

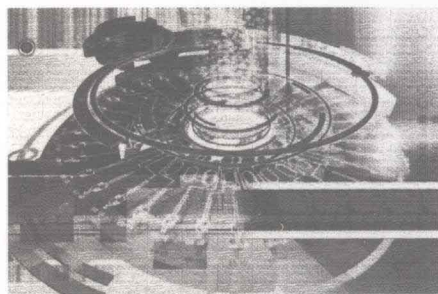


普通高等教育“十一五”国家级规划教材  
教育部普通高等教育精品教材

工业和信息化人才培养规划教材

高职高专计算机系列

# 计算机网络 安全技术(第3版)



**Network Security Technology**

深圳职院出品  
广东省精品课程配套教材  
全面介绍计算机网络安全技术

石淑华 池瑞楠 ◎ 主编

 人民邮电出版社  
POSTS & TELECOM PRESS

  
精品系列

INDUSTRY AND INFORMATION TECHNOLOGY TRAINING PLANNING MATERIALS  
TECHNICAL AND VOCATIONAL EDUCATION



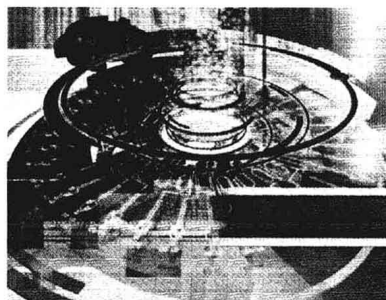
普通高等教育“十一五”国家级规划  
教育部普通高等教育精品教材



工业和信息技术人才培养规划教材

高职高专计算机系列

# 计算机网络 安全技术(第3版)



Network Security Technology

石淑华 池瑞楠 © 主编

人民邮电出版社

北京

## 图书在版编目 (C I P) 数据

计算机网络安全技术 / 石淑华, 池瑞楠主编. — 3  
版. — 北京: 人民邮电出版社, 2012. 8  
工业和信息化人才培养规划教材. 高职高专计算机系  
列  
ISBN 978-7-115-28372-6

I. ①计… II. ①石… ②池… III. ①计算机网络—  
安全技术—高等职业教育—教材 IV. ①TP393.08

中国版本图书馆CIP数据核字(2012)第145399号

## 内 容 提 要

本书根据高职院校的教学特点和培养目标, 全面介绍计算机网络安全的基本框架、基本理论, 以及计算机网络安全方面的管理、配置和维护。全书共 8 章, 主要内容包括计算机网络安全概述、黑客常用的系统攻击方法、计算机病毒、数据加密技术、防火墙技术、Windows Server 的安全、Web 的安全性以及网络安全工程。本书注重实用, 以实验为依托, 将实验内容融合在课程内容中, 使理论紧密联系实际。

本书可作为高职高专计算机及相关专业的教材, 也可作为相关技术人员的参考书或培训教材。

工业和信息化人才培养规划教材——高职高专计算机系列

### 计算机网络安全技术 (第 3 版)

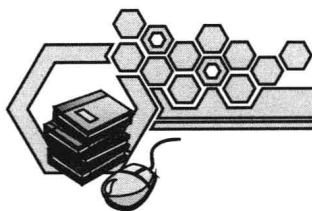
- 
- ◆ 主 编 石淑华 池瑞楠  
责任编辑 王 威
  - ◆ 人民邮电出版社出版发行 北京市崇文区夕照寺街 14 号  
邮编 100061 电子邮件 315@ptpress.com.cn  
网址 <http://www.ptpress.com.cn>  
北京新华印刷有限公司印刷
  - ◆ 开本: 787×1092 1/16  
印张: 19.75 2012 年 8 月第 3 版  
字数: 506 千字 2012 年 8 月北京第 1 次印刷

---

ISBN 978-7-115-28372-6

定价: 39.80 元

读者服务热线: (010)67170985 印装质量热线: (010)67129223  
反盗版热线: (010)67171154



## 第3版前言

本书的第1版自2005年出版,受到广大师生的欢迎,被许多高职院校选用,并于2008年9月再版,累计重印20多次,发行数万册。在这几年里我们也不断积累、总结,2008年我们的“计算机网络安全技术”课程被评为省级精品课程,第2版的教材也被评为国家级精品教材。随着时间的推移,网络安全技术在不断地发展,所以我们在保留原版教材特色的基础上,对教材进行了全面修订,力争体现如下的特色。

- 注重培养学生的动手能力。本书理论“以必需、够用为度”,特别注重实践环节,主要体现在两个方面:一方面是每章中都增加了大量的实验案例,通过大量的图片,使得实验操作步骤尽量详尽,这些案例遵循“源于实际、自主练习、层层递进、提高能力”的设计思路;另一方面是在第8章中安排了课程设计的内容,让学生自主学习,提高自身的综合能力。

- 注重知识的更新。计算机网络安全技术领域的一个典型特点就是技术更新速度较快。本书对第2版教材中的许多技术内容都进行了更新,增加了Windows Server 2008系统的内容,一些软件也更新了版本,并增加了很多新的知识,同时适当兼顾CIW的课程内容。

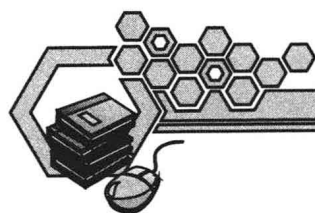
对于书中提到的一些工具软件,读者可以在Internet上自行下载。本书还配有PPT课件、教学大纲、习题答案等教学资源,任课教师可登录人民邮电出版社教学服务与资源网([www.ptpedu.com.cn](http://www.ptpedu.com.cn))免费下载,或者到我们的精品课程网站(<http://jpkc.szpt.edu.cn/2008/wlaqjs/>)免费下载。

本书第1章、第2章、第3章、第5章、第6章由石淑华编写,第4章、第7章、第8章由池瑞楠编写,全书由石淑华统稿并审定。在本书的编写过程中,深圳职业技术学院网络技术专业的王隆杰、梁广民、张立涓、杨名川、邹润生、刘平等老师在实验和绘图方面也做了很多工作,并提出了许多宝贵的意见,在此一一表示衷心的感谢!

