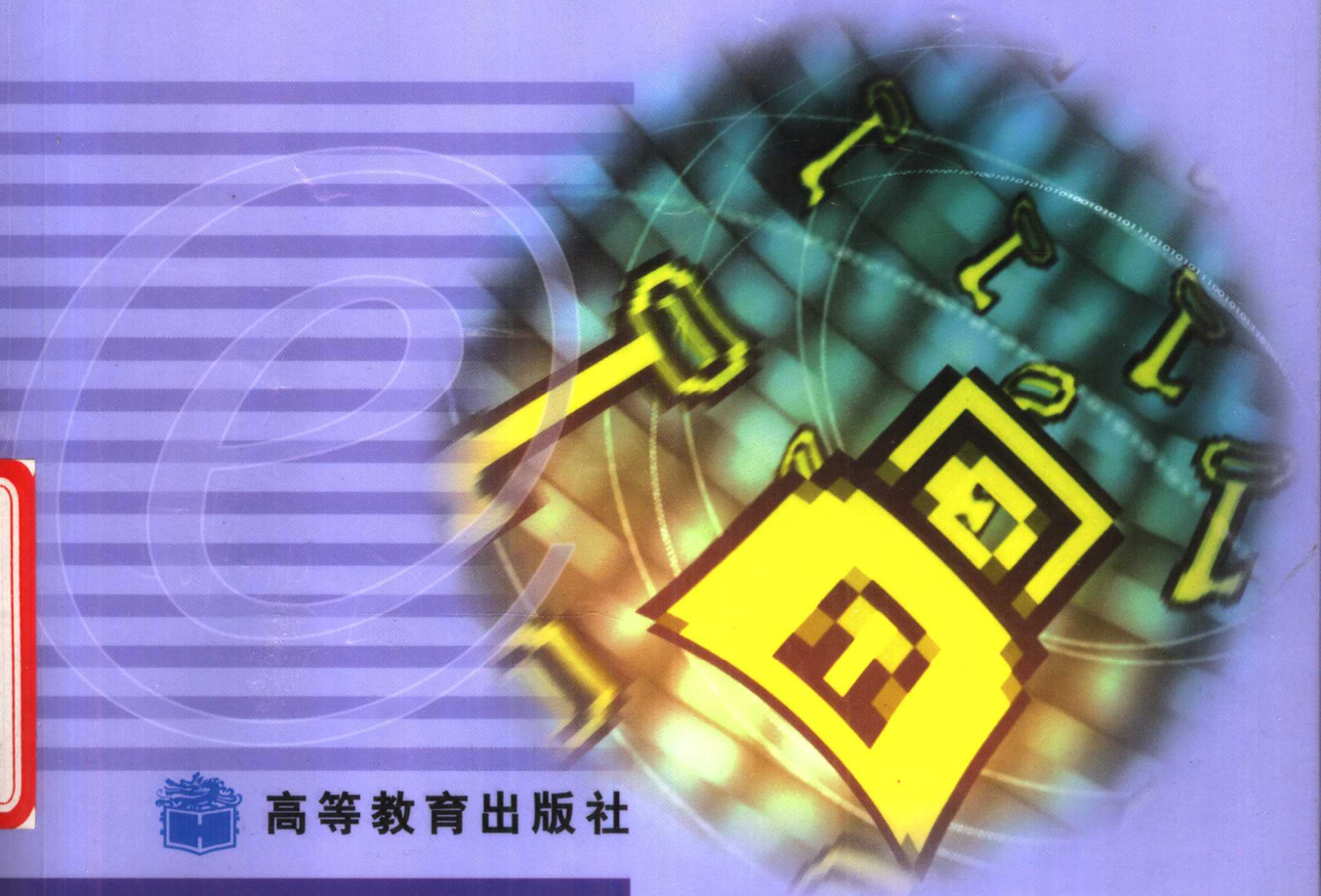
教育部高职高专规划教材
Jiaoyubu Gaozhi Gaozhuan Guihua Jiaocai

计算机网络安全

林 海 杨晨光 顾巧论 许 彦



高等教育出版社

教育部高职高专规划教材

计算机网络安全

林 海 杨晨光 顾巧论 许 彦 编著

高等教育出版社

内容提要

本书是教育部高职高专规划教材。本书全面地阐述了计算机网络安全的各种问题，包括电子商务对网络安全的需求，网络安全的模型、机制和服务，建立网络安全系统的实际步骤和方法，常见的网络平台的各种漏洞和修补的方法，网络物理环境的安全问题，病毒和黑客攻击的防范，防火墙的种类以及选购和配置的原则，数据库的安全、备份和灾难恢复，数据加密的原理和方法，认证的作用和功能，我国有关网络安全的法律法规和管理制度，等等。

