21世纪 21世纪高等院校规划教材

网络与信息安全教程

（第二版）

吴煜煌 编著

中国水利水电出版社
www.waterpub.com.cn

21世纪高等院校规划教材

网络与信息安全教程

（第二版）

吴煜煌　编著

中国水利水电出版社
www.waterpub.com.cn

内 容 提 要

本书介绍了网络与信息安全的基本理论和关键技术，全书共 12 章，主要内容包括：网络安全概述、密码技术与应用、数字签名与身份认证技术、防火墙技术、入侵检测技术、网络病毒与防治、黑客常用的攻击技术、网络服务的安全、操作系统的安全、数据库系统的安全、电子商务安全和无线网络安全技术。

通过对本书的学习，读者能够对计算机网络与信息安全知识有一个比较系统的了解，掌握计算机网络特别是计算机互联网安全的基本概念，了解网络与信息安全的各种关键技术及其系统安全的基本手段和常用方法。

本书内容丰富、结构合理，可作为普通高等院校和高等职业技术学校信息安全、计算机网络及相关专业课程的教材，也可供从事网络安全、网络管理、信息系统开发的科研人员和相关行业技术人员参考。

本书配有电子教案，读者可以从中国水利水电出版社以及万水书苑（http://www.waterpub.com.cn/softdown/或 http://www.wsbookshow.com）免费下载。

图书在版编目（CIP）数据

网络与信息安全教程 / 吴煜煌编著. -- 2版. -- 北京 : 中国水利水电出版社, 2015.8
21世纪高等院校规划教材
ISBN 978-7-5170-3476-6

Ⅰ. ①网… Ⅱ. ①吴… Ⅲ. ①计算机网络－信息安全－安全技术－高等学校－教材 Ⅳ. ①TP393.08

中国版本图书馆CIP数据核字(2015)第185894号

策划编辑：雷顺加　责任编辑：杨元泓　加工编辑：祝智敏　封面设计：李　佳

书　　名	21 世纪高等院校规划教材 网络与信息安全教程（第二版）
作　　者	吴煜煌　编著
出版发行	中国水利水电出版社 （北京市海淀区玉渊潭南路 1 号 D 座　100038） 网址：www.waterpub.com.cn E-mail：mchannel@263.net（万水） sales@waterpub.com.cn 电话：（010）68367658（发行部）、82562819（万水）
经　　售	北京科水图书销售中心（零售） 电话：（010）88383994、63202643、68545874 全国各地新华书店和相关出版物销售网点
排　　版	北京万水电子信息有限公司
印　　刷	三河市鑫金马印装有限公司
规　　格	184mm×260mm　16 开本　19 印张　466 千字
版　　次	2008 年 6 月第 1 版　2008 年 6 月第 1 次印刷 2015 年 8 月第 2 版　2015 年 8 月第 1 次印刷
印　　数	0001—4000 册
定　　价	36.00 元

第二版前言

在信息化社会中，人们对计算机网络的依赖日益加强。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已成为当前主要的信息沟通方式之一，并且这种趋势还在不断地发展。尤其网络上各种新业务（如网上购物、网上炒股、视频会议、远程教育、电子商务、网络银行、数字图书馆等）的广泛应用，对网络信息的安全性提出了更高的要求。非法入侵、病毒施虐，重要数据被窃取或毁坏、网络系统损坏或瘫痪等，给政府和企业带来巨大的经济损失，也为网络的健康发展造成巨大的障碍。网络与信息安全问题已成为各国政府普遍关注的问题，网络安全与防护也成为网络信息技术领域的重要课题。

本书注重跟踪网络与信息安全领域内的最新研究成果，以基础理论、技术机制和应用实践相结合的方式对信息安全进行了分层次、有重点的阐述，使读者较全面地了解网络与信息安全领域内应研究的问题和相应的解决机制。全书共分 12 章，主要内容包括：网络安全概述、密码技术与应用、数字签名与身份认证技术、防火墙技术、入侵检测技术、网络病毒与防治、黑客常用的攻击技术、网络服务的安全、操作系统的安全、数据库系统的安全、电子商务安全和无线网络安全技术。

在本书的编写中，作者对第一版中的部分内容进行了修正，并增补了近年来密码学和网络信息安全领域广泛应用的一些新理论和新技术（如无线网络安全技术、移动安全支付技术等），使第二版的内容更丰富、技术更新颖、实用性更强，希望第二版的出版能给读者带来新的感受和帮助。

本书的出版，得到了许多专家、老师和同行的支持，在此，本人对支持、帮助和关心本书出版的广大读者表示感谢。特别感谢武汉软件职业学院的王路群教授、罗保山副教授对本书的支持。在本书的撰写过程中，参考了大量相关的著作和网站资料，在此向有关作者致谢！武汉轻工大学的汪军、樊昌秀、陈珂、彭正街、周浩、张佳、龚能武、袁操、李雅琴、吴海华、潘可、朱阿兰等老师为本书的出版做了部分工作，在此一并表示感谢！

随着网络与信息安全技术研究的深入和应用领域的延伸，网络与信息安全的内涵在不断地丰富和充实。由于编者水平有限，我们对这一领域的研究还有待深入，书中难免存在错误和不足之处，欢迎广大读者和专家提出批评改进意见。编者的电子邮件地址为：wyh@whpu.edu.cn。

编　者

2015 年 5 月

第一版前言

随着计算机网络技术的迅猛发展和网络信息系统的深入应用，信息网络的国际化和社会化使人类社会的生活方式发生了重大变化。网络化、数字化应用业务大量涌现，网上购物、网上炒股、视频会议、远程教育、电子政务、网络银行、数字图书馆等走进了我们的生活。而网络与信息系统的开放性和潜藏的商业、经济、军事利益给网络黑客、计算机犯罪人员、国外敌对势力和恐怖分子等创造了大量可乘之机，使网络与信息安全问题受到了前所未有的关注和重视。

