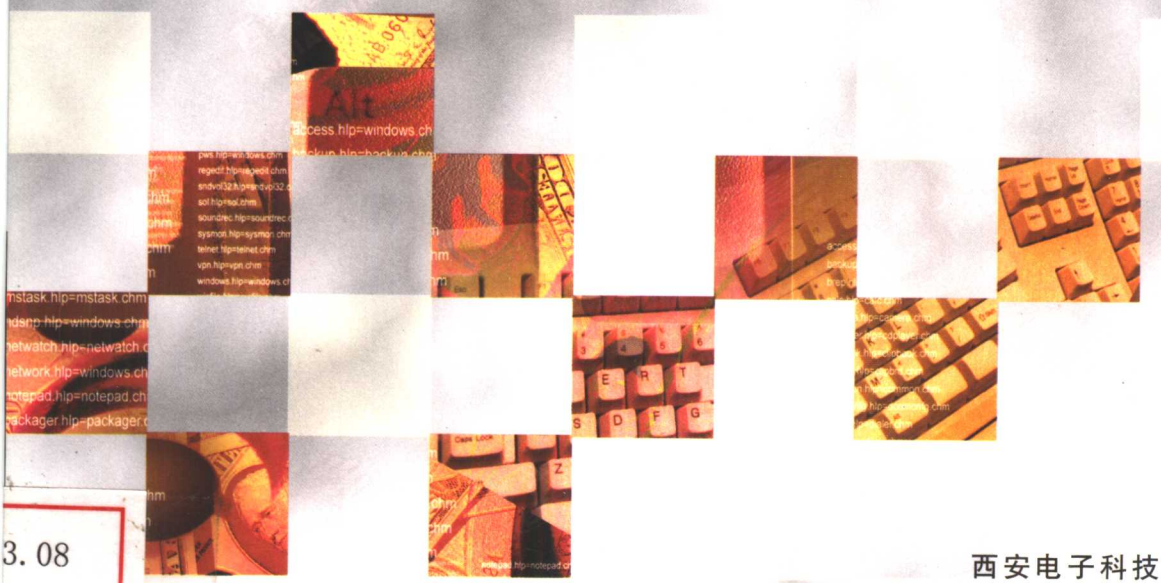
普通高等院校计算机类专业系列教材

Network & Information Security Technology

网络信息安全技术

周明全　吕林涛　李军怀　编著



西安电子科技大学出版社
http://www.xduph.com

普通高等院校计算机类专业系列教材

网络信息安全技术

Network & Information Security Technology

周明全　吕林涛　李军怀　编著

西安电子科技大学出版社

2003

内 容 简 介

全书共分为11章，介绍了计算机网络安全的基本理论和关键技术。主要内容包括：网络安全、密码技术基础、密钥管理技术、数字签名和认证技术、网络入侵检测原理与技术、Internet的基础设施安全、防火墙技术、电子商务的安全技术及应用、包过滤技术原理及应用、代理服务技术原理及应用、信息隐藏技术。

通过对本书的学习，使读者能够对计算机网络安全有一个系统的了解，掌握计算机网络特别是计算机互联网安全的基本概念，了解设计和维护安全的网络体系及其应用系统的基本手段和常用方法。

本书可作为高等学校计算机软件工程、计算机网络工程、计算机科学与技术、商务信息等有关专业本科生和研究生的教材，也可作为从事网络信息方面人员的参考书。

图书在版编目(CIP)数据

网络信息安全技术＝Network & Information Security Technology/周明全等编著．
—西安：西安电子科技大学出版社，2003.11
(普通高等院校计算机类专业系列教材)
ISBN 7-5606-1304-7
Ⅰ．网… Ⅱ．周… Ⅲ．网络信息-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(2003)第089483号

策　　划　臧延新
责任编辑　杨宗周
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)8242885　8201467　　邮　编　710071
http://www.xduph.com　　E-mail：xdupfxb@pub.xaonline.com
经　　销　新华书店
印刷单位　西安兰翔印刷厂
版　　次　2003年11月第1版　2003年11月第1次印刷
开　　本　787毫米×1092毫米　1/16　印张16.875
字　　数　397千字
印　　数　1～4 000册
定　　价　17.00元
ISBN 7-5606-1304-7/TP・0687
XDUP 1575001-1

普通高等院校计算机类专业系列教材

编审专家委员会名单

前　言

计算机网络是计算机技术和通信技术密切结合形成的新的技术领域。Internet/Intranet的发展，对整个社会的科学技术、经济发展、国防建设、文化思想带来了巨大的影响和推动。信息化带动了社会的工业化、现代化。网络技术为人类的进步做出了巨大的贡献。

网络技术的本质是信息共享。网络的发展使世界变得越来越小，人类的交往变得越来越多。在人类共享网络技术的利益之时，相伴而来的信息安全问题也日益突出。随着信息技术的普及与推广，人们已清醒地认识到在发展信息网络技术的同时，做好网络安全方面的理论研究与应用技术开发，是信息技术发展的重要内容。近年来，各国政府都把网络安全作为国家安全的一部分来认识，是国家海、陆、空之外的重要关防建设。无疑，网络信息安全问题的研究和技术的开发是现在和将来相当时期内重要的热点。

在信息学科的专业教育中开设网络安全的课程，旨在让学生们从学习网络技术时就树立建造安全网络的观念，掌握网络安全的基本知识，了解设计和维护安全的网络体系及其应用系统的基本手段和常用方法，为从事信息网络的研究和开发打下良好的基础。