本书是高等职业学校、高等专科学校、成人高等学校电子商务专业、信息安全专业、计算机网络专业的教材，也可以作为从事计算机系统集成、网站建设和管理、网络安全服务的工程师和项目管理人员的参考书或在校大学生和社会青年的自修读物。

图书在版编目(CIP)数据

计算机网络安全 / 林海等编著. —北京：高等教育出版社，2001.7

ISBN 7-04-010467-9

Ⅰ. 计… Ⅱ. 林… 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（2001）第 088518 号

责任编辑 李 慧 **封面设计** 王凌波 **责任绘图** 尹 莉
版式设计 周顺银 **责任校对** 康晓燕 **责任印制** 杨 明

计算机网络安全
林 海 杨晨光 顾巧论 许 彦 编著

出版发行	高等教育出版社	**购书热线**	010－64054588
社 址	北京市东城区沙滩后街 55 号	**免费咨询**	800－810－0598
邮政编码	100009	**网 址**	http://www.hep.edu.cn
传 真	010－64014048		http://www.hep.com.cn
经 销	新华书店北京发行所		
印 刷	中国农业出版社印刷厂		
开 本	787×1092 1/16	**版 次**	2002 年 7 月第 1 版
印 张	14.75	**印 次**	2002 年 7 月第 1 次印刷
字 数	350 000	**定 价**	18.80 元

本书如有缺页、倒页、脱页等质量问题，请到所购图书销售部门联系调换。

教育部高职高专规划教材

电子商务系列

电子商务概论	费名瑜
电子商务实用教程	宋文官
知识型企业管理	汪　治
网络营销	钱东人
连锁配送网络技术	高海辰
国际贸易实务	刘文广
国际金融	孙连铮
证券投资	孙可娜
EDI 实务与操作	吉庆彬
数据库应用技术	铁　军
计算机网络安全	林　海
网页制作实用教程	陈建红
图形与动画设计	周　力
电子商务解决方案	费名瑜

出版说明

教材建设工作是整个高职高专教育教学工作中的重要组成部分。改革开放以来，在各级教育行政部门、学校和有关出版社的共同努力下，各地已出版了一批高职高专教育教材。但从整体上看，具有高职高专教育特色的教材极其匮乏，不少院校尚在借用本科或中专教材，教材建设仍落后于高职高专教育的发展需要。为此，1999 年教育部组织制定了《高职高专教育基础课程教学基本要求》（以下简称《基本要求》）和《高职高专教育专业人才培养目标及规格》（以下简称《培养规格》），通过推荐、招标及遴选，组织了一批学术水平高、教学经验丰富、实践能力强的教师，成立了“教育部高职高专规划教材”编写队伍，并在有关出版社的积极配合下，推出一批“教育部高职高专规划教材”。

“教育部高职高专规划教材”计划出版 500 种，用 5 年左右时间完成。出版后的教材将覆盖高职高专教育的基础课程和主干专业课程。计划先用 2~3 年的时间，在继承原有高职、高专和成人高等学校教材建设成果的基础上，充分汲取近几年来各类学校在探索培养技术应用性专门人才方面取得的成功经验，解决好新形势下高职高专教育教材的有无问题；然后再用 2~3 年的时间，在《新世纪高职高专教育人才培养模式和教学内容体系改革与建设项目计划》立项研究的基础上，通过研究、改革和建设，推出一大批教育部高职高专教育教材，从而形成优化配套的高职高专教育教材体系。

“教育部高职高专规划教材”是按照《基本要求》和《培养规格》的要求，充分汲取高职、高专和成人高等学校在探索培养技术应用性专门人才方面取得的成功经验和教学成果编写而成的，适用于高等职业学校、高等专科学校、成人高校及本科院校举办的二级职业技术学院和民办高校使用。