本书重点讲述网络与信息安全技术问题，涵盖了网络安全的基本概念、密码技术、数字签名与身份认证技术、防火墙技术、入侵检测技术、病毒防治与黑客攻击技术、网站安全技术、数据库安全技术等方面的知识，力求从简洁、全面、前沿、深刻的视角分析网络与信息应用领域中存在的相关安全的问题、技术和方法。本书共分 11 章，第 1 章介绍网络安全的基本概念，概述了网络安全的目标、缺陷、发展历史和现状。第 2 章讲解密码技术的相关概念、网络加密方式、密码算法、密钥的管理和分发以及密码技术的应用。第 3 章讲述数字签名技术、CA 身份认证技术、数字证书的标准和使用。第 4 章介绍防火墙的概念和功能、防火墙管理的 TCP/IP 基础、防火墙的体系结构、防火墙的主要技术。第 5 章讲述入侵检测系统的基本概念、分类、分析方式、设置部署以及入侵检测系统的优缺点。第 6 章讲解计算机病毒的产生、种类和具体特征，计算机病毒的预防、检测和清除。第 7 章讲述黑客攻击的一些常用技术，包括端口扫描、特洛伊木马、拒绝服务攻击等。第 8 章介绍网络站点的安全基本知识，包括一些针对 Web、E-mail、DNS 站点的攻击手段及预防措施。第 9 章讲述操作系统的安全机制以及几种常见网络操作系统的安全。第 10 章讲述数据库安全系统特性、数据库安全的威胁、数据库的数据保护。第 11 章讲解电子交易的基本流程、SET 的基本原理与安全需求、SET 中的支付处理。

本书适合高等学校电子、计算机网络和信息安全专业或相近专业的学生使用，也可作为从事网络安全、网络管理、信息系统开发的科研人员和相关行业技术人员的参考书。

本书由吴煜煌负责全书的统稿定稿工作，主要由吴煜煌、汪军、阚君满编写，参加本书编写的还有李禹生、刘兵、欧阳峥峥、陈学文、高艳霞、蒋丽华、向云柱、李鸣、严华、李承犁、镇涛等。丰洪才教授审阅了全书，并提出了宝贵意见。另外，本书在编写过程中，得到了网络中心和计算机系领导的关系和支持，在此一并表示衷心的感谢。

由于网络与信息安全技术的发展非常快，本书的选材还有一些不尽如人意的地方，加上作者水平所限，书中难免存在不足之处，敬请读者批评指正。作者的电子邮件地址为：wyh@whpu.edu.cn。

