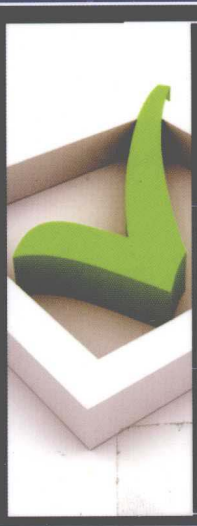
21世纪高等院校计算机专业规划教材



网络与信息安全

（第二版）

王凤英　程　震　主编

中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE

21 世纪高等院校计算机专业规划教材

网络与信息安全

（第二版）

王凤英　程　震　主编

中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE

内 容 简 介

本书系统地阐述了网络与信息安全的各种知识，主要内容包括：网络与信息安全的基本概念；密码学及加密技术的使用；操作系统、数据库和防火墙的安全配置；公钥基础设施、访问控制、系统审计、VPN、入侵检测等安全技术；现代加密的新型研究方向——混沌密码和量子密码；近几年的研究热点——信息隐藏与数字水印；IPv6 的安全；网络与信息安全实验等。为了学以致用，每章后面都有习题，可以作为课程作业或复习要点。本书将理论知识和实际应用有机地结合在一起，以实际应用中经常遇到的问题作为案例。

本书的内容经过精心编排，适合作为计算机、信息安全、通信、计算机网络等专业本科生、研究生的教材或学习参考书，对相关领域研究人员和专业技术人员也具有一定的参考价值。

图书在版编目（CIP）数据

网络与信息安全/王凤英，程震主编. --2 版. --
北京：中国铁道出版社，2010.6
21 世纪高等院校计算机专业规划教材
ISBN 978-7-113-11413-8

Ⅰ. ①网… Ⅱ. ①王… ②程… Ⅲ. ①计算机网络－安全技术－高等学校－教材 Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字（2010）第 088523 号

书　　名：网络与信息安全（第二版）
作　　者：王凤英　程　震　主编

策划编辑：秦绪好　孟　欣
责任编辑：孟　欣　　**编辑部电话：**（010）63560056
编辑助理：赵　鑫
封面设计：付　巍　　**封面制作：**白　雪
版式设计：郑少云　　**责任印制：**李　佳

出版发行：中国铁道出版社（北京市宣武区右安门西街 8 号　　邮政编码：100054）
印　　刷：三河市华丰印刷厂
版　　次：2006 年 6 月第 1 版　2010 年 6 月第 2 版　2010 年 6 月第 3 次印刷
开　　本：787mm×1092mm　1/16　**印张：**20.25　**字数：**498 千
印　　数：3 000 册
书　　号：ISBN 978-7-113-11413-8
定　　价：32.00 元

版权所有　侵权必究
本书封面贴有中国铁道出版社激光防伪标签，无标签者不得销售
凡购买铁道版图书，如有印制质量问题，请与本社计算机图书批销部联系调换。

第二版前言

FOREWORD >>>

本书是《网络与信息安全》(王凤英、程震主编，书号：978-7-113-07058-2/TP·1810，中国铁道出版社)的第二版。本书本次修订的指导思想是：摒弃相对陈旧、过时的技术，增加了对信息安全有重要影响的一些新内容；对一些章节的内容和顺序进行了较大幅度的调整，在许多章节中增加了案例；为了增加可读性，新加了对某些领域有重要贡献的科技人物的扩展阅读；为了学以致用，增加了6个实验。

信息时代，人们越来越多地依赖信息进行研究和决策。互联网是人类文明的巨大成就，它带给人们获取信息和交换信息的极大便利。但互联网是开放的系统，具有很多的不安全因素。如何保证网络中计算机和信息的安全是一个重要且复杂的问题。目前，研究网络信息安全已经不仅仅只是为了信息和数据的安全，网络信息安全已经渗透到国家的政治、经济、军事等领域。

本书力求精练、新颖、实用，作者除了将最近研究的成果加进来以外，还查阅了大量资料，将最新、最有研究和应用价值的内容补充进来。为做到理论和应用技术的结合，使之对实践有一定的指导作用，花费了较多的时间和精力收集了一些实际应用中的案例，这在其他同类著作中是难得一见的。本书具有如下特点：

(1)系统的理论体系。本书力求介绍完善的理论知识，在介绍密码知识时涉及加密算法的各个方面，系统地介绍了各种重要的访问控制模型，有利于读者系统全面地了解和掌握书中内容。