由于编写水平有限,时间仓促,书中难免有不妥和错误之处,恳请广大读者批评指正。编者邮箱为 [sshua@szpt.edu.cn](mailto:sshua@szpt.edu.cn)。

编者

2012年3月



第 1 章 计算机网络安全概述	1	过程	20
1.1 网络安全简介	1	2.2 目标系统的探测方法	20
1.1.1 网络安全的重要性	1	2.2.1 常用的网络探测方法	21
1.1.2 网络脆弱性的原因	3	2.2.2 扫描器概述	22
1.1.3 网络安全的定义	4	2.2.3 端口扫描器演示实验	25
1.1.4 网络安全的基本要素	5	2.2.4 综合扫描器演示实验	29
1.1.5 典型的网络安全事件	5	2.2.5 CGI 扫描器	32
1.2 信息安全的发展历程	6	2.2.6 专项扫描器	34
1.2.1 通信保密阶段	7	2.3 口令破解	34
1.2.2 计算机安全阶段	7	2.3.1 口令破解概述	35
1.2.3 信息技术安全阶段	7	2.3.2 口令破解演示实验	35
1.2.4 信息保障阶段	8	2.4 网络监听	38
1.3 网络安全所涉及的内容	8	2.4.1 网络监听概述	39
1.3.1 物理安全	8	2.4.2 Sniffer 演示实验	41
1.3.2 网络安全	9	2.5 ARP 欺骗攻击	46
1.3.3 系统安全	9	2.5.1 ARP 欺骗的工作原理	46
1.3.4 应用安全	10	2.5.2 交换环境下的 ARP 欺骗 攻击及其嗅探演示实验	47
1.3.5 管理安全	10	2.6 木马	49
1.4 网络安全防护体系	11	2.6.1 木马的工作原理	50
1.4.1 网络安全的威胁	11	2.6.2 木马的分类	50
1.4.2 网络安全的防护体系	12	2.6.3 木马的工作过程	51
1.4.3 数据保密	13	2.6.4 传统木马演示实验	52
1.4.4 访问控制技术	14	2.6.5 反弹端口木马演示实验	53
1.4.5 网络监控	15	2.6.6 木马的隐藏与伪装方式	55
1.4.6 病毒防护	15	2.6.7 木马的启动方式	57
练习题	15	2.6.8 木马的检测	58
第 2 章 黑客常用的系统攻击 方法	17	2.6.9 木马的防御与清除	60
2.1 黑客概述	18	2.7 拒绝服务攻击	61
2.1.1 黑客的由来	18	2.7.1 拒绝服务攻击概述	61
2.1.2 黑客攻击的动机	19	2.7.2 拒绝服务攻击原理	62
2.1.3 黑客入侵攻击的一般		2.7.3 拒绝服务攻击演示实验	64
		2.7.4 分布式拒绝服务攻击 原理	65



2.7.5 分布式拒绝服务攻击 演示实验.....	66	3.5.1 计算机病毒引起的异常 现象.....	97
2.7.6 冰盾防火墙的演示实验.....	67	3.5.2 计算机防病毒技术.....	98
2.8 缓冲区溢出.....	68	3.6 防病毒应具有的基础知识.....	99
2.8.1 缓冲区溢出攻击概述.....	69	3.6.1 常用的单机杀毒软件.....	99
2.8.2 缓冲区溢出原理.....	69	3.6.2 网络防病毒方案.....	103
2.8.3 缓冲区溢出演示实验.....	70	3.6.3 Symantec 校园网防病毒 案例.....	104
2.8.4 缓冲区溢出的预防.....	72	3.6.4 选择防病毒软件的 标准.....	110
练习题.....	72	练习题.....	111
<b>第3章 计算机病毒.....</b>	<b>75</b>	<b>第4章 数据加密技术.....</b>	<b>113</b>
3.1 计算机病毒概述.....	75	4.1 概述.....	114
3.1.1 计算机病毒的基本概念.....	75	4.1.1 密码学的有关概念.....	114
3.1.2 计算机病毒发展简史.....	76	4.1.2 密码学发展的3个 阶段.....	115
3.1.3 计算机病毒的发展历程.....	77	4.1.3 密码学与信息安全的 关系.....	116
3.2 计算机病毒的特征.....	79	4.2 古典加密技术.....	116
3.2.1 传染性.....	80	4.2.1 替换密码技术.....	116
3.2.2 破坏性.....	80	4.2.2 换位密码技术.....	119
3.2.3 潜伏性及可触发性.....	81	4.3 对称加密算法及其应用.....	119
3.2.4 非授权性.....	81	4.3.1 DES 算法及其基本 思想.....	120
3.2.5 隐蔽性.....	81	4.3.2 DES 算法的安全性 分析.....	121
3.2.6 不可预见性.....	82	4.3.3 其他常用的对称加密 算法.....	122
3.3 计算机病毒的分类.....	82	4.3.4 对称加密算法在网络 安全中的应用.....	123
3.3.1 按照计算机病毒依附的 操作系统分类.....	82	4.4 公开密钥算法及其应用.....	124
3.3.2 按照计算机病毒的传播 媒介分类.....	83	4.4.1 RSA 算法及其基本 思想.....	124
3.3.3 按照计算机病毒的宿主 分类.....	84	4.4.2 RSA 算法的安全性 分析.....	126
3.3.4 蠕虫病毒.....	85	4.4.3 其他常用的公开密钥 算法.....	126
3.4 计算机病毒的原理与实例.....	86	4.4.4 公开密钥算法在网络 安全中的应用.....	127
3.4.1 计算机病毒的结构.....	86		
3.4.2 文件型病毒的实例 ——CIH 病毒.....	86		
3.4.3 宏病毒.....	88		
3.4.4 蠕虫病毒的实例—— “熊猫烧香”病毒.....	91		
3.4.5 2008 年新病毒的实例 ——“磁碟机”病毒.....	93		
3.5 计算机病毒的防治.....	97		

