21世纪高校规划教材

网络安全与管理

主编 涂 敏 胡颖辉

江西高校出版社

21世纪高校规划教材

网络安全与管理

主　编：涂　敏　胡颖辉
副主编：雷　虎　冯为华　邹贤芳
龙全圣　刘　锦

江西高校出版社

图书在版编目(CIP)数据

网络安全与管理/涂敏,胡颖辉主编. —南昌:江西高校出版社,2009.1

ISBN 978-7-81132-454-9

Ⅰ.网... Ⅱ.①涂... ②胡... Ⅲ.计算机网络-安全技术 Ⅳ.TP393.08

中国版本图书馆 CIP 数据核字(2009)第 013381 号

出版发行	江西高校出版社
社　　址	江西省南昌市洪都北大道 96 号
邮政编码	330046
总编室电话	(0791)8504319
销售电话	(0791)8508191
网　　址	www.juacp.com
印　　刷	江西农业大学印刷厂
照　　排	江西太元科技有限公司照排部
经　　销	各地新华书店
开　　本	787mm×1092mm　1/16
印　　张	20.25
字　　数	492 千字
版　　次	2009 年 2 月第 1 版第 1 次印刷
印　　数	1~3000 册
书　　号	ISBN 978-7-81132-454-9
定　　价	32.80 元

21世纪高校规划教材计算机专业

编委会(按姓氏笔画排列)

前 言

随着计算机网络技术与应用的不断发展，计算机系统和网络广泛应用于国家的许多部门，伴随而来的计算机系统安全问题越来越引起人们的关注。许多重要资料存储于计算机中，计算机系统一旦遭受破坏，将给使用单位造成重大经济损失，并严重影响正常工作的顺利开展。如果一些重要部门的计算机被攻击，将造成不可估量的损失。如何避免这些损失，网络安全意义重大。学习与普及计算机网络安全知识，是信息化建设工作的重要内容之一。

本教材吸收了国内外教材的优点，结合我们多年的网络安全教学经验，充分强调实践操作，突出培养职业技能。在编写本教材时，对计算机网络安全的理论知识和工作原理介绍得简单一些，更多的内容侧重于对计算机具体网络安全技术应用的介绍，体现出注重培养学生实际应用技术能力的特点。

网络安全是一门涉及计算机科学、网络技术、通信技术、密码技术等多种学科的综合性学科。全书介绍了网络安全基础知识、网络安全的协议、网络操作系统安全、网络攻防技术、恶意代码分析与防治、数据加密技术与数据完整性保护、防火墙技术与入侵检测、IP 安全与 WEB 安全等内容，并附有实训及习题。在编写的过程中，力求体现教材的系统性、先进性和实用性。

本书由涂敏、胡颖辉任主编，雷虎、冯为华、邹贤芳、龙全圣和刘锦任副主编，罗磊、朱晶、刘锦、胡颖辉、邹贤芳、冯为华、雷虎、马俊祺、龙全圣、张亮、徐涌、彭志德、黄雅琼、郭春兰、涂敏共同完成本书的编写。涂敏、胡颖辉、冯为华、龙全圣、刘锦负责本教材的统稿及审阅。

由于编者水平有限，不当之处在所难免，恳请广大读者不吝指正。

编 者

2009 年 1 月

目 录

第 1 章 网络安全概述 …… 1
1.1 网络安全概述 …… 1
1.1.1 网络安全基本概念 …… 1
1.2 网络安全的威胁与现状 …… 2
1.2.1 网络安全面临的威胁 …… 2
1.3 网络安全体系结构 …… 3
1.3.1 物理安全 …… 3
1.3.2 网络安全 …… 4
1.3.3 信息安全 …… 6
1.3.4 安全管理 …… 8
1.4 网络安全的评价体系 …… 9
1.4.1 网络安全评价的重要性 …… 9
1.4.2 计算机系统的安全标准 …… 10
1.4.3 计算机系统的安全等级 …… 11
1.5 相关法律法规 …… 11
1.5.1 计算机安全立法的必要性 …… 11
1.5.2 计算机安全法规简介 …… 12
1.6 实训 …… 12
1.6.1 虚拟机的配置 …… 12
1.6.2 网络嗅探器的安装与作用 …… 18
习题 …… 25

