十一五

高等学校电子与通信类专业“十一五”规划教材

信息安全技术

赵泽茂　吕秋云　朱　芳　编著

西安电子科技大学出版社
http://www.xduph.com

高等学校电子与通信类专业“十一五”规划教材

信息安全技术

赵泽茂　吕秋云　朱芳　编著

西安电子科技大学出版社

2009

内 容 简 介

全书共分15章，内容包括信息安全概述、信息保密技术、信息隐藏技术、消息认证技术、密钥管理技术、数字签名技术、物理安全、操作系统安全、网络安全协议、应用层安全技术、网络攻击技术、网络防御技术、计算机病毒、信息安全法律与法规、信息安全解决方案等。

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。

★ 本书配有电子教案，需要者可登录出版社网站，免费下载。

图书在版编目(CIP)数据

信息安全技术/赵泽茂，吕秋云，朱芳编著.
—西安：西安电子科技大学出版社，2009.2
高等学校电子与通信类专业“十一五”规划教材
ISBN 978-7-5606-2195-1

Ⅰ.信… Ⅱ.①赵… ②吕… ③朱… Ⅲ.信息系统—安全技术—高等学校—教材
Ⅳ.TP309

中国版本图书馆CIP数据核字(2009)第012782号

策　　划　毛红兵
责任编辑　王　瑛　毛红兵
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　2009年2月第1版　2009年2月第1次印刷
开　　本　787毫米×1092毫米　1/16　印张22
字　　数　517千字
印　　数　1～4000册
定　　价　31.00元
ISBN 978-7-5606-2195-1/TN·0483
XDUP　2487001—1

