CMP 电信专家

通信网络安全技术

杨远红 刘飞 王旭 赵彦卓 编著

Communication Network Security

机械工业出版社
CHINA MACHINE PRESS

通信网络安全技术

杨远红　刘　飞　王　旭　赵彦卓　编著

机械工业出版社

本书深入浅出地介绍了通信与网络方面的安全技术，是作者多年来在众多工程项目中实际经验的结晶。本书先对网络安全的现状做了简单分析，并介绍了一些网络安全的基础知识；接下来用较多的篇幅详细阐述了密码学、认证技术、网络安全管理技术、防火墙技术、IDS 技术和 Honeypot 技术；最后，本书对无线网络和电子商务的安全进行了深入探讨。

本书面向所有对通信网络安全技术感兴趣的人员，主要针对从事网络安全通信行业具有一定通信安全基础知识的工程技术人员而写，同时也可作为广大高等院校相关专业的教学参考用书。

图书在版编目（CIP）数据

通信网络安全技术/杨远红等编著. —北京：机械工业出版社，2005
ISBN 7-111-17548-4

Ⅰ. 通 … Ⅱ. 杨 … Ⅲ. 通信网—安全技术 Ⅳ. TN915.08

中国版本图书馆 CIP 数据核字（2005）第 116786 号

机械工业出版社（北京市百万庄大街 22 号 邮政编码 100037）
责任编辑：张俊红 版式设计：张世琴 责任校对：王 欣
封面设计：王伟光 责任印制：杨 曦
成都新华印务有限责任公司印刷
2006 年 1 月第 1 版第 1 次印刷
787mm × 1092mm 1/16 · 19.25 印张 · 473 千字
0 001 - 4 000 册
定价：30.00 元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换
本社购书热线电话(010)68326294
封面无防伪标均为盗版

前　言

最近10年，通信网络的飞速发展已经大大地改变了我们的生活方式，人们进入了一个崭新的信息时代。通信技术的发展，对整个社会的科学技术、经济发展、国防建设、文化思想带来了巨大的影响和推动。通过网络，我们可以很方便地存储、交换以及搜索信息，给人们的工作、生活和娱乐带来了极大的方便。

在人们享受着迅猛发展的通信网络技术所带来的利益之时，相伴而来的信息安全问题也日益突出。随着通信技术的日益普及，人们已经开始认识到在发展通信网络技术的同时，做好通信网络安全方面的理论研究与应用技术开发，是通信网络技术发展的重要内容。本书的主要目标就是把目前有关通信网络安全的技术放在一个结构比较清楚的框架下，从整个通信网络的角度来谈论通信网络安全技术，使广大读者可以更快、更深刻地掌握通信网络安全的知识。

本书共分为14章。第1章阐述网络安全的意义、技术体系结构以及国内外的信息技术安全标准；第2章主要介绍TCP/IP以及IPsec、SSL等安全协议；第3～5章主要论述了密码技术，对密钥加密技术原理作了详细描述；第6章主要介绍安全认证技术；第7章介绍安全网络管理；第8章介绍防火墙技术，对防火墙的原理、配置等做了比较详细的解释，并介绍了几个主要防火墙产品；第9章介绍入侵检测技术，因为入侵检测是对以防火墙为核心的网络安全体系的重要补充；第10章介绍了新的安全技术——Honeypot技术；第11～13章介绍无线网络安全，包括移动通信系统、篮牙、IEEE802.11的安全机制；第14章介绍Web服务安全及电子商务安全，并对当前热门的移动电子商务安全做了一定的介绍。

本书内容丰富、层次分明，是为有志从事安全通信领域的读者而写，主要针对有一定理论基础、从事安全通信的读者，帮助他们了解最新技术原理和动向；同时可作为初级读者全面了解安全通信的基本原理及最新动态的读物；也可作为高等院校通信与信息系统、信号与信息处理、密码学、网络安全等相关专业的教学参考用书和通信网络安全领域相关人员培训的教材。

本书第1、2、10、14章由杨远红撰写，第3～7章由刘飞撰写，第8、9章由王旭撰写，第11～13章由赵彦卓撰写，全书由杨远红统稿。

由于作者水平有限，编写时间仓促，且通信网络安全技术发展迅猛，书中难免存在一些错误和不足之处，殷切希望广大读者批评指正。

作　者

目　录

第 1 章　网络安全概论

自从计算机网络诞生以来，网络安全是一个受到人们普遍关注的课题。可以预言，今后的社会将进入全面的网络时代和信息共享时代。网络安全极其重要，网络只有安全才可以保证网络生活能够有序进行、网络系统不遭破坏、信息不被窃取、网络服务不被非法中断等。但另一方面，目前的网络正在遭受很多威胁和攻击，网络中存在很多不安全的因素，诸如黑客入侵、信息泄露等。甚至可以说，目前尚没有绝对安全的网络。因此，我们需要研究和掌握更多安全技术，尽可能地保证网络安全。

