高等学校电子信息类“十三五”规划教材
应用型网络与信息安全工程技术人才培养系列教材

信息安全理论与技术

（卓越工程师计划）

李飞　吴春旺　王敏　编著

西安电子科技大学出版社
http://www.xduph.com

应用型网络与信息安全工程技术人才培养系列教材
高等学校电子信息类“十三五”规划教材

信息安全理论与技术

（卓越工程师计划）

李 飞　吴春旺　王 敏　编著

西安电子科技大学出版社

内容简介

本书涵盖了信息安全的理论、技术与管理三大体系，主要介绍信息安全的基本概念、方法和技术，为今后进一步学习、研究信息安全理论与技术或者从事计算机网络信息安全技术与管理工作奠定理论和技术基础。

全书共13章，前两章为信息安全基础知识和密码学的基本理论，第3～10章为密钥管理技术、数字签名与认证技术、PKI技术、网络攻击与防御技术、恶意代码及防范技术、访问控制技术、虚拟专用网络(VPN)和系统安全技术，第11～13章为安全审计技术、信息安全体系结构与安全策略、信息安全评估标准与风险评估。

为了提高学生的综合能力，本书设计了四个综合训练，以提高学生的综合设计能力。

本书可以作为信息安全与计算机网络安全类课程的教材，也可作为电子商务专业相关课程的教材。

图书在版编目(CIP)数据

信息安全理论与技术/李飞，吴春旺，王敏编著. —西安：西安电子科技大学出版社，2016.3
高等学校电子信息类"十三五"规划教材
ISBN 978-7-5606-3977-2

Ⅰ. ① 信… Ⅱ. ① 李… ② 吴… ③ 王… Ⅲ. ① 信息安全—安全技术—高等学校—教材
Ⅳ. ① TP309

中国版本图书馆CIP数据核字(2016)第013321号

策划编辑　李惠萍
责任编辑　马武装　宁晓蓉
出版发行　西安电子科技大学出版社(西安市太白南路2号)
电　　话　(029)88242885　88201467　　邮　　编　710071
网　　址　www.xduph.com　　电子邮箱　xdupfxb001@163.com
经　　销　新华书店
印刷单位　陕西华沐印刷科技有限责任公司
版　　次　2016年3月第1版　2016年3月第1次印刷
开　　本　787毫米×1092毫米　1/16　印张　18.5
字　　数　430千字
印　　数　1～3000册
定　　价　33.00元
ISBN 978-7-5606-3977-2/TP

XDUP　426900-1

序

进入21世纪以来，信息技术迅速改变着人们传统的生产和生活方式，社会的信息化已经成为当今世界发展不可逆转的趋势和潮流。信息作为一种重要的战略资源，与物资、能源、人力一起已被视为现代社会生产力的主要因素。目前，世界各国围绕着信息获取、利用和控制的国际竞争日趋激烈，网络与信息安全问题已成为一个世纪性、全球性的课题。党的十八大报告明确指出，要“高度关注海洋、太空、网络空间安全”。党的十八届三中全会决定设立国家安全委员会，成立中央网络安全和信息化领导小组，并把网络与信息安全列入了国家发展的最高战略方向之一。这为包含网络空间安全在内的非传统安全领域问题的有效治理提供了重要的体制机制保障，是我国国家安全体制机制的一个重大创新性举措，彰显了我国政府治国理政的战略新思维和“大安全观”。

人才资源是确保我国网络与信息安全第一位的资源，信息安全人才培养是国家信息安全保障体系建设的基础和必备条件。随着我国信息化和信息安全产业的快速发展，社会对信息安全人才的需求不断增加。2015年6月11日，国务院学位委员会和教育部联合发出“学位[2015]11号”通知，决定在“工学”门类下增设“网络空间安全”一级学科，代码为“0839”，授予工学学位。这是国家推进专业化教育，在信息安全领域掌握自主权、抢占先机的重要举措。