西安电子科技大学出版社
高等学校电子与通信类专业“十一五”规划教材
编审专家委员会名单

主　任：杨　震（南京邮电大学校长、教授）

副主任：张德民（重庆邮电大学通信与信息工程学院副院长、教授）

秦会斌（杭州电子科技大学电子信息学院院长、教授）

通信工程组

组　长：张德民（兼）

成　员：（成员按姓氏笔画排列）

王　晖（深圳大学信息工程学院副院长、教授）

巨永锋（长安大学信息工程学院副院长、教授）

成际镇（南京邮电大学通信与信息工程学院副院长、副教授）

刘顺兰（杭州电子科技大学通信工程学院副院长、教授）

李白萍（西安科技大学通信与信息工程学院副院长、教授）

张邦宁（解放军理工大学通信工程学院卫星系系主任、教授）

张瑞林（浙江理工大学信息电子学院院长、教授）

张常年（北方工业大学信息工程学院院长、教授）

范九伦（西安邮电学院信息与控制系系主任、教授）

姜　兴（桂林电子科技大学信息与通信学院副院长、教授）

姚远程（西南科技大学信息工程学院副院长、教授）

康　健（吉林大学通信工程学院副院长、教授）

葛利嘉（中国人民解放军重庆通信学院军事信息工程系系主任、教授）

电子信息工程组

组　长：秦会斌（兼）

成　员：（成员按姓氏笔画排列）

王　荣（解放军理工大学通信工程学院电信工程系系主任、教授）

朱宁一（解放军理工大学理学院基础电子学系系主任、工程师）

李国民（西安科技大学通信与信息工程学院院长、教授）

李邓化（北京信息工程学院信息与通信工程系系主任、教授）

吴　谨（武汉科技大学信息科学与工程学院电子系系主任、教授）

杨马英（浙江工业大学信息工程学院副院长、教授）

杨瑞霞（河北工业大学信息工程学院院长、教授）

张雪英（太原理工大学信息工程学院副院长、教授）

张　彤（吉林大学电子科学与工程学院副院长、教授）

张焕君（沈阳理工大学信息科学与工程学院副院长、副教授）

陈鹤鸣（南京邮电大学光电学院院长、教授）

周　杰（南京信息工程大学电子与信息工程学院副院长、教授）

欧阳征标（深圳大学电子科学与技术学院副院长、教授）

雷　加（桂林电子科技大学电子工程学院副院长、教授）

项目策划：毛红兵

策　　划：曹　昳　寇向宏　杨　英　郭　景

前　言

近年来，信息技术的飞速发展已经大大改变了人们的生活方式，人们对计算机网络的依赖程度日益增强。越来越多的信息和重要数据资源存储和传输于网络中，通过网络获取和交换信息的方式已成为当前主要的信息沟通方式。与此同时，网络安全事件频繁发生，严重地威胁着互联网的安全，极大地损害了网络使用者的利益，也为网络的健康发展带来了巨大的障碍。信息安全问题已成为关系国家安全、经济发展和社会稳定的关键性问题，也是通信和计算机领域探讨和研究的热点问题之一。因此，世界各国政府、学术界及产业界都高度重视信息安全问题。越来越多的高等院校先后开设了信息安全本科专业，且越来越多的本科专业开设了信息安全相关课程，可见，信息安全的研究队伍在逐渐壮大。

从学科研究的角度来看，信息安全是一个综合性强、交叉性广的学科领域，涉及数学、通信、计算机和电子等诸多学科的知识和研究成果。同时，信息安全技术又是一门实践性较强的课程，其许多技能是从实践中得来的，需要经受实践的检验。因此，系统地掌握信息安全理论基础和应用技能是需要长时期积累的，特别是网络安全防护技术，更不是一夜之间可以速成的。有人把信息安全形容成中医，是老来吃香，就说明了经验的重要性。

本书的目的是向本科生介绍信息安全的基本知识，提高计算机安全防护水平。因此，本书的定位是一本普及性的本科通用教材，理论方面要求学生理解信息安全基本原理而不要求理论的系统性和完整性，应用方面要求学生掌握信息安全维护的基本技能而不要求学生具备网络安全系统设计、软件开发的水平，但强调学生应能全面地了解信息安全的基本理论、方法和应用情况，学习内容力求涵盖面宽、适应范围广，符合学生实际水平。在学习本教材之前，读者应具备一定的数学、编程语言、操作系统和计算机网络等方面的基础知识。

本书内容涵盖信息安全领域的各个方面，主要包括密码学、信息隐藏、消息认证、密钥管理、数字签名、系统安全、协议安全、网络攻击、网络防御、计算机病毒、信息安全法律与法规及信息安全解决方案等。本书的体系结构相对灵活，各章内容相对独立，在教学中，教师可以根据不同专业、不同层次的教学大纲要求和学时数限制，选用不同的章节。我们认为适当取舍后仍能反映信息安全学科的特点，仍然可以看成是连贯的、相对完整的教材。附录包含部分实验内容，这样安排主要是考虑到本课程的实践性强的特点。建议选用本教材的学时数为 48～64 学时，其中包含 8 学时的实验。特意安排这 8 个学时的实验，意在引导读者一定要在学习本课程的过程中，加强实践环节的训练，因为信息安全技术的学习是离不开实践环节的。本书习题比较丰富，书末还给出了部分习题的参考答案。

本书由杭州电子科技大学通信工程学院“信息安全技术”课程教学团队集体编写，是作者多年来在教学、科研和工程实践方面经验的结晶。本书第 1、2、4、5、6 章由赵泽茂编写，第 7、9、10、11、12 章由吕秋云编写，第 8、13、14、15 章由朱芳编写，第 3 章由岳恒立和汪云路共同编写；实验 1、2、4 由赵泽茂、章晨曦、李爱宁和李孟婷共同编写，实验 3、6 由朱芳编写，实验 5 由吕秋云编写。本书由赵泽茂统稿。另外，李孟婷、何菲、张丽丽和

徐瑞等研究生参与了部分实验的验证和文字校验工作。在此，对上述所有人员表示感谢。书中部分内容选自同行专家、学者的教材和专著，有的甚至是他们多年来潜心教学实践的成果，在参考文献中我们都力求一一列出，如有疏忽和错漏，在此致以歉意，恳请给予提出，我们一并谨表感谢！特别要感谢的是西安电子科技大学出版社通信与电子编辑室主任毛红兵，她的支持是本书能顺利出版的关键。还要感谢周建钦教授、王小军等老师和同学们的支持，他们参与讨论和提出的每一个问题，都是本书力求克服并解决的知识点，广大同学们的认可更是我们写作本书的最大动力，特别献给同学们，献给广大读者。

