高等院校信息安全专业规划教材

计算机系统安全原理与技术 第2版

- 计算机系统安全问题及安全机制
- 应急响应与灾难恢复
- 计算机安全等级评测

免费提供电子教案
http://www.cmpedu.com

陈 波 于 泠 肖军模 编著

机械工业出版社
CHINA MACHINE PRESS

高等院校信息安全专业规划教材

计算机系统安全原理与技术

第2版

陈　波　于　泠　肖军模　编著

机 械 工 业 出 版 社

本书全面介绍了计算机系统各层次可能存在的安全问题和普遍采用的安全机制，包括计算机硬件与环境安全、操作系统安全、计算机网络安全、数据库系统安全、应用系统安全、应急响应与灾难恢复、计算机系统安全风险评估、计算机安全等级评测与安全管理等内容。

本书还对各种安全技术的实践作了指导，帮助读者理解并掌握相关安全原理，提高信息安全防护意识和安全防护能力。本书每章附有思考与练习题，还给出了大量的参考文献以供进一步阅读。

本书可以作为信息安全专业、信息对抗专业、计算机专业、信息工程专业或其他相关专业的本科生和研究生教材，也可以作为网络信息安全领域的科技人员与信息系统安全管理员的参考书。

图书在版编目(CIP)数据

计算机系统安全原理与技术/陈波等编著. —2 版. —北京：机械工业出版社，2009.1
(高等院校信息安全专业规划教材)
ISBN 978-7-111-25856-8

Ⅰ. 计… Ⅱ. 陈… Ⅲ. 电子计算机-安全技术-高等学校-教材
Ⅳ. TP309

中国版本图书馆 CIP 数据核字（2008）第 203798 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：唐德凯
责任印制：李　妍
北京蓝海印刷有限公司印刷
2009 年 2 月第 2 版 · 第 1 次印刷
184mm×260mm · 24.75 印张 · 615 千字
0001— 3000 册
标准书号:ISBN 978-7-111-25856-8
定价：39.00 元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换
销售服务热线电话：(010) 68326294 68993821
购书热线电话：(010) 88379639 88379641 88379643
编辑热线电话：(010) 88379753 88379739
封面无防伪标均为盗版

高等院校信息安全专业规划教材

编委会成员名单

出版说明

信息技术的发展和推广，为人类开辟了一个新的生活空间，它正对世界范围内的经济、政治、科教及社会发展各方面产生重大的影响。如何建设安全的网络空间，已成为一个迫切需要人们研究、解决的问题。目前，与此相关的新技术、新方法不断涌现，社会也更加需要这类专门人才。为了适应对信息安全人才的需求，我国许多高等院校已相继开设了信息安全专业。为了配合相关的教材建设，机械工业出版社邀请了解放军信息工程大学、解放军理工大学通信工程学院、上海交通大学、西安电子科技大学、湖南大学、中山大学、南京邮电学院等高校的专家和学者，成立了教材编委会，共同策划了这套面向高校信息安全专业的教材。

本套教材的特色：

1. 作者队伍强。本套教材的作者都是全国各院校从事一线教学的知名教师和学术带头人，具有很高的知名度和权威性，保证了本套教材的水平和质量。

2. 系列性强。整套教材根据信息安全专业的课程设置规划，内容尽量涉及该领域的方方面面。

3. 系统性强。能够满足专业教学需要，内容涵盖该课程的知识体系。

4. 注重理论性和实践性。按照教材的编写模式编写，在注重理论教学的同时注意理论与实践的结合，使学生能在更大范围内、更高层面上掌握技术，学以致用。

5. 内容新。能反映出信息安全领域的最新技术和发展方向。

本套教材可作为信息安全、计算机等专业的教学用书，同时也可以供从事信息安全工作的科技人员以及相关专业的研究生参考。

机械工业出版社

前　言

信息安全技术的发展日新月异，新思想和新方法不断产生，教学内容必须跟踪新技术的发展。同时，信息安全是一个整体概念，解决某一个安全问题常常要综合考虑硬件、系统软件、应用软件、网络协议、评估、管理等多个层次的安全问题。“计算机安全”是信息安全课程体系中的一门重要课程，也是一门直接面向应用、实践性很强的课程，教学中需要重视理论的讲授，使学生掌握解决问题的基本理论和技术，还要强调实验教学，培养学生解决安全问题的实践应用能力。