教育部高等教育司

2000 年 4 月 3 日

前　言

互联网的迅猛发展所推动的全球信息化的浪潮，深刻地改变着社会的面貌和人们的生活方式。电子商务、政府上网、远程教育、信息战等竞相崛起。然而，互联网和信息化在带来繁荣与进步的同时，也带来了烦恼与不安。网上垃圾泛滥，谣言四起，病毒猖獗，黑客横行，数据丢失，秘密泄露，信道阻塞，系统瘫痪，造成的损失难以估量。网络安全问题已经引起了人们普遍的关注，它不仅关系到个人的权益和企业的兴衰，而且关系到社会的稳定和国家的安全。随着加入 WTO，我国必然更深地融入全球信息化的进程，安全问题也必将更为急剧地凸现出来。具备网络安全知识和技能的专门人才为社会所急需。

本书囊括了网络安全的方方面面。第 1 章“电子商务与网络安全”分析了电子商务对网络安全的需求，从理论上阐述了网络安全的模型、机制和服务，并给出了建立网络安全系统的实际步骤和方法。第 2 章“网络平台漏洞与安全”指出了常见的三种网络平台的各种漏洞和修补的方法。第 3 章“物理与环境安全”列举了网络的物理与环境的安全问题，这些基本的安全问题所带来的致命的危害往往被某些安全专家所忽视。第 4 章“病毒与黑客攻击的防范”分析了病毒和黑客的斑斑劣迹，指出了防范的措施。第 5 章“防火墙”介绍了防火墙的种类以及选购和配置的原则。第 6 章“数据库的安全、备份和灾难恢复”谆谆告诫如何保护你的数据。第 7 章“加密与认证”深入浅出地阐述了最常用的几种加密方法，介绍了认证的作用和功能。第 8 章“法律法规和管理制度”介绍了我国有关网络安全的法律法规和管理制度。网络安全不是单纯地依托于某一学科的技术，尤其它不是简单地等同于数据加密技术，而是综合了法律、管理、技术、服务等要素的新的领域，本书的结构和内容生动地体现了这一观念。

本书作为高等职业学校电子商务专业、信息安全专业、计算机网络专业的教材，坚持实用第一的原则，以学生的素质和能力的培养为中心。在理论的阐述上尽可能通俗易懂，在实际操作上尽量详细而具体。开设“计算机网络安全”课程的学校应当有相应的实验室或实训基地，实验和实训的课时要占 40%以上。

本书可以作为从事计算机系统集成、网站建设和管理、网络安全服务的工程师和项目管理人员的参考书，也可以作为对网络安全问题有兴趣的各个专业的在校大学生和社会青年的自修读物。

编者

2001 年 11 月

目　录

第 1 章　电子商务与网络安全

1.1　什么是网络安全

1.1.1　电子商务的网络环境

1. 互联网

互联网的出现与发展是上个世纪末人类生活中最具影响的重大事件之一。

根据 Global Reach（网址：www.glreach.com）2001 年 9 月的全球在线统计，全球上网用户为 5.05 亿，其中使用英语的用户数为 2.20 亿，占全球上网用户总数的 43.9%，非英语用户数为 2.93 亿，占全球上网用户总数的 57.0%，在非英语用户中，使用汉语的用户数为 4 750 万，占全球上网用户总数的 9.2%。估计到 2003 年，全球上网用户为 7.9 亿，其中使用英语的用户数为 2.3 亿，占全球上网用户总数的 29.1%，非英语用户数为 5.6 亿，占全球上网用户总数的 70.9%，在非英语用户中，使用汉语的用户数为 1.6 亿，占全球上网用户总数的 20.3%。

根据 Internet 网络信息中心的统计，全球已注册域名 35 244 448 个，其中以 .com 注册的公司域名为 21 285 794 个。中国大陆以.cn 注册的域名 106 272 个，中国台湾以 .tw 注册的域名 36 546 个，澳门以 .mo 注册的域名 395 个，香港不详。

另据香港政府的资讯科技及广播局的统计资料，全港所有住戶中，49.7%的家庭中有个人电脑，其中 73.3%的个人电脑已接入互联网，37.3%的机构单位已联接互联网。1999 年，所有机构单位通过电子途径售卖产品、服务或资料而获得的业务收益合计为 46 亿元港币。

根据中国互联网络信息中心（CNNIC）2001 年 7 月 1 日在北京发布的《中国互联网络发展状况统计报告》，截止到 2001 年 6 月 30 日止，我国上网计算机数约有 1 002 万台，其中专线上网计算机 163 万台，拨号上网计算机 839 万台。我国上网用户人数约 2 650 万人，其中专线上网的用户人数约为 454 万，拨号上网的用户人数约为 1 793 万，同时使用专线与拨号的用户人数为 403 万，除计算机外同时使用其他设备（移动终端、信息家电等）上网的用户人数为 107 万。CN 下注册的域名总数为 122 099 个，WWW 站点数（包括.CN，.COM，.NET，.ORG 下的网站）约为 265 405 个，我国国际线路的总容量为 2 799 MB。

