HZ BOOKS
华章教育

高等院校信息安全专业规划教材

信息安全导论

Introduction to Information Security

何泾沙 主编

机械工业出版社
China Machine Press

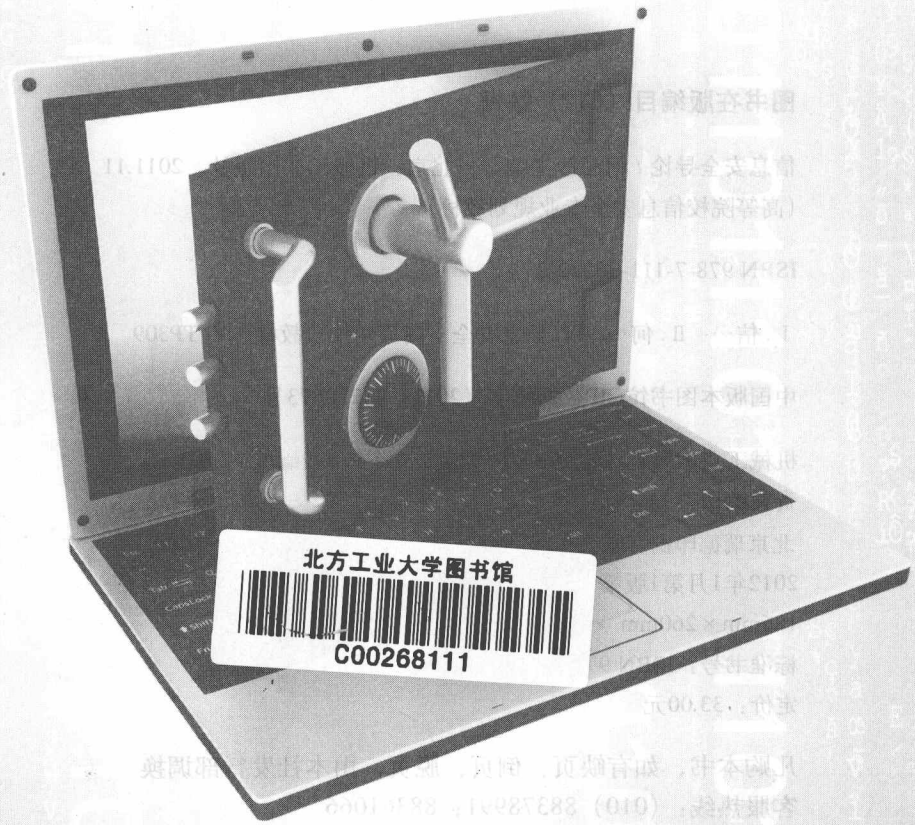
TP3-0
20
TP309/204
2012

息安全专业规划教材

信息安全导论

Introduction to Information Security

何泾沙 主编
何泾沙 韦潜 等编著



北方工业大学图书馆
C00268111

机械工业出版社
China Machine Press

本书作为一本信息安全方面的导论书籍，结合信息安全领域的前沿研究，借鉴和引用国内外的相关文献资料，较全面、系统地介绍了信息安全的基本概论和知识。本书介绍了信息安全所涉及的基本概念、所依赖的模型和理论基础以及所使用的信息保护方法，从数据加密保护及密钥管理、数字签名、身份识别及认证、访问控制、信息流安全分析及安全保障方法等方面全面介绍了信息安全的相关技术和手段，最后以网络安全为主线介绍了信息安全在网络环境中所面临的挑战和应对措施以及当前信息安全方法和技术的研究和发展现状。通过阅读本书，读者能够对计算机系统和网络环境中的信息安全问题和基本解决思路及方法有一个初步的、较全面的理解和掌握，为读者今后在信息安全领域进行深入研究和进一步学习打下良好的基础。

本书可作为高等院校信息安全、计算机科学与技术、软件工程及相关信息类专业“信息安全概论”或“信息安全导论”课程的教材，同时也适合希望了解信息安全领域中基本知识的其他读者阅读。