本书第1版自2006年出版以来，得到了许多读者的鼓励和很好的建议，因此，结合信息安全技术的发展，在第1版教材基础上，进行了认真全面的修订。

在第2章中增加了高级加密标准AES的介绍，散列函数一节删除了MD5算法，改为SHA算法的介绍；第3章中，对可信计算与安全芯片一节作了新技术的补充；第4章中修改了存储保护的内容，Windows系统安全的介绍围绕Windows XP/Vista展开，内容进行了重新组织；第5章中防火墙及入侵检测的介绍增加了实例，使得学生更加容易理解较深奥的这部分原理；第8章中删去了报文标记追踪技术这部分较深的内容；第9章围绕新的风险评估标准展开，修订了大部分内容；第10章补充了最新的法律法规，系统介绍了我国计算机知识产权的法律保护措施。这样，基于信息保障模型（PDRR）——防护、检测、反应与恢复的理论，本书内容涉及计算机系统安全各层次可能存在的安全问题和普遍采用的安全机制，具体包括：计算机硬件与环境安全、操作系统安全、计算机网络安全、数据库系统安全、应用系统安全以及应急响应与灾难恢复、计算机系统安全风险评估、安全管理和安全立法等。

本书第2版还丰富了课后习题，增加了操作实验题、编程实验题、材料分析题，并提供了很多相关网站和参考书供读者拓展知识面和进行实践。在一些具体章节中，例如第7章，重新编写了代码安全技术，补充了代码的静态和动态检测技术，增加了软件保护的实践方法；第8章中补充了计算机取证的操作内容。

本书第2版在注重内容全面系统的同时，力求做到叙述清晰、深入浅出。

为了方便教师利用本书教学，便于学生通过本书自学，本书提供了修订后的配套电子教案，读者可在机械工业出版社网站www.cmpedu.com上免费下载。同时，习题中的实验指导已集结成《计算机系统安全实验教程》出版，为广大读者完成实验给予指导和提供参考，这也使得本套教材的面向应用、提高能力的特色得到更好体现。

本书由陈波、于泠和肖军模共同完成编写。本书及配套实验教程的编写得到了南京师范大学的支持。

在此，向所有为本书做出贡献的同志致以衷心的感谢。

计算机信息系统安全仍是一个不断发展的研究领域，书中难免存在不足之处，恳请广大读者和专家提出批评和改进意见。

作　者

目　录

第1章　计算机系统安全概论

随着计算机技术的不断发展和网络的日益普及，人们对计算机和网络的依赖也越来越强，计算机和网络构成了当今信息社会的基础。本书所讨论的计算机系统是指在计算机网络环境下的信息处理系统。

目前，计算机信息系统面临着极大的安全威胁，针对计算机信息系统的攻击与破坏事件层出不穷，如果不对其加以及时和正确的保护，这些攻击与破坏事件轻则干扰人们的日常生活，重则造成巨大的经济损失，甚至威胁到国家的安全，所以信息系统的安全问题已引起许多国家的高度重视，人们不惜投入大量的人力、物力和财力来提高计算机信息系统的安全性。

本章对计算机信息系统安全问题进行了概述，1.1 节将介绍目前信息系统面临的主要安全威胁，并指出安全问题的根源，1.2 节将讲述信息安全概念的发展，1.3 节将介绍计算机系统安全研究的主要内容。

1.1　计算机信息系统安全问题

1.1.1　计算机信息系统

按照我国颁布的《计算机信息系统安全保护等级划分准则》的定义，“计算机信息系统是由计算机及其相关的配套设备、设施（含网络）构成的，按照一定的应用目标和规格对信息进行采集、加工、存储、传输、检索等处理的人机系统。”

