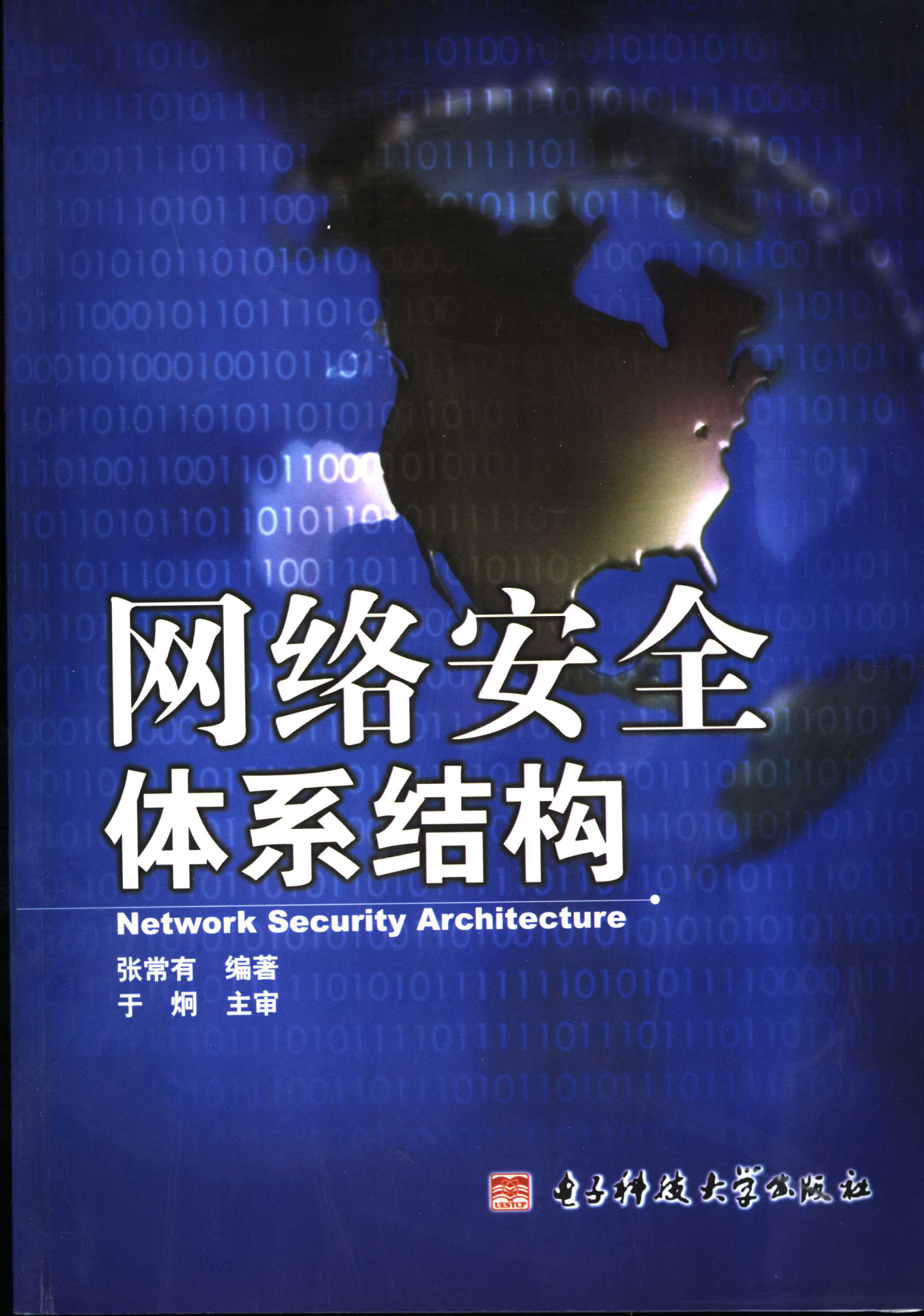

网络安全体系结构

Network Security Architecture

张常有　编著
于　炯　主审

电子科技大学出版社

网络安全体系结构

张常有　编著

于　炯　主审

电子科技大学出版社

图书在版编目（CIP）数据

网络安全体系结构 / 张常有编著. —成都：电子科技大学出版社，2006.9

ISBN 7-81094-597-1

Ⅰ.网… Ⅱ.张… Ⅲ.计算机网络—安全技术 Ⅳ.TP393.08

中国版本图书馆 CIP 数据核字（2006）第 089421 号

内 容 提 要

网络安全的重要性正伴随着 Internet 应用的发展和普及而日益突出。本书系统讲述了网络安全的理论、原理、技术和应用等。主要内容包括：对称加密算法、公钥加密算法、安全散列算法、数字签名、网络安全协议（PPP、IPSec、SSL 等）、操作系统平台安全加固措施、网络隔离（物理隔离、逻辑隔离等）、防火墙、虚拟专用网 VPN、入侵检测与入侵防御、数字证书、公钥基础设施 PKI、特权管理基础设施 PMI、Web 安全、电子邮件安全、电子商务安全（SET 协议）、PGP 软件、网络安全评估标准（TCSEC、ITSEC、CTCPEC、CC、GB17895 等）、网络安全审计等。