编　者

2006 年 7 月

目　　录

第二版前言

第一版前言

第 1 章　网络安全概述 …… 1

学习目标 …… 1

1.1　网络安全的基本知识 …… 1

1.1.1　网络安全的基本概念 …… 1

1.1.2　网络安全目标 …… 3

1.1.3　网络安全模型 …… 4

1.1.4　网络安全策略 …… 5

1.2　网络安全类别 …… 8

1.2.1　物理安全 …… 8

1.2.2　逻辑安全 …… 8

1.2.3　操作系统安全 …… 9

1.2.4　连网安全 …… 9

1.3　网络安全威胁 …… 9

1.3.1　物理威胁 …… 9

1.3.2　系统漏洞威胁 …… 9

1.3.3　身份鉴别威胁 …… 10

1.3.4　病毒和黑客威胁 …… 10

1.4　网络安全标谁 …… 11

1.4.1　TCSEC 标准 …… 11

1.4.2　我国的安全标准 …… 12

本章小结 …… 13

习题一 …… 13

第 2 章　密码技术与应用 …… 14

学习目标 …… 14

2.1　密码技术概述 …… 14

2.1.1　密码学的发展概述 …… 14

2.1.2　密码系统 …… 15

2.1.3　密码体制分类 …… 16

2.2　对称密码体制 …… 17

2.2.1　古典密码 …… 17

2.2.2　DES 密码算法 …… 20

2.3　非对称密码体制 …… 27

2.3.1　RSA 密码算法 …… 27

2.3.2　ElGamal 密码算法 …… 30

2.4　密钥的管理和分发 …… 32

2.4.1　密钥管理 …… 32

2.4.2　保密密钥的分发 …… 33

2.5　密码技术的应用 …… 34

2.5.1　电子商务（E-business） …… 34

2.5.2　虚拟专用网（Virtual Private Network） …… 35

2.5.3　PGP（Pretty Good Privacy） …… 35

本章小结 …… 36

习题二 …… 36

第 3 章　数字签名与身份认证技术 …… 37

学习目标 …… 37

3.1　数字签名技术 …… 37

3.1.1　数字签名技术 …… 37

3.1.2　带加密的数字签名 …… 38

3.1.3　RSA 公钥签名技术 …… 40

3.1.4　数字签名的应用 …… 41

3.2　身份认证技术 …… 41

3.2.1　身份认证技术的概述 …… 41

3.2.2　身份认证技术的分类 …… 42

3.2.3　身份认证技术的应用 …… 45

3.3　数字证书与认证中心 …… 51

3.3.1　数字证书 …… 51

3.3.2　认证中心 …… 53

3.3.3　数字证书的使用 …… 55

3.4　Outlook Express 的操作实例 …… 58

本章小结 …… 62

习题三 …… 62

第 4 章　防火墙技术 …… 63
学习目标 …… 63
4.1　防火墙概述 …… 63
4.1.1　防火墙的概念 …… 63
4.1.2　防火墙的分类 …… 64
4.1.3　防火墙的基本功能 …… 65
4.1.4　防火墙的局限性 …… 66
4.2　防火墙的体系结构 …… 67
4.2.1　多宿主主机防火墙 …… 67
4.2.2　屏蔽主机型防火墙 …… 68
4.2.3　屏蔽子网型防火墙 …… 68
4.2.4　防火墙的各种变化和组合 …… 69
4.3　防火墙的主要技术 …… 71
4.3.1　包过滤技术 …… 71
4.3.2　代理技术 …… 74
4.3.3　状态包检查技术 …… 76
4.3.4　其他技术 …… 79
4.4　常用防火墙功能介绍 …… 82
4.4.1　CheckPoint NG 防火墙 …… 83
4.4.2　Cisco PIX 防火墙 …… 84
4.4.3　NetScreen 防火墙 …… 84
4.4.4　其他防火墙 …… 85
本章小结 …… 85
习题四 …… 85
第 5 章　入侵检测技术 …… 87
学习目标 …… 87
5.1　入侵检测概述 …… 87
5.1.1　基本概念 …… 87
5.1.2　入侵检测系统的结构 …… 88
5.2　入侵检测系统分类 …… 89
5.2.1　基于主机的入侵检测系统 …… 89
5.2.2　基于网络的入侵检测系统 …… 91
5.2.3　基于内核的入侵检测系统 …… 93
5.2.4　两种入侵检测系统的结合运用 …… 93
5.2.5　分布式的入侵检测系统 …… 93
5.3　入侵检测系统的分析方式 …… 94
5.3.1　异常检测技术——基于行为的检测 …… 94
5.3.2　误用检测技术——基于知识的检测 …… 97
5.3.3　异常检测技术和误用检测技术的比较 …… 98
5.3.4　其他入侵检测技术的研究 …… 99
5.4　入侵检测系统的设置 …… 100
5.5　入侵检测系统的部署 …… 101
5.5.1　基于网络入侵检测系统的部署 …… 101
5.5.2　基于主机入侵检测系统的部署 …… 103
5.5.3　报警策略 …… 103
5.6　入侵检测系统的优点与局限性 …… 103
5.6.1　入侵检测系统的优点 …… 104
5.6.2　入侵检测系统的局限性 …… 104
本章小结 …… 105
习题五 …… 105
第 6 章　网络病毒与防治 …… 106
学习目标 …… 106
6.1　计算机病毒概述 …… 106
6.1.1　计算机病毒的概念 …… 106
6.1.2　计算机病毒的发展历史 …… 107
6.1.3　计算机病毒的特征 …… 107
6.1.4　计算机病毒的分类 …… 109
6.2　计算机病毒的工作原理 …… 110
6.2.1　计算机病毒的组成 …… 110
6.2.2　计算机病毒的运作过程 …… 111
6.2.3　计算机病毒的引导过程 …… 111
6.2.4　计算机病毒的触发机制 …… 111
6.3　病毒的防范与清除 …… 112
6.3.1　病毒防范概述 …… 112
6.3.2　防病毒技术 …… 113
6.3.3　计算机病毒的清除 …… 116
6.4　网络病毒的实例 …… 118
6.4.1　CIH 病毒 …… 119
6.4.2　宏病毒 …… 120
6.4.3　梅丽莎病毒 …… 120
6.4.4　熊猫烧香病毒 …… 122
本章小结 …… 124
习题六 …… 124
第 7 章　黑客常用的攻击技术 …… 125
学习目标 …… 125
7.1　黑客攻击的过程和类型 …… 125
7.1.1　黑客攻击的一般步骤 …… 125

7.1.2 黑客攻击的类型 …… 126
7.2 端口扫描 …… 127
7.2.1 端口的基本概念 …… 127
7.2.2 端口扫描的原理 …… 128
7.2.3 常用的端口扫描技术 …… 129
7.2.4 常见的扫描工具及典型应用 …… 131
7.3 网络监听 …… 136
7.3.1 网络监听概述 …… 136
7.3.2 网络监听的原理 …… 136
7.3.3 网络监听的检测与防范 …… 137
7.3.4 网络监听工具 …… 138
7.4 口令破解 …… 141
7.4.1 口令破解方法 …… 142
7.4.2 口令破解机制 …… 143
7.4.3 安全口令的设置原则 …… 143
7.5 特洛伊木马 …… 144
7.5.1 特洛伊木马概述 …… 144
7.5.2 特洛伊木马的原理 …… 144
7.5.3 特洛伊木马的种类 …… 146
7.5.4 特洛伊木马的检测与清除 …… 147
7.5.5 特洛伊木马防范 …… 150
7.6 缓冲区溢出 …… 150
7.6.1 缓冲区溢出概述 …… 150
7.6.2 缓冲区溢出的攻击方式 …… 151
7.6.3 缓冲区溢出的防范 …… 153
7.7 拒绝服务攻击 …… 154
7.7.1 拒绝服务攻击概述及原理 …… 154
7.7.2 DoS 的攻击方法与防范措施 …… 155
7.7.3 分布式拒绝服务概念及原理 …… 158
7.7.4 DDoS 攻击方法、检测与防范 …… 159
7.8 ARP 欺骗 …… 162
7.8.1 ARP 欺骗概述 …… 162
7.8.2 ARP 欺骗攻击原理 …… 162
7.8.3 ARP 攻击防护 …… 163
本章小结 …… 163
习题七 …… 164
第 8 章 网络服务的安全 …… 165
学习目标 …… 165
8.1 网络服务概述 …… 165
8.1.1 网络服务的类型 …… 165
8.1.2 网络服务的安全隐患 …… 166
8.2 Web 服务的安全 …… 167
8.2.1 Web 面临的威胁 …… 167
8.2.2 Web 攻击手段 …… 168
8.2.3 Web 安全体系 …… 173
8.3 E-mail 服务的安全 …… 175
8.3.1 E-mail 服务的工作原理 …… 176
8.3.2 E-mail 服务攻击方法 …… 176
8.3.3 E-mail 服务安全设置 …… 178
8.4 FTP 服务的安全 …… 178
8.4.1 FTP 服务的工作原理 …… 179
8.4.2 FTP 服务的安全威胁 …… 179
8.4.3 FTP 服务的安全防护 …… 180
8.5 DNS 服务的安全 …… 181
8.5.1 DNS 服务的工作原理 …… 181
8.5.2 DNS 服务的安全威胁 …… 182
8.5.3 DNS 服务的安全防护 …… 183
本章小结 …… 184
习题八 …… 184
第 9 章 操作系统的安全 …… 186
学习目标 …… 186
9.1 操作系统安全概述 …… 186
9.1.1 操作系统安全的重要性 …… 186
9.1.2 操作系统的安全等级 …… 188
9.1.3 操作系统安全的设计原则 …… 189
9.1.4 操作系统的安全机制 …… 190
9.2 Windows 7 系统的安全 …… 193
9.2.1 Windows 7 的登录控制 …… 193
9.2.2 Windows 7 用户账号控制（UAC） 196
9.2.3 家长控制 …… 202
9.2.4 Windows Defender 恶意软件防护 …… 203
9.2.5 AppLocker 应用程序控制策略 …… 206
9.3 UNIX 系统的安全 …… 209
9.3.1 UNIX 的用户账号与口令安全 …… 209
9.3.2 UNIX 的文件访问控制 …… 213
9.3.3 UNIX 的安全管理 …… 215
9.3.4 UNIX 的安全审计 …… 216
本章小结 …… 217

