21世纪 高等学校电子信息类专业规划教材

网络安全技术基础

周海刚 主 编
邱正伦 石爱军 扶树刚 副主编

清华大学出版社
http://www.tup.tsinghua.edu.cn
北京交通大学出版社
http://press.bjtu.edu.cn

21世纪高等学校电子信息类专业规划教材

网络安全技术基础

周海刚　**主编**

邱正伦　石爱军　扶树刚　**副主编**

清华大学出版社

北京交通大学出版社

·北京·

内 容 提 要

网络信息系统将成为21世纪人类社会运转的基础，网络信息安全将是信息社会正常运转的保证。本书在内容安排上首先介绍了信息安全和网络安全的基本概念和PDRR安全模型，然后详细地论述网络信息安全的核心基础理论——密码技术及其应用。根据PDRR模型，本书对网络防护的“保护”、“检测”、“响应”、“恢复”等几个方面进行了详细的论述，包括服务器的安全管理、路由器和防火墙技术、数据库安全、入侵检测、应急响应和系统恢复以及网络安全增强的技术。最后，从较为宏观的角度讨论信息保障和信息战，这是网络安全发展的最新阶段。本书可以作为网络安全专业、计算机专业、信息工程专业或相近专业的大专、本科和研究生的教科书，也可以作为从事网络安全领域的科技人员与信息系统安全管理员的参考书。

图书在版编目（CIP）数据

网络安全技术基础/周海刚主编. —北京：清华大学出版社；北京交通大学出版社，2004.8
（21世纪高等学校电子信息类专业规划教材）
ISBN 7-81082-394-9

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

中国版本图书馆CIP数据核字（2004）第085625号

责任编辑：陈文诠
出 版 者：清华大学出版社　邮编：100084　电话：010-62776969
　　北京交通大学出版社　邮编：100044　电话：010-51686045，62237564
印 刷 者：北京鑫海金澳胶印有限公司
发 行 者：新华书店总店北京发行所
开　本：185×260　印张：18　字数：440千字
版　次：2004年9月第1版　2004年9月第1次印刷
书　号：ISBN 7-81082-394-9/TP·145
印　数：1~5000册　定价：24.00元

前　言

近年来，Internet 中所发生的网络攻击事件越来越频繁，网络黑客的手段越来越高级，世界各国在网络攻击事件中的损失也越来越严重。为此，世界各国都投入了大量的资金和人员进行网络攻击和网络防护技术的研究。世界各国在积极开展网络攻击和防护技术研究的同时，网络黑客们也在不停地制造着网络入侵事件。1988 年 11 月 3 日这一天被称为“黑色的星期四”，一个美国年轻人 Robert Morris 把一个“蠕虫”程序放到了 Internet 上，导致了上千台网上机器瘫痪。这个称为“Morris 蠕虫”程序的出现改变了许多人对 Internet 安全性的看法，引起人们对计算机网络安全问题的重视。20 世纪 90 年代以来，Internet 走向商业化，上网计算机数量急剧增加，网络“黑客”与“入侵者”的非法活动呈猖獗趋势。人们发现网络安全问题无法仅用数据加密技术完全加以解决，还需要解决硬件系统、操作系统、网络、数据库系统和应用系统的整体安全问题，信息安全问题也就进入了网络信息安全阶段。进入 21 世纪后，各国对信息安全的重要性与作用有更高地认识，美国首先提出了信息保障的概念，提出了防护、检测、反应与恢复（PDRR）模型，使信息安全进入主动防御阶段。

最近几年来的网络攻击手段也开始从单一型向综合性转变：2000 年 2 月发生的攻击 Yahoo!、eBay、CNN 等站点的分布式拒绝服务攻击就采用了缓冲区溢出、特洛伊木马、口令攻击及一般拒绝服务的综合性攻击；2001 年出现的对整个 Internet 世界造成恐慌的“红色代码”及其变种“红色代码Ⅱ”网络病毒，以及 2003 年出现的“冲击波”和“震荡波”病毒则综合了蠕虫病毒、特洛依木马和缓冲区溢出等攻击手段。网络攻击的方式和方法也经历了从早期的粗糙、单一的攻击方法发展到今天的精致、综合的攻击方法的过程。早期主要的攻击方法以口令破解、洪泛式拒绝服务和特洛伊木马为主；20 世纪 90 年代开始兴起缓冲区溢出、网络信息探测和网络漏洞扫描攻击；近几年出现了综合各种网络攻击手段的网络欺骗攻击和分布式拒绝服务攻击。