2. 电子商务

互联网的迅猛发展极大地改变了人类的生活方式，给世界的经济、政治、文化带来了深刻的影响。在这种背景之下，电子商务的异军突起掀起了网络上的浩荡风云。这首先是由于，互联网加速了经济全球化的进程，人们通过网络可以更快、更省地处理经济事务，大大减少了交易费用，节余了更多的社会财富。其次，互联网极大地拓展了市场交易的时间和空间，创造

了更多的市场交易机会，为经济的发展起到了推波助澜的作用。互联网可以帮助人们挖掘潜在的市场需求，甚至在创造着人类前所未有的新需求，例如创造和激发了巨大的信息消费市场。同时，互联网还创造了互联网基础建设、互联网应用、互联网中介、互联网商务等市场需求。这些新增长的需求必然带来更多的就业机会。再次，互联网促进竞争、促进创新，提高整个社会资源的配置效率。互联网使每一个厂商都面临着同样的全球化的市场，自由竞争将导致经济资源的优化配置，极大地推动经济的发展。这是由于互联网使得供需双方的信息能够充分流通，减少双方的信息不对称、不完全状况，从而为资源的最优配置创造了必要的条件，也十分自然地优化着社会资源的配置。

根据贝克利大学世界经济圆桌会议的报告，2000 年的全球网络购物和网络交易额已达 4 200 亿美元，2003 年估计将超过 3 万亿美元。

面对这样一个巨大的市场，世界各国无不磨拳擦掌，惟恐裂肉分羹之不及。美国作为网络技术和应用最先进的经济发达国家，正逐步加强自己在世界经济中的霸主地位。欧洲各国也不甘落后，1999 年 12 月 7 日，欧盟 15 国在布鲁塞尔召开部长级会议，通过了《欧盟电子商务统一法》，明确规定凡在一个成员国签署的有关电子商务合同，其法律效力在欧盟其他成员国都将得到承认，以此推动电子商务在欧洲的发展。2001 年 2 月 15 日，德国议会通过了使电子签名具有与手写签名同样的法律效力的议案，用电子签名签订的合同将具有同样的合法性，这使德国成为第一个电子签名合法化的欧洲国家。目前欧元区信息技术部门共雇佣了 80 万人，至 2020 年还将创造 75 万个就业机会。日本则于 1999 年推出纲领性文件《迈向 21 世纪的数字经济》，并投资几十亿美元发展本国的电子商务。新加坡政府把推动电子商务作为 21 世纪的经济发展策略，并立志将新加坡建设成为国际电子商务中心。随着我国加入 WTO 的日子的到来，在国际经济贸易的竞争更加激烈、机遇与挑战并存的时代，如果我国能够及时调整对策，变革传统的贸易方式，我们将在 21 世纪国际贸易竞争中有望占有我们应得的市场份额，由此将对我国的经济发展、社会稳定和人民的生活幸福产生深远的影响。

3. 网络安全

互联网为电子商务铺设了四通八达的道路，但是在这些道路上不是很安全，而是危机四伏、险象环生。当然，我们不能因为路上不太安全，就关张落板，缩回到“老死不相往来”的封闭时代。我们要做的是权衡利弊，评估风险，以适当的代价，建立起电子商务的安全系统，争取在电子商务活动中获得较高的收益。

说到安全，我们满耳朵灌进来的是各种各样的令人头昏的字眼。诸如“网络安全”、“信息安全”、“计算机安全”、“数据安全”，等等。界定这些名词的内涵与外延，是语义学专家们的事情。我们也不想从那些难以咀嚼的定义出发，来圈定本书的内容。

我们的想法是很直接、很朴素的，经过调查研究，从电子商务的实际需要出发，来组织本书的内容。电子商务在网络上遇到的安全问题是错综复杂的，我们经过梳理，勾画出本书的轮廓，方方面面有关安全的问题尽量都要点到，做适当的介绍。这本书作为高职高专学校电子商务等专业的教材，我们的目的不是去探讨高深的网络理论，而是要引导学生通过实践获得切合实际需要的知识和能力。