(2)有针对性的案例。为了体现这些知识的重要性，在重要的理论知识之后，紧接着就是实际应用案例。通过这些案例的学习，一方面能加深对知识的理解，另一方面易激发学生的学习兴趣，同时还有利于培养学生解决实际问题的能力。

(3)密切联系实际。本书在介绍操作系统安全、数据库安全、防火墙和 PGP 等内容时，实时介绍它们的安全配置和使用方法，让读者觉得本书的内容在自己的计算机中就能找到，达到了学以致用的目的。第16章设计了6个网络与信息安全方面的实验，具有一定深度的实践知识。

(4)可读性强。为了增加教材的可读性，在每章开头用简洁生动的语言表达编者鲜明的立场，以达到循循善诱的目的；为了激发读者的兴趣，介绍了对信息安全有重要影响的科技人物。

如果读者想获得与本书配套的教学大纲、实验大纲、教学幻灯片、源代码等其他资源，可发邮件到以下邮箱：chengzhen@sdut.edu.cn；wfy@sdut.edu.cn。

本书的教学课时为40～60学时，实验需另外安排。

感谢所有对本书的出版做出贡献的人，没有他们的帮助和督促，就没有本教材的面世。在成书的过程中，他们给予了热忱的帮助和关怀。当然还要感谢广大的读者，欢迎您提出宝贵的建议和批评，我们将会在本书再版时进行更正和补充。

限于编者水平和所涉及知识范畴，书中难免存在纰漏和错误之处，殷切希望各位读者批评指正。

编　者

2010年4月

第一版前言

信息时代，人们越来越依赖信息进行研究和决策，互联网是人类文明的巨大成就，它给人们带来了极大的便利。但是，计算机网络是开放的系统，具有众多的不安全因素。如何保证网络中计算机和信息的安全是一个重要且复杂的问题。目前研究网络信息安全已经不仅仅只是为了信息和数据的安全，网络信息安全已经渗透到国家的政治、经济、军事等领域。

本书分为4个部分。

第一部分是网络与信息安全综述，涵盖了网络与信息安全方面的基本概念。包括网络安全的层次结构、安全模型、基本安全技术以及网络安全的国内外评价标准。

第二部分是信息加密与信息隐藏。包括对称密钥密码体系、单向散列函数、非对称密钥密码体系、混沌密码和量子密码体系、信息隐藏技术和数字水印等。

第三部分是系统安全机制，涵盖了操作系统安全、因特网安全、VPN、IPSec和数据库系统安全。

第四部分是安全技术与产品，包括身份认证、PKI技术、WPKI、电子邮件安全及PGP、Web电子商务安全、防火墙技术、访问控制、系统审计、PMI、计算机病毒与防范、入侵检测和网络安全管理。

本书力求精炼、新颖、实用，除了将作者最近研究的成果加进来以外，还查阅了大量资料，将最新、最有研究和应用价值的内容补充进来。为做到理论和应用技术的结合，使之对实践有一定的指导作用，花费了较多的时间和精力，列举了一些实际应用例子，这在其他同类著作中是难得一见的。

如果读者想获得与本书配套的教学大纲、实验大纲、教学幻灯片、源代码等其他资源，可发邮件联系我们。我们的邮箱是：chengzhen@sdut.edu.cn；wfy@sdut.edu.cn。

本书的教学课时为40～60学时，实验需另外安排。

感谢所有对本书的出版产生了影响的人，特别要致谢杨东晓先生，没有他们的帮助和督促，就没有这本书的面世。在成书的过程中，他们给予了热忱帮助和关怀。

当然还要感谢广大的读者，欢迎提出宝贵的建议和批评，我们将会在本书的新版本中更正和补充。

编　者

2006年4月

试读结束：需要全本请在线购买：　www.ertongbook.com

目 录

CONTENTS >>>

第1章 网络信息安全综述

学习目标

- 掌握网络信息安全的基本概念。
- 理解网络提供的安全服务。
- 了解网络安全标准。
- 掌握网络安全的层次。
- 理解安全机制的内容。

关键术语

- 国际标准化组织（International Standard Organization, ISO）
- 开放系统互连参考模型（Open Systems Interconnection Reference Model，OSI/RM）
- 因特网工程任务组（Internet Engineering Task Force，IETF）
- 安全超文本传输协议（Secure HyperText Transfer Protocol，S-HTTP）
- 安全套接字层（Secure Sockets Layer，SSL）
- 保密通信技术（Private Communication Technology，PCT）
- 身份认证（Authentication）
- 完整性（Integrity）
- 保密性（Privacy）
- 不可否认（Non-repudiation）
- 审计（Accountability）
- 访问控制（Access Control）

