21世纪高等院校计算机网络工程专业规划教材

# 电子商务安全技术

吴翠红　闫季鸿　主编

清华大学出版社

21世纪高等院校计算机网络工程专业规划教材

# 电子商务安全技术

吴翠红　闫季鸿　主编

清华大学出版社
北京

## 内 容 简 介

本书全面介绍电子商务安全涉及的基础理论和应用，内容精练，目标明确。

全书按照电子商务安全体系结构自底向上的顺序安排章节，共分 9 章，第 1 章主要阐述电子商务安全要素和安全体系以及电子商务安全的现状与发展，第 2 章主要阐述与电子商务相关的网络技术、防火墙、入侵检测等，第 3 章主要阐述计算机病毒的基本知识和网络攻防的方法和工具，第 4 章主要阐述跟密码技术相关的数学知识和相关概念、密码的两种基本体制和代表算法、数字签名和数字摘要，第 5 章主要介绍信息隐藏及其应用，数字水印和数字版权技术，第 6 章主要阐述 PKI 工作原理以及数字证书的类型、内容以及认证中心的功能，第 7 章电子商务安全协议主要阐述电子商务的两种重要协议(SSL 和 SET)，第 8 章主要阐述当前发展迅速的移动商务存在的安全隐患和安全技术，第 9 章主要阐述保障电子商务安全的一些基本策略和方法；每章后均附有习题。

本书适合作为高等院校计算机、电子商务、经济管理、安全等专业应用型本科生的教材，同时可供对电子商务有所了解的专业技术人员参考。



**图书在版编目(CIP)数据**

电子商务安全技术/吴翠红，闫季鸿主编. --北京：清华大学出版社，2015
21 世纪高等院校计算机网络工程专业规划教材
ISBN 978-7-302-40882-6

Ⅰ. ①电… Ⅱ. ①吴… ②闫… 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(2015)第 164179 号

**责任编辑**：魏江江　薛　阳
**封面设计**：常雪影
**责任校对**：焦丽丽
**责任印制**：刘海龙

**出版发行**：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦 A 座　　邮　　编：100084
社 总 机：010-62770175　　邮　　购：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质 量 反 馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
课 件 下 载：http://www.tup.com.cn，010-62795954

**印 装 者**：三河市吉祥印务有限公司
**经　　销**：全国新华书店
**开　　本**：185mm×260mm　　**印　　张**：12.5　　**字　　数**：305 千字
**版　　次**：2015 年 9 月第 1 版　　**印　　次**：2015 年 9 月第1 次印刷
**印　　数**：1～2000
**定　　价**：26.00 元

产品编号：053211-01

# 前言

随着电子商务的兴起，网络购物已经成为一种时尚，但是有70%的消费者表示，他们对网上购物最担心的就是安全问题，因此电子商务安全问题成为制约电子商务发展的关键问题之一，如何能够更好地建设安全的电子商务交易环境成为当前迫切需要解决的问题。国内外的同类教材越来越多，但教材的侧重点不尽相同。

结合电子商务专业的人才培养目标，本书比较详尽地介绍了电子商务安全的各种方法与手段，以及影响电子商务安全的主要因素及采用何种方法进行解决，能够更好地解决电子商务交易中所涉及的安全问题。

本书根据电子商务安全技术体系结构来组织，以网络安全技术、现代加密技术、数字签名技术、身份认证技术、密钥管理技术为主线进行章节安排，同时增加了最新的移动电子商务安全的内容。每一章内容都从电子商务的某一个实际需求开始，由浅入深，讲解涉及的概念和具体的实施过程，每章前面都有学习目标，使学生学习前有一定的方向，达到知识的掌握和应用能力的培养。

