网络信息安全技术

主　编　张　靖
副主编　黄　萍
参　编　周　伟　鄢　莉　吴婷婷

北京理工大学出版社
BEIJING INSTITUTE OF TECHNOLOGY PRESS

前　言

IT 技术广泛运用并已渗透到各行各业，成为当前行业产业发展和社会服务的重要驱动与支撑。全球信息化越来越快，基于网络的各种应用更是主流和发展趋势，网络安全稳定就成为各种网络应用的基础和前提。网络信息安全主要是保护网络系统的硬件、软件及其系统中的数据，不受偶然或恶意的原因而遭到破坏、更改、泄露，系统能连续、可靠、正常地运行，网络服务不中断。网络信息安全已经成为网络应用系统重要的热点解决问题，并演化成关系个人信息安全、社会稳定等方面的重要问题，且重要性越来越突出。同时，网络信息安全又是一个复杂系统问题，涉及计算机科学、网络技术、通信技术、信息安全、应用数学、数论、信息论和社会学等多种学科与专业，也涉及硬件、软件、数据、制度、应用、运维等多维多层次问题，复杂性特点明显。

本书主要从网络信息安全概述、密码学、网络安全协议、网络安全技术、网络攻防技术来介绍有关应用现状、基本理论、工作原理和技术方法。学生通过对这些内容的学习，可牢固树立信息安全防护意识，理解信息安全的基础理论与技术应用，掌握网络信息安全的基本原理、系统安全防护的基本方法与主要技术，提高网络信息安全系统分析与设计能力、网络系统安全保障能力。全书内容主要分为以下五部分。

第一部分：网络信息安全概述

第 1 章，网络信息安全概述。主要内容：网络信息安全的概念；网络信息安全面临的挑战；网络信息安全的现状；网络信息安全的发展趋势；网络信息安全的目标；网络信息安全的研究内容。

第二部分：密码学

第 2 章，密码学基础。主要内容：密码学概述；传统密码学；对称密码体制；公钥密码体制。

第 3 章，信息认证。主要内容：信息认证概述；消息加密函数；消息鉴别码；哈希函数；经典哈希函数。

第 4 章，身份认证和数字签名。主要内容：身份认证技术；数字签名。

第 5 章，密钥管理。主要内容：对称密码体制的密钥管理；公钥体制的密钥管理。

第三部分：网络安全协议

第 6 章，网络安全协议。主要内容：网络安全协议概述；IPSec 协议；SSL 协议；Kerberos协议。

第四部分：网络安全技术

第 7 章，网络隔离技术。主要内容：网络隔离概述；物理网络隔离；逻辑网络隔离。

第 8 章，防火墙技术。主要内容：防火墙技术概述；防火墙的核心技术；防火墙的分

类；防火墙的体系结构；智能防火墙。

第9章，入侵检测与响应。主要内容：入侵检测概述；入侵检测系统的原理；入侵检测系统的分类；入侵检测中的响应机制；入侵检测系统的标准化和发展。

第10章，网络安全扫描技术。主要内容：端口扫描；漏洞扫描；实用扫描器。

第11章，无线网络安全技术。主要内容：无线网络概述；无线网络安全机制。

第五部分：网络攻防技术

第12章，常见的网络攻防技术。主要内容：网络攻防技术概述；缓冲区溢出攻击及防御；ARP欺骗攻击及防御；DDoS攻击及防御；常见的Web安全威胁及防御。

本书在1～12章都附有习题，以加深读者对章节内容的理解和掌握。此外，本书引入了7个与网络信息安全相关的实验，有助于读者更好地将网络信息安全原理应用于实践。本书既可以作为高等学校及有关培训机构的教材和教学参考书，也可以作为网络信息安全自学人员或网络信息安全开发人员的参考书。

本书的编者团队均多年负责校园计算机网的建设、运维与管理工作，主编自2000年起就致力于计算机科学与技术、网络工程等专业的本科“计算机网络”“网络管理”“网络安全”等专业课的教授。本书的内容以编者团队多年来的授课经验为基础，并吸收了工作经验及应用研究成果。在本书的编写过程中，团队成员之间配合协作，尽力完善内容，而且得到了许多教师和学生的建议与支持。

