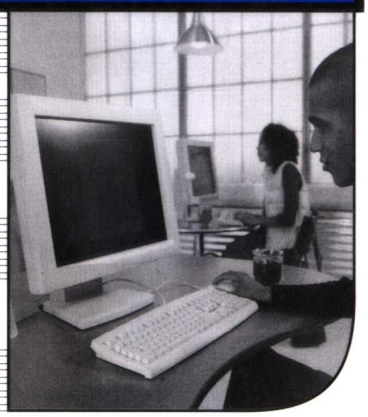
高职高专电子商务系列教材

# 计算机网络信息安全保密技术

雷咏梅 赵霖 编著
张泽增 审



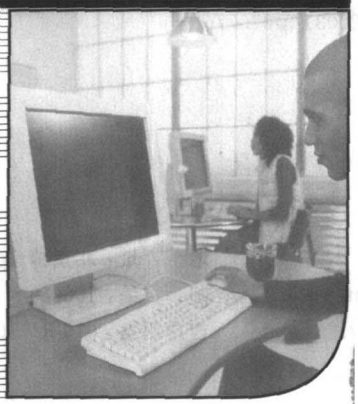


清华大学出版社

高职高专电子商务系列教材

# 计算机网络信息安全保密技术

雷咏梅 赵霖 编著
张泽增 审



清华大学出版社
北京

## 内 容 简 介

本书从实用角度讲述数据加密和身份认证技术，简要地介绍操作系统与数据库安全方面的基础知识，分析了常见操作系统的安全特性，同时对 Internet 中的安全业务和安全协议进行了介绍。本书在内容选材上从实用出发，对理解实用技术的基本原理也有充分的论述。因此，只需要读者具有基本的计算机网络知识就可以掌握本书的全部内容。

本书选材新颖，内容丰富，条理清晰，每一章都有具体的应用实例分析，便于读者学以致用。

本书可作为高职高专的教材，也可供相关专业的科技人员参考。



**图书在版编目(CIP)数据**

计算机网络信息安全保密技术/雷咏梅，赵霖编著. —北京：清华大学出版社，2003
(高职高专电子商务系列教材)
ISBN 7-302-07019-9

Ⅰ. 计… Ⅱ. ①雷… ②赵… Ⅲ. 计算机网络－安全技术－高等学校：技术学校－教材
Ⅳ. TP393.08

中国版本图书馆 CIP 数据核字(2003)第 070776 号

**出 版 者**：清华大学出版社　　**地　　址**：北京清华大学学研大厦
http://www.tup.com.cn　　**邮　　编**：100084
**社 总 机**：010-62770175　　**客户服务**：010-62776969

**组稿编辑**：王敏稚
**文稿编辑**：徐跃进
**印 刷 者**：北京国马印刷厂
**发 行 者**：新华书店总店北京发行所
**开　　本**：185×260　**印张**：12　**字数**：275 千字
**版　　次**：2003 年 9 月第 1 版　2003 年 9 月第 1 次印刷
**书　　号**：ISBN 7-302-07019-9/TP・5165
**印　　数**：1～6000
**定　　价**：16.00 元

# 高职高专电子商务系列教材

## 丛书编委会

# 序

近代人类社会经历了三次科学技术革命。每一次科技革命的爆发都会带来生产力的一次大的进步，促使社会经济形态发生变革，产业结构发生重大变化。

最新的一次科技革命始于20世纪40年代，以核技术、电子计算机和空间通信技术的发展成熟为标志，产生了原子弹、人造地球卫星等。尤其是计算机的发展不仅可以解决数学计算问题，而且作为人的脑力的扩展和肢体的延伸，直接进入了生产过程，代替了人在生产过程中的检验、调试和控制等，而微机的出现与发展又使这种扩展与延伸普及化。20世纪80年代以后，第三次科技革命进入第二阶段，网络化发展逐步走向普及，形成了信息产业和以信息技术为基础的新兴工业群，并极大地推动了社会的现代化进程。

进入21世纪以来，第三次科技革命有可能进入又一个新的阶段，这一阶段的一个重要标志之一就是因特网的应用，有人说20世纪最伟大的发明是计算机，计算机最伟大的发展是因特网，因特网最伟大的应用是电子商务。电子商务的根本性变革在于把商品流、资金流、技术流、业务流统统反映在信息流上，并由信息流来组织和支配，从而导致增值链重组，产生革命性的整合，使这一商务过程产业化。发展电子商务的关键在于人才，电子商务需要各种各样的人才，我国的信息技术发展总体上并不落后，但技术的推广速度较慢，除软、硬件等技术环境的因素外，人才的结构性矛盾较为突出，表现在缺少善于从事技术推广的职业性人才。本套教材面向高等职业教育，旨在培养从事电子商务等方面工作的技术应用性人才。