由于信息安全是一门涉及面广、不断发展的交叉学科，加之作者水平有限，时间又仓促，书中难免存在疏漏和不妥之处，敬请同行和读者不吝批评指正。

作者的联系方式：zhaozm @hdu. edu. cn。

作　者

2008 年 11 月

目　录

第 1 章　信息安全概述 …… 1
1.1　信息安全现状 …… 1
1.1.1　信息安全的威胁 …… 1
1.1.2　信息安全涉及的问题 …… 2
1.1.3　信息安全的困惑 …… 4
1.2　信息安全需求 …… 4
1.2.1　信息安全的含义 …… 4
1.2.2　基本服务需求 …… 5
1.3　网络不安全的根本原因 …… 6
1.3.1　系统漏洞 …… 6
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 …… 9
1.4.2　TCP/IP 安全体系结构 …… 11
1.4.3　信息安全保障体系 …… 12
小结 …… 14
习题 …… 15
第 2 章　信息保密技术 …… 16
2.1　密码学的发展简史 …… 16
2.2　密码学中的基本术语 …… 19
2.3　古典密码 …… 20
2.4　对称密码体制 …… 23
2.4.1　序列密码 …… 23
2.4.2　分组密码 …… 27
2.4.3　数据加密标准——DES …… 28
2.5　非对称密码体制 …… 36
2.5.1　RSA 密码算法 …… 36
2.5.2　Diffie - Hellman 密钥交换算法 …… 38
2.5.3　ElGamal 加密算法 …… 39
2.6　密码学的应用 …… 39
2.6.1　密码应用模式 …… 39
2.6.2　加密方式 …… 42
2.6.3　PGP 软件的应用 …… 43
小结 …… 47
习题 …… 48
第 3 章　信息隐藏技术 …… 50
3.1　信息隐藏的发展历史 …… 50
3.1.1　传统的信息隐藏技术 …… 50

3.1.2 数字信息隐藏技术的发展 …… 52
3.2 信息隐藏的基本原理 …… 53
3.2.1 信息隐藏的概念 …… 54
3.2.2 信息隐藏的分类 …… 54
3.2.3 信息隐藏的特性 …… 55
3.3 信息隐藏的算法 …… 56
3.4 数字水印 …… 60
3.5 隐通道技术 …… 62
3.5.1 隐通道的概念 …… 62
3.5.2 隐通道的分类 …… 63
3.5.3 隐通道分析方法 …… 65
3.6 匿名通信技术 …… 66
3.6.1 匿名通信的概念 …… 66
3.6.2 匿名通信技术的分类 …… 67
3.6.3 重路由匿名通信系统 …… 68
3.6.4 广播式和组播式路由匿名通信 …… 69
小结 …… 69
习题 …… 70
第 4 章 消息认证技术 …… 71
4.1 Hash 函数 …… 71
4.1.1 一个简单的 Hash 函数 …… 72
4.1.2 完整性检验的一般方法 …… 72
4.2 消息认证码 …… 72
4.3 MD5 算法 …… 74
4.4 SHA-1 算法 …… 76
4.5 Hash 函数的攻击分析 …… 77
小结 …… 78
习题 …… 79
第 5 章 密钥管理技术 …… 80
5.1 密钥的分类 …… 80
5.2 密钥的生成与存储 …… 82
5.3 密钥的分配 …… 82
5.3.1 秘密密钥的分配 …… 82
5.3.2 公开密钥的分配 …… 83
5.4 密钥的更新与撤销 …… 84
5.5 密钥共享 …… 84
5.6 会议密钥分配 …… 86
5.7 密钥托管 …… 87
小结 …… 87
习题 …… 88
第 6 章 数字签名技术 …… 89
6.1 数字签名的原理 …… 89
6.2 RSA 数字签名和加密 …… 90
6.3 Schnorr 数字签名 …… 90