本书适合于作为网络信息安全及计算机相关专业的本科高年级学生和研究生的专业教材，也可供企事业单位的网络管理人员、安全维护人员、系统管理人员和其他相关技术人员阅读参考。

网络安全体系结构

张常有 编著

于 炯 主审

出　　版：电子科技大学出版社(成都建设北路二段四号　邮编：610054)

责任编辑：万晓桐

发　　行：新华书店经销

印　　刷：成都金龙印务有限责任公司

开　　本：787mm×1092mm　1/16　印张　15　字数　365 千字

版　　次：2006 年 9 月第一版

印　　次：2006 年 9 月第一次印刷

书　　号：ISBN 7-81094-597-1/TP・352

定　　价：29.00 元

前　言

随着互联网的发展和普及，网络攻击以及网络犯罪达到空前猖獗的程度。今天的病毒已能在十几分钟内迅速传遍全球，能在瞬间扰乱全球经济。当国民经济的众多关键部门日益依赖网络时，却发现网络如此脆弱。于是，网络信息安全日益得到全世界的重视，并已经成为衡量一个信息系统是否完善的重要标志。

在 2003 年 7 月 22 日召开的国家第三次信息化工作会议上，信息安全这一话题被提升到关系国家政治、经济、社会稳定的高度。在这次大会上，国家首次提出了《关于加强信息安全保障工作的意见》，提出“积极防御、综合防范”的方针，首次倡导从用户的层面加强信息安全保障工作。为了贯彻《意见》精神，2004 年 1 月 9 日国务院召开了全国信息安全保障工作会议，标志着保障网络信息安全工作的全面召开。会议强调：“必须充分认识到做好信息安全保障工作的极端重要性，全面提高信息防护能力，重点保障基础信息网络和重要信息系统安全，创建安全健康的网络环境，保障和促进信息化健康发展。”

自 2003 年开始，作者为计算机科学与技术专业的本科生开设了《网络信息安全技术》这门专业课，并担任主讲教师。本书的内容编排以作者多年来授课讲义为基础，并吸收了最新的科研成果，所以，兼顾了内容的完整性和新颖性。作者本着“实用、完整、理论联系实际”的原则，与众多从事网络信息安全工作和研究的同仁一起分享自己的感受。

本书共分 11 章。第 1 章，主要介绍网络信息安全的基本概念。第 2 章，介绍密码学的有关基础知识。密码学是网络信息安全的基础，对于理解安全协议和技术有重要作用。第 3 章，介绍网络体系结构中各层上的安全协议。这些安全协议是工作在网络中的通用标准，为上层协议和应用提供透明服务。第 4 章，介绍系统平台加固，研究网络中主机的操作系统平台的安全性。第 5 章，介绍网络隔离技术，通过逻辑隔离或物理隔离，将网络分割成不同的通信域，以达到网络信息高度安全的目的。第 6 章，介绍虚拟专用网（VPN）。VPN 是一种保证跨越 Internet 通信安全的有效技术，且建设和运行费用较低。第 7 章，介绍入侵检测系统（IDS）。IDS 监控系统边界的经过者和系统内部实体，其作用是保证系统内部的安全性。第 8 章，介绍公钥基础设施（PKI）。PKI 是对公开密码技术的完整应用，其作用是在 Internet 社区建立严格的信任关系。第 9 章，介绍常用的网络应用程序的安全性，主要有：Web 安全、电子商务安全、电子邮件安全、PGP 工具的使用等。第 10 章，介绍安全评估的标准和实施方法。第 11 章，阐述网络安全审计相关内容。

参加本书编写工作的还有：樊金生、朴春慧、张庆红、郑丽娟、韩伟、杨子光、徐红、李彦华、刘仁芬、冯红、蒋文保、张黎群、郭跃显等。还要特别感谢清华大学戴一奇教授、

北京理工大学曹元大教授、河北省经济信息中心王凤兰教授，他们对本书提出了很多宝贵的意见。新疆大学的于炯严格审核了本书全稿，在此特别致谢。

本书得到“国家自然科学基金项目（60563002）”、“河北省教育厅重点研究发展规划项目（2003250）”和“石家庄铁道学院科学技术学术著作出版基金”的资助。

由于作者水平有限，时间仓促，书中定有不妥甚至错误之处，恳请读者批评指正。对于本书中出现的任何问题，欢迎 E-mail 至chyv@vip.sina.com，作者表示衷心感谢。

作 者

2006 年 3 月

目 录

第 1 章 绪论 1

1.1 网络信息安全基本概念 1
1.2 网络信息面临的主要威胁 2
1.3 网络信息安全目标 2
1.4 网络信息安全的发展过程 3
1.5 网络信息安全体系结构 5
1.6 网络信息安全的主要研究内容 6
1.7 小结 12
思考与练习 12