本书共分9章，第1章为概述，主要介绍电子商务安全现状、安全要素以及安全体系结构；第2章为网络安全技术，主要介绍网络安全技术基础、防火墙技术、虚拟专用网、入侵检测；第3章为计算机病毒与网络攻防，主要介绍计算机病毒的防治和黑客的攻防；第4章为电子商务加密技术，主要介绍密码学的基本数学知识、密码体制、认证技术和数字签名；第5章为信息隐藏技术，主要介绍信息隐藏技术和数字水印技术、数字版权保护技术；第6章为公钥基础设施，主要介绍PKI和数字证书；第7章为电子商务安全协议，主要介绍SSL协议和SET协议；第8章为移动电子商务安全，主要介绍移动网络安全技术和移动电子商务安全技术；第9章为电子商务安全策略，主要介绍安全防范策略、访问权限控制和风险管理。

本书由吴翠红和闫季鸿任主编，并感谢上海第二工业大学电子商务系全体教师的帮助。鉴于编者学术水平有限，书中可能存在错误和不妥，敬请专家和读者批评指正。

编　者

2015年6月

# 目 录

# 第1章 电子商务安全概述

**本章学习目标**

- 熟练掌握电子商务安全要素。
- 了解电子商务安全的发展。
- 熟练掌握电子商务安全体系。

本章介绍电子商务安全的现状、发展趋势，电子商务安全的基本要素，涉及的电子商务技术，以及电子商务的安全体系结构。

## 1.1 电子商务安全现状

基于互联网应运而生的电子商务，孕育了一种全新的电子商务模式。这种以互联网为基础的商务模式市场前景广阔，发展潜力巨大，深受企业和电商人士的青睐，不过由于模式本身还存在功能和运作上的缺陷，日积月累下来的问题也更加明显和突出。网络安全、互联网基础设施建设、互联网诚信等几大问题成了阻碍电子商务发展的主要因素。其中，电子商务安全是制约电子商务发展的一个核心和关键问题。

互联网是虚拟的现实社会，以其网络的开放性、技术的渗透性、信息传播的交互性而广泛渗透到各个领域，有力地促进了经济社会的发展。特别是 Web 2.0 的出现和普及，除了带给互联网企业更大的发展机遇和动力，也同样使它们面临了更多的压力和安全隐患：海量的数据，复杂的应用，频繁的攻击。

互联网安全问题已经不单单是独立问题，而是牵一发而动全身的联动性问题，在电子商务领域也已经造成了极大的影响。作为一家电子商务公司，当网站不能正常访问时，会引发一系列问题：客户会投诉，代理商会埋怨，公司更要为这次恶性事件背负极大的债务支出和补偿。

电子商务安全隐患具体如下：

由于互联网的完全开放性以及不可预知的管理漏洞、技术威胁等严重问题，如果得不到及时解决，可能会产生一些不可预见的安全问题，尤其在信息安全、交易安全和财产安全方面会产生恶劣的影响：

(1) 信息安全方面：信息安全是指由于各种原因引起的信息泄露、信息丢失、信息篡改、信息虚假、信息滞后、信息不完善等，以及由此带来的风险；

(2) 交易安全方面：交易安全是指电子商务交易过程中存在的各种不安全因素，包括交易的确认、产品和服务的提供、产品和服务的质量、价款的支付等方面的安全问题；

(3) 财产安全方面：财产安全是指由于各种原因造成电子商务参与者面临的财产等经济利益风险。财产安全往往是电子商务安全问题的最终形式，也是信息安全问题和交易安

全问题的后果。

这几个方面的问题确实对电子商务是致命的，电子商务并不是人们想象中那般完美无瑕，处理不好同样危机重重。企业在选择电子商务的时候，要认清电子商务的两面性，投资有风险，电子商务的安全问题只有首先得到解决，才能还原电子商务无穷的生机与活力。

当许多传统的商务方式应用在 Internet 上时，便会带来许多源于安全方面的问题，如传统的贷款和借记卡支付/保证方案及数据保护方法、电子数据交换系统、对日常信息安全的管理等。电子商务的大规模使用虽然只有几年时间，但不少公司都已经推出了相应的软硬件产品。由于电子商务的形式多种多样，因此涉及的安全问题各不相同，但在 Internet 上的电子商务交易过程中，最核心和最关键的问题就是交易的安全性。一般来说商务安全中普遍存在着以下几种安全隐患。