习题九 …… 217
第 10 章　数据库系统的安全 …… 219
学习目标 …… 219
10.1　数据库安全概述 …… 219
10.1.1　数据库系统简介 …… 219
10.1.2　数据库系统安全的含义 …… 220
10.1.3　数据库的安全威胁 …… 221
10.1.4　数据库系统的安全性 …… 222
10.2　数据库系统的安全技术 …… 223
10.2.1　用户标识与鉴别 …… 223
10.2.2　存取控制 …… 224
10.2.3　数据库加密 …… 225
10.2.4　数据库的并发控制 …… 228
10.2.5　数据库的安全审计 …… 231
10.3　数据备份和恢复 …… 231
10.3.1　数据备份 …… 232
10.3.2　数据恢复 …… 235
本章小结 …… 238
习题十 …… 238
第 11 章　电子商务安全 …… 239
学习目标 …… 239
11.1　电子商务安全概述 …… 239
11.1.1　电子商务简介 …… 239
11.1.2　电子商务系统的结构 …… 240
11.1.3　电子商务的安全需求 …… 240
11.1.4　电子商务的安全体系结构 …… 242
11.2　电子商务中的安全机制 …… 242
11.2.1　加密技术 …… 242
11.2.2　认证技术 …… 242
11.2.3　网络安全技术 …… 245
11.2.4　电子商务的安全交易标准 …… 245
11.3　电子商务中的支付系统 …… 245
11.3.1　电子支付系统简介 …… 245
11.3.2　电子信用卡 …… 246
11.3.3　电子现金 …… 248
11.3.4　电子支票 …… 249
11.3.5　移动支付 …… 250
11.4　电子商务安全协议 …… 256
11.4.1　安全套接层协议 …… 257
11.4.2　安全电子交易协议 …… 260
本章小结 …… 266
习题十一 …… 267
第 12 章　无线网络安全技术 …… 268
学习目标 …… 268
12.1　无线网络概述 …… 268
12.1.1　无线网络的概念 …… 268
12.1.2　无线网络的分类 …… 268
12.1.3　无线网络的安全特点 …… 269
12.1.4　无线网络的安全隐患和配置要点 …… 269
12.2　无线局域网的安全 …… 271
12.2.1　访问点安全 …… 271
12.2.2　无线局域网安全技术 …… 272
12.3　无线广域网的安全 …… 275
12.3.1　无线广域网技术 …… 275
12.3.2　无线设备与数据安全 …… 276
12.3.3　无线蜂窝网络技术 …… 277
12.3.4　无线蜂窝网络的安全 …… 279
12.4　无线 Ad Hoc 网络的安全 …… 285
12.4.1　无线 Ad Hoc 网络概述 …… 285
12.4.2　无线 Ad Hoc 网络的安全威胁 …… 285
12.4.3　无线 Ad Hoc 网络的安全机制 …… 286
12.5　传感器网络的安全 …… 290
12.5.1　传感器网络概述 …… 290
12.5.2　传感器网络的安全威胁 …… 290
12.5.3　传感器网络的安全机制 …… 291
本章小结 …… 293
习题十二 …… 293
参考文献 …… 295

第 1 章　网络安全概述

随着网络与信息技术广泛应用于社会经济、政治、军事、个人生活等各个领域，网络化、信息化已成为现代社会的一个重要特征，如何确保计算机网络与信息的安全变得非常重要。本章主要介绍网络安全的基本知识、网络安全类别、网络安全威胁、网络安全标准等内容。通过对本章的学习，读者应该掌握以下主要内容：

- 网络安全的含义、目标
- 网络安全的模型、策略
- 网络安全的类别
- 网络安全的威胁
- 网络安全的标准

1.1　网络安全的基本知识

1.1.1　网络安全的基本概念

国际标准化组织（ISO）对计算机系统安全的定义是：为数据处理系统建立和采用的技术和管理的安全保护，保护计算机硬件、软件和数据不因偶然或恶意的原因遭到破坏、更改和泄露。由此，可以将计算机网络的安全理解为：通过采用各种技术和管理措施，使网络系统正常运行，从而确保网络数据的机密性、完整性和可用性。所以，建立网络安全保护措施的目的是确保经过网络传输和交换的数据不会发生增加、修改、丢失和泄露等。从广义上来说，凡是涉及到网络上信息的可靠性、可用性、保密性、完整性、不可否认性和可控性的相关技术和理论都是网络安全所要研究的领域。网络安全从其本质上来讲就是网络上的信息安全。