第 2 章 密码学基础 13

2.1 密码学基础知识 13
2.2 对称密码体制 15
2.3 公钥密码体制 26
2.4 信息认证与数字签名 31
2.5 小结 37
思考与练习 37

第 3 章 网络安全协议 39

3.1 安全协议概述 39
3.2 数据链路层安全协议 40
3.3 网络层安全协议 47
3.4 传输层安全协议 53
3.5 小结 60
思考与练习 61

第 4 章 系统平台加固 62

4.1 平台加固步骤 62
4.2 系统平台加固工具分类 63
4.3 实用平台加固工具介绍 64
4.4 Windows 系统的安全加固 72
4.5 Linux 系统安全加固 80
4.6 小结 86
思考与练习 86

第 5 章　网络隔离与防火墙 87
5.1　网络隔离的模型 87
5.2　逻辑隔离 92
5.3　物理隔离 96
5.4　防火墙技术 101
5.5　小结 110
思考与练习 110
第 6 章　虚拟专用网（VPN） 111
6.1　VPN 原 理 111
6.2　VPN 的分类 118
6.3　VPN 解决方案的选择和实施 120
6.4　在 Windows 2000 中配置 VPN 124
6.5　小结 126
思考与练习 126
第 7 章　入侵检测系统 127
7.1　入侵检测系统概述 127
7.2　IDS 的分类 129
7.3　入侵检测系统的关键技术 132
7.4　入侵检测系统的测试与评估 136
7.5　标准化工作 139
7.6　IDS 产品介绍 141
7.7　小结 146
思考与练习 146
第 8 章　公钥基础设施 PKI 147
8.1　PKI 提供的服务 147
8.2　公钥基础设施体系结构 151
8.3　PKI 的信任模型 167
8.4　特权管理基础设施 PMI 简介 173
8.5　小结 178
思考与练习 178
第 9 章　应用安全 179
9.1　Web 安全 179
9.2　电子邮件安全 183
9.3　电子商务安全 194

9.4　小结 201
思考与练习 201

第 10 章　安全评估 202

10.1　国际安全标准 202
10.2　安全评估方案 217
10.3　小结 221
思考与练习 221

第 11 章　系统安全审计 222

11.1　安全审计的原理 222
11.2　安全审计应用实例 227
11.3　小结 229
思考与练习 230

参考文献 231

第1章 绪 论

随着计算机和网络应用在社会、政治、经济、文化、生产等领域的普及，社会信息化建设已初具规模，这给我国经济发展和社会进步带来了前所未有的机遇。然而，由于网络带来的信息安全问题，不仅阻碍了计算机和网络应用的进一步普及，而且还影响了现有的应用，直接给国家和人民带来经济或名誉的损害；网络和相关信息系统价值的进一步挖掘更是受到制约，信息安全已成为制约社会信息化发展的重要因素之一。

1.1 网络信息安全基本概念

网络 通常意义上的网络术语多指计算机网络。计算机网络就是利用通信设备和线路将地理位置不同的、功能独立的多个计算机系统互连起来，以功能完善的网络软件（即网络通信协议、信息交换方式、网络操作系统等）实现网络中资源共享和信息传递的系统。简单地说计算机网络是由两台或两台以上的计算机通过网络设备连接起来组成的一个系统，在这个系统中计算机与计算机之间可以进行数据通信、数据共享及协同完成某些数据处理工作。

信息 广义上讲，信息是从调查、研究和教育中获得的知识，是情报、新闻、事实、数据，是代表数据的信号或字符，是代表物质的或精神的经验信息及经验数据、图片。1988年，钟义信在《信息科学原理》一书中认为，信息是事物运动的状态与方式，是物质的一种属性。信息不同于消息，消息只是信息的外壳，信息则是消息的内核；信息不同于信号，信号是信息的载体，信息则是信号所载荷的内容；信息不同于数据，数据是记录信息的一种形式，同样的信息也可以用文字或图像来表述。信息还不同于情报和知识。

安全 安全是避免危险、恐惧、忧虑的度量和状态。RFC（Request For Comment）中把安全定义为：1．为保护一个系统而采用的措施；2．一种系统状态，得益于建立和维护一套保护系统的措施；3．一种系统状态，在这种状态下，系统资源免于被非授权访问，并免于被非授权或意外篡改、毁坏或丢失。

网络信息 指在网络环境中存储、传递的各种信息以及网络系统为了维护其正常运行而产生的各种信息的总和。

网络安全 网络安全（Network Security）是在分布网络环境中，对信息载体（处理载体、存储载体、传输载体）和信息的处理、传输、存储、访问提供安全保护，以防止数据、信息内容、拒绝服务被非授权使用和篡改。网络安全是一门涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等多种学科的综合性科学。从总体上，网络安全可以分成两大方面：网络攻击技术和网络防御技术，只有全面把握两方面的内容，才能真正掌握计算机网络安全技术。

信息安全 信息安全是防止对知识、事实、数据或能力非授权使用、误用、篡改或拒

绝使用所采取的措施。维护信息自身的安全就要抵抗对信息的安全威胁。ISO定义：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、更改和暴露。