面对网络攻击事件的频频发生和网络攻击手段的日益强大，我们需要了解网络攻击的方式和方法，更有必要对网络防护所涉及的网络安全技术进行深入研究，这样我们才能在当前这个不安全的网络中保护自己。

本书出版的目的是用作网络安全专业或相近专业的教材，通过对本课程的学习，将让学生全面了解网络安全的知识和网络空间中进行信息对抗的技术与知识。在内容选择上既考虑实时性（安全领域中的最新发展），也考虑系统性与理论性，同时还注重了实用性。

本书重点是讨论计算机网络中的信息安全问题与实现信息安全的措施。为了让读者了解各种安全威胁的严重性及各种安全防护措施的作用，也介绍了一些网络黑客与入侵者常用的网络攻击手段。了解这些攻击手段是为了更好进行防御。当然，一些好奇者可能会仿效黑客的某些手法去尝试网络攻击，我们劝说这些人应该学习法律，在未经许可的情况下这样做是违法的。对于那些别有用心的人来说，他们这样做总有一天会受到法律制裁。我

们编写本书的目的是提高读者的安全知识和安全管理的技术，管理好自己所在单位的网络信息系统，防止各种有意与无意的安全威胁，保证信息系统安全可靠的运行。

本书的内容安排如下。第 1 章介绍网络和信息安全以及 PDRR 安全模型的基本概念。第 2 章介绍密码技术及其应用。第 3 章主要讨论网络安全问题，包括网络安全机制、网络攻击手段、网络服务的安全问题、IPv4 和 IPv6 的安全问题和安全机制。第 4 章以 Windows 和 UNIX 操作系统为对象介绍了服务器和 IIS、Apache 的安全管理。第 5 章介绍路由器和防火墙的防护原理，还包括 Cisco 路由器的安全配置。第 6 章首先讨论数据库的一般安全问题，然后以 SQL Server 2000 和 Oracle9i 为目标介绍数据库的安全管理。第 7 章介绍网络安全防护中重要的技术——入侵检测技术。第 8 章为应急响应与系统恢复，讨论在遭受到网络攻击后如何应对。第 9 章介绍其他的一些网络安全增强技术，如 Kerberos、SSL、VPN 和信息隐藏等。第 10 章介绍信息保障的概念，并讨论信息战这个热点问题。

全书由周海刚主编，邱正伦、石爱军、扶树刚任副主编并参加了部分内容的编写和资料搜集工作，花春春女士也为本书的录入、校正和图表制作付出了辛勤的劳动，在此一并表示感谢！

本书可作为电子信息类专业高年级本科或研究生的教材，也可作为相关研究领域技术人员的参考资料。由于网络安全技术是一个新兴的研究领域，许多技术还处于完善与发展中，加上编写时间短，书中难免存在错误，非常欢迎广大读者和专家提出批评改进意见。