本套教材共8册，它们是：

1.《电子商务概论》；

2.《网络营销》；

3.《电子商务网站建设实例》；

4.《数据库技术及其在网络中的应用》；

5.《计算机网络信息安全保密技术》；

6.《电子商务网络技术基础》；

7.《电子商务网站建设与程序设计》；

8.《网页设计与制作》。

本套教材力求突出高等职业教育的特色，反映国内外在电子商务应用领域的最新研究成果，引入国外教学和教材编写的先进思想。在理论上有一定的深度，更注重实际应用能力的培养；在内容组织上突出从问题出发，引出概念，增强针对性；在写作上突出案例教学；在内容安排上每本教材都附有大量的实训和习题，以增强应用能力的培养。

本套教材适用于电子商务专业大学专科的高等职业教育学生，也适用于非电子商务专业的其他经济或管理的大学专科学生。同时还可用作从事电子商务技术工作或经济管理干部的培训教材或参考书。

高　林

2002 年 12 月于北京

# 前言

本书全面系统地论述了信息系统安全的基础理论及实用技术。书中围绕保障电子商务活动的安全性展开论述，包括信息加密技术、网络安全技术、系统安全技术和电子支付安全技术等保障措施。电子商务要为各参与方提供一个安全可靠的交易环境，其中一个重要的技术特征是利用IT技术来传输和处理商务信息。电子商务的安全涉及到通信网络的安全、传输信息的安全、电子资金支付的安全等方面。在电子商务中，安全是一个至关重要的问题，网上交易只有做到安全可靠，人们才能接受和使用这种交易方式。

全书分为4部分共7章。各部分内容简介如下：第一部分包括第1章和第2章，概述了计算机信息系统安全保密的重要性及研究内容，分析电子商务的安全需求，建立电子商务的安全架构；第二部分包括第3章，介绍了网络安全所需的密码学原理，包括加解密算法及其设计原理、网络加密与密钥管理，讲述传统密钥体制和公开密钥体制，论述密钥管理与加密技术的应用；第三部分包括第4章、第5章和第6章，该部分详细讲述了信息系统安全保密的实用技术，重点强调网络安全实用技术，如防火墙安全措施的应用、虚拟专用网的安全性、数字签名与数字证书等，通过对计算机病毒危害及症状的分析，论述防止病毒的常用方法，详细讲述认证机构与身份鉴别技术、操作系统的安全技术、数据库的安全保密技术等常用技术，并且对各种技术的应用进行分析，进一步指出各种技术的特征与应用范围、技术的局限性以及解决方案；第四部分包括第7章，着重论述电子商务中安全电子交易的基本原理，讲述保障支付安全所使用的核心安全技术，并且对安全电子交换协议SSL和SET进行比较分析。

本书在写作和出版过程中，得到张泽增教授的支持和帮助，他审阅了全书，作者在此表示深深的感谢。作者也在此感谢清华大学出版社为本书的顺利出版所付出的辛勤劳动。

本书选材新颖、内容丰富、条理清晰，运用大量实例生动地描述信息系统中各种安全技术的应用。基于实例和算法的讲解会使广大读者深入理解本书所讲述的内容，达到学以致用的目的。

本书可作为高职高专电子商务教材，也适合企业各部门管理人员、信息技术人员使用，亦可用作电子商务培训班的教材。

作者

2003年8月

# 目录

# 第1章 概 述

在电子计算机、通信和网络等技术迅猛发展的推动下，信息技术、信息产业和信息网络在社会经济的各个领域所发挥的作用日益突出，并逐渐主导国民经济和社会发展的过程。信息产业高速发展，成为经济发展的强大推动力；信息网络迅速崛起，成为社会经济活动的重要依托。随着全球信息化的飞速发展，我国大量建设的各种信息化系统已经成为国家的关键基础设施，其中许多业务必须与国际接轨，诸如电信、电子商务、金融网络等。

信息化在我国国民经济和社会发展中所起的作用也越来越大。随着信息化、网络化的迅速推进，非常需要保护那些存储在计算机中的文件和其他信息。对于通过数据网络进行访问的系统，这种需求更为迫切。网络信息安全问题已成为亟待解决、影响国家大局和长远利益的重大关键问题，信息安全是发挥信息革命带来的高效率、高效益的有利保证。

