21世纪 高等学校信息安全专业规划教材

信息安全与技术

朱海波 主 编
刘湛清 副主编

清华大学出版社

21世纪高等学校信息安全专业规划教材

信息安全与技术

朱海波　主　编
刘湛清　副主编

清华大学出版社
北京

内 容 简 介

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。在每章后面都设有思考题，并在实践性、可操作性的章节安排有相应的实训环节。

本书可作为计算机、通信、电子工程、信息对抗、信息管理、信息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. —北京：清华大学出版社，2014
21世纪高等学校信息安全专业规划教材
ISBN 978-7-302-32606-9

Ⅰ. ①信… Ⅱ. ①朱… Ⅲ. ①信息安全－安全技术－高等学校－教材 Ⅳ. ①TP309

中国版本图书馆CIP数据核字(2013)第117670号

责任编辑：魏江江　王冰飞
封面设计：杨　兮
责任校对：梁　毅
责任印制：李红英

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：北京国马印刷厂
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　　张**：24.25　　**字　　数**：606千字
版　　次：2014年1月第1版　　**印　　次**：2014年1月第1次印刷
印　　数：1～2000
定　　价：39.50元

产品编号：050879-01

出版说明

由于网络应用越来越普及，信息化的社会已经呈现出越来越广阔的前景，可以肯定地说，在未来的社会中电子支付、电子银行、电子政务以及多方面的网络信息服务将深入到人类生活的方方面面。同时，随之面临的信息安全问题也日益突出，非法访问、信息窃取、甚至信息犯罪等恶意行为导致信息的严重不安全。信息安全问题已由原来的军事国防领域扩展到了整个社会，因此社会各界对信息安全人才有强烈的需求。

信息安全本科专业是2000年以来结合我国特色开设的新的本科专业，是计算机、通信、数学等领域的交叉学科，主要研究确保信息安全的科学和技术。自专业创办以来，各个高校在课程设置和教材研究上一直处于探索阶段。但各高校由于本身专业设置上来自于不同的学科，如计算机、通信和数学等，在课程设置上也没有统一的指导规范，在课程内容、深浅程度和课程衔接上，存在模糊不清、内容重叠、知识覆盖不全面等现象。因此，根据信息安全类专业知识体系所覆盖的知识点，系统地研究目前信息安全专业教学所涉及的核心技术的原理、实践及其应用，合理规划信息安全专业的核心课程，在此基础上提出适合我国信息安全专业教学和人才培养的核心课程的内容框架和知识体系，并在此基础上设计新的教学模式和教学方法，对进一步提高国内信息安全专业的教学水平和质量具有重要的意义。

为了进一步提高国内信息安全专业课程的教学水平和质量，培养适应社会经济发展需要的、兼具研究能力和工程能力的高质量专业技术人才。在教育部相关教学指导委员会专家的指导和建议下，清华大学出版社与国内多所重点大学共同对我国信息安全人才培养的课程框架和知识体系，以及实践教学内容进行了深入的研究，并在该基础上形成了“信息安全人才需求与专业知识体系、课程体系的研究”等研究报告。

本系列教材是在课程体系的研究基础上总结、完善而成，力求充分体现科学性、先进性、工程性，突出专业核心课程的教材，兼顾具有专业教学特点的相关基础课程教材，探索具有发展潜力的选修课程教材，满足高校多层次教学的需要。

本系列教材在规划过程中体现了如下一些基本组织原则和特点。

(1) 反映信息安全学科的发展和专业教育的改革，适应社会对信息安全人才的培养需求，教材内容坚持基本理论的扎实和清晰，反映基本理论和原理的综合应用，在其基础上强调工程实践环节，并及时反映教学体系的调整和教学内容的更新。

(2) 反映教学需要，促进教学发展。教材要适应多样化的教学需要，正确把握教学内容和课程体系的改革方向，在选择教材内容和编写体系时注意体现素质教育、创新能

力与实践能力的培养，为学生知识、能力、素质协调发展创造条件。

（3）实施精品战略，突出重点。规划教材建设把重点放在专业核心（基础）课程的教材建设上；特别注意选择并安排一部分原来基础比较好的优秀教材或讲义修订再版，逐步形成精品教材；提倡并鼓励编写体现工程型和应用型的专业教学内容和课程体系改革成果的教材。