第 2 章 网络安全的协议基础 …… 26

2.1 OSI 参考模型与 TCP/IP 协议簇 …… 26
2.1.1 OSI 参考模型 …… 26
2.1.2 OSI 七层模型功能简介 …… 27
2.1.3 TCP/IP 协议簇 …… 27
2.1.4 OSI 参考模型与 TCP/IP 协议的对比 …… 28
2.2 分组交换与数据包的结构 …… 29
2.2.1 分组交换 …… 29
2.2.2 包结构分析 …… 30
2.2.3 IPV6 与 IPV4 的分析 …… 31
2.2.4 IPV6 数据包结构 …… 32
2.3 数据包的捕获与分析 …… 32

2.3.1 数据包的捕获 …… 33
2.3.2 数据包的分析—以太网工作方式 …… 34
2.4 数据的分析 …… 34
2.4.1 捕获 FTP 命令底层数据包 …… 35
2.4.2 网络接口层 DLC 帧结构详解 …… 35
2.4.3 网络层 IP 数据包结构详解 …… 36
2.4.4 传输层 TCP 数据包结构详解 …… 37
2.4.5 TCP 的三次握手与四次挥手 …… 39
2.5 实训 …… 40
习题 …… 51

第 3 章 网络操作系统安全 …… 53

3.1 网络操作系统 …… 53
3.1.1 UNIX 操作系统 …… 53
3.1.2 Linux 操作系统 …… 55
3.1.3 Windows 网络操作系统 …… 57
3.2 操作系统的安全与访问控制 …… 59
3.2.1 计算机操作系统安全 …… 59
3.2.2 安全操作系统的机制与访问控制 …… 60
3.3 常用网络安全命令 …… 62
3.3.1 Ipconfig 命令 …… 62
3.3.2 Ping 命令 …… 63
3.3.3 ARP 命令 …… 65
3.3.4 Netstat 命令 …… 66
3.3.5 NET 命令 …… 68
3.3.6 AT 命令 …… 71
3.3.7 Tracert 命令 …… 72
3.3.8 Nslookup 命令 …… 73
3.4 Windows Server 2003 的安全 …… 73
3.4.1 使用 NTFS 文件系统 …… 74
3.4.2 计算机账户和用户账户配置 …… 76
3.4.3 安全策略配置 …… 77
3.4.4 加密与备份 …… 81
3.4.5 关闭不必要的端口和服务 …… 83
3.4.6 其他安全配置 …… 86
3.4.7 借助第三方软件增强 Windows Server 2003 操作系统安全 …… 88
3.5 其他网络操作系统的安全 …… 91
3.5.1 UNIX 系统的安全 …… 91
3.5.2 LINUX 系统的安全 …… 92

3.6 实训 …… 93
3.6.1 常用的网络安全命令的使用实训 …… 93
3.6.2 Windows Server 2003 操作系统安全配置 …… 93
习题 …… 94

第 4 章 网络攻防技术 …… 96

4.1 网络攻防概述 …… 96
4.1.1 黑客简介 …… 96
4.1.2 网络攻击防御体系 …… 97
4.1.3 网络攻击的分类 …… 99
4.1.4 网络攻击步骤 …… 100
4.2 网络攻防工具 …… 101
4.2.1 木马程序 …… 101
4.2.2 扫描工具 …… 104
4.2.3 破解工具 …… 106
4.2.4 炸弹工具 …… 107
4.2.5 安全防御工具 …… 108
4.3 基于协议的攻击技术与防御技术 …… 109
4.3.1 ARP 协议漏洞攻击与防御 …… 109
4.3.2 ICMP 协议漏洞攻击与防御 …… 113
4.3.3 TCP 协议漏洞攻击与防御 …… 116
4.3.4 其他协议明文传输漏洞攻击与防御 …… 118
4.4 操作系统漏洞攻击技术与防御技术 …… 121
4.4.1 输入法漏洞攻击与防御 …… 121
4.4.2 IPC $ 攻击与防御 …… 124
4.4.3 RPC(Remote Procedure Call)漏洞攻击与防御 …… 127
4.5 针对 IIS 漏洞攻击技术与防御技术 …… 130
4.5.1 Unicode 漏洞攻击与防御 …… 130
4.5.2 IDA&IDQ 缓冲区溢出漏洞攻击与防御 …… 135
4.5.3 Pinter 溢出漏洞入侵与防御 …… 136
4.6 Web 应用漏洞攻击技术与防御技术 …… 138
4.6.1 针对数据库漏洞 …… 138
4.6.2 Cookie 攻击 …… 140
4.6.3 上传漏洞 …… 143
4.6.4 跨站攻击 XSS …… 144
4.7 实训 …… 147
4.7.1 网络攻防工具的使用实训 …… 147
4.7.2 基于协议的攻击与防御实训 …… 152
4.7.3 操作系统漏洞攻击与防御实训 …… 155