4.5 数据加密技术的应用 .....	129	6.1.2 Windows Server 的 模型 .....	190
4.5.1 报文鉴别 .....	129	6.2 Windows Server 2003 的安全 模型 .....	193
4.5.2 PGP 加密系统演示 实验 .....	133	6.2.1 Windows Server 2003 的 安全元素 .....	193
4.5.3 SSL 协议和 SET 协议 .....	146	6.2.2 Windows Server 2003 的 登录过程 .....	194
4.5.4 PKI 技术及其应用 .....	147	6.2.3 Windows Server 2003 的 安全认证子系统 .....	194
练习题 .....	157	6.2.4 Windows Server 的安全 标识符 .....	195
<b>第 5 章 防火墙技术 .....</b>	<b>159</b>	6.3 Windows Server 的账户 管理 .....	196
5.1 防火墙概述 .....	159	6.3.1 Windows Server 的安全 账号管理器 .....	197
5.1.1 防火墙的基础知识 .....	159	6.3.2 SYSKEY 双重加密账户 保护 .....	197
5.1.2 防火墙的功能 .....	160	6.3.3 使用 L0phtCrack5 审计 Windows Server 2003 本 地账户实验 .....	199
5.1.3 防火墙的局限性 .....	161	6.3.4 使用 Cain 审计 Windows Server 2008 本地账户 实验 .....	204
5.2 防火墙分类 .....	162	6.3.5 账户安全防护 .....	205
5.2.1 软件防火墙和硬件 防火墙 .....	162	6.3.6 账户安全策略 .....	206
5.2.2 单机防火墙和网络 防火墙 .....	162	6.4 Windows Server 注册表 .....	209
5.2.3 防火墙的体系结构 .....	163	6.4.1 注册表的由来 .....	209
5.2.4 防火墙技术分类 .....	165	6.4.2 注册表的基本知识 .....	209
5.2.5 防火墙 CPU 架构分类 .....	166	6.4.3 根键 .....	210
5.3 防火墙实现技术原理 .....	167	6.4.4 注册表的备份与恢复 .....	212
5.3.1 包过滤防火墙 .....	167	6.4.5 注册表的操作 .....	214
5.3.2 代理防火墙 .....	169	6.4.6 注册表的应用 .....	215
5.3.3 状态检测防火墙 .....	173	6.4.7 注册表的权限 .....	217
5.3.4 复合型防火墙 .....	175	6.4.8 注册表的维护工具 .....	218
5.4 防火墙的应用 .....	175	6.5 Windows Server 常用的系统 进程和服务 .....	220
5.4.1 瑞星个人防火墙的 应用 .....	176	6.5.1 进程 .....	220
5.4.2 代理服务器的应用 .....	180	6.5.2 Windows Server 2003 常用的系统进程 .....	221
5.5 防火墙产品 .....	185		
5.5.1 防火墙的主要参数 .....	185		
5.5.2 选购防火墙的注意点 .....	186		
练习题 .....	187		
<b>第 6 章 Windows Server 的 安全 .....</b>	<b>189</b>		
6.1 Windows Server 2008 概述 .....	190		
6.1.1 Windows Server 2008 的 新特性 .....	190		

6.5.3	进程管理实验 .....	222	实验 .....	270
6.5.4	Windows Server 的系统 服务 .....	228	7.4 Web 浏览器的安全性 .....	274
6.5.5	Windows Server 的系统 日志 .....	231	7.4.1 浏览器本身的漏洞 .....	274
6.6	Windows Server 系统的安全 模板 .....	235	7.4.2 ActiveX 的安全性 .....	275
6.6.1	安全模板概述 .....	235	7.4.3 Cookie 的安全性 .....	277
6.6.2	安全模板的使用 .....	236	练习题 .....	281
6.6.3	安全配置和分析 .....	237	<b>第 8 章 网络安全工程</b> .....	283
	练习题 .....	238	8.1 网络安全策略 .....	283
<b>第 7 章 Web 的安全性</b> .....	240	8.1.1 网络安全策略的制定 原则 .....	284	
7.1 Web 的安全性概述 .....	240	8.1.2 常用的网络安全策略 .....	285	
7.1.1 Internet 的脆弱性 .....	241	8.2 网络安全标准 .....	288	
7.1.2 Web 的安全问题 .....	241	8.2.1 国际上的网络安全 标准 .....	288	
7.1.3 Web 安全的实现方法 .....	242	8.2.2 国内的网络安全标准 .....	291	
7.2 Web 服务器的安全性 .....	242	8.3 网络安全系统的设计、管理 和评估 .....	291	
7.2.1 Web 服务器的作用 .....	242	8.3.1 网络安全系统的设计 原则 .....	292	
7.2.2 Web 服务器存在的 漏洞 .....	244	8.3.2 网络安全系统的管理 .....	293	
7.2.3 IIS 的安全 .....	245	8.3.3 网络安全系统的风险 评估 .....	295	
7.2.4 SSL 安全演示实验 .....	251	8.4 典型网络安全工程实例 .....	297	
7.3 脚本语言的安全性 .....	267	8.4.1 数据局 163/169 网络的 设计和实施 .....	297	
7.3.1 CGI 程序的安全性 .....	267	8.4.2 TF 公司信息安全管理 体系的实施 .....	300	
7.3.2 CGI 程序的常见漏洞 实例 .....	268	练习题 .....	308	
7.3.3 ASP 的安全性 .....	269			
7.3.4 ASP/SQL 注入演示				



