时，我也逐渐长大，谢谢你，我的儿子，我愿意为你变得更好。

祝所有的人都变得越来越好！

祝凌曦

2014 – 07 – 09

目　录

第1章 绪 论

内容提要：

本章对电子商务的安全现状进行了描述；分析了触发这些问题的原因；讲解了威胁电子商务发展的安全隐患及其防治措施。通过介绍电子商务的安全需求，提出了电子商务的安全体系结构。并介绍了电子商务中常用的安全标准。

学习目标：

- 了解电子商务的现状，以及造成这种现状的原因。
- 了解电子商务发展的隐患，以及防治措施。
- 掌握电子商务的安全需求。
- 了解电子商务的安全威胁，以及采用什么的方法避免威胁。
- 了解电子商务安全的体系结构。
- 掌握涉及电子商务安全的主要安全标准。

引导案例：

密码传奇：世界最难破解的密码锁17年被攻克

参见：http://mil.gmw.cn/2012-03/16/content_3784271.htm

1.1 电子商务安全现状与趋势

1.1.1 电子商务安全现状

近年来，随着数字化、网络化技术的不断发展，社会信息化的程度越来越高。随着互联网在中国的日益普及，网络已经深入到人们生活的方方面面。现在人们在网络上可以进行各种商务活动，从企业和企业之间的商务合作，国际间贸易的发展；到个人生活的各个方面，大到房屋、汽车的购买，小到购买音像制品、图书和日常用品；实体的如购买电视、冰箱等家用电器，数字的如购买音乐、电影。数量金额从B2B的几十万上百万元，到下载一个铃声花费的几元钱，购买一篇论文花费的三角五角，甚至几分钱的游戏点数。

如果说20世纪90年代，没有了电，没有了计算机，好多人不知该如何工作，那么到了现在的21世纪，如果没有了网络，同样会有好多人无法正常生活。

随着电影《天下无贼》的放映，人们感受到了人间的真情。但是随之而来铺天盖地的巨幅广告“用支付宝，天下真的无贼”，才是中国历史上对于网络安全的一次真正的冲击。这不仅标志着中国的IT（Information Technology，信息技术）业在电子商务中已经发展到了很深的程度，而且使得电子商务的安全问题也第一次浮出水面，那么真实地面对普通的老百姓，而不是像以往那样面对的是西装革履的IT精英们。画面上傻根安心的笑容，不但体现了普通老百姓对电子商务安全的渴望，也表现出了中国IT人士对电子商务安全的信心。

在阻碍电子商务发展的三座大山——电子商务安全、电子支付和电子商务物流中，人们普遍认为电子商务物流正在蓬勃发展，物流快递公司在不断涌现，而且物流行业较为容易被人们所熟悉。电子支付系统是银行建设的，和老百姓没有多大关系。只有安全问题是老百姓（也就是电子商务最大的受众者）所深深担忧的，是电子商务推进中的最大路障。人们对电子商务安全问题十分关心，但是大多数人对安全问题又缺少必要的了解，对人们而言这个领域充满了神秘感，人们经常在报纸上、电视上看到或听到黑客的种种消息，使他们对电子商务的网上支付在心理上产生了畏惧感。此外，尽管政府及一些企业已意识到这一问题，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存在的原因所在。因此，让更多的人了解电子商务安全的基本体系和原理是电子商务发展过程中最为重要的工作。

历史上最严重的网络安全事件是发生在2000年2月7日、8日、9日这三天的互联网被黑事件。在这黑色的三天里，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。黑客三天来的袭击，造成的间接和直接经济损失达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。当时雅虎是全球第二大搜索引擎网站，每天被浏览页次达4.65亿次，其股市价值达930亿美元。2月8日上午，先是当天股市的网络销售公司购买网站死机；再是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1000万，是每月浏览达15亿次的网上拍卖网站，2月8日下午6时，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。

国外最近一次著名的网络安全事件是2013年6月份，大约有650万个LinkedIn用户密码的哈希密码字段被盗并被公布在互联网上。目前LinkedIn已经承认了该事件，LinkedIn的悲剧发生后，eHarmony交友网站也确认大约有150万密码被盗。该消息一经报道，立即引起了媒体、网民等多方的关注，转载、评论量在短期内迅速增多，呈现出极大程度的爆发趋势。