通过网络的攻击侵入，设置网络安全机制，是一对矛与盾的关系。而掌握矛和盾的人均是熟悉计算机网络的“行内人”。网络安全不仅是一个技术问题，也是法律问题和社会问题，所以网络安全教育必须与信息教育同步开展。信息科技工作者除了专业技术以外，还应具有良好的网络文化道德，懂得网络管理的政策法规，营造良好的网络文化氛围，不做网上违法的事情。因此，网络安全教育包括网络安全技术与网络安全法规两个方面。

本书共分为11章，通过对网络安全的基本概念、安全标准和网络安全防护体系，数据加密技术，密钥管理技术，数字签名和认证协议，网络攻击与检测技术，Internet的基础设施安全，防火墙，信息隐藏等技术的阐述，较全面的介绍了计算机网络安全的基本理论和关键技术；对当前常用的网络安全技术的原理和应用进行了详细的阐述，每章均附有习题。在这些基础之上，信息隐藏技术、包过滤技术，代理服务技术可作为进一步学习的技术。为了加强网络法规的教育，在附录部分摘录了与网络安全相关的部分法规，供工作学习参考之用。因此，本书既能够作为初学者的教材与自学用书，也可作为网络工作者常备的参考书。

本书的第1、2、3、5、11章由周明全、李军怀、茹少峰共同撰写，第4、7、8、9、10章由吕林涛撰写，第6章由张翔撰写。西北大学耿国华教授、西安理工大学张景教授对本书的编写提出了许多宝贵意见，周明全教授完成统稿。西北大学计算机科学系耿国华教授审阅了全书并提出了宝贵意见。西北大学计算机科学系研究生魏佼佼、李康、康华，西安理工大学计算机学院研究生刘海玲、张晓丽、马臻等参加了本书的相关工作。本书在编写过程中参考了许多相关的文献，在此一并表示感谢。

由于作者水平有限，编写时间仓促，对书中存在的错误和问题，殷切希望读者批评指正，各位专家给予指教。

编　者

2003年8月

目　录

第 1 章　网络安全 …… 1
1.1　网络安全的基础知识 …… 1
1.1.1　网络安全的基本概念 …… 2
1.1.2　网络安全的特征 …… 2
1.1.3　网络安全的目标 …… 3
1.1.4　网络安全需求与安全机制 …… 3
1.2　威胁网络安全的因素 …… 4
1.2.1　网络的安全威胁 …… 5
1.2.2　网络安全的问题及原因 …… 8
1.3　网络安全防护体系 …… 9
1.3.1　网络安全策略 …… 9
1.3.2　网络安全体系 …… 13
1.4　网络安全的评估标准 …… 19
1.4.1　可信任计算机标准评估准则简介 …… 19
1.4.2　国际安全标准简介 …… 21
1.4.3　我国安全标准简介 …… 22
习题 …… 22
第 2 章　密码技术基础 …… 23
2.1　密码技术的基本概念 …… 23
2.2　古典加密技术 …… 24
2.2.1　置换密码 …… 24
2.2.2　代换密码 …… 25
2.3　现代加密技术 …… 28
习题 …… 38
第 3 章　密钥管理技术 …… 39
3.1　密钥的管理内容 …… 39
3.2　密钥的分配技术 …… 42
3.2.1　密钥分配实现的基本方法 …… 42
3.2.2　密钥分配实现的基本工具 …… 43
3.2.3　密钥分配系统实现的基本模式 …… 43
3.2.4　密钥的验证 …… 44
3.3　公钥密码 …… 45
3.3.1　公钥密码体制的基本概念 …… 45
3.3.2　公钥密码体制的原理 …… 46
3.4　RSA 算法 …… 48
3.4.1　RSA 算法描述 …… 48
3.4.2　RSA 算法中的计算问题 …… 49
3.4.3　RSA 算法的安全性 …… 51
3.4.4　RSA 的实用性及数字签名 …… 51
3.4.5　RSA 算法和 DES 算法 …… 52
3.5　椭圆曲线密码体制 …… 53
3.5.1　椭圆曲线 …… 53
3.5.2　有限域上的椭圆曲线 …… 58
3.5.3　椭圆曲线上的密码 …… 58
习题 …… 60
第 4 章　数字签名和认证技术 …… 61
4.1　数字签名的基本概念 …… 61
4.1.1　数字签名概念 …… 61
4.1.2　数字签名技术应满足的要求 …… 61
4.1.3　直接方式的数字签名技术 …… 63
4.1.4　具有仲裁方式的数字签名技术 …… 63
4.1.5　利用公钥实现数字签名技术原理 …… 64
4.1.6　其它数字签名技术 …… 65
4.2　认证及身份验证技术 …… 67
4.2.1　相互认证技术 …… 67
4.2.2　单向认证技术 …… 71
4.2.3　身份验证技术 …… 72
4.2.4　身份认证系统实例——Kerberos 系统 …… 73
4.3　数字签名标准及数字签名算法 …… 75
4.3.1　数字签名算法 DSS …… 75
4.3.2　数字签名算法 DSA …… 76
4.3.3　数字签名算法 HASH …… 77
4.3.4　数字签名算法 RSA …… 78
4.4　其它数字签名体制 …… 78
4.4.1　基于离散对数问题的数字签名体制 …… 78
4.4.2　基于大数分解问题的签名体制 …… 81
4.5　数字证明技术 …… 83
习题 …… 83
第 5 章　网络入侵检测原理与技术 …… 84
5.1　黑客攻击与防范技术 …… 84