本章介绍关于计算机安全的一般概念，信息系统所受到的安全威胁，以及国内外的研究现状和发展趋势。

## 1.1 引 论

从古到今，人们对土地、财产和钱财进行行之有效的保护，以防止由于入侵者、窃贼或其他原因造成损失，如用城堡来保护土地，用保险箱来保护钱财。在现代社会，计算机已经深入到每个角落，人们用计算机进行通信、存储数据、处理数据，人们的工作、生活深深依赖于计算机。试想，如果计算机系统被破坏，将会出现不能存取钱，不能和远方的朋友通话，公司陷入财务混乱、人员混乱，这些损失将是不可估计的。

发展信息化，必须重视网络安全和信息安全，正确处理信息化与国家安全的关系。一方面要扩大信息交流；另一方面，必须树立高度的安全意识，采取一切措施，防范可能来自不同方面对网络和信息源的攻击和破坏，确保信息安全和国家安全。

目前，互联网已遍及全球 180 多个国家，为 1 亿多用户提供多样化的网络与信息服务。互联网是 20 世纪人类最伟大的发明之一，它已经在人类社会的诸多方面造成了影响。随着网络的深入发展，人们也逐渐意识到网络安全的重要性。现今，网络攻击活动非常频繁，从美国微软、雅虎、亚马逊到中国的新浪，黑客的攻击无处不在。据统计，全球每 20 秒发生一次黑客攻击，每日出现 5～10 种新病毒，病毒总数目前已达 40 000 种，黑客攻击手段多达 1500 种。20 世纪 80 年代，美国在互联网上的损失每年达 50 亿美元；20 世纪 90 年代每年损失已达到 70 亿美元，甚至更多；到 2000 年，仅 2 月 7 日至 10 日 3 天就损失了 12 亿美元……

美国安全服务商 Riptech 发表的关于 2002 年 1 月至 6 月计算机攻击状况的调查结

果显示，全球计算机攻击事件正在以每年64%的速度增加。

这项以30多个国家的400多家企业为对象的调查，不仅分析了计算机攻击给特定业界、个别企业带来影响，而且对整体因特网业界计算机攻击的新动向进行了分析。

因此，必须充分意识到网络安全的重要性。应该了解互联网世界中有关安全的基本情况，知道互联网上的个人数据和通信记录随时都有可能被公布于众或被滥用，我们必须防患于未然。

## 1.2 什么是计算机安全

由于计算机信息有共享和易于扩散等特性，它在处理、存储、传输和使用上有着严重的脆弱性，很容易被干扰、滥用、遗漏和丢失，甚至被泄露、窃取、篡改、冒充和破坏，还有可能受到计算机病毒的感染。

信息安全涉及信息的秘密性(confidentiality)、完整性(integrity)、可用性(availability)、可控性(controllability)。综合起来说，就是要保障电子信息的有效性。保密性就是对抗对手的被动攻击，保证信息不泄露给未经授权的人；完整性就是对抗对手主动攻击，防止信息被未经授权的篡改；可用性就是保证信息及信息系统确实为授权使用者所用；可控性就是对信息及信息系统实施安全监控。

计算机安全的内容应包括两方面：即物理安全和逻辑安全。物理安全指系统设备及相关设备受到物理保护，免于破坏、丢失等。逻辑安全包括信息完整性、保密性和可用性：

- 保密性指高级别信息仅在授权情况下流向低级别的客体与主体；
- 完整性指信息不会被非授权修改及信息保持一致性等；
- 可用性指合法用户的正常请求能及时、正确、安全地得到服务或回应。

一个系统存在的安全问题可能主要来源于两方面：或者是安全控制机构有故障；或者是系统安全定义有缺陷。前者是一个软件可靠性问题，可以用优秀的软件设计技术配合特殊的安全方针加以克服；而后者则需要精确描述安全系统。

目前有关计算机信息系统安全的定义不一，国际标准化组织(ISO)的定义如下：

“所谓计算机安全，是指为数据处理系统建立和采取的技术和管理的安全保护，保护计算机硬件、软件和数据不因偶然和恶意的原因而遭到破坏、更改和泄露”。此概念偏重于静态信息保护。

也有人将“计算机安全”定义为：“计算机的硬件、软件和数据受到保护，不因偶然和恶意的原因而遭到破坏、更改和泄露，系统连续正常运行。”该定义着重于动态意义描述。

由于现代的数据处理系统都是建立在计算机网络基础上的，计算机网络安全也就是信息系统的安全，即利用网络管理控制和技术措施，保证在一个网络环境里，信息数据的机密性、完整性和可使用性受到保障。