# 第1章

## 计算机网络安全概述

### 职业能力要求

- 专业能力：掌握网络安全行业的基本情况，了解网络安全行业的新技术；培养良好的职业道德。
- 社会能力：具有认真负责、严谨细致的工作态度和的工作作风，具备良好的团队协作和沟通交流能力。
- 方法能力：具有良好的自学能力，对新技术有学习、研究精神，具有较强的动手操作能力。

### 学习目标

- 了解网络安全的重要性。
- 掌握网络安全的定义。
- 了解信息安全的发展历程。
- 了解网络安全所涉及的知识领域。
- 了解网络安全常见的防护技术。

本章概要地介绍了网络安全领域中的问题：网络安全的重要性以及网络安全的定义、信息安全的发展历程和网络安全的防护体系。在本章的学习过程中，除了掌握网络安全领域中的基本概念外，还应该掌握信息安全领域的新技术。本章的重点是培养读者的兴趣，使读者的学习有一个良好的开端。

## 1.1 网络安全简介

### 1.1.1 网络安全的重要性

随着信息科技的迅速发展以及计算机网络的普及，计算机网络深入到国家的政府、军事、

文教、金融、商业等诸多领域,可以说网络无处不在。资源共享和计算机网络安全一直作为一对矛盾体而存在着,计算机网络资源共享进一步加强,信息安全问题日益突出。

据 CNNIC (中国互联网络信息中心) 最新发布的中国互联网络发展状况统计报告显示,截至 2011 年 6 月底,中国网民规模达到 4.85 亿,较 2010 年底增加 2770 万人,增幅 6.1%; 2011 年上半年,中国微博用户数量从 6311 万快速增长到 1.95 亿,如图 1-1 所示。

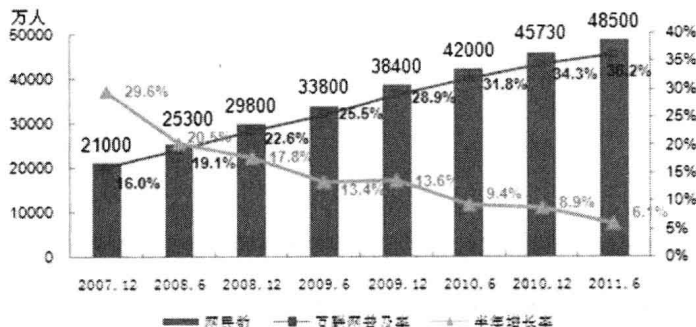


图 1-1 网民数量统计

互联网在我国政治、经济、文化以及社会生活中发挥着愈来愈重要的作用,作为国家关键基础设施和新的生产、生活工具,互联网的发展极大地促进了信息流通和共享,提高了社会生产效率和人民生活水平,促进了经济社会的发展。互联网的影响日益扩大、地位日益提升,维护网络安全工作的重要性日益突出。

网络系统失灵会造成通信瘫痪、基础设施损坏、大范围停电、船只停航的重大事故。1992 年,美国联邦航空管理局的一条光缆被无意间挖断,所属的 4 个主要空中交通管制中心关闭 35 小时,成百上千航班被延误或取消。1996 年,世界最大计算机信息服务网络公司——美国联机公司,在正常维护中更换一款新软件后发生故障,造成了大规模服务中断事件,包括众多企业在内的 600 多万用户 19 小时无法使用电子邮件、互联网接入等,有的企业遭受了巨大的经济损失。2008 年 3 月,英国伦敦希斯罗机场第五航站楼的电子网络系统在启用当天就发生故障,致使五号航站楼陷入混乱。

据国家计算机网络应急技术处理协调中心 (CNCERT) 监测,每年都会有非常多的网络安全攻击事件发生。除了攻击事件,病毒对网络安全的影响也越来越大,金山网络公司为近年来的新增病毒/木马数量进行了对比,如图 1-2 所示。2009 年,计算机病毒/木马仍处于一种高速“出新”的状态。2010 年病毒/木马增长速度与 2009 年相比有所放缓,但仍处于大幅增长状态,总数量还是非常庞大的。各种计算机病毒和网上黑客对 Internet 的攻击越来越猛烈,网站遭受破坏的事例不胜枚举。

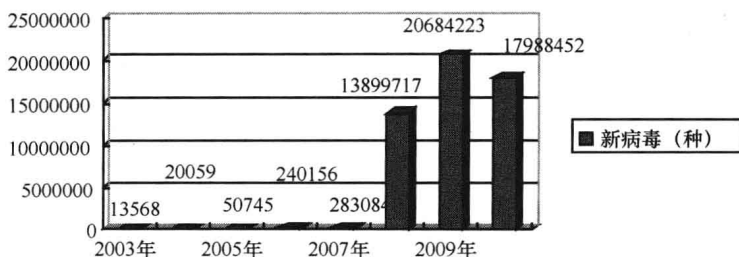


图 1-2 新增加病毒统计 (2003~2010 年)