网络信息安全 指保护网络信息安全而采取的措施或表示网络信息的一种安全状态。网络信息安全以信息安全为目标，以网络安全为手段。

1.2 网络信息面临的主要威胁

网络信息面临的安全威胁有多个方面，主要有：假冒、窃听、篡改、否认（包括对信息产生源的否认和对信息接收的否认等）、信息延误、拒绝服务攻击、恶意代码、电磁泄漏、硬件故障、自然灾害等。主要形式如图 1-1 所示。

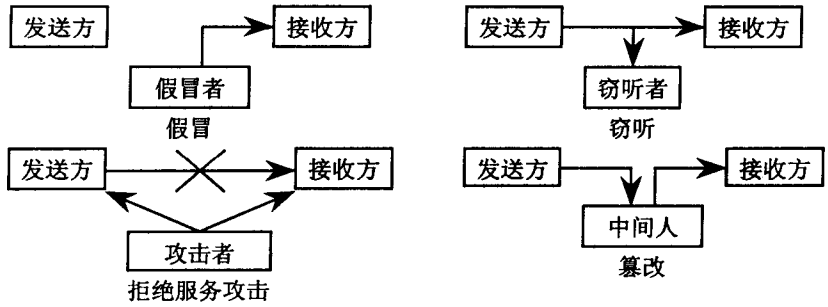

图 1-1 网络威胁的主要形式

1.3 网络信息安全目标

通信、计算机和网络等信息技术的发展大大提升了信息的获取、处理、传输、存储和应用能力，信息数字化已经成为普遍现象。互联网的普及更方便了信息的共享和交流，使信息技术的应用扩展到社会经济、政治、军事、个人生活等各个领域。因此，信息安全的重要性可以上升到国家安全的高度。

无论在计算机上存储、处理和应用，还是在通信网络上传输，信息都可能被非授权访问而导致泄密，被篡改破坏而导致不完整，被冒充替换而导致否认，也可能被阻塞拦截而导致无法存取。这些破坏可能是有意的，如黑客攻击、病毒感染；也可能是无意的，如误操作、程序错误等。

那么，信息安全究竟应该关注哪些方面呢？尽管目前说法不一，但普遍被接受的观点是，信息安全的目标是保护信息的机密性、完整性、不可否认性、可用性、可控性等；也有观点认为是机密性、完整性和可用性，即 CIA（Confidentiality，Integrity，Availability）。

机密性（Confidentiality）

机密性是指保证信息不被非授权访问；即使非授权用户得到信息也无法知晓信息内容，因而不能使用。通常通过访问控制阻止非授权用户获得机密信息，通过加密变换阻止非授

权用户获知信息内容。

完整性（Integrity）

完整性是指维护信息的一致性，即信息在生成、传输、存储和使用过程中不应发生人为或非人为、非授权篡改。一般通过访问控制阻止篡改行为，同时通过消息摘要算法来检验信息是否被篡改。

不可否认性（Non-repudiation）

不可否认性是指能保障用户无法在事后否认曾经对信息进行的生成、签发、接收等行为，是针对通信各方信息真实统一性的安全要求。一般通过数字签名来提供不可否认服务。

可用性（Availability）

可用性是指保障信息资源随时可提供服务的特性，即授权用户根据需要可以随时访问所需信息。可用性是信息资源服务功能可靠性的度量，涉及物理、网络、系统、数据、应用和用户等多方面的因素，是对信息网络总体可靠性的要求。

可控性（Controllability）

信息安全的可控性是指能够控制使用信息资源的人或实体的使用方式。对于信息系统中的敏感信息资源，如果任何人都能访问、篡改、窃取以及恶意散播的话，那么安全系统显然失去了效用。对访问信息资源的人或实体的使用方式进行有效的控制，是信息安全的必然要求。

1.4 网络信息安全的发展过程

以上提到的网络信息安全目标并没有出现在同一历史时期，而是与信息技术的发展相伴发展的，受到不同历史时期应用需求的驱动。普遍认为，现代信息安全的发展可以划分为三个阶段。

通信保密阶段（COMSEC）

通信保密阶段的开始时间约为20世纪40年代，其时代标志是1949年Shannon发表的《保密系统的信息理论》，该理论将密码学的研究纳入了科学的轨道。在这个阶段所面临的主要安全威胁是搭线窃听和密码学分析，其主要的防护措施是数据加密。

在该阶段人们关心的只是通信安全，而且主要关心对象是军方和政府。需要解决的问题是在远程通信中拒绝非授权用户的信息访问以及确保通信的真实性，包括：加密、传输保密、发射保密以及通信设备的物理安全。通信保密阶段的技术重点是通过密码技术解决通信保密问题，保证数据的保密性和完整性。当时涉及的安全性有：保密性，保证信息不泄露给未经授权的人或设备；可靠性，确保信道、信息源、发信人的真实性以及核对信息接受者的合法性。