封底无防伪标均为盗版
版权所有，侵权必究
本书法律顾问　北京市展达律师事务所

图书在版编目（CIP）数据

信息安全导论 / 何泾沙主编. —北京：机械工业出版社，2011.11
（高等院校信息安全专业规划教材）

ISBN 978-7-111-36272-2

Ⅰ.信… Ⅱ.何… Ⅲ.信息安全－高等学校－教材 Ⅳ.TP309

中国版本图书馆CIP数据核字（2011）第220673号

机械工业出版社（北京市西城区百万庄大街22号 邮政编码 100037）
责任编辑：刘立卿
北京瑞德印刷有限公司印刷
2012年1月第1版第1次印刷
185mm×260mm · 15印张
标准书号：ISBN 978-7-111-36272-2
定价：33.00元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换
客服热线：（010）88378991；88361066
购书热线：（010）68326294；88379649；68995259
投稿热线：（010）88379604
读者信箱：hzjsj@hzbook.com

编委会

■ 主任委员

卿斯汉（中科院软件所/北京大学）

■ 副主任委员（按姓氏笔画排列）

王清贤（解放军信息工程大学）
杨永川（中国人民公安大学）
罗　平（清华大学）
贾春福（南开大学）

■ 委　　员（按姓氏笔画排列）

李　涛（四川大学）
庄　毅（南京航空航天大学）
苏金树（国防科技大学）
钮心忻（北京邮电大学）
陶　然（北京理工大学）
温莉芳（机械工业出版社）
蔡皖东（西北工业大学）

丛书序

经过数年的筹划与努力，信息安全系列丛书终于和广大读者见面了。

众所周知，进入21世纪以来，信息化对社会发展的影响日益深刻。全球信息化正在引发当今世界的深刻变革，重塑世界政治、经济、社会、文化和军事发展的新格局。

人们在享受信息化所带来的便利的同时，也不得不面对各种信息安全问题。信息安全是信息化的关键，各种天灾（如地震、洪水、飓风）和“人祸”（如网络故障、黑客入侵、病毒等）都会影响信息化进程。因此，在发展信息化的同时要重视信息安全，要在安全中发展，在发展中确保安全。

目前，世界各国都将信息安全视为国家安全的重要组成部分。党的十六届四中全会在《中共中央关于加强党的执政能力建设的决定》中明确提出：“坚决防范和打击各种敌对势力的渗透、颠覆和分裂活动，有效防范和应对来自国际经济领域的各种风险，确保国家的政治安全、经济安全、文化安全和信息安全”。党中央把信息安全和政治安全、经济安全、文化安全并列，作为我们国家四大安全内容之一，可见信息安全之重要，绝不能掉以轻心。近年来，我国在信息安全保障方面的工作逐步加强，制定并实施了国家信息安全战略，建立了信息安全管理体制和工作机制。基础信息网络和重要信息系统的安全防护水平明显提高，互联网信息安全管理进一步加强。

信息安全问题的解决，既要依靠技术的发展，更要重视人的作用。随着科技的进步，信息安全的概念和内涵不断发生变化，今天我们所说的信息安全是一个涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等领域的交叉学科，各种保障信息安全的技术也不断推陈出新。我们应大力培养信息安全的专业人才，对从业人员进行技术、职业道德、法律等全方位的教育。同时，要普及信息安全教育，增强国民的信息安全意识，提高全民的信息化知识水平和防范意识。

面对社会对信息安全人才的迫切需求，国内已有几十所高校设立了信息安全专业，还有众多高校开设了信息安全相关的必修与选修课。为了有力地支持信息安全相关课程的教学，促进信息安全的科学研究，在机械工业出版社华章分社的精心策划与组织下，国内高校从事信息安全领域研究、教学的专家和教师共同编写了这套“高等院校信息安全专业规划教材”。这套丛书是各位作者多年教学、科研成果的结晶，其特点是理论与实践紧密结合、深入浅出、实例丰富，既包括基础知识，也反映最新科研成果与发展趋势。我深信，丛书的出版必将对信息安全知识的普及和推广、信息安全人才的培养、教学与科研产生积极影响并作出重要的贡献。