由于编者水平和时间有限，书中不足在所难免，恳请读者批评指正。

编　者

2020年3月

CONTENTS 目录

第1章 网络信息安全概述

信息技术和信息产业正在以前所未有的趋势渗透各行各业，改变着人们的生产生活，推动着社会的进步。但是，随着信息网络的不断扩展，口令入侵、木马入侵、非法监听、网络钓鱼、拒绝服务等攻击充斥网络，信息网络的安全问题日益严峻。网络信息安全不仅关系到个人用户的利益，还是影响社会经济的发展、政治稳定和国家安全的战略性问题。因此，网络信息安全问题已成为国内外专家学者广泛关注的课题。

网络信息安全是一个关系国家安全和主权、社会的稳定、民族文化的继承和发扬的重要问题。随着全球信息化步伐的加快，网络信息安全正变得越来越重要。网络信息安全技术的应用，可以减少信息的泄露和数据破坏的事件的发生。

本章主要介绍网络信息安全的概念、网络信息安全面临的挑战、网络信息安全的现状、网络信息安全的发展趋势、网络信息安全的目标、网络信息安全的研究内容。

1.1 网络信息安全的概念

1. 计算机安全

计算机安全是指为数据处理系统而采取的技术和管理方面的安全保护，以保护计算机硬件、软件、数据不因偶然的或恶意的原因而遭到破坏、更改、泄露。

计算机安全的目的是保护信息免受未经授权的访问、中断和修改，并为系统的预期用户保持系统的可用性。

2. 网络安全

网络安全是指网络系统的硬件、软件及其系统中的数据受到保护，不因偶然的或恶意的原因而遭受破坏、更改、泄露，以确保经过网络传输和交换的数据的安全性。本质上，网络

安全就是网络上的信息安全。从广义来说，凡是涉及网络上信息的保密性、完整性、可用性、真实性和可控性的相关技术和理论，都是网络安全的研究领域。

网络安全涉及的内容既有技术方面的，也有管理方面的，这两方面相互补充，缺一不可。在技术方面，其侧重于如何防范外部非法攻击；在管理方面，其侧重于内部人为因素的管理。如何更有效地保护重要的信息数据、提高计算机网络系统的安全性，已经成为所有计算机网络应用都必须考虑和解决的重要问题。

网络安全涉及的领域有密码学设计、各种网络协议的通信、各种安全实践等。

3. 网络信息安全

信息安全是指信息网络的硬件、软件及其系统中的数据受到保护，不因偶然的或恶意的原因而遭受破坏、更改、泄露，系统能连续可靠正常地运行，信息服务不中断。

信息安全主要包括五方面内容，即需保证信息的保密性、真实性、完整性、未授权拷贝、所寄生系统的安全性。信息安全包括的范围很广，如防范商业企业机密泄露、防范青少年对不良信息的浏览、个人信息的泄露等。网络环境下的信息安全体系是保证信息安全的关键，包括计算机安全操作系统、各种安全协议、安全机制（如数字签名、消息认证、数据加密等）、安全系统（如 UniNAC、DLP 等）。只要存在安全漏洞便可能威胁全局安全。

信息安全学科可分为狭义安全与广义安全两个层次。狭义安全建立在以密码论为基础的计算机安全领域，我国早期的信息安全专业通常以此为基准，辅以计算机技术、通信网络技术与编程等方面的内容；广义信息安全是一门综合性学科，安全不再是单纯的技术问题，而是将管理、技术、法律等方面的安全问题相结合的产物。信息安全学科主要培养能够从事计算机、通信、电子商务、电子政务、电子金融等领域的信息安全高级专门人才。

从应用范围来看，信息安全包含网络安全和计算机安全的内容。但是，随着安全问题的不断延伸，网络中的信息安全已成为最主要的问题，信息安全和网络安全的定义界线越来越模糊，“网络信息安全”的提法越来越多。严格意义上，“网络信息安全”就是信息安全。

1.2 网络信息安全面临的挑战

1. 互联网体系结构的开放性

网络基础设施和协议的设计者遵循着一条原则：尽可能创造用户友好性、透明性高的接口，使网络能够为尽可能多的用户提供服务。但是，这带来了另外的问题：一方面，用户容易忽视系统的安全状况；另一方面，不法分子会利用网络的漏洞来达到个人的目的。