**1. 窃取信息**

由于未采用加密措施，数据信息在网络上以明文形式传送，入侵者在数据包经过的网关或路由器上可以截获传送的信息。通过多次窃取和分析，可以找到信息的规律和格式，进而得到传输信息的内容，造成网上传输信息泄密。

**2. 篡改信息**

当入侵者掌握了信息的格式和规律后，通过各种技术手段和方法，将网络上传送的信息数据在中途修改，然后再发向目的地。这种方法并不新鲜，在路由器或网关上都可以做此类工作。

**3. 假冒**

由于掌握了数据的格式，并可以篡改通过的信息，攻击者可以冒充合法用户发送假冒的信息或者主动获取信息，而远端用户通常很难分辨。

**4. 恶意破坏**

由于攻击者可以接入网络，则可能对网络中的信息进行修改，掌握网上的机密信息，甚至可以潜入网络内部，其后果非常严重。

因此，电子商务的安全性主要体现在以下 4 个方面：

信息保密性：交易中的商务信息均有保密的要求。如信用卡的账号和用户名等不能被他人知悉，因此在信息传播中一般均有加密的要求。

交易者身份的确定性：网上交易的双方很可能素昧平生，相隔千里。要使交易成功，首先要能确认对方的身份，商家要考虑客户端不能是骗子，而客户也会担心网上的商店不是一家黑店。因此能方便而可靠地确认对方的身份是交易的前提。

不可否认性：由于商情的千变万化，交易一旦达成是不能被否认的，否则必然会损害一方的利益，因此电子交易通信过程的各个环节都必须是不可否认的。

不可修改性：交易的文件是不可被修改的，否则也必然会损害一方的商业利益，因此电子交易文件也要能做到不可修改，以保障商务交易的严肃和公正。

## 1.2 电子商务安全要素及安全技术

### 1.2.1 电子商务安全要素

信息安全通常强调所谓 CIA 三元组的目标，即保密性、完整性和可用性。CIA 概念的阐述源自信息技术安全评估标准（Information Technology Security Evaluation Criteria，

ITSEC)，它也是信息安全的基本要素和安全建设所应遵循的基本原则。

(1) 保密性(Confidentiality)：确保信息在存储、使用、传输过程中不会泄露给非授权用户或实体。

(2) 完整性(Integrity)：确保信息在存储、使用、传输过程中不会被非授权用户篡改，同时还要防止授权用户对系统及信息进行不恰当的篡改，保持信息内部、外部表示的一致性。

(3) 可用性(Availability)：确保授权用户或实体对信息及资源的正常使用不会被异常拒绝，允许其可靠而及时地访问信息及资源。

当然，不同机构和组织，因为需求不同，对 CIA 原则的侧重也会不同，如果组织最关心的是对私密信息的保护，就会特别强调保密性原则，如果组织最关心的是随时随地向客户提供正确的信息，那就会突出完整性和可用性的要求。

而电子商务安全是一个复杂的系统问题，在使用电子商务的过程中会涉及以下 6 个有关安全方面的要素。

(1) 可靠性。

可靠性是指电子商务系统的可靠程度，是指为防止由于计算机失效、程序错误、传输错误、硬件故障、系统软件错误、计算机病毒和自然灾害等所产生的潜在威胁，采取的一系列的控制和预防措施来防止数据信息资源不受到破坏的可靠程度。

(2) 真实性。

真实性是指商务活动中交易者身份的真实性，确保交易双方确实是存在的，不是假冒的。网上交易的双方相隔很远，互不了解，要使交易成功，必须互相信任，确认对方是真实的。能否方便而又可靠地确认交易双方身份的真实性，是顺利进行电子商务交易的前提。

