公安院校
招录培养体制改革
试点专业
系列教材

计算机犯罪侦查方向

丛书主编 李锦

信息网络安全管理

黄波 主编　刘洋洋 纪芳 副主编

清华大学出版社

公安院校招录培养体制改革试点专业系列教材

丛书主编 李锦

信息网络安全管理

黄波 主编

刘洋洋 纪芳 副主编

清华大学出版社

北京

内 容 简 介

本书系统地介绍了信息网络安全管理工作中涉及的业务内容、流程标准和规范，主要包括信息网络安全概念，信息网络安全保障体系构成，信息网络安全管理措施，信息网络安全法律法规体系，网络安全监督管理的内容、任务和方法，互联网信息内容安全体系及互联网有害信息和热点信息的查处与管理，互联网上网营业服务场所安全监管，信息安全等级保护工作，信息网络安全违法案件查处等涉及网络安全管理与执法中的知识。全书内容翔实，涵盖面广。

本书可以作为公安院校招录培养体制改革网络犯罪侦查专业学生的教材，也可以作为公安院校、普通高校相关专业本、专科学生的教材和教学参考书及公安民警普及信息网络安全管理知识、了解信息网络安全保卫工作的参考书。

图书在版编目(CIP)数据

信息网络安全管理/黄波主编. —北京：清华大学出版社，2013.2
(公安院校招录培养体制改革试点专业系列教材)
ISBN 978-7-302-29345-3

Ⅰ. ①信… Ⅱ. ①黄… Ⅲ. ①信息网络－安全管理－高等学校－教材 Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字(2012)第 157008 号

责任编辑：闫红梅　李　晔
封面设计：常雪影
责任校对：梁　毅
责任印制：王静怡

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦 A 座　　邮　　编：100084
社 总 机：010-62770175　　邮　　购：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质 量 反 馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
课 件 下 载：http://www.tup.com.cn，010-62795954

印 装 者：北京密云胶印厂
经　　销：全国新华书店
开　　本：185mm×230mm　　**印　　张**：12.25　　**字　　数**：270 千字
版　　次：2013 年 2 月第 1 版　　**印　　次**：2013 年 2 月第1 次印刷
印　　数：1～3000
定　　价：23.00 元

产品编号：043369-01

序

期待已久的由李锦同志主编的《公安院校招录培养体制改革试点专业系列教材》终于出版了！该系列教材是我国第一套计算机犯罪侦查专业系列教材，它的出版解决了国内相关院校教师与学生急需的教课书问题，也为从事信息安全专业和侦查执法人员提供一套极有价值的参考丛书。这实属一件可喜可贺的事！

由于信息技术空前迅速的发展，极具挑战的计算机网络空间形成了一个变幻无穷的虚拟空间。现实社会中的犯罪越来越多地涉及到计算机、手机等工具，各种数字技术与网络虚拟空间的交汇，使计算机犯罪侦查技术变得空前重要与紧迫。从20世纪90年代兴起的数字取证调查，涌现出各种各样的技术和工具，使得数字取证成为计算机专业的一门新兴学科。国际上的一些大学近年来已设置了专门的系和研究生学位的授予，为计算机犯罪侦查的教学内容增添了丰富而又精彩的情景。他山之石可以攻玉，许多技术和教材可以借鉴，但数字取证牵涉到法学、法规，各国的国情不尽相同，唯一的解决办法就是必须自主创新、撰写适合国内需要的相应教材。

面临这一劈山开路的挑战，本教材从专业的技术层面为国内的本科生尝试提供全面的教学培训，内容包括了从互联网体系结构原理到电子商务应用与各种法规，以及计算机网络攻防技术与信息系统安全等级保护与管理等基础知识，重点围绕着计算机犯罪调查的手段、工具与方法以及数据证据的分析与鉴定等基础知识；教材注重在传授理论知识的同时，强化面向实战能力的培训，全套教材既适应了学科特点又考虑到学生层次的具体情况，处处反映出作者们的精心思索。

本系列教材参编的作者全部来自辽宁警官高等专科学校的师资队伍，该校地处辽东半岛，面临蓝色的大海，大浪淘沙涌现一批时代的人杰。庄严整洁的校园具有公安教育突出的特色，更为可贵的是他们倡导教学、科研、警务实践紧密结合，不断创新教学模式的一贯校风，每年从那里培养出大量信息时代专业特色明显、创新能力强的人才队伍。本套系列教材的出版充分体现了该校的学术水平与精神面貌，尤其映射出参编作者们拥有第一线资深的教学经验和扎实的实际专业知识，以及始终保持一股奋发上进、开拓创新的风范。我在此由衷地对本教材的出版表示祝贺，并预祝他们再接再厉，取得更加辉煌的成功！