1. 信息安全

信息安全已经历了漫长的发展过程。从某种意义上说，从人类有信息交流开始就涉及信息的安全问题。从古代烽火传信到今天的通信网，只要存在信息交流，就可能存在信息欺骗。信息安全的概念也是与时俱进的，过去是通信保密（COMSEC），昨天是信息安全（INFOSEC），而今天以至于今后是信息保障（IA，Information Assurance）。

（1）通信保密。信息安全的初级阶段，人们似乎更关注信息通信的机密性。通常采用一些简单的替代或置换来保护信息。这些变换是密码学的雏形。这一阶段发展了很多密码算法，但基本的方法都是将字母编号后进行平移、旋转、置换、扩展等变换。此外，还发展了密码分析和破译方法。

（2）信息安全。随着数学、计算机和通信技术的发展，信息的处理能力和传输能力大大

提高，靠传统的密码变换已不能满足信息化的要求。因此，信息安全的发展速度也在加速，出现了现代密码理论、计算机安全和通信安全的新理论和新技术。这一阶段的信息安全包括在信息系统的物理层、运行层，以及对信息自身的保护（数据层）及攻击（内容层）的层面上，所反映出的对信息自身与信息系统在机密性、可用性与真实性方面的保护与攻击等内容。

（3）信息保障。目前，国际研究前沿已将信息安全上升到信息保障的高度，提出了计算环境安全、通信网安全、边界安全及安全支撑环境和条件的概念，并开始研究信息网络的生存性等课题。美国国家安全局（NSA）在 IATFV3.1 中提出了深度防御（Defense-in-Deepth）的概念，把信息安全上升到信息保障的高度，并提出了人（People）、技术（Technology）、操作（Operation）三方面并举的核心策略，基于这个核心，IATF 定义了各种环境下的安全需求和技术方案的框架，对现有的信息安全技术提出了许多新的挑战。

总之，信息安全还没有形成完整的学科概念，但其发展速度正在加快，信息安全研究人员正在增加，信息安全作为独立产业的形态开始显现，主管部门也在加大管理力度，并加紧制定信息安全法律法规。信息安全学科正应时代需要发展和完善。

2. 网络安全

过去的信息安全主要是通信保密，通信发展到今天，在以分布系统网络化的前提下，互联网的触角延伸到人们生产、生活的每个角落，由此引出了网络安全这一新课题。

网络安全在不同的环境和应用中会得到不同的解释。对于用户（个人、企业等）而言，网络安全意味着涉及个人隐私和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、抵赖等手段对用户的隐私和利益造成侵犯和损害；对于网络运行和管理者而言，网络安全意味着对本地网络信息的访问、读写等操作进行保护和控制，避免出现“陷门”、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；对安全保密部门而言，网络安全更侧重于对非法的、有害的或涉密的信息进行过滤和防堵，避免其通过网络泄漏，同时避免由于这类信息的泄密而对社会产生危害，对国家造成重大损失。

一般可以认为网络安全包括物理安全、运行安全和数据安全三个层次，它们涵盖的范围如图 1-1 所示。

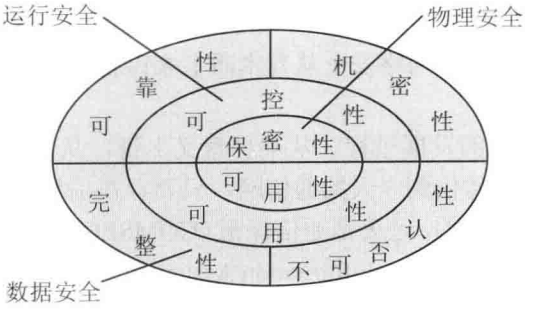

图 1-1 网络安全涵盖的范围

网络安全与其所保护的信息对象相关，本质是在信息的安全期内保证其在网络上流动时或静态存放时不被非授权用户非法访问，但授权用户却可以访问。显然，网络安全、信息安全和系统安全的研究领域是相互交叉和紧密联系的。

网络安全的含义是指通过各种计算机、网络、密码技术和信息安全技术、网络控制技术，保护网络中传输、交换、处理和存储的信息的可靠性、可用性、保密性、完整性、不可否认性和可控性。

3. 网络安全观

网络安全的特征决定了网络安全本身是一个不断变化、快速更新的领域，也意味着人们对于网络安全领域的投资是长期的行为。但现在的问题是，到底该如何利用技术来保护计算机和网络不受安全的威胁。许多用户在应用计算机接入网络时，往往存在侥幸心理，不会将安全作为首要问题考虑，希望其安全措施能永保安全。

首先，网络安全是网络动态发展的问题。从发展趋势来看，信息网络的安全日益显示出其重要性。不同国家、地区之间的政治、军事、文化等冲突也动辄引发一轮又一轮的网络攻击，如中美、中日之间都曾多次爆发大规模的、有组织的网络攻击。这些有组织、有目的的网络攻击行为一方面提醒了网络建设者要始终把安全问题放在首位，另一方面也将大大促进网络攻击技术的发展。

其次，网络安全实施是一个系统工程。安全问题涉及身份鉴别、访问控制、数据机密、数据完整性、抗抵赖、审计、可用性和可靠性等多种基本的安全服务，涉及 ISO/OSI 所有的七个协议层次（物理层、链路层、网络层、传输层、会话层、表示层和应用层），覆盖了信息网络中物理环境、通信平台、网络平台、主机平台和应用平台等多个系统单元。因此，这是一个立体的、多方位、多层次的系统问题，在规划、设计、实施信息网络的安全系统时也必须用系统工程的方法论来考虑。