2. 通信协议的缺陷

数据包网络需要在传输结点之间存在信任关系，以保证数据包在传输过程中拆分、重组

过程的正常工作。由于在传输过程中，数据包需要被拆分、传输和重组，因此必须保证每个数据包以及中间传输单元的安全。然而，目前的网络协议并不能做到这一点。

网络中的服务器主要有 UDP 和 TCP 两个主要的通信协议，都使用端口号来识别高层的服务。服务器的一条重要的安全规则就是：在服务没有被使用时，应关闭其所对应的端口号，如果服务器不提供相应的服务，那么端口就一直不能打开。即使服务器提供相应的服务，也只有在服务被合法使用时，端口号才能被打开。很多非正常使用的端口极易被攻击者利用，以实现其对系统的渗透。

客户端和服务器进行通信之前，需通过三次握手过程来建立 TCP 连接。但是，TCP 的三次握手会带来新的网络信息安全问题。

3. 用户安全意识薄弱

互联网自 20 世纪 60 年代早期诞生以来，经历了快速的发展，特别是近十来年，在用户使用数量和联网的计算机数量上都有了爆炸式的增加。随着互联网的易用性增强和准入性降低，用户安全意识的薄弱为网络信息安全带来了新的挑战。

4. 黑客行为

计算机黑客利用系统中的安全漏洞非法进入他人计算机系统，其危害性非常大。某种意义上，计算机黑客对信息安全的危害甚至比一般的计算机病毒更为严重。

5. 恶意软件

恶意软件是指在未明确提示用户或未经用户许可的情况下，在用户计算机或其他终端上安装运行、侵犯用户合法权益的软件。

恶意软件（malware，俗称“流氓软件”），也可能被称为广告软件（adware）、间谍软件（spyware）、恶意共享软件（malicious shareware）。与病毒（或蠕虫）不同，很多恶意软件并非由小团体（或个人）秘密地编写和散播，反而有很多知名企业和团体涉嫌此类软件。

恶意软件的特点主要有以下几点。

（1）强制安装：指在未明确提示用户或未经用户许可的情况下，在用户计算机或其他终端上安装软件的行为。

（2）难以卸载：指未提供通用的卸载方式，或在不受其他软件影响、人为破坏的情况下，卸载后仍活动程序的行为。

（3）浏览器劫持：指未经用户许可，修改用户浏览器或其他相关设置，迫使用户访问特定网站或导致用户无法正常上网的行为。

（4）广告弹出：指未明确提示用户或未经用户许可的情况下，利用安装在用户计算机或其他终端上的软件弹出广告的行为。

（5）恶意收集用户信息：指未明确提示用户或未经用户许可，恶意收集用户信息的行为。

（6）恶意卸载：指未明确提示用户或未经用户许可，或误导、欺骗用户的情况下，卸载非恶意软件的行为。

（7）恶意捆绑：指在软件中捆绑已被认定为恶意软件的行为。

（8）其他侵犯用户知情权、选择权的恶意行为。

6. 操作系统漏洞

操作系统漏洞是指应用软件或操作系统在逻辑设计上的缺陷或在编写时产生的错误。这些缺陷（或错误）是黑客进行攻击的首选目标。黑客通过这些缺陷（或错误）来注入木马、病毒等，以攻击（或控制）整台计算机，从而窃取计算机中的重要资料和信息，甚至破坏计算机系统。每款操作系统问世时，本身都难免存在一些安全问题或技术缺陷。操作系统的安全漏洞是不可避免的。攻击者会利用操作系统的漏洞来取得操作系统中的高级用户权限，进行更改文件、安装和运行软件、格式化硬盘等操作。

操作系统漏洞影响的范围很大，包括系统本身及其支撑软件、网络客户和服务器软件、网络路由器和安全防火墙等。换言之，在不同的软件、硬件中都可能存在不同的安全漏洞问题。

7. 内部安全

现在绝大多数的安全系统都会阻止恶意攻击者靠近系统，用户所面临的更困难的挑战是控制防护体系的内部人员进行的破坏活动。所以，在设计安全控制时，应注意不要赋予某位管理员过多的权利。