没有绝对的安全，安全总是相对的。要求构成网络和信息安全的某个要素一枝独秀会得不偿失，只有各安全要素齐头并进才能达到事半功倍的安全效果。

信息时代，人们越来越多地依赖信息进行研究和决策，信息的安全性决定了研究和决策的水平，对信息的安全性要求与日俱增。互联网是人类文明的巨大成就，它在给人们带来了巨大便利的同时，也蕴含着诸多安全方面的隐患，保证网络中计算机和信息的安全是一个系统工程。本章首先概要地讨论网络与信息安全的标准及一般问题，使读者对网络与信息安全有一个概括性的认识，为学习以后章节打下基础。

1.1 网络与信息安全的基本概念

网络用来传输信息、交换信息，计算机用来处理信息、存储信息。没有计算机，网络难以完成传输信息、交换信息的任务。同样地，没有网络，计算机就不能充分发挥处理信息、存储信息

试读结束：需要全本请在线购买： www.ertongbook.com

的作用。若没有计算机和网络，海量的信息就无法传输、处理、存储，我们这个时代也就不能称为信息时代。21 世纪，计算机、网络和信息这三个概念已变得唇齿相依、相辅相成、不可分割，探讨和研究三者中的任何一个问题，都离不开另外的两者。涉及网络安全的问题，也都与信息安全和计算机安全相关。

网络是把双刃剑，人们在享受着网络所提供的各种便利的同时，也面临着网络安全隐患带来的各种困扰。若想无忧地使用网络和信息，必须研究并解决存在的诸多安全问题。网络安全已发展为计算机科学的一个重要分支，而网络安全的内涵非常丰富，它涉及法律学、犯罪学、心理学、经济学、应用数学、数论、计算机科学、加密学及审计学等相关学科。

由于网络的定义有多种，所以各种关于网络与信息安全的定义也不同。有的定义说：网络安全就是保护网上保存和流动的数据不被他人偷看、窃取或修改。也有的定义为：信息安全是指保护信息财产，以防止偶然的或未授权者对信息的泄露、修改和破坏，从而导致信息的不可信或无法处理。综合来看，我们认为，计算机网络安全是指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保密性、完整性及可使用性受到保护。网络安全的主要目标是要确保经网络传送的信息，在到达目的站时没有任何增加、改变、丢失或被非法读取。要做到这一点，必须保证网络中系统软件、应用软件系统、数据库系统具有一定的安全保护功能，并保证所有网络部件，如终端、调制解调器、数据链路等的功能不被改变，而且只有那些经过认证的被授权的用户才可以访问。

网络的安全性问题实际上包括两方面的内容。一是网络的系统安全，保护计算机不被黑客入侵就属于系统安全的范畴；二是网络的信息安全，一般有以下 4 项要求：

（1）机密性，即消息只有合法的接收者才能读出，其他人即使收到也读不出。

（2）真实性，即消息的确是由宣称的发送者发送的，如冒名顶替则会被发现。

（3）完整性，即消息在传输过程中如果篡改则会被发现。

（4）抗抵赖，即消息的发送者在发送后不能否认他发送过该消息。

近年来利用广泛开放的物理网络环境进行全球通信已成为时代发展的趋势，但是如何在一个开放的物理环境中构造一个封闭的逻辑环境来满足部门或个人的实际需要，已成为必须要考虑的现实问题。开放性的系统常常由于结点分散、难于管理等特点而易受到攻击和蒙受不法操作带来的损失，若没有安全保障，则系统的开放性将会带来灾难性的后果。网络的开放和安全本身是一对矛盾，如果想“鱼和熊掌”兼得，就必须对开放系统的安全性进行深入和自主的研究，找到并理清实现开放系统的安全性所涉及的关键技术环节，并掌握设计和实现开放系统的安全性的方案和措施。

