21世纪高等学校网络空间安全专业规划教材

信息安全与技术（第2版）

◎ 朱海波 主 编
辛海涛 刘湛清 副主编

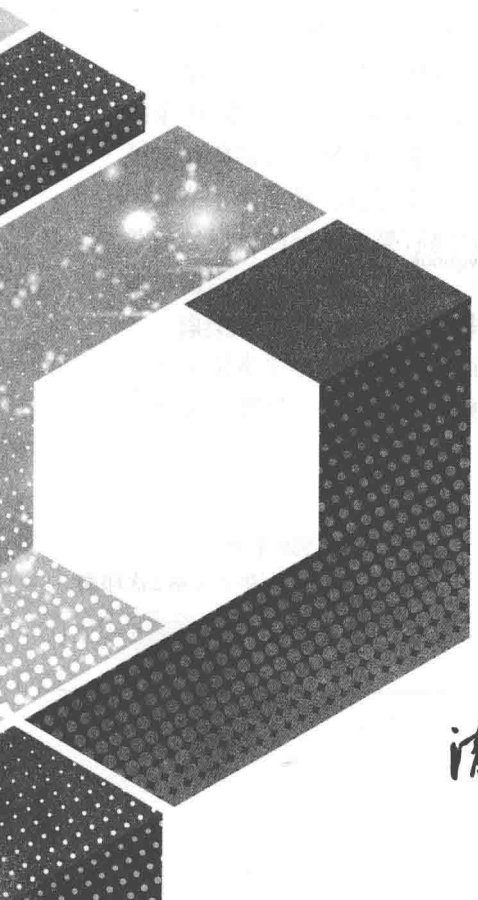
教学课件
教学大纲
实训软件
期末试卷

清華大學出版社

21世纪高等学校网络空间安全专业规划教材

信息安全与技术（第2版）

◎ 朱海波 主　编
辛海涛 刘湛清　副主编



清華大學出版社
北京

内 容 简 介

本书共分13章，内容包括信息安全概述、物理安全体系、信息加密技术、信息隐藏技术、网络攻击技术、入侵检测技术、黑客攻防剖析、网络防御技术、无线网络安全与防御技术、应用层安全技术、计算机病毒与防范技术、操作系统安全技术、信息安全解决方案。

本书既可作为计算机、通信、电子工程、信息对抗、信息管理、信息安全、网络空间安全及其他电子信息类相关专业的本科生教材，也可作为高等学校及各类培训机构相关课程的教材或教学参考书，还可供从事信息安全、信息处理、计算机、电子商务等领域工作的科研人员和工程技术人员参考。

图书在版编目(CIP)数据

信息安全与技术/朱海波主编. —2版. —北京：清华大学出版社，2019（2019.7重印）
(21世纪高等学校网络空间安全专业规划教材)
ISBN 978-7-302-50506-8

Ⅰ. ①信… Ⅱ. ①朱… Ⅲ. ①信息安全—安全技术 Ⅳ. ①TP309

中国版本图书馆CIP数据核字(2018)第134720号

策划编辑：魏江江
责任编辑：王冰飞
封面设计：刘　键
责任校对：时翠兰
责任印制：宋　林

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×260mm　　**印　　张**：23　　**字　　数**：559千字
版　　次：2014年1月第1版　2019年6月第2版　　**印　　次**：2019年7月第2次印刷
印　　数：5901～7900
定　　价：59.00元

产品编号：073486-01

第 2 版前言

随着科学技术的迅猛发展和信息技术的广泛应用，特别是我国国民经济和社会信息化进程的全面加快，网络与信息系统的基础性、全局性作用日益增强，信息安全已经成为国家安全的重要组成部分。如何保护企业或个人的信息系统免遭非法入侵，如何防止计算机病毒对内部网络的侵害，这些都是信息时代企业或个人面临的实际问题。因此，社会对信息安全技术的需求也越来越迫切。为了满足社会的需要，各高等院校计算机相关专业相继开设了信息安全方面的课程。为了满足信息安全技术教学方面的需求，编者编写了本书。本书在第 1 版(2014 年出版)的基础上，删除了冗余陈旧的知识，补充了信息安全领域的最新发展技术和成果，并增加了更实用的实训操作知识和技能。