8. 社会工程学

社会工程学（Social Engineering）是指利用受害者的心理弱点、本能反应、好奇心、信任、贪婪等心理陷阱来实施欺骗、伤害等危害手段。

社会工程学通过搜集大量信息来针对对方的实际情况进行心理战术，常采用交谈、欺骗、假冒或口语等方式，从合法用户中套取用户系统的秘密。

1.3 网络信息安全的现状

据国家互联网应急中心（CNCERT）近年发布的网络安全态势综述分析，我国的网络信息安全主要呈现以下特点。

1. 我国网络安全法律法规政策保障体系逐步健全

自《中华人民共和国网络安全法》于2017年6月1日正式实施以来，我国网络安全相关法律法规及配套制度逐步健全，逐渐形成了综合法律、监管规定、行业与技术标准的综合化、规范化体系，我国网络安全工作法律保障体系不断完善，网络安全执法力度持续加强。

2. 我国互联网网络安全威胁治理取得新成效

我国互联网网络安全环境经过多年的持续治理，得到了明显改善。特别是党中央加强了对网络安全和信息化工作的统一领导，党政机关和重要行业加强网络安全防护措施，针对党

政机关和重要行业的木马僵尸恶意程序、网站安全、安全漏洞等传统网络安全事件大幅减少。

3. 分布式拒绝服务攻击频次下降，但峰值流量持续攀升

分布式拒绝服务（Distributed Denial of Services，DDoS）攻击是难以防范的网络攻击手段之一，其攻击手段和强度不断更新，逐步形成了“DDoS 即服务”的互联网黑色产业服务，普遍用于行业恶意竞争、敲诈勒索等网络犯罪。得益于我国网络空间环境治理取得的有效成果，经过对 DDoS 攻击资源的专项治理，我国境内的分布式拒绝服务攻击频次总体呈下降趋势。

2019 年以来，CNCERT 持续开展 DDoS 攻击团伙的追踪和治理工作。2018 年活跃的较大规模 DDoS 攻击团伙大部分已不再活跃，仅有几个攻击团伙通过不断变换资源而持续活跃。其中最活跃的攻击团伙主要使用 XorDDoS 僵尸网络发起 DDoS 攻击，常使用包含特定字符串的恶意域名对僵尸网络进行控制，对游戏私服、色情、赌博等相关的服务器发起攻击。分析发现，恶意域名大多在境外域名注册商注册，且不断变换控制端 IP 地址，持续活跃并对外发起大量攻击。

4. 虚假和仿冒移动应用增多且成为网络诈骗新渠道

近年来，随着互联网与经济、生活的深度捆绑交织，通过互联网对网民实施的远程非接触式诈骗手段不断更新，出现了“网络投资”“网络交友”“网购返利”等新型网络诈骗手段。随着我国移动互联网技术的快速发展和应用普及，通过移动应用来实施网络诈骗的事件日益突出，如大量虚假的“贷款”APP 并无真实贷款业务，仅用于诈骗分子骗取用户的隐私信息和钱财。CNCERT 抽样监测发现，在此类虚假“贷款”APP 上提交姓名、身份证照片、个人资产证明、银行账户、地址等个人隐私信息的用户超过 150 万人，大量受害用户向诈骗分子支付了上万元所谓的“担保费”“手续费”等，经济利益受到实质损害。CNCERT 还发现，与正版软件的图标（或名称）相似的仿冒 APP 呈数量上升趋势。

5. 数据安全问题引起前所未有的关注

2018 年 3 月，Facebook 公司被爆出大规模数据泄露且这些数据被恶意利用，引起国内外普遍关注。2018 年，我国也发生了包括十几亿条快递公司的用户信息、2.4 亿条某连锁酒店的用户入住信息、900 万条某网站用户数据信息、某求职网站用户个人求职简历等数据泄露事件，这些数据包含大量个人隐私信息，如姓名、地址、银行卡号、身份证号、联系电话、家庭成员等。2018 年 5 月 25 日，欧盟颁布执行个人数据保护条例《通用数据保护条例》（GDPR），掀起了国内外的广泛讨论，该条例监管收集个人数据的行为，重点保护自然人的“个人数据”，如姓名、地址、电子邮件地址、电话号码、生日、银行账户、汽车牌照、IP 地址以及 Cookies 等。GDPR 实施三天后，Facebook 和谷歌等美国企业成为 GDPR 法案下第一批被告，这不但给业界敲响了警钟，而且督促更多企业投入精力保护数据安全，尤其是保护个人隐私数据安全。