实际上，人们所讨论的典型的计算机信息系统，应该是在计算机网络环境下运行的信息处理系统。一个计算机信息系统由硬件、软件系统和使用人员两部分组成。

硬件系统包括组成计算机、网络的硬设备及其它配套设备。软件系统包括操作平台软件、应用平台软件和应用业务软件。操作平台软件通常指操作系统和语言及其编译系统；应用平台软件通常指支持应用开发的软件，如数据库管理系统及其开发工具，各种应用编程和调试工具等；应用业务软件是指专为某种应用而开发的软件。

众多的计算机信息系统，从应用角度可分为两类：一类是以客户机/服务器模式运行的信息系统，重点是提供信息服务，如 Web 网信息系统等；另一类是以信息交换模式运行的信息系统，重点是进行信息交换，如电子商务信息系统等。不论是何种应用模式，计算机信息系统的最终服务对象是人。人员是计算机信息系统的设计者、使用者，而计算机信息系统的安全问题也主要由各类使用人员引入，而且使用人员由合法使用人员和非法使用人员组成。

20 世纪 40 年代，随着计算机的诞生，计算机安全问题也随之产生。70 年代以来，随着计算机的广泛应用，以计算机网络为主体的信息处理系统迅速发展。同以前的计算机安全保密相比，计算机信息系统的安全问题要多得多，也复杂得多，涉及到物理环境、硬件、软件、数据、传输、体系结构等多个方面。

接下来,我们首先介绍与计算机信息系统安全相关的几个概念:威胁(Threat)、脆弱点(Vulnerability)、攻击(Attack)、控制(Control)。

1.1.2 安全威胁

对计算机信息系统的威胁是指:潜在的、对信息系统造成危害的因素。对信息系统安全的威胁是多方面的,目前还没有统一的方法对各种威胁加以区别和进行准确的分类。而且不同威胁的存在及其危害性是随环境的变化而变化的。下面是对现代信息系统及网络通信系统常遇到的一些威胁及其来源的概述。

正常的信息流向应当是从合法发送端源地址流向合法接收端目的地址,如图 1-1 所示:

1. 中断威胁

如图 1-2,中断(Interruption)威胁使得在用的信息系统毁坏或不能使用,即破坏可用性(Availability)。

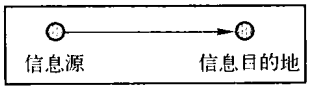

图 1-1 正常的信息流向

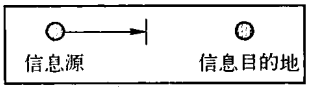

图 1-2 中断威胁

攻击者可以从下列几个方面破坏信息系统的可用性。

- 使合法用户不能正常访问网络资源。
- 使有严格时间要求的服务不能及时得到响应。
- 摧毁系统。物理破坏网络系统和设备组件使网络不可用,或者破坏网络结构使之瘫痪等。如硬盘等硬件的毁坏,通信线路的切断,文件管理系统的瘫痪等。

最常见的中断威胁是造成系统的拒绝服务,即信息或信息系统资源的被利用价值或服务能力下降或丧失。

2. 截获威胁

如图 1-3,截获(Interception)威胁是指一个非授权方介入系统,使得信息在传输中被丢失或泄露的攻击,它破坏了保密性(Confidentiality)。非授权方可以是一个人、一个程序或一台计算机。

这种攻击主要包括:

- 利用电磁泄漏或搭线窃听等方式可截获机密信息,通过对信息流向、流量、通信频度和长度等参数的分析,推测出有用信息,如用户口令、账号等。
- 非法复制程序或数据文件。

3. 篡改威胁

如图 1-4,篡改(Modification)威胁以非法手段窃得对信息的管理权,通过未授权的创建、修改、删除和重放等操作使信息的完整性(Integrity)受到破坏。