最后，作为本丛书的编委会主任，我对各位编委的努力工作、各位作者的辛勤劳动、机械工业出版社华章分社的大力支持表示衷心的感谢。

丛书编委会主任　卿斯汉

2009年6月

此为试读，需要完整PDF请访问：www.ertongbook.com

前言

随着互联网以其灵活的方式、丰富的信息资源及种类繁多的信息服务方式广泛进入人们的生活，依赖于网络的各种应用及服务迅速普及，全球范围内的信息资源共享程度变得越来越高。在错综复杂的网络及信息环境中，越来越多的信息被共享，被相互传递，信息安全的问题也变得越来越突出，并成为整个社会中网络应用不可回避的一个尖锐问题。在网络技术和应用日新月异的今天，对信息安全相关知识的学习和研究已经成为人们生活和工作中必不可少的重要组成部分。信息安全在成为众多高校为信息安全或相关信息类专业开设的一门专业基础课的同时，也越来越多地被众多其他读者所关注。

本书适合作为高等院校信息安全、计算机科学与技术、软件工程及相关信息类专业“信息安全概论”或“信息安全导论”课程的教材，同时也可作为其他读者获得信息安全领域中基本、普遍知识的读本。

全书首先对信息安全技术发展至今的最基本的概念和原理进行清晰的阐述，然后系统地介绍信息安全领域所涉及的技术和方法，目的是使学生对计算机系统和网络环境中信息安全的问题和基本解决思路及方法有一个初步的、较全面的理解和掌握，为今后学生在某些信息安全的专门领域进行深入研究和进一步学习打下良好基础。

本书作为一本信息安全方面的导论类书籍，撰写的主要思路为：首先介绍信息安全所涉及的基本概念、所依赖的数学模型和基础理论以及所使用的信息保护方法；在介绍了以上基本概念和理论的基础上，再从数据加密保护及密钥管理、数字签名、身份识别及认证、访问控制、信息流安全分析及安全保障方法等方面全面介绍信息安全的相关技术和手段；最后，以网络安全为主线介绍信息安全在网络环境中所面临的挑战、应对存在的安全问题的措施以及当前信息安全方法和技术的研究和发展现状。

本书主要包含以下五个方面的内容：

- 信息安全的基本概念，包括信息在计算机和网络系统中所面临的安全挑战及信息安全所关注的主要问题；
- 信息安全的基本模型和策略；
- 针对信息安全所关注的关键问题的解决方法和技术；
- 当前所面临的信息安全挑战以及基本解决方法和技术；
- 国际上信息安全领域的研究现状。

本书以作者丰富的国内外学习和工作经历以及长期在信息安全领域从事科学研究及教学取得的丰硕成果为基础编写而成，书中的关键内容不仅大量借鉴和引用国外的相关文献资料，也涉及国际上信息安全领域的最新研究成果，对于学生进一步深入学习或开展信息安全领域的研究能够起到很好的引导作用。

本书由北京工业大学教授何泾沙负责编写，各章内容主要基于何泾沙教授的“信息安全概论”国家级双语教学示范建设课程的教学内容和讲义。韦潜主要撰写了第3章，并协助对全书进行了统稿，张婷、朱娜斐、马书南、于虹、高枫、李晓会、张玉强、徐晶、彭淑芬、吴旭、张兴、郭燕杰、付皖青先后协助了部分章节的撰写。

限于我们的水平和经验，教材中的错误和缺憾在所难免，敬请广大同行和读者在使用本书时对发现的错误和问题能够及时指出。我们欢迎任何对于本书的批评和建设性意见，以便我们对本书修改时参考。