在当时，虽然计算机系统的脆弱性已日益为美国政府和私营部门的一些机构所认识，但由于当时计算机的速度和性能比较落后，使用范围有限，加之美国政府将其作为敏感问题而加以控制，因此，有关计算机安全的研究一直局限在比较小的范围内。

计算机安全（COMPUSEC）**和信息安全阶段**（INFOSEC）

进入20世纪70年代，通信保密阶段转变到计算机安全阶段。这一时代的标志是1977

年美国国家标准局（NBS）公布的《国际数据加密标准》（DES）和 1985 年美国国防部（DoD）公布的《可信计算机系统评估准则》（TCSEC）。这些标准的提出意味着解决计算机信息系统保密性问题的研究和应用又迈上了历史的新台阶。

进入 20 世纪 80 年代，计算机的性能得到了千百倍提高，应用范围也在不断扩大，计算机已遍及到世界各个角落，而且人们正努力利用通信网络把孤立的单机系统连接起来，相互通信和共享资源。但是，随之而来并日益严峻的问题是计算机信息的安全问题，人们在这方面作的研究与计算机性能和应用的飞速发展不相适应。因此，它已成为未来信息技术中的主要问题之一。

由于计算机信息有共享和易于扩散等特性，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。

于是该阶段最初的重点是确保计算机系统中的硬件、软件及在处理、存储、传输信息中的保密性。主要安全威胁是信息的非授权访问，主要保护措施是安全操作系统的可信计算基技术（TCB），其局限性在于仍旧没有超出保密性的范畴。

TCSEC 将计算机安全与操作系统可信计算紧密联系在了一起，通过访问控制防止对信息的非授权访问，从而保护信息的保密性，其思想至今仍对安全操作系统的研究具有指导意义。但是，随着计算机病毒、计算机软件 Bug 等问题的不断显现，保密性已经不足以满足人们对计算机安全的需求，完整性和可用性等新需求于是开始出现。

20 世纪 90 年代以来，通信和计算机技术相互依存，数字化技术促进了计算机网络发展成为全天候、通全球、个人化、智能化的信息高速公路，Internet 成了寻常百姓可及的家用技术平台，安全的需求不断地向社会的各个领域扩展，人们的关注对象已经逐步从计算机转向更具本质性的信息本身，信息安全的概念随之产生。人们需要保护信息在存储、处理或传输过程中不被非法访问或更改，确保对合法用户的服务并限制非授权用户的服务，包括必要的检测、记录和抵御攻击的措施。于是除保密性、完整性和可用性之外，人们对安全性有了新的需求：可控性和不可否认性。

计算机安全过渡到信息安全后，世界各地的安全文献已经很少谈及计算机安全，多代之以“IT 安全”。

这一时期，在密码学方面，公钥技术得到了长足的发展，著名的 RSA 公开密钥密码算法获得了日益广泛的应用，用于完整性校验的 Hash 函数的研究应用也越来越多。为了奠定 21 世纪的分组密码算法基础，美国国家技术和标准研究所（NIST）推行了高级加密标准（AES）的项目。1998 年 7 月选出了 15 种分组密码算法作为候选算法。继而经过广泛评价，从中选出 5 个较好的算法，经过更加广泛和严谨的评审后，5 个算法中的 Rijndael 胜出，最终成为 AES 算法。另外，人们已经把更强更快的公钥密码算法的研究和应用投向了椭圆曲线公开密钥密码算法上。

虽然该阶段包括了计算机安全和信息安全两个不同的阶段，但它们的时间区分不明显，可将其统称为 INFOSEC 阶段。

信息保障阶段（IA）

信息系统受到的攻击日趋频繁，安全的概念逐渐发生了两个方面的变化：

安全不再局限于信息的保护，人们需要的是对整个信息和信息系统的保护和防御，包括了保护、检测、反应和恢复能力（PDRR）；

安全与应用的结合更加紧密，其相对性、动态性等特征日趋引起注意，追求适度风险的信息安全成为共识。安全不再单纯以功能或机制的强度作为评判指标，而是结合了应用环境和应用需求，强调安全是一种信心的度量，使信息系统的使用者确信其预期的安全目标已获得满足。于是美国军方提出了信息保障（IA）的概念："保护和防御信息及信息系统，确保其可用性、完整性、保密性、鉴别、不可否认性等特性。这包括在信息系统中融入保护、检测、反应功能，并提供新系统的恢复功能。"

信息保障除强调信息安全的保护能力外，还提出要重视提高系统的入侵检测能力、系统的时间反应能力以及系统在遭到入侵引起破坏后的快速恢复能力。它关注的是信息系统整个生命周期的防御和恢复。

信息保障是信息安全发展的最新阶段，由于习惯的原因，很多人仍然沿用"信息安全"的称谓。为了区别上述两个概念，同时体现出继承性，可采用"信息安全保障"的概念，指"保证信息与信息系统的保密性、完整性、可用性、可控性和不可否认性的信息安全保护和防御过程。它要求加强对信息和信息系统的保护，加强对信息安全事件和各种脆弱性的检测，提高反应能力和系统恢复能力"。