1.1　计算机网络的发展

计算机网络是计算机技术和通信技术紧密结合的产物，涉及到通信与计算机两个领域的知识，它的诞生使计算机体系结构发生了巨大的变化，同时在当今社会经济中也起着重要的作用，并对人类社会的进步作出了巨大贡献。现在，计算机网络已成为人们社会生活中不可缺少的一个基本组成部分，计算机网络已经遍布各个领域。从某种意义上讲，计算机网络的发展水平不但反映了一个国家的计算机科学和通信技术水平，而且已成为衡量其综合国力及现代化程度的重要标志之一。

自 20 世纪 50 年代开始，人们及各种组织机构使用计算机来管理他们的信息的速度迅速增长。在早期，限于技术条件，当时的计算机都非常庞大、非常昂贵，任何机构都不可能为雇员个人单独提供整台计算机。主机一定是共享的，它被用来存储和组织数据，集中控制和管理整个系统。所有用户都有连接系统的终端设备，将数据库录入到主机中处理，或者将主机中的处理结果通过集中控制的输出设备取出来。通过专用的通信服务器，系统也可以构成一个集中式的网络环境，使用单台主机可以为多个配有 I/O 设备的终端用户（包括远程用户）服务。这就是早期的集中式计算机网络，一般也称为集中式计算机模式。它的最典型特征是，通过主机系统形成大部分的通信流程，构成系统的所有通信协议都是系统专有的，大型主机在系统中占据着绝对的支配地位，所有控制和管理功能都是由主机来完成的。

随着计算机技术的不断发展，尤其是大量功能先进的个人计算机（PC）的问世，使得每一个人可以完全控制自己的计算机，进行他所希望的作业处理。以个人计算机方式呈现的计算能力发展成为独立的平台，导致了一种新的计算结构——分布式计算模式的诞生。

一般来讲，计算机网络的发展可分为 4 个阶段：

第 1 阶段：计算机技术与通信技术相结合，形成计算机网络的雏形。

第 2 阶段：在计算机通信网络的基础上，完成网络体系结构与协议的研究，形成了计算机网络。

第 3 阶段：在解决计算机连网与网络互连标准化问题的背景下，提出开放系统互连参考模型与协议，促进了符合国际标准的计算机网络技术的发展。

第 4 阶段：计算机网络向互连、高速、智能化方向发展，并获得广泛的应用。

任何一种新技术的出现都必须具备两个条件，即强烈的社会需求与先期技术的成熟。计算机网络技术的形成与发展也证实了这条规律。1946 年世界上第 1 台电子数字积分器与计算机（ENIAC）在美国诞生时，计算机技术与通信技术并没有直接的联系。20 世纪 50 年代初，由于美国军方的需要，美国半自动地面防空系统（SAGE）进行了计算机技术与通信技术相结合的尝试，它将远程雷达与其他测量设施测到的信息通过总长度为 241km 的通信线路与一台 IBM 计算机连接，进行集中的防空信息处理与控制。要实现这样的目的，首先要完成数据通信技术的基础研究。在这项研究的基础上，人们完全可以将地理位置分散的多个终端通信线路连到一台中心计算机上。用户可以在自己办公室内的终端键入程序，通过通信线路传送到中心计算机，分时访问和使用其资源进行信息处理，处理结果再通过通信线路回送到用户终端显示或打印。人们把这种以单个为中心的联机系统称做面向终端的远程联机系统，它是计算机通信网络的一种，20 世纪 60 年代初，美国航空公司建成的由一台计算机与分布在全美国的 2000 多个终端组成的 SABRE-1 航空订票系统就是这种计算机通信网络。

随着计算机应用的发展，出现了多台计算机互连的需求。这种需求主要来自军事、科学研究、地区与国家经济信息分析决策、大型企业经营管理。他们希望将分布在不同地点的计算机通过通信线路互连成为计算机—计算机网络。网络用户可以通过计算机使用本地计算机的软件、硬件与数据资源，也可以使用连网的其他地方的计算机软件、硬件与数据资源，以达到计算机资源共享的目的。这一阶段研究的典型代表是美国国防部高级研究计划局（Advanced Research Projects Agency，ARPA）的 ARPANet（通常称为 ARPA 网）。1969 年，美国国防部高级研究计划局提出将多个大学、公司和研究所的多台计算机互连的课题。1969 年 ARPA 网只有 4 个节点，1973 年发展到 40 个节点，1983 年已经达到 100 多个节点。ARPA 网通过有线、无线与卫星通信线路，使网络覆盖了从美国本土到欧洲与夏威夷的广阔地域。ARPA 网是计算机网络技术发展的一个重要的里程碑，它对发展计算机网络技术的主要贡献表现在以下几个方面：