最后，网络安全实施是一个社会工程。在信息网络中，用户接口是至关重要的。在采取了各种复杂的安全技术之后，如果系统的最终用户没有足够的安全意识和安全常识，不能正确应用各项安全措施，那么其后果要么是安全系统不能工作，影响信息网络的正常运转，要么是安全系统演出空城计，不能起实际的作用（如在一个安全系统中使用简单的用户密码）。因此，在安全系统建设工程中，必须充分重视用户的安全，加强对用户安全意识的培训，加强安全常识的普及，加强安全系统的使用培训。

所以说，网络安全是一个动态发展的系统工程和社会工程，需要长期、持久的巨大财力、物力、人力的投入，需要从组织、管理等方面采取强有力的措施，才能确保网络在信息的大洋中永远坚固、安全、可靠。

1.1.2　网络安全目标

网络安全的目标主要表现在系统的可靠性、可用性、保密性、完整性、不可否认性和可控性等方面。

1. 可靠性

可靠性是网络信息系统能够在规定条件下和规定时间内实现规定功能的特性。可靠性是系统安全的最基本要求之一，是所有网络信息系统的建设和运行目标。可靠性用于保证系统在人为或者随机性破坏下的安全程度。

2. 可用性

可用性是网络信息可被授权实体访问并按需求使用的特性。可用性是网络信息系统面向用户的安全性能。可用性应满足身份识别与确认、访问控制、业务流控制、路由选择控制、审计跟踪等要求。

3. 保密性

保密性是网络信息不被泄露给非授权的用户、实体或过程，或供其利用的特性。也就是说，防止信息泄漏给非授权的个人或实体，信息只为授权用户使用。保密性主要通过信息加密、身份认证、访问控制、安全通信协议等技术实现，它是在可靠性和可用性的基础之上，保障网络信息安全的重要手段。

4. 完整性

完整性是网络信息未经授权不能进行改变的特性，即网络信息在存储或传输过程中保持不被偶然或蓄意地删除、修改、伪造、乱序、重放、插入的特性。完整性是一种面向信息的安全性，它要求保持信息的原样，即信息的正确生成、存储和传输。

5. 不可否认性

不可否认性也称作抗否认性，在网络信息系统的信息交互过程中，确信参与者的真实同一性，即所有参与者都不可能否认或抵赖曾经完成的操作和承诺。利用信息源证据防止发信方不真实地否认已发送信息，利用递交接收证据防止收信方事后否认已经接收的信息。

6. 可控性

可控性是对网络信息的传播及内容具有控制能力的特性。保障系统依据授权提供服务，使系统在任何时候都不被非授权人使用，对黑客入侵、口令攻击、用户权限非法提升、资源非法使用等采取防范措施。

1.1.3 网络安全模型

网络安全模型是动态网络安全过程的抽象描述。通过对安全模型的研究，了解安全动态过程的构成因素，是构建合理而实用的安全策略体系的前提之一。为了达到安全防范的目标，需要建立合理的网络安全模型，以指导网络安全工作的部署和管理。目前，在网络安全领域存在较多的网络安全模型，下面介绍常见的 PDRR 和 PPDR 模型。

1. PDRR 安全模型

PDRR 是美国国防部提出的常见安全模型。它概括了网络安全的整个环节，即防护（Protection）、检测（Detection）、响应（Reaction）、恢复（Restore）。这四个部分构成了一个动态的信息安全周期，如图 1-2 所示。

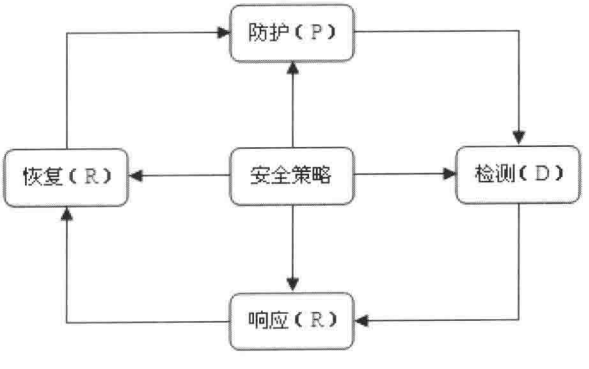

图 1-2 PDRR 安全模型

（1）防护。防护是 PDRR 模型最重要的部分。防护是预先阻止攻击可能发生的条件产生，

让攻击者无法顺利地入侵。防护可以抵御大多数的入侵事件，它包括缺陷扫描、访问控制及防火墙、数据加密、鉴别等。

（2）检测。检测是 PDRR 模型的第二个环节。通常采用入侵检测系统（IDS）来检测系统漏洞和缺陷，增加系统的安全性能，从而消除攻击和入侵的条件。检测根据入侵事件的特征进行。

（3）响应。响应是 PDRR 模型的第三个环节。响应就是已知一个入侵事件发生之后进行的处理过程。通过针对入侵事件的警报进行响应通告，从而采取一定的措施来实现安全系统的补救过程。

（4）恢复。恢复是 PDRR 模型中的最后一个环节。恢复是指事件发生后进行初始化恢复的过程。通常，用户通过系统的备份和还原来进行恢复，然后安装系统对应的补丁程序，实现安全漏洞的修复等。

2. PPDR 安全模型

PPDR 是美国国际互联网安全系统公司（ISS）提出的可适应网络安全模型，它包括策略（Policy）、保护（Protection）、检测（Detection）、响应（Response）四个部分。PPDR 模型如图 1-3 所示。

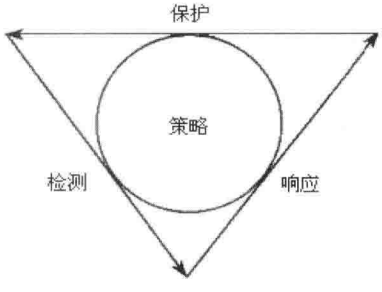

图 1-3　PPDR 安全模型

（1）策略。PPDR 安全模型的核心是安全策略，所有的防护、检测、响应都是依据安全策略实施的，安全策略为安全管理提供管理方向和支持手段。策略体系的建立包括安全策略的制定、评估、执行等。