1.4 网络信息安全的发展趋势

结合近几年我国的网络安全状况，以及5G、IPv6等新技术的发展和应用，CNCERT对我国网络信息安全的趋势预测有以下几方面。

1. 有特殊目的、针对性更强的网络攻击越来越多

目前，网络攻击者发起网络攻击的针对性越来越强，有特殊目的的攻击行动频发。近年来，有攻击团伙长期以我国政府部门、事业单位、科研院所的网站为主要目标，实施网页窜改，境外攻击团伙持续对我国政府部门网站实施DDoS攻击。网络安全事件与社会活动紧密结合趋势明显，网络攻击事件高发。

2. 国家关键信息基础设施保护受到普遍关注

作为事关国家安全、社会稳定和经济发展的战略资源，国家关键信息基础设施保护的工作尤为重要。当前，应用广泛的基础软硬件安全漏洞不断被披露、具有特殊目的的黑客组织不断对我国关键信息基础设施实施网络攻击，我国关键信息基础设施面临的安全风险不断加大。随着关键信息基础设施承载的信息价值越来越高，针对国家关键信息基础设施的网络攻击将愈演愈烈。

3. 个人信息和重要数据泄露危害更加严重

2018年Facebook信息泄露事件让我们重新审视个人信息和重要数据的泄露可能引发的危害，信息泄露不仅侵犯个人利益，甚至可能对国家政治安全造成影响。近年来，我国境内发生了多起个人信息和重要数据泄露事件，犯罪分子利用大数据等技术手段，整合获得的各类数据，可形成对用户的多维度精准画像，所产生的危害将更为严重。

4. 5G、IPv6等新技术广泛应用带来的安全问题值得关注

目前，我国5G、IPv6等新技术的规模部署和使用工作逐步推进，关于5G、IPv6等新技术自身的安全问题以及衍生的安全问题值得关注。5G技术的应用，代表增强的移动宽带、海量的机器通信以及超高可靠低时延的通信，其与IPv6技术应用共同发展，将真正实现让万物互连，互联网上承载的信息将更丰富，物联网将大规模发展。但是，重要数据泄露、物联网设备安全问题在目前尚未得到有效解决，物联网设备被大规模利用来发起网络攻击的问题也将更加突出。同时，区块链技术也受到国内外广泛关注并快速应用，从数字货币到智能合约，并逐步向文化娱乐、社会管理、物联网等领域延伸。随着区块链应用的发展，数字货币被盗、智能合约、钱包和挖矿软件漏洞等安全问题将更加凸显。

1.5 网络信息安全的目标

网络信息安全的目的是保护信息免受各种威胁的损害，以确保业务的连续性，将业务风险最小化、投资回报和商业机遇最大化。在提出网络信息安全的目标之前，应分析各种安全攻击以及这些攻击对信息系统造成的影响。

1.5.1 安全性攻击

攻击者为了获取有用信息和达到某种攻击目的，采用各种方法来攻击信息系统。这些攻击方法主要分为被动攻击和主动攻击。

1. 被动攻击

被动攻击主要收集信息而不进行访问，数据的合法用户对这类攻击不会有所觉察。被动攻击包括窃听和流量分析。

（1）窃听：用各种可能的合法（或非法）手段来窃取系统中的信息资源和敏感信息。例如，对通信线路中传输的信号搭线监听，或者利用通信设备在工作过程中产生的电磁泄露来截取有用信息等。

（2）流量分析：通过对系统进行长期监听，利用统计分析方法对诸如通信频度、通信的信息流向、通信总量的变化等参数进行研究，从中发现有价值的信息和规律。

由于被动攻击不涉及对数据的更改，所以对其难以察觉。防御者可以通过对数据加密来防止这类攻击。

2. 主动攻击

主动攻击包含攻击者访问其所需信息的故意行为。例如，远程登录指定机器的端口25，找出公司运行的邮件服务器的信息；伪造无效 IP 地址连接服务器，使接受错误 IP 地址的系统浪费时间去连接该非法 IP 地址。由于攻击者主动地做一些不利于被攻击系统的事情，因此查找主动攻击并不困难。主动攻击包括拒绝服务非法使用、假冒、旁路控制等攻击方法。