从计算机信息系统形态和运行过程出发，可把安全内容分为：实体安全、运行安全、信息安全和管理安全4个方面。

实体安全是指保护计算机设备、设施(含网络)以及其他媒体免遭地震、水灾、有害气体和其他环境事故(如电磁污染等)破坏的措施、过程。保护计算机系统的全部硬件及计

算机辅助设备的安全，包括计算机房地理环境的选择、建筑结构、布局各种防火、防盗措施及手段。

运行安全是指为保障系统功能的安全实现，提供一套安全措施（如安全评估、审计跟踪、备份与恢复、应急措施等）来保证信息处理过程的安全。

信息安全是指防止信息资源被故意的或偶然的非授权泄露、更改、破坏，或使信息被非法系统辨识、控制和否认。即确保信息的完整性、秘密性、可用性、可控性和不可否认性。

信息安全包括软件安全和数据安全。软件安全是指软件的防复制、防篡改、防非法执行等。数据安全是指计算机中的数据不被非法读出更改、删除等。它是计算机安全的关键。

几乎所有的计算机犯罪，都是对数据进行非法操作。要想保持长久平安就必须防患于未然，问题是现在以及将来可以做什么以保护自己的数据。

网络信息既有存储于网络节点上的信息资源，即静态信息，又有传播于网络节点间的信息，即动态信息。而这些静态信息和动态信息中有些是开放的，如广告、公共信息等；有些是保密的，如私人间的通信、政府及军事部门的机密、商业机密等。网络信息安全一般是指网络信息的秘密性、完整性、可用性及真实性。网络信息的秘密性是指网络信息的内容不会被未授权的第三方所知。网络信息的完整性是指信息在存储或传输时不被修改、破坏，不出现信息包的丢失、乱序等，即不能为未授权的第三方修改。信息的完整性是信息安全的基本要求，破坏信息的完整性是影响信息安全的常用手段。当前，运行于互联网上的协议（如 TCP/IP 等），能够确保信息在数据包级别的完整性，即做到了传输过程中不丢信息包，不重复接收信息包，但却无法制止未授权第三方对信息包内部的修改。网络信息的可用性包括对静态信息的可得到和可操作性，以及对动态信息内容的可见性。网络信息的真实性是指信息的可信度，主要是指对信息所有者或发送者的身份的确认。

前不久，美国计算机安全专家又提出了一种新的安全框架，包括秘密性、完整性、可用性、真实性、实用性、占有性，即在原来的基础上增加了实用性、占有性，认为这样才能解释各种网络安全问题。网络信息的实用性是指信息加密密钥不可丢失（不是泄密），丢失了密钥的信息也就丢失了信息的实用性，成为垃圾。网络信息的占有性是指存储信息的节点、磁盘等信息载体被盗用，导致对信息的占用权的丧失。保护信息占有性的方法有使用版权、专利、商业秘密性，提供物理和逻辑的存取限制方法，维护和检查有关盗窃文件的审查记录、使用标签等。

管理安全是指通过采用有关的法律法令、规章制度以及安全管理手段，确保系统安全运营。管理手段是对安全服务和安全机制进行管理，把管理信息分配到有关的安全服务和安全机制中去，并收集与它们的操作有关的信息。

计算机安全是一个非常重大的问题，这是一个值得计算机专家、管理人员、甚至用户研究的领域。学习的目的是了解计算机中的安全问题是什么，以及采用什么方法来处理这些问题。

随着计算机的发展，计算机硬件、软件技术的进步，计算机应用技术的广泛使用，如信息高速公路，Internet、信息战等，影响安全的一个主要原因是分布式系统的引入以及网络

和通信设施的使用。这些网络和通信设施用来在终端用户与计算机之间以及计算机与计算机之间传输数据。在数据传输过程中需要用网络安全措施来保护数据。例如，对于信息系统最为引人注目的攻击形式之一是计算机病毒。某病毒可能通过一张软盘被引入一个系统，进而加载于一台计算机，也可能通过互联网进入计算机。无论在哪种情况下，一旦该病毒驻留于一个计算机系统，就需要使用内部计算机安全工具来监测和清除病毒。

虽然采用了防火墙技术，但是网络病毒很猖獗，如 CIH 病毒、美丽沙病毒、求职者病毒等都造成了很大危害和损失。因此，非常需要用自动化的工具来保护那些存储在计算机中的文件和其他信息，这对一个共享系统（如分时系统）则更为必要。对于那些能够通过公用电话或数据网络进行访问的系统，这种需求尤为迫切。计算机安全同时也包括了设计用来保护数据、阻挡黑客的工具集合。