许榕生

2012-6 写于北京

前言

随着计算机和网络通信技术的快速发展，信息网络在社会政治、经济、文化以及生活中发挥着愈来愈重要的作用，信息网络的发展极大地提高了我国的综合国力。同时因信息网络的开放性、互连性，进入21世纪后我国国内政治、经济、军事、科技等重要领域网络安全保护能力不强、信息网络安全技术的落后、信息网络安全保障政策及法律建设不协调、个人信息网络安全意识淡化等因素给国家安全和社会稳定带来了威胁。如何实现信息网络的安全有效运行成为当前保障国家安全和社会稳定发展的主要问题。

目前我国信息网络安全面临着严峻的挑战。特别是近年来，我国网络犯罪不断呈上升趋势，各种传统犯罪与网络犯罪结合的趋势日益明显，网络诈骗、网络盗窃等侵害他人财产的犯罪增长迅速，制作传播计算机病毒、入侵和攻击计算机与网络的犯罪日趋增多，利用互联网传播淫秽色情及从事赌博等犯罪活动仍然突出。据统计，1998年公安机关办理各类网络犯罪案件142起，2007年增长到2.9万起，2008年为3.5万起，2009年为4.8万起。

信息网络安全管理是国家法律法规赋予公安机关的一项重要职能，是公安机关在信息网络领域承担的一项重要的工作。公安机关要依照信息安全法律法规对互联网运营单位、联网服务单位、联网单位，上网营业服务场所和重要的信息系统依法进行管理，依法打击网络违法犯罪行为，在虚拟空间建立“打防结合”的安全保障机制，为我国信息网络健康发展保驾护航。

本书是编者在多年教学、研究积累的基础上，紧密围绕公安工作，结合在公安一线实习和挂职锻炼的学习心得，深刻体会信息网络安全保障体系的建设与应用的思路，紧密围绕信息网络安全管理这一公安工作的流程和业务需要，围绕实践编写的一本具有理论和实践指导意义的教程。

本书共包括7章内容，其中，第1章由黄波、杨虹编写；第2章和第6章由黄波、卢睿编写；第4章和第7章由刘洋洋编写；第3章和第5章由纪芳编写；全书由黄波统稿。在编写过程中得到了米佳教授的支持与帮助，在此表示衷心感谢。

由于编写水平和时间有限，书中难免有疏漏和不妥之处，敬请广大读者提出宝贵意见。

编者

2012年3月

目录

第1章

信息网络安全管理概述

【内容提要】

本章介绍了信息网络安全的发展现状、保障体系、安全措施。通过学习，要求学生了解信息网络安全的概念及层次划分，掌握信息网络安全保障体系结构及措施。

1.1 信息网络安全问题

信息网络安全目前已成为信息时代人类共同面临的新挑战。信息网络在我国政治、经济、文化以及社会生活中发挥着愈来愈重要的作用，作为国家关键基础设施和新的生产、生活工具，信息网络的发展极大地促进了信息传递和共享，提高了社会生产效率和人民生活水平，促进了经济社会的发展。信息网络的影响日益扩大、地位日益提升，维护信息网络安全工作的重要性日益突出，同时信息网络中的不安全因素也使得世界各行各业的安全受到严重威胁，如何实现信息网络的安全有效运行成为当前保障国家安全和社会稳定发展的主要问题。

1.1.1 信息网络安全现状

随着科学技术的发展，信息网络技术进入了高速发展的时期。信息网络是人类智慧的结晶，20世纪的重大科技发明，当代先进生产力的重要标志。人们对信息网络安全的需求从单一的通信保密，发展到今天的信息网络安全产品、技术手段等多方面。

在信息网络飞速发展的同时，信息网络安全也引起了人们的普遍关注。据有关方面统计，美国每年因网络安全问题而遭受的经济损失超过170亿美元，德国、英国也均在数十亿美元以上，法国大约为100亿法郎，日本、新加坡等国的问题也很严重。在国际刑法界列举的现代社会新型犯罪排行榜上，计算机犯罪已名列榜首。据统计，全球平均每20秒就发生1次网上入侵事件，黑客一旦找到系统的薄弱环节，所有用户均会遭殃。