教学及阅读建议

教学内容	学习要点及教学要求	课时安排
第1章 绪论	• 了解信息安全的概念、现状及特点 • 掌握信息安全面临的威胁 • 熟悉信息安全策略和机制	2
第2章 信息安全模型与策略	• 掌握访问控制矩阵模型、保护状态及模型描述 • 了解安全策略概念、内涵及职能 • 掌握安全策略的类型及访问控制的类型 • 了解保密性策略的目标及Bell-LaPadula模型的拓展及其局限性 • 熟悉Bell-LaPadula模型 • 熟悉Biba完整性模型与策略 • 了解Lipner完整性模型及Clark-Wilson完整性模型 • 了解混合型模型的目标及Chinese Wall模型 • 掌握基于创建者的访问控制模型及基于角色的访问控制模型	6
第3章 密码学原理及 密钥管理	• 了解密码学发展简史、研究目标及密码体制安全性 • 熟悉密码分析 • 掌握基于共享密钥和公钥的加密方法及技术 • 掌握基于共享密钥和公钥系统的密钥管理方法及技术	4
第4章 数字签名	• 了解数字签名的概念、功能与性质及对数字签名的攻击 • 掌握数字签名体制、过程及分类 • 了解直接方式的数字签名技术 • 了解仲裁方式的一般实施方案 • 掌握基于传统密钥明文可见、不可见及公钥的仲裁方案 • 掌握RSA、Rabin、ElGamal及DSA数字签名技术 • 了解盲签名、不可否认签名及批量签名	4
第5章 认证及身份验证技术	• 了解身份及身份鉴别、认证 • 掌握口令、质询-应答协议身份验证技术 • 了解利用信物的身份认证、生物认证 • 熟悉Kerberos认证系统	2
第6章 访问控制技术及实现	• 了解访问控制和安全机制的设计原则 • 掌握访问控制矩阵与访问控制列表 • 掌握能力表的概念及基于能力表的自主访问控制 • 了解能力表的保护和权限的撤销、能力表和访问控制列表的比较 • 掌握锁与钥匙密码学实现及机密共享 • 熟悉基于环的访问控制方法和用于传播性的访问控制列表	6
第7章 信息流安全分析	• 了解信息流控制策略、模型与机制 • 了解基于编译器机制和执行机制的信息流检测及动态安全检查 • 理解信息流控制实例 • 掌握隐信道概念、分类及分析	4

（续）

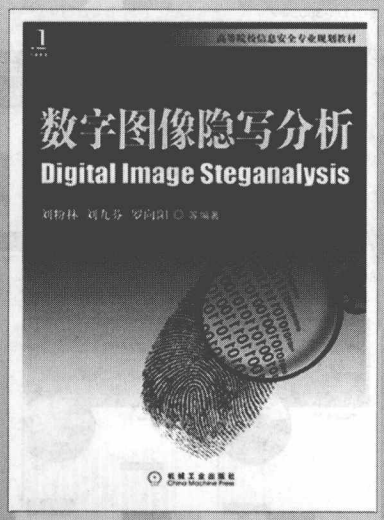
教学内容	学习要点及教学要求	课时安排
第8章 安全保障	• 理解安全保障和信任，建造安全可信的系统及形式化方法 • 了解审计、审计系统设计及审计机制 • 了解可信计算机标准评估、国际安全标准及我国安全标准	2
第9章 网络安全	• 了解恶意攻击概念及类型 • 理解网络安全漏洞概念和漏洞分类 • 掌握入侵检测原理、模型及体系结构 • 了解P2DR安全模型 • 了解网络安全常用技术、策略开发及网络组织 • 掌握可用性和泛洪攻击	4
	建议教学总学时	34

本书可作为计算机、通信及信息管理等专业教材，也是相关工程技术人员学习信息安全知识的入门读物。本书各章之间的独立性较强，每章分别讲述一个与信息安全相关的主题，读者完全可以根据自己的兴趣有选择地阅读本书。但是，信息安全模型和密码学原理是信息安全的基础，先阅读前面3章对于后续章节的理解将很有帮助。

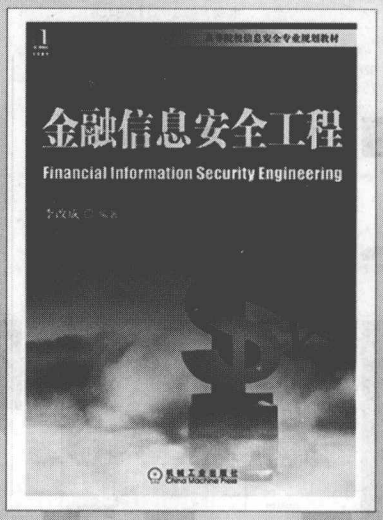
说明

- 本书可作为计算机、通信及信息管理等相关专业“信息安全”课程的教材，不同专业可根据不同的教学需求酌情做出调整。
- 非计算机类专业使用本书可适当降低教学要求。
- 本书理论授课学时为34学时，包含课堂讨论、练习等必要的教学环节。
- 建议授课时间比例为：基础理论部分70%，实践部分30%。