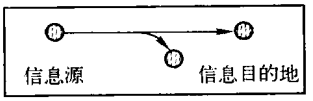

图 1-3 截获威胁

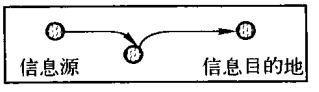

图 1-4 篡改威胁

这种攻击主要包括：

- 改变数据文件，如修改数据库中的某些值等。
- 替换某一段程序使之执行另外的功能，设置修改硬件。

4. 伪造威胁

如图 1-5，在伪造(Fabrication)威胁中，一个非授权方将伪造的客体插入系统中，破坏信息的可认证性(Authenticity)。例如，在网络通信系统中插入伪造的事务处理或者向数据库中添加记录。

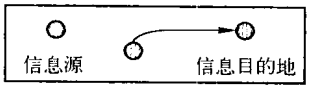

图 1-5 伪造威胁

1.1.3 脆弱点与安全控制

脆弱点(Vulnerability)是指信息系统中的缺陷，实际上脆弱点就是安全问题的根源所在，如原理设计及实现中的缺陷，它能被攻击者利用来进行破坏活动。下面从物理安全、操作系统、应用软件、TCP/IP 网络协议和人的因素等几个方面分析脆弱点。

1. 物理安全

计算机系统物理方面的安全主要表现为物理可存取、电磁泄漏等方面的问题。此外，物理安全问题还包括设备的环境安全、位置安全、限制物理访问、物理环境安全和地域因素等。由于这种问题是设计时所遗留的固有问题，一般除在管理上强化人工弥补措施外，采用软件程序的方法见效不大。

2. 软件系统

计算机软件可分为操作系统软件、应用平台软件(如数据库管理系统)和应用业务软件三类，以层次结构构成软件体系。操作系统软件处于基础层，它维系着系统硬件组件协调运行的平台，因此操作系统软件的任何风险都可能直接危及、转移或传递到应用平台软件。

应用平台软件处于中间层次，它是在操作系统支撑下，运行支持和管理应用业务的软件。一方面，应用平台软件可能受到来自操作系统软件风险的影响；另一方面，应用平台软件的任何风险可以直接危及或传递给应用业务软件。

应用业务软件处于顶层，直接与用户或实体打交道。应用业务软件的任何风险，都直接表现为信息系统的风险。

随着软件系统规模的不断增大，软件组件中的安全漏洞或“后门”也不可避免地存在，这也是信息安全问题的主要根源之一。比如常用的操作系统，无论是 Windows 还是 UNIX 几乎都存在或多或少的安全漏洞，各类服务器(典型的如微软的 IIS 服务器)、浏览器、数据库管理系统、一些桌面软件等都被发现过存在安全漏洞。可以说任何一个软件系统都会因为程序员的一个疏忽、设计中的一个缺陷等原因而存在漏洞，

3. 网络和通信协议

人们在享受因特网技术给全球信息共享带来的方便性和灵活性的同时，必须认识到基于 TCP/IP 协议栈的因特网及其通信协议存在很多的安全问题。TCP/IP 协议栈在设计时，只考虑了互联互通和资源共享的问题，并未考虑也无法同时解决来自网络的大量安全问题。例如，SYN Flooding 拒绝服务攻击，即是利用 TCP 协议三次握手中的脆弱点进行的攻击，用超过系统处理能力的消息来淹没服务器，使之不能提供正常的服务功能(第 5 章中将详细分析)。

4. 人的因素

人是信息活动的主体，人的因素其实是影响信息安全问题的最主要因素，看下面 3 种

情况。

1）人为的无意失误。如操作员安全配置不当造成的安全漏洞，用户安全意识不强，用户口令选择不慎，用户将自己的账号随意转借他人或与别人共享等都会给网络安全带来威胁。

2）人为的恶意攻击。人为的恶意攻击也就是黑客攻击，攻击可以分为以下两类：一类是主动攻击，它以各种方式有选择地破坏信息的有效性和完整性；另一类是被动攻击，它是在不影响网络正常工作的情况下，进行截获、窃取、破译以获得重要机密信息。由于现在还缺乏针对网络攻击卓有成效的反击和跟踪手段，使得许多黑客攻击的隐蔽性好、杀伤力强。