1）完成了对计算机网络的定义、分类与子课题研究内容的描述；

2）提出了资源子网、通信子网的两级网络结构的概念；

3）研究了报文分组交换的数据交换方法；

4）采用了层次结构的网络体系结构模型与协议体系。

ARPA 网络研究成果对推动计算机网络发展的意义是深远的。在它的基础之上，20 世纪 70～80 年代计算机网络发展十分迅速，出现了大量的计算机网络，仅美国国防部就资助建立了很多计算机网络。同时还出现了一些研究试验性网络、公共服务网络、校园网，例如美国加利福尼亚大学劳伦斯原子能研究的 OCTOPUS 网、法国信息与自动化研究所的 CYCLADES 网、国际气象监测网（WWWN）、欧洲情报网（EIN）等。在这一阶段，公用数据网（Public Data Network，PDN）与局部网络（Local Network，LN）技术发展尤其迅速。

计算机网络的资源子网与通信子网的结构使网络的数据处理与数据通信有了清晰的功能界面。计算机网络可以分成资源子网与通信子网来组建。通信子网可以是专用的，也可以是公用的。为每一个计算机网络都建立一个专用通信子网的方法显然是不可取的，因为专用通信子网造价很高、线路利用率低、重复组建通信子网投资很大，同时也没有必要。随着计算

机网络与通信技术的发展，20 世纪 70 年代中期，世界上便出现了由国家邮电部门统一组建和管理的公用通信子网，即公用数据网（PDN）。早期的公用数据网采用模拟通信的电话通信网，新型的公用数据网采用数字传输技术和报文分组交换方法。典型的公用分组交换数据网有美国的 TELENET、加拿大的 DATAPAC、法国的 TRANSPAC、英国的 PSS、日本的 DDX 等。公用分组交换网的组建为计算机网络的发展提供了良好的外部通信条件。

以上讲的是利用远程通信线路组建的远程计算机网络，也称为广域网（Wide Area Network，WAN）。随着计算机的广泛应用，局部地区计算机连网的需求日益强烈。20 世纪 70 年代初，一些大学和研究所为实现实验室或校园内多台计算机共同完成科学计算和资源共享的目的，开始了局部计算机网络的研究。1972 年，美国加州大学研制了 Newhall 环网；1976 年，美国 XEROX 公司研究了总线拓朴的实验性 Ethernet（以太网）；1974 年，英国剑桥大学研制了 Cambridge Ring 网。这些都为 20 世纪 80 年代多种局部网络产品的出现提供了理论研究与技术实现的基础，对局部网络技术的发展起到了十分重要的作用。

与此同时，一些大的计算机公司纷纷开展了计算机网络研究与产品开发工作，提出了各种网络体系结构与网络协议，如 IBM 公司的 SNA（System Network Architecture）、NEC 公司的 DNA（Digital Network Architecture）与 UNIVAC 公司的 DCA（Distributed Computer Architecture）。

计算机网络发展的第 2 阶段所取得的成果对推动网络技术的成熟和应用极其重要，它研究的网络体系结构与网络协议的理论成果为以后网络理论的发展奠定了基础。很多网络系统经过适当修改与充实后仍在广泛使用。目前国际上应用广泛的因特网（Internet）就是在 ARPA 网的基础上发展起来的。但是，20 世纪 70 年代后期，人们已经看到了计算机网络发展中出现的危机，那就是网络体系结构与协议标准的不统一限制了计算机网络自身的发展和应用，网络体系结构与网络协议标准必须走国际标准化的道路。

计算机网络发展的第 3 阶段是加速体系结构与协议国际标准化的研究与应用阶段。国际标准化组织（ISO）的计算机与信息处理标准化技术委员会 TC 97 成立了一个分委员会 SC16，研究网络体系结构与网络协议国际标准化问题。经过多年卓有成效的工作，ISO 正式制订、颁布了开放系统互连参考模型（Open System Interconnection Referance Model，OSI RM），即国际标准 ISO/IEC 7498。ISO/OSI RM 已被国际社会所公认，成为研究和制订新一代计算机网络标准的基础。20 世纪 80 年代，ISO 与 CCITT（国际电话电报咨询委员会）等组织为参考模型的各个层次制订了一系列的协议标准，组成了一个庞大的 OSI 基本协议集。我国也于 1989 年在《国家经济系统设计与应用标准化规范》中明确规定选定 OSI 标准作为我国网络建设标准。ISO/OSI RM 及标准协议的制定和完善正在推动计算机网络朝着健康的方向发展。很多大的计算机厂商相继宣布支持 OSI 标准，并积极研究和开发符合 OSI 标准的产品。各种符合 OSI RM 与协议标准的远程计算机网络、局部计算机网络与城市（地区）计算机网络已开始广泛应用。随着研究的深入，OSI 标准将日趋完善。