(3) 机密性。

机密性是指交易过程中必须保证信息不会泄露给非授权的人或实体。电子商务的交易信息直接代表着个人、企业或国家的商业机密。传统的纸面贸易都是通过邮寄封装的信件或通过可靠的通信渠道发送商业报文来保守机密的；而电子商务则建立在一个较为开放的网络环境之上，商业保密就成为电子商务全面推广的重要屏障。因此要预防非法的信息存取和信息在传输过程中被非法窃取，确保只有合法用户才能看到数据，防止泄密事件。

(4) 完整性。

完整性是指数据在输入、输出和传输过程中，要求能保证数据的一致性，防止数据非授权建立、修改和破坏。电子商务简化了贸易过程，减少了人为的干预，但同时也带来了需要维护商业信息完整、统一的问题。由于数据输入时的意外差错或欺诈行为，可能导致贸易各方信息的差异。此外数据传输过程中的信息丢失、信息重复或信息传送的次序差异也会导致贸易各方信息不相同。信息的完整性将影响到贸易各方的交易和经营策略，保持这种完整性是电子商务应用的基础。

(5) 有效性。

电子商务以电子形式取代了纸张，那么如何保证这种电子形式贸易信息为交易各方共同认可是开展电子商务的前提。电子商务作为一种新的贸易形势，其信息的有效性将直接关系到个人、企业或国家的经济利益和声誉。一旦签订交易后，这项交易就应受到保护，以防止被篡改或伪造。交易的有效性在其价格、期限及数量作为协议的一部分时尤为重要。

(6) 不可抵赖性。

电子商务可能直接关系到贸易双方的商业交易，如何确定将要进行的交易方正是所期望的贸易方这一问题，则是保证电子商务顺利进行的关键。在电子商务方式下，通过手写签名和印章是不可能的。因此要求在交易信息中为参与交易的个人、企业或国家提供可靠的标识，使原发送方在发送数据后不能抵赖；接收方在接收数据后也不能抵赖。

## 1.2.2 电子商务安全标准和技术

在早期的电子交易中，曾采用过如下一些简易的安全措施。

(1) 部分告知(Partial Order)：即在网上交易中将最关键的数据如信用卡号码及成交数额等略去，然后再用电话告之，以防泄密。

(2) 另行确认(Order Confirmation)：即当在网上传输交易信息后，再用电子邮件对交易做确认，才认为有效。

此外还有其他一些方法，这些方法均有一定的局限性，且操作麻烦，不能实现真正的安全可靠性。

近年来，针对电子交易安全的要求，IT 业界与金融行业一起，推出了不少有效的安全交易标准和技术。

**1. 主要的协议标准**

安全超文本传输协议(HTTPS)：依靠密钥对的加密，保障 Web 站点间交易信息传输的安全性。

安全套接层协议(SSL)：由 Netscape 公司提出的安全交易协议，提供加密、认证服务和报文的完整性。SSL 被用于 Netscape Communicator 和 Microsoft IE 浏览器，以完成需要的安全交易操作。

安全交易技术协议(Secure Transaction Technology，STT)：由 Microsoft 公司提出，STT 将认证和解密在浏览器中分离开，用以提高安全控制能力。Microsoft 在 Internet Explorer 中采用这一技术。

安全电子交易协议(Secure Electronic Transaction，SET)：1996 年 6 月，由 IBM、MasterCard International、Visa International、Microsoft、Netscape、GTE、VeriSign、SAIC、Terisa 就共同制定的标准 SET 发布公告，并于 1997 年 5 月底发布了 SET Specification Version 1.0，它涵盖了信用卡在电子商务交易中的交易协定、信息保密、资料完整及数据认证、数据签名等。

SET 标准已获得 IETF 标准的认可，已经成为事实上的工业标准。

**2. 主要的安全技术**

1) 密码技术

密码技术主要包括加密、签名认证和密钥管理三大技术。

保证电子商务安全最重要的一点就是使用加密技术对敏感的信息进行加密。现在，一些专用密钥加密(如 3DES、IDEA、RC4 和 RC5)和公钥加密(如 RSA、SEEK、PGP 和 EU)可用来保证电子商务的保密性、完整性、真实性和非否认服务。然而，这些技术的广泛使用却不是一件容易的事情。