6.4 DSA 数字签名 …… 91
6.5 特殊的数字签名 …… 92
6.6 数字签名的应用 …… 93
小结 …… 94
习题 …… 95
第 7 章 物理安全 …… 96
7.1 环境安全 …… 96
7.1.1 机房安全设计 …… 96
7.1.2 机房环境安全措施 …… 98
7.2 设备安全 …… 99
7.2.1 访问控制技术 …… 99
7.2.2 防复制技术 …… 100
7.2.3 硬件防辐射技术 …… 101
7.2.4 通信线路安全技术 …… 102
7.3 媒体安全 …… 103
7.3.1 数据备份 …… 103
7.3.2 数据备份的常用方法 …… 105
7.3.3 磁盘阵列(RAID)技术简介 …… 108
小结 …… 109
习题 …… 110
第 8 章 操作系统安全 …… 111
8.1 系统漏洞 …… 111
8.2 Windows 系统安全模型 …… 113
8.3 Windows 注册表安全 …… 115
8.4 Windows 帐号与密码 …… 118
8.5 Windows 2000 安全策略 …… 120
8.6 Windows 系统的其他安全措施 …… 125
小结 …… 127
习题 …… 128
第 9 章 网络安全协议 …… 129
9.1 TCP/IP 协议簇 …… 129
9.1.1 TCP/IP 协议簇的基本组成 …… 129
9.1.2 TCP/IP 协议的封装 …… 130
9.1.3 TCP 连接的建立与关闭过程 …… 132
9.1.4 TCP/IP 协议簇的安全问题 …… 133
9.2 网络安全协议 …… 134
9.2.1 应用层的安全协议 …… 135
9.2.2 传输层的安全协议 …… 136
9.2.3 网络层的安全协议 …… 136
9.2.4 网络接口层的安全协议 …… 136
9.3 SSL 协议 …… 137
9.3.1 SSL 安全服务 …… 137
9.3.2 SSL 记录协议 …… 138
9.3.3 SSL 握手协议 …… 138

9.3.4 SSL 协议性能分析 …… 138
9.4 IPSec 协议 …… 139
9.4.1 IPSec 的安全体系结构 …… 139
9.4.2 IPSec 的工作模式 …… 140
9.4.3 认证头 …… 141
9.4.4 安全封装载荷 …… 142
9.4.5 安全关联 …… 143
9.4.6 因特网密钥交换协议 …… 144
小结 …… 145
习题 …… 146
第 10 章 应用层安全技术 …… 148
10.1 Web 安全技术 …… 148
10.1.1 Web 概述 …… 148
10.1.2 Web 安全目标 …… 150
10.1.3 Web 安全技术的分类 …… 150
10.2 电子邮件安全技术 …… 151
10.2.1 电子邮件系统的组成 …… 152
10.2.2 电子邮件安全目标 …… 152
10.2.3 电子邮件安全技术分类 …… 153
10.2.4 电子邮件安全标准——PGP …… 153
10.3 身份认证技术 …… 154
10.3.1 身份认证的含义 …… 154
10.3.2 身份认证的方法 …… 155
10.4 PKI 技术 …… 158
10.4.1 PKI 技术概述 …… 158
10.4.2 PKI 的组成 …… 158
10.4.3 数字证书 …… 159
小结 …… 163
习题 …… 164
第 11 章 网络攻击技术 …… 165
11.1 信息收集技术 …… 165
11.1.1 网络踩点 …… 165
11.1.2 网络扫描 …… 167
11.1.3 网络监听 …… 173
11.2 攻击实施技术 …… 177
11.2.1 社会工程学攻击 …… 177
11.2.2 口令攻击 …… 178
11.2.3 漏洞攻击 …… 181
11.2.4 欺骗攻击 …… 183
11.2.5 拒绝服务攻击 …… 185
11.3 隐身巩固技术 …… 188
11.3.1 网络隐藏技术 …… 188
11.3.2 设置代理跳板 …… 189
11.3.3 清除日志 …… 192