（4）支持一纲多本，合理配套。专业核心课和相关基础课的教材要配套，同一门课程可以有多本具有各自内容特点的教材。处理好教材统一性与多样化，基本教材与辅助教材、教学参考书，文字教材与软件教材的关系，实现教材系列资源的配套。

（5）依靠专家，择优落实。在制定教材规划时依靠各课程专家在调查研究本课程教材建设现状的基础上提出规划选题。在落实主编人选时，要引入竞争机制，通过申报、评审确定主编。书稿完成后认真实行审稿程序，确保出书质量。

繁荣教材出版事业，提高教材质量的关键是教师。建立一支高水平的、以老带新的教材编写队伍才能保证教材的编写质量，希望有志于教材建设的教师能够加入到我们的编写队伍中来。

21 世纪高等学校信息安全专业规划教材

联系人：魏江江 weijj@tup.tsinghua.edu.cn

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 …… 1
1.1　信息安全的基本概念和需求 …… 1
1.1.1　信息安全的含义 …… 1
1.1.2　信息安全的需求 …… 2
1.1.3　研究信息安全的必要性 …… 2
1.2　信息安全环境及现状 …… 3
1.2.1　信息安全的威胁 …… 3
1.2.2　信息安全的目标 …… 5
1.2.3　网络安全技术发展的趋势 …… 6
1.3　网络不安全的原因 …… 7
1.3.1　系统漏洞 …… 7
1.3.2　协议的开放性 …… 7
1.3.3　人为因素 …… 7
1.4　信息安全体系结构 …… 8
1.4.1　OSI 安全体系结构 …… 8
1.4.2　TCP/IP 安全体系结构 …… 10
1.4.3　信息安全保障体系 …… 11
1.4.4　网络信息安全系统设计原则 …… 12
实训 1　虚拟机的配置使用 …… 14
本章小结 …… 32
思考题 …… 33
第 2 章　物理安全体系 …… 34
2.1　环境安全 …… 34
2.1.1　机房安全设计 …… 34
2.1.2　机房环境安全措施 …… 36
2.2　设备安全 …… 36
2.2.1　硬件设备的维护和管理 …… 37
2.2.2　硬件防辐射技术 …… 37
2.2.3　通信线路安全技术 …… 38

2.3 媒体安全 …… 39
2.3.1 数据备份 …… 39
2.3.2 数据备份的常用方法 …… 41
2.3.3 磁盘阵列技术简介 …… 43
本章小结 …… 45
思考题 …… 46
第3章 信息保密技术 …… 47
3.1 密码学的发展历程 …… 47
3.2 密码学中的基本术语 …… 49
3.3 古典密码体制 …… 51
3.3.1 替代密码 …… 51
3.3.2 置换密码 …… 56
3.4 对称密码体制 …… 56
3.4.1 序列密码 …… 57
3.4.2 分组密码 …… 61
3.4.3 数据加密标准 …… 62
3.5 非对称密码体制 …… 70
3.5.1 RSA 密码算法 …… 71
3.5.2 Diffie-Hellman 密钥交换算法 …… 72
3.5.3 EIGamal 加密算法 …… 73
3.6 密码学的应用 …… 73
3.6.1 密码应用模式 …… 73
3.6.2 加密方式 …… 76
实训2 密码学实验 …… 76
实训3 PGP 加密软件的使用 …… 80
本章小结 …… 84
思考题 …… 84
第4章 信息隐藏技术 …… 86
4.1 信息隐藏技术的发展历史 …… 86
4.1.1 传统的信息隐藏技术 …… 86
4.1.2 数字信息隐藏技术的发展 …… 87
4.2 信息隐藏技术的概念、分类及特性 …… 88
4.2.1 信息隐藏技术的概念 …… 88
4.2.2 信息隐藏技术的分类 …… 90
4.2.3 信息隐藏技术的特性 …… 91
4.3 信息隐藏技术的算法 …… 92
4.4 数字水印技术 …… 95
4.4.1 数字水印的基本原理 …… 96
4.4.2 数字水印算法 …… 97