4.7.4 针对 IIS 漏洞攻击与防御实训 …… 158
4.7.5 针对 Web 应用漏洞攻击实训 …… 159
习题 …… 161

第 5 章 恶意代码分析与防治 …… 163

5.1 恶意代码概述 …… 163
5.1.1 研究恶意代码的必要性 …… 163
5.1.2 恶意代码的发展史 …… 164
5.1.3 恶意代码长期存在的原因 …… 164
5.1.4 恶意代码的定义 …… 165
5.2 恶意代码实现的关键技术 …… 166
5.2.1 恶意代码生存技术 …… 166
5.2.2 恶意代码攻击技术 …… 168
5.2.3 恶意代码的隐蔽技术 …… 169
5.3 恶意代码查杀与防范 …… 171
5.3.1 常见的恶意代码 …… 171
5.3.2 木马 …… 172
5.3.3 蠕虫 …… 177
5.3.4 恶意代码防范方法 …… 182
5.4 实训 …… 185
5.4.1 宏病毒工作原理 …… 185
5.4.2 U 盘病毒的工作原理 …… 187
5.4.3 查杀病毒 …… 188
习题 …… 189

第 6 章 数据加密技术与数据完整性保护 …… 191

6.1 数据加密技术概述 …… 191
6.1.1 密码技术的起源和概述 …… 191
6.1.2 什么是数据加密 …… 192
6.1.3 基本概念 …… 193
6.1.4 密码的分类 …… 194
6.2 密码学发展史 …… 195
6.2.1 古典密码 …… 195
6.2.2 近代密码 …… 196
6.2.3 现代密码学的发展 …… 198
6.3 传统和现代密码体制 …… 199
6.3.1 密码体制 …… 199
6.3.2 DES 简介 …… 202
6.3.3 RSA 简介 …… 203

6.3.4 PKI(公共密钥基础设施)与 CA(认证机构) …… 204
6.4 信息摘要技术 …… 206
6.4.1 信息摘要简介 …… 206
6.4.2 信息摘要算法 MD5 …… 207
6.5 数字签名技术 …… 208
6.5.1 数字签名的概念 …… 208
6.5.2 带加密的数字签名 数字签名的应用 RSA 公钥签名技术 …… 209
6.5.3 数字签名的应用 …… 212
6.6 实训 …… 213
6.6.1 免费数字证书申请与导入 …… 213
6.6.2 使用加密软件 PGP 加密邮件与邮件签名 …… 226
习题 …… 230

第 7 章 防火墙技术与入侵检测 …… 232

7.1 防火墙概念 …… 232
7.1.1 防火墙基本概念 …… 232
7.1.2 防火墙的目的与作用 …… 233
7.2 防火墙的技术分类 …… 233
7.2.1 包过滤型防火墙 …… 233
7.2.2 IP 级包过滤型防火墙 …… 233
7.2.3 代理服务器型防火墙 …… 235
7.2.4 其他类型的防火墙 …… 236
7.3 防火墙基本体系结构 …… 237
7.3.1 过滤路由器防火墙结构 …… 237
7.3.2 双宿主主机防火墙结构 …… 237
7.3.3 主机过滤型防火墙结构 …… 238
7.3.4 子网过滤型防火墙结构 …… 239
7.3.5 吊带式防火墙结构 …… 239
7.3.6 典型的防火墙结构 …… 240
7.4 入侵检测概念 …… 240
7.5 入侵检测的基本方法 …… 241
7.5.1 Linux 系统入侵检测方法 …… 241
7.5.2 Window 系统下入侵检测方法 …… 244
7.6 入侵检测步骤 …… 247
7.6.1 通常黑客入侵步骤介绍 …… 247
7.6.2 入侵检测步骤介绍 …… 248
7.6.3 常用检查是否安装了入侵工具或后门的方法介绍 …… 249
7.6.4 Linux 系统入侵检测 …… 252
7.7 实训 …… 252