如果说远程计算机网络扩大了信息社会中资源共享的范围，那么局部网络则是增强了信息社会中资源共享的深度。局部网络是继远程网之后又一个网络研究与应用的热点。远程网技术与微型机的广泛应用推动了局部网络技术研究的发展。局部网络可以分为局域网、高速局部网与计算机交换分机 3 类。20 世纪 80～90 年代，局域网技术取得了突破性进展。在局域网领域中，采用以太网（Ethernet）、令牌总线（Token Bus）、令牌环（Token Ring）原理

的局域网产品形成了三足鼎立之势，采用光纤传输介质的 FDDI（光纤分布式数字接口）产品在高速与主干环网应用方面起了重要性的作用。20 世纪 90 年代局域网技术在传输介质、局域网操作系统与客户/服务器（Client/Server）应用方面取得了重要的进展。由于数据通信技术的发展，在以太网中用非屏蔽双绞线实现了 10Mbit/s 的数据传输。在此基础上形成了网络结构化布线技术，使以太网在办公自动化环境中得到更为广泛的应用。局域网操作系统 Novell NetWare、Windows NT Server、IBM LAN Server 使局域网应用进入到成熟的阶段。客户/服务器应用使网络服务功能达到更高水平。

目前计算机网络的发展正处于第 4 阶段。这一阶段计算机网络发展的特点是互连、高速、智能与更为广泛的应用。

因特网（Internet）是覆盖全球的信息基础设施之一，对于用户来说，它像是一个庞大的远程计算机网络。用户可以利用因特网实现全球范围的电子邮件、电子传输、信息查询、语音与图像通信服务功能。实际上因特网是一个用路由器（Router）实现多个远程网和局域网互连的网际网，到 1998 年连入因特网的计算机数量已达 4000 万台之多，它将对推动世界经济、社会、科学、文化的发展产生不可估量的影响。

在互联网发展的同时，高速与智能网的发展也引起人们越来越多的注意。高速网络技术发展表现在宽带综合业务数字网（B-ISDN）、帧中继（FR）、异步传输模式（ATM）、高速局域网（HSLAN）、交换局域网（SLAN）与虚拟网络（VN）上。随着网络规模的增大与网络服务功能的增多，各国正在开展对智能网络（Intelligent Network，IN）的研究。

计算机网络技术的迅速发展和广泛应用必将对 21 世纪的经济、教育、科技、文化的发展产生重要影响。

1.2 计算机网络受到的安全威胁

计算机系统容易受到许多威胁，从而造成各种各样损害而导致严重损失，这些损害包括从由于错误而破坏数据库的安全性到火灾摧毁整个计算机中心。损害的原因是多种多样的，例如，看上去可信的员工欺骗系统的行为、外部黑客或粗心的数据录入员等。由于很多损害永远也无法被发现，有些机构为了避免公众形象受损所以对损害情况加以掩盖，所以准确地评估计算机安全相关的损害是不可能的。不同的威胁其后果也有所不同：一些是影响数据的机密性或完整性，而另一些则影响系统的可用性。这些威胁包括：

1. 错误和遗漏

错误和遗漏是数据和系统完整性的重要威胁。这些错误不仅由每天处理几百条交易的数据录入员造成，创建和编辑数据的任何类型的用户都可能造成。许多程序，特别是那些被设计用来供个人计算机用户使用的程序缺乏质量控制手段。但是，即使是最复杂的程序也不可能探测到所有类型的输入错误或遗漏。良好的意识和培训项目可以帮助机构减少错误和遗漏的数量与严重程度。

2. 欺诈和盗窃

计算机系统会受到欺诈和盗窃的伤害，这种伤害可以是通过“自动化”了的传统手段进行的，也可以是通过新的手段进行的。例如，有人可能会使用计算机在大型账户中稍微减少一小部分数量的金钱，期望这个微小的差异不会被调查。金融系统不是这种风险的惟一受害

者。控制资源访问的系统（如时间和考勤系统、存货系统、学籍系统以及长途电话系统等）都可能成为受害者。

计算机欺诈和盗窃可以是内部人员所为，也可以是外部人员所为。欺诈主要是内部人员（如系统的授权用户）所为。因为内部人员既可以访问受害的计算机系统（包括其控制资源和流动资源）对系统又比较熟悉，被授权的用户在进行计算机犯罪时处于有利的地位。内部人员可以是普通用户（如职员），也可以是技术人员。了解机构运行情况的机构的前员工也可能是一种威胁，在其访问权限没有得到适当终止的时候尤其如此。另外，对于使用技术手段进行欺诈和盗窃，计算机硬件和软件都容易被窃取。