本书以解决具体信息安全问题为目的，全面介绍信息安全领域的实用技术，帮助读者了解信息安全技术体系，掌握维护信息系统安全的常用技术和手段，解决实际信息系统的安全问题，使读者全方位建立起对信息安全体系的认识。

本书由朱海波任主编，由辛海涛、刘湛清任副主编。全书共 13 章，其中第 1～4 章和第 10 章由朱海波编写，第 8 章和第 11～13 章由辛海涛编写，第 5～7 章和第 9 章由刘湛清编写。全书由朱海波负责统稿和定稿。

在本书的编写过程中，吸收了许多专家的宝贵意见，参考了大量的网站资料和国内外众多同行的研究成果，同时得到了清华大学出版社的大力支持和帮助，在此表示衷心的感谢。

由于信息安全技术发展非常快，本书的选材和编写也许有不尽如人意的地方，加上编者学识水平和时间所限，书中难免存在不足之处，恳请同行专家和读者指正，以便进一步完善提高。编者联系方式：chnhsd@163.com。

编　者

2019 年 1 月

第1版前言

信息安全学科对国家安全和经济建设有着极其重要的作用。近年来，随着我国国民经济和社会信息化进程的全面加快，计算机网络在政治、军事、金融、商业等部门的广泛应用，网络与信息系统的基础性、全局性作用不断增强，全社会对计算机网络的依赖越来越大。网络系统如果遭到破坏，不仅会引起社会混乱，还将带来经济损失。信息安全已经成为国家安全的重要组成部分。加快信息安全保障体系的建设、培养高素质的网络安全人才队伍，已经成为我国经济社会发展和信息安全体系建设中的一项长期性、全局性和战略性的任务。为此，我们根据自己的科学实践，结合信息安全与技术的教学经验，编写了本书。

信息安全与技术是一门涉及计算机科学、网络技术、密码技术、信息论、通信技术等多种学科的综合性科学。全书共13章，内容包括信息安全概述、物理安全体系、信息保密技术、信息隐藏技术、网络攻击技术、入侵检测技术、黑客攻防剖析、网络防御技术、无线网络安全与防御技术、应用层安全技术、计算机病毒与防范技术、操作系统安全技术、信息安全解决方案。

第1章信息安全概述，介绍信息安全的基本概念及需求，并系统地分析信息安全环境的现状和网络不安全的原因，最后引出信息安全的体系结构。

第2章物理安全体系，介绍计算机系统的物理安全及其主要内容。物理安全在整个计算机网络信息系统安全中占有重要地位，主要包括环境安全、设备安全和媒体安全3个方面。

第3章信息保密技术，介绍密码学的发展历程，着重介绍古典密码体制、对称密码体制和非对称密码体制，最后介绍密码学的应用，包括密码应用模式和加密方式。

第4章信息隐藏技术，介绍信息隐藏技术的发展历程，着重介绍信息隐藏技术的概念、分类及特性，以及信息隐藏技术的常用算法、数字水印技术、隐通道技术和匿名通信技术。

第5章网络攻击技术，介绍网络攻击的目标、手段、层次、分类和一般模型，以及信息收集技术的步骤、方法、工具，着重介绍网络后门与网络隐身技术等。

第6章入侵检测技术，介绍入侵检测的概念、功能及工作过程，以及网络入侵检测系统产品，重点介绍入侵攻击可利用的系统漏洞类型、漏洞检测技术分类、系统漏洞检测方法、常见的系统漏洞及防范以及系统漏洞检测工具。