7.7.1 费尔个人防火墙配置与管理 …… 252
7.7.2 Snort 使用 …… 258
习题 …… 262

第 8 章 Internet 安全 …… 264

8.1 IPSec 安全 …… 264
8.1.1 IPSec 协议簇 …… 265
8.1.2 IPSec 的作用方式 …… 266
8.1.3 IPSec 的实施 …… 267
8.1.4 密钥交换协议 IKE …… 269
8.1.5 IPSec 的优势 …… 270
8.1.6 IPSec 的用途 …… 271
8.1.7 虚拟专用网技术 …… 271
8.2 Web 安全概述 …… 273
8.2.1 SSL 协议简介 …… 274
8.2.2 安全的电子交易协会 …… 276
8.3 DNS 安全 …… 278
8.3.1 DNS 域名系统 …… 278
8.3.2 DNS 安全面临的挑战 …… 279
8.3.3 DNS 安全攻击与防范 …… 280
8.4 实训 …… 281
8.4.1 实训:在 WINDOWS 2000 操作系统中利用 PPTP 配置 VPN 网络 …… 281
8.4.2 实训:在 WINDOWS 中配置 IPSec 实现 VPN 的连接 …… 288
8.4.3 应用 SSL 建立安全 Web …… 299
习题 …… 310

参考书目 …… 312

第1章 网络安全概述

【本章重点与难点】

网络安全的6个要求；网络安全体系结构的组成方面。

【教学要求】

理解网络安全定义、网络安全6大要求，了解网络安全面临的威胁及现状，掌握网络安全体系结构的几个组成部分，了解我国计算机安全的相关法律法规。

1.1 网络安全概述

随着计算机网络技术的飞速发展和网络覆盖范围的迅速扩大，计算机网络安全问题也日益显得复杂和突出起来。网络安全涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等多种学科。网络安全从其本质上来讲就是网络安全和网络上的信息安全。如何更有效的保护重要的信息数据，以及提高计算机网络系统的安全性已经成为所有计算机网络应用必须考虑和解决的一个重要问题。

1.1.1 网络安全基本概念

网络安全的定义在不同的环境和应用中会得到不同的解释：有的是指运行系统的安全，保证系统的合法操作和正常运行；有的是指网络上系统信息的安全，包括用户口令鉴别、存取权限控制和数据加密信息等；有的是指网络上信息内容的安全，侧重保护信息的保密性、真实性和完整性等。从此可以看出，网络安全与其所保护的信息对象有关。从本质上来讲，网络安全就是网络中信息的安全，它涉及的领域相当广泛，凡涉及网络信息的保密性、完整性、真实性、可用性、可控性和可靠性的相关技术和理论均是网络安全研究的内容。

网络安全是指保护网络系统中的软件、硬件及信息资源，使之免受偶然或恶意的破坏、篡改和泄露，保证网络系统的正常运行、网络服务不中断。网络安全技术主要包括计算机安全技术、信息交换设备安全技术、身份认证技术、访问控制技术、密码技术、防火墙技术和安全管理技术等。

随着网络技术和应用的飞速发展，人们对系统安全也不断提出新的要求。网络系统安全主要要求如下：

1. 保密性

保密性包含两点内容：一是保证计算机及网络系统的硬件、软件和数据只为合法用户所使用。可以采用专用的加密线路实现，如使用虚拟专网(VPN)建构网络；二是由于无法绝对防止非法用户截取网络上的数据，故必须采用数据加密技术以确保数据本身的保密性。

2. 完整性

完整性是指应确保信息在传递过程中的一致性，即收到的可能是发出的。为了防止非法用户对数据的增加、删除或改变顺序，必须采用数据加密和校验技术。用户信息和网络信息都要求完整性，例如涉及金融的用户信息，如果用户账号被修改、伪造或删除，将带来巨大的经济损失。网络中的网络信息一旦受到破坏，严重的还会造成通信网的瘫痪。

3. 可靠性

可靠性是指系统在规定条件下和规定时间内完成规定功能的概率。可靠性是网络安全最基本的要求之一。如果网络不可靠，事故不断，也就根本谈不上网络的安全。目前，对于网络的可靠性的研究基本上偏重于硬件可靠性方面。研制高可靠性元器件设备，采取合理的备份措施仍是最基本的可靠性对策。

