世纪高等学校信息安全专业规划教材

计算机信息安全技术

（第2版）

◎ 付永钢 主编

清華大學出版社

21世纪高等学校信息安全专业规划教材

计算机信息安全技术

（第2版）

◎ 付永钢　主编

洪玉玲　曹煦晖　陈杰　刘年生　副主编

清华大学出版社

北京

内 容 简 介

本书对计算机信息安全体系的各个部分做了完整的介绍，主要内容包括计算机信息安全技术概述、密码技术、信息认证技术、计算机病毒、网络攻击与防范技术、防火墙技术、入侵检测技术、操作系统安全、数据备份与恢复技术、软件保护技术、虚拟专用网技术、电子商务安全、网络安全检测与评估。每章都有习题，附录提供了与部分章节相对应的实验。

本书可作为计算机和通信专业本科或专科学生的计算机信息安全技术课程教材，也可作为从事信息安全研究的工程技术人员的参考用书。

图书在版编目(CIP)数据

计算机信息安全技术/付永钢主编. —2 版. —北京：清华大学出版社，2017
(21 世纪高等学校信息安全专业规划教材)
ISBN 978-7-302-46846-2

Ⅰ. ①计… Ⅱ. ①付… Ⅲ. ①电子计算机－信息安全－安全技术 Ⅳ. ①TP309

中国版本图书馆 CIP 数据核字(2017)第 064053 号

责任编辑：魏江江　王冰飞
封面设计：刘　键
责任校对：白　蕾
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**：24.5　　**字　　数**：595 千字
版　　次：2012 年 3 月第 1 版　2017 年 9 月第 2 版　　**印　　次**：2017 年 9 月第1 次印刷
印　　数：11501～13500
定　　价：49.50 元

产品编号：069948-01

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们生活的方方面面。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来自不同的学科，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、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以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。处理好教材的统一性与多样化,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

第2版前言

随着全球信息化技术的快速发展，在信息技术的广泛应用中，安全问题正面临着前所未有的挑战，信息安全日渐成为国家的一个重点关注的研究领域，成为关系着国计民生的一个重要的应用学科。

目前因特网(Internet)已遍布世界240个国家和地区，每时每刻都为用户提供着各种类型的信息服务，除了最初的电子邮件、万维网外，还出现了越来越多的集视频、声音、数据于一体的服务。我们的社会已经是一个高度信息化的社会，计算机已经被应用到政治、军事、金融、商业、电信、教育等各行各业，人们在日常生活中对计算机的依赖程度越来越高，尤其是近年来国家实施的信息系统工程和信息基础设施建设，已经使计算机系统成为当今社会特征的一个重要组成部分。多年来，黑客对信息系统的攻击一直都没有停止过，其手段也越来越高明，从最初的猜测用户密码、利用计算机应用软件漏洞进行攻击，发展到现在通过操作系统的源代码分析操作系统漏洞，这无疑给计算机信息安全带来了更大的威胁。

本书内容由浅入深，介绍计算机信息安全技术所涉及的相关知识，阅读本书可以了解我国计算机信息系统的安全现状、网络安全的隐患和风险，以及其给计算机信息系统运行带来的危害、具体的安全防护措施和技术。

本书从实用和新颖的角度对内容进行了精心的挑选，具有以下特色。

(1) 实用、丰富、新颖的内容。编写基于一般普通高等院校计算机专业信息安全技术的应用人才培养的需要，以知识实用、丰富、新颖为原则，使学生初步掌握计算机信息安全使用技能，为今后进一步学习、研究信息安全技术打下坚实的基础。

本书在有限的篇幅中，尽可能减少概念和理论性的知识介绍，而更加注重解决实际问题，同时吸取目前已出版的信息安全技术类教材、论文的精髓，充分反映计算机信息安全领域的前沿技术和成果。

(2) 完整的信息安全体系。目前计算机信息安全研究的主要方向包括密码学、计算机网络安全、计算机病毒、信息隐藏、软件保护、数据备份与恢复等方面，本书力求融合信息安全研究的基础知识与核心内容，全面反映计算机信息安全体系。通过学习本书，既可以了解到信息安全的概貌，又可以迅速掌握信息安全的基本技能。