被网络安全界广泛采用的著名的“木桶理论”认为，整个系统的安全防护能力，取决于系统中安全防护能力最薄弱的环节。木桶原理指的是：一个木桶由许多块木板组成，如果组成木桶的这些木板长短不一，那么木桶的最大容量不取决于长的木板，而取决于最短的那块木板。信息从产生到销毁的生命周期中包括了产生、收集、加工、交换、存储、检索、存档、销毁等多个事件，表现形式和载体会发生各种变化，这些环节中的任何一个都可能影响整体信息安全水平。以一份需要保密的内部文件为例，它的生命周期包括起草、审批、传送、分发、归档、销毁这些环节。在这份文件存在的生命周期内，有无数可能会导致信息安全的问题。例如，电子文件保存在非授权用户可以访问的磁盘位置、文件分发时没有明确的接收对象、在基层组织的阅读范围被擅自扩大、传输中被非法者截获、文件内容被篡改、文件内容的可信程度、文件来源的可靠性等。

网络与信息安全有一个整体安全要求，任何一个安全环节的疏漏都有可能功亏一篑、事倍功半。因此，要从整体上提高一个组织的信息安全水平，必须保证信息在整个生命周期中的安全。要实现这个目标，一个组织必须制定严格的、系统的安全保密办法来保证信息安全，包括高层领导授权、保密政策、实施办法、监督检查制度、员工安全意识培训、可靠的技术设备等，也就是要使构成安全防范体系的这只“木桶”的所有木板拥有相近的长度。

1.2　网络安全威胁

因特网在设计之初以提供广泛的互联、互操作、信息资源共享为目的，仅考虑使用的便利性，没有考虑安全问题，导致今天的因特网存在诸多不安全因素。随着因特网的发展，其规模越来越大，通信链路越来越长，网络的安全问题也随之增加。这在当初把因特网作为科学研究用途时是可行的，但是在当今电子商务和电子政务炙手可热之时，网络安全问题已经成了一种障碍。

因特网上缺乏统一的安全标准，尽管标准众多，但没有达成共识。众所周知，IETF（Internet Engineering Task Force，因特网工程任务组）负责开发和发布因特网标准。随着因特网商业味道越来越浓，各个制造商为了各自的经济利益均采用自己的标准，而不是遵循 IETF 的标准化进程，这使得 IETF 的地位变得越来越模糊不清，从下面列举的由不同组织开发的安全通信协议标准，便可见一斑，包括安全超文本传输协议（Secure HyperText Transfer Protocol，S-HTTP）、安全套接字层（Secure Sockets Layer，SSL）和保密通信技术（Private Communication Technology，PCT）。

1.2.1　网络安全威胁的类型

威胁定义为对缺陷的潜在利用，这些缺陷可能导致非授权访问、信息泄露、资源耗尽、资源被盗或者被破坏等。网络安全所面临的威胁可来自很多方面，并且是随着时间的变化而变化的。网络安全的威胁既可以来自内部网又可以来自外部网，根据不同的研究结果表明，大约有 70%～85%的安全事故来自内部网。显然，只有少数网络攻击是来自因特网的。一般而言，主要的威胁种类有如下几种：

（1）窃听。在广播式网络信息系统中，每个结点都能读取网上传输的数据。对广播网络的双绞线进行搭线窃听是很容易的，安装通信监视器和读取网上的信息也很容易。网络体系结构允许监视器接收网上传输的所有数据帧而不考虑帧的传输目的地址，这种特性使得黑客等很容易窃取网上的数据或非授权访问且不易被发现。

（2）假冒。当一个实体假扮成另一个实体时就发生了假冒。一个非授权结点，或一个不被信任的、有危险的授权结点都能冒充一个完全合法的授权结点，而且不会有多大困难。很多网络适配器都允许网络数据帧的源地址由结点自己来选取或改变，这就使冒充变得较为容易。

（3）重放。重放是攻击方重新发送一份合法报文或报文的一部分，以使被攻击方认为自己是合法的或被授权的。当某结点复制发到其他结点的报文并在其后重发它们时，如果不能检测重发，目标结点会依据此报文的内容接受某些操作。例如，报文的内容是以前发送过的合法口令，则将会出现严重的后果。

（4）流量分析。指通过对网上信息流的观察和分析推断出网上的数据信息，例如有无传输，传输的数量、方向、频率等。因为网络信息系统的所有结点都能访问全网，所以流量的分析易