新中国成立以来，我国高等工科院校一直是培养各类高级应用型专门人才的主力。培养网络与信息安全高级应用型专门人才，高等院校也应责无旁贷。目前，许多高等院校和科研院所已经开办了信息安全专业或开设了相关课程。作为国家首批61所“卓越工程师教育培养计划”试点院校之一，成都信息工程大学以《国家中长期教育改革和发展规划纲要(2010—2020年)》、《国家中长期人才发展规划纲要(2010—2020年)》、《卓越工程师教育培养计划通用标准》为指导，以专业建设和工程技术为主线，始终贯彻“面向工业界、面向未来、面向世界”的工程教育理念，按照“育人为本、崇尚应用”、“一切为了学生”的教学教育理念和“夯实基础、强化实践、注重创新、突出特色”的人才培养思路，遵循“行业指导、校企合作、分类实施、形式多样”的原则，实施了一系列教育教学改革。令人欣喜的是，该校信息安全工程学院与西安电子科技大学出版社近期联合组织了一系列网络与信息安全专业教育教学改革的研讨活动，共同研讨培养应用型高级网络与信息安全工程技术人才的教育教学方法和课程体系，并在总结近年来该校信息安全专业实施“卓越工程师教育培养计划”教育教学改革成果和经验的基础上，组织编写了“应用型网络与信息安全工程技术人才培养系列教材”。本套教材总结了该校信息安全专业教育教学改革的成果和经验，相关课程有配套的课程过程化考核系统，是培养应用型网络与信息安全工程技术人才的一套比较完整、实用的教材，相信可以对我国高等院校网络与信息安全专业的建设起到很好的促进作用。该套教材为中国电子教育学会高教分会推荐教材。

信息安全是相对的，信息安全领域的对抗永无止境。国家对信息安全人才的需求是长期的、旺盛的。衷心希望本套教材在培养我国合格的应用型网络与信息安全工程技术人才的过程中取得成功并不断完善，为我国信息安全事业做出自己的贡献。

高等学校电子信息类“十三五”规划教材
应用型网络与信息安全工程技术人才培养系列教材
名誉主编（中国密码学会常务理事）

何大可

二〇一五年十月

中国电子教育学会高教分会推荐

高等学校电子信息类“十三五”规划教材

应用型网络与信息安全工程技术人才培养系列教材

编审专家委员会名单

名誉主任：何大可（中国密码学会常务理事）

主　　任：张仕斌（成都信息工程大学信息安全学院副院长、教授）

副 主 任：李　飞（成都信息工程大学信息安全学院院长、教授）

何明星（西华大学计算机与软件工程学院院长、教授）

苗　放（成都大学计算机学院院长、教授）

赵　刚（西南石油大学计算机学院院长、教授）

李成大（成都工业学院教务处处长、教授）

宋文强（重庆邮电大学移通学院计算机科学系主任、教授）

梁金明（四川理工学院计算机学院副院长、教授）

易　勇（四川大学锦江学院计算机学院副院长、成都大学计算机学院教授）

杨瑞良（成都东软学院计算机科学与技术系主任、教授）

编审专家委员：（排名不分先后）

范太华　叶安胜　黄晓芳　黎忠文　张　洪　张　蕾

贾　浩　赵　攀　陈　雁　韩　斌　李享梅　曾令明

何林波　盛志伟　林宏刚　王海春　索　望　吴春旺

韩桂华　赵　军　陈　丁　秦　智　王中科　林春蔷

张金全　王祖俪　蔺　冰　王　敏　万武南　甘　刚

王　燚　闫丽丽　昌　燕　黄源源　张仕斌　李　飞

王海春　何明星　苗　放　李成大　宋文强　梁金明

万国根　易　勇　杨瑞良

前　言

“信息安全理论与技术”是计算机科学技术类、通信工程和信息对抗技术等专业本科生的专业基础必修课程，一般安排2～3个学分，学时从32个到48个不等。这门课程内容较多，不仅要介绍信息安全学科相关的理论知识，还要介绍信息安全的相关技术，同时涉及多个学科的基础知识。在通常的教学实践中，有的专业只开设这一门课程(或者“网络安全”课程)，就希望学生能基本上掌握信息安全的基础知识和技术，从而给这门课程的教学带来巨大的困难。本教材的编写出版就希望解决该困难。