密码学界有一句名言：加密技术本身都很优秀，但是它们实现起来却往往很不理想。

现在虽然有多种加密标准，但人们真正需要的是针对企业环境开发的标准加密系统。加密技术的多样化为人们提供了更多的选择余地，但也同时带来了一个兼容性问题，不同的商家可能会采用不同的标准。另外，加密技术向来是由国家控制的，例如 SSL 的出口受到美国国家安全局(NSA)的限制。目前，美国的商家一般都可以使用 128 位的 SSL，但美国只允许加密密钥为 40 位以下的算法出口。虽然 40 位的 SSL 也具有一定的加密强度，但它的安全系数显然比 128 位的 SSL 要低得多。据报载，最近美国加州已经有人成功地破译了 40 位的 SSL，这已引起了人们的广泛关注。美国以外的国家很难真正在电子商务中充分利用 SSL，这不能不说是一种遗憾。上海市电子商务安全证书管理中心推出 128 位的 SSL 算法，弥补了国内的空缺，并采用数字签名等技术确保电子商务的安全。

加密技术是认证技术和其他很多安全技术的基础，也是信息安全的核心技术。

签名认证技术是保证信息真实性的一种重要手段。它力图解决互联网交易面临的几个根本问题：数据保密、数据不被篡改、交易方能互相验证身份、交易发起方对自己的数据不能否认。“数字签名”是目前电子商务、电子政务中应用最普遍、技术最成熟、可操作性最强的一种电子签名方法。

它采用了规范化的程序和科学化的方法，用于鉴定签名人的身份以及对一项电子数据内容的认可。它还能验证出文件的原文在传输过程中有无变动，确保传输电子文件的完整性、真实性和不可抵赖性。

密钥管理不仅影响系统的安全性，也涉及系统的可靠性、有效性和经济性。因为再强的密码算法，只要密钥泄露，信息的安全性就不复存在了。

2) 网络安全技术

(1) 防火墙技术。

防火墙是一种保护计算机网络安全的技术性措施，它是一个用以阻止网络中的黑客访问某个机构网络的屏障，也可称之为控制进/出两个方向通信的门槛。在网络边界上通过建立起来的相应网络通信监控系统来隔离内部和外部网络，以阻挡外部网络的侵入。目前的防火墙主要有以下三种类型：包过滤防火墙、代理防火墙、双穴主机防火墙。

(2) 入侵检测技术。

入侵检测系统能够监视和跟踪系统、事件、安全记录和系统日志，以及网络中的数据包，识别出任何不希望有的活动，在入侵者对系统发生危害前，检测到入侵攻击，并利用报警与防护系统进行报警、阻断等响应。

(3) 虚拟专用网(VPN)。

这是用于 Internet 交易的一种专用网络，它可以在两个系统之间建立安全的信道(或隧道)，用于电子数据交换(EDI)。它与信用卡交易和客户发送订单交易不同，因为在 VPN 中，双方的数据通信量要大得多，而且通信的双方彼此都很熟悉。这意味着可以使用复杂的专用加密和认证技术，只要通信的双方默认即可，没有必要为所有的 VPN 进行统一的加密和认证。现有的或正在开发的数据隧道系统可以进一步增加 VPN 的安全性，因而能够保证数据的保密性和可用性。

3) 认证技术

数字认证可用电子方式证明信息发送者和接收者的身份、文件的完整性(如一个发票未被修改过)，甚至数据媒体的有效性(如录音、照片等)。随着商家在电子商务中越来越多地

使用加密技术，人们都希望有一个可信的第三方，以便对有关数据进行数字认证。

目前，数字认证一般都通过单向 Hash 函数来实现，它可以验证交易双方数据的完整性，Java JDK1.1 也能够支持几种单向 Hash 算法。另外，S/MIME 协议已经有了很大的进展，可以被集成到产品中，以便用户能够对通过 E-mail 发送的信息进行签名和认证。同时，商家也可以使用 PGP(Pretty Good Privacy)技术，它允许利用可信的第三方对密钥进行控制。可见，数字认证技术将具有广阔的应用前景，它将直接影响电子商务的发展。