3. 员工破坏

员工最熟悉其雇主的计算机和应用，包括知道何种行为会导致最大的损害、故障或破坏。公共和私营机构中人员的不断缩减造成有一些人员对整个机构都很熟悉，这些人员可能会保留潜在的系统访问权（如系统账户没有被及时删除）。从数量上看，员工破坏事件比盗窃事件要少，但是这种事件造成的损失却很高。当员工在工作中感到受了欺骗、厌烦、疲倦以及受到威胁或背叛的时候，破坏将被当做获得工作满足感的直接手段，这种手段老板当然是不会同意的 。

4. 丧失物理和基础设施的支持

丧失基础设施的支持，包括电力故障（中断、瞬间高压或电压不足）、丧失通信能力、水的中断和泄漏、下水管道问题、缺乏运输服务、火灾、洪水、国内混乱和罢工等。基础设施的丧失通常导致系统停机，有时结果是无法预料的。例如，在暴风雪的天气下员工无法上班，而计算机系统依然在工作。

5. 有害黑客

有害黑客这一术语，有时被称为黑客，是指未经授权侵入计算机的人。他们可以是外部人员，也可以是内部人员。黑客的威胁应该被认为是过去的或未来潜在的损害。虽然目前由黑客造成的损失远小于由内部盗窃和破坏造成的损失，但是黑客问题分布广泛而且情况严重。

黑客威胁受到的关注通常会比其他更普遍更危险的威胁还要多，原因有以下 3 种：

首先，黑客的威胁是最近才遭遇到的威胁。很多机构一直以来只关注内部员工的行为，并能够采用惩戒手段减少威胁。但是，这些手段对于防止外部的不受员工规章约束的人来说是无效的。

其次，机构不知道黑客的目的，有些黑客只是浏览信息，有些则盗窃信息，而有些进行破坏。受害机构无法确定黑客的目的就会觉得其攻击会很严重。

第三，黑客的攻击会使人们觉得很脆弱，在不知道对方的身份的情况下尤其如此。例如，假如雇佣一名油漆工油漆房屋，有一次他偷窃了珠宝，邻居们不会因此感到威胁，也不会采取措施防备那个油漆工。但是，如果强盗闯入同一间房屋偷走了同样的珠宝，所有的邻居都会觉得自己是受害者，并且感到很容易受到攻击。

6. 工业间谍

工业间谍是指从企业或政府收集专有数据以达到协助其他公司的目的的行为。工业间谍行为可能是公司为了提高自身的竞争力或政府为了帮助其国内企业所为。由政府派出的工业间谍通常被称为经济间谍。因为信息通常在计算机系统中进行处理和存储，所以计算机安全可以帮助防范这种威胁。但是，这无法减少由于授权的员工出卖信息而造成的威胁。

7. 有害代码

有害代码是指病毒、蠕虫、特洛伊木马、逻辑炸弹和其他“不受欢迎的软件”。有时人们会错误地认为这些只与个人计算机有关，事实上有害代码可以攻击其他平台。有害代码所造成的实际损失主要来自系统的中断和修复系统所花费的人力资源。无论如何，费用是巨大的。

8. 外国政府间谍

在有些场合，可能会出现外国政府情报部门造成的威胁。除了可能的经济间谍之外，外国情报部门可能会为了进一步的情报工作而瞄准非保密系统。有些非保密信息可能对其有价值，如高官的旅行计划、国内防卫和应急准备情况、制造技术、卫星数据、人事和工资数据以及执法、调查和安全文件。具有管辖权的安全官员可以提供有关处理此类威胁的指导。

总之，计算机网络的威胁既有来自内部的如设计、物理、管理等方面的，也有来自外部的如黑客、病毒等。为了控制运行信息系统的风险，管理人员和用户需要了解系统的缺陷和利用缺陷可能造成的威胁。对威胁环境的了解使系统管理人员得以实施最具成本效益的安全措施。在有些情况下，管理人员发现简单容忍预期损害更具有成本效益，这一决策应该基于风险分析的结果。

1.3 网络安全技术体系

1.3.1 网络安全保障的基本内容

网络安全保障是一个很大的社会课题，该课题需要解决的是保障整个网络社会的所有网络用户的安全，这里主要包括通信安全、环境安全、内容安全，也就是要为广大网络用户提供一个健康、通畅、舒适、安全、可靠的网络社会生活环境。