3）管理上的因素。网络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安全方面的管理。此外，管理的缺陷还可能出现在系统内部，例如，内部人员泄露机密或外部人员通过非法手段截获而导致机密信息的泄漏，从而为一些不法分子制造了可乘之机。

攻击者利用信息系统的脆弱点对系统进行攻击（Attack）。人们使用控制（Control）进行安全防护。控制是一些动作、装置、程序或技术，它能消除或减少脆弱点。可以这样描述威胁、控制和脆弱点的关系："通过控制脆弱点来阻止或减少威胁。"本书后续篇幅将主要介绍各种安全控制原理及技术。

1.1.4 计算机信息系统的安全需求

计算机信息系统的安全需求主要有：保密性、完整性、可用性、可控性、不可抵赖性和可存活性等。

1. 保密性（Confidentiality）

保密性是指确保信息资源仅被合法的用户、实体或进程访问，使信息不泄漏给未授权的用户、实体或进程。实现保密性的方法一般是通过信息的加密、对信息划分密级，并为访问者分配访问权限，系统根据用户的身份权限控制对不同密级信息的访问。

特别要说明的是，对计算机中央处理器、存储、打印设备的使用也必须实施严格的保密技术措施，以避免产生电磁泄露等安全问题。

2. 完整性（Integrity）

完整性是指信息资源只能由授权方或以授权的方式修改，在存储或传输过程中不丢失、不被破坏。完整性的破坏一般来自3个方面：未授权、未预期、无意。目前对于动态传输的信息，许多协议确保信息完整性的方法大多是收错重传、丢弃后续包。实际上，不仅仅要考虑数据的完整性，还要考虑操作系统的逻辑正确性和可靠性，要实现保护机制的硬件和软件的逻辑完备性、数据结构和存储的一致性。

3. 可用性（Availability）

可用性是指信息可被合法用户访问并按要求的特性使用而不遭拒绝服务。可用的对象包括：信息、服务和IT资源。例如，在网络环境下破坏网络和有关系统的正常运行就属于对可用性的攻击。信息的可用性与保密性之间存在一定的矛盾。为了控制非法访问，系统可以采取许多安全措施，但不应该阻止合法用户对系统中信息的利用。

4. 可控性（Controllability）

可控性是指保证信息和信息系统的认证授权和监控管理，确保某个实体（人或系统）身份的真实性，确保信息内容的安全性和合法性，确保系统状态可被授权方所控制。

5. 不可抵赖性(Non-Repudiation)

不可抵赖性通常又称为不可否认性,是指信息的发送者无法否认已发出的信息或信息的部分内容,信息的接收者无法否认已经接收的信息或信息的部分内容。不可否认性措施主要有:数字签名,可信第三方认证技术等。

6. 可存活性(Survivability)

可存活性是近年来学术界提出的一个安全概念。可存活性是指计算机系统的这样一种能力:它能在面对各种攻击或错误的情况下继续提供核心的服务,而且能够及时地恢复全部服务。这是一个新的融合计算机安全和业务风险管理的课题,它的焦点不仅是对抗计算机入侵者,还要保证在各种网络攻击的情况下业务目标得以实现,关键的业务功能得以保持。提高面对网络攻击的系统可存活性,同时也提高了业务系统在面对一些并非恶意的事故与故障的可存活性。

从广义上说,可存活性是一个工程的概念,它提供了一个自然的框架,可以把已有的或正在出现的软件工程概念集成到一个普通目标的服务中。这些已有的与可存活性相关的软件工程领域包括安全、容错、可靠、重用、性能、验证和测试等。

计算机安全专家又在已有计算机系统安全需求的基础上增加了可认证性(Authenticity)、实用性(Utility),认为这样才能解释各种网络安全问题。

信息的可认证性是指信息的可信度,主要是指对信息的完整性、准确性和对信息所有者或发送者身份的确认。可认证性比鉴别(Authentication)有更深刻的含义,它包含了对传输、消息和消息源的真实性进行核实。