(3) 丰富的习题。为了加深学生对相关内容的理解，每章后面都附有难易程度不同的习题，以帮助读者更加深入和扎实地掌握相关知识。

本书第3、4、12章由陈杰编写，第9、10章由洪玉玲编写，第6、7、11章由曹煦晖编

写,第2章的第2.1～2.3节由刘年生编写。付永钢编写了其余章节,并对全书进行了修改和统稿。

在本书的编写过程中,得到了茅剑等老师的帮助,在此表示衷心的感谢。

为了配合本书的教学工作,作者还提供了配套的电子课件,请在清华大学出版社网站(www.tup.com.cn)下载,或者通过电子邮箱 yonggangfu@jmu.edu.cn 获取。本书主要内容的课堂授课需要50学时左右,也可根据教学对象和教学目的进行删减,建议再安排一定学时的课外实验。另外,本书所有截图来自相关软件,未做改动。

信息安全技术是一个不断发展和完善的研究领域,由于作者水平有限,书中错误和不当之处在所难免,敬请广大读者和专家批评指正。

作 者

2017年5月

目　录

第 1 章　计算机信息安全技术概述 …… 1
1.1　计算机信息安全的威胁因素 …… 1
1.2　信息安全的含义 …… 2
1.3　计算机信息安全的研究内容 …… 3
1.3.1　计算机外部安全 …… 3
1.3.2　计算机内部安全 …… 6
1.3.3　计算机网络安全 …… 6
1.4　信息安全模型 …… 7
1.4.1　通信安全模型 …… 7
1.4.2　信息访问安全模型 …… 8
1.4.3　动态安全模型 …… 8
1.4.4　APPDRR 模型 …… 9
1.5　OSI 信息安全体系 …… 10
1.5.1　OSI 的七层结构与 TCP/IP 模型 …… 10
1.5.2　OSI 的安全服务 …… 11
1.5.3　OSI 安全机制 …… 12
1.6　信息安全中的非技术因素 …… 14
1.6.1　人员、组织与管理 …… 14
1.6.2　法规与道德 …… 15
1.7　信息安全标准化知识 …… 15
1.7.1　技术标准的基本知识 …… 15
1.7.2　标准化组织 …… 16
1.7.3　信息安全相关标准 …… 17
习题 1 …… 18
第 2 章　密码技术 …… 19
2.1　密码学概述 …… 19
2.1.1　密码体制的模型 …… 19

2.1.2 密码体制的分类 …… 19
2.1.3 密码体制的攻击 …… 21
2.1.4 密码体制的评价 …… 23
2.2 传统密码体制 …… 24
2.2.1 置换密码 …… 24
2.2.2 代换密码 …… 25
2.2.3 传统密码的分析 …… 29
2.3 现代对称密码体制 …… 31
2.3.1 DES …… 32
2.3.2 AES …… 41
2.3.3 序列密码 …… 46
2.4 非对称密码体制 …… 48
2.4.1 RSA 非对称密码体制 …… 49
2.4.2 椭圆曲线非对称密码体制 …… 51
2.4.3 Diffie-Hellman 密钥交换 …… 54
2.5 密码学新进展 …… 55
2.5.1 可证明安全性 …… 55
2.5.2 基于身份的密码技术 …… 55
2.5.3 量子密码学 …… 56
习题 2 …… 57
第 3 章 信息认证技术 …… 59
3.1 概述 …… 59
3.2 哈希函数 …… 59
3.2.1 哈希函数概述 …… 60
3.2.2 MD5 …… 60
3.2.3 SHA-1 …… 64
3.3 消息认证技术 …… 67
3.3.1 概述 …… 68
3.3.2 消息认证方法 …… 68
3.4 数字签名 …… 72
3.4.1 数字签名概述 …… 72
3.4.2 数字签名的实现 …… 73
3.4.3 数字签名标准 …… 76
3.5 身份认证 …… 78
3.5.1 概述 …… 78
3.5.2 基于口令的身份认证 …… 80
3.5.3 基于对称密钥的身份认证 …… 82
3.5.4 基于公钥的身份认证 …… 84
习题 3 …… 86