5.1.1 网络入侵及其原因 …… 84
5.1.2 黑客攻击策略 …… 87
5.1.3 网络入侵的防范技术 …… 89
5.2 入侵检测原理 …… 89
5.2.1 入侵检测概念 …… 89
5.2.2 入侵检测模型 …… 91
5.2.3 IDS 在网络中的位置 …… 92
5.3 入侵检测方法 …… 93
5.3.1 基于概率统计的检测 …… 93
5.3.2 基于神经网络的检测 …… 94
5.3.3 基于专家系统 …… 94
5.3.4 基于模型推理的攻击检测技术 …… 95
5.3.5 基于免疫的检测 …… 95
5.3.6 入侵检测的新技术 …… 96
5.3.7 其它相关问题 …… 96
5.4 入侵检测系统 …… 96
5.4.1 入侵检测系统的构成 …… 97
5.4.2 入侵检测系统的分类 …… 97
5.4.3 入侵检测系统的介绍 …… 98
5.5 入侵检测系统的测试评估 …… 102
5.5.1 测试评估概述 …… 102
5.5.2 测试评估的内容 …… 102
5.5.3 测试评估标准 …… 104
5.5.4 IDS 测试评估现状以及
存在的问题 …… 105
5.6 几种常见的 IDS 系统 …… 106
5.7 入侵检测技术发展方向 …… 108
习题 …… 110
第 6 章 Internet 的基础设施安全 …… 111
6.1 Internet 安全概述 …… 111
6.2 DNS 的安全性 …… 112
6.2.1 目前 DNS 存在的安全威胁 …… 112
6.2.2 Windows 下 DNS 欺骗 …… 113
6.2.3 拒绝服务攻击 …… 114
6.3 安全协议 IPSec …… 115
6.3.1 IP 协议简介 …… 115
6.3.2 下一代 IP - IPv6 …… 115
6.3.3 IP 安全协议 IPSec 的用途 …… 116
6.3.4 IPSec 的结构 …… 117
6.4 电子邮件的安全性 …… 119
6.4.1 PGP …… 119
6.4.2 S/MIME …… 122
6.5 Web 的安全性 …… 123
6.5.1 Web 的安全性要求 …… 123
6.5.2 安全套接字层(SSL) …… 125
6.5.3 安全超文本传输协议 …… 127
6.6 虚拟专用网及其安全性 …… 128
6.6.1 VPN 简介 …… 128
6.6.2 VPN 协议 …… 129
6.6.3 VPN 方案设计 …… 133
6.6.4 VPN 的安全性 …… 134
6.6.5 微软的点对点加密技术 …… 135
6.6.6 第二层隧道协议 …… 136
6.6.7 VPN 发展前景 …… 136
习 题 …… 137
第 7 章 防火墙技术 …… 138
7.1 防火墙概念 …… 138
7.2 防火墙原理及实现方法 …… 139
7.2.1 防火墙的原理 …… 139
7.2.2 防火墙的实现方法 …… 140
7.3 防火墙体系结构 …… 143
7.3.1 双宿主主机体系结构 …… 143
7.3.2 堡垒主机过滤体系结构 …… 148
7.3.3 过滤子网体系结构 …… 160
7.3.4 应用层网关体系结构 …… 162
7.4 防火墙的构成 …… 164
7.4.1 防火墙的类型及构成 …… 164
7.4.2 防火墙的配置 …… 167
7.5 防火墙所采用的技术及其作用 …… 168
7.5.1 隔离技术 …… 168
7.5.2 管理技术 …… 169
7.5.3 防火墙操作系统的技术 …… 169
7.5.4 通信堆叠技术 …… 170
7.5.5 网络地址转换技术 …… 173
7.5.6 多重地址转换技术 …… 173
7.5.7 虚拟专用网络技术(VPN) …… 174
7.5.8 动态密码认证技术 …… 174
7.6 防火墙选择原则 …… 175
7.6.1 防火墙安全策略 …… 175
7.6.2 选择防火墙的原则 …… 176
7.7 防火墙建立实例 …… 177
7.7.1 包过滤路由器的应用 …… 177
7.7.2 屏蔽主机防火墙的应用 …… 177
7.7.3 屏蔽子网防火墙的应用 …… 178
7.7.4 某企业销售系统中
防火墙建立实例 …… 179