11.3.4 留后门 …… 194
小结 …… 201
习题 …… 202
第 12 章 网络防御技术 …… 203
12.1 防火墙技术 …… 203
12.1.1 防火墙的功能 …… 203
12.1.2 防火墙的分类 …… 204
12.1.3 防火墙系统的结构 …… 205
12.1.4 创建防火墙系统的步骤 …… 207
12.1.5 利用 WinRoute 创建防火墙过滤规则 …… 209
12.2 入侵检测技术 …… 213
12.2.1 入侵检测的任务 …… 213
12.2.2 入侵检测的分类 …… 213
12.2.3 入侵检测的步骤 …… 215
12.3 计算机取证技术 …… 217
12.3.1 计算机取证概述 …… 218
12.3.2 计算机取证的步骤 …… 219
12.3.3 计算机取证技术的内容 …… 223
12.4 蜜罐技术 …… 223
12.4.1 蜜罐的关键技术 …… 223
12.4.2 蜜罐的分类 …… 224
12.4.3 蜜罐在网络中的位置 …… 225
12.4.4 蜜网 …… 226
小结 …… 227
习题 …… 227
第 13 章 计算机病毒 …… 229
13.1 计算机病毒概述 …… 229
13.1.1 计算机病毒的发展历史 …… 229
13.1.2 计算机病毒的特征 …… 232
13.2 计算机病毒的基本结构 …… 233
13.3 计算机病毒的基本原理 …… 234
13.3.1 引导型病毒 …… 234
13.3.2 文件型病毒 …… 235
13.3.3 宏病毒 …… 236
13.3.4 脚本病毒 …… 238
13.3.5 蠕虫病毒 …… 239
13.4 反病毒技术 …… 241
13.5 典型病毒的特征及清除方法 …… 244
小结 …… 249
习题 …… 249
第 14 章 信息安全法律与法规 …… 251
14.1 计算机犯罪与公民隐私权 …… 251
14.1.1 计算机犯罪的概念 …… 251
14.1.2 计算机犯罪的特点 …… 252

14.1.3 公民隐私权 …… 254
14.2 信息安全立法 …… 254
14.2.1 信息安全立法的目标 …… 254
14.2.2 我国信息安全立法现状 …… 255
14.2.3 国际信息安全法律法规建设概况 …… 255
14.2.4 我国信息安全法律法规建设 …… 256
14.3 我国法律对计算机犯罪的规定 …… 257
14.3.1 刑法关于计算机犯罪的规定 …… 257
14.3.2 《关于维护互联网安全的决定》的部分规定 …… 258
14.3.3 《计算机信息系统安全保护条例》的主要内容 …… 259
14.3.4 《计算机病毒防治管理办法》的主要内容 …… 259
14.3.5 电子签名法 …… 259
14.4 我国信息安全法律法规中存在的问题 …… 261
14.5 案例分析 …… 262
小结 …… 265
习题 …… 266
第 15 章 信息安全解决方案 …… 267
15.1 信息安全体系结构现状 …… 267
15.2 网络安全需求 …… 268
15.3 网络安全产品 …… 270
15.4 某大型企业网络安全解决方案实例 …… 271
15.4.1 威胁分析 …… 272
15.4.2 制订策略 …… 273
15.4.3 应用部署方案 …… 276
15.5 电子政务安全平台实施方案 …… 277
15.5.1 电子政务平台 …… 277
15.5.2 物理隔离 …… 278
15.5.3 电子政务平台安全解决方案 …… 278
小结 …… 280
习题 …… 280
附录 实验 …… 281
实验 1 DES 加密和解密演示程序 …… 281
实验 2 RSA 算法应用 …… 295
实验 3 Windows 帐号克隆 …… 301
实验 4 Windows 2000 Server 证书配置 …… 304
实验 5 防火墙配置 …… 317
实验 6 Word 宏病毒 …… 319
部分习题参考答案 …… 327
参考文献 …… 339

第 1 章　信息安全概述

本章知识要点

- 信息安全现状
- 信息安全需求
- 网络不安全的根本原因
- 信息安全体系结构

信息安全起源于计算机安全。计算机安全就是确保计算机硬件的物理位置远离外部威胁，同时确保计算机软件正常、可靠地运行。随着网络技术的发展，计算机安全的范围扩大了，涉及数据的安全、对数据的随机访问限制和对未授权访问的控制等问题。由此，单纯的计算机安全开始向信息安全演进。互联网的出现，把上百万台计算机连接起来相互通信，互联网的商业化又使得这种通信更加复杂和频繁。技术的局限和利益的驱使影响着网络的发展，伴随互联网而滋生的信息安全问题层出不穷，逐渐演变成为一个社会问题，各国政府都非常重视，必须依靠法律、制度、教育、培训和技术等多种手段，才能从根本上保护信息安全。