联系地址：zhouhg@yahoo.com

编者

2004 年 8 月

目　　录

第 1 章　概述 …… 1

1.1　信息安全与信息对抗 …… 1

1.1.1　信息的安全需求 …… 1

1.1.2　信息对抗的阶段性 …… 2

1.2　信息安全概念与技术的发展 …… 2

1.2.1　单机系统的信息保密阶段 …… 3

1.2.2　网络信息安全阶段 …… 3

1.2.3　信息保障阶段 …… 4

1.3　PDRR 安全模型 …… 6

习题 1 …… 7

第 2 章　密码技术 …… 8

2.1　密码技术简介 …… 8

2.1.1　密码学基本概念 …… 8

2.1.2　对称密钥密码系统 …… 10

2.1.3　公钥密码系统 …… 17

2.1.4　散列函数 …… 18

2.2　密码技术的应用 …… 19

2.2.1　数据加密 …… 19

2.2.2　鉴别协议 …… 20

2.2.3　消息完整性协议 …… 23

2.3　公开密钥分发 …… 24

习题 2 …… 26

第 3 章　网络安全问题 …… 27

3.1　网络安全框架 …… 27

3.2　网络安全机制 …… 29

3.3　网络攻击原理与步骤 …… 30

3.3.1　网络攻击 …… 30

3.3.2　利用漏洞进行攻击 …… 32

3.3.3　网络攻击的一般过程 …… 36

3.3.4 常见的网络攻击手段 …… 39
3.3.5 网络攻击的等级 …… 46
3.4 IPv4 的安全问题 …… 49
3.4.1 网络安全目标 …… 49
3.4.2 IPV4 版本 TCP/IP 的缺陷 …… 50
3.5 Internet 网络服务的安全问题 …… 50
3.5.1 Web 服务的安全问题 …… 50
3.5.2 FTP 服务的安全问题 …… 53
3.5.3 Telnet 的安全问题 …… 54
3.5.4 电子邮件的安全问题 …… 55
3.5.5 DNS 的安全问题 …… 57
3.6 IPv6 新一代网络的安全机制 …… 58
3.6.1 加密和认证 …… 58
3.6.2 密钥的分发 …… 62
3.6.3 IPv6 安全机制的应用 …… 63
习题 3 …… 65
第 4 章 服务器的安全管理 …… 66
4.1 Windows 服务器的安全管理 …… 66
4.1.1 Windows NT/2000 Server 安全基础 …… 66
4.1.2 Window 2000 的安全管理 …… 67
4.2 UNIX 服务器的安全管理 …… 73
4.2.1 用户标识 ID 和组标识 ID …… 73
4.2.2 存取控制列表 …… 75
4.2.3 passwd 文件 …… 76
4.2.4 文件加密 …… 79
4.2.5 终端锁定 …… 84
4.2.6 安全注销 …… 84
4.2.7 特洛依木马程序 …… 84
4.2.8 病毒与蠕虫程序 …… 85
4.2.9 限制 shell (rsh) …… 86
4.2.10 用户的安全策略与措施 …… 87
4.3 IIS 的安全管理 …… 88
4.3.1 以登录方式进行访问控制 …… 88
4.3.2 对文件夹的访问控制 …… 89
4.3.3 利用 IP 地址进行访问控制 …… 90

4.3.4 其他安全措施 …… 90
4.4 Apache 的安全管理 …… 91
4.4.1 Apache 中的模块 …… 92
4.4.2 根据客户来源进行限制 …… 93
4.4.3 根据用户标志进行限制 …… 95
4.5 计算机病毒攻击 …… 100
4.5.1 网络病毒特点 …… 101
4.5.2 常见网络病毒 …… 101
4.5.3 网络防毒措施 …… 104
习题 4 …… 105
第 5 章 路由器与防火墙 …… 106
5.1 路由器的包过滤功能 …… 106
5.1.1 包过滤路由器的操作方式与过滤规则 …… 106
5.1.2 包过滤路由器的特点 …… 107
5.1.3 应用协议的包过滤 …… 108
5.2 路由器访问表原理与配置 …… 110
5.2.1 Cisco 访问表基础 …… 110
5.2.2 标准访问表举例 …… 120
5.2.3 扩展访问表举例 …… 123
5.3 安全路由器原理 …… 130
5.3.1 安全路由器的设计原则 …… 130
5.3.2 双协议栈结构 …… 131
5.3.3 系统结构 …… 132
5.3.4 构建 IP-VPN …… 133
5.4 防火墙系统的安全原理 …… 134
5.4.1 防火墙的基本概念 …… 134
5.4.2 防火墙的逻辑构造与安全策略 …… 137
5.4.3 防火墙的安全技术 …… 137
5.5 防火墙系统 …… 139
5.5.1 网络层防火墙 …… 139
5.5.2 应用层防火墙 …… 142
5.6 基于 Linux 的防火墙 …… 145
5.6.1 术语 …… 145
5.6.2 工作原理 …… 146
5.6.3 功能实现 …… 148