第 4 章　计算机病毒 …… 88
4.1　概述 …… 88
4.1.1　定义 …… 88
4.1.2　计算机病毒的发展 …… 89
4.1.3　计算机病毒的危害 …… 90
4.2　计算机病毒的特征及分类 …… 91
4.2.1　计算机病毒的特征 …… 91
4.2.2　计算机病毒的分类 …… 92
4.3　常见的病毒类型 …… 94
4.3.1　引导型与文件型病毒 …… 94
4.3.2　网络蠕虫与计算机木马 …… 96
4.3.3　其他病毒介绍 …… 98
4.4　计算机病毒制作与反病毒技术 …… 101
4.4.1　计算机病毒的一般构成 …… 101
4.4.2　计算机病毒制作技术 …… 102
4.4.3　病毒的检测 …… 103
4.4.4　病毒的预防与清除 …… 104
习题 4 …… 105
第 5 章　网络攻击与防范技术 …… 107
5.1　网络攻击概述和分类 …… 107
5.1.1　网络安全漏洞 …… 107
5.1.2　网络攻击的基本概念 …… 108
5.1.3　网络攻击的步骤概览 …… 109
5.2　目标探测 …… 110
5.2.1　目标探测的内容 …… 110
5.2.2　目标探测的方法 …… 111
5.3　扫描的概念和原理 …… 114
5.3.1　主机扫描 …… 114
5.3.2　端口扫描 …… 115
5.3.3　漏洞扫描 …… 118
5.4　网络监听 …… 119
5.4.1　网络监听原理 …… 119
5.4.2　网络监听检测与防范 …… 120
5.5　缓冲区溢出攻击 …… 122
5.5.1　缓冲区溢出原理 …… 122
5.5.2　缓冲区溢出攻击方法 …… 123
5.5.3　防范缓冲区溢出 …… 124
5.6　注入式攻击 …… 125
5.7　拒绝服务攻击 …… 126

5.7.1 IP碎片攻击 …… 126
5.7.2 UDP洪泛 …… 129
5.7.3 SYN洪泛 …… 129
5.7.4 Smurf攻击 …… 130
5.7.5 分布式拒绝服务攻击 …… 130
5.8 欺骗攻击与防范 …… 131
5.8.1 IP欺骗攻击与防范 …… 132
5.8.2 ARP欺骗攻击与防范 …… 134
习题5 …… 136
第6章 防火墙技术 …… 139
6.1 防火墙概述 …… 139
6.1.1 防火墙的定义 …… 139
6.1.2 防火墙的特性 …… 140
6.1.3 防火墙的功能 …… 140
6.1.4 防火墙的局限性 …… 141
6.2 防火墙的分类 …… 142
6.2.1 防火墙的发展简史 …… 142
6.2.2 按防火墙软硬件形式分类 …… 143
6.2.3 按防火墙技术分类 …… 143
6.3 防火墙技术 …… 144
6.3.1 包过滤技术 …… 144
6.3.2 代理服务技术 …… 147
6.3.3 状态检测技术 …… 149
6.3.4 NAT技术 …… 151
6.4 防火墙的体系结构 …… 153
6.4.1 堡垒主机体系结构 …… 153
6.4.2 双宿主主机体系结构 …… 154
6.4.3 屏蔽主机体系结构 …… 155
6.4.4 屏蔽子网体系结构 …… 156
6.4.5 防火墙的结构组合策略 …… 159
6.5 防火墙的部署 …… 161
6.5.1 防火墙的设计原则 …… 161
6.5.2 防火墙的选购原则 …… 162
6.5.3 常见防火墙产品 …… 164
6.6 防火墙技术的发展趋势 …… 167
6.6.1 防火墙包过滤技术发展趋势 …… 167
6.6.2 防火墙的体系结构发展趋势 …… 167
6.6.3 防火墙的系统管理发展趋势 …… 168
6.6.4 分布式防火墙技术 …… 169