4. 可用性

可用性是指信息和通信服务在需要时允许授权人或实体使用。可用性是网络面向用户的基本安全要求。网络最基本的功能是向用户提供所需的信息和通信服务，而用户的通信要求是随机的、多方面的，有时还要求时效性。网络必须随时满足用户通信的要求。从某种意义上讲，可用性是可靠性的更高要求，特别是在重要场合下，特殊用户的可用性显得十分重要。为此，网络需要采用科学合理的网络拓扑结构、容错和备份措施以及网络自愈技术、分配配置、负荷分担、各种完善的物理安全和应急措施等，从满足用户需要出发，保证信网的安全。

5. 不可抵赖性

不可抵赖性也称作不可否认性，是面向通信双方（人、实体或进程）信息真实、同一的安全要求。它包括收发双方均不可抵赖。随着通信业务的不断扩大，电子贸易、电子金融、电子商务和办公自动化等许多信息处理过程都需要通信双方对信息内容的真实性进行认同，为此，应采用数字签名、认证、数据完备、鉴别等有效措施，以实现信息的不可抵赖性。

6. 可控性

可控性是指对信息的传播路径、范围及其内容所具有的控制能力。它规定了合法用户对数据的访问能力，包括哪些用户有权访问数据、访问哪些数据、何时访问和对数据拥有什么操作权限等。

1.2 网络安全的威胁与现状

1.2.1 网络安全面临的威胁

计算机网络面临的威胁大体可分为两种：一是对网络中信息的威胁；二是对网络中设备的威胁。影响计算机网络安全的因素很多，如系统存在的漏洞、系统安全体系的缺陷、使用人员薄弱的安全意识及管理制度等，诸多的原因使网络安全面临的威胁日益严重。主要来自下面几方面：

1. 窃听

攻击者通过搭线或在电磁波辐射的范围内安装接受装置等方式，截取机密信息，或通过对信息流的流向、通信频度和长度等参数的分析，推出有用信息。它不破坏传输信息的内容，不易被察觉。

2.非法访问

没有预先经过同意,就使用网络或计算机资源被看做非法访问。它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。

3.破坏信息的完整性

可以从篡改、删除、插入3方面破坏信息的完整性。篡改指改变信息流的次序、时序,更改信息的内容、形式。删除指删除某个信息或信息的某些部分。插入指在信息中插入另一些信息,让接收方读不懂或接收错误的信息。

4.破坏系统的可用性

破坏系统的可用性包括使合法用户不能正常访问网络资源、使有严格时间要求的服务不能及时得到响应、恶意摧毁系统等。

5.来自内部的威胁

来自内部的威胁主要包括内部涉密人员有意或无意的泄密、更改记录信息、内部非授权人员有意或无意的偷窃机密信息、更改网络配置和记录信息,内部人员破坏网络系统等。

6.重演

重演指截获并录制信息,然后在必要的时候重发或反复发送这些信息。

7.行为否认

行为否认包括发信者事后否认曾经发送过某条消息或其内容、收信者事后否认曾经接收过某条消息或其内容。

8.拒绝服务攻击

拒绝服务攻击指通过某种方法使系统响应减慢甚至瘫痪,阻止合法用户获得服务。

9.病毒传播

通过网络传播计算机病毒,其破坏性非常高,而且用户很难防范。

10.其他威胁

对网络系统的威胁还包括电磁泄露、软硬件故障、各种自然灾害、人为操作失误等。

1.3 网络安全体系结构

通过对网络的全面了解,按照安全策略的要求及风险分析的结果,整个网络措施应按系统体系建立。具体的安全控制系统由以下几个方面组成:物理安全、网络安全、信息安全。

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或错误及各种计算机犯罪行为导致的破坏过程。它主要包括三个方面:

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;(参见国家标准GB50173-93《电子计算机机房设计规范》、国标GB2887-89《计算站场地技术条件》、GB9361-88《计算站场地安全要求》);

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

网络安全是整个安全解决方案的关键，本小节从以下几个方面分别进行说明：

1.隔离及访问控制系统

主要分内外网隔离及访问控制系统和内部网不同网络安全域的隔离及访问控制两大部分。

(1)内外网隔离及访问控制系统

在内部网与外部网之间，设置防火墙(包括分组过滤与应用代理)实现内外网的隔离与访问控制是保护内部网安全的最主要，同时也是最有效、最经济的措施之一。

防火墙技术可根据防范的方式和侧重点的不同而分为很多种类型，但总体来讲有两大类较为常用：分组过滤、应用代理。

1)分组过滤(Packet Filtering)：作用在网络层和传输层，它根据分组包头源地址，目的地址和端口号、协议类型等标志确定是否允许数据包通过。只有满足过滤逻辑的数据包才被转发到相应的目的地出口端，其余数据包则被从数据流中丢弃。