习题 5 …… 153
第 6 章　数据库安全技术 …… 155
6.1　数据库的安全问题 …… 155
6.1.1　数据库特点概述 …… 155
6.1.2　数据库的安全威胁 …… 158
6.1.3　数据库的安全要求 …… 159
6.1.4　数据库的安全措施 …… 162
6.2　SQL Server 2000 数据库安全管理 …… 165
6.2.1　SQL Server 安全概述 …… 165
6.2.2　验证方法 …… 165
6.2.3　SQL Server 安全:登录 …… 167
6.2.4　SQL Server 安全:用户 …… 167
6.2.5　SQL Server 安全:角色 …… 168
6.2.6　管理 SQL Server 登录 …… 170
6.2.7　管理 SQL Server 用户 …… 172
6.2.8　管理 SQL Server 角色 …… 173
6.2.9　管理 SQL Server 权限 …… 175
6.2.10　使用加密 …… 177
6.3　Oracle9i 数据库安全管理 …… 177
6.3.1　用户管理 …… 177
6.3.2　权限和角色 …… 181
6.3.3　资源限制 …… 187
6.3.4　数据审计 …… 188
6.3.5　标签安全 …… 189
习题 6 …… 193
第 7 章　入侵检测技术 …… 194
7.1　IDS 的基本概念 …… 194
7.2　IDS 检测的活动 …… 195
7.3　入侵检测方法 …… 196
7.3.1　基本方法 …… 196
7.3.2　异常入侵检测方法 …… 197
7.3.3　误用入侵检测方法 …… 202
7.3.4　其他检测方法 …… 204
7.4　入侵监测系统的设计 …… 205
7.4.1　基于主机的 IDS 系统 …… 205

7.4.2 基于局域网的 IDS …… 207
7.4.3 分布式 IDS …… 209
习题 7 …… 211
第 8 章 应急响应与系统恢复 …… 212
8.1 应急响应 …… 212
8.1.1 概述 …… 212
8.1.2 应急响应方法学 …… 214
8.1.3 应急响应组 …… 224
8.1.4 应急响应设计的关键技术 …… 224
8.1.5 应急响应的发展方向 …… 225
8.2 系统恢复 …… 226
习题 8 …… 227
第 9 章 网络安全的增强技术 …… 228
9.1 Kerberos 系统 …… 228
9.1.1 Kerberos 的认证协议 …… 229
9.1.2 Kerberos 的密钥交换协议 …… 230
9.1.3 Kerberos 的不足 …… 231
9.2 SSL 安全协议 …… 231
9.2.1 SSL 简介 …… 231
9.2.2 SSL 协议的状态与状态变量 …… 232
9.2.3 SSL 握手协议 …… 233
9.2.4 SSL 记录协议 …… 234
9.2.5 SSL 使用的安全机制以及提供的安全服务 …… 234
9.3 IP Sec …… 237
9.4 虚拟专用网 …… 239
9.4.1 VPN 简介 …… 239
9.4.2 VPN 的分类 …… 240
9.4.3 隧道技术 …… 240
9.4.4 国外主要厂商的 VPN 解决方案 …… 241
9.5 网络多级安全技术 …… 241
9.5.1 可信网络基 …… 242
9.5.2 安全通信服务器 …… 243
9.5.3 多级安全信道 …… 244
9.6 信息隐藏技术 …… 246
9.6.1 信息隐藏技术的分类 …… 246

9.6.2 隐写术及其通信模型 …… 247
9.6.3 数字水印及其安全性分析 …… 249
习题 9 …… 251
第 10 章 信息保障与信息战 …… 252
10.1 信息保障 …… 252
10.1.1 定义 …… 252
10.1.2 信息保障技术框架 …… 252
10.2 21 世纪的信息战争与信息安全 …… 255
10.2.1 定义 …… 255
10.2.2 网络信息战的主要手段 …… 256
10.2.3 关于信息战的思考 …… 257
10.2.4 安全防御体系 …… 258
10.3 网络空间信息战 …… 259
10.3.1 网络空间的构成与对抗模型 …… 259
10.3.2 网络信息战的阶段与对抗样式 …… 262
10.3.3 可用的网络信息战手段探讨 …… 264
10.3.4 用于网络信息战的武器系列 …… 266
习题 10 …… 268
附录 A 计算机信息网络国际联网安全保护管理办法 …… 269
附录 B 中华人民共和国计算机信息系统安全保护条例 …… 273
参考文献 …… 276

第1章 概 述

人类已经进入信息化社会，随着 Internet 在全世界日益普及，政府、军队、企业等部门越来越需要利用网络传输与管理信息。虽然计算机与网络技术为信息的获取、传输与处理利用提供了越来越先进的手段，但也为入侵者提供了方便之门，使得计算机与网络中的信息变得越来越不安全。由于网络“黑客”与“入侵者”的活动越来越频繁，人们对计算机与网络中信息的安全越来越担心。不仅金融、商业、政府部门担心，军事部门更为担心。信息技术发展到今天，迫切要求发展各种信息安全技术。怎样才能使计算机与网络中的信息更安全，必须研究网络与计算机本身的安全机制和措施，研究“黑客”与“入侵者”的攻击方法和对他们的防范措施，这也是编写本书的主要宗旨。