习　题 …… 181
第 8 章　电子商务的安全技术及应用 … 182
8.1　电子商务概述 …… 182
8.1.1　电子商务的概念 …… 182
8.1.2　电子商务的分类 …… 183
8.1.3　电子商务系统的支持环境 …… 184
8.2　电子商务的安全技术要求 …… 185
8.2.1　电子商务与传统商务的比较 …… 185
8.2.2　电子商务面临的威胁和安全技术要求 …… 186
8.2.3　电子商务系统所需的安全服务 … 188
8.2.4　电子商务的安全体系结构 …… 188
8.3　电子支付系统的安全技术 …… 188
8.3.1　电子支付系统的安全要求 …… 188
8.3.2　电子支付手段 …… 190
8.4　电子现金应用系统 …… 193
8.4.1　电子现金应用系统的安全技术 … 193
8.4.2　脱机实现方式中的密码技术 …… 195
8.4.3　电子钱包 …… 197
8.5　电子现金协议技术 …… 198
8.5.1　不可跟踪的电子现金协议技术 … 198
8.5.2　可分的电子现金协议技术 …… 199
8.5.3　基于表示的电子现金协议技术 … 201
8.5.4　微支付协议技术 …… 203
8.5.5　可撤销匿名性的电子现金系统实现技术 …… 203
8.6　电子商务应用系统实例 …… 205
8.6.1　××海关业务处理系统 …… 205
8.6.2　××海关电子申报系统网络平台 …… 206
8.6.3　××海关电子申报系统的软件体系结构 …… 207
习　题 …… 207
第 9 章　包过滤技术原理及应用 …… 208
9.1　高层 IP(因特网协议)网络的概念 …… 208
9.2　包过滤的工作原理 …… 208
9.2.1　包过滤技术传递的判据 …… 208
9.2.2　包过滤技术传递操作 …… 208
9.2.3　包过滤方式的优缺点 …… 210
9.3　包过滤路由器的配置 …… 210
9.3.1　协议的双向性 …… 210
9.3.2　“往内”与“往外” …… 211
9.3.3　“默认允许”与“默认拒绝” …… 211
9.4　包的基本构造 …… 211
9.5　包过滤处理内核 …… 212
9.5.1　包过滤和网络策略 …… 212
9.5.2　一个简单的包过滤模型 …… 212
9.5.3　包过滤器操作 …… 213
9.5.4　包过滤设计 …… 214
9.6　包过滤规则 …… 216
9.6.1　制订包过滤规则时应注意的事项 …… 216
9.6.2　设定包过滤规则的简单实例 …… 217
9.7　依据地址进行过滤 …… 218
9.8　依据服务进行过滤 …… 219
9.8.1　往外的 Telnet 服务 …… 219
9.8.2　往内的 Telnet 服务 …… 220
9.8.3　Telnet 服务 …… 220
9.8.4　有关源端口过滤问题 …… 221
习题 …… 221
第 10 章　代理服务技术原理及应用 …… 222
10.1　代理服务的基本概念 …… 222
10.2　代理服务的优缺点 …… 223
10.2.1　代理服务的优点 …… 223
10.2.2　代理服务的缺点 …… 223
10.3　代理服务的工作方法 …… 224
10.3.1　使用定制客户软件进行代理 …… 224
10.3.2　使用定制的客户过程进行代理 …… 225
10.4　代理服务器的使用 …… 225
10.4.1　应用级与回路级代理 …… 225
10.4.2　公共与专用代理服务器 …… 226
10.4.3　智能代理服务器 …… 226
10.5　使用代理的若干问题 …… 226
10.5.1　TCP 与其它协议 …… 226
10.5.2　不使用代理服务器的代理 …… 226
10.5.3　无法代理的原因及解决办法 …… 227
10.6　用于因特网服务的代理特性 …… 227
10.6.1　电子邮件(E-mail) …… 227
10.6.2　简单邮件传输协议(SMTP)的代理特点 …… 228
10.6.3　邮局协议(POP)的代理特点 …… 228
10.6.4　文件传输(FTP) …… 229
10.6.5　远程登录(Telnet) …… 230
10.6.6　存储转发协议(NNTP) …… 230
10.6.7　万维网(WWW) …… 230

10.6.8 域名服务(DNS) …… 230
习题 …… 231
第 11 章 信息隐藏技术 …… 232
11.1 基本概念 …… 232
11.2 信息隐藏技术的应用领域及分类 …… 234
11.2.1 信息隐藏技术的应用 …… 234
11.2.2 信息隐藏技术的分类 …… 235
11.3 数字图像水印技术 …… 236
11.3.1 数字水印技术的基本原理 …… 236
11.3.2 空域的图像水印技术 …… 238
11.3.3 频域的图像水印技术 …… 239
11.4 数字文本水印技术 …… 242
11.4.1 数字文本水印技术的一般原理 …… 242
11.4.2 行移编码 …… 243
11.4.3 字移编码 …… 244
11.4.4 特征编码 …… 245
11.4.5 编码方式的综合运用 …… 245
11.5 数字语音水印技术 …… 245
11.5.1 最不重要位(LSB)方法 …… 246
11.5.2 小波变换方法 …… 246
11.6 数字视频水印技术 …… 247
11.6.1 数字视频水印技术的一般原理 …… 247
11.6.2 原始视频水印 …… 249
11.6.3 压缩视频水印 …… 249
习题 …… 250

附录 A 《中华人民共和国计算机信息网络国际联网管理暂行办法》 …… 251
附录 B 《中华人民共和国计算机信息网络国际联网安全保护管理办法》 …… 253
附录 C 《中华人民共和国计算机信息系统安全保护条例》 …… 256
参考文献 …… 259

第1章 网络安全

随着 Internet/Intranet 技术的发展和普及使用，全球信息化已成为人类发展的大趋势。但由于计算机网络具有连接形式多样性、终端分布不均匀性和网络的开放性、互联性等特征，致使网络易受黑客、恶意软件和其他不轨人员的攻击，使得计算机网络安全问题日益突出。网络安全涉及到国民经济的各个领域，已经成为信息化建设的一个核心问题。

