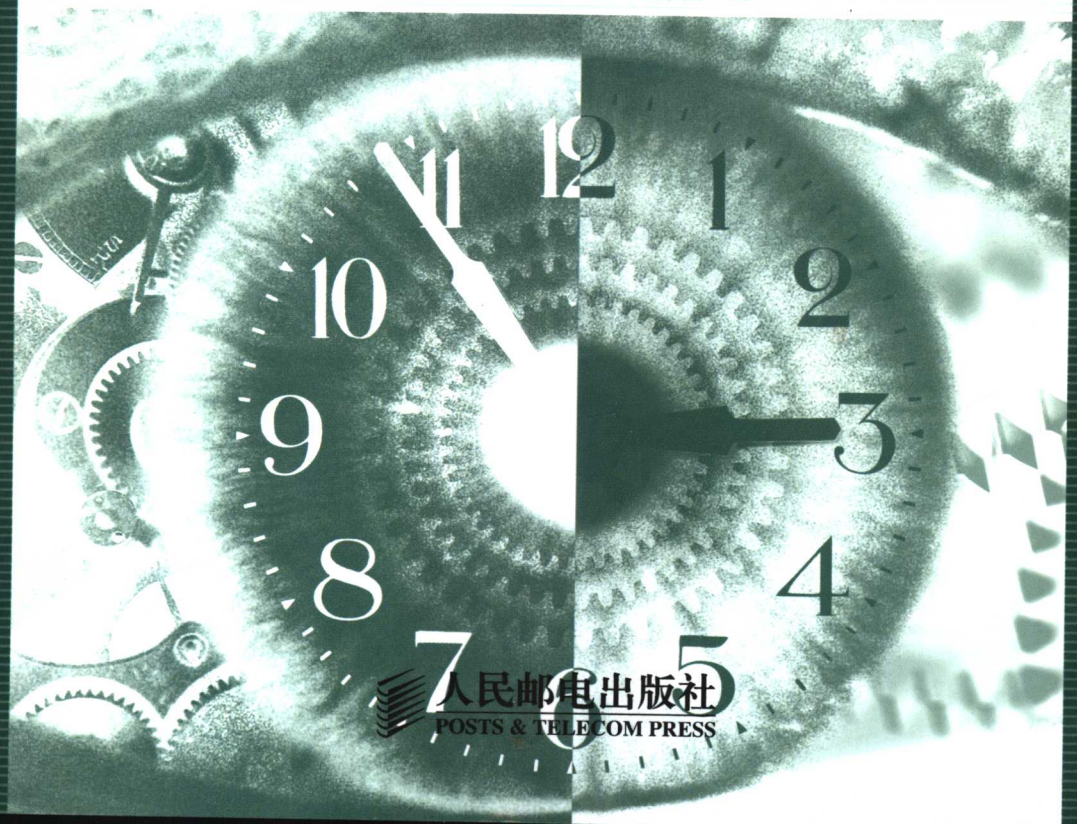
高职高专21世纪规划教材
GAOZHI GAOZHUAN 21 SHIJI GUIHUA JIAOCAI

计算机网络安全基础

■ 石淑华 池瑞楠 编著 ■



人民邮电出版社
POSTS & TELECOM PRESS

高职高专21世纪规划教材

计算机网络安全基础

石淑华　池瑞楠　编著

人民邮电出版社

图书在版编目（CIP）数据

计算机网络安全基础 / 石淑华，池瑞楠编著. —北京：人民邮电出版社，2005.5
ISBN 7-115-13368-9

Ⅰ. 计… Ⅱ. ①石…②池… Ⅲ. 计算机网络－安全技术－高等学校：技术学校－教材
Ⅳ. TP393.08

中国版本图书馆 CIP 数据核字（2005）第 024094 号

内 容 提 要

本书从网络安全维护的角度出发，全面介绍网络安全的基本框架，网络安全的基本理论，以及计算机网络安全方面的管理、配置和维护。全书共分 9 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、网络防病毒、数据加密、防火墙技术、入侵检测技术、Windows 2000 的安全、Web 的安全以及网络安全工程。