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。

总之,计算机信息系统安全的最终目标集中体现为系统保护和信息保护两大目标。

1) 系统保护。保护实现各项功能的技术系统的完整性、可用性和可控性等。

2) 信息保护。保护系统运行中有关敏感信息的保密性、完整性、可用性和可控性。

1.2 信息安全概念的发展

信息安全的最根本属性是防御性的,主要目的是防止己方信息的保密性、完整性与可用性遭到破坏。信息安全的概念与技术随着人们的需求,随着计算机、通信与网络等信息技术的发展而不断发展。早期,在计算机网络广泛使用之前,人们主要是开发各种信息保密技术,随着因特网在全世界范围商业化应用之后,信息安全进入网络信息安全阶段,近几年又发展出了"信息保障"(Information Assurance,IA)的新概念。下面对此做一综述。

1. 单机系统的信息保密阶段

20 世纪 50 年代,计算机应用范围很小,安全问题并不突出,计算机系统并未考虑安全防护的问题。后来发生了袭击计算中心的事件,才开始对机房采取实体防护措施。但这时计算机的应用主要是单机,计算机安全主要是实体安全防护和硬、软件防护。多用户使用计算机时,将各进程所占存储空间划分成物理或逻辑上相互隔离的区域,使用户的进程并发执行而互不干扰,即可达到安全防护的目的。

20 世纪 70 年代,随着计算机在政府机关、金融、商业等部门的广泛应用,重要机密信息一

般都采用计算机处理,间谍和罪犯因此将计算机网络系统作为了侵犯的目标,计算机犯罪的案件不断发生。人们认识到,计算机安全关系到国家的安全和社会的稳定,并开始重视这个问题。许多人开始进行研究,并出现了计算机安全的法律、法规和各种防护手段,如防止非法访问的口令、身份卡、指纹识别等措施。这时计算机已由单机应用发展到计算机网络,除存储和数据处理外,发展到信息的远程传输,使网络受到攻击的部件增多,特别是传输线路和网络终端最为薄弱。这时,针对网络安全防护,出现了强制性访问控制机制、完善的鉴别机制和可靠的数据加密传输措施。

20 世纪 70 年代中期,在安全保密研究中出现了两个引人注目的事件。一是 Diffie 和 Hellman 冲破人们长期以来一直沿用的单钥体制,提出一种崭新的公开密钥密码体制;二是美国国家标准局(NBS)公开征集,并于 1977 年正式公布实施的美国数据加密标准(DES)。公开 DES 加密算法,并广泛应用于商用数据加密,这在安全保密研究史上是第一次,它揭开了密码学的神秘面纱,极大地推动了密码学的应用和发展。

除非不正确地使用密码系统,一般来说,好的密码难以破译。因此人们企图寻找别的方法来截获加密传输的信息。在 20 世纪 50 年代发现了寻找在电话线上的信号来达到获取报文的目的。大家知道,所有的电子系统都会释放电子辐射,包括电传机和正在使用发送加密报文的密码机。密码机将报文加密,并且通过电话线发送出去。可是代表原始信号的电信号也能在电话线上发现,这意味着可用某种好的设备来恢复原始信号。20 世纪 80 年代,国外发展出了以抑制计算机信息泄露为主的 TEMPEST 计划,它制定了用于十分敏感环境的计算机系统电子辐射标准,其目的是降低辐射以免信号被截获。

在 20 世纪 70 年代,David Bell 和 Leonard LaPadula 开发了一个安全计算机的操作模型(BLP 模型)。该模型是基于政府概念的各种级别分类信息(一般、秘密、机密、绝密)和各种许可级别。如果主体的许可级别高于文件(客体)的分类级别,则主体能访问客体;如果主体的许可级别低于文件(客体)的分类级别,则主体不能访问客体。

这个模型的概念进一步发展,20 世纪 80 年代中期,美国国防部计算机安全局公布了可信计算机系统安全评估准则(the Trusted Computing System Evaluation Criteria, TCSEC),即桔皮书,主要是规定了操作系统的安全要求。准则提高了计算机的整体安全防护水平,为研制、生产计算机产品提供了依据,至今仍具权威性。