目前国内大多数高校正在推行工程教育理念，加上学生还需要参加各种专业认证，这就要求学生不仅要掌握扎实的理论知识，还要具有较强的动手能力，以便满足社会需求。但目前许多高校培养的工科学生有一个通病，要么强调理论轻视技术，要么重视技术轻视理论，不同层次的高校学生犯同层次相同的毛病。如何结合工程教育理念来教育学生，使他们明白，理论是基础，技术只是理论指导下的实现手段，没有理论作指导，技术无法达到一定的高度，这是摆在教师面前的一个巨大问题。解决不了这个问题，就无法教育出优秀的学生，也无法成为一个优秀的教育者。

具体到“信息安全理论与技术”这门课程来说，首先要使学生明白系统概念，它要求学生能将之前学习过的课程，如高等数学相关课程以及“C语言程序设计”、“数据结构”、“操作系统原理”、“数据库原理与技术”和“计算机网络”等课程的理论与本课程有关理论知识贯穿起来，同时在讲解信息安全体系结构相关内容时，使学生明白仅仅一种信息安全技术是无法完成系统安全保障要求的，要有一个系统概念，即在管理制度约束下，在信息安全相关理论指导下进行多种技术集成，才能构成一个系统安全的保障体系。没有系统的思维，单靠一门技术会给系统留下巨大的隐患。在讲解信息安全理论时，教师要注意理论的承前启后，强调理论指导技术的重要性，让学生明白没有理论作指导，是无法实现好的设计的。同时，对于信息安全技术课程的相关内容，可以预先布置，让学生预习并分组讨论，然后请学生代表在课堂作总结，教师和学生共同点评，培养学生的表达能力、团队协作能力以及发现问题和解决问题的能力。这样，通过一门课程的教学，可以实现现代工程教育理念所要求的培养学生的目标。

本书的主要任务是介绍信息安全的基本概念、方法和技术，使学生掌握信息安全的基本知识、信息安全模型、当代主流的密码技术、访问控制技术、数字签名和信息认证技术、安全审计与监控技术、网络攻防技术、病毒及防范技术、信息安全体系结构以及各种安全服务及安全机制，为今后进一步学习与研究信息安全理论与技术或者从事计算机网络信息安全技术与管理工作奠定理论和技术基础。全书内容涵盖了信息安全的理论、技术与管理三大体系，有助于学生信息安全整体理念的形成。

为了提高学生的综合设计能力，本书设计了四个综合训练，通过实验的方式巩固理论知识，提升学生综合水平。有些实验没有标准答案，只是考察学生的综合设计能力。这些实验涉及的知识面较广，在指导学生做这些实验时，希望教师能安排完成这些设计实验的同学进行讲解，以便大家共享相关知识，共同提高。

本书也可以作为计算机网络安全类课程的相关教材，还可以作为电子商务专业本科生相关课程的教材。

由于时间仓促，许多地方还不完善，敬请专家指正。

编　者

2015 年 10 月

目　录

第 1 章　信息安全基础知识

信息是当今社会发展的重要战略资源，也是衡量一个国家综合国力的重要指标。对信息的开发、控制和利用已经成为国家间利用、争夺的重要内容；同时信息的地位和作用也随着信息技术的快速发展而急剧上升，信息的安全问题也同样因此而日益突出和被各国高度重视。

1.1　信息与信息的特征

信息是客观世界中各种事物的变化和特征的最新反映，是客观事物之间联系的表征，也是客观事物状态经过传递后的再现。因此，信息是主观世界联系客观世界的桥梁。在客观世界中，不同的事物具有不同的特征，这些特征给人们带来不同的信息，而正是这些信息使人们能够认识客观事物。

信息的特征如下：

- 普遍性和可识别性。
- 储存性和可处理性。
- 时效性和可共享性。
- 增值性和可开发性。
- 可控性和多效用性。

此外，信息还具有转换性、可传递性、独立性和可继承性等特征。同时，信息还具有很强的社会功能，主要表现为资源功能、启迪功能、教育功能、方法论功能、娱乐功能和舆论功能等。信息的这些社会功能都是由信息的基本特征所决定和派生的。由此，可以看到保证信息安全的重要性！

1.2　网络空间安全

网络空间安全关系到国家安全和社会稳定，有效维护网络空间安全已成为人类的共同责任。当前，网络空间已被视为继陆、海、空、天之后的“第五空间”，网络空间安全已成为各国高度关注的重要领域。近年来，多个国家纷纷制定网络政策，提高网络基础设施的安全性和可靠性，完善相关法律法规和管理制度，打击各种危害网络安全的行为，网络空间治理水平得到一定提高。