1.1 信息安全与信息对抗

在本书中，“信息”是一个广泛的概念，不仅包括计算机文件系统或数据库系统中存储的各种数据、正文、图形、图像、声音等形式的多媒体数据文件、软件或各种文档资料，也包括存放或管理这些信息的硬件信息，如计算机硬件及其网络地址、网络结构、网络服务等都属于本书中所涉及的“信息”。尽管在许多文献中都大量引用“数据”与“信息”两个术语，但却没有一个被公认的对数据和信息的定义。本书将不对信息与数据加以区分，信息安全与数据安全是指同一个概念。在字典中，“安全”一词是指“远离危险、威胁的状态或特性”和“为防范间谍活动或蓄意破坏、犯罪、攻击等而采取的措施。”信息安全则是指防止任何对数据进行未授权访问的措施，或者防止造成信息有意无意泄露、破坏、丢失等问题的发生，让数据处于远离危险、免于威胁的状态或特性。而网络安全则是指计算机网络环境下的信息安全。

“信息对抗”也是一个概念广泛的术语，其主要含义是指争斗的双方利用各种手段获取信息的控制权，进而使己方在争斗过程中处于主动地位。信息对抗的主要表现形式有：敌对双方或利益竞争的双方通过电视广播进行宣传战；对立的双方互相进行心理战；通过侦察、间谍等手段窃取对方的信息；双方通过计算机网络进行信息的对抗等等。信息战是信息对抗的另一种称呼，只不过军事气息更浓一些。在本书中对“信息战”和“信息对抗”这两个术语也将不做区分，而且只讨论争斗的双方通过计算机网络进行的信息对抗。

1.1.1 信息的安全需求

计算机系统的安全需求主要用三方面表征：保密性、完整性和可用性。

保密性表示对信息资源开放范围的控制，不让不应涉密的人涉及秘密信息。实现保密性的方法一般是通过信息的加密、对信息划分密级，并为访问者分配访问权限，系统根据用户的身份权限控制对不同密级信息的访问。除了考虑数据加密、访问控制外，还要考虑计算机电磁泄露可能造成的信息泄露。

完整性是指保证计算机系统中的信息处于“保持完整或一种未受损的状态”。任何对系统信息应有特性或状态的中断、窃取、篡改、伪造都是破坏系统信息完整性的行为。其中中断是指在某一段时间内因系统的软、硬件的故障或恶意的破坏、删除造成系统信息的受损、丢失或不可利用；窃取是指系统的信息被未经授权的访问者非法获取，造成信息不应有的泄露，使得信息的价值受到损失或者失去了存在的意义；篡改是指故意更改正确的数据，破坏了数据的真实性状态；伪造是指恶意的未经授权者故意在系统信息中添加假信息，造成真假信息难辨，破坏了信息的可信性。

可用性是指合法用户在需要的时候，可以正确使用所需的信息而不遭服务拒绝。系统为了控制非法访问可以采取许多安全措施，但系统不应该阻止合法用户对系统中信息的利用。信息的可用性与保密性之间存在一定的矛盾。

1.1.2 信息对抗的阶段性

信息的生命期是指信息从产生到消亡的整个过程，可以划分为信息获取、信息传输、信息储存、决策处理、信息作用、信息废弃等若干个阶段。任何主体要想达到某种目的，比如某公司希望到某国开拓市场，那么首先应该派人到该国了解市场的需求信息，这叫信息获取；这些信息通过无线与有线信道传输到国内公司的计算机系统中存储到数据库中，这里经历了信息传输和信息存储两个阶段，当然在数据库中还存放着该公司的生产能力、销售网络、成本核算等信息。为了决策是否到国外开拓市场，需要利用决策软件对信息进行处理和做出相应的决策。信息作用则是把决策信息返回给前端的执行机构，由执行机构实现决策的意图。信息一般都具有时效性，过了某个时效后，信息也就失去了作用，失去效用的信息应该及时废弃。信息的时效可以根据需要决定，为了留作历史资料，需要对一些信息做长时间的存储保留。