针对危害安全的某些因素，我们采取了相应的安全措施。也许由于我们的安全措施存在某些遗漏或缺陷，一些不安全因素会得以扩张它的危害，我们必须想法弥补和加固我们的防护

堤坝。然而，新的不安全因素是会在你一眨眼之间随时出现的，维护系统安全的战斗将永不停息。因此，本书并没有企图罗列若干万无一失的安全解决方案，以为铸造几个坚固的铁壳就可以钻在里面高枕无忧了，而是着眼于培养学生分析问题、解决问题的能力，去应对不断出现的新挑战。

1.1.2 网络安全隐患分析

电子商务之所以非要在危机四伏、险象环生的网络环境中谋求生存，其根本原因出自以下的四大矛盾：

（1）商务活动要求广泛的互联而不能与世隔绝，然而这也给盗贼的潜入架桥开路；

（2）网络的体系结构和协议以及计算机的操作系统为互联就必须开放，然而这也给病毒制造者和黑客们尽数亮开了家底；

（3）电子商务的操作必须简单、方便，然而这就给严格的安全检查出了难题；

（4）互联网的建立的初衷是友善的交流、合作、资源共享，它的结构和协议也不曾想到什么安全不安全，然而谁曾料想美好的乌托邦竟然成为刀光剑影的打斗场。

网络安全的隐患主要来自操作系统、网络和数据库的脆弱性以及安全管理上的疏忽。

1. 操作系统的脆弱性

操作系统为了系统集成和系统扩张的需要，采用了支持动态联接的系统结构。系统的服务和 I/O 操作都可以用打补丁的方式进行动态联接。打补丁的方法为黑客们所熟知，也是病毒孳生的营养缸。

操作系统的进程是可以创建的，而且这种进程可以在远程的网络节点上创建和激活，更加要命的是被创建的进程还继承了再创建进程的权力。这样，黑客们在远程把间谍补丁打在一个合法用户特别是超级用户的身上，就能够逃脱系统作业与进程的监视程序的眼睛。

操作系统为维护方便而预留的免口令入口和各种隐蔽通道，实际上也是黑客们进出的方便之门。

操作系统提供的具有与系统核心层同等权力的 daemon 软件和远程过程调用（RPC）服务、网络文件系统（NFS）服务，以及 Debug、Wizard 等工具，更是黑客们翻云覆雨的百宝囊。

2. 计算机网络的脆弱性

互联网的体系结构和 TCP/IP 协议在创建之时并没有适当地考虑安全的需要，因而存在着许多安全漏洞和根本性的缺陷，给攻击者留下了可乘之机。计算机网络安全的脆弱性主要表现在以下几个方面。

1）很容易被窃听和欺骗

数据包在互联网上传输的时候，往往要经过很多个节点的重发。而在局域网内，通常采用的以太网或令牌网技术都是广播类型的，这样，窃听者便可以轻而易举地得到你的数据包。如果你的数据包没有强有力的加密措施，就等于把信息拱手送给了窃听者。比较陈旧的域名系统（DNS）服务软件易受虚假的 IP 地址信息的欺骗。另外一种 IP 地址的欺骗方式是在阻塞了受害的某台主机后再用受害者的 IP 地址在网络上冒充行骗。

2）脆弱的 TCP/IP 服务

基于传送控制协议/互联网间协议（TCP/IP）的服务很多，最常用的有万维网（WWW）、

文件传输协议（FTP）、电子函件（E-mail），此外还有简单文件传输协议（TFTP）、NFS、Finger等，它们都存在着各种各样的安全问题。WWW服务所使用的通用网关接口（CGI）程序、Java Applet小应用程序和SSI都有可能成为黑客的得力工具。FTP的匿名服务有可能浪费甚至耗尽系统的资源。TFTP则无安全性可言，它常被用来窃取口令文件。E-mail的安全漏洞曾经导致蠕虫病毒在互联网上的蔓延。E-mail的电子炸弹和附件里经常携带的病毒严重地威胁着互联网的安全。至于Linux的X Windows服务、基于RPC的NFS服务、BSD Unix的“r”族服务如rlogin，rsh，rexec等，如果你在配置防火墙时忘记了关闭它们在互联网上的使用，那么你的内部网络就等于裸露在黑客们的面前。

3）配置的错误和疏忽

由于网络系统本身的复杂性，配置防火墙是一件相当复杂的事情。在没有更好的辅助工具出现之前，缺乏训练的网络管理员很有可能发生配置错误，给黑客造成可乘之机。在系统配置时过于宽容，或者由于对某些服务的安全性了解不够而没有限制或禁止这些不安全的服务，或者对于某些节点的访问要求给予太多的权力，都会给安全带来危害。