于完成。由于报头信息不能被加密，所以即使对数据进行了加密处理，也可以进行有效的流量分析。

（5）破坏完整性。有意或无意地修改或破坏信息系统，或者在非授权和不能监测的方式下对数据进行修改，使得接收方得不到正确的数据。

（6）拒绝服务。当一个授权实体不能获得应有的对网络资源的访问或紧急操作被延迟时，就发生了拒绝服务。拒绝服务可能由网络部件的物理损坏而引起，也可能由使用不正确的网络协议（如传输了错误的信号或在不适当的时候发出了信号）、超载或者某些特定的网络攻击（如信息包洪水——Packet Flood）引起。

（7）资源的非授权使用。即与所定义的安全策略不一致的使用。因常规技术不能限制结点收发信息，也不能限制结点侦听数据，所以一个合法结点能访问网络上的所有数据和资源，为此，必须采用某些措施加以限制。

（8）特洛伊木马。非法程序隐藏在一个合法程序里从而达到其特定的目的（如盗取用户的敏感数据）。这可以通过替换系统合法程序，或者在合法程序里插入恶意代码来实现。

（9）病毒。目前，全世界已经发现了上万种计算机病毒，而且新型病毒还在不断出现。比如，保加利亚计算机专家迈克·埃文杰制造出的一种计算机病毒——“变换器”，它可以设计出新的更难发现的“多态变形”病毒。该病毒具有类似神经网络细胞式的自我变异功能，在一定的条件下，病毒程序可以无限制地衍生出各种各样的变种病毒。随着计算机技术的不断发展和人们对计算机系统和网络依赖程度的增加，计算机病毒已经对计算机和网络构成了严重威胁。

（10）诽谤。利用网络信息系统的广泛互联性和匿名性，散布错误的消息以达到诋毁某人或某组织形象和知名度的目的。

1.2.2 网络安全威胁的动机

俗话说，知己知彼百战百胜。互联网上面临如此众多的安全威胁，找到这些安全威胁的动机是解决安全问题的重要问题。威胁安全问题的实体是入侵者，因此识别入侵者是一项烦琐而艰巨的任务。了解攻击的动机可以帮助用户洞察网络中哪些部分容易受攻击以及攻击者最可能采取什么行动。在网络入侵的背后，通常有以下 5 种形式的动机。

1. 商业间谍

所谓商业间谍，就是为了获取商业秘密，渗透进入某公司内部，搜寻该公司的秘密并出卖给其竞争者的人。攻击者的主要目的是阻止被攻击站点检测到公司的系统安全已受到危害，同时大量窃取机密信息。随着企业内部网大量接入因特网，商业间谍引起了人们广泛关注。按照 FBI 的估计，由于商业间谍的危害，美国各大公司每年要损失 100 亿美元以上。

最近的研究表明，商业贸易经常受到来自公司内部持有异议和不诚实雇员的攻击。这些攻击包括收集机密信息、滥用职权及其物理访问权、内部黑客、雇佣外来黑客等。

2. 经济利益

经济利益是另外一种比较普遍的网络攻击目的。攻击者获取非授权访问，然后偷取钱财或者资源以获得经济利益。如一名不诚实的职员将资金从公司的账号上转移到自己的私人账号上；因特网上的一名黑客可能进入银行系统进行非授权访问并转移资金。

3. 报复或引人注意

网络同样可以出于报复目的或者为了扬名的目的而被攻击。被解雇的职员可以在离开公司之前安装特洛伊木马程序到公司的网络上。有时候，一名黑客会攻破一个网络来炫耀其技能以便扬名。有些销售商为了完善自己的网络安全产品也会给成功入侵他们网络安全产品的人们提供奖金。

4. 恶作剧

入侵者闲得无聊又具备一定的计算机知识，因此总想访问他所感兴趣的但又被拒绝访问或要求付费的站点。

5. 无知

入侵者正在学习计算机和网络，无意中发现的一些弱点可能导致数据被毁或者执行非法操作。

1.3　网络安全的层次结构

网络安全的层次结构主要包括物理安全、安全控制和安全服务。

1.3.1　物理安全

物理安全是指在物理介质层次上对存储和传输的网络信息的安全保护。物理安全是网络信息安全的最基本保障，是整个安全系统不可缺少和不可忽视的组成部分。

一方面，在各种软件和硬件系统中要充分考虑到系统所受的物理安全威胁和相应的防护措施；另一方面，也要通过安全意识的提高、安全制度的完善、安全操作的提倡等方式使用户和管理维护人员在物理层次上实现对网络信息的有效保护。目前，该层次上常见的不安全因素包括三大类：