利益冲突的双方进行的信息对抗遍布信息生命期的每个阶段，而且在不同的阶段采取不同的对抗形式。在信息获取阶段，对抗的一方需要获取对方真实完整的信息，而另一方则可以通过各种手段，如伪装、欺骗的方法使对方不能获取所需要的信息。在信息传输阶段，对抗的一方要设法让信息正确传输到目的地，而另一方则通过截获、弄假、干扰等手段妨碍信息的正确传输。在信息的存储阶段，对抗的双方围绕信息的完整性和保密性展开争斗。决策处理阶段的信息对抗体现为双方信息处理与决策支持系统之间的对抗。在信息作用阶段的信息对抗则体现为对双方信息执行机构控制权的争夺。网络黑客对信息的攻击一般都集中在信息的传输、存储和决策处理 3 个阶段中。针对不同阶段中信息所处的不同状态，研究不同的对抗手段更为有效。

1.2 信息安全概念与技术的发展

随着人类社会对信息的依赖程度越来越大，人们对信息的安全性越来越关注。随着应用与研究的深入，信息安全的概念与技术不断得到创新。早期在计算机网络广泛使用之前主要是开发各种信息保密技术，在 Internet 在全世界范围商业化应用之后，信息安全进入网络信息安全阶段。近几年又发展出了“信息保障（IA——Information Assurance）”的新概念。本文以下部分将介绍信息安全的各个发展阶段的主要内涵与所开发的新概念与新技术。

信息安全的最根本属性是防御性的，主要目的是防止己方信息的完整性、保密性与可用性遭到破坏。信息安全的概念与技术是随着人们的需求，随着计算机、通信与网络等信息技术的发展而不断发展的。大体可以分为信息保密、网络信息安全和信息保障等三个阶段，下面对此做一综述。

1.2.1 单机系统的信息保密阶段

早在几千年前，人类就会使用加密的办法传递信息。在1988年莫里斯“蠕虫”事件发生以前，信息保密技术的研究成果主要有两类：一类是发展各种密码算法及其应用，另一类是计算机信息系统保密性模型和安全评价准则。主要开发的密码算法有：1977年美国国家标准局采纳的分组加密算法DES（数据加密标准）；双密钥的公开密钥体制RSA（该体制是由Rivest、Shamir和Adleman三个人创造的）；1985年由N. koblitz和V. Miller提出的椭圆曲线离散对数密码体制（ECC），该体制的优点是可以利用更小规模的软件、硬件实现有限域上同类体制的相同安全性；另外，还创造出一批用于实现数据完整性和数字签名的杂凑函数。如数字指纹、消息摘要（MD）、安全杂凑算法（SHA——用于数字签名的标准算法）等，当然，其中有的算法是90年代中提出的。

为了验证与评价计算机信息系统的安全性，在20世纪70～80年代期间，研究出一批信息系统安全模型和安全性评价准则。主要有以下几种：访问监视器模型，这是一种最基本的访问控制模型；多级安全模型，包括军用安全模型、基于信息保密性的Bell-LaPadula信息流模型与基于信息完整性的Biba信息流模型；一些用于理论研究的抽象安全模型，如Graham-Denning（GD）模型、对GD模型的修正模型——HRU模型和Take-Grant保护系统（TGS）等。1985年美国国防部推出了可信计算机系统评价准则TCSEC。该标准是信息安全领域中的重要创举，也为后来由英、法、德、荷四国联合提出的包含保密性、完整性和可用性概念的“信息技术安全评价准则”（ITSEC）及“信息技术安全评价通用准则”（CC for ITSEC）的制定打下了基础。

1.2.2 网络信息安全阶段

1988年11月3日莫里斯“蠕虫”造成Internet几千台计算机瘫痪的严重网络攻击事件，引起了人们对网络信息安全的关注与研究，并与第二年成立了计算机紧急事件处理小组负责解决Internet的安全问题，从而开创了网络信息安全的新阶段。在该阶段中，除了采用和研究各种加密技术外，还开发了许多针对网络环境的信息安全与防护技术，这些防护技术是以被动防御为特征的。主要有以下一些：