2006 年第 38 个世界电信日暨首个世界信息社会日的主题是“Promoting Global Cyber Security” (推进全球网络安全)。这充分体现出网络安全不再是一个潜在的问题,已经成为当前信息社会现

实存在的重大问题，与国家安全息息相关，涉及国家政治和军事命脉，影响国家的安全和主权。一些发达国家如英国、美国、日本、俄罗斯等把国家网络安全纳入了国家安全体系。

信息安全空间将成为传统的国界、领海、领空的三大国防和基于太空的第四国防之外的第五国防，称为 Cyber-Space。美国政府在 2009 年 5 月发表的《网络空间政策评估报告》，将网络空间定义为“全球相互连接的数字信息和通信基础设施”。

因此，网络安全不仅成为商家关注的焦点，还是技术研究的热门领域，同时也是国家和政府关注的焦点。

## 1.1.2 网络脆弱性的原因

### 1. 开放性的网络环境

正如一句非常经典的语句所说：“Internet 的美妙之处在于你和每个人都能互相联接，Internet 的可怕之处在于每个人都能和你互相联接。”

网络空间之所以易受攻击，是因为网络系统具有开放、快速、分散、互联、虚拟、脆弱等特点。网络用户可以自由访问任何网站，几乎不受时间和空间的限制。信息传输速度极快，病毒等有害信息可在网上迅速扩散和放大。网络基础设施和终端设备数量众多，分布地域广阔，各种信息系统互联互通，用户身份和位置真假难辨，构成了一个庞大而复杂的虚拟环境。此外，网络软件和协议存在许多技术漏洞，为攻击者提供了可乘之机。这些特点都给网络空间的管控造成了巨大的困难。

Internet 是跨国界的，这意味着网络的攻击不仅仅来自本地网络的用户，也可以来自 Internet 上的任何一台机器。Internet 是一个虚拟的世界，所以无法得知联机的另一端是谁。图 1-3 所示为网上非常出名的一幅图片。在这个虚拟的世界里，已经超越了国界，某些法律也受到了挑战，因此网络安全面临的是一个国际化的挑战。

网络建立初期只考虑方便性、开放性，并没有考虑总体安全构想，因此任何一个人、团体都可以接入，网络所面临的破坏和攻击可能是多方面的。例如，可能是对物理传输线路的攻击，也可能是对网络通信协议及应用的攻击；可能是对软件的攻击，也可能是对硬件的攻击。

### 2. 协议本身的脆弱性

网络传输离不开通信协议，而这些协议也有不同层次、不同方面的漏洞，针对 TCP/IP 等协议的攻击非常多，在以下几个方面都有攻击的案例。

(1) 网络应用层服务的安全隐患。例如，攻击者可以利用 FTP、Login、Finger、Whois、WWW 等服务来获取信息或取得权限。

(2) IP 层通信的易欺骗性。由于 TCP/IP 本身的缺陷，IP 层数据包是不需要认证的，攻击者可以假冒其他用户进行通信，即 IP 欺骗。

(3) 针对 ARP 的欺骗性。ARP 是网络通信中非常重要的协议，基于 ARP 的工作原理，攻击者可以假冒网关，阻止用户上网，即 ARP 欺骗。近一年来 ARP 攻击更与病毒结合在一起，破坏



图 1-3 网上图片

网络的连通性。

(4) 局域网中以太网协议的数据传输机制是广播发送，使系统和网络具有易被监视性。在网络上，黑客能用嗅探软件监听到口令和其他敏感信息。

### 3. 操作系统的漏洞

网络离不开操作系统，操作系统的安全性对网络安全同样有非常重要的影响，有很多网络攻击方法都是从寻找操作系统的缺陷入手的。操作系统的缺陷有以下几个方面。

(1) 系统模型本身的缺陷。这是系统设计初期就存在的，无法通过修改操作系统程序的源代码来弥补。

(2) 操作系统程序的源代码存在 Bug。操作系统也是一个计算机程序，任何程序都会有 Bug，操作系统也不会例外。例如，冲击波病毒针对的就是 Windows 操作系统的 RPC 缓冲区溢出漏洞。那些公布了源代码的操作系统所受到的威胁更大，黑客会分析其源代码，找到漏洞进行攻击。

(3) 操作系统程序的配置不正确。许多操作系统的默认配置安全性很差，进行安全配置比较复杂，并且需要一定的安全知识，许多用户并没有这方面的能力，如果没有正确地配置这些功能，也会造成一些系统的安全缺陷。

Microsoft 公司在 2010 年发布了 106 个安全公告，修补了 247 个操作系统的漏洞，比 2009 年多 57 个。漏洞的大量出现和不断快速增加补丁是网络安全总体形势趋于严峻的重要原因之一。不仅仅操作系统存在这样的问题，其他应用系统也一样。比如：微软公司在 2010 年 12 月推出 17 款补丁，用于修复 Windows 操作系统、IE 浏览器、Office 软件等存在的 40 个安全漏洞。在我们实际的应用软件中，可能存在的安全漏洞更多。

### 4. 人为因素

许多公司和用户的网络安全意识薄弱、思想麻痹，这些管理上的人为因素也影响了安全。

## 1.1.3 网络安全的定义

国际标准化组织 (ISO) 引用 ISO 74982 文献中对安全的定义：安全就是最大程度地减少数据和资源被攻击的可能性。

《计算机信息系统安全保护条例》的第三条规范了包括计算机网络系统在内的计算机信息系统安全的概念：“计算机信息系统的安全保护，应当保障计算机及其相关的和配套的设备、设施（含网络）的安全，运行环境的安全，保障信息的安全，保障计算机功能的正常发挥，以维护计算机信息系统的安全运行。”