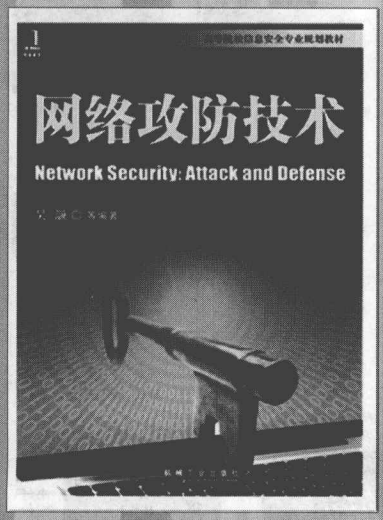
高等院校信息安全专业规划教材



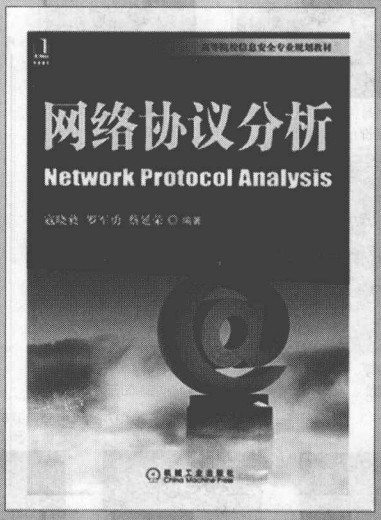
书号：978-7-111-30517-0
定价：29.00



书号：978-7-111-28262-4
定价：35.00



书号：978-7-111-27632-6
定价：29.00

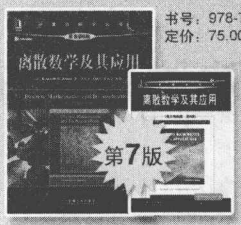


书号：978-7-111-26832-1
定价：33.00

机械工业出版社华章优秀教材推荐

书号：978-7-111-31871-2
定价：75.00元

书号：978-7-111-34236-6
定价：79.00元



书号：978-7-111-31329
定价：75.00元

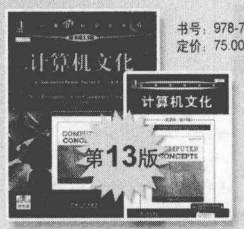
书号：978-7-111-30537-8
定价：39.00元

书号：978-7-111-33581-8
定价：79.00元

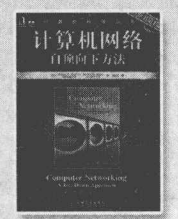
书号：978-7-111-34081-2
定价：75.00元

书号：978-7-111-35039-2
定价：99.00元

书号：978-7-111-30964-2
定价：39.00



书号：978-7-111-31799-9
定价：75.00元



书号：7-111-24687-9
定价：66.00元

书号：7-111-16505-7
定价：66.00元

书号：978-7-111-32878-0
定价：79.00元

书号：978-7-111-30426-5
定价：69.00元

书号：978-7-111-31280
定价：45.00元

书号：978-7-111-31204-8
定价：29.80元

书号：987-7-111-33368-5
定价：33.00元

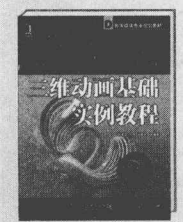
书号：978-7-111-28374-4
定价：38.00元

书号：978-7-111-18234-4
定价：33.00元

书号：978-7-111-26801-7
定价：35.00元

书号：978-7-111-23711-2
定价：33.00元

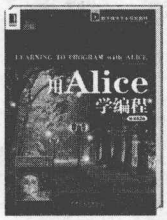
书号：978-7-111-20682-8
定价：45.00元



书号：978-7-111-30035-9
定价：36.00元

书号：978-7-111-27734-7
定价：39.00元

书号：978-7-111-31311-3
定价：33.00元



书号：978-7-111-27462-9
定价：39.00元

书号：978-7-111-27014-0
定价：35.00元

书号：978-7-111-31561-2
定价：35.00元

书号：978-7-111-27808-
定价：25.00元

书号：978-7-111-34971-6
定价：35.00元

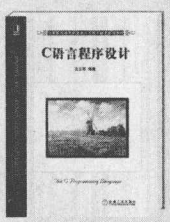
书号：978-7-111-28381-6
定价：36.00元

书号：978-7-111-28297-6
定价：33.00元

书号：7-111-22791-5
定价：26.00元

书号：978-7-111-26753
定价：36.00元

书号：7-111-26758-4
定价：32.00元



书号：978-7-111-34972-3
定价：29.00元

书号：978-7-111-29197-8
定价：29.80元

书号：978-7-111-30002-1
定价：36.00元

书号：978-7-111-26907-6
定价：29.00元

书号：978-7-111-32866-7
定价：29.00元

书号：978-7-111-31007-5
定价：33.00元

书号：978-7-111-33183-4
定价：30.00元

书号：978-7-111-24448-6
定价：30.00元

书号：978-7-111-33081-3
定价：28.00元

书号：978-7-111-33364-7
定价：26.00元

书号：978-7-111-30443-2
定价：29.80元

教师服务登记表

尊敬的老师：

您好！感谢您购买我们出版的_____教材。