目前网络安全的脆弱性，以及黑客软件和技术的普及，使得很多的黑客攻击事件已经不像以前那样是专业黑客所为，一些普通人经过适当学习，就可以进行黑客的活动。发生在2010年的初中文化黑客盗卖他人账户的事件，就给证券行业的网络安全敲响了警钟。为了应对网络的冲击，尽快给公众提供网上服务是应该的也是必要的，但前提条件是要做好安全工作，特别是涉及用户信息和财务往来这些关系到公众利益的重要方面更应如此。

为了对电子商务的安全问题有更感性的认识，下面分析黑客盗取信用卡卡号的过程。黑客在互联网的新闻组上发布带有后门病毒的程序，通过各种方式使上网者下载到自己的 PC 上，一旦某台 PC 下载了此程序，他就成为黑客可以侵略的对象。黑客可以浏览被入侵者 PC 上的全部信息资源，可以实时地掌握被入侵者的桌面使用情况。如果被入侵者此时输入信用卡号和密码，那么黑客就可以易如反掌地窃取到这些信息。

即使不在公共信息场所下载软件，也很有可能成为无辜的受害者，因为黑客程序中的后门病毒具有很强的蔓延性，即一台 PC 被感染后，病毒可通过此 PC 上的地址簿向这些地址的 PC 传播，然后按同样的方法再进一步把态势扩大。这样呈几何级的增长使病毒的蔓延速度极快，覆盖范围极广。所以，不经意间或许你的 PC 就已成为黑客的盘中餐，而一个网上交易的网站一旦发生消费者信用卡泄露事件，那么将不会再有人去访问这个站点。因此，要使电子商务能健康、蓬勃地发展，就必须用全面的电子商务安全解决方案提供交易的信任保障。

电子商务站点上的安全漏洞会造成网上交易用户的账号、交易密码泄露，恶意攻击者可以使他人资金泄露，甚至可以使用他人资金进行网上交易。《2011—2012 中国互联网安全研究报告》指出，中国每天有 4% ~8% 的计算机上会发现病毒；钓鱼网站取代病毒木马成为互联网第一大安全威胁，每月拦截网民访问次数比 2010 年激增了 100 倍。商务安全漏洞的存在，直接影响国内电子商务站点的信誉程度。网上交易安全性若不能得到保证，就必将影响我国电子商务的顺利发展。

1.1.2 触发电子商务安全问题的原因

日益严重的网络信息安全问题，不仅使上网企业、机构及用户蒙受了巨大经济损失，而且使国家的安全与主权面临严重威胁。要避免网络信息安全出现问题，首先必须搞清楚触发这一问题的原因，归纳起来，主要有以下几个方面。

1. 黑客的攻击

由于缺乏卓有成效的针对网络犯罪的反击和跟踪手段，因此黑客的攻击不仅“杀伤力”强，而且隐蔽性好。目前，世界上有 20 多万个黑客网站，其攻击方法达几千种之多。在现实世界中，黑客最能吸引人们目光的焦点。为了应对黑客的威胁，人们开始检讨长久以来实行的个人密码，开始转向更为安全的保护措施来防止信息泄露，如动态密码等。

2. 管理的欠缺

网站或系统的严格管理是企业、机构及用户免受攻击的重要措施。事实上，很多企业、机构及用户的网站或系统都疏于这方面的管理。

据中国电子商务研究中心发布的《试论电子商务面临的若干网络安全问题》中所述，由于电子商务企业缺乏警惕性，不重视网络安全的管理，通常只有在受到攻击以后才会去加强网站安全；部分企业则以为只要安装了入侵监测系统、杀毒软件、防火墙等安全产品，就能保障网站的安全，所以没有根据企业实际情况建立相应的管理制度，也没有加强技术防范，给入侵者提供了机会。

3. 网络的缺陷

因特网的共享性和开放性使网上信息安全存在先天不足，因为因特网最初的设计考虑是该网不会因局部故障而影响信息的传输，但它仅是信息高速公路的雏形，在安全可靠、服务

质量、带宽和方便性等方面还存在着不适应性。

4. 软件的漏洞或“后门”