1. 通信安全

通信安全保障就是要保证信息高效、可靠地传输，实现通信数据的机密性和完整性。一般至少要从如下 3 方面进行保障：

1）保障通信线路的畅通，国际出口线、国家主干线、地区主干线、城市主干线首先要保证线路高质量地提供全年每天 24h 无故障服务；

2）保障通信线路的高效使用，要防止各类无效的信息对网络的影响，如垃圾邮件、有害信息、DOS 与 DDOS（诊断磁盘操作系统）等攻击、病毒泛滥等，保障网络用户正常通信的信息得到及时传输；

3）保障通信信息的机密性、完整性和高可靠性，要防止国家机密或秘密信息、军队机密或秘密信息、企业或商业秘密信息、个人隐私、基于电子商务的重要信息被窃取、被篡改。

2. 环境安全

现实社会中的生活环境和工作环境的安全问题是人们十分关注的热点，而虚拟社会的网络环境安全同样是人们担心和急需解决的问题。事实上，任何一种环境，无论现实环境或虚拟的网络环境，如果不能得到较好的净化，必将影响人们的生活健康和质量。因此，我们应

该从如下方面来保障网络环境的安全：

1）控制网络环境污染的源头，防止个人（终端）成为网络环境污染的源头；

2）控制网络环境中的应用服务点，防止对外提供服务的服务器成为网络环境污染的渠道，既要防止成为被用于攻击的跳板或工具，并且还要起到消除攻击、阻断攻击链的作用；

3）控制各级网关，防止局部网络成为污染源，防止局部网络的受攻击的影响迅速蔓延到其他网络，必要时通过控制网关限制局部网络的污染影响扩大，实现整体网络净化。

3. 内容安全

内容安全是信息网络安全的本质安全问题。人们在网络上活动，最终所获取的是信息内容，因此，获取内容的真实性、可靠性、有效性、机密性就成为人们最关心的话题。为此，我们应该从如下方面着手做好相关工作：

1）保障公共信息的真实性和完整性。网络已经成为人们获取公共信息的主要渠道之一，保障网络空间的各类信息的真实性和完整性，尤其是政府部门发布的、商业交换的、科学教育的信息的真实性和完整性是内容安全的首要任务。

2）保障网络空间信息的合法性。而事实上大量的非法信息通过网络得以大面积的传播，这些非法信息严重影响了人们的正常生活和社会稳定，需要采取措施限制这些非法信息的传播。公共网络已逐步成为有效商业环境之一，保障商业信息交换的合法性，包括商品信息、资金信息、身份信息、购销信息等的合法性，同样是内容安全的重要任务。

3）保障网络空间信息的健康性。在自由化的网络环境中充斥着大量不健康的信息，如黄色信息、虚假广告等，严重影响了网络的有效作用，尤其会影响青少年的健康成长，因此，保障网络空间信息的健康性是公共信息网络安全保障的基本工作之一。

4）保障网络空间信息的有效性。大量的垃圾信息、垃圾邮件、大量虚假信息的发布和传播，严重影响了网络通信的效率，影响了人们获取信息的效用，这一点已成为公共信息网络安全必须关注的热点之一。

需要特别说明的是，由于互联网信息服务与电话业务的融合越来越多，我们所讨论的网络环境不再单纯是人们通常所认为的因特网、单位内部局域网等，实际上还包括人们日常使用的基本通信工具，比如有线电话和无线电话。

1.3.2 网络安全体系的实现

网络信息系统的安全体系需要从技术和安全管理两个方面来共同实现。

1. 技术实现

利用现有的、成熟的网络安全技术和产品，可以很方便地实现对整个网络信息系统的安全防护。目前网络安全市场上常见的安全产品有防火墙、入侵检测系统、网络安全扫描及安全评估工具、防病毒软件、线路数据加密等，它们缺一不可，因为没有一个单一的安全工具或网络安全方案能够满足全部用户的所有安全要求。只有根据实际的应用需求，确立分层防护的安全设计理念，才能真正达到网络安全的目标。针对具体业务的安全需求制定整体网络安全方案是大势所趋。

1）防火墙技术是现在市场上应用范围最广、最容易被用户接受的网络安全产品之一。防火墙将内部可信区域与外部威胁区域有效隔离，将网络的安全策略制定和信息流集中管理控制，为网络边界提供保护。使用防火墙，可以防止非法用户对网络资源的访问。防火墙具

有如下特点：采用安全主用的操作系统；防止黑客攻击；具有很强的访问控制功能；提供代理服务；支持网络地址转换；强大的审计和日志管理功能；具有生动、灵活和人机交互的配置界面，可用于多种网络结构。但是防火墙也有自身的局限性。首先，防火墙提供的是静态防御，它的规则都是事先设置的，对于实时的攻击或异常行为不能作出实时反映；其次，防火墙规则的制定，对一些协议细节无法做到完全解析；而且，防火墙无法自动调整策略设置来阻断正在进行的攻击，也无法防范基于协议的攻击；再有，防火墙具有防外不防内的局限性，对于内部用户的非法行为或已经渗透的攻击无法检查和响应。