网络空间安全是一个近几年新出现的概念，它与信息安全、网络安全的关系，需要大家有一个清楚的认识。

1.2.1 信息安全的定义与特征

“信息安全”没有公认和统一的定义，国内外对信息安全的论述大致可以分成两大类：一是指具体的信息系统的安全；二是指某一特定信息体系(例如一个国家的金融系统、军事指挥系统等)的安全。但现在很多专家都认为这两种定义均失之于其范畴过窄，目前公认的“信息安全”的定义为：(一个国家的)信息化状态和信息技术体系不受外来的威胁与侵害。因为信息安全，首先应该是一个国家宏观的社会信息化状态是否处于自控之下，是否稳定的问题；其次才是信息技术的安全问题。

在网络出现以前，信息安全指对信息的机密性、完整性和可控性的保护——面向数据的安全。互联网出现以后，信息安全除了上述概念以外，其内涵又扩展到面向用户的安全——鉴别、授权、访问控制、抗否认性和可服务性以及内容的个人隐私、知识产权等的保护。这两者结合就是现代的信息安全体系结构。

因此，在现代信息安全的体系结构中，信息安全包括面向数据的安全和面向用户的安全，即信息安全是指信息在产生、传输、处理和存储过程中不被泄露或破坏，确保信息的可用性、保密性、完整性和不可否认性，并保证信息系统的可靠性和可控性。因此，信息安全具有这样一些特征：

(1) 保密性：保密性是指信息不泄露给非授权的个人、实体和过程，也不能供其使用的特性。

(2) 完整性：完整性是指信息未经授权不被修改、不被破坏、不被插入、不延迟、不乱序和不丢失的特性。

(3) 可用性：可用性是指合法用户访问并能按要求顺序使用信息的特性，即保证合法用户在需要时可以访问信息及相关资产。

(4) 可控性：可控性是指授权机构对信息的内容及传播具有控制能力的特性，可以控制授权范围内的信息流向以及传播方式。

(5) 可审查性：在信息交流过程结束后，通信双方不能抵赖曾经做出的行为，也不能否认曾经接收到对方的信息。

由此，信息安全应包含三层含义：

(1) 系统安全(实体安全)，即系统运行的安全性。

(2) 系统中信息的安全，即通过控制用户权限、数据加密等确保信息不被非授权者获取和篡改。

(3) 管理安全，即综合运用各种手段对信息资源和系统运行安全性进行有效的管理。

1.2.2 网络安全的定义与特征

网络安全从其本质上讲就是网络上信息的安全，指网络系统的硬件、软件及其系统中的数据的安全。网络信息的传输、存储、处理和使用都要求处于安全的状态之下。

1. 网络安全的定义

网络安全所涉及的领域相当广泛。因为目前的公用通信网络中存在各种各样的安全漏洞和威胁。从广义上讲，凡是涉及到网络上信息的保密性、完整性、可用性和可控性等的相关技术和理论，都是网络安全所要研究的领域。

网络安全从本质上讲就是网络上信息的安全，即网络上信息保存、传输的安全，指网络系统的硬件、软件及系统中的数据受到保护，不因偶然和或者恶意的原因而遭到破坏、更改、泄露，系统连续、可靠、正常地运行，网络服务不中断。

从用户(个人、企业等)的角度来说，他们希望涉及个人隐私或商业利益的信息在网络上传输时受到机密性、完整性和真实性的保护，避免他人或对手利用窃听、冒充、篡改和抵赖等手段对用户的利益和隐私进行损坏和侵犯，同时也希望当用户的信息保存在某个计算机系统中时，不被非授权用户访问和破坏。

从网络运行和管理者的角度来说，他们希望对本地网络信息的访问、读写等操作受到保护和控制，避免出现病毒、非法存取、拒绝服务和网络资源的非法占用及非法控制等威胁，制止和防御网络“黑客”的攻击。

从安全保密部门的角度来说，他们希望对非法的、有害的或涉及国家机密的信息进行过滤和防堵，避免其通过网络泄露，避免由于这类信息的泄露对社会产生危害，给国家造成巨大的经济损失，甚至威胁到国家安全。