1.1　信息安全现状

我们经常在媒体上看到有关信息安全事件的报道，比如某大型网站遭到黑客攻击、某种新型病毒出现、犯罪分子利用计算机网络诈骗钱财等。无疑，信息安全的现状十分令人焦虑和不安。

1.1.1　信息安全的威胁

现在谈论的信息安全，实际上是指面向网络的信息安全。Internet 最初是作为一个国防信息共享的工具来开发的，这种连接的目的在于数据共享，并没有把信息的安全看做一个重要因素来考虑。随着 Internet 的扩张和壮大，特别是电子商务的应用，系统的脆弱性和安全漏洞不能完全满足安全服务的需要，再加上商业信息时常被非法窃取、篡改、伪造或删除，因此，Internet 受到的威胁不可避免。

尽管目前学术界对信息安全威胁的分类没有统一的认识，但是，总体上可以分为人为因素和非人为因素两大类。

1. 人为因素

人为因素的威胁分为无意识的威胁和有意识的威胁两种。无意识的威胁是指因管理的

疏忽或使用者的操作失误而造成的信息泄露或破坏。有意识的威胁是指行为人主观上恶意攻击信息系统或获取他人秘密资料，客观上造成信息系统出现故障或运行速度减慢，甚至系统瘫痪的后果。有意识的威胁又分为内部攻击和外部攻击。外部攻击又可分为主动攻击和被动攻击。

2. 非人为因素

非人为因素的威胁包括自然灾害、系统故障和技术缺陷等。自然灾害包括地震、雷击、洪水等，可直接导致物理设备的损坏或零部件故障，这类威胁具有突发性、自然性和不可抗拒性等特点。自然灾害还包括环境的干扰，如温度过高或过低、电压异常波动、电磁辐射干扰等，这些情况都可能造成系统运行的异常或破坏系统。系统故障指因设备老化、零部件磨损而造成的威胁。技术缺陷指因受技术水平和能力的限制而造成的威胁，如操作系统漏洞、应用软件瑕疵等。这里的划分是针对信息系统的使用者而言的。

信息安全威胁的分类如图 1－1－1 所示。

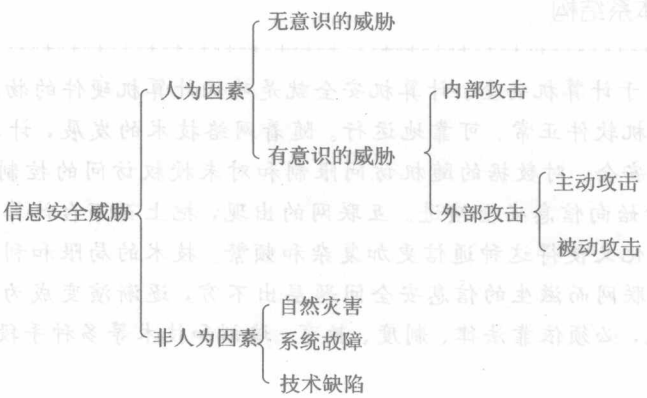

图 1－1－1 信息安全威胁的分类

1.1.2 信息安全涉及的问题

许多人一提到信息安全，自然会联想到密码、黑客、病毒等专业技术问题。实际上，网络环境下的信息安全不仅涉及到这些技术问题，而且还涉及到法律、政策和管理问题，技术问题虽然是最直接的保证信息安全的手段，但离开了法律、政策和管理的基础，纵有最先进的技术，信息安全也得不到保障。

1. 信息安全与政治

近十年来，电子政务发展迅速，政府网站的安全代表着一个国家或一个地区的形象。电子政务中政府信息安全的实质是由于计算机信息系统作为国家政务的载体和工具而引发的信息安全。电子政务中的政府信息安全是国家安全的重要内容，是保障国家信息安全所不可或缺的组成部分。由于互联网发展在地域上极不平衡，信息强国对于信息弱国已经形成了战略上的“信息位势差”。“信息疆域”不再是以传统的地缘、领土、领空、领海来划分的，而是以带有政治影响力的信息辐射空间来划分的。