互联网在我国得到了飞速发展：到2012年6月底中国网民人数达到5.38亿，中国手机网民规模达到3.88亿，国际出口带宽达到1 548 811Mbps，中国网站规模达到250.3万个，".CN"域名注册量达到398万个。我国网络安全同样也面临着巨大的威胁。据不完全统计，2009年中国被境外控制的计算机IP地址达100多万个；被黑客篡改的网站达4.2万

个；被“飞客”蠕虫网络病毒感染的计算机每月达 1800 万台，约占全球感染主机数量的 30%。公安机关办理的各类网络犯罪案件也呈上升趋势：1998 年 142 起，2007 年增长到 2.9 万起，2008 年为 3.5 万起，2009 年为 4.8 万起。2010 年，我国互联网上出现病毒 750 万个，受害网民 7.03 亿人次，被挂马网站 3382 万个，钓鱼网站 175 万个。病毒与经济利益深度结合，商业公司成为黑客套现的主要手段。

2009 年 1 月，中国政府开始发放第三代移动通信(3G)牌照，目前 3G 网络已基本覆盖全国。网民上网方式已从最初以拨号上网为主，发展到以宽带和手机上网为主。移动设备的快速普及，使得移动互联网与互联网之间的界限越来越模糊，而肆虐互联网的木马和网络钓鱼开始侵入移动互联网领域，截至 2010 年 11 月，新增手机病毒 1513 个，累积病毒数量达 2357 个，累计感染手机 800 万部以上。

因此，采取各种措施加强信息网络安全已是当务之急。

1.1.2 信息网络安全的概念

信息网络安全涉及到国家、社会、企业和个人生活等各个领域，从本质上说就是保护信息网络系统中硬件、软件和系统中数据的安全。从广义的角度，凡是涉及信息网络的保密性、完整性、可用性、可控性、不可否认性的相关技术和理论都是信息网络安全所要研究的领域，这五个特性也是信息网络安全所要达到的目标。从国家和社会的角度，信息网络安全就是要保护国家和社会的信息安全，避免威胁国家安全、社会稳定；从企业团体的角度，保护企业的商业机密、经济利益和企业的品牌声誉，避免出现病毒、非法读写、拒绝服务、资源非法占用及非法控制等现象；从个人的角度，就是要保护个人隐私和利益，避免他人利用窃听、冒充、篡改等手段损害个人利益。

因此，信息网络安全在不同的环境和应用中有不同的含义，《中华人民共和国计算机信息系统安全保护条例》的第三条规范了包括计算机网络系统在内的计算机信息系统安全的概念：“计算机信息系统的安全保护，应当保障计算机及其相关的和配套的设备、设施(含网络)的安全，运行环境的安全，保障信息的安全，保障计算机功能的正常发挥，以维护计算机信息系统的安全运行。”

信息网络安全具有以下五个特性，这也是信息网络安全所要达到的目标。

保密性(Confidentiality)：指保证关键信息和敏感信息不被非授权者获取、解析或恶意利用。

完整性(Integrity)：指保证信息从真实的信源发往真实的信宿，在传输、存储过程中未被非法修改、替换、删除；信息完整性是信息网络安全的基本要求。破坏信息的完整性是影响信息网络安全的常用手段。

可用性(Availability)：指保证信息和信息系统随时可为授权者提供服务而不被非授权者滥用和阻断。

可控性(Access Control)：即对信息、信息处理过程及信息系统本身都可以实施合法的安全监控和检测。

不可否认性(Non-repudiation)：保证出现信息网络安全问题后可以有据可查，可以追踪责任到人或到事，又称信息的抗抵赖性。

具体来说，信息网络安全保护的对象是信息。其中信息的保密性、完整性和可用性是保证信息网络安全的基本特性。此外还包括可控性、合法性、不可否认性等特性。

信息的保密性针对信息被允许访问对象的多少而不同。所有人员都可以访问的信息为公开信息，需要限制访问的信息一般为敏感信息或秘密。秘密可以根据信息的重要性及保密要求分为不同的密级，例如，国家根据秘密泄露后对国家经济、安全利益产生的影响及后果不同，将国家秘密分为秘密、机密和绝密三个等级，组织可根据其信息网络安全的实际，在符合《国家保密法》的前提下将其信息划分为不同的密级；对于具体信息的保密性有时效性，如秘密到期即可解密等。