从社会教育和意识形态的角度来说，网络上不健康的内容不仅会给青少年造成不良影响，甚至会对社会的稳定和人类的发展造成阻碍，必须对其进行控制。

由此，网络安全应包含四层含义：

(1) 运行系统安全，即保证信息处理和传输系统的安全。其本质上是保护系统的合法操作和正常运行。包括计算机系统机房环境的保护，法律、政策的保护，计算机结构设计上的安全性考虑，硬件系统的可靠安全运行，计算机操作系统和应用软件的安全，电磁信息泄露的防护等。它侧重于保证系统的正常运行，避免因系统的崩溃和损坏而对系统存储、处理和传输的信息造成破坏和损失，避免因电磁泄漏产生信息泄露，干扰他人(或受他人干扰)。

(2) 网络上系统信息的安全，包括用口令鉴别、用户存取权限控制、数据存取权限、方式控制、安全审计、安全问题跟踪、计算机病毒防治、数据加密等。

(3) 网络上信息传播的安全，即信息传播中的安全，包括信息过滤技术。它侧重于防止和控制非法、有害的信息进行传播后的不良后果，避免公用通信网络上大量自由传输的信息失控，本质上是维护道德、法则或国家利益。

(4) 网络上信息内容的安全。它侧重于网络信息的保密性、真实性和完整性，避免攻击者利用系统的安全漏洞进行窃听、冒充和诈骗等行为，本质上是保护用户的利益和隐私。

由此可见，网络安全与其所保护的信息对象有关，本质上是在信息的安全期内保证其在网络上流动时或静态存储时不被非法用户所访问，但授权用户可以访问。

因此，网络安全的结构层次包括物理安全、安全控制和安全服务。

2. 网络安全的主要特征

(1) 保密性：指网络上的信息不泄露给非授权用户、实体或过程，或只供合法用户使用的特性。

(2) 完整性：指信息在存储或传输过程中保持不被修改、不被破坏和丢失的特性，也即未经授权不能进行改变的特性。

(3) 可用性：指当需要时应能存取所需的信息，也即可以被授权实体访问并按需求使

用的特性。网络环境下的拒绝服务、破坏网络和有关系统的正常运行等都属于对可用性的攻击。

(4) 可控性：指对信息的传播及内容具有控制的能力。

因此，网络安全与 信息安全研究的内容是紧密相关的，其发展是相辅相成的。但是信息安全的研究领域包括网络安全的研究领域。

1.2.3 网络空间(Cyberspace)安全

网络空间是哲学和计算机领域中的一个抽象概念，指在计算机以及计算机网络里的虚拟现实。网络空间一词是控制论(cybernetics)和空间(space)两个词的组合，是由居住在加拿大的科幻小说作家威廉·吉布森在 1982 年发表于《OMNI》杂志的短篇小说《融化的铬合金(Burning Chrome)》中首次提出来的。Cyberspace 的译法繁多，有人将它译作“网络空间”，更有“异次元空间”、“多维信息空间”、“电脑空间”、“网络空间”等译法。目前在国内信息安全界一般翻译为网络空间，它是自然空间中的一个域，由网络、电磁场以及人在其中的信息交互共同组成，已成为继陆地、海洋、天空和外太空之后人类生存的第五空间。

“网络空间”理论最早由美国科学家提出，实质就是指网络电磁空间。进入 21 世纪，随着网络以指数速度渗透到社会生活的各个角落，并创造出人类活动的第五维空间——网络电磁空间，传统的战争形态及战争观由此发生了急剧变化。崭新形态的网络政治、网络经济、网络文化、网络军事和网络外交等形成了新空间的道道风景，催生了网络战的闪亮登场。由此可见，网络空间是一个广泛、无所不在的网络(Ubiquitous and Pervasive Networks)。