2)应用代理(Application Proxy)：也叫应用网关(Application Gateway)，它作用在应用层，其特点是完全“阻隔”了网络通信流，通过对每种应用服务编制专门的代理程序，实现监视和控制应用层通信流的作用。实际中的应用网关通常由专用工作站实现。

无论何种类型防火墙，从总体上看，都应具有以下五大基本功能：过滤进、出网络的数据；管理进、出网络的访问行为；封堵某些禁止的业务；记录通过防火墙的信息内容和活动；对网络攻击的检测和告警。

应该强调的是，防火墙是整体安全防护体系的一个重要组成部分，而不是全部。因此必须将防火墙的安全保护融合到系统的整体安全策略中，才能实现真正的安全。

(2)内部网不同网络安全域的隔离及访问控制

在这里，防火墙被用来隔离内部网络的一个网段与另一个网段。这样，就能防止影响一个网段的问题穿过整个网络传播。针对某些网络，在某些情况下，它的一些局域网的某个网段比另一个网段更受信任，或者某个网段比另一个更敏感。而在它们之间设置防火墙就可以限制局部网络安全问题对全局网络造成的影响。

2.网络安全检测

网络安全性分析系统，网络系统的安全性取决于网络系统中最薄弱的环节。如何及时发现网络系统中最薄弱的环节？如何最大限度地保证网络系统的安全？最有效的方法是定期对网络系统进行安全性分析，及时发现并修正存在的弱点和漏洞。

网络安全检测工具通常是一个网络安全性评估分析软件，其功能是用实践性的方法扫描分析网络系统，检查报告系统存在的弱点和漏洞，建议补救措施和安全策略，达到增强网络安全性的目的。

3.审计与监控

审计是记录用户使用计算机网络系统进行所有活动的过程，它是提高安全性的重要工具。它不仅能够识别谁访问了系统，还能指出系统正被怎样地使用。对于确定是否有网络

攻击的情况，审计信息对于确定问题和攻击源很重要。同时，系统事件的记录能够更迅速和系统地识别问题，并且它是后面阶段事故处理的重要依据。另外，通过对安全事件的不断收集与积累并且加以分析，有选择性地对其中的某些站点或用户进行审计跟踪，以便对发现或可能产生的破坏性行为提供有力的证据。

因此，除使用一般的网管软件和系统监控管理系统外，还应使用目前以较为成熟的网络监控设备或实时入侵检测设备，以便对进出各级局域网的常见操作进行实时检查、监控、报警和阻断，从而防止针对网络的攻击与犯罪行为。

4.网络反病毒

由于在网络环境下，计算机病毒有不可估量的威胁性和破坏力，所以计算机病毒的防范是网络安全性建设中重要的一环。

网络反病毒技术包括预防病毒、检测病毒和消毒三种技术：

(1)预防病毒技术：它通过自身常驻系统内存，优先获得系统的控制权，监视和判断系统中是否有病毒存在，进而阻止计算机病毒进入计算机系统和对系统进行破坏。这类技术有：加密可执行程序、引导区保护、系统监控与读写控制(如防病毒卡等)。

(2)检测病毒技术：它是通过对计算机病毒的特征来进行判断的技术，如自身校验、关键字、文件长度的变化等。

(3)消毒技术：它通过对计算机病毒的分析，开发出具有删除病毒程序并恢复原文件的软件。

网络反病毒技术的具体实现方法包括对网络服务器中的文件进行频繁地扫描和监测；在工作站上用防病毒芯片和对网络目录及文件设置访问权限等。

5.网络备份系统

备份系统为一个目的而存在：尽可能快地全盘恢复运行计算机系统所需的数据和系统信息。根据系统安全需求可选择的备份机制有：场地内高速度、大容量自动的数据存储、备份与恢复；场地外的数据存储、备份与恢复；对系统设备的备份。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，同时亦是系统灾难恢复的前提之一。

一般的数据备份操作有三种。一是全盘备份，即将所有文件写入备份介质；二是增量备份，只备份那些上次备份之后更改过的文件，是最有效的备份方法；三是差分备份，备份上次全盘备份之后更改过的所有文件，其优点是只需两组磁带就可恢复最后一次全盘备份的磁带和最后一次差分备份的磁带。