要使我国的信息安全保障综合能力达到理想水平，就必须强化国家的信息安全保障体系建设，它是实施信息安全保障的法制、组织管理和技术等层面有机结合的整体，是一个复杂的社会系统工程，是信息社会国家安全的基本组成部分，是保证国家信息化顺利进行的基石。当前，可从完善法制、健全组织管理、强化技术防护、夯实基础设施建设等四个层面、两个支撑来构建一个国家信息安全保障体系的框架（如图 1-2 所示）。

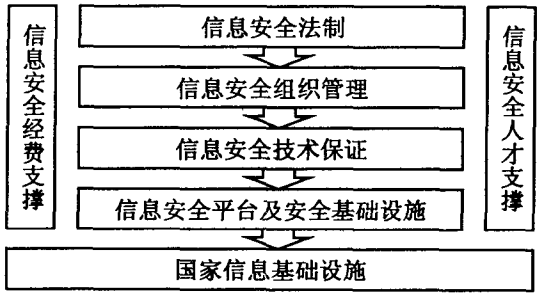

图 1-2 信息安全保障体系结构

1.5 网络信息安全体系结构

所谓安全体系结构，指的是一个计划和一套原则。它描述了：1．为满足其用户需求而必须提供的一套安全服务；2．要求所有系统元素都要实现的服务；3．为应付威胁环境而要求系统元素达到的安全级别。一个安全体系结构是采用系统工程过程的结果。一个完整的安全体系结构包括：管理安全、通信安全、计算机安全、辐射安全、人员安全和物理安全等。它既需要应付恶意威胁，也需要应付意外的威胁。如图 1-3 所示为与 OSI（Open Systems Interconnection ）参考模型对应的网络信息安全体系结构三维模型。其中 X 轴表示安全机制，Y 轴表示 OSI 参考模型，Z 轴表示安全服务。

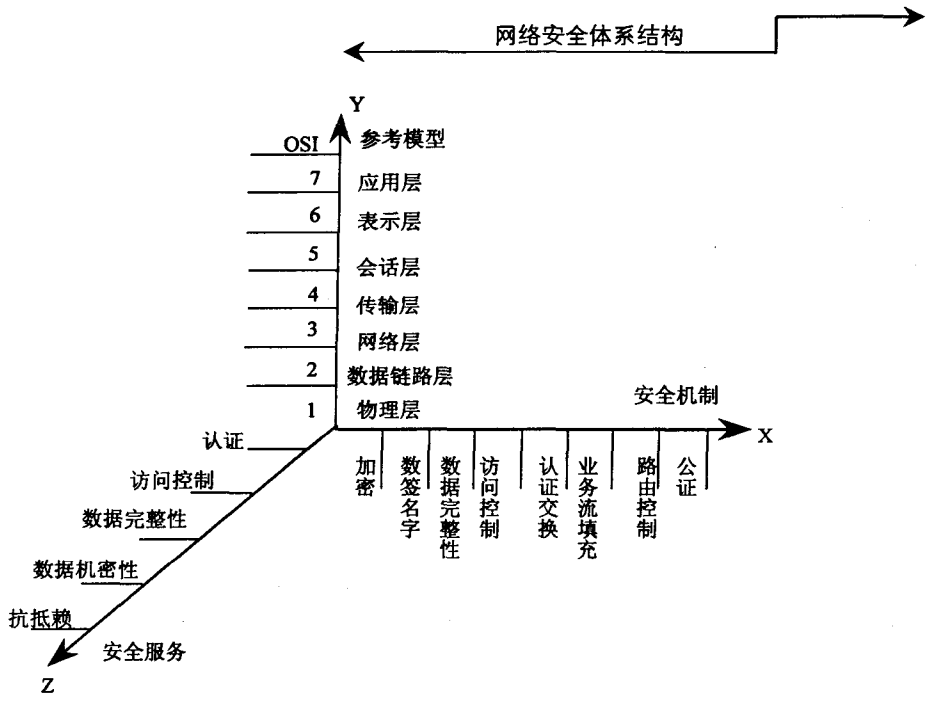

图 1-3　OSI 中的三维安全体系

与安全体系结构相关的概念还有：安全机制、安全模型、安全服务、安全策略等。

安全机制：安全机制是一个过程（或与该过程绑定的一种设备）。它能用于一个系统，使该系统能够实现其对外或对内提供的安全服务。安全机制的例子有鉴别交换、校验和、数字签名、加密、传输填充等。

安全模型：它描述了一个系统对外或对内提供的一套规定的安全服务。安全模型的例子有 Bell-LaPadula 模型、基于角色的访问控制模型（Role-based Access Model）、基于任务的访问控制模型（Task-based Access Control Model）等。