网络空间具有四大特性：

(1) 网络融合性：融合了互联网、电信网络、广播电视网络、物联网(IoT)等 。

(2) 终端多样性：智能手机、电视、PC、iPad 等都可成为终端。

(3) 内容多样化：内容涉及云计算、社交网络、对等网络服务等。

(4) 领域广泛性：涉及政治、经济、文化等应用领域。

网络空间互联互通、多路由、多节点的特性为我们带来了一条“无形但有界”的复杂“新疆界”，其“边境线”根据网络建设能力、利用能力和控制能力大小而划分，即“网络疆域＝已建网络＋控制网络－被控网络”，它是变化的、非线性的，在实时对抗中此消彼长。国家利益拓展到哪里，维护国家第五维空间安全的“边境线”就要延伸到哪里。

智慧地球、网络云将全球连为一体，网络空间的对抗将是全球性、高速性、大范围的对抗，网络空间的博弈以网络为中心，以信息为主导。防的是基础网络、信息数据、心理认知和社会领域不受侵犯；打的是基于“芯片”直接瘫痪敌人战争基础和战争潜力的“比特战”；拼的是智力而不是体力，是让对手失能，而不是流血。因此，中国必须立足形成全局性战略威慑能力和复杂网络电磁环境掌控能力，加强多领域、多类型、多层次的力量建设，构建优势互补、联合一体的全球化战略布局。

1.3 安全威胁与攻击类型

在网络这个不断更新换代的世界里，网络中的安全漏洞无处不在。即便旧的安全漏洞

补上了，新的安全漏洞又将不断涌现。网络攻击正是利用这些存在的漏洞和安全缺陷对系统和资源进行攻击。

目前，主要有 10 个方面的网络安全问题急需解决，分别叙述如下：

(1) 信息应用系统与网络的关系日益紧密，人们对网络的依赖性增强，因而网络安全的影响范围日益扩大，建立可信的网络信息环境已成为一个迫切的需求。

(2) 网络系统中安全漏洞日益增多，不仅技术上有漏洞，管理上也有漏洞。

(3) 恶意代码危害性高。恶意代码通过网络途径广泛扩散，其影响越来越大。

(4) 网络攻击技术日趋复杂，而攻击操作容易完成，攻击工具广为流行。

(5) 网络安全建设缺乏规范操作，常常采取“亡羊补牢”的方式进行维护，导致信息安全共享难度递增，并留下安全隐患。

(6) 网络系统有着种类繁多的安全认证方式，一方面使得用户应用时不方便，另一方面也增加了安全管理工作的难度。

(7) 国内信息化技术严重依赖国外，从硬件到软件都不同程度地受制于人。

(8) 网络系统中软、硬件产品的单一性易导致大规模网络安全事件的发生，特别是网络蠕虫安全事件的发生。

(9) 网络安全建设涉及人员众多，安全性和易用性特别难以平衡。

(10) 网络安全管理问题依然是一个难题，主要包括：

· 用户信息安全防范意识不强。例如，选取弱口令，使得攻击者从远程即可直接控制主机。

· 网络服务配置不当，开放了过多的网络服务。例如，网络边界没有过滤掉恶意数据包或切断网络连接，允许外部网络的主机直接 ping 内部网主机，允许建立空连接。

· 安装有漏洞的软件包。

· 选取缺省配置。例如，网络设备的口令直接用厂家的缺省配置。

· 网络系统中软件不打补丁或补丁不全。

· 网络安全敏感信息泄露。例如 DNS 服务信息泄露。

· 网络安全防范缺乏体系。

· 网络信息资产不明，缺乏分类、分级处理。

· 网络安全管理信息单一，缺乏统一分析与管理平台。

· 重技术，轻管理。例如，没有明确的安全管理策略、安全组织及安全规范。

网络安全问题的存在，造成了网络攻击技术的泛滥。目前，对计算机用户来说，最大的安全威胁主要是黑客技术和木马技术。

1.3.1　黑客与黑客技术

1. 黑客和黑客类型

提起黑客，总是那么神秘莫测。在人们眼中，黑客是一群聪明绝顶、精力旺盛的年轻人，一门心思地破译各种密码，以便偷偷地、未经允许地打入政府、企业或他人的计算机系统，窥视他人的隐私。那么，什么是黑客呢？黑客(hacker)，源于英语动词 hack，意为“劈，砍”，引申为“干了一件非常漂亮的工作”。在早期麻省理工学院的校园俚语中，“黑客”则有“恶作剧”之意，尤指手法巧妙、技术高明的恶作剧。在日本《新黑客词典》中，对黑