许多软件研发单位研发的技术不成熟的电子商务软件，存在许多安全漏洞，防护极易被外来入侵者利用漏洞攻破，导致电子商务企业受到很大的经济损失；有的企业即使安装了防护软件，但由于软件没有得到及时升级，致使软件丧失了应有防护功能。

5. 人为的触发

基于信息战和对他国监控的考虑，个别国家或组织有意识触发网络信息安全问题。

1.2 电子商务的安全需求及体系结构

1.2.1 电子商务的安全要求

电子商务是将传统的商务活动移到网络环境中来，特别是建立在互联网上的商务活动，其安全问题倍受关注。所谓电子商务的安全，不但是网络安全问题，还需要从电子商务对网络系统的安全需求出发，采取安全技术措施，提供安全服务，以满足电子商务的各种安全需求。电子商务安全的基本要求如下。

1. 交易的认证性

交易的认证性是指在交易开始之前，买卖双方能够认证对方的身份，即可以识别对方的身份是否真实。

电子商务是在网络上进行的电子交易，买卖双方实际上都是在和虚拟的对方进行交易。在这种情况下，可能存在的风险是：对方的身份是否与其在网络上所声称的一致，是否存在着诈骗的可能。在现实社会中，都无法避免存在的诈骗现象，在网络的社会里，买卖的双方更是可能相距千里，甚至在不同的国家，在这种情况下，辨别交易双方的实际身份就显得更为重要。

交易的认证性类似现实社会中的“中间人”或“担保人”，交易的双方都可能对对方不信任，但是只要他们都信任“中间人”CA（Certificate Authority，认证授权机构或认证中心），而由 CA 来确认双方的身份，那么买卖双方就可以取得彼此的信任。这种认证是需要一定的手段进行的，一般是通过数字证书进行身份的验证，而数字证书有良好的安全性，有些时候还可以要求有硬件（如 IC（Integrated Circuit，集成电路）卡、USB（Universal Serial Bus，通用串行总线）KEY 等）来进行验证。

2. 交易的保密性

交易的保密性，国外也称为交易的隐私性，是指交易双方的信息在网络传输或存储中不被他人窃取。在传统的商务交易中，敏感性的数据，如：商务合同、信用卡号码、交易机密等可以通过文件的封装或其他可靠的途径来传递，以此来保证数据的安全。而在开放的因特网上，由于 TCP/IP（Transmission Control Protocol/Internet Protocol，传输控制协议/网际协议）协议采用 IP 报文交换方式，因而存在数据被窃取的可能。所以，电子交易过程中保证交易数据的隐秘尤为重要。

电子商务的保密性主要是通过“数据不被窃取、窃取不可破译”的思路来设计的。具体来说，“数据不被窃取”，可以通过防火墙、IPSec（Internet 协议安全性）等手段实现，而

“窃取不可破译”，则主要通过各种加密手段来保证，如采用 DES（Data Encryption Standard，数据加密标准）、RSA 加密等方法。

在交易的隐私性中，还包括了一点就是交易的不可跟踪性。也就是在进行电子交易的时候，其他人无法通过对消费者采用支付手段的分析，发现消费者的身份，这方面在数字现金等领域的应用尤为重要。一般可以采用强盲签名、有限的匿名性等方式来进行保证。

3. 交易的完整性

交易的完整性是指交易数据在传输过程中不被恶意或意外的改变、损坏。

交易的保密性固然能够保证交易数据在传输过程中不被窃取，但是不能保证传输过程中可能发生某种意外或非授权情况下的破坏，同时也难以保证数据传输的顺序统一。而完整性对交易中的敏感数据是非常重要的。例如，在交易中的扣款过程，需要在双方的账号上进行操作，如果交易不完整，只在一方账号上进行了操作，那么产生的结果是难以预料的。