（1）自然灾害（如地震、火灾、洪水等）、物理损坏（如硬盘损坏、设备使用寿命到期、外力破损等）和设备故障（如停电、断电、电磁干扰等）等。此类不安全因素的特点是：突发性、自然性及非针对性。这类不安全因素对网络信息的完整性和可用性威胁最大，而对网络信息的保密性影响却较小，因为在一般情况下，物理上的破坏将销毁网络信息本身。解决此类不安全隐患的有效方法是采取各种防护措施，制定安全规章制度，随时进行数据备份等。

（2）电磁辐射（如侦听计算机操作过程）、乘机而入（如合法用户进入安全区域后未采取措施离开）和痕迹泄露（如口令密钥等保管不善，被非法用户获得）等。此类不安全因素的特点是：隐蔽性、人为实施的故意性、信息的无意泄露性。这类不安全因素主要破坏网络信息的保密性，而对网络信息的完整性和可用性影响不大。解决此类不安全隐患的有效方法是采取辐射防护、制定安全规章制度、屏幕保护口令、隐藏销毁、提高用户安全意识等。

（3）操作失误（如偶然删除文件、格式化硬盘、线路拆除等）和意外疏漏（如系统断电、系统崩溃）等。此类不安全因素的特点是：人为实施的无意性和非针对性。这类不安全因素主要破坏网络信息的完整性和可用性，而对保密性影响不大。解决此类不安全隐患的有效方法是状态检测、报警确认、应急恢复等。

1.3.2　安全控制

安全控制是指在网络信息系统中对存储和传输信息的操作和进程进行控制和管理，重点是在网络信息处理层次上对信息进行初步的安全保护。安全控制可以分为以下 3 个层次：

（1）操作系统的安全控制。包括对用户的合法身份进行核实（如开机时要求键入口令）和对文件的读/写存取的控制（如文件属性控制机制）等。此类安全控制主要保护被存储数据的安全。

（2）网络接口模块的安全控制。指在网络环境下对来自其他机器的网络通信进程进行安全控制。此类控制主要包括身份认证、客户权限设置与判别、审计日志等。

（3）网络互连设备的安全控制。指对整个子网内的所有主机的传输信息和运行状态进行安全监测和控制。此类控制主要通过网管软件或路由器配置实现。

需要指明的是，安全控制主要通过现有的操作系统或网管软件、路由器配置等实现；安全控制只提供了初步的安全功能和网络信息保护。

1.3.3 安全服务

提供安全服务是网络服务的终极目标。安全服务是指在应用程序层对网络信息的保密性、完整性和信源的真实性进行保护和鉴别，以满足用户的安全需求，防止和抵御各种安全威胁和攻击。安全服务可以在一定程度上弥补和完善现有操作系统和网络信息系统的安全漏洞。安全服务的主要内容包括：安全机制、安全连接、安全协议、安全策略等。

（1）安全机制是系统用来检测、预防或从安全攻击中恢复的机制。它可以利用密码算法对重要而敏感的数据进行处理。例如：以保护网络信息的保密性为目标的数据加密和解密；以保证网络信息来源的真实性和合法性为目标的数字签名和签名验证；以保护网络信息的完整性，防止和检测数据被修改、插入、删除和改变为目标的信息认证等。也可以采取其他一些安全技术，如防火墙、入侵检测系统等来实现安全机制。安全机制是安全服务乃至整个网络信息安全系统的核心和关键。

（2）安全连接是在安全处理前网络通信双方之间的连接过程。安全连接为安全处理进行了必要的准备工作。安全连接主要包括会话密钥的产生、分发和身份验证，后者旨在保护信息处理和操作的对等、双方身份的真实性和合法性。

（3）安全协议是多个实体为完成某些安全任务所采取的一系列有序步骤。协议的特性是：预先建立、相互同意、非二义性和完整性。安全协议使网络环境下互不信任的通信方能够相互配合，并通过安全连接和安全机制的实现来保证通信过程的安全性、可靠性和公平性。

（4）安全策略是决策的集合。它集中体现了一个组织对安全的态度。更确切地说，安全策略对于可接受的行为以及应对违规行为作出何种响应确定了界限。安全策略是安全机制、安全连接和安全协议的有机组合，是网络信息系统安全的完整解决方案。安全策略决定了网络信息安全系统的整体安全性和实用性。不同的网络信息系统和不同的应用环境需要不同的安全策略。