本章主要介绍网络安全的概念、威胁网络安全的因素、网络安全防护体系以及网络安全的评估标准等内容。

1.1 网络安全的基础知识

在社会日益信息化的今天，信息已成为一种重要的战略资源，信息的应用也从原来的军事、科技、文化和商业渗透到当今社会的各个领域，其在社会生产、生活中的作用日益显著。传播、共享和自增值是信息的固有属性，与此同时，又要求信息的传播是可控的，共享是授权的，增值是确认的。因此信息的安全和可靠在任何状况下都是必须要保证的。信息网络的大规模全球互联趋势，Internet 的开放性，以及人们的社会与经济活动对计算机网络依赖性的与日俱增，使得计算机网络的安全性成为信息化建设的一个核心问题。

以 Internet 为代表的信息网络技术的应用正日益普及和广泛，应用层次正在深入，应用领域从传统的小型业务系统，逐渐向大型关键业务系统扩展，典型的如党政部门信息系统、金融业务系统、企业商务系统等。伴随网络的普及，安全日益成为影响网络效能的重要问题，而 Internet 所具有的开放性、国际性和自由性在增加应用自由度的同时，对安全提出了更高的要求，这主要表现在：

(1) 开放性的网络，导致网络的技术是全开放的，任何一个人、团体都可能从中获得所需的东西，因而网络所面临的破坏和攻击可能是多方面的。例如，来自物理传输线路的攻击能对网络通信协议和实现实施攻击；对软件实施攻击，也可以对硬件实施攻击。

(2) 国际性的一个网络还意味着网络的攻击不仅仅来自本地网络的用户，它可以来自 Internet 上的任何一个机器，也就是说，网络安全所面临的是一个国际化的挑战。

(3) 自由意味着网络最初对用户的使用并没有提供任何的技术约束，用户可以自由地访问网络，自由地使用和发布各种类型的信息。用户只对自己的行为负责，而没有任何的法律限制。

尽管开放的、自由的、国际化的 Internet 的发展给政府机构、企事业单位带来了革命性的改革和开放，使得他们能够利用 Internet 提高办事效率和市场反应能力，以便更具竞争力。通过 Internet，他们可以从异地取回重要数据，同时又要面对网络开放带来的数据安全的新挑战和新危险。如何保护企业的机密信息不受黑客和工业间谍的入侵，已成为政府机构、企事业单位信息化健康发展所要考虑的重要事情之一。

1.1.1 网络安全的基本概念

网络安全从其本质上来讲就是网络上的信息安全。它涉及的领域相当广泛，这是因为在目前的公用通信网络中存在着各种各样的安全漏洞和威胁。从广义来说，凡是涉及到网络上信息的保密性、完整性、可用性、真实性和可控性的相关技术与原理，都是网络安全所要研究的领域。

网络安全是指网络系统的硬件、软件及其系统中的数据的安全，它体现在网络信息的存储、传输和使用过程中。所谓的网络安全性就是网络系统的硬件、软件及其系统中的数据受到保护，不受偶然的或者恶意的原因而遭到破坏、更改、泄露，系统连续可靠正常地运行，网络服务不中断。它的保护内容包括：

(1) 保护服务、资源和信息；

(2) 保护结点和用户；

(3) 保护网络私有性。

从不同的角度来说，网络安全具有不同的含义。

从一般用户的角度来说，他们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、篡改等手段对用户信息的损害和侵犯，同时也希望用户信息不受非法用户的非授权访问和破坏。

从网络运行和管理者角度来说，他们希望对本地网络信息的访问、读写等操作受到保护和控制，避免出现病毒、非法存取、拒绝服务和网络资源的非法占用及非法控制等威胁，制止和防御网络“黑客”的攻击。

对安全保密部门来说，他们希望对非法的、有害的或涉及国家机密的信息进行过滤和防堵，避免其通过网络泄露，避免由于这类信息的泄密对社会产生危害，给国家造成巨大的经济损失，甚至威胁到国家安全。

从社会教育和意识形态角度来讲，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。

由此可见，网络安全在不同的环境和应用中会得到不同的解释。

1.1.2 网络安全的特征

根据网络安全的定义，网络安全应具有以下 6 个方面的特征：

(1) 保密性　指信息不泄露给非授权的用户、实体或过程，或供非授权用户、实体或过程利用的特性。

(2) 完整性　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。

(3) 可用性　指可被授权实体访问并按需求使用的特性，即当需要时应能存取所需的信息。网络环境下拒绝服务、破坏网络和有关系统的正常运行等都属于对可用性的攻击。

(4) 可控性　指对信息的传播及内容具有控制能力，可以控制授权范围内的信息流向及行为方式。

(5) 可审查性　对出现的安全问题提供调查的依据和手段，用户不能抵赖曾做出的行为，也不能否认曾经接到对方的信息。

(6) 可保护性 保护软、硬件资源不被非法占有，免受病毒的侵害。

1.1.3 网络安全的目标

网络安全的目标是确保网络系统的信息安全。网络信息安全主要包括两个方面：信息存储安全和信息传输安全。

信息存储安全就是指信息在静态存放状态下的安全，如是否会被非授权调用等，一般通过设置访问权限、身份识别、局部隔离等措施来保证。针对"外部"的访问、调用而言的访问控制技术是解决信息存储安全的主要途径。

在网络系统中，任何调用指令和任何信息反馈均是通过网络传输实现的，所以网络信息传输上的安全就显得特别重要。信息传输安全主要是指信息在动态传输过程中的安全。为确保网络信息的传输安全，尤其需要防止以下问题：

(1) 截获(Interception) 对网上传输的信息，攻击者只需在网络的传输链路上通过物理或逻辑的手段，就能对数据进行非法的截获与监听，进而得到用户或服务方的敏感信息。