习题 6 …… 172
第 7 章　入侵检测技术 …… 174
7.1　入侵检测概述 …… 174
7.1.1　入侵检测技术的发展 …… 174
7.1.2　入侵检测的定义 …… 175
7.2　入侵检测系统的特点和分类 …… 176
7.2.1　入侵检测系统的特点 …… 176
7.2.2　入侵检测系统的基本结构 …… 176
7.2.3　入侵检测系统的分类 …… 177
7.3　入侵检测的技术模型 …… 178
7.3.1　基于异常的入侵检测 …… 179
7.3.2　基于误用的入侵检测 …… 180
7.4　分布式入侵检测 …… 182
7.4.1　分布式入侵检测的优势 …… 182
7.4.2　分布式入侵检测技术的实现 …… 183
7.5　入侵防护系统 …… 184
7.5.1　入侵防护系统的原理 …… 185
7.5.2　IPS 关键技术 …… 185
7.5.3　IPS 系统分类 …… 186
7.6　常用入侵检测系统介绍 …… 187
7.7　入侵检测技术存在的问题与发展趋势 …… 190
7.7.1　入侵检测系统目前存在的问题 …… 190
7.7.2　入侵检测系统的发展趋势 …… 191
习题 7 …… 192
第 8 章　操作系统安全 …… 194
8.1　操作系统安全概述 …… 195
8.1.1　操作系统安全准则 …… 195
8.1.2　操作系统安全防护的一般方法 …… 197
8.1.3　操作系统资源防护技术 …… 198
8.2　UNIX/Linux 系统安全 …… 199
8.2.1　Linux 系统概述 …… 199
8.2.2　UNIX/Linux 系统安全概述 …… 200
8.2.3　UNIX/Linux 的安全机制 …… 201
8.2.4　UNIX/Linux 安全配置 …… 205
8.3　Windows 系统安全 …… 208
8.3.1　Windows 系统的发展 …… 208
8.3.2　Windows 的特点 …… 210
8.3.3　Windows 7 安全基础 …… 210
8.3.4　Windows 7 系统安全机制 …… 212

8.3.5 Windows 7 安全措施 …… 215
习题 8 …… 218
第 9 章 数据备份与恢复技术 …… 220
9.1 数据备份概述 …… 220
9.1.1 数据备份及其相关概念 …… 221
9.1.2 备份的误区 …… 221
9.1.3 数据备份策略 …… 222
9.1.4 日常维护有关问题 …… 224
9.2 系统数据备份 …… 224
9.2.1 系统还原卡 …… 225
9.2.2 克隆大师 Ghost …… 225
9.2.3 其他备份方法 …… 226
9.3 用户数据备份 …… 227
9.3.1 Second Copy …… 227
9.3.2 File Genie 2000 …… 229
9.4 网络数据备份 …… 229
9.4.1 DAS-Based 结构 …… 230
9.4.2 LAN-Based 结构 …… 230
9.4.3 LAN-Free 备份方式 …… 231
9.4.4 Server-Free 备份方式 …… 232
9.5 数据恢复 …… 233
9.5.1 数据的恢复原理 …… 233
9.5.2 硬盘数据恢复 …… 236
习题 9 …… 246
第 10 章 软件保护技术 …… 248
10.1 软件保护技术概述 …… 248
10.2 静态分析技术 …… 248
10.2.1 静态分析技术的一般流程 …… 248
10.2.2 文件类型分析 …… 249
10.2.3 W32Dasm 简介 …… 250
10.2.4 可执行文件代码编辑工具 …… 253
10.3 动态分析技术 …… 255
10.4 常用软件保护技术 …… 258
10.4.1 序列号保护机制 …… 258
10.4.2 警告窗口 …… 260
10.4.3 功能限制的程序 …… 260
10.4.4 时间限制 …… 261
10.4.5 注册保护 …… 261
10.5 软件加壳与脱壳 …… 262