1.4 安全评价标准

在很长的一段时间里，计算机系统的安全性依赖于计算机系统的设计者、使用者和管理者对安全性的理解和所采取的措施，因此所谓安全的计算机对于不同的用户有不同的标准和实际安全水平。为了规范对计算机安全的理解和实际的计算机安全措施，许多发达国家相继建立了用于评价计算机系统的可信程度的标准。

1.4.1　可信计算机系统评估准则

为了保障计算机系统的信息安全，1985 年，美国国防部发表了《可信计算机系统评估准则》（缩写为 TCSEC，因为其封面是橙色的，所以也称网络安全橙皮书），它依据处理的信息等级采取相应的对策，划分了 4 类 7 个安全等级。依照各类、级的安全要求从低到高，依次是 D、C1、C2、B1、B2、B3 和 A1 级。

（1）D 级：最低安全保护（Minimal Protection）。没有任何安全性防护，如 DOS 和 Windows 95/98 等操作系统。

（2）C1 级：自主安全保护（Discretionary Security Protection）。这一级的系统必须对所有的用户进行分组；每个用户必须注册后才能使用；系统必须记录每个用户的注册活动；系统对可能破坏自身的操作将发出警告。用户可保护自己的文件不被别人访问，如典型的多用户系统。

（3）C2 级：可控访问保护（Controlled Access Protection）。在 C1 级基础上，增加了以下要求：所有的客体都只有一个主体；对于每个试图访问客体的操作，都必须检验权限；只有主体和主体指定的用户才可以更改权限；管理员可以取得客体的所有权，但不能再归还；系统必须保证自身不能被管理员以外的用户改变；系统必须有能力对所有的操作进行记录，并且只有管理员和由管理员指定的用户可以访问该记录。具备审计功能，不允许访问其他用户的内存内容和恢复其他用户已删除的文件。SCO UNIX 和 Windows NT 系统属于 C2 级。

（4）B1 级：标识的安全保护（Labeled Security Protection）。在 C2 的基础上，增加以下要求：不同组的成员不能访问对方创建的客体，但管理员许可的除外；管理员不能取得客体的所有权；允许带级别的访问控制，如一般、秘密、机密、绝密等。Windows NT 的定制版本可以达到 B1 级。

（5）B2 级：结构化保护（Structured Protection）。在 B1 的基础上，增加以下几条要求：所有的用户都被授予一个安全等级；安全等级较低的用户不能访问高等级用户创建的客体。银行的金融系统通常达到 B2 级，提供结构化的保护措施，对信息实现分类保护。

（6）B3 级：安全域保护（Security Domain）。在 B2 的基础上，增加以下要求：系统有自己的执行域，不受外界干扰或篡改；系统进程运行在不同的地址空间从而实现隔离；具有高度的抗入侵能力，可防篡改，进行安全审计事件的监视，具备故障恢复能力。

（7）A1 级：可验证设计（Verified Design）。在 B3 的基础上，增加以下要求：系统的整体安全策略一经建立便不能修改；计算机的软、硬件设计均基于正式的安全策略模型，可通过理论分析进行验证；生产过程和销售过程也绝对可靠，但目前尚无满足此条件的计算机产品。

其中，C 类称为酌情保护，B 类称为强制保护，A 类称为核实保护。

这个标准过分强调了保密性，而对系统的可用性和完整性重视不够，因此实用性较低。为此，美国 NIST 和国家安全局于 1993 年为那些需要十分重视计算机安全的部门制定了一个“多用户操作系统最低限度安全要求”，其中为系统安全定义了 8 种特性：

（1）识别和验证：系统应该建立和验证用户身份，这包括用户应提供一个唯一的用户标识符，使系统可用它来确认用户身份；同时用户还需提供系统知晓的确认信息，如一个口令，以便系统确认。系统应具有保护这些鉴别信息不被越权访问的能力。

（2）访问控制：系统应确保履行其职责的用户和过程不能对其未授权的信息或资源进行访问；系统访问控制的粒度应为单个用户；识别和验证应在系统和用户的其他交互动作之前进行；对系统和其他资源的访问应限于获得相应访问权的用户。

试读结束：需要全本请在线购买：　www.ertongbook.com