信息的完整性主要包括两方面：一方面是指信息在利用、传输、存储等过程中不被篡改、丢失或缺损等；另一方面是指信息处理的方法的正确性，不正当的操作，如误删除文件，有可能造成重要文件的丢失。

信息的可用性指信息及相关的信息资产在授权人需要时，可以立即被获得。例如，通信线路中断故障会造成信息在一段时间内不可用，影响正常的商业运作，这是信息可用性的破坏。

信息的可控性主要指对危害国家的信息进行监视审计，控制授权范围内信息的流向及行为方式，使用授权机制，控制信息传播的范围、内容。

信息的不可否认性是对出现的安全问题提供调查的依据和手段，使用审计、监控、防抵赖等安全机制，使得攻击者、破坏者无法抵赖，从而实现信息网络安全的可审计性。

信息的合法性是保证信息内容和制作、发布、复制、传播信息的行为符合宪法和法律的规定。我国的信息网络安全具有中国特色，不仅包括信息、数据安全的本身属性，还具有社会对信息网络安全所要求的“内容合法性”。我国现有信息网络安全法律规范对信息的合法性有明确规定，任何人不得利用信息网络制作、发布、复制、传播违反宪法和法律规定的信息。信息发送应事先取得信息接收者的授权。任何单位和个人不得利用电子邮件、通信短信息等信息服务方式发送未经信息接收者事先授权或者不能有效拒绝的信息。

信息网络安全的侧重点和重视程度会随着使用者的需求而变。如某些专有技术、市场营销计划等商业秘密，其保密性尤其重要；对于工业自动控制系统，控制信息的完整性相对其保密性重要得多；而对于瞬息万变的金融证券市场来说，保证信息的可用性是用户的第一需求；对网络运行和管理者来说，在使用过程中希望本地网络信息的访问、读、写等操作受到保护和控制；电子商务交易过程中的一些协议和合同的签署过程中不可否认性尤为重要；电子出版过程中的著作权使用的合法性非常关键。

1.1.3 信息网络安全的层次

为了使信息网络实现上面提到的五大特性，必须从物理设备、网络、系统、应用和管理各层面出发，保证各层面的安全。信息网络安全层次如图 1-1 所示。

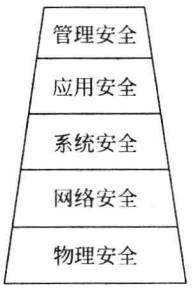

图 1-1 信息网络安全层次

1. 物理安全

物理安全是保护计算机设备、设施(含网络)以及其他媒体等实体免遭地震、水灾、火灾等环境事故(如电磁污染等)，以及因为操作失误或各种计算机犯罪行为导致破坏的措施和过程。为了保证实体安全必须做到环境安全、设备安全和媒体安全，其用来保证硬件和软件本身的安全，是整个信息网络安全的基石。

2. 网络安全

网络安全的组成如图 1-2 所示。

网络安全	局域网、子网安全	访问控制安全
		网络安全检测
	网络中数据传输安全	数据加密
	网络运行安全	备份与恢复
		应急
	网络协议安全	TCP/IP
		其他协议

图 1-2 网络安全的组成

在网络安全中，在内网和外网之间，设置合理的访问控制，可使内网对外网和外网对内网的访问都变得安全可靠又具有实用性。网络安全检测通常对内网的硬件和软件进行安全评估，检测出存在的漏洞和潜在的威胁，以达到增强网络安全的目的。数据备份不仅在网络系统硬件故障或因为失误时起到保护作用，也在入侵者实施非授权访问或对网络进行攻击及破坏数据完整性时起到保护作用，使网络系统及时获得恢复。互联网采用的主流协议是 TCP/IP，其设计初期强调开放性和便利性，没考虑安全性，因此协议存在严重安全漏洞，给网络安全留下隐患。