3. 数据库管理系统脆弱性

数据库管理系统（DBMS）主要通过用户的登录验证、用户的权限、数据的使用权限以及审计功能提供安全性能。但是黑客通过探访工具强行登录和越权使用数据库的数据，有可能带来巨大的损失。对数据进行加密可以提高安全性，但是加密往往与数据库管理系统的功能发生冲突或者影响了数据库的运行效率，不一定总是可行。使用“服务器—浏览器”结构的网络应用程序因为由应用程序直接对数据库进行操作，应用程序的某些缺陷有可能威胁到数据库的安全。使用“数据库—服务器—浏览器”的三层结构的应用程序通过标准的工具对数据库进行操作，其安全性有所加强。数据库的安全等级应当与操作系统的安全等级相适应，否则缺口会首先从最薄弱的环节打开。

系统管理员对系统和数据库的绝对的控制权力也是安全的一个突出问题。作为一个系统管理员，他有权查阅和删改任何敏感数据，系统对他的权力没有任何约束，这就可能出事。应当实行系统管理员、安全员、审计员三权分立的互相制约的机制。而且这种机制必须得到操作系统和数据库管理系统的支持才能生效。

4. 安全管理的不力

调查表明，国内的多数计算机网络，都缺少经过正规教育和训练的专职的网络安全管理员，缺少网络安全管理的技术规范，没有定期的安全测试和检查，更没有安全监控。甚至有许多网络已经运行多年了，而系统管理员和用户的登录名字和口令还是缺省状态未予改动。对于病毒和黑客们来说，这些网络真是漏洞百出、不堪一击。

1.1.3 危害网络安全的典型案例

世界上第一个病毒程序是在1983年11月由Fred Cohen博士研究出来的。它潜伏在DEC公司的VAX 11/750型计算机系统上，具有自我复制能力，当它在一定条件下发作时，具有一定的破坏性。从此，在神奇美丽的计算机王国里，开始了一场挥之不去的恶梦。

1988年11月3日，由Cornell大学的23岁的研究生Robert Morris制造的“蠕虫”病毒感染了当时的互联网上将近1/10的6 000多台计算机，使网络陷入瘫痪，造成的经济损失估计

在 1 500 万到 1 亿美元。Robert Morris 也因此被判 3 年监禁缓刑，罚款 1 万美元和做 400 小时的社区服务。Robert Morris 的父亲老 Morris 是一个对互联网的创立做出杰出贡献的工程师，他服务于美国国家安全局。Robert Morris 以自己的“蠕虫”盖过了他父亲的一代英名。

最离奇的一个案例是 Randal Schwartz。他是一个 在编程方面特别是 Perl 语言上功绩彰著的优秀程序员。1993 年他在俄勒冈州为 Intel 公司工作，作为系统管理员维护计算机系统的安全。他为网络安全而安装了一个 Crack 工具软件，这个工具软件可以用来破译 Unix 中的密码和网络口令。1993 年 10 月 28 日，另一个系统管理员发现了这个 Crack 软件，并于 4 天后向警方作证而导致 Schwartz 被捕，罪名是违反了俄勒冈州的计算机犯罪条例。

1995 年，俄罗斯的列文（Левин）在英国被捕。他被指控使用笔记本电脑从纽约的花旗银行非法转移至少 370 万美元到他自己的账户。后来列文被引渡到了美国，被判处 3 年监禁。花旗银行除了蒙受了经济损失之外，尤其严重的是商业信誉上的损失。当时就有 6 家竞争对手立即利用这个事件游说花旗银行最大的 20 个客户改换门庭。有许多金融和商业机构在遭受黑客袭击时却严格保密不敢露出风声，惟恐因为自己的计算机网络系统的安全缺陷而导致丢失自己的客户。

1998 年我国某银行的网络管理员郝金龙和他的弟弟内外勾结，在银行的电脑终端机植入一个控制软件，同时用各种化名在该银行开设了 16 个账户。他们利用这个软件将虚拟的 720 000 元人民币电汇划入银行账户，之后从该银行的 8 个分行提取真实的人民币 260 000 元。后来，郝金龙兄弟 2 人被江苏省扬州市人民法院依法判处了死刑。