4. 交易的不可否认性

不可否认性也称不可抵赖性，主要指交易的双方不能否认彼此之间所进行的信息交流。

在传统的交易过程中，就算双方可能并不见面，如邮购过程。但是双方对交易的行为是很难抵赖的，因为有足够的证据（如邮购中的单据、凭证等）来证明买方或卖方的行为。

而网络上的交易，由于采用的是电子化的信息，如果没有相关的手段进行保证，确实很难证明某笔订单是来自某个买家的。如常见的网络购物中的“送货上门、货到付款”。

电子商务交易的不可否认性无法像传统交易那样通过签订“白纸黑字”的合同、盖章来加以确认，但是可以采取类似的思路，通过使用数字签名来加以确认。

5. 其他安全需求

除了以上主要的安全需求之外，电子商务安全的需求还包括以下内容。

（1）可访问性：保证系统、数据和服务能由合法的人员访问。

（2）防御性：能够阻挡不希望的信息或黑客的入侵。

（3）合法性：保证各方的业务符合可适用的法律和法规。

1.2.2 安全策略

所谓安全策略，就是实施计算机信息系统的安全措施及安全管理的指导思想，是在计算机信息系统内，用于所有与安全活动相关的一套规则。这些规则是由这个系统中的新设立的一个安全权力机构建立的，并由安全控制机构来描述、实施和实现。

安全策略主要包括以下主要内容。

1. 授权

授权（Authorization）是一个安全策略的基本组成部分。所谓授权，是指赋予主体（用户、终端、程序等）对客体（数据、程序等）的支配权利，等于规定了谁可以对什么做什么。

在机构安全策略等级上授权描述的一些例子如下。

例 1：文件 Project - X - Status 只能够由甲修改，并由甲或乙，以及 Project - X 计划小组中的成员阅读。

例 2：一个人事记录只能由人事部的职员进行增删和修改，并且只能由人事部职员、执行经理，以及该记录所属于的级别阅读。

例3：假设在多级安全系统中有一密级 Confidential - secret - topSecret，只有所持许可证级别等于或高于此密级的人员，才有权访问此密级中的信息。

这些安全策略的描述也对各类防护措施提出了要求。例如，采用人事防护措施来决定人们的许可证级别。在计算机和通信系统中，主要的要求以一种被称做“访问控制策略”的系统安全策略反映出来。

2. 访问控制策略

访问控制技术最早产生于20世纪60年代，是网络安全防范和保护的主要策略。它主要是按用户身份及其所归属的某项定义组来限制用户对某些信息的访问，或限制对某些控制功能的使用。它管理所有资源访问请求，即根据安全策略的要求，对每个资源访问请求做出是否许可的判断，能有效地防止非法用户访问系统资源和合法用户非法使用资源。访问控制通常用于系统管理员控制用户对服务器、目录、文件等网络资源的访问。

访问控制系统一般包括：主体、客体、安全访问策略。

主体：访问操作、存取要求的发起者，通常指用户或用户的某个进程。

客体：被调用的程序或欲存取的数据，即必须进行控制的资源或目标，如网络中的进程等活跃元素、数据与信息、各种网络服务和功能、网络设备与设施。

安全访问策略：一套用以确定一个主体是否对客体拥有访问能力的规则，它定义了访问控制规则的主体与客体可能的相互作用途径。访问控制规则如表1-1所示。

表1-1 访问控制规则

用户	目 标		
	x	y	z
用户a	读、修改、管理		读、修改、管理
用户b		读、修改、管理	
用户c	读	读、修改	
用户d	读	读、修改	

访问控制策略根据其作用对象的不同分为以下三种。

（1）基于对象的访问控制（Object - based Access Control Model，OBAC Model）。

（2）基于任务的访问控制模型（TBAC Model，Task - based Access Control Model）是从应用和企业层角度解决安全问题，以面向任务的观点，从任务（活动）的角度建立安全模型和实现安全机制，在任务处理的过程中提供动态实时的安全管理。TBAC模型由工作流、授权结构体、受托人集、许可集四部分组成。

（3）基于角色的访问控制模型（Role - based Access Model，RBAC Model）：RBAC模型的基本思想是将访问许可权分配给一定的角色，用户通过饰演不同的角色获得角色所拥有的访问许可权。

3. 责任

支撑所有安全控制策略的一个根本原则是责任（Accountability）。受到安全策略制约的任何个体在执行任务时，需要对他们的行为负责任，并应与其人事履历有十分重要的关联。某些网络防护措施，包括认证工作人员的身份，以及与这种身份相关的活动，都直接支持这一原则。