（1）拒绝服务：使合法用户对信息或其他资源的合法访问被无条件阻止。

（2）非法使用（非授权访问）：某一资源被某个非授权的人（或以非授权的方式）使用。

（3）假冒：通过欺骗通信系统（或用户）达到非法用户冒充成为合法用户，或者权限小的用户冒充权限大的用户的目的。黑客通常采用假冒攻击。

（4）旁路控制：攻击者利用系统的安全缺陷或安全性上的脆弱之处来获得非授权的权利或特权。例如，攻击者通过各种攻击手段发现原本应保密但暴露出的一些系统“特性”，利用这些“特性”，攻击者可以绕过防线守卫者，进而侵入系统内部。

（5）授权侵犯：被授权以某种目的使用某系统（或资源）的某个用户将此权限用于其他非授权的目的。授权侵犯又称为“内部攻击”。

（6）特洛伊木马：在软件中嵌入一段用户觉察不出的有害程序段，当它被执行时，就会破坏用户系统的安全。

（7）陷阱门：在某个系统（或某个部件）中设置“机关”，当输入特定的数据时，允许该系统（或部件）违反安全策略。

（8）抵赖：一种来自用户的攻击。例如，否认自己曾经发布过的某条消息、伪造一份对方来信等。

（9）重放：出于非法目的，将所截获的某次合法的通信数据进行复制，并重新发送。

当前网络攻击的方法尚无规范的分类模式，各种方法的运用往往非常灵活。从攻击的目的来看，有拒绝服务攻击、获取系统权限的攻击、获取敏感信息的攻击等；从攻击的切入点来看，有缓冲区溢出攻击、系统设置漏洞的攻击等；从攻击的纵向实施过程来看，有获取初级权限攻击、提升最高权限攻击、后门攻击、跳板攻击等；从攻击的类型来看，有对各种操作系统的攻击、对网络设备的攻击、对特定应用系统的攻击等。所以，很难以统一的模式对各种攻击手段进行分类。

实际上，黑客实施入侵行为时，为达到其攻击目的，往往会结合多种攻击手段，在不同的入侵阶段使用不同的方法。

1.5.2 网络信息安全的目标

信息安全最基本的目标是实现信息的机密性，保证数据的完整性，保障信息资源和服务的可用性。不同的信息系统根据业务类型的不同，还可以通过提高不可否认性来认证通信双方，通过提高系统可控性来监控信息及信息系统。

1. 机密性

机密性是指保证机密信息不被窃听，或窃听者无法了解信息的真实含义。机密性服务通过加密算法来对数据进行加密，以确保信息即使处于不可信环境中也不会泄露。

在网络环境中，对数据机密性构成最大威胁的是嗅探者。嗅探者会在通信信道中安装嗅探器，检查所有流经该信道的数据流量，而加密算法是对付嗅探器的最好手段。

2. 完整性

完整性是指保证数据的一致性，防止数据被非法用户窜改。数据在传输过程中会处于很多不可信的环境，这些环境中难免会有一些攻击者试图对数据进行恶意修改，完整性服务用于保护数据免受非授权的修改。

哈希算法是保护数据完整性的最好方法。由于哈希函数具有单向性，发送方在发送信息前会对信息附上一段报文摘要，以保护其完整性。

3. 可用性

可用性是指保证合法用户对信息和资源的使用不会被不正当地拒绝。破坏信息（或系

统）的可用性的主要攻击是拒绝服务攻击。

4. 不可否认性

不可否认性是指建立有效的责任机制，防止用户否认其行为，这在电子商务中极其重要。不可否认服务可用于追溯信息（或服务）的源头，目前采用数字签名技术即可实现。

5. 可控性

可控性是指对信息及信息系统实施安全监控。实现可控性的关键是对网络中的资源进行标识，通过身份标识来达到对用户进行认证的目的。通常，系统会使用“用户所知”或“用户所有”来对用户进行标识，从而验证用户是否是其声称的身份。管理机构应对危害国家信息的来往、使用加密手段从事的非法通信活动等进行监视审计，对信息的传播及内容具有控制能力。

1.6 网络信息安全的研究内容

网络信息安全的研究范围非常广泛，其研究内容可划分为三个层次，即信息安全基础理论研究、信息安全应用技术研究、信息安全管理研究，如图 1－1 所示。本书重点介绍信息安全基础理论中的密码理论和安全理论、信息安全应用技术中的安全实现技术，对信息安全管理的内容没有涉及。

图 1－1 网络信息安全的研究内容