2）入侵检测系统能够实时地监测所有访问服务器资源的用户行为，监控网络上的数据流，从中检测出攻击的行为并给予响应和处理。对出现的大量可能危害服务器的行为及时作出报警、阻断响应，并提供日志记录和分析。实时入侵检测技术还能检测到绕过防火墙的攻击，是对防火墙技术、漏洞扫描及修补技术的有力补充。实时入侵检测系统是建立高级别网络安全不可缺少的一环。

3）网络安全扫描及安全评估工具可以及时地发现网络服务漏洞，提出修改建议，是网络安全防御中的一项重要技术。其原理是根据已知的安全漏洞知识库，对目标可能存在的安全隐患进行逐项检查，目标可以是工作站、服务器、交换机、数据库应用等各种对象，然后根据扫描结果向系统管理员提供周密可靠的安全分析报告，为提高网络系统安全性提供重要依据。该工具操作简单，可以大大减少网络管理员的手工劳动，有利于及早弥补漏洞，保持网络系统的安全和稳定。

4）线路数据加密。对于通过公用电话拨号接入的线路，可以在拨号终端与用户调制解调器（Modem）之间以及计算机网络的接入路由器与调制解调器池之间分别接入异步数据密码机。要求异步数据密码机有单机式（支持台式机/笔记本电脑）和列架式（支持接入路由器/调制解调器池）两种类型。

2. 安全管理体系

从行政管理的角度建立网络安全管理体系，其主要内容包括建立网络安全管理机构、建立各项安全管理制度、明确安全管理责任和建立监督机制、对人员的安全管理等。

1）建立网络安全管理机构。为保障网络安全建设和运行，必须建立一个有效的网络安全管理机构，协调全网的安全事宜，负责监督各项安全制度和措施的落实，负责并领导经常性的网络安全管理工作。

2）建立安全管理制度。根据实际情况，建立和健全各种安全管理制度，例如机房安全管理制度、病毒防范制度、安全操作规程和工作守则、保密设备安全管理制度、维护和维修管理制度、安全考核制度等。严格遵守操作规程，爱护设备，磁介质保护完好，对外来软件只有进行严格的检查合格后才允许在系统中使用。禁止使用来源不可靠的存储介质，以防止计算机病毒的侵入。

3）建立职责和监督机制。实行分权制约、优先授权的原则，落实职责，建立有关人员的工作日志以进行有效的追踪、监督和审计。

4）人员的安全管理。必须对要害岗位的人员进行严格审查，以保证关键人员的安全可靠，如系统管理员、数据库管理员等。严格划分人员的权限，采取有效的相互制约措施，禁止职责交叉、混岗操作。加强对内部人员的安全保密教育和业务培训。对工作调动和离职人员要及时调整有关的安全控制手段。

1.4 信息技术安全标准与法律法规

法律保障是公共信息网络安全的基础。从国际的角度来看，本应该有相应的公约，但是，由于公约制订的客观困难而至今没有合适的公约条例出台。可是，公共信息网络安全的国际性又非常强，需要各国的共同努力来推动公约的建设。在没有统一公约的情况下，国际相关的安全组织做了大量的标准化工作，这为建立全面的公共信息网络安全法律保障体系起到了良好的推动作用。与此同时，各国在自身的网络安全管理上出台了相当多的计划、标准、法规、条例，来规范网络世界的行为，对公共信息网络安全的建设起到了良好的保障作用。

1.4.1 国际、国外信息安全法律法规

1.4.1.1 国际合作组织在电子商务立法方面所做的工作

1. 联合国国际贸易法委员会（UNCITRAL）

联合国国际贸易法委员会一直十分关注计算机商业应用所引起的法律问题。1985 年，该委员会在第 18 次会议上提出了题为“计算机记录的法律价值”报告；为了金融业务电子化的需要，该委员会于 1992 年制定了《国际贷记传输示范法》。1996 年，联合国大会通过了国际贸易法委员会经过 5 年时间起草的《电子商务示范法》。该示范法本身没有法律效力，只是提供给政府和法律执行部门以协助其工作，示范法将成为电子商务中促进国家法律法规建设的有效工具，每个国家都将其纳入自己的国家法律之中。2000 年 9 月，国际贸易法委员会电子商务工作组制定了《电子签名统一规则》。