## 1.3 电子商务安全体系结构

电子商务系统需要一个完整的安全体系，作为制约电子商务发展的核心问题，电子商务安全问题是由它的安全结构及协议的安全等级决定的，如图 1.1 所示。建立在安全体系上的协议安全性是由其内在的关键技术支撑的，这决定了安全协议在电子商务安全运行中的重要作用。

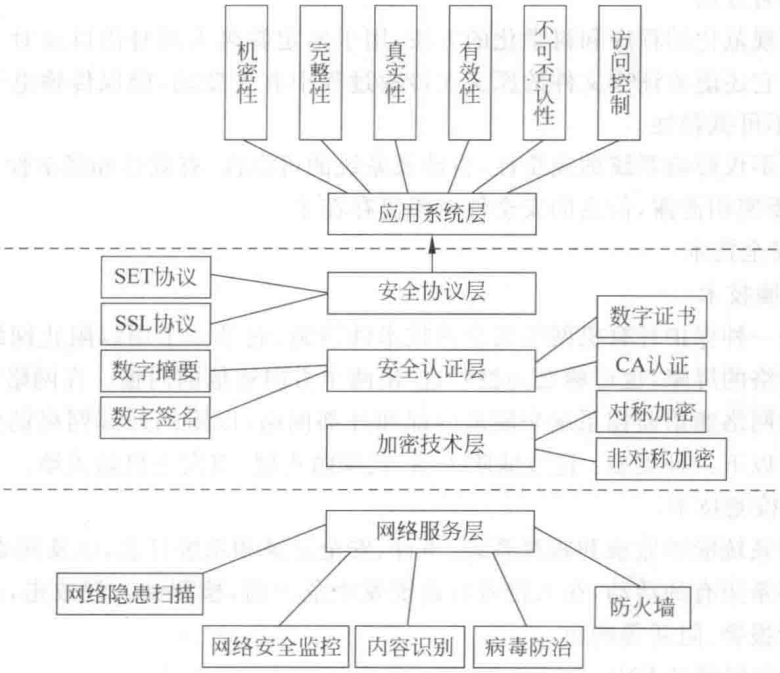


图 1.1 电子商务安全体系结构

电子商务的安全技术体系结构是保证电子商务中数据安全的一个完整的逻辑结构。电子商务安全体系结构从下至上由网络服务层、加密技术层、安全认证层、安全协议层、应用系统层组成。各层采用各种安全控制技术，来实现其安全策略，以保证商业交易的安全。此安全框架的底层是网络服务层，它提供信息传送的载体和用户接入的手段，通过入侵检测、安全扫描、防火墙等技术保证网络层的安全。而加密技术层、安全认证层和安全协议层，是为电子交易数据的安全而构筑的。加密技术是保证电子商务系统安全所采用的最基本的安全措施，它用于满足电子商务对保密性的需求。安全认证层中的认证技术对加密技术层中提供的多种加密算法进行综合运用。

## 1.4 电子商务法律要素

安全的电子商务仅靠单一的技术手段来保证是不会奏效的，必须依靠法律手段、行政手段和技术手段的完美结合来最终保护参与电子商务各方的利益。法律法规的建设成为当前电子商务发展之必须。

开展电子商务需要在企业和企业之间、政府和企业之间、企业和消费者之间、政府和政府之间明确各自需要遵守的法律义务和责任，主要涉及的法律要素如下：

(1) 有关认证(CA)中心的法律。CA 中心是电子商务中介于买卖双方之外的公正的、权威的第三方，是电子商务中的核心角色，它担负着保证电子商务公正、安全进行的任务。因而必须由国家法律来规定 CA 中心的设立程序和设立资格以及必须承担的法律义务和责任，也必须由法律来规定由何部门来对 CA 中心进行监管并明确监管的方法以及违规后的处罚措施。