第7章黑客攻防剖析，介绍黑客和骇客的起源及概念、黑客的攻击分类和步骤，重

点介绍了国产经典软件和常用软件,最后介绍黑客攻击防御方法。

第8章网络防御技术,介绍网络体系结构、IPSec协议、SSL/TLS协议,以及防火墙的基本概念、分类、实现模型,最后介绍VPN技术、蜜罐主机与欺骗网络等。

第9章无线网络安全与防御技术,介绍无线网络安全的基本概念和无线局域网常见的设备,着重介绍无线局域网的标准、无线网面临的安全威胁、网络安全协议和安全技术等。

第10章应用层安全技术,介绍Web安全技术,着重介绍电子邮件安全技术、身份认证技术和PKI安全体系等。

第11章计算机病毒与防范技术,从概念、分类、特征、破坏行为和作用机理等方面详细地介绍了计算机病毒,并从检测、清除以及防范的角度介绍了计算机病毒的防治。

第12章操作系统安全技术,介绍UNIX、Linux和Windows的特点,着重介绍安全操作系统的原理,介绍Windows操作系统的安全配置方案。

第13章信息安全解决方案,介绍信息安全体系结构的现状、网络安全需求,以及常见的网络安全产品,从网络安全工程的角度介绍某大型企业和电子政务的信息安全解决方案。

本书由朱海波、刘湛清、程日来和郭春阳编写。全书共13章,其中,第2、3、4、10、13章由朱海波编写,第5、6、7、9、12章由刘湛清编写,第8章由程日来编写,第1、11章由郭春阳编写。全书最后由朱海波负责统稿、定稿工作。本书在编写过程中吸收了许多专家的宝贵意见,参考了大量的网站资料和国内外众多同行的研究成果,在此,编者对有关人士和网站表示衷心的感谢,同时也感谢清华大学出版社的大力支持。

由于信息安全技术内容广泛且发展迅速,加之编者水平有限,本书难免有疏漏与不足之处,恳请各位专家和读者批评指正,以便进一步完善和提高。

编 者

2013年7月

目　录

第1章　信息安全概述

随着全球经济和信息化的发展，信息资源已成为社会发展的重要战略资源，信息技术和信息产业正在改变传统的生产和生活方式，逐步成为国家经济增长的主要推动力之一。信息化、网络化的发展已成为不可阻挡、不可回避、不可逆转的历史潮流和历史事实，信息技术和信息的开发应用已渗透到国家政治、经济、军事和社会生活的各个方面，成为生产力的重要因素。在全球化和信息化的潮流下，信息安全面临诸多挑战，因此信息安全的研究与开发显得更加迫切，许多国家和地区采取了有力的措施推进信息安全技术与相关技术的发展。信息安全面临的问题较多，在方法上涉及数学、物理、微电子、通信及计算机等众多领域，有着系统的技术体系和丰富的科学内涵。

1.1　信息安全基本概念

1.1.1　信息安全的含义

信息安全既是传统通信保密的延续和发展，又是网络互联时代出现的新概念。信息安全概念是随着信息技术的发展而不断拓展、不断深化的。信息安全概念的外延不断扩大、内涵不断丰富，由单一的通信保密发展到计算机安全、信息系统安全，又扩展到对信息基础设施、应用服务和信息内容实施全面保护的信息安全保障；由单一的对通信信息的保密，扩展到对信息完整性、真实性的保护，再深化到对信息的保密性、完整性、真实性、可控性，以及信息基础设施的可用性和交互行为的不可否认性的全面保护。

信息安全是一个包括信息安全行为主体、保护对象、防护手段、任务目的等内容的综合性概念。各国国情和信息化水平不同，信息安全概念的表述也不尽相同。我国信息安全的概念可表述为：信息安全是指在政府主导和社会参与下，综合运用技术、法律、管理、教育等手段，在信息空间积极应对敌对势力攻击、网络犯罪和意外事故等多种威胁，有效保护信息基础设施、信息系统、信息应用服务和信息内容的安全，为经济发展、社会稳定、国家安全和公众权益提供安全保障的活动。

1.1.2　对信息安全重要性的认识

对信息安全重要性的认识主要表现在以下3个层面。

1. 第一个层面的认识

信息安全的重要性主要体现在信息内容安全、信息系统安全、信息网络安全、信息基础设施安全等方面。信息内容的被泄露、被假冒、被伪造等，信息系统被攻击、被入侵、被染毒，信息网络被堵塞、被中断、被致瘫等，信息基础设施被损伤、被破坏、被损毁等，这些都是重要的信息安全事件，必须引起高度重视和迅速解决。但是，对信息安全重要性的认识仅仅停留