从本质上讲，网络安全是指网络系统的硬件、软件和系统中的数据受到保护，不受偶然的或者恶意的攻击而遭到破坏、更改、泄露，系统连续可靠正常地运行，网络服务不中断。广义上讲，凡是涉及网络上信息的保密性、完整性、可用性、可控性和不可否认性的相关技术和理论都是网络安全所要研究的领域。

欧共体对信息安全给出如下定义：“网络与信息安全可被理解为在既定的密级条件下，网络与信息系统抵御意外事件或恶意行为的能力。这些事件和行为将危及所存储或传输的数据，以及经由这些网络和系统所提供的服务的可用性、真实性、完整性和秘密性。”

网络安全的具体含义会随着重视“角度”的变化而变化。例如，从用户（个人、企业等）的角度来说，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,避免其他人或对手利用窃听、冒充、篡改、抵赖等手段侵犯用户的利益和隐私。从网络运行和管理者的角度来说,希望对本地网络信息的访问、读、写等操作受到保护和控制,避免出现后门、病毒、非法存取、拒绝服务和网络资源非法占用和非法控制等威胁,制止和防御网络黑客的攻击。从安全保密部门的角度来说,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,避免机密信息泄露,避免对社会产生危害、对国家造成巨大损失。从社会教育和意识形态的角度来说,网络上不健康的内容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。

### 1.1.4 网络安全的基本要素

网络安全的目的如图 1-4 所示:保障网络中的信息安全,防止非授权用户的进入以及事后的安全审记。

上述目的也就是网络安全的基本要素,即保密性 (Confidentiality)、完整性 (Integrity)、可用性 (Availability)、可控性 (Controllability) 与不可否认性 (Non-Repudiation)。

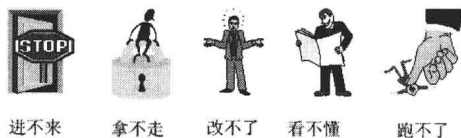


图 1-4 网络安全的目的

#### 1. 保密性

保密性是指保证信息不能被非授权访问,即非授权用户得到信息也无法知晓信息内容,因而不能使用。通常通过访问控制阻止非授权用户获得机密信息,还通过加密阻止非授权用户获知信息内容,确保信息不暴露给未授权的实体或者进程。

#### 2. 完整性

完整性是指只有得到允许的人才能修改实体或者进程,并且能够判断实体或者进程是否已被修改。一般通过访问控制阻止篡改行为,同时通过消息摘要算法来检验信息是否被篡改。

#### 3. 可用性

可用性是指信息资源服务功能和性能可靠性的度量,涉及物理、网络、系统、数据、应用和用户等多方面的因素,是对信息网络总体可靠性的要求。授权用户根据需要,可以随时访问所需信息,攻击者不能占用所有的资源而阻碍授权者的工作。使用访问控制机制阻止非授权用户进入网络,使静态信息可见,动态信息可操作。

#### 4. 可控性

可控性主要是指对危害国家信息(包括利用加密的非法通信活动)的监视审计,控制授权范围内的信息的流向及行为方式。使用授权机制,控制信息传播的范围、内容,必要时能恢复密钥,实现对网络资源及信息的可控性。

#### 5. 不可否认性

不可否认性是指对出现的安全问题提供调查的依据和手段。使用审计、监控、防抵赖等安全机制,使攻击者、破坏者、抵赖者“逃不脱”,并进一步对网络出现的安全问题提供调查依据和手段,实现信息安全的可审查性,一般通过数字签名等技术来实现不可否认性。