10.5.1 壳的介绍 …… 262
10.5.2 软件加壳工具简介 …… 262
10.5.3 软件脱壳 …… 267
10.6 设计软件的一般性建议 …… 268
习题 10 …… 270
第 11 章 虚拟专用网技术 …… 271
11.1 VPN 的基本概念 …… 271
11.1.1 VPN 的工作原理 …… 271
11.1.2 VPN 的分类 …… 272
11.1.3 VPN 的特点与功能 …… 274
11.1.4 VPN 安全技术 …… 276
11.2 VPN 实现技术 …… 277
11.2.1 第二层隧道协议 …… 277
11.2.2 第三层隧道协议 …… 279
11.2.3 多协议标签交换 …… 283
11.2.4 第四层隧道协议 …… 284
11.3 VPN 的应用方案 …… 284
11.3.1 L2TP 应用方案 …… 284
11.3.2 IPSec 应用方案 …… 285
11.3.3 SSL VPN 应用方案 …… 287
习题 11 …… 288
第 12 章 电子商务安全 …… 290
12.1 电子商务安全概述 …… 290
12.2 SSL 协议 …… 291
12.2.1 SSL 概述 …… 291
12.2.2 SSL 协议规范 …… 292
12.2.3 SSL 安全性 …… 299
12.3 SET 协议 …… 300
12.3.1 SET 概述 …… 300
12.3.2 SET 的安全技术 …… 302
12.3.3 SET 的工作原理 …… 305
12.3.4 SET 的优缺点 …… 310
12.4 SSL 与 SET 的比较 …… 311
习题 12 …… 311
第 13 章 网络安全检测与评估 …… 313
13.1 网络安全评估标准 …… 313
13.1.1 网络安全评估标准的发展历程 …… 313
13.1.2 TCSEC、ITSEC 和 CC 的基本构成 …… 316
13.1.3 CC 的评估类型 …… 320

13.2 网络安全评估方法和流程 …… 321
13.2.1 CC评估的流程 …… 322
13.2.2 CC评估的现状和存在的问题 …… 323
13.2.3 CC评估发展趋势 …… 323
13.3 网络安全检测评估系统简介 …… 324
13.3.1 Nessus …… 324
13.3.2 AppScan …… 329
习题13 …… 335
附录A 实验 …… 336
实验1 数据的加密与解密 …… 336
实验2 Windows口令破解与安全 …… 338
实验3 网络嗅探与欺骗 …… 344
实验4 网络攻击与防范 …… 348
实验5 冰河木马的攻击与防范 …… 352
实验6 个人防火墙配置 …… 359
实验7 软件动态分析 …… 362
实验8 Windows 2000/XP/2003安全设置 …… 365
参考文献 …… 371

第1章　计算机信息安全技术概述

21世纪是信息技术快速发展的一个世纪，信息技术已经成为一个国家的政治、军事、经济和文教等事业发展的决定性因素。但是，目前的网络和信息传播途径中却蛰伏着诸多不安全因素，信息文明还面临着诸多威胁和风险，计算机信息安全问题已成为制约信息化发展的瓶颈，是关系国家发展的重要问题，其重要性随着全球信息化进程的加快而显得越来越重要。

本章是计算机信息安全技术的引导篇，主要介绍信息安全的基本概念、基本原则、安全体系结构、安全服务机制、信息安全现状与展望等知识，使读者掌握必要的信息安全基础知识，了解信息安全的重要意义，提高信息安全意识。

随着因特网技术的发展，因特网成为日常生活中不可或缺的一部分，人们越来越多地借助因特网来获取信息和知识。在享受信息社会带来的巨大经济利益和娱乐的同时，计算机信息安全问题日渐成为人们必须面对的一个严峻的问题。通过网络，攻防双方可以轻易地获得对方的机密，可以篡改、破坏对方的重要信息，破坏对方的信息处理设备等。因此，随着冷战的结束，因特网成为又一个看不见硝烟的全球性战场。

到目前为止，因特网已经深入到了生活中的方方面面，如日常生活中的银行、电话、购物、出行、电力等都严重依赖因特网的存在，现在已经很难想象没有了因特网以后，人们的生活会变成什么样子。随着人们对因特网的依存度逐渐提高，信息安全已经成为一个全世界性的现实问题，信息安全与国家的政治稳定、军事安全、经济发展、民族兴衰等都息息相关，提高国家信息安全体系的保障能力已成为各国政府优先考虑的战略问题。在我国的“十一五”规划中，信息安全是作为一项重要的研究课题来进行攻关的内容。

对每个普通民众来讲，信息安全问题同样严峻，每个人的重要数据存储在硬盘设备上，可能会因操作不当或计算机病毒、恶意软件攻击等瞬间化为乌有。我们的计算机系统有可能在毫无察觉的情况下被破坏而无法运行，有时被别人利用，成为攻击、破坏其他计算机系统的工具，甚至成为犯罪的工具。