每年 4 月 26 日发作的 CIH 病毒感染了全球 6 000 万台计算机。这种病毒是一种恶性的病毒，它发作时能用垃圾数据填充硬盘而毁坏所有文件和数据，尤其可恶的是它能改写 Flash 芯片的基本输入输出系统（BIOS）程序，使计算机完全瘫痪。CIH 病毒是台湾大同工学院的 4 年级的学生陈盈豪在 1998 年制作的。当年因为无人起诉，警方不能采取行动，使陈盈豪长期逍遥法外。毕业后在台军方服役，曾扬言要制作针对大陆的简体汉字系统的病毒。1999 年 4 月 30 日，有 CIH 病毒受害者曾先生起诉陈盈豪，陈被台北警方逮捕。

2000 年 2 月在 3 天的时间里，来自世界各地的黑客攻击了美国的数家顶级网站，包括 Yahoo，Amazon，eBay，CNN 等。黑客们用大量的垃圾信息阻塞了网站的服务器，使其无暇为用户提供正常的服务而陷入瘫痪，称为“拒绝服务”攻击。一时间，引起这些顶级网站的股票一路下跌。

2000 年 5 月 4 日，一种称为“爱虫”（ILoveYou）的电脑病毒开始在全球迅速蔓延，短短的一两天内就侵袭了 100 多万台计算机。美国和欧洲的计算机系统损失尤为惨重。“爱虫”病毒通过电子邮件传播，与 1999 年席卷美国的“梅丽莎”病毒类似。它的攻击对象是使用微软视窗操作系统及 Outlook 电子邮件系统的计算机。这种病毒能删除计算机上的部分文件，并制造大量新的电子邮件，使用户文件泄密、网络负荷剧增。英国约有 10%的企业遭到了它的攻击，英国劳埃德银行估计，这一病毒将给英国造成数千万英镑的损失。美国参议院、国务院和国防部、美国在线一时代华纳公司等诸多机构也受到“爱虫”病毒的攻击。在瑞士，“爱虫”病毒袭击了瑞士通讯社、法语广播电台等机关和企业，甚至苏黎世州警察局也未能幸免。另外，在 4 日德国至少有 5 万台电脑被传染上“爱虫”病毒，丹麦议会、丹麦电信局和挪威一家电视台都宣布受到“爱虫”病毒的侵害。追查“爱虫”病毒扑簌迷离。有人说是菲律宾的一些

黑客，也有人说是一名在澳大利亚学习的名叫迈克尔的德国学生。

物理上的破坏也严重地威胁着网络的安全。我们经常可以反复看到一些如出一辙的报道，称某某地方的架空光缆又被无知的盗贼割断了，不同的只是时间和地点的变换。以至于光缆的架空杆子上挂出了这样的牌子："光缆割断不能卖钱……"就是沉入海底的光缆也不能幸免于难。2001 年 2 月 9 日上午中美海底光缆被鱼船在该海域非法作业时钩断，一时间，使用这一光缆的中国、日本、新加坡和韩国的数百万互联网用户发生"大堵车"，直至 2 月 23 日才得以修复。直接维修费用估计在 500 万至 600 万人民币，间接经济损失更是无法估算。据了解，1999 年中国海域内海底光缆被阻断达 18 次之多。为了避免再发生类似的事故，中国海底电缆公司准备增加 4 条巡逻船，加强 24 小时雷达监控。同时，上海有关部门加强了打击破坏光缆的力度，严禁渔船在海缆路由及两侧各两海里范围内抛锚及进行捕捞作业。

1.1.4 解决网络安全问题的途径

1. 加强国际合作，从根本上改善网络体系结构和协议的安全性能

例如 IPSEC 工作组推出的 IP 协议新版本 IP v6，Netscape 公司在国际标准化组织/开放式系统互联（ISO/OSI）七层体系结构的传输层加装的安全套接层协议（SSL），以及 Phil Zimmermann 在应用层开发的邮件加密系统（PGP）软件包等，都可以看作是在这个方向上的努力。

2. 加强国家的安全立法工作，为网络安全提供法律依据

有关安全的法律体系包括：①国家的根本大法即宪法有关国家安全、社会稳定和人民权利的根本性的法律规定；②国家安全法、保密法等涉及国家安全和信息活动的法律；③有关互联网和电子商务、网络安全的专门法律；④有关具体信息行为的法律界定。

我们国家的法律，不但要规范中国公民的行为，维护国家的统一和政权的稳定，而且要在一个经济全球化的进程中，能够维护国家的利益和本国公民的权益。日本等一些发达国家之所以胆敢把一些有问题的产品销往中国，其原因之一就是中国的法律不完善。中国公民在国际交往中受到了损害，却拿不出索赔的法律依据。