（2）保护。保护就是采用一切手段保护信息系统的保密性、完整性、可用性、可控性和不可否认性，应该依据不同等级的系统安全要求来完善系统的安全功能、安全机制。保护通常采用身份认证、防火墙、客户端软件、加密等传统的安全技术来实现。

（3）检测。检测是 PPDR 模型中非常重要的环节，检测是进行动态响应和动态保护的依据，同时强制网络落实安全策略，检测设备不间断地检测、监控网络和系统，及时发现网络中的威胁和存在的弱点，通过循环的反馈来及时做出响应。网络的安全风险是无时不在的，检测的对象主要针对系统自身的脆弱性及外部威胁。

（4）响应。响应是指在系统检测到安全漏洞后做出的处理，它在 PPDR 安全系统中占有重要的位置，是解决潜在安全问题最有效的方法。

1.1.4　网络安全策略

安全策略是指在某个安全区域内，所有与安全活动相关的一套规则，这些规则由此安全区域内所设立的一个权威建立。网络安全策略包括对企业的各种网络服务的安全层次和用户的

权限进行分类，确定管理员的安全职责，如何实施安全故障处理、网络拓扑结构、入侵和攻击的防御和检测、备份和灾难恢复等内容。主要涉及四个大的方面：物理安全策略、访问控制策略、信息加密策略、安全管理策略。

1. 物理安全策略

制定物理安全策略的目的是保护路由器、交换机、工作站、各种网络服务器、打印机等硬件实体和通信链路免受自然灾害、人为破坏和搭线窃听攻击；验证用户的身份和使用权限、防止用户越权操作；确保网络设备有一个良好的电磁兼容工作环境；建立完备的机房安全管理制度，妥善保管备份磁带和文档资料；防止非法人员进入机房进行偷窃和破坏活动。

2. 访问控制策略

访问控制是网络安全防范和保护的主要策略，它的主要任务是保证网络资源不被非法使用和非法访问。它也是维护网络系统安全、保护网络资源的重要手段。各种安全策略必须相互配合才能真正起到保护作用，但访问控制可以说是保证网络安全最重要的核心策略之一，下面分别讲述各种访问控制策略。

（1）入网访问控制。入网访问控制为网络访问提供了第一层访问控制。它控制哪些用户能够登录到服务器并获取网络资源，控制准许用户入网的时间和准许他们在哪台工作站入网。用户的入网访问控制可分为三个步骤：①用户名的识别与验证；②用户口令的识别与验证；③用户账号的缺省限制检查。三道关卡中只要任何一关未通过，该用户便不能进入该网络。

对网络用户的用户名和口令进行验证是防止非法访问的第一道防线。用户注册时首先输入用户名和口令，服务器将验证所输入的用户名是否合法。如果验证合法，才继续验证用户输入的口令，否则用户将被拒于网络之外。用户的口令是用户入网的关键所在，为保证口令的安全性，用户口令不能显示在显示屏上，口令长度应不少于 6 个字符，口令字符最好是数字、字母和其他字符的混合，用户口令必须经过加密，经过加密的口令，即使是系统管理员也难以得到它。用户还可采用一次性用户口令，也可用便携式验证器（如智能卡）来验证用户的身份。

网络管理员应该可以控制和限制普通用户的账号使用、访问网络的时间、访问方式。用户名或用户账号是所有计算机系统中最基本的安全形式，用户账号应只有系统管理员才能建立。用户口令应是每一位用户访问网络所必须提交的“证件”，用户可以修改自己的口令，但系统管理员应该可以控制口令的以下几个方面的限制：最小口令长度、强制修改口令的时间间隔、口令的唯一性、口令过期失效后允许入网的宽限次数。

用户名和口令验证有效之后，再进一步履行用户账号的缺省限制检查。网络应能控制用户登录入网的站点、限制用户入网的时间、限制用户入网的工作站数量。当用户将交费网络的访问“资费”用尽时，网络还应能对用户的账号加以限制。网络应对所有用户的访问进行审计。如果多次输入口令不正确，则认为是非法用户的入侵，应给出报警信息。

（2）网络的权限控制。网络的权限控制是针对网络非法操作所提出的一种安全保护措施。用户和用户组被赋予一定的权限。网络控制用户和用户组可以访问哪些目录、子目录、文件和其他资源。可以指定用户对这些文件、目录、设备能够执行哪些操作。可以根据访问权限将用户分为以下几类：①特殊用户（即系统管理员）；②一般用户，系统管理员根据他们的实际需要为他们分配操作权限；③审计用户，负责网络的安全控制与资源使用情况的审计。用户对网络资源的访问权限可以用一个访问控制表来描述。

（3）目录级安全控制。网络应允许控制用户对目录、文件、设备的访问。用户在目录一级

指定的权限对所有文件和子目录有效，用户还可进一步指定对目录下的子目录和文件的权限。对目录和文件的访问权限一般有八种：系统管理员权限（Supervisor）、读权限（Read）、写权限（Write）、创建权限（Create）、删除权限（Erase）、修改权限（Modify）、文件查找权限（File Scan）、存取控制权限（Access Control）。一个网络系统管理员应当为用户指定适当的访问权限，这些访问权限控制着用户对服务器的访问。八种访问权限的有效组合可以让用户有效地完成工作，同时又能有效地控制用户对服务器资源的访问，从而加强了网络和服务器的安全性。

（4）属性安全控制。当用文件、目录和网络设备时，网络系统管理员应给文件、目录等指定访问属性。属性安全控制可以将给定的属性与网络服务器的文件、目录和网络设备联系起来。属性安全在权限安全的基础上提供更进一步的安全性。网络上的资源都应预先标出一组安全属性来控制以下几个方面的权限：向某个文件写数据、拷贝一个文件、删除目录或文件、查看目录和文件、执行文件、隐含文件、共享、系统属性等。网络的属性可以保护重要的目录和文件，防止用户对目录和文件的误删除、执行修改、显示等。