1.1　计算机信息安全的威胁因素

计算机系统是用于信息存储、信息加工的设施。从技术的角度来看，因特网的不安全因素是：一方面由于它是面向所有用户的，所有资源通过网络共享；另一方面，它的技术是开放和标准的。因此，尽管因特网已从过去用于科研和学术目的阶段进入到商用阶段，但是它的技术基础仍是不安全的。从一般意义上来说，计算机系统一般是指具体的计算机系统，但有时也用计算机系统来表示一个协作处理信息的内部网络。计算机系统面临着各种各样的威胁，这些威胁大致可以分为以下3个方面。

(1) 直接对计算机系统的硬件设备进行破坏。

(2) 对存放在系统存储介质上的信息进行非法获取、篡改和破坏。

(3) 在信息传输过程中对信息非法获取、篡改和破坏。

从形式上来讲,自然灾害、意外事故、计算机犯罪、人为行为、黑客行为、内部泄密、外部泄密、信息丢失、电子谍报、信息战、网络协议中的缺陷等,都是威胁网络安全的重要因素。从人为的因素来考虑,影响信息安全的因素还存在着人为和非人为的两种情况。影响计算机信息安全的因素很多,这些因素可以分为以下几类。

(1) 人为的无意失误。操作员使用不当,安全配置不规范造成的安全漏洞,用户安全意识不强,选择用户口令不慎,将自己的账号随意转告他人或与别人共享等情况,都会对网络安全构成威胁。

(2) 人为的恶意攻击。此类攻击可以分为两种:一种是主动攻击,它的目的在于篡改系统中所含的信息,或者改变系统的状态和操作,它以各种方式有选择地破坏信息的有效性、完整性和真实性;另一种是被动攻击,它在不影响网络正常工作的情况下,进行信息的截获和窃取,分析信息流量,并通过信息的破译获得重要机密信息,它不会导致系统中信息的任何改动,而且系统的操作和状态也不会被改变,因此被动攻击主要威胁信息的保密性。这两种攻击均可对网络安全造成极大的危害,并导致机密数据的泄露。

(3) 计算机软件的漏洞和后门。计算机软件从规模和技术上来讲,不可能百分之百无缺陷和无漏洞,如广为人知的 TCP/IP 协议的安全问题等。然而,这些漏洞和缺陷恰恰是黑客进行攻击的首选目标。导致黑客频频攻入计算机系统内部的主要原因就是相应系统和应用软件本身的脆弱性和安全措施的不完善。另外,软件在设计之初,某些编程人员为了方便而设置的软件"后门",虽然通常都不为外人所知,但一旦后门洞开,将使黑客对计算机系统资源的非法使用成为可能。

虽然人为因素和非人为因素都可以对网络安全构成威胁,但相对物理实体和硬件系统及自然灾害而言,精心设计的人为攻击对计算机的信息安全威胁最大,因为人为因素最为复杂,人的思想最为活跃,不可能完全用静止的方法和法律、法规加以防护,这是计算机信息安全所面临的最大威胁。

要保证信息安全,就必须设法在一定程度上克服以上种种威胁,学会识别这些破坏手段,以便采取技术、管理和法律制约等方面的努力,确保网络的安全。需要指出的是,无论采用哪种防范措施,都不可能保证计算机信息的绝对安全。安全是相对的,不安全才是绝对的。

1.2 信息安全的含义

安全的本意是采取保护措施,防止来自攻击者有意或无意的破坏。信息安全是一个随着历史发展,其内涵不断丰富的概念。在 20 世纪 60～70 年代,军事通信提出了通信保密的需求,即必须考虑秘密消息在传送途中被除发信者和收信者以外的第三者(特别是敌方)截获的可能性,使截获者即使截获信息,也无法得到其中的信息内容,在这里,信息安全只具有信息保密的含义。到了 20 世纪 80～90 年代,信息安全不仅指机密性,它还包含完整性和可用性,俗称 CIA。C 代表机密性(Confidentiality),即保证信息为授权者拥有而不泄露给未