本书注重实用，以实验为依托，实验内容融合在课程内容中，使理论联系实际。书末附录中给出了每章练习题的参考答案，并列出了常用端口的信息。

本书可作为高职高专计算机及相关专业学生的教材，也可作为技术参考书或培训教材。

高职高专 21 世纪规划教材

计算机网络安全基础

◆ 编　　著　石淑华　池瑞楠
责任编辑　潘春燕

◆ 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　　电子函件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
读者热线　010-67170985
北京隆昌伟业印刷有限公司印刷
新华书店总店北京发行所经销

◆ 开本：787×1092　1/16
印张：15
字数：357 千字　　2005 年 5 月第 1 版
印数：1－5 000 册　　2005 年 5 月北京第 1 次印刷

ISBN 7-115-13368-9/TP・4644

定价：20.00 元

本书如有印装质量问题，请与本社联系　电话：（010）67129223

编者的话

目前，互联网正在不断改变我们工作、生活、学习以及娱乐的方式，并给我们带来了极大的便利。但是，随着互联网的空前发展以及互联网技术的不断普及，使得我们面临另外一个困境：私人数据、重要的企业资源以及政府机密等信息被暴露在公共网络空间之下，而互联网和 IP 体系的开放性使得这些重要的信息很容易被获取。黑客们可以通过不同类型的攻击威胁上述信息，而且这种威胁日益明显。计算机病毒的种类和数量迅猛增长，其危害和破坏也越来越大，不仅严重影响当前的信息化建设与工作，而且威胁到信息化长远战略。因此网络安全越来越受到重视。

根据高职高专院校的教学思想以及培养目标，通过调研社会上目前对网络安全方面人才的需求及技术要求，我们组织编写了这本教材。本书突出了网络安全管理与维护的培养目标，并参考了国际上权威认证 CIW 的课程。

本书是网络安全的入门教材。通过本书的学习，可以使学生了解网络安全的基本框架，网络安全的基本理论，以及计算机网络安全方面的管理、配置和维护。为学生今后进行网络管理、维护，以及安全技术服务奠定基础。

本书以实验为依托，实验内容融合在平时授课的内容中，使理论联系实际。本书的内容按照如下的思路进行安排。

在网络安全中，“攻与防”一直是矛盾的焦点，只有了解了攻击的原理、方法，才能够更好地防范，攻与防的技术都需要了解。因此本书首先分析网络所受到的威胁，介绍黑客的原理、常用工具，以及病毒的危害。本书的第 1 章为计算机网络安全概述；第 2 章介绍黑客常用的系统攻击方法；第 3 章介绍网络防病毒。

数据加密是信息安全的基础，许多产品、操作系统中都有各种各样的加密技术存在，数据加密在信息安全中的地位非常重要。目前网络安全技术(产品)有 4 大项：防病毒、防火墙、入侵检测（IDS）、VPN。因此接下来安排这些内容。本书第 4 章介绍数据加密技术；第 5 章介绍防火墙技术；第 6 章介绍入侵检测技术。

操作系统是一个网络应用的平台，因此有必要介绍操作系统的安全性、安全配置与管理，以及 IIS、Web 的安全。在网络安全管理中，专家们一致认为“30%的技术，70%的管理”，因此最后安排网络安全工程与管理的内容。本书第 7 章介绍 Windows 2000 的安全；第 8 章介绍 Web 的安全；第 9 章介绍网络安全工程。

本书共 9 章，课程的总体学时为 64～72 学时，各学校可以根据本校的教学设置和实验条件，对讲授内容、授课课时与实验课时进行适当调整。

本书由石淑华组织编写及统稿。其中第 1、2、3、5、6、7 章由石淑华编写，第 4、8、9 章由池瑞楠编写。在教材的编写过程中，深圳职业技术学院网络技术专业教研室的蔡学军、邹润生、梁广民、仵博、王隆杰、杨名川、张立涓老师在实验和绘图方面做了不少工作，并提出了许多宝贵意见，在此一并表示衷心感谢！