2. 信息安全与经济

随着信息化程度的提高，国民经济和社会运行对信息资料和信息基础设施的依赖程度

越来越高。然而，我国计算机犯罪的增长速度远远超过了传统意义犯罪的增长速度，计算机犯罪从 1997 年的 20 多起，发展到 1998 年的 142 起，再到 1999 年的 908 起。1999 年 4 月 26 日，CIH 病毒大爆发，据统计，我国受到影响的计算机总量达到 36 万台，经济损失可能达到 12 亿元。2008 年公安部网监局调查了 7 起销售网络木马程序案件，每起案件的木马销售获利均超过 1000 万元。据公安机关的估算，7 起案件实施的网络盗窃均获利 20 亿元以上。

据有关方面统计，目前美国每年由于网络信息安全问题而遭受的经济损失超过了 170 亿美元，德国、英国也均在数十亿美元以上，日本、新加坡在这方面的问题也很严重。

3. 信息安全与文化

文化是一个国家民族精神和智慧的长期积淀和凝聚，是民族振兴发展的价值体现。在不同文化相互交流的过程中，一些国家为了达到经济和政治上的目的，不断推行“文化殖民”政策，形成了日益严重的“文化帝国主义”倾向。同时，互联网上散布着一些虚假信息、有害信息，包括网络色情、赌博等不健康的信息，对青少年的价值观、文化观造成了严重的负面影响。

4. 信息安全与法律

要使网络安全运行、数据安全传递，仅仅靠人们的良好愿望和自觉意识是不够的，需要必要的法律建设，以法制来强化信息安全。这主要涉及网络规划与建设的法律问题、网络管理与经营的法律问题、用户(自然人或法人)数据的法律保护、电子资金划转的法律认证、计算机犯罪与刑事立法、计算机证据的法律效力等。

法律是信息安全的防御底线，也是维护信息安全的最根本保障，任何人都必须遵守，带有强制性。不难设想，若计算机网络领域没有法制建设，那么网络的规划与建设必然是混乱的，网络将没有规范、协调的运营管理，数据将得不到有效的保护，电子资金的划转将产生法律上的纠纷，黑客将受不到任何惩罚。但是，有了相关法律的保障，并不等于安全问题就解决了，还需要相应的配套政策，才能使保障信息安全的措施具有可操作性。

5. 信息安全与管理

在网络威胁多样化的时代，单纯追求技术方面的防御措施是不能全面解决信息安全问题的，计算机网络管理制度是网络建设的重要方面。信息安全的管理包括三个层次的内容：组织建设、制度建设和人员意识。组织建设是指有关信息安全管理机构的建设，也就是说，要建立健全安全管理机构。信息安全的管理包括安全规划、风险管理、应急计划、安全教育培训、安全系统评估、安全认证等多方面的内容，只靠一个机构是无法解决这些问题的，因此应在各信息安全管理机构之间，依照法律法规的规定建立相关的安全管理制度，明确职责，责任到人，规范行为，保证安全。明确了各机构的职责后，还需要建立切实可行的规章制度，如对从业人员的管理，需要解决任期有限、职责隔离和最小权限的问题。有了组织机构和相应的制度，还需要加强人员意识的培养。通过进行网络信息安全意识的教育和培训，增强全民的网络安全意识和法制观念，以及对信息安全问题的重视，尤其是对主管计算机应用工作的领导和计算机系统管理员、操作员要通过多种渠道进行计算机及网络安全法律法规和安全技术知识培训与教育，使主管领导增强计算机安全意识，使计算机应用人员掌握计算机安全知识，知法、懂法、守法。

6. 信息安全与技术

目前，出现的许多信息安全问题，从某种程度上讲，可以说是由技术上的原因造成的，因此，对付攻击也最好采用技术手段。如：加密技术用来防止公共信道上的信息被窃取；完整性技术用来防止对传输或存储的信息进行篡改、伪造、删除或插入的攻击；认证技术用来防止攻击者假冒通信方发送假信息；数字签名技术用于防否认和抗抵赖。

1.1.3 信息安全的困惑

不论采取何种安全措施，一个计算机系统很难保证不会受到计算机病毒、黑客的攻击。人们不禁要问，什么样的计算机系统才算是安全的系统？

1. 严格意义下的安全性

无危为安，无损为全。安全就是指人和事物没有危险，不受威胁，完好无损。对人而言，安全就是使人的身心健康免受外界因素干扰和威胁的一种状态，也可看做是人和环境的一种协调平衡状态。一旦打破这种平衡，安全就不存在了。据此原则，现实生活中，安全实际上是一个不可能达到的目标，计算机网络也不例外。事实上，即使采取必要的网络保护措施，信息系统也会出现故障和威胁，从这个角度讲，计算机网络的绝对安全是不可能实现的。