机械工业出版社华章公司为了进一步加强与高校教师的联系与沟通，更好地为高校教师服务，特制此表，请您填妥后发回给我们，我们将定期向您寄送华章公司最新的图书出版信息！感谢合作！

个人资料（请用正楷完整填写）

<table>
<tr><td>教师姓名</td><td></td><td>□先生
□女士</td><td>出生年月</td><td></td><td>职务</td><td></td><td colspan="2">职称：□教授 □副教授
□讲师 □助教 □其他</td></tr>
<tr><td>学校</td><td colspan="2"></td><td>学院</td><td colspan="2"></td><td>系别</td><td colspan="2"></td></tr>
<tr><td rowspan="2">联系电话</td><td colspan="3" rowspan="2">办公：
宅电：
移动：</td><td>联系地址及邮编</td><td colspan="3"></td></tr>
<tr><td>E-mail</td><td colspan="3"></td></tr>
<tr><td>学历</td><td></td><td>毕业院校</td><td colspan="2"></td><td>国外进修及讲学经历</td><td colspan="3"></td></tr>
<tr><td>研究领域</td><td colspan="8"></td></tr>
<tr><td colspan="2">主讲课程</td><td colspan="3">现用教材名</td><td>作者及出版社</td><td>共同授课教师</td><td colspan="2">教材满意度</td></tr>
<tr><td colspan="2">课程：
□专 □本 □研
人数： 学期：□春□秋</td><td colspan="3"></td><td></td><td></td><td colspan="2">□满意 □一般
□不满意 □希望更换</td></tr>
<tr><td colspan="2">课程：
□专 □本 □研
人数： 学期：□春□秋</td><td colspan="3"></td><td></td><td></td><td colspan="2">□满意 □一般
□不满意 □希望更换</td></tr>
<tr><td colspan="9">样书申请</td></tr>
<tr><td colspan="2">已出版著作</td><td colspan="3"></td><td colspan="2">已出版译作</td><td colspan="2"></td></tr>
<tr><td colspan="3">是否愿意从事翻译/著作工作 □是 □否</td><td>方向</td><td colspan="5"></td></tr>
<tr><td>意见和建议</td><td colspan="8"></td></tr>
</table>

填妥后请选择以下任何一种方式将此表返回：（如方便请赐名片）

地 址：北京市西城区百万庄南街1号 华章公司营销中心 邮编：100037

电 话：(010) 68353079 88378995 传真：(010)68995260

E-mail:hzedu@hzbook.com marketing@hzbook.com 图书详情可登录http://www.hzbook.com网站查询

目录

Chapter

第1章 绪论

随着Internet在全世界日益普及，人类已经进入信息化社会。计算机与网络技术为信息的获取和利用提供了越来越先进的手段，同时也为好奇者和入侵者打开了方便之门，于是信息安全问题也越来越受关注。信息系统的安全性不仅关系到金融、商业、政府部门的正常运作，更关系到军事和国家的安全。研究保障信息系统安全的策略和机制，研究各种攻击方法及相应的防范措施，使信息系统安全运行，正是信息安全学科的研究目标。

1.1 信息安全概述

信息安全是指信息系统的硬件、软件和数据不因偶然和恶意的原因而遭到破坏、更改和泄露，保障系统连续正常运行和信息服务不中断。信息安全的本质和目的就是保护合法用户使用系统资源和访问系统中存储的信息的权利和利益，保护用户的隐私。

信息安全工作的基本原则就是在安全法律、法规、政策的支持与指导下，通过采用适当的安全技术与安全管理措施，防止信息财产被恶意地或偶然地未经合理授权地泄露、更改、破坏或使信息被非法的系统辨识、控制，避免攻击者利用信息系统的安全漏洞进行窃听、冒充、诈骗等等。