进入 20 世纪 90 年代以来,信息系统安全保密研究出现了新的侧重点。一方面,对分布式和面向对象数据库系统的安全保密进行了研究;另一方面,对安全信息系统的设计方法、多域安全和保护模型等进行了探讨。随着信息系统的广泛建立和各种不同网络的互连、互通,人们意识到,不能再从安全功能、单个网络来个别地考虑安全问题,而必须从系统上、从体系结构上全面地考虑安全保密。

2. 网络信息安全阶段

因特网的快速发展与普及,使得老的安全问题仍以不同的形式出现,同时新的安全问题也不断出现。例如,各种局域网、城域网的安全不同于以往的远距离点到点的通信安全;高速网络以及由很多连接器连到一个公共的通信介质,原有的专用密码机已经完全不能解决问题;有很多用户从不同的系统经过网络访问,而没有对单个计算机的集中控制。如何解决在开放网络环境下的信息安全问题便成为迫切需要解决的问题。

人们不仅需要考虑信息系统本身的安全问题,还要考虑可能来自网络环境的攻击造成的

问题。1988 年 11 月 3 日莫里斯“蠕虫”造成因特网几千台计算机瘫痪的严重网络攻击事件，引起了人们对网络信息安全的关注与研究，并于第二年成立了计算机紧急事件处理小组负责解决因特网的安全问题，从而开创了网络信息安全的新阶段。

国际标准化组织在开放系统互联标准中定义了 7 个层次的 OSI 网络参考模型，它们分别是物理层、数据链路层、网络层、传输层、会话层、表示层和应用层。TCP/IP 是因特网的通信协议，通过它将不同特性的计算机和网络（甚至是不同的操作系统、不同硬件平台的计算机和网络）互联起来。TCP/IP 协议族包括 4 个功能层：应用层、传输层、网络层和网络接口层。这 4 层概括了相对于 OSI 参考模型中的 7 层。

从安全角度来看，一个单独的层次无法提供全部的网络安全服务，各层都能提供一定的安全手段，针对不同层的安全措施是不同的。

应用层的安全主要是指针对用户身份进行认证并且建立起安全的通信信道。有很多针对具体应用的安全方案，它们能够有效地解决诸如电子邮件、HTTP 等特定应用的安全问题，能够提供包括身份认证、不可否认、数据保密、数据完整性检查乃至访问控制等功能（本书 5.7.1 介绍）。

在传输层，因为 IP 包本身不具备任何安全特性，很容易被修改、伪造、查看和重播。在传输层设置密码算法（SSL）来保护 Web 通信安全是很实用的选择（本书 5.7.2 介绍）。

在网络层，可以使用防火墙技术控制信息在内外网络边界的流动；可以使用 IPsec 对网络层上的数据包进行安全处理（本书 5.7.3 介绍）。

在数据链路层，点对点的链路可能采用通信保密机进行加密和解密，当信息离开一台机器时进行加密，而进入另外一台机器时进行解密。所有的细节可以全部由底层硬件实现，高层根本无法察觉。但是这种方案无法适应需要经过多个路由器的通信信道，因为在每个路由器上都需要进行加密和解密，在这些路由器上会出现潜在的安全隐患，在开放网络环境中并不能确定每个路由器都是安全的。当然，链路加密在因特网环境中并不完全适用。