3. 研究开发具有中国独立版权的安全产品

我国现在所用的大多数安全产品都是进口的，这种状况潜伏着巨大的危险。一方面，发达国家的政府禁止向我国出口高等级的安全产品，我们只能拿到低等级的安全产品。另一方面是各种安全产品都存在着后门和隐蔽通道，有的进程甚至可以远程激活。

从单纯的经济角度看，在一个社会信息化的进程中，安全产品是一个巨大的市场。对这样一个市场熟视无睹拱手让人确实有欠明智。

4. 研究中国独立的加密体制

加密体制是安全的一个核心问题。在加密体制上受制于人就更不可取了。中国人的思维方式是和西方人的思维方式有很大的不同的，在加密上我们会有一些更加奇特的思想。我国目前的法律规定加密的算法只有特定的部门才能研究，这当然有利于阻止民间产生一些政府安全部门所不了解的密码。如何在更加广泛的基础上集中民族的智慧维护国家的利益，这是一个有待探讨的问题。

5. 培养网络安全的各个层次的人才

目前我国的网络安全人才，无论是高级的研究开发人才，还是大量需要的管理应用人才，

都存在较大的缺口。在正规的教育体系中，只有少数学校开设有信息安全专业，而一般电子商务专业、网络工程专业、计算机应用专业等开设网络安全课程的也不是很多。有的学校不是不想开设网络安全的课程，而是苦于师资无法解决。

6. 建立网络安全的组织机构

国家通过一定的组织机构对网络进行分类、分级的管理。在种类上网络分为：互联网；国际专业计算机信息网络；通过专线接入互联网的企业内部网络。在级别上分为：互联网络；接入网络；用户网络。

在各个部门和企事业单位，在建立计算机网络的同时，也应该建立相应的安全组织机构。这个机构应当赋予相当的权力，能够处理涉及安全的各种问题和协调单位内部的各种关系。同时机构内部的各个成员的权力必须有互相制约的机制，避免内部成员的权力失控带来的安全危害。在网络管理中心，系统管理员、安全员、审计员的三权分立是一种有效的安全机制。

7. 建立网络安全的规章制度

网络的所有用户在网络上的行为必须有章可循。必须做什么，可以做什么，禁止做什么，都必须明确规定，并有相应的奖励和惩罚制度。规章制度要简明扼要、严密详尽、具有较强的可操作性。要通过各种形式，经常性地反复宣传和教育，使之深入人心，得到切实的执行。

8. 网络安全要贯穿于网络生存的全过程

在规划设计一个网络时，就应当列入网络安全的需求。在建设一个网络时，网络安全要同步地建设。在发展一个网络时，网络安全必须同步地发展。在维护一个网络时，网络安全必须同步地维护。任何一种延误、迟缓和失误，都有可能给网络安全带来危害。

应当看到，网络安全的工作并不是一劳永逸的，同各种危害网络安全的内外因素的斗争，是一个长期的反复的过程，任何时候都不能有懈怠和侥幸的心理。

1.2 电子商务对网络安全的要求

1.2.1 系统运行的可靠性和坚韧性

人首先要吃饭穿衣，然后才能谈论艺术哲学。房子首先要牢固结实，然后才能够装饰陈设。电子商务对网络安全的需求是什么呢？首先便是系统运行的可靠性和坚韧性。这当然要做许多扎扎实实的基础工作，比如说，机房的选址，基础电气和通信线路的铺设，门窗和环境的防盗监控，以及防火灾、防水灾、防地震等。另外还有备份的系统和数据的磁带、磁盘、光盘要存放在哪里，怎样销毁包含敏感性数据的文件。这些工作都要慎之又慎，持之以恒，通过严格的管理和经常的维护才能保证系统可靠地运行。

系统绝对不受到攻击几乎是不可能的。问题是经受攻击时系统必须有一定的坚韧性。在受到攻击时系统能够化解攻击的强度使之不造成破坏，或者把破坏限制在一定的范围内，或者具有自行恢复的能力。

在系统遭受破坏时，必须有预先研究制定的替代方案和应急措施。系统冗余是一个主要的方法。快速反应力量的常备不懈也很重要。在系统已经受到破坏时，如何在灾难中恢复系统和数据，如何尽量减少损失，避免引发连带灾害的发生，如何向媒体封锁消息，如何稳定军心