在这个层面上是不够的。

2. 第二个层面的认识

美国在1990年即将网络攻击武器视为与核、生、化武器并列的大规模破坏性武器,这是对信息安全重要性认识的较高层面。可以想象,一个国家或一个行业的信息系统瘫痪了,其影响和损失远远比大规模杀伤性武器要大得多。例如,一个国家的银行信息系统瘫痪了,整个国家将陷入混乱,这远比核、生、化武器的破坏性更广泛、更深入、更持久。网络攻击武器是实现"不战而屈人之兵"的最有效的武器之一。

3. 第三个层面的认识

科学技术不断发展使得国家疆域不断改变。航海技术的发展,使得国家疆域从领土扩展到了领海;航空技术的发展,又使得国家疆域扩展到了领空。航天技术的发展,再使得国家疆域扩展到了太空。网络技术的发展,将会使得国家的疆域再次扩展。简单来讲,网络疆域将是国家疆域不可分割的一部分,是不容他人侵犯的国家疆域。这是对信息安全重要性认识的更高层面。

1.1.3 信息安全的作用和地位

随着社会信息化发展进程的不断加快,信息技术已渗透到国家政治、经济、军事和社会生活的各个方面,国家、社会和个人对信息的依赖程度越来越高,信息已成为重要的战略资源,信息化水平已成为衡量一个国家和地区的国际竞争力、现代化水平、综合国力和经济成长能力的重要标志。与此同时,社会面临的信息安全威胁也成为影响和制约国家发展的重要因素。

从国家层面上看,当前我国国民经济和社会信息化建设进程全面加快,信息安全在保障经济发展、社会稳定、国家安全、公众权益中的作用和地位日显重要,主要表现为以下几个方面。

1. 关乎经济发展

目前,我国已建立了覆盖全国的公用电信网、广播电视网等基础信息网络,银行、民航、铁路、电力、证券、海关、税务等关系国民经济发展和正常运行的重要支撑领域基本完成了行业信息系统建设,传统工业的信息化改造正逐步展开,电子政务、电子商务、电子事务也在不断推进,它们在国家经济发展中起着十分重要的作用。这些信息系统的安全一旦受到威胁和破坏,轻则影响经济发展,重则损害国家经济利益,甚至导致整个国民经济的瘫痪或崩溃。信息安全在经济领域中的保障作用将会越来越重要。

2. 关乎社会稳定

以Internet为代表的信息网络,是继报刊、广播、电视之后新兴的大众媒体,具有传播迅速、渗透力强、影响面大的特点,形成了一个不受地域限制的新空间。在这个空间里,不同的意识形态、价值观念、行为规范、生活方式等在激烈碰撞,毒害人民、污染社会的色情、迷信、暴力等反动腐朽文化,经济诈骗、敲诈勒索、非法传销等网络犯罪活动,以制造恐怖气氛、造成社会混乱为目的的网络恐怖活动,这些都对我国的社会稳定和公共秩序构成了严重危害。有效应对网络空间中的上述危害,已成为信息化条件下维护社会稳定、巩固国家政权的重要工作。

3. 关乎国家安全

信息空间已成为与领土、领海、领空等并列的国家主权疆域，信息安全是国家安全的重要组成部分。国内外各种敌对、分裂、邪教等势力利用网络对我国进行的反动宣传和政治攻击，敌对国家和地区对我国实施的网络渗透、网络攻击等信息对抗行动，西方有害价值观和文化观在网络上的大肆传播，使我国的政治安全、国防安全和文化安全面临着前所未有的挑战。随着信息技术的迅速普及、广泛应用和深层渗透，信息安全在政治安全、国防安全、文化安全等国家安全领域将具有越来越重要的作用。

4. 关乎公众权益

随着科学技术和国民经济的发展，社会公众对信息的依赖程度越来越高，网络的触角已经深入到社会生活的各个方面。网络应用服务的普及直接涉及个人的合法权益，宪法规定的多项公众权益在网络上将逐步得到体现，需要得到保护。这种普遍的、社会化的需求，对信息安全问题提出了比以往更广、更高的要求。