(2) 有关保护个人隐私、个人秘密的法律。本着最小限度收集个人数据、最大限度保护个人隐私的原则来制定法律，以消除人们开展电子商务时对泄露个人隐私以及重要个人信息如信用卡账号和密码的担忧，从而吸引更多的人上网进行电子商务。

(3) 有关电子合同的法律。需要制定有关法律对电子合同的法律效力予以明确，需要对数字签名、电子商务凭证的合法性予以确认，需要对电子商务凭证、电子支付数据的伪造、变更、涂改等做出相应的法律规定。

(4) 有关电子商务的消费者权益保护法。由于网络交易中消费者和商家互不见面，消费者对商家信誉的信心只能寄托于为交易提供服务的第三方如 CA 中心和收款银行等。其中，CA 中心能够核实商家的合法身份，收款银行则能掌握商家的信誉情况。一旦因商家不付货、不按时付货或者货不符实而产生对消费者的损害时，可以由银行先行赔偿消费者，再由银行向商家追索损失，并降低商家在银行的信誉。如果商家屡次违规，银行可以取消商家电子支付的账号，并可以将商家违规情况通报给 CA 中心，由 CA 中心记入黑名单，情况严重时可以取消商家的数字证书，由此商家将失去开展电子商务的权利。

(5) 有关网络知识产权保护的法律。网络对知识产权的保护提出了新的挑战，因此在研究技术保护措施时，还必须建立适当的法律框架，以便侦测仿冒和欺诈行为，并在上述行为发生时提供有效的法律援助。

在制定电子商务法律时，要坚持灵活性和安全性的高度辩证统一。为了电子商务的安全性，必须要加快电子商务立法。但另一方面，由于电子商务还处在快速发展之中，在电子商务的很多方面(如数字身份认证)应该首先考虑行业的自律机制，以避免不灵活的或不协调的政府法规的“锁定”效应。

## 1.5 电子商务安全技术的发展

随着云计算和大数据的出现，电子商务的技术也发生了相应的变化，尤其是移动商务的飞速发展。安全方面也出现了很多新的问题。

当前，移动领域面临的安全威胁趋于多元化，手机木马的危害正由最初的扣费、耗流量

向操纵手机发送诈骗短信、隐私窃取等方向转变，具备盗取网银密码能力的手机木马也日益增加。手机木马由简单化到复杂化发展的趋势，造成了移动安全形势的日益严峻，手机用户面临更多、更危险的安全威胁。

据360互联网安全中心发布的《2014年中国手机安全状况报告》显示，2014年全年，360互联网安全中心累计截获Android平台新增恶意程序样本326万个，用户感染恶意程序3.19亿人次，骚扰电话165.9亿次，垃圾短信613亿条，移动安全的危机正在加剧。

新的互联网安全形势包括：终端安全在基础设施保护中变得更加重要；云服务的安全性已成为企业的痛处；大数据不大安全，移动设备安全也面临技术挑战等。

## 1.6 本章小结

本章详细介绍了电子商务安全的要素：可靠性、机密性、完整性、真实性、有效性、不可否认性。要保证电子商务的安全，6大要素都要保证，所有的安全技术都是为了保证这6项内容。本章还介绍了电子商务安全的主要协议标准和安全技术，这些协议和技术的综合运用可以保证电子商务的安全。读者可以把协议技术和电子商务安全要素结合起来学习。

本章也介绍了电子商务安全的体系结构，本书的全部内容都是围绕该体系结构展开的，理解该体系结构可以帮助读者整体把握电子商务安全的层次。

## 习 题 1

1. 电子商务安全要素有哪些？
2. 描述电子商务的体系结构。
3. 举例说明电子商务安全有哪些新趋势。
4. 针对移动商务的现状，了解目前存在的安全问题。