安全策略：安全策略指一套规则和惯例。它详细说明了系统或组织如何提供安全服务去保护敏感的关键系统资源。例如，基于身份的安全策略、基于规则的安全策略等。

安全服务：系统提供的一种处理服务或通信服务。它能够为系统资源提供特定的保护，如访问控制服务、审计服务、有效性服务、数据机密性服务、数据完整性服务、数据源认证服务、不可抵赖性服务、对等实体认证服务、系统完整性服务等。安全服务实现了安全策略，并且由安全机制实现。

1.6　网络信息安全的主要研究内容

信息技术发展到今天，信息安全的内涵在不断地延伸。从最初的信息机密性发展到信息的完整性、可用性、可控性和不可否认性，进而又发展为“攻（攻击）、防（防范）、测（检测）、控（控制）、管（管理）、评（评估）”等多方面的基础理论和实施技术。

以上内容可以归结为基础理论研究、应用技术研究、安全管理研究等。基础理论研究包括密码学研究、安全理论研究等；应用技术研究包括安全实现技术研究、安全平台技术

研究等；安全管理研究包括安全标准、安全策略、安全测评等。各部分研究内容及相互关系如图 1-4 所示。

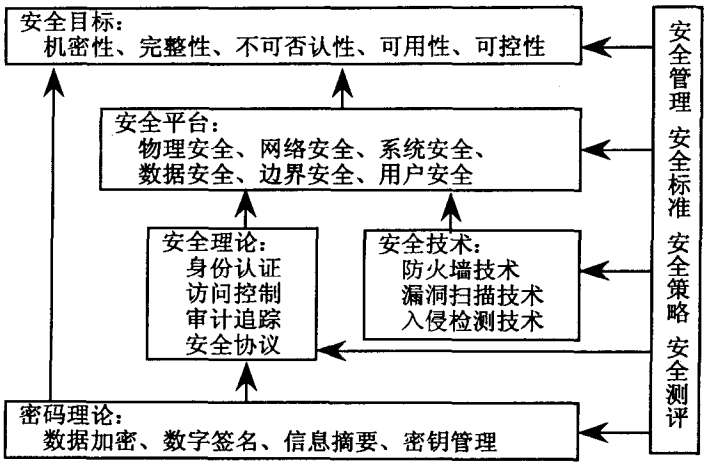

图 1-4 研究内容及其关系

密码理论的研究重点是算法，包括数据加密算法、数字签名算法、消息摘要算法及相应的密钥管理协议等。这些算法提供两方面的服务：一方面，直接对信息进行运算，保护信息的安全特性，即通过加密变换保护信息的机密性，通过消息摘要变换检测信息的完整性，通过数字签名保护信息的不可否认性；另一方面，提供对身份认证和安全协议等理论的支持。

安全理论的研究重点是在单机或网络环境下信息防护的基本理论，主要有访问控制（授权）、身份认证、审计追踪（这三者常被称为 AAA，即 Authorization，Authentication，Audit）、安全协议等。这些研究成果为建设安全平台提供了理论依据。

安全技术的研究重点是在单机或网络环境下信息防护的应用技术，目前主要有防火墙技术、入侵检测技术、漏洞扫描技术、防病毒技术等。其研究思路与具体的平台环境关系密切，研究成果直接为平台安全防护和监测提供了技术依据。

平台安全是指保障承载信息产生、存储、传输和处理的平台的安全和可控。平台由网络设备、主机（服务器、终端）、通信网、数据库等有机组合而成，这些设备组成网络并形成特定的连接边界。平台安全不仅涉及物理安全、网络安全、系统安全、数据安全和边界安全，还包括用户行为的安全。

此外安全管理也很重要。普遍认为，信息安全三分靠技术，七分靠管理，可见管理的分量。管理应该有统一的标准、可行的策略和必要的测评，因此，安全管理包括安全标准、安全策略、安全测评等。这些管理措施作用于安全理论和技术的各个方面。

1.6.1 信息安全基础研究

信息安全基础研究的主要内容包括密码学研究和网络信息安全基础理论研究。

1. 密码理论

密码理论（Cryptography）是信息安全的基础，信息安全的机密性、完整性和不可否认

性都依赖于密码算法。通过加密可以保护信息的机密性；通过信息摘要可以检测信息的完整性；通过数字签名可以保护信息的不可否认性。加密变换需要密钥参与，因而密钥管理也是十分重要的研究内容。因此，密码学的主要研究内容是加密算法、消息摘要算法、数字签名算法以及密钥管理。

● **数据加密**（Data Encryption）

数据加密算法是一种数学变换，在选定参数（密钥）的参与下，将信息从易于理解的明文加密为不易理解的密文，同样也可以将密文解为明文。加、解密时用的密钥可以相同，也可以不同。加、解密密钥相同的算法称为对称算法，典型的算法有 DES、AES 等；加、解密密钥不同的算法称为非对称算法，通常一个密钥公开，另一个密钥私藏，因而也称为公钥算法，典型的算法有 RSA、ECC 等。

● **消息摘要**（Message Digest）

消息摘要算法也是一种数学变换，通常是单向（不可逆）的变换，它将不定长度的信息变换为固定长度（如 16 字节）的摘要，信息的任何改变（即使是 1bit）都能引起摘要面目全非，因而可以通过消息摘要检测消息是否被篡改。典型的算法有 MD5、SHA 等。