3. 系统安全

系统安全的组成如图 1-3 所示。

系统安全	操作系统安全	反病毒
		系统安全检测
		入侵检测
		审计分析
	数据库系统安全	数据库安全
		数据库管理系统安全

图 1-3　系统安全的组成

用户常用的系统包括操作系统和数据库系统两种。

一般用户对操作系统的安全还比较重视，但对数据库系统的安全并不重视，实际上，数据库系统作为许多应用系统的底层平台其安全性也十分重要。

4. 应用安全

应用安全的组成如图 1-4 所示。

应用安全	应用软件开发平台安全	各种编程语言平台安全
		程序本身的安全
	应用系统安全	应用软件系统安全

图 1-4　应用安全的组成

应用安全建立在系统平台之上，人们普遍会重视系统安全，而忽视应用安全。主要原因包括两个方面：第一，对应用安全缺乏认识；第二，应用系统过于灵活，需要较高的安全技术。恰恰因为应用程序存在很多漏洞，其配置也会存在很多问题，通常容易成为恶意软件攻击或利用的目标。只有通过及时的更新才能避免受到攻击。

5. 管理安全

管理安全是信息网络安全体系中不可缺少的一部分。完整的信息网络安全解决方案不仅包括物理安全、网络安全、系统安全和应用安全等这些技术手段，还需要以人为核心的策略和管理支持。网络安全至关重要的往往不是技术手段，而是对人的管理。

1.1.4　信息网络安全的特征

综合来看，信息网络安全具有以下特征：

(1) 信息网络安全是多维的安全。

信息网络安全是一个系统问题。一个安全的信息系统不仅仅要考虑环境安全和技术安全，还要考虑管理安全的问题；一个安全的信息系统不仅仅能够提供静态的保护能力，还需要具备主动防御的能力，能够及时发现攻击，并能够从破坏中恢复。

(2) 信息网络安全是动态的安全。

从信息系统的角度看,信息网络安全不是一个静止的状态,它是一个动态变化的过程。从历史的角度看,信息网络安全也不是一个静止的概念,它随着信息技术的进步而发展,随着产业基础、用户认识、投入产出的不同而变化。

(3) 信息网络安全是相对的安全。

信息网络安全是相对的,由于技术局限性、环境复杂性以及需求变化等因素的限制,目前现实世界中不存在百分之百的绝对安全。信息网络安全通常是指一定程度上的安全,如遵循适度安全原则的信息网络安全强调的是适度安全,实现投入产出平衡。

(4) 信息网络安全是过程的安全。

信息网络安全不是一个孤立的问题,应在系统建设过程中加以同步考虑,从规划设计阶段开始一直到系统终止,贯穿整个信息系统的生命周期。

(5) 信息网络安全是无国界的安全。

信息网络安全是无国界的。Internet 在发挥重大积极作用的同时,消极作用也体现了世界性和国际性,如网上攻击事件大幅上升。信息网络安全不是一个国家能完全控制的问题,具有全球化特点,应从全球信息化角度考虑和布局。

(6) 信息网络安全是多层次的安全。

与只涵盖保密性的狭义信息网络安全不同,广义的信息网络安全是一个宽泛的概念。不同层次的主体从不同角度分析不同的对象,会导致对信息网络安全有着不同的理解。如从主体层次看,国家层面的信息网络安全是指维护国家基础设施相关信息系统的安全,保障国家不受信息战争的威胁;国家机关、企事业单位层面的信息网络安全关注的是其负责建设和维护的信息系统的安全,确保信息的保密性以及服务的及时性与有效性;而个人层面的信息网络安全主要是指保护个人隐私。一般情况下,信息网络安全是指某个特定环境中的指定信息系统的安全。

1.2 信息网络面临的不安全因素

导致信息网络安全问题的主要因素是信息网络自身的脆弱性和信息网络面临的威胁。

1.2.1 信息网络自身的脆弱性

信息网络自身的脆弱性主要指网络系统和设备、计算机软硬件在设计时由于考虑不周等留下的缺陷,容易被威胁主体所利用从而危害系统的正常运行。其主要包括以下几个方面:

1. 计算机硬件系统及网络物理环境的脆弱性

计算机硬件本身存在易丢失、易损坏,且本身没有为对其访问和使用设计防护措施,以

及硬件漏磁等缺陷；网络物理环境也存在脆弱性，包括温度、湿度、灰尘、静电、电磁干扰、雷电、火灾、水患等对网络硬件设备和信息网络安全的影响。

2. 计算机网络和信息传输中的脆弱性

TCP/IP 协议本身的开放性带来的脆弱性。主要体现在信息输入、处理、传输、存储、输出过程中存在的信息容易被篡改、伪造、破坏、窃取、泄漏等不安全因素，包括信息泄漏、电子干扰等。