（1）安全漏洞扫描器。用于检测网络信息系统存在的各种漏洞，并提供相应的解决方案。

（2）安全路由器。在普通路由器的基础上增加更强的安全性过滤规则，增加认证与预防瘫痪性攻击的各种措施。安全路由器完成在网络层与传输层的报文过滤功能。

（3）防火墙。在内部网与外部网的入口处安装的堡垒主机，在应用层利用代理功能实现对信息流的过滤功能。

（4）入侵检测系统（IDS）。根据已知的各种入侵行为的模式判断网络是否遭到入侵的一类系统，IDS一般也同时具备告警、审计与简单的防御功能。

(5) 各种防网络攻击技术。其中包括网络防病毒、防木马、防口令破解、防非授权访问等技术。

(6) 网络监控与审计系统。监控内部网络中的各种访问信息流，并对指定条件的事件做审计记录。

当然在这个阶段中还开发了许多网络加密、认证、数字签名的算法和信息系统安全评价准则（如 CC 通用评价准则）。这一阶段的主要特征是对于自己部门的网络采用各种被动的防御措施与技术，目的是防止自己内部网络受到攻击，保护内部网络的信息安全。

1.2.3 信息保障阶段

1.2.3.1 信息保障基本概念

信息保障的概念与思想是 20 世纪 90 年代末提出来的，思想的基本完善是在 2000 年下半年。因此信息保障阶段可以大致认为是从新千年开始的。

信息保障（IA）这一概念最初是由美国国防部长办公室提出来的，后被写入命令《DoD Directive S-3600.1：Information Operation》中，在 1996 年 12 月 9 日以国防部的名义发表。在这个命令中信息保障被定义为：通过确保信息和信息系统的可用性、完整性、可验证性、保密性和不可抵赖性来保护信息系统的信息作战行动，包括综合利用保护、探测和反应能力以恢复系统的功能。1998 年 1 月 30 日美国防部批准发布了《国防部信息保障纲要》（DIAP），认为信息保障工作是持续不间断的，它贯穿与平时、危机、冲突及战争期间的全时域。信息保障不仅能支持战争时期的国防信息攻防，而且能够满足和平时期国家信息的安全需求。

1998 年 5 月美国公布了由国家安全局 NSA 起草的 1.0 版本《信息保障技术框架》IATF，在 1999 年 8 月 31 日 IATF 论坛发布了 IATF2.0 版本，2000 年 9 月 22 日又推出了 IATF3.0 版本。遵循 IATF3.0 中定义的原则，就可以对信息基础设施做到多重保护。这称为“纵深防卫策略”DiD（Defense-in-Depth Strategy），其内涵已经超出了传统的信息安全保密，而是保护（Protection）、检测（Detection）、反应（Reaction）、恢复（Restore）的有机结合。信息保障阶段不仅包含安全防护的概念，更重要地是增加主动的和积极的防御观念。我们将在第 10 章详细讨论信息保障的概念。

1.2.3.2 信息系统安全工程过程（ISSE）

ISSE 主要告知人们如何根据系统工程的原则构建安全信息系统的方法、步骤与任务。系统工程过程主要包括以下步骤与任务：

1. 发现需求

(1) 使命/业务的描述。使命是指一个单位所担负的特定任务，由任务可以划分为功能。

(2) 有关政策方面的考虑。如国家或军队的信息管理要求；原始与历史资源的管理要求；与 C3I 系统的兼容性、互操作与集成要求等。

2. 系统功能的定义

(1) 目标：确定系统的功能及与外部的接口，并转换成工程图的定义、接口与系统的边界。

(2) 系统的上下文环境：包括系统的物理及逻辑边界、连接到系统的输入和输出的特

点，还应标明支持用户完成使命所需的信息处理类型（交互通信、广播通信、信息存储、一般访问、受限访问等）。

（3）要求：描述任务、行动及完成系统需求的活动等。

3．系统的设计

（1）功能分配；

（2）概要设计；

（3）详细设计。

4．系统的实现

（1）通过各种手段获取一切必要的资源，包括通过采办手段；

（2）按照需求构建系统；

（3）系统测试；

（4）评估性能。

5．ISSE过程

ISSE作为上述系统工程过程的一个子过程，其重点是针对信息保护方面的需求，从理论上讲它是与上述系统工程平行出现的，分布在各个阶段。ISSE的活动包括：

（1）描述信息保护的需求；

（2）基于前述系统工程过程，形成信息安全方面的要求（安全要适度）。

（3）根据这些要求构建功能性的信息安全体系结构；

（4）把信息保护功能分配给物理体系结构及逻辑体系结构；

（5）在系统设计中实现信息保护体系结构；

（6）实现适度安全，在费用、进度及运作合适度与有效度的总体范围内平衡信息保护风险管理及ISSE的其他方面的考虑。

（7）参与和其他信息保护及系统工程条令有关平衡、折中的研究，以及使命、威胁、政策对信息保护要求的影响。

1.2.3.3 信息安全的技术反制措施的强度

反制措施是一种防御网络攻击的专门技术、产品或程序。在有效的安全总体解决方案中，不管技术的还是非技术的反制措施都是非常重要的。但制定合适的技术反制措施需要遵循一些原则，其中包括对各种威胁、重要安全服务的鲁棒性（Robust）策略、互操作性框架、KML/PKI的评估。