4.5　隐通道技术 …… 98
4.5.1　隐通道的概念 …… 98
4.5.2　隐通道的分类 …… 98
4.5.3　隐通道分析方法 …… 100
4.6　匿名通信技术 …… 102
4.6.1　匿名通信的概念 …… 102
4.6.2　匿名通信技术的分类 …… 102
4.6.3　重路由匿名通信技术 …… 104
4.6.4　广播式和组播式路由匿名通信系统 …… 104
实训4　用易秀软件实现信息隐藏 …… 105
本章小结 …… 111
思考题 …… 112
第5章　网络攻击技术 …… 113
5.1　网络攻击概述 …… 113
5.1.1　网络攻击的目标 …… 113
5.1.2　网络攻击的手段 …… 113
5.1.3　网络攻击的层次 …… 113
5.1.4　网络攻击的分类 …… 114
5.1.5　网络攻击的一般模型 …… 115
5.2　信息收集技术 …… 115
5.2.1　网络踩点 …… 116
5.2.2　网络扫描 …… 119
5.2.3　网络监听 …… 122
5.3　网络入侵 …… 123
5.3.1　社会工程学攻击 …… 123
5.3.2　口令攻击 …… 124
5.3.3　漏洞攻击 …… 131
5.3.4　欺骗攻击 …… 135
5.3.5　拒绝服务攻击 …… 137
5.4　网络后门与网络隐身技术 …… 140
5.4.1　网络后门 …… 141
5.4.2　设置代理跳板 …… 141
5.4.3　清除日志 …… 142
实训5　信息收集与漏洞扫描 …… 143
本章小结 …… 150
思考题 …… 151
第6章　入侵检测技术 …… 152
6.1　入侵检测的概念 …… 152
6.1.1　入侵检测系统的功能及工作过程 …… 152

6.1.2 入侵检测技术的分类 …… 153
6.1.3 入侵检测系统的性能指标 …… 155
6.2 网络入侵检测系统产品 …… 156
6.2.1 入侵检测系统简介 …… 156
6.2.2 Snort 入侵检测系统 …… 156
6.3 漏洞检测技术和系统漏洞检测工具 …… 165
6.3.1 入侵攻击可利用的系统漏洞类型 …… 165
6.3.2 漏洞检测技术的分类 …… 166
6.3.3 系统漏洞检测的方法 …… 167
6.3.4 常见的系统漏洞及防范 …… 168
6.3.5 系统漏洞检测工具 …… 172
实训 6 使用 Snort 进行入侵检测 …… 173
本章小结 …… 173
思考题 …… 173
第 7 章 黑客攻防剖析 …… 175
7.1 概述 …… 175
7.1.1 黑客与骇客 …… 175
7.1.2 黑客的分类及目的 …… 176
7.2 黑客攻击的分类 …… 177
7.3 黑客攻击的步骤 …… 178
7.4 黑客工具软件 …… 179
7.4.1 黑客工具软件的分类 …… 179
7.4.2 黑客工具软件介绍 …… 181
7.5 黑客攻击防范 …… 183
7.5.1 网络访问控制技术 …… 183
7.5.2 防火墙技术 …… 184
7.5.3 数据加密技术 …… 184
7.5.4 入侵检测技术 …… 184
7.5.5 安全审计 …… 185
7.5.6 网络安全管理 …… 185
7.5.7 发现黑客入侵后的对策 …… 185
实训 7 IPC$ 攻击及防御 …… 186
本章小结 …… 191
思考题 …… 192
第 8 章 网络防御技术 …… 193
8.1 网络安全协议 …… 193
8.1.1 网络体系结构 …… 193
8.1.2 IPSec 协议 …… 194
8.1.3 SSL/TLS 协议 …… 199