计算机安全的主要目标是保护计算机资源免受毁坏、替换、盗窃和丢失，这些计算机资源包括计算机设备、存储介质、软件和计算机数据等。计算机安全包括广泛的策略和解决方案，具体内容如下所示。

**1. 访问控制**

对人们访问计算机系统进行控制，只允许合法用户使用计算机系统，而把非法用户拒之门外，这就像守在大楼门口的门卫一样，对进入大楼的人进行安全检查。

**2. 选择性访问控制**

对不同的合法用户授予不同的权力，使他们具有不同的系统资源访问权力，如一个非正式用户就不能访问敏感性数据，而系统的管理者——系统管理员对系统具有全面的控制。还有，如果用户 A 想对他的目录下的数据进行保密，则用户 A 可以控制其目录，不让其他用户访问他的目录。

**3. 防御计算机病毒**

病毒对计算机系统具有很大程度的破坏性，这是计算机安全长期要面对的问题。

**4. 加密**

加密就是把数据转换成不可读的形式，并在必要时再转换回来，这可以保证只有被授权的人才能阅读该信息。

**5. 系统计划和管理**

计划、组织和管理计算机设备，并根据用户的要求制定安全策略并实施。它就像企业管理的其他部分一样，具有十分重要的意义。

**6. 物理安全**

保证计算机装置和设备的安全，防止非法人员进入机房对计算机设备进行破坏，或直接窃取机密信息。

**7. 生物统计学**

用生物惟一性特征来识别用户，如指纹、视网膜和声音等。

**8. 网络和通信安全**

这是计算机安全中很重要的一部分，网络入侵、窃听都属于这个范畴。

计算机安全在现代企业中有着极其重要的地位，但它常常被人们忽略，并在灾难发生后令人追悔莫及。例如，网站被黑客入侵，并受损破坏，导致了网站服务的关闭。这种危害似

乎并不严重，但是经常被黑客破坏的站点，怎么能吸引到众多稳定的访问者呢？这种损失不但是经济上的，也是商业名誉上的。再如，某公司的投标计划被竞争对手劫获，该公司就可能失去一次绝好的商业机会。一个企业的计算机系统遭受水灾或火灾，公司财务数据全部被损害，如果该企业对数据没有很好地保护和备份措施，公司可能就此不能开业了。

总之，计算机安全就是一个组织机构本身的安全。

为了有效评估一个机构的安全需求以及评价和选择各种安全产品的策略，负责安全需求的管理员需要采用某些系统方法来定义安全需求和表达满足这些需求的方法。常用的一种方法是考虑信息安全性的 3 个方面。

- 安全攻击：危及由某个机构拥有的信息安全的任何行为。
- 安全机制：设计用于检测、防止安全攻击的一种机制。
- 安全服务：加强一个组织的数据处理系统和信息传送安全性的一种服务。该服务的目的是对抗安全攻击，它们利用一种或多种安全机制来提供该服务。

## 1.3　计算机系统受到的安全威胁

### 1.3.1　对安全的攻击

任何一个信息网络系统都存在有限的边界，并且由具体的硬件设备、系统软件、服务功能、数据资源和网络用户等几个基本元素所构成。分析网络安全风险必然要从以上的基本构成元素入手。

从广泛的意义上讲，网络安全风险可以划分为自然灾害威胁、电子系统故障、人工操作失误和人为蓄意破坏 4 个方面。应用单纯的技术手段可以对前 3 个方面的风险实施有效的防御和控制；而对于人为蓄意破坏，必须像对待社会上的违法犯罪活动一样，采取多种技术和行政手段，进行预防和制止。本章将对安全风险进行深入分析，提出切实的安全对策。

对互联网络的攻击包括对静态数据的攻击和对动态数据的攻击。对静态数据的攻击主要有：

- 口令猜测，通过穷举方式搜索口令空间，逐一测试，得到口令，进而非法入侵系统；
- IP 地址欺骗，攻击者伪装成源自一台内部主机的一个外部地点传送信息包，这些信息包中包含有内部系统的源 IP 地址，冒名他人，窃取信息；
- 指定路由，发送方指定一信息包到达目的站点的路由，而这条路由是经过精心设计的、绕过设有安全控制的路由。

根据对动态信息的攻击形式不同，可以将攻击分为主动攻击和被动攻击两种。

对一个计算机系统或网络安全的攻击，最好通过观察正在提供信息的计算机系统的功能来表述。一般而言，一个信息流从一个源（例如，另一个文件或主存储器的一个区域）流到一个目的地（例如，另一个文件或主存储器的一个区域），正常流动如图 1-1 所示。


图 1-1　信息的正常流动