1.2　信息安全环境及现状

1.2.1　信息安全的威胁

信息安全威胁是指某些因素(人、物、事件、方法等)对信息系统的安全使用可能构成的危害。信息安全威胁来自方方面面，无处不在，如图 1-1 所示。

图 1-1　威胁来自方方面面

一般来说，人们把可能威胁信息安全的行为称为攻击。在计算机网络中，常见的信息安全威胁有以下几类。

(1) 信息泄露。信息泄露是指信息被泄露给未授权的实体，泄露的形式主要包括窃听、截收、侧信道攻击和人员疏忽等。其中，截收一般是指窃取保密通信的电波、网络信息等；侧信道攻击是指攻击者虽然不能直接取得保密数据，但是可以获得这些保密数据的相关信

息,而这些信息有助于分析出保密数据的内容。

(2) 篡改。篡改是指攻击者擅自更改原有信息的内容,但信息的使用者并没有意识到信息已经被更改的事实。在传统环境下,篡改者对纸质文件的篡改可以通过一些鉴定技术识别出来;但是在数字环境下,对电子内容的篡改不会留下明显的痕迹。

(3) 重放。重放是指攻击者可能截获合法的通信信息,此后出于非法的目的重新发送已截获的信息,而接收者可能仍然按照正常的通信信息受理,从而被攻击者所欺骗。

(4) 假冒。假冒是指某用户冒充其他的用户登录信息系统,但是信息系统可能并不能识别出冒充者,这就使冒充者获得本不该得到的权限。

(5) 否认。否认是指参与某次数据通信或数据处理的一方事后拒绝承认本次数据通信或数据处理曾经发生过,这会导致这类数据通信或数据处理的参与者逃避应承担的责任。

(6) 非授权使用。非授权使用是指信息资源被某些未授权的人或系统使用,当然也包括被越权使用的情形。

(7) 网络与系统攻击。由于网络和主机系统在设计或实现上往往存在一些漏洞,攻击者可能利用这些漏洞来攻击主机系统;此外攻击者仅通过对某一信息服务资源进行长期占用,使系统不能够正常运转,这种攻击一般被称为拒绝服务攻击。

(8) 恶意代码。恶意代码是指恶意破坏计算机系统、窃取机密信息或秘密地接受远程操控的程序。恶意代码由居心叵测的用户编写和传播,隐藏在受害方的计算机系统中,这些代码也可以进行自我复制和传播。恶意代码主要包括木马程序、计算机病毒、后门程序、蠕虫病毒及僵尸网络等。

(9) 故障、灾害和人为破坏。管理信息系统也可能因硬件故障、自然灾害(水灾、火灾及地震等)或人为破坏而受到破坏。

上面提到的信息安全威胁直接危及信息安全的不同属性。信息泄露危及机密性;篡改危及真实性和完整性;重放、假冒和非授权使用危及真实性和可控性;否认危及非否认性;网络与系统攻击、故障、灾害和人为破坏危及可用性;恶意代码依照其意图可能分别危及可用性、机密性和可控性等。以上分析说明,可用性、机密性、完整性、非否认性、真实性和可控性6个属性反映了信息安全的本质特征和基本需求。

也可以进一步地将信息安全威胁划分为4类:暴露(Disclosure),指对信息进行未授权访问,主要是来自信息泄露的威胁;欺骗(Deception),指信息系统被误导接收到错误的数据甚至做出错误的判断,包括来自篡改、重放、假冒、否认等的威胁;打扰(Disruption),指干扰或中断信息系统的执行,主要包括来自网络与系统攻击、灾害、故障与人为破坏的威胁;占用(Usurpation),指未授权使用信息资源或系统,包括来自未授权使用的威胁。类似地,恶意代码按照其意图不同可以划归到不同的类别中。

还可以将前面论及的信息安全威胁分为被动攻击和主动攻击两类。被动攻击仅窃听、截收和分析受保护的数据,这种攻击形式并不篡改受保护的数据,更不会插入新的数据;主动攻击试图篡改受保护的数据,或者插入新的数据。

1.2.2 信息安全的目标

信息安全旨在确保信息的机密性、完整性和可用性,即CIA(Confidentiality、Integrity、Availability)。用户A想和用户B进行一次通信,下面以这两个用户的通信过程为例来介