8.2 防火墙技术 …… 203
8.2.1 防火墙的概念 …… 203
8.2.2 防火墙的分类 …… 204
8.2.3 防火墙的不同形态 …… 205
8.2.4 防火墙设备的性能指标 …… 206
8.2.5 防火墙系统的结构 …… 207
8.2.6 创建防火墙系统的步骤 …… 211
8.3 VPN 技术 …… 213
8.3.1 VPN 的含义 …… 213
8.3.2 VPN 的分类 …… 214
8.3.3 VPN 关键技术 …… 219
8.3.4 VPN 的优点 …… 220
8.4 蜜罐主机与欺骗网络 …… 220
8.4.1 蜜罐主机 …… 220
8.4.2 欺骗网络 …… 222
实训 8 Windows 防火墙配置 …… 222
实训 9 Windows 平台上的 PPTP VPN 配置 …… 227
本章小结 …… 230
思考题 …… 231
第 9 章 无线网络安全与防御技术 …… 232
9.1 无线网络安全概述及无线网络设备 …… 232
9.1.1 无线网络安全概述 …… 232
9.1.2 无线网络设备 …… 233
9.2 无线局域网的标准 …… 235
9.2.1 IEEE 的 802.11 标准系列 …… 235
9.2.2 ETSI 的 HiperLAN2 …… 239
9.2.3 HomeRF …… 240
9.3 无线局域网安全协议 …… 241
9.3.1 WEP 协议 …… 241
9.3.2 IEEE 802.11i 安全标准 …… 244
9.3.3 WAPI 协议 …… 244
9.4 无线网络的主要信息安全技术 …… 246
9.4.1 服务集标识符 …… 246
9.4.2 IEEE 802.11 的认证机制 …… 246
9.4.3 无线网卡物理地址过滤 …… 248
9.4.4 数据加密 …… 248
9.5 无线网络的安全缺陷与解决方案 …… 249
9.5.1 无线网络的安全缺陷 …… 249
9.5.2 无线网络的安全防范措施 …… 250

实训 10 组建安全的无线网络——WPA-PSK …… 252
本章小结 …… 256
思考题 …… 257
第 10 章 应用层安全技术 …… 258
10.1 Web 安全技术 …… 258
10.1.1 Web 概述 …… 258
10.1.2 Web 安全目标 …… 259
10.1.3 Web 安全技术的分类 …… 260
10.2 电子邮件安全技术 …… 261
10.2.1 电子邮件系统的组成 …… 261
10.2.2 电子邮件安全的目标 …… 262
10.2.3 电子邮件安全技术的分类 …… 262
10.2.4 电子邮件安全标准 …… 263
10.3 身份认证技术 …… 264
10.3.1 身份认证的含义 …… 264
10.3.2 身份认证的方法 …… 264
10.4 公钥基础设施技术 …… 268
10.4.1 PKI 技术概述 …… 268
10.4.2 PKI 的组成 …… 269
10.4.3 数字证书 …… 270
10.5 电子商务安全技术 …… 273
10.5.1 电子商务安全问题 …… 273
10.5.2 电子商务安全需求 …… 275
10.5.3 电子商务安全协议 …… 276
实训 11 构建基于 Windows 2003 的 CA 系统 …… 281
本章小结 …… 293
思考题 …… 293
第 11 章 计算机病毒与防范技术 …… 294
11.1 计算机病毒概述 …… 294
11.1.1 计算机病毒的概念 …… 294
11.1.2 计算机病毒的特征 …… 295
11.1.3 计算机病毒的分类 …… 296
11.1.4 计算机病毒的破坏行为和作用机理 …… 301
11.2 计算机蠕虫病毒 …… 302
11.2.1 蠕虫病毒的原理与特征 …… 302
11.2.2 蠕虫病毒实例分析 …… 304
11.3 计算机病毒的检测与防范 …… 307
11.3.1 计算机病毒的检测 …… 307
11.3.2 计算机病毒的防范 …… 307

11.3.3　计算机病毒的清除 …… 309
11.3.4　网络病毒的防范措施 …… 310
11.4　软件防病毒技术 …… 311
11.4.1　计算机杀毒软件的运作机制 …… 311
11.4.2　流行杀毒软件介绍 …… 312
实训 12　计算机病毒与防范 …… 314
本章小结 …… 329
思考题 …… 329
第 12 章　操作系统安全技术 …… 330
12.1　操作系统安全基础 …… 330
12.2　Windows XP 系统安全配置 …… 331
12.2.1　策略管理 …… 331
12.2.2　文件的安全 …… 336
12.2.3　注册表设置 …… 338
12.2.4　日志审核 …… 340
12.2.5　系统服务 …… 342
12.2.6　其他安全设置 …… 350
实训 13　Windows XP 系统安全配置 …… 351
本章小结 …… 354
思考题 …… 354
第 13 章　信息安全解决方案 …… 355
13.1　信息安全体系结构现状 …… 355
13.2　网络安全需求 …… 356
13.3　网络安全产品 …… 357
13.4　某大型企业网络安全解决方案实例 …… 359
13.4.1　网络安全需求分析 …… 359
13.4.2　安全管理策略 …… 362
13.4.3　安全解决方案分析 …… 362
13.5　电子政务安全平台实施方案 …… 365
13.5.1　电子政务平台 …… 365
13.5.2　电子政务安全平台解决方案 …… 366
本章小结 …… 372
参考文献 …… 373