### 1.1.5 典型的网络安全事件

网络安全事件不计其数,典型的网络安全事件如表 1-1 所示。

表 1-1

典型安全事件

时 间	发生的主要事件
1983 年	美国联邦调查局首次逮捕了 6 名少年黑客, 因其所居住的地区密尔沃基电话区号是 414 而被称做“414 黑客”。这 6 名少年黑客被控侵入 60 多台计算机, 其中包括斯洛恩-凯特林癌症纪念中心和洛斯阿拉莫斯国家实验室
1988 年	康奈尔大学研究生罗伯特·莫里斯(22 岁)向 Internet 上传了一个“蠕虫”程序。这个程序是他为攻击 UNIX 系统的缺陷而设计的, 能够进入网络中的其他计算机并自我繁衍。当时使得美国 6000 多个系统(几乎占当时 Internet 的 1/10)陷入瘫痪, 专家称这个“蠕虫”程序造成了 1500 万到 1 亿美元的经济损失
1995 年	米特尼克被逮捕。他被指控闯入许多计算机网络, 偷窃了 2 万个信用卡号和复制软件。他曾闯入“北美空中防务指挥系统”, 破译了美国著名的“太平洋电话公司”在南加利福尼亚州通信网络的“改户密码”, 入侵过美国 DEC 等 5 家大公司的网络。专家们测算, 米特尼克一人就造成了美国一些公司 8000 万美元的巨额损失
1999 年 4 月	台湾大同工学院资讯工程系学生陈盈豪所制造的“CIH”病毒, 在 26 日发作, 引起全球震撼。保守估计全球有 6 千万台计算机受害
2000 年 2 月	以“雅虎”为首的美国一系列大型网站遭到了黑客有组织的攻击, 他们攻击的目标包括雅虎、电子港湾、亚马孙、微软网络等美国大型网站。据统计, 在 2 月 7、8、9 日这短短的 3 天里, 这些受害公司的损失就超过了 10 亿美元, 其中仅营销和广告收入一项便高达 1 亿美元
2001 年 9 月	“9·11”事件促使人们更加重视网络安全以及灾后恢复能力, 事件后, 美国国务院在贝尔茨维尔建立了一个网络监视中心。美国加大了网络安全技术的研发力度, 并积极采取措施, 在网络防御实践中使用新的安全防护技术
2002 年 10 月	黑客用 DDoS 攻击影响了 13 个根 DNS (Domain Name Server) 中的 8 个, 作为整个 Internet 通信路标的关键系统遭到严重的破坏
2003 年 1 月	出现“蠕虫王”病毒, 利用 Microsoft SQL Server 的漏洞进行传播, 由于 Microsoft SQL Server 在世界范围内都很普及, 因此此次病毒攻击导致全球范围内的 Internet 瘫痪, 全世界范围内损失额高达 12 亿美元
2004 年 10 月	国内的腾讯 QQ、神州数码、江民公司、一家著名电子商务网站陆续被黑客攻陷或入侵。其中一些网站还受到了黑客的巨额敲诈勒索, 这是国内首起网络黑客勒索事件
2006 年	防止恶意软件对内核的非授权修改, Microsoft 通过 Patch Guard 技术能够封杀对 64 位版 Windows Vista 内核的访问, 以赛门铁克、McAfee 为代表的安全厂商声称, 它们需要访问操作系统内核, 探测 rootkit 等恶意软件。在受到来自欧盟委员会和韩国监管机构的压力后, Microsoft 同意开放访问内核的 API。但是, 厂商需要等到 Microsoft 发布 Vista SP1 后才能够使用这些 API
2007 年	超过 9400 万名用户的 Visa 和 MasterCard 信用卡信息被黑客窃取
2008 年	云安全无疑是 2008 年网络安全行业最热的关键词
2009 年	奥巴马在竞选期间就一直强调网络安全对美国的重要性, 他甚至将来自网络空间的威胁等同于核武器和生物武器对美国的威胁
2010 年	2010 年 11 月 3 日晚, 腾讯发布公告, 在装有 360 软件的电脑上停止运行 QQ 软件。360 随即推出了“WebQQ”的客户端, 但腾讯随即关闭 WebQQ 服务, 使客户端失效

## 1.2 信息安全的发展历程

随着科学技术的发展, 信息安全技术也进入了高速发展的时期。人们对信息安全的需求也从单一的通信保密发展到各种各样的信息安全产品、技术手段等多方面。总地来说, 信息安全技术在发展过程中经历了以下 4 个阶段。



## 1.2.1 通信保密阶段

20世纪40年代~70年代,通信技术还不发达,面对电话、电报、传真等信息交换过程中存在的安全问题,重点是通过密码技术解决通信保密问题,保证数据的保密性与完整性,对安全理论和技术的研究也只侧重于密码学,这一阶段的信息安全可以简单地称为通信安全,即COMSEC(Communication Security)。

这个阶段的标志性事件是:1949年Shannon发表的《保密通信的信息理论》,该理论将密码学纳入了科学的轨道;1976年Diffie与Hellman在“New Directions in Cryptography”一文中提出了公钥密码体制;美国国家标准协会在1977年公布的《国家数据加密标准》(Data Encryption Standard, DES)。这时人们关心的只是通信安全,重点是通过密码技术解决通信保密问题,而且主要的关心对象是军方和政府。

当时,美国政府和一些大公司已经认识到了计算机系统的脆弱性。但是,由于计算机使用范围不广,再加上美国政府将其当作敏感问题而施加控制,因此,有关计算机安全的研究一直局限在比较小的范围。

## 1.2.2 计算机安全阶段

20世纪80年代后,计算机的性能迅速提高,应用范围不断扩大,计算机和网络技术的应用进入了实用化和规模化阶段,人们利用通信网络把孤立的计算机系统连接起来,共享资源,信息安全问题也逐渐受到重视。人们对安全的关注已经逐渐扩展为以保密性、完整性和可用性为目标的计算机安全阶段,即COMPSEC(Computer Security)。

这一时期的标志是美国国防部在1983年出版的《可信计算机系统评价准则》(Trusted Computer System Evaluation Criteria, TCSEC),为计算机安全产品的评测提供了测试方法,指导信息安全产品的制造和应用。美国国防部1985年再版的《可信计算机系统评价准则》(又称橙皮书)使计算机系统的安全性评估有了一个权威性的标准。

这个阶段的重点是确保计算机系统中的软、硬件及信息在处理、存储、传输中的保密性、完整性和可用性。安全威胁已经扩展到非法访问、恶意代码、口令攻击等。

## 1.2.3 信息技术安全阶段

20世纪90年代,主要安全威胁发展到网络入侵、病毒破坏、信息对抗的攻击等,网络安全的重点放在确保信息在存储、处理、传输过程中及信息系统不被破坏,确保合法用户的服务和限制非授权用户的服务,以及必要的防御攻击的措施。强调信息的保密性、完整性、可控性、可用性的信息安全阶段,即ITSEC(Information Technology Security)。

这个阶段的主要保护措施包括防火墙、防病毒软件、漏洞扫描、入侵检测、PKI、VPN等措施。

这一时期的主要标志是在1993年至1996年美国国防部在TCSEC的基础上提出了新的安全评估准则《信息技术安全通用评估准则》,简称CC标准。1996年12月,ISO采纳CC,并作为国际标准ISO/IEC 15408发布。2001年,我国将ISO/IEC 15408等同转化为国家标准——GB/T 18336—2001《信息技术安全性评估准则》。