3. 计算机操作系统和软件系统的脆弱性

包括信息系统自身运行所需要的操作系统、数据库管理系统以及系统应用软件自身存在的漏洞及使用不当等造成的不安全因素。

4. 信息网络安全管理的脆弱性

由于信息网络使用人员繁杂、网络安全技术素质及安全意识参差不齐，导致信息网络安全管理的脆弱性。

另外，网络安全的脆弱性还和网络的规模有密切关系，网络规模越大，其脆弱性越大。

1.2.2　信息网络系统面临的威胁

目前信息网络面临的威胁主要包括来自电磁泄露、雷击等环境因素构成的威胁，软硬件故障和工作人员误操作等人为或偶然事故构成的威胁，利用计算机实施盗窃、诈骗等违法犯罪活动的威胁，网络攻击和计算机恶意代码构成的威胁以及信息战的威胁等，概括起来主要有以下几类。

1. 内部泄密和破坏

包括内部涉密人员有意或无意泄密、更改记录信息；内部非授权人员有意偷窃机密信息、更改记录信息；内部人员破坏信息系统等。

2. 截获

网络攻击者可能通过搭线或在电磁波辐射范围内安装截收装置等方式，截获机密信息，或通过对信息流量和流向、通信频度和长度等参数的分析，推出有用信息。

3. 非法访问

未经授权使用信息资源或以未授权的方式使用信息资源，它包括非法用户（通常称为黑客）进入网络或系统进行违法操作、合法用户以未授权的方式进行操作。

4. 破坏信息的完整性

网络攻击者通过篡改、删除、插入等操作破坏信息的完整性。

5. 冒充

冒充领导发布命令、调阅密件，冒充主机欺骗合法主机及合法用户，冒充网络控制程序套取或修改使用权限、口令、密钥等信息，越权使用网络设备和资源等。

6. 破坏系统的可用性

网络攻击者破坏网络系统的可用性，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等。

7. 其他威胁

对信息网络系统的威胁还包括计算机病毒、电磁泄漏、各种灾害、操作失误等。

1.3 信息网络安全保障体系结构

为了保证信息网络安全策略得以完整准确地实现，安全需求得以全面准确地满足，人们开始对信息网络安全体系进行研究，希望通过对信息网络安全体系的功能、服务、安全机制、技术、管理和操作，以及这些因素在整个体系中的合理部署和相互关系的研究，为信息安全的解决方案和工程实施提供依据和参考。

1.3.1 OSI 网络保障体系结构

国际标准化组织(ISO)制定了开放系统互连(OSI)参考模型，将计算机网络分为七个层次以实现网络互联。1989 年该组织提出了 OSI 安全体系结构：ISO 7498—2:1989。该标准被我国等同采用，即《信息处理系统一开放系统互连一基本参考模型一第二部分：安全体系结构 GB/T 9387.2—1995》。作为 OSI 参考模型的新补充，ISO 7498—2 标准现在已经成为网络安全专业人员的重要参考，它不是解决某一特定的安全问题，而是为解决网络安全共同体提出了一组公共的概念和术语，用来描述和讨论安全问题和解决方案。OSI 安全体系结构主要包括三部分内容，即安全服务、安全机制和安全管理，三者关系如图 1-5 所示。

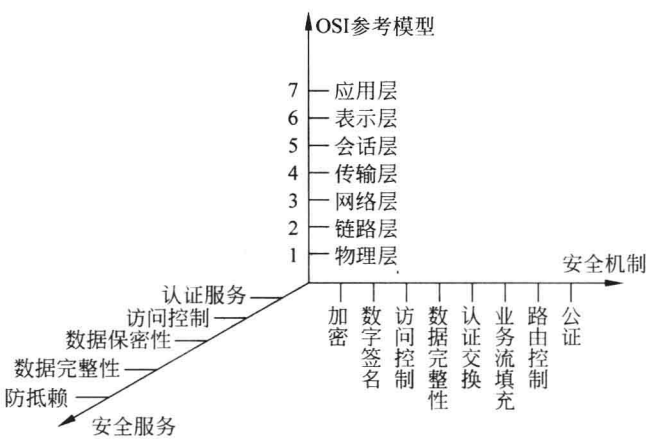

图 1-5 OSI 安全体系结构

1. 安全服务

ISO 对 OSI 规定了五种级别的安全服务，安全服务与 OSI 七层的关系如表 1-1 所示。