第1章　信息安全概述

信息安全在古代就已经受到了学者、军事家和政治家的重视。当前，随着社会信息化程度的提高，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活跃，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、通信以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　信息安全的基本概念和需求

1.1.1　信息安全的含义

虽然计算机用户最近几年才注意到信息安全术语，但是信息安全方面的问题却影响着人们生活的方方面面。信息安全涵盖的内容广泛，密码技术、消息认证、身份认证与数字签名、防火墙技术以及安全协议都是信息安全研究的方向。网络安全技术是信息安全技术的重要分支，已经形成了比较完备的理论体系，成为了信息安全问题的研究热点。然而，网络安全技术不能够涵盖信息安全技术的全部内容，作为信息安全的一般性讨论，有必要首先明确信息安全的含义：影响信息的正常存储、传输和使用，以及不良信息的散布问题属于信息安全问题。

据此，可以把信息安全问题分为以下3个层次。

(1) 信息自身安全性。这类问题涉及信息的可用性、可信性、完整性以及保密性。解决这些问题仅仅依靠技术(密码技术、信息隐藏技术和网络技术)支持是远远不够的，管理与策略的维护也是必不可少的。

(2) 信息系统安全性。信息从产生到运用要经历存储、传输和处理等过程，这些过程的载体构成了信息系统。信息系统包含的范围很广，计算机网络、程控机床、工业控制系统以及办公自动化系统都属于信息系统的范畴。在考虑信息系统安全性时，设计者往往将注意力集中在计算机网络方面，而对其他信息系统不够重视。例如，如果在设计时设计人员充分地考虑到信息系统的安全性，那么我国的鑫诺卫星就不会遭到非法的干扰。

(3) 某些信息的传播对社会造成的不良影响。不仅是Internet，其他信息系统(广播系统、通信系统等)也面临着同样严峻的问题。这些不良影响可以被认为是信息安全的反面问题，但对信息安全工作者来说，其正、反两方面都是不可忽视的。

这3个层次问题虽然都属于信息安全问题，但是它们研究的目的和内容各不相同，使用的技术手段也存在着较大的差异。

信息自身安全性和信息系统安全性属于技术问题的范畴。它们的联系非常密切，信息系统的损坏会直接地导致信息存储载体的失效，当然会影响信息自身的安全；在某些特殊的情况下，信息自身的问题也会波及信息系统的安全。消除信息传播对社会造成的不良影

响虽然需要技术的支持，但就其本身而言含有更多的政治和人文因素。世界各国都把某些信息传播对社会造成的不良影响看做不可忽视的重要问题，这反映了信息安全的特殊性。

1.1.2 信息安全的需求

对现代商业而言，信息、信息处理过程、信息系统和信息网络都是重要的资产。商业企业若想保持竞争优势、资金的流动性和良好的企业形象必须要确保信息的保密性、完整性与可用性。可是，许多商业组织的管理信息系统正面临着大量的安全威胁，诸如网络诈骗、间谍、人为破坏、水灾以及火灾等。计算机病毒、计算机入侵与拒绝服务攻击等手段导致的信息灾难层出不穷。信息服务的普及意味着作为信息载体的管理信息系统更容易成为黑客的攻击目标，公共网络和私人网络的互联及信息资源的共享增大了实现访问控制的难度。许多信息系统在设计之初并未充分考虑系统的安全性，因此仅靠技术手段无法确保信息系统的安全性，信息系统的安全性还依赖于管理制度和程序控制的支持。信息安全管理涉及的人员众多，如企业员工、供应商、顾客以及股东，此外还需要信息安全专家的建议。如果在信息系统设计之初，设计人员就充分地考虑系统的安全需求和程序控制，那么商业企业就能够降低开发成本，提高开发效率。