● **数字签名**（Digital Signature）

数字签名主要是消息摘要和非对称加密算法的组合应用。从原理上讲，通过私有密钥，用非对称算法对信息本身进行加密，即可实现数字签名功能。用私钥加密只能用公钥解密使得接受者可以解密信息，但无法生成用公钥解密的密文，从而证明此密文肯定是拥有加密私钥的用户所为，因而是不可否认的。实际实现时，由于非对称算法加 / 解密速度很慢，通常先计算消息摘要，再用非对称加密算法对消息摘要进行加密而获得数字签名。

● **密钥管理**（Key Management）

密码算法是可以公开的，但密钥必须严格保护。如果非授权用户获得加密算法和密钥，则很容易破解或伪造密文，加密也就失去了意义。密钥管理研究就是研究密钥的产生、发放、存储、更换和销毁的算法和协议等。

2. 安全理论

● **身份认证**（Authentication）

身份认证是指验证用户身份与其所声称的身份是否一致的过程。最常见的身份认证是口令认证。口令认证是在用户注册时记录下其用户名和口令，在用户请求服务时出示用户名和口令，通过比较其出示的用户名和口令与注册时记录下的是否一致来鉴别身份的真伪。复杂的身份认证则需要基于可信的第三方权威认证机构的保证和复杂的密码协议来支持，如基于证书认证中心（CA）和公钥算法的认证等。

身份认证研究的主要内容包括认证的特征（知识、推理、生物特征等）和认证的可信协议及模型。

● **授权和访问控制**（Authorization and Access Control）

授权和访问控制是两个关系密切的概念，常常替换使用。它们的细微区别在于，授权侧重于强调用户拥有什么样的访问权限，这种权限是系统预先设定的，并不关心用户是否发起访问请求；而访问控制是对用户访问行为进行控制，它将用户的访问行为控制在授权允许的范围之内，因此，也可以说，访问控制是在用户发起访问请求时才起作用的。打个形象的比喻，授权是签发通行证，而访问控制则是卫兵，前者规定用户是否有权出入某个

区域，而后者检查用户在出入时是否超越了禁区。

授权和访问控制研究的主要内容是授权策略、访问控制模型、大规模系统的快速访问控制算法等。

● **审计追踪**（Auditing and Tracing）

审计和追踪也是两个关系密切的概念，审计是指对用户的行为进行记录、分析和审查，以确认操作的历史行为。追踪则有追查的意思，通过审计结果追查用户的全程行踪。审计通常只在某个系统内进行，而追踪则需要对多个系统的审计结果进行综合分析。

审计追踪研究的主要内容是审计素材的记录方式、审计模型及追踪算法等。

● **安全协议**（Security Protocol）

安全协议指构建安全平台时所使用的与安全防护有关的协议，是各种安全技术和策略具体实现时共同遵循的规定，如安全传输协议、安全认证协议、安全保密协议等。典型的安全协议有网络层安全协议 IPSec、传输层安全协议 SSL、应用层安全电子商务协议 SET 等。

安全协议研究的主要内容是协议的内容和实现层次、协议自身的安全性、协议的互操作性等。

1.6.2 信息安全应用研究

信息安全应用研究是针对信息在应用环境下的安全保护而提出的，是信息安全基础理论的具体应用。它包括安全技术研究和平台安全研究。

1．安全技术

安全技术是对信息系统进行安全检查和防护的技术，包括防火墙技术、漏洞扫描技术、入侵检测技术、防病毒技术等。

● **防火墙技术**（Firewall）

防火墙技术是一种安全隔离技术，它通过在两个安全策略不同的域之间设置防火墙来控制两个域之间的互访行为。隔离可以在网络层的多个层次上实现，目前应用较多的是网络层的包过滤技术和应用层的安全代理技术。包过滤技术通过检查信息流的信源和信宿地址等方式确认是否允许数据包通行，而安全代理则通过分析访问协议、代理访问请求来实现访问控制。

防火墙技术的主要研究内容包括防火墙的安全策略、实现模式、强度分析等。

● **漏洞扫描技术**（Venearbility Scanning）

漏洞扫描是针对特定信息网络中存在的漏洞而进行的。信息网络中无论是主机还是网络设备都可能存在安全隐患，有些是系统设计时考虑不周而留下的，有些是系统建设时出现的。这些漏洞很容易被攻击，从而危及信息网络的安全。由于安全漏洞大多是非人为的、隐蔽的，因此，必须定期扫描检查、修补加固。操作系统经常出现的补丁模块就是为加固发现的漏洞而开发的。由于漏洞扫描技术很难自动分析系统的设计和实现，因此很难发现未知漏洞。目前的漏洞扫描更多的是对已知漏洞进行检查定位。

漏洞扫描技术研究的主要内容包括漏洞的发现、特征分析以及定位、扫描方式和协议等。