2. 适当的安全性

适当的安全性，是计算机网络世界理性的选择，也是网络环境现存的状态。从经济利益的角度来讲，所谓适当的安全，是指安全性的选择应建立在所保护的资源和服务的收益预期大于为之付出的代价的基础之上，或者说，我们采取控制措施所降低的风险损失要大于付出的代价，如果代价大于损失就没有必要了。因此，面对这个有缺陷的网络，采取安全防护措施是必要的，但应权衡得失，不能矫枉过正。

1.2 信息安全需求

所谓信息安全需求，是指计算机网络给我们提供信息查询、网络服务时，保证服务对象的信息不受监听、窃取和篡改等威胁，以满足人们最基本的安全需要(如隐密性、可用性等)的特性。下面先介绍信息安全在不同层面的含义，然后从不同角度分析信息安全的需求。

1.2.1 信息安全的含义

1. 信息安全的相对概念

从用户(个人或企业)的角度来讲，他们希望：

(1) 在网络上传输的个人信息(如银行帐号和上网登录口令等)不被他人发现，这就是用户对网络上传输的信息具有保密性的要求；

(2) 在网络上传输的信息没有被他人篡改，这就是用户对网络上传输的信息具有完整性的要求；

(3) 在网络上发送的信息源是真实的，不是假冒的，这就是用户对通信各方的身份提

出的身份认证的要求；

(4) 信息发送者对发送过的信息或完成的某种操作是承认的，这就是用户对信息发送者提出的不可否认的要求。

从网络运行和管理者的角度来讲，他们希望本地信息网正常运行，正常提供服务，不受网外攻击，未出现计算机病毒、非法存取、拒绝服务、网络资源非法占用和非法控制等威胁。

从安全保密部门的角度来讲，他们希望对非法的、有害的、涉及国家安全或商业机密的信息进行过滤和防堵，避免通过网络泄露关于国家安全或商业机密的信息，避免对社会造成危害，对企业造成经济损失。

从社会教育和意识形态的角度来讲，我们应避免不健康内容的传播，正确引导积极向上的网络文化。

2. 信息安全的狭义解释

信息安全在不同的应用环境下有不同的解释。针对网络中的一个运行系统而言，信息安全就是指信息处理和传输的安全。它包括硬件系统的安全可靠运行、操作系统和应用软件的安全、数据库系统的安全、电磁信息泄露的防护等。狭义的信息安全，就是指信息内容的安全，包括信息的保密性、真实性和完整性。

3. 信息安全的广义解释

广义的信息安全是指网络系统的硬件、软件及其系统中的信息受到保护。它包括系统连续、可靠、正常地运行，网络服务不中断，系统中的信息不因偶然的或恶意的行为而遭到破坏、更改和泄露。

网络安全侧重于网络传输的安全，信息安全侧重于信息自身的安全，可见，这与其所保护的对象有关。

1.2.2　基本服务需求

1. 保密性

保密性是指网络中的信息不被非授权实体(包括用户和进程等)获取与使用。这些信息不仅包括国家机密，也包括企业和社会团体的商业机密和工作机密，还包括个人信息。人们在应用网络时很自然地要求网络能提供保密性服务，而被保密的信息既包括在网络中传输的信息，也包括存储在计算机系统中的信息。就像电话可以被窃听一样，网络传输信息也可以被窃听，解决的办法就是对传输信息进行加密处理。存储信息的机密性主要通过访问控制来实现，不同用户对不同数据拥有不同的权限。

2. 完整性

完整性是指数据未经授权不能进行改变的特性，即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。数据的完整性的目的是保证计算机系统上的数据和信息处于一种完整和未受损害的状态，这就是说数据不会因为有意或无意的事件而被改变或丢失。

除了数据本身不能被破坏外，数据的完整性还要求数据的来源具有正确性和可信性，也就是说需要首先验证数据是真实可信的，然后再验证数据是否被破坏。