虽然商业信息需要采取必要的措施加以保护，但是在采取具体的安全措施以前，商业组织必须首先明确自身的安全需求。信息系统设计者通过需求分析来明确组织的安全需求。

一般来说，商业组织的信息安全需求来自以下 3 个方面。

(1) 法律法规与合同条约的要求。信息安全法律法规对商业组织提出了强制性的要求，商业组织应该学习这些法律法规，从这些法律法规中提炼出自身的信息安全需求。这里提及的法律法规涉及 3 个层次，即国家法律、行政法规、各部委和地方的规章及规范性文件。此外，商业组织还要考虑合作伙伴和商业客户对组织提出的具体信息安全要求，包括招标条件、合同约定和承诺等。

(2) 商业组织的原则、目标和规定。为了确保支持业务运作的信息处理活动的安全性，商业组织通常根据自身的信息安全方针、需要实现的安全目标和标准来确定商业组织的信息安全要求。

(3) 风险评估的结果。除了以上两方面信息安全需求之外，商业组织还可以通过风险评估的方式明确自身的安全需求。通过风险评估的方式，商业组织确定了信息资产的保护程度和控制方式。一般来说，通过综合考虑每项资产所面临的威胁、自身的弱点、威胁造成的潜在影响和发生的可能性等因素，商业组织能够分析并确定具体的安全需求。信息安全管理建立在信息风险评估的基础上。

1.1.3 研究信息安全的必要性

当前，企业信息管理系统往往采用开放性的系统平台，而信息系统的组成部分(计算机网络、操作系统和数据库系统等)又往往包含很多的漏洞，在开放性的系统平台下这些系统漏洞更容易成为黑客攻击的目标。另外，通过 Internet 普通网民可以轻易地获取各种黑客工具，这使得网络黑客发动针对网站服务器的攻击比以往更加容易，由此潜在的黑客群体不断地扩大。

安全漏洞不断地增加。例如，微软公司 2005 年为 IE 浏览器提供了 80 余个安全漏洞的

补丁；然而，还有 30 多个 IE 浏览器的安全漏洞没有提供补丁。这些安全漏洞就能够让恶意的代码进入到商业组织的计算机网络。

随着 Internet 的广泛普及，越来越多的恶意代码将自身伪装成共享软件和广告软件。某些特洛伊木马程序将自己伪装成图像文件，一旦网民下载了这些图像文件，恶意程序的编写者就可以肆无忌惮地入侵恶意程序所在的计算机。广告软件可以侵犯网民的隐私，这种软件通常是在网民下载其他软件工具时一同下载的。这种软件监视网民浏览过的每个网页并且根据其兴趣爱好设计一个图表，这样就能提供适合的广告。一方面由于 Internet 的开放性以及安全防范措施不足，另一方面各种攻击手段和工具不断涌现并且容易获得，同时商业组织网络面临的黑客攻击风险的发生概率与其业务性质有关，因此商业组织的应对措施必须是消除并在实际风险发生后要尽量减轻风险的破坏后果。

不管商业企业内部连接的是企业的核心数据库，还是仅仅承担企业内部电子邮件的传输服务，保证商业企业网络的信息安全都是极其重要的工作。如果一个商业企业使用广域网连接到 Internet 上进行商务活动时，每一分钟的掉线都将使商业企业蒙受巨大的经济损失。

计算机网络主要存在以下三类安全问题。

(1) 机房安全。机房是硬件设备运行的关键场所，一旦出现安全事故，如物理安全事故(水灾、火灾、盗贼等)、电气安全事故(断电、负载不均等)等情况，势必影响信息的安全。

(2) 病毒的入侵和黑客的攻击。随着计算机网络的普及，恶意病毒的发作可能给网络造成灾难性的后果。网络黑客以多种手段选择性地破坏信息的有效性和完整性，他们截获、窃取和破译网络信息，从中获取重要的商业机密。

(3) 因管理不健全而导致的安全漏洞。从广义上讲，网络安全不仅涉及技术问题也涉及管理问题。网络安全包括管理机构、法律、技术、经济等诸多方面，依靠网络安全技术作为实现工具。因此，应该设计综合的解决方案来解决网络安全问题。

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。一般来说，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，截收泛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