(2) 伪造(Fabrication) 对用户身份仿冒这一常见的网络攻击方式，传统的对策一般采用身份认证方式防护，但是，用于用户身份认证的密码在登录时常常是以明文的方式在网络上进行传输的，很容易被攻击者在网络上截获，进而可以对用户的身份进行仿冒，使身份认证机制被攻破。身份认证的密码90%以上是用代码形式传输的。

(3) 篡改(Modification) 攻击者有可能对网络上的信息进行截获并且篡改其内容(增加、截去或改写)，使用户无法获得准确、有用的信息或落入攻击者的陷阱。

(4) 中断(Interruption) 攻击者通过各种方法，中断用户的正常通信，达到自己的目的。

(5) 重发(Repeat) "信息重发"的攻击方式，即攻击者截获网络上的密文信息后，并不将其破译，而是把这些数据包再次向有关服务器(如银行的交易服务器)发送，以实现恶意的目的。

网络安全不仅仅是一个纯技术问题，单凭技术因素确保网络安全是不可能的。网络信息因为其自身的特点，在复制、获取上的便捷性使得网络安全问题成为涉及到法律、管理和技术等多方因素的复杂系统问题。

1.1.4 网络安全需求与安全机制

1. 网络安全的需求

(1) 解决网络的边界安全问题；
(2) 保证网络内部的安全；
(3) 实现系统安全及数据安全；
(4) 建立全网通行的身份识别系统，并实现用户的统一管理；
(5) 在用户和资源之间进行严格的访问控制；
(6) 实现信息传输时数据完整性和保密性；
(7) 建立一整套审计、记录的机制；

(8) 融合技术手段和行政手段，形成全局的安全管理。

网络安全机制包括访问控制机制、加密机制、认证交换机制、数字签名机制、业务流分析机制、路由控制机制。

2. 网络安全机制

(1) 物理层信息安全，主要防止物理通路的损坏，物理通路的窃听，对物理通路的攻击如干扰等。

(2) 链路层的网络安全需要保证通过网络链路的数据不被窃听。

(3) 网络层的安全需要保证网络只给授权的用户使用授权的服务，保驻网络路由正确，避免被拦截或监听。

(4) 操作系统安全要求保证用户资料、操作系统访问控制的安全，同时能够对该操作系统上的应用进行审计。

(5) 应用平台指建立在网络系统之上的应用软件服务，如数据库服务器、电子邮件服务器、Web 服务器等。由于应用平台的系统非常复杂，通常采用多种技术(如 SSL 等)来增强应用平台的安全性。

(6) 应用系统完成网络系统的最终目的——为用户服务，应用系统的安全与系统设计和实现关系密切。

综上所述，在一般情况下，分布在网络层的安全机制，主要保护网络服务的可用性，解决系统安全问题；分布在应用层的安全机制，主要保护合法用户对数据的合法存取，解决数据安全问题。通过网络层和应用层，集成系统安全和数据安全，可构成立体的网络安全防护体系。通常，网络层的安全措施包括防火墙和安全检测手段，防火墙主要是限制访问，安全检测主要是预防黑客的攻击。应用层的安全措施包括：建立全局的电子身份认证系统；实现全局资源的统一管理；为实现数据完整性和数据保密性的信息传输加密；实现通信记录和统计分析等。

1.2　威胁网络安全的因素

计算机安全事业始于 20 世纪 60 年代。当时，计算机系统的脆弱性已日益为美国政府和私营的一些机构所认识。但是，由于当时计算机的速度和性能比较落后，使用的范围也不广，再加上美国政府把它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内。

进入 20 世纪 80 年代后，计算机的性能得到了成百上千倍的提高，应用的范围也在不断扩大，计算机已遍及世界各个角落。并且，人们利用通信网络把孤立的单机系统连接起来，相互通信和共享资源。但是，随之而来并日益严峻的问题是计算机信息的安全问题。人们在这方面所做的研究与计算机性能和应用的飞速发展不相适应，因此，网络安全已成为未来信息技术中的主要问题之一。

由于计算机信息有共享和易扩散等特性，它在处理、存储、传输和使用上有着严重的脆弱性，因此很容易被干扰、滥用、遗漏和丢失，甚至被泄露、窃取、篡改、冒充和破坏，还有可能受到计算机病毒的感染。

根据美国FBI的调查，美国每年因为网络安全造成的经济损失超过1.7亿美元。75%的公司报告财政损失是由于计算机系统的安全问题造成的。超过50%的安全威胁来自内部；入侵的来源首先是内部心怀不满的员工，其次为黑客，另外是竞争者等。无论是有意的攻击，还是无意的误操作，都将会给系统带来不可估量的损失。黑客威胁的报道如今已经屡见不鲜了，国内外甚至美国国防部的计算机网络也都常被黑客们光顾。

国内由于计算机及网络的普及较低，加之黑客们的攻击技术和手段都相应较为落后，因此，前几年计算机安全问题暴露得不是太明显，但随着计算机技术的飞速发展、普及，黑客的攻击技术和手段的不断提高，对我们本来就十分脆弱的系统带来了严重的威胁。据调查，国内考虑并实施完整安全措施的机构寥寥无几，很多机构仅仅简陋的用了一点点安全策略或根本无任何安全防范。