敌对方信息攻击的目的可以归纳为三大类：非法访问、非法修改和阻止提供合法服务。安全总体解决方案就是为了不让敌方达到他们的目的。己方网络需要提供的五种基本安全服务是访问控制、保密性、完整性、可用性及不可否认性。这些安全服务需要利用以下安全机制完成：加密、鉴别或识别（identification）、认证、访问控制、安全管理及可信赖技术，这些机制综合到一起可以构成防止攻击的壁垒。

鲁棒性策略针对某种信息价值和可能遭到的威胁水平，提供一种在确定信息安全机制强度的指导思想。这种策略还定义了对技术性反制措施的测量及评估其鲁棒性不同等级的策略。在鲁棒性策略中把信息的价值分为5级（V1～V5），其价值依次递升；威胁分为7级（T1～T7），其大小也依次递升。表1-1根据待保护信息的价值及威胁程度，给出了对应安全强度的安全机制。

表 1-1 鲁棒性的等级分类表

信息价值	威胁程度						
	T1	T2	T3	T4	T5	T6	T7
V1	SML1 EAL1	SML1 EAL1	SML1 EAL1	SML1 EAL2	SML1 EAL2	SML1 EAL2	SML1 EAL2
V2	SML1 EAL1	SML1 EAL1	SML1 EAL1	SML2 EAL2	SML2 EAL2	SML2 EAL3	SML2 EAL3
V3	SML1 EAL1	SML1 EAL2	SML1 EAL2	SML2 EAL3	SML2 EAL3	SML2 EAL4	SML2 EAL4
V4	SML2 EAL1	SML2 EAL2	SML2 EAL3	SML3 EAL4	SML3 EAL5	SML3 EAL5	SML3 EAL6
V5	SML2 EAL2	SML2 EAL3	SML3 EAL4	SML3 EAL5	SML3 EAL6	SML3 EAL6	SML3 EAL7

表中：SML——机制强度的等级；EAL——保障评估的等级；

SML1——基本强度，抗非复杂威胁（T1～T3 级）用以保护低价值数据；

SML2——中等强度，抗复杂威胁（T4～T5 级）用以保护中等价值数据；

SML3——高等强度，抗国家级威胁（T6～T7 级）用以保护高等价值数据。

美国社会高度依赖信息，投入巨额经费研究信息安全的新技术，发展出许多信息安全的新概念。本文介绍的“信息保障”概念，就是由美国国防部提出的。随着我国现代化建设的进展，我国党、政、军、企各部门对信息的依赖程度越来越高，各单位领导对信息安全问题也越来越重视。美国对信息安全的新理论，如信息保障技术框架，是值得我国参考与借鉴的。我们应该研究这些新概念与新理论，并结合我国自己的情况，提出符合我国国情的信息保障技术框架，作为指导我国各部门信息安全建设的参考。

1.3 PDRR 安全模型

PDRR 安全模型是从经典的 P2DR 模型基础上演变而来的，随同信息保障概念一起为大家所接收和重视。PDRR 安全模型强调网络防护不再是单纯被动式的防护，而是保护（Protection）、检测（Detection）、响应（Reaction）、恢复（Restore）的有机结合，如图 1-1 所示。因此 PDRR 模型不仅包含安全防护的概念，更重要地是增加主动的和积极的防御观念。

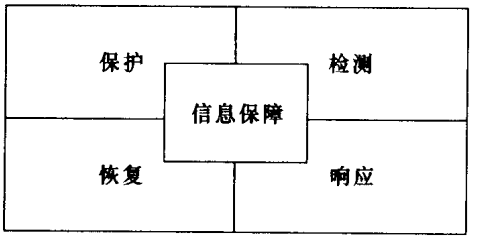

图 1-1 PDRR 模型

1．保护

保护就是采用一切的手段保护我们信息系统的可用性、机密性、完整性、可控性和不