（5）网络服务器安全控制。网络允许在服务器控制台上执行一系列操作。用户使用控制台可以装载和卸载模块，可以安装和删除软件等。网络服务器的安全控制包括可以设置口令锁定服务器控制台，以防止非法用户修改、删除重要信息或破坏数据，可以设定服务器登录时间限制、非法访问者检测和关闭的时间间隔。

（6）网络监测和锁定控制。网络管理员应对网络实施监控，服务器应记录用户对网络资源的访问，对非法的网络访问，服务器应以图形、文字或声音等形式报警，以引起网络管理员的注意。如果非法用户试图进入网络，网络服务器应自动记录企图尝试进入网络的次数，如果非法访问的次数达到设定数值，那么该账户将被自动锁定。

（7）网络端口和结点的安全控制。网络中服务器的端口往往使用自动回呼设备、静默调制解调器加以保护，并以加密的形式来识别结点的身份。自动回呼设备用于防止假冒合法用户，静默调制解调器用于防范黑客的自动拨号程序对计算机进行攻击。网络还经常对服务器端和用户端采取控制，用户必须携带证实身份的验证器（如智能卡、磁卡、安全密码发生器），在对用户的身份进行验证之后，才允许其进入用户端。然后，用户端和服务器端再进行相互验证。

（8）防火墙控制。防火墙是一种保护计算机网络安全的技术性措施，它是一个用以阻止黑客访问某个机构网络的屏障，是控制进/出两个方向通信的门槛。在网络边界上通过建立起来的相应网络通信监控系统来隔离内部网络和外部网络，以阻挡外部网络的非法侵入。

3. 信息加密策略

信息加密的目的是保护网内的数据、文件、口令和控制信息，保护网络会话的完整性。网络加密可以在链路层、网络层、应用层等进行，分别对应网络体系结构中的不同层次形成加密通信通道。用户可以根据不同的需要来选择适当的加密方式。

加密过程由加密算法来具体实施。据不完全统计，到目前为止，已经公开发表的各种加密算法多达数百种。如果按照收发双方使用的密钥是否相同来分类，可以将这些加密算法分为对称密码算法和非对称密码算法。

在对称密码中，加密和解密使用相同的密钥。比较著名的对称密码算法有美国的 DES 及其各种变形，欧洲的 DEA、RC4、RC5 以及以代换密码和转轮密码为代表的古典密码等。对称密码的优点是有很强的保密强度，且能经受住时间的检验和攻击，但其密钥必须通过安全的途径传送。因此，其密钥管理成为系统安全的重要因素。

非对称密码算法中，加密和解密使用的密钥互不相同，而且很难从加密密钥推导出解密密钥。比较著名的非对称密码算法有 RSA、Diffe-Hellman、LUC、Rabin 等，其中最有影响的公钥密码算法是 RSA。非对称密码的优点是可以适应网络的开放性要求，且密钥管理问题也较为简单，可方便地实现数字签名和验证。但其算法复杂，加密数据的速率较低。

针对两种密码体系的特点，一般的实际应用系统中都采用两类密码算法进行组合，对称密码算法加密长消息，非对称密码算法加密短消息。比如：用对称密码算法来加密数据，用非对称密码算法来加密对称密码算法所使用的密钥，这样既解决了对称密码算法密钥管理的问题，又解决了非对称密码算法加密速度的问题。现在流行的 PGP 和 SSL 等加密技术就是将对称密码算法和非对称密码算法结合在一起使用，利用 DES 或 IDEA 来加密信息，而采用 RSA 来传递会话密钥。因此，信息加密是实现网络安全的最有效技术之一。

4. 安全管理策略

安全与方便往往是相互矛盾的。有时虽然知道自己网络中存在的安全漏洞以及可能招致的攻击，但是出于管理协调方面的问题而无法更正。因为管理使用一个网络，包括用户数据更新管理、路由政策管理、数据流量统计管理、新服务开发管理、域名和地址管理等，网络安全管理只是其中的一部分，并且在服务层次上，处于对其他管理提供服务的地位上。这样，在与其他管理服务存在冲突时，网络安全往往需要做出让步。因此，制定一个好的安全管理策略，协调好安全管理与其他网络管理业务、安全管理与网络性能之间的关系，对于确保网络安全、可靠地运行是必不可少的。

网络的安全管理策略包括：①确定安全管理等级和安全管理范围；②制订有关网络操作使用规程和人员出入机房管理制度；③制定网络系统的维护制度和应急措施等。安全管理的落实是实现网络安全的关键。

1.2 网络安全类别

1.2.1 物理安全

物理安全指网络系统中相关设备的物理保护措施是使用物理隔离设备，物理隔离设备的作用是使网络之间无连接的物理途径，这样，内网的信息就不可能外泄。

在确保网络物理安全的措施中，目前比较流行的是采用物理隔离卡。物理隔离卡使用双硬盘物理隔离技术，隔离器与主板之间无数据交换途径，真正实现了网络隔离和数据隔离。内网和外网的切换通过手动物理开关来实现，且只能由用户自己操作，任何通过网络或运行软件的操作方式都无效，不存在软件操作隐患。

另外，在网络管理中建立一套严格的安全制度非常必要，如做好防盗、防火措施。在非常机密的网络环境下做好网络信息的屏蔽工作也非常必要，例如在无线网络环境中，为防止信息被窃取，在网络中安装屏蔽层等。

1.2.2 逻辑安全

逻辑安全指的是通过软操作方式来实现网络安全的措施，通常指的是用户通过安装杀毒软件、系统补丁，关闭服务、端口，加密等多种方式实现网络安全的过程。逻辑安全包括信息