信息安全建立在保密性（confidentiality）、完整性（integrity）和可用性（availability）之上。对这三种信息安全基本特性的解释随着适用环境的不同而不同。在某种特定环境下，对这三种特性的解释是由个体需求、习惯和特定组织的法律法规决定的。

保密性是确保信息不泄露给未获得授权的实体或进程的特性。这里所指的信息涵盖范围非常广，不但包括国家秘密，而且还包括各种社会团体和企业组织的工作信息和商业机密以及涉及个人隐私的各类信息，如上网浏览习惯、购物习惯等等。

完整性是指信息不被未获得授权的实体或进程偶然或恶意地删除、修改、伪造、乱序、重放、插入等破坏的特性。完整性包括数据完整性（即信息的内容）和来源完整性（即信息的来源）。信息的来源可能会涉及来源的准确性和可信性，也涉及人们对此信息的信任度。完整性与保密性有较大的差别，保密性主要针对数据有没有遭受破坏或泄露，完整性则要同时保证数据的正确性和可信性。

可用性是指对信息或资源的期望使用能力，即获得授权的实体或进程在需要时可访问信息及系统资源和服务。无论何时，只要用户需要并获得授权，信息系统必须保证是可用的，系统不能拒绝给用户提供服务。攻击者通常采取占用资源的方式来阻碍系统执行授权者的正常请求。可用性还包括研究如何有效地避免因各种灾难（如战争、自然灾害等）引起系统资源和信息的不可用。

信息安全特性还包括其他的方面，如可监控性（accountability）、可审查性（auditability）、可认证性（authenticity）等。可监控性是对信息及信息系统实施安全监控的能力，使管理机构可以对造成安全问题的行为进行监视和审计。审计是对系统资源使用情况进行事后分析的有效手段，它通过对访问情况进行日志记录，并对日志进行统计分析，发现和追踪违反安全策略的事件。可审查性是指使用审计、监控、防抵赖等安全机制，使得使用者（包括合法用户、攻击者、破坏者、抵赖者）的行为有证可查，并能够对系统和网络中出现的安全问题提供调查依据和手段。可认证性的目的是保证信息使用者和信息提供者都是真实的声称者，防止假冒和重放。

1.2 信息安全面临的威胁

信息安全问题是一个系统问题，而不是信息本身的问题，因此要从信息系统的角度来分析组成系统的软硬件及处理过程中信息可能面临的风险。一般认为，系统风险是系统脆弱性或漏洞以及以系统为目标的威胁的总称。系统的脆弱性和漏洞是安全风险产生的原因，威胁或攻击则是安全风险引发的结果。从另一个角度看，风险的客体是系统的脆弱性和漏洞，风险的主体是针对客体的威胁或攻击。可见，当风险的因果或主客体在时空上一致时，风险就威胁或破坏了系统的安全，系统处于不稳定、不安全的状态中。

威胁是普遍存在的。对威胁的分类有多种方法，在此着重介绍两种。第一种方法是将信息安全面临的威胁分为两类：自然威胁和人为威胁。自然威胁不以人的意志为转移，主要来自于各种自然灾害、恶劣环境、电磁辐射、电磁干扰和设备老化等等。自然灾害（地震、火灾、洪水、海啸等）、物理损坏（硬盘损坏、设备使用寿命到期、外力破损等）、设备故障（停电断电、电磁干扰等）所造成的威胁，具有突发性、自然性、非针对性，但是这类威胁所造成的不安全因素对系统中信息的保密性影响却较小。例如，2009年8月，某省电信业务部门的通信设备被雷击中，造成惊人的损失；某铁路计算机系统遭受雷击，造成设备损失，铁路运输中断等。这类自然威胁对信息系统破坏严重，但数据信息并没有泄露给未授权的实体或进程，从一定程度上讲，对信息的保密性破坏很小。

人为威胁又包括无意威胁和有意威胁两种。无意威胁是指由于人为的偶然事故引起的，没有明显的恶意企图和目的，但却使信息资源受到破坏的威胁，如操作失误（未经允许使用、操

此为试读，需要完整PDF请访问：www.ertongbook.com