在确定备份的指导思想和备份方案之后，就要选择安全的存储媒介和技术进行数据备份，有“冷备份”和“热备份”两种。热备份是指“在线”的备份，即下载备份的数据还在整个计算机系统和网络中，只不过传到另一个非工作的分区或是另一个非实时处理的业务系统中存放。“冷备份”是指“不在线”的备份，下载的备份存放到安全的存储媒介中，而这种存储媒介与正在运行的整个计算机系统和网络没有直接联系，在系统恢复时重新安装，有一部分原始的数据长期保存并作为查询使用。热备份的优点是投资大，但调用快，使用方便，在系统恢复中需要反复调试时更显优势。热备份的具体做法是：可以在主机系统开辟一块非工作运行空间，专门存放备份数据，即分区备份；另一种方法是，将数据备份到另一个子系统中，通过主机系统与子系统之间的传输，同样具有速度快和调用方便的特点，但投资比较昂贵。

冷备份弥补了热备份的一些不足，二者优势互补，相辅相成，因为冷备份在回避风险中还具有便于保管的特殊优点。

在进行备份的过程中，常使用备份软件，它一般应具有以下功能。保证备份数据的完整性，并具有对备份介质的管理能力；支持多种备份方式，可以定时自动备份，还可设置备份自动启动和停止日期；支持多种校验手段（如字节校验、CRC 循环冗余校验、快速磁带扫描），以保证备份的正确性；提供联机数据备份功能；支持 RAID 容错技术和图像备份功能。

1.3.3 信息安全

主要涉及鉴别、信息传输的安全、信息存储的安全以及对网络传输信息内容的审计等方面。

1.鉴别

鉴别是对网络中的主体进行验证的过程，通常有三种方法验证主体身份。

一是只有该主体了解的秘密，如口令、密钥；口令机制：口令是相互约定的代码，假设只有用户和系统知道。口令有时由用户选择，有时由系统分配。通常情况下，用户先输入某种标志信息，比如用户名和 ID 号，然后系统询问用户口令，若口令与用户文件中的相匹配，用户即可进入访问。口令有多种，如一次性口令，系统生成一次性口令的清单，第一次时必须使用 X，第二次时必须使用 Y，第三次时用 Z，这样一直下去；还有基于时间的口令，即访问使用的正确口令随时间变化，变化基于时间和一个秘密的用户钥匙。这样口令每分钟都在改变，使其更加难以猜测。

二是主体携带的物品，如智能卡和令牌卡；智能卡：访问不但需要口令，也需要使用物理智能卡。在允许其进入系统之前检查是否允许其接触系统。智能卡大小形如信用卡，一般由微处理器、存储器及输入、输出设施构成。微处理器可计算该卡的一个唯一数（ID）和其他数据的加密形式。ID 保证卡的真实性，持卡人就可访问系统。为防止智能卡遗失或被窃，许多系统需要卡和身份识别码（PIN）同时使用。若仅有卡而不知 PIN 码，则不能进入系统。智能卡比传统的口令方法进行鉴别更好，但其携带不方便，且开户费用较高。

三是只有该主体具有的独一无二的特征或能力，如指纹、声音、视网膜或签字等。主体特征鉴别：利用个人特征进行鉴别的方式具有很高的安全性。目前已有的设备包括：视网膜扫描仪、声音验证设备、手型识别器。

2.数据传输安全系统

数据传输加密技术的目的是对传输中的数据流加密，以防止通信线路上的窃听、泄漏、篡改和破坏。如果以加密实现的通信层次来区分，加密可以在通信的三个不同层次来实现，即链路加密（位于 OSI 网络层以下的加密）、节点加密、端到端加密（传输前对文件加密，位于 OSI 网络层以上的加密）。

一般常用的是链路加密和端到端加密这两种方式。链路加密侧重于在通信链路上而不考虑信源和信宿，是对保密信息通过各链路采用不同的加密密钥提供安全保护。链路加密是面向节点的，对于网络高层主体是透明的，它对高层的协议信息（地址、检错、帧头帧尾）都加密，因此数据在传输中是密文的，但在中央节点必须解密得到路由信息。端到端加密则指信息由发送端自动加密，并进入 TCP/IP 数据包回封，然后作为不可阅读和不可识别的数据穿过互联网，当这些信息一旦到达目的地，将自动重组、解密，成为可读数据。端到端加密是