在物理层，可以在通信线路上使得搭线监听变得不可能。

虽然上述各层解决方案都有一定的作用，但是研究者还在不断研究探索，提高这些技术。

总结前面的讨论，可以用图 1-6 来表示网络安全层次。

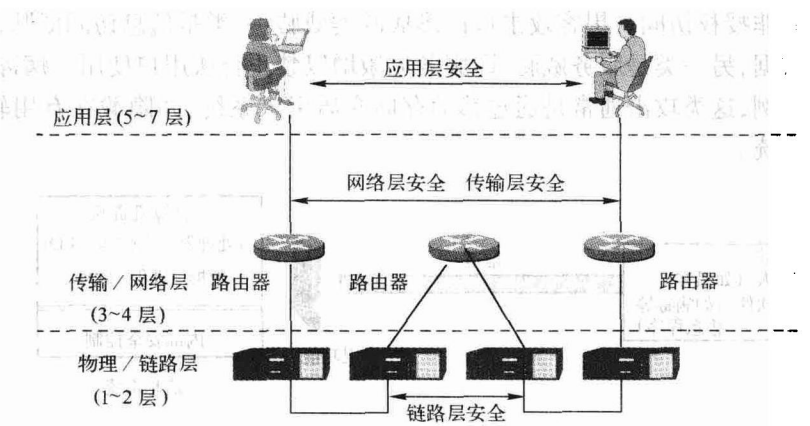

图 1-6 网络安全层次图

图 1-7 给出了一个网络保密安全基本模型，通信双方要传递某个消息，需要建立一个逻辑信息通道包括：确定从发送方到接受方的路由以及两方协同使用诸如 TCP/IP 协议。

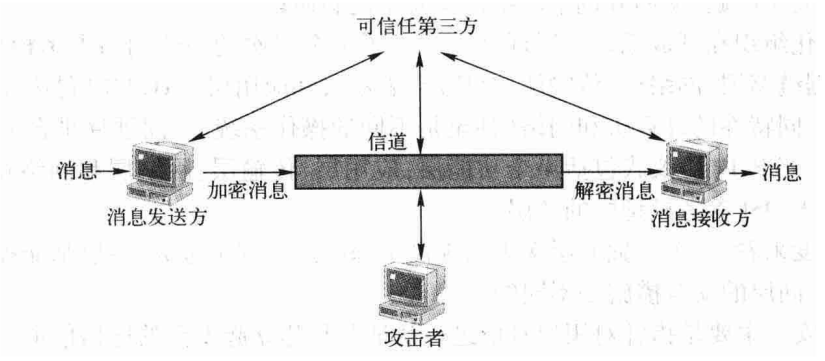

图 1-7　网络保密安全模型

为了在开放网络环境中保护信息的传输，需要提供安全机制和安全服务，主要包含以下两个部分。

1）消息的安全传输，包括对消息的加密与认证。例如，消息的加密，使开放网络对加密的消息不可读；又如附加一些基于消息内容的编码，用来验证发送者的身份。

2）双方共享秘密信息的分发。例如，用于发送前的加密密钥和接收后的解密密钥。

为了完成安全的消息传递，常常需要可信的第三方。其作用是负责为通信双方分发秘密信息，或者是在双方有争议时进行仲裁。

归纳起来，该网络保密安全模型必须包含以下 4 个基本内容。

1）建立一种加密算法。

2）产生一个用于加密算法的密钥。

3）开发一个分发和共享秘密信息的方法。

4）使用加密算法与秘密信息以得到特定安全服务所需的协议。

图 1-7 的网络保密安全模型虽是一个通用的模型，但它着重保护信息的机密性和可认证性，不能涵盖所有安全需求。图 1-8 给出了一个网络访问安全模型，该模型考虑了黑客攻击、病毒与蠕虫等的非授权访问。黑客攻击可以形成两类威胁：一类是信息访问威胁，即非授权用户截获或修改数据；另一类是服务威胁，即服务流激增以禁止合法用户使用。病毒和蠕虫是软件攻击的两个实例，这类攻击通常是通过移动存储介质引入系统，并隐藏在有用软件中，也可通过网络接入系统。

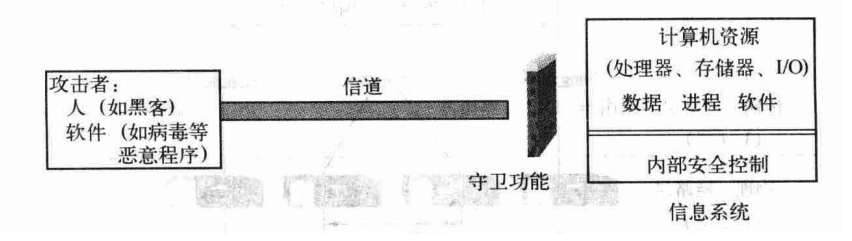

图 1-8　网络访问安全模型