## 1.2.4 信息保障阶段

20 世纪 90 年代后期，随着电子商务等的发展，由此衍生出了诸如可控性、抗抵赖性、真实性等其他原则和目标。对安全性有了新的需求：可控性，即对信息及信息系统实施安全监控管理；不可否认性，即保证行为人不能否认自己的行为。信息安全也转化为从整体角度考虑其体系建设的信息保障（Information Assurance）阶段，也称为网络信息系统安全阶段。

这一时期，在密码学方面，公开密钥密码技术得到了长足的发展，著名的 RSA 公开密钥密码算法获得了广泛的应用，用于完整性校验的散列函数的研究也越来越多。主要的保护措施包括防火墙、防病毒软件、漏洞扫描、入侵检测系统、PKI、VPN 等。

信息安全受到空前的重视，各个国家分别提出自己的信息安全保障体系。1998 年美国国家安全局（NSA）制定了《信息保障技术框架》（Information Assurance Technical Framework, IATF），提出了“深度防御策略”，确定了包括网络与基础设施防御、区域边界防御、计算环境防御和支撑性基础设施的深度防御目标。

## 1.3 网络安全所涉及的内容

在 Internet 中，网络安全的概念和日常生活中的安全一样常被提及，而“网络安全”到底包括什么，具体又涉及哪些技术，大家未必清楚，可能会认为“网络安全”只是防范黑客和病毒。其实网络安全是一门交叉学科，涉及多方面的理论和应用知识。除了数学、通信、计算机等自然科学外，还涉及法律、心理学等社会科学，是一个多领域的复杂系统。网络安全所涉及的知识领域如图 1-5 所示。

网络安全涉及上述多种学科的知识，而且随着网络应用的范围越来越广，以后涉及的学科领域有可能会更加广泛。一般地，把网络安全涉及的内容分为以下几个方面，如图 1-6 所示。

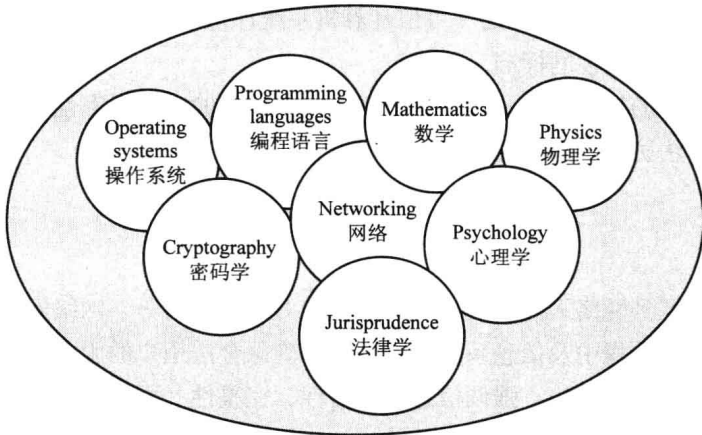


图 1-5 网络安全所涉及的知识领域

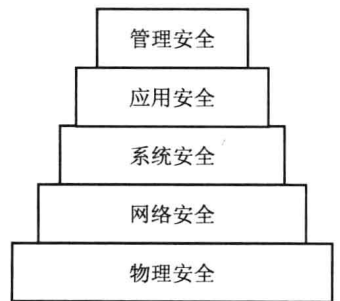


图 1-6 网络安全所涉及的内容

### 1.3.1 物理安全

保证计算机信息系统各种设备的物理安全，是整个计算机信息系统安全的前提。物理安全是

保护计算机网络设备、设施以及其他媒体,免遭地震、水灾、火灾等环境事故,以及人为操作失误、错误或者各种计算机犯罪行为导致的破坏。物理安全主要包括以下3个方面。

(1) 环境安全:对系统所在环境的安全保护,如区域保护和灾难保护。

(2) 设备安全:主要包括设备的防盗、防毁、防电磁信息辐射泄漏、防止线路截获、抗电磁干扰及电源保护等。

(3) 媒体安全:包括媒体数据的安全及媒体本身的安全。

### 1.3.2 网络安全

网络安全主要包括网络运行和网络访问控制的安全,如表 1-2 所示。下面对其中的重要组成部分予以说明。

在网络安全中,在内部网与外部网之间,设置防火墙实现内外网的隔离和访问控制,是保护内部网安全的最主要措施,同时也是最有效、最经济的措施之一。网络安全检测工具通常是一个网络安全性的评估分析软件或者硬件,用此类工具可以检测出系统的漏洞或潜在的威胁,以达到增强网络安全性的目的。

表 1-2 网络安全的组成

网 络 安 全	局域网、子网安全	访问控制(防火墙)
		网络安全检测 (网络入侵检测系统)
	网络中数据传输安全	数据加密(VPN等)
	网络运行安全	备份与恢复
		应急
	网络协议安全	TCP/IP
其他协议		

备份系统为一个目的而存在,即尽可能快地全面恢复运行计算机系统所需的数据和系统信息。备份不仅在网络系统硬件故障或人为失误时起到保护作用,也在入侵者非授权访问或对网络攻击及破坏数据完整性时起到保护作用,同时也是系统灾难恢复的前提之一。

### 1.3.3 系统安全

系统安全的组成如表 1-3 所示。

表 1-3 系统安全的组成

系 统 安 全	操作系统安全	反病毒
		系统安全检测
		入侵检测(监控)
		审计分析
	数据库系统安全	数据库安全
		数据库管理系统安全