在计算机网络和系统安全问题中，常用的攻击手段和方式有：利用系统管理的漏洞直接进入系统；利用操作系统和应用系统的漏洞进行攻击；进行网络窃听，获取用户信息及更改网络数据；伪造用户身份、否认自己的签名；传输释放病毒和如Java/ActiveX控件来对系统进行有效控制；IP欺骗；摧毁网络结点；消耗主机资源致使主机瘫痪和死机等等。

1.2.1 网络的安全威胁

由于互联网络的发展，整个世界经济正在迅速地融为一体，而整个国家犹如一部巨大的网络机器。计算机网络已经成为国家的经济基础和命脉。计算机网络在经济和生活的各个领域正在迅速普及，整个社会对网络的依赖程度越来越大。众多的企业、组织、政府部门与机构都在组建和发展自己的网络，并连接到Internet上，以充分共享、利用网络的信息和资源。网络已经成为社会和经济发展的强大动力，其地位越来越重要。伴随着网络的发展，也产生了各种各样的问题，其中安全问题尤为突出。了解网络面临的各种威胁，防范和消除这些威胁，实现真正的网络安全已经成了网络发展中最重要的事情。

1. 网络面临的主要威胁

(1) 黑客的攻击　黑客对于大家来说，不再是一个高深莫测的人物，黑客技术逐渐被越来越多的人掌握和发展，目前，世界上有20多万个黑客网站，这些站点都介绍一些攻击方法和攻击软件的使用以及系统的一些漏洞，因而系统、站点遭受攻击的可能性就变大了。尤其是现在还缺乏针对网络犯罪卓有成效的反击和跟踪手段，使得黑客攻击的隐蔽性深，“杀伤力”强，这是网络安全的主要威胁。

(2) 管理的欠缺　网络系统的严格管理是企业、机构及用户免受攻击的重要措施。事实上，很多企业、机构及用户的网站或系统都疏于这方面的管理。据IT界企业团体ITAA的调查显示，美国90%的IT企业对黑客攻击准备不足。目前，美国有75%～85%的网站都抵挡不住黑客的攻击，约有75%的企业网上信息失窃，其中25%的企业损失在25万美元以上。

(3) 网络的缺陷　因特网的共享性和开放性使网上信息安全存在先天不足，因为其赖以生存的TCP/IP协议族，缺乏相应的安全机制，所以因特网最初的设计考虑是该网不会因局部故障而影响信息的传输，基本没有考虑安全问题，因此它在安全可靠、服务质量、带宽和方便性等方面存在着不适应性。

（4）软件的漏洞或“后门”　随着软件系统规模的不断增大，系统中的安全漏洞或“后门”也不可避免地存在，比如我们常用的操作系统，无论是 Windows 还是 UNIX 几乎都存在或多或少的安全漏洞，众多的各类服务器、浏览器、一些桌面软件都被发现过存在安全隐患。大家熟悉的“尼母达”、“中国黑客”等病毒都是利用微软系统的漏洞给企业造成了巨大损失；2003 年 8 月发生的“冲击波”病毒，给全球带来了巨大的灾难。可以说任何一个软件系统都可能会因为程序员的一个疏忽，或设计中的一个缺陷等原因而产生漏洞，这也是网络安全的主要威胁之一。

（5）企业网络内部　用户的误操作，资源滥用和恶意行为使得再完善的防火墙也无法抵御来自网络内部的攻击，也无法对网络内部的滥用做出反应。

2. 目前网络存在的威胁

（1）非授权访问　没有预先经过同意，就使用网络或计算机资源被看作是非授权访问，如有意避开系统访问控制机制，对网络设备及资源进行非正常使用，或擅自扩大权限，越权访问信息等。非授权访问主要有以下几种形式：假冒、身份攻击、非法用户进入网络系统进行违法操作、合法用户以未授权方式进行操作等。

非授权访问的威胁涉及到受到影响的用户数量和可能被泄露的信息。对于某些组织来说，侵入是一件很难办的事，它将动摇该组织中其他人的信心。而入侵者往往将目标对准政府部门或学术组织。

（2）信息泄漏或丢失　指敏感数据在有意或无意中被泄漏出去或丢失，它通常包括，信息在传输中丢失或泄漏（如“黑客”们利用电磁泄漏或搭线窃听等方式可截获机密信息，或通过对信息流向、流量、通信频度和长度等参数的分析，推出有用信息，如用户口令、帐号等重要信息。），信息在存储介质中丢失或泄漏，通过建立隐蔽隧道等窃取敏感信息等。

信息泄露取决于可能泄密的信息的类型。具有严格分类的信息系统不应该直接连接 Internet。私人信息、健康信息、公司计划、信用记录等都具有一定程度的机密性，必须给予保护。

（3）破坏数据完整性　以非法手段窃得对数据的使用权，删除、修改、插入或重发某些重要信息，以取得有益于攻击者的响应；恶意添加，修改数据，以干扰用户的正常使用。

（4）拒绝服务攻击　它不断对网络服务系统进行干扰，改变其正常的作业流程，执行无关程序使系统响应减慢甚至瘫痪，影响正常用户的使用，甚至使合法用户被排斥而不能进入计算机网络系统或不能得到相应的服务。

拒绝服务会影响许多与用户或单位的生存至关重要的任务。攻击者通过一些常用的黑客手段侵入并控制一些网站，使得网络系统拒绝服务，造成其网络严重瘫痪。因此，在将这种系统连接网络之前，必须慎重地评价使系统丢失服务的威胁。