制定示范法的目的在于为国家立法部门提供一套国际承认的法规，使其明确如何改进原法律中没有关于使用无纸信息的条款、未考虑到电子商务应用（例如，规定使用“书面”形式“签字”或“原本”文件）等各种弊端，为电子商务的发展建立更加可靠的法律环境，建立国际贸易经济秩序，促进其快速发展。当一些用户选择了使用电子通信手段进行电子商务活动时，通过将示范法中有关规定纳入其国家的法律法规，这些国家将建立一个拥有多种有效途径开展国际贸易业务的环境。

示范法对数据报文的法律认证、可接受性和确认、保存，对数据报文的通信、合同格式与有效性、数据报文的归属，对运输文件、运输合同等问题都做了规定。但是，示范法只是一个法律框架，还有待于进一步补充和完善。

2. 经济合作与发展组织

经济合作与发展组织（OECD）是由北美、欧洲和亚太地区的 29 个国家和地区组成的国际组织。1997 年 11 月在芬兰，OECD 就曾召集了 400 多位政府与企业界领袖确定电子商务的发展面临哪些障碍问题。对通过因特网做交易缺乏信任与信心是障碍之一。其他障碍还包括对网络和市场的访问，诸如付款系统不足等后勤保障问题，以及缺乏明确稳定的规章环境等。最后，该组织发表了题为《克服全球电子贸易障碍》的文件，并通过了《加密政策指南》。该指南就加密技术的使用，规定了指导各成员国立法及制定政策的原则，且承认了加密对商业的重要性。

1998 年 10 月，OECD 在渥太华举行部长会议，共同探讨为全球电子商务制定“竞赛规

则”。此次大会名为“渥太华专题讨论会：全球一体化——认识全球电子商务的潜力”，电子商务问题，诸如税制、消费者保护与隐私以及密码问题都是被讨论的内容。

OECD 致力于研究在渥太华会议上提交的有关税制与消费者保护的指导原则，以及有关隐私、鉴定、访问和数字签名的声明，这些原则能够帮助 OECD 成员国规划政策和制定法律。

3. 国际因特网方案委员会

1996 年 11 月，由因特网学会（ISOC）、因特网号码分配管理局（IANA）、因特网体系结构委员会（IAB）、美国联邦网络技术委员会（FNC）、国际电信联盟（ITU）、国际商标协会（INTA）、世界知识产权组织（WIPO）等多家相关机构共同发起并成立了国际因特网方案委员会（IAHC）。IAHC 于 1997 年 2 月 4 日宣布了一系列有关域名注册的新方案，在这些新方案中特别对域名抢注问题提供了对策，即以商标作为域名注册时，除了要向注册机构提供商标注册文件外，还为域名的最终生效预留了 60 天的争议期。在 60 天内如果没有另一个机构对该商标的所有权提出异议，域名即可生效，否则将由世界知识产权组织进行仲裁。

此外，负责管理因特网上所有主机的 IP（网际协议）地址和域名分配的网络分解公司（Network Goution-Inc）针对域名抢注现象的日益严重，也增加了详细的补充条文，即对域名所属权有争议的任何一方只要能向法院提供商标注册的文件，证明商标注册的时间是在域名被抢注之前，就可以通过法律手段将域名夺回。这一系列旨在解决域名抢注问题的方案和对策收到了一系列的成效。

同时，该委员会还发布了《国际数字化安全商务应用指南》，该指南是由一系列在因特网上进行可靠的数字化交易的方针构成的，其中包括了公开密钥加密的数字签名和可靠第三方的认证等。国际商会银行委员会拟定的《银行间支付规则草案》，也与电子商务有着直接关系。

4. 因特网法律及政策论坛

因特网法律及政策论坛（ILPF）成立于 1995 年，是由一些有志于促进因特网电子商务和通信发展的因特网中心公司组成的全球性组织机构。ILPF 于 1998 年初在美国华盛顿成功地举行了一个国际会议“发布互联网经济——内容及电子商务”。此次特殊会议是政府与因特网中心公司及其他因特网股东之间的有关因特网过去、现在和将来的一次对话。该组织 1998 年以来陆续进行了一系列卓有成效的工作，包括在自己的主页上添加有关数字签名法律启蒙的程序、保证会员有一个交换信息的平台、与世界各地的因特网工作组合作选择最佳成员等。

5. 欧盟（EU）立法状况

法律作为电子商务发展的软性环境，在保障和促进欧盟内部电子商务的发展过程中发挥了积极的作用。欧盟委员会于 1997 年提出了《欧洲电子商务行动方案》，为规范欧洲电子商务活动制定了框架；1998 年又颁布了《关于信息社会服务的透明度机制的指令》；1999 年通过了《关于建立有关电子签名共同法律框架的指令》，又公布了欧洲议会《关于统一市场电子商务的某些法律方面的建议》，它包括一些市场进入、认证服务、电子证书及其责任以及国际方面的问题。