（5）利用网络传播病毒　通过网络传播计算机病毒，其破坏性大大高于单机系统，而且用户很难防范。

当然，网络威胁并不是对计算机安全性的惟一威胁，也不是惟一的原因。因为网络安全性仅是一个大的计算机安全规划的一部分，还应包括物理安全性和灾害恢复计划等。

3. 网络安全威胁的几种类型

(1) 物理方式 所谓物理安全就是指，保护网络信息相关的硬件设备不受到破坏和接触。最常见的物理威胁包括偷窃、废物搜寻、间谍行为与证件伪造等内容。

(2) 认证系统 所谓认证系统就是指，通过一定手段识别用户是否具有接受或者提供某种服务的权力。如果没有认证系统，网络服务就没有安全性可言。

(3) 物理连接 网络的使用，即网络线缆的连接，对计算机数据造成了新的安全威胁，这些威胁包括窃听、拨号进入、冒名顶替等内容。

(4) 系统漏洞 系统漏洞是指系统的建立者或者用户在有意或者无意的情况下，在系统中产生了不经过认证就能访问系统资源或者享有系统的服务。这种威胁包括服务安全、初始化、配置和用户疏忽。

(5) 编程 许多网络信息安全问题来自编程，包括构建系统的代码本身的问题和人为构建恶意代码破坏系统。这种攻击往往都是致命的。

各种威胁对网络安全特性的影响如表 1.1 所示。

表 1.1 各种威胁对网络安全特性的影响

威胁	保密性	完整性	可访问性	法律/伦理
偷窃	×	×	×	×
废物回收	×			
间谍行为	×	×	×	×
证件伪造	×	×		×
口令圈套	×	×	×	
口令破解	×	×	×	
算法问题	×	×	×	
口令过简	×	×	×	
窃听	×			×
拨号进入	×	×	×	
冒名顶替	×	×	×	
服务安全	×	×	×	
初始化	×	×	×	
配置	×	×	×	
用户疏忽	×	×	×	
计算机病毒	×	×	×	×
特洛伊木马	×	×	×	
逻辑炸弹		×	×	×
恶意代码	×	×	×	
“×”表示此项威胁影响到网络安全特性				

1.2.2 网络安全的问题及原因

随着 Internet 的商业化，越来越多的企业也进入网络并在网上开展业务，从而使得网际互联的安全问题日益突出，网上犯罪及侵权行为加速增长。

(1) 微软网络软件中一个原来未知的缺陷让一名在线攻击者控制了美国国防部服务器的公开接口。

(2) 中国工商银行在网上发出重要提示，称有黑客利用工行网管公开邮箱向顾客发出信件索要银行卡帐户和密码。

(3) Linus 称 Linux 内核存在漏洞，该故障能使那些只许登录某机器的局部用户获得"根目录"访问权，并对该机器进行完全控制。这种局部缺陷造成的不良后果比远程缺陷要轻，远程缺陷能让网络攻击者接管某机器，即使这些攻击者连基本的用户帐号都没有。

(4) 中文搜索网站百度遭到中国互联网有史以来罕见黑客攻击。攻击最严重的时候，每秒钟攻击次数高达 1000 次，同一个词被查询次数最多达 38 863 次。据互联网技术专家介绍，每秒钟攻击 100 次就已经属于非常严重的攻击，而每秒钟 1000 次的攻击就实属罕见。

(5) 市场调查机构 IDC 研究发现，亚洲企业网络曾遭黑客入侵的比例高达 72%，另外则有 39%的受访者反映，他们觉得过去一年的网络安全威胁在升高。

从上述例子中，不难发现网络信息安全的问题不但已经广泛的深入到了日常生活的很多领域，而且无论是硬件产品、软件产品、操作系统还是应用软件都可能存在安全漏洞。据悉，全球至少有 100 多个国家制定了计算机间谍计划。美国国家安全局(NSA)通过对美国宇航局控制的两组路由器进行监测，已经侦破了数十万个外国计算机系统的口令和地址，并用于侵入 Internet 网，以获取情报。美国国防部对其加入 Internet 网的 12 000 台计算机系统所做的安全测试，发现入侵的成功率竟高达 88%。在 1995 年美国曾受到 25 万次攻击，其中有 16 万次得手。美国国家安全局已把防止美国五角大楼信息系统遭受非法入侵作为一项重要的工作任务。

自从互联网诞生以来，安全缺陷、侵犯以及灾难性的事件的数量正在随着时间的推移而增加。Internet 是跨时空的，其开放性决定了网络安全无国界，尽管我国对 Internet 的应用不如发达国家，但依旧受到网络安全问题的严重威胁。中国公安部公众信息网络安全监察局统计发现 2002 年中国互联网用户中，83.98%的用户受到了网络安全问题的影响，比 2001 年上升十个百分点；因为网络安全问题造成损失的用户占到了总用户的 64.05%。

目前，攻击 Internet 的手段是多种多样的，攻击方法已超过计算机病毒种类，总数达数千种，而且很多都是致命的。围绕着信息与信息技术，建立在深刻的科学理论和高新技术基础上，大到国家、小至个人之间都展开了尖锐激烈的斗争。谁掌握了信息——当今最重要的战略资源，谁就掌握了主动权，信息安全问题已经成为信息化社会的焦点。因此根据我国的特点，制定适合的网络安全策略，构筑我国的信息安全防范体系，开发我国的信息安全产品，形成信息安全的民族产业，是关系国计民生和国家安全的大事，无论从政治上还是从经济上，信息安全技术都是极为重要的。