本书提供了部分练习题的参考答案，书中提到的一些工具软件在 Internet 上都可以下载

到，并且为了老师教学方便，订购本教材的老师可以登录出版社网站下载电子教案。

由于计算机网络安全技术发展迅速，加上编者水平有限，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@oa.szpt.net。

编　者

2005 年 2 月于深圳职业技术学院

目　录

第 1 章　计算机网络安全概述 …… 1

1.1　网络安全简介 …… 1
1.1.1　网络安全的重要性 …… 1
1.1.2　网络脆弱性的原因 …… 2
1.1.3　典型的网络安全事件 …… 3
1.2　信息安全的发展历程 …… 4
1.2.1　通信保密阶段 …… 4
1.2.2　信息安全阶段 …… 4
1.2.3　信息保障阶段 …… 5
1.3　网络安全的定义 …… 5
1.3.1　网络安全的定义 …… 5
1.3.2　网络安全的基本要素 …… 6
1.4　网络安全所涉及的内容 …… 6
1.5　网络安全防护体系 …… 9
1.5.1　网络安全的威胁 …… 9
1.5.2　网络安全的防护体系 …… 10
1.5.3　数据保密 …… 11
1.5.4　访问控制技术 …… 12
1.5.5　网络监控 …… 13
1.5.6　病毒防护 …… 13
1.6　网络安全的现状 …… 13
1.6.1　美国、俄罗斯网络安全的现状 …… 13
1.6.2　国内网络安全的现状 …… 14
练习题 …… 15

第 2 章　黑客常用的系统攻击方法 …… 17

2.1　黑客概述 …… 17
2.1.1　黑客的由来 …… 17
2.1.2　黑客攻击的动机 …… 18
2.1.3　黑客入侵攻击的一般过程 …… 19
2.2　网络扫描工具原理与使用 …… 20
2.2.1　扫描器的作用 …… 20
2.2.2　扫描器概述 …… 20

2.2.3 扫描器的原理 …… 25
2.3 网络监听原理与工具 …… 33
2.3.1 网络监听原理 …… 33
2.3.2 Sniffer 工具的介绍和使用 …… 36
2.4 木马 …… 40
2.4.1 木马的工作原理 …… 40
2.4.2 木马的分类 …… 40
2.4.3 木马的工作过程 …… 41
2.4.4 木马的隐藏与伪装方式 …… 42
2.4.5 木马的启动方式 …… 44
2.4.6 木马的检测 …… 46
2.4.7 木马的防御与清除 …… 47
2.4.8 木马的实例 …… 47
2.5 拒绝服务攻击 …… 49
2.5.1 拒绝服务攻击定义 …… 49
2.5.2 DoS 攻击分类 …… 50
2.5.3 分布式拒绝服务攻击 …… 52
2.6 缓冲区溢出 …… 53
2.6.1 缓冲区溢出原理 …… 53
2.6.2 缓冲区溢出实例分析 …… 55
2.6.3 缓冲区溢出的预防 …… 55
练习题 …… 56

第 3 章 网络防病毒 …… 58

3.1 计算机病毒的基本概念 …… 58
3.1.1 什么是计算机病毒 …… 58
3.1.2 计算机病毒发展简史 …… 58
3.1.3 计算机病毒的发展历程 …… 59
3.2 计算机病毒的特征 …… 61
3.3 计算机病毒的分类 …… 64
3.3.1 按照计算机病毒依附的操作系统分类 …… 64
3.3.2 按照计算机病毒的传播媒介分类 …… 64
3.3.3 按照计算机病毒的寄生方式和传染途径分类 …… 65
3.3.4 宏病毒 …… 67
3.4 计算机病毒的防治 …… 69
3.4.1 计算机病毒引起的异常现象 …… 69
3.4.2 计算机病毒诊断技术 …… 70
3.5 防病毒软件 …… 71
3.5.1 常用的单机杀毒软件的使用 …… 71

3.5.2 网络防病毒 …… 73
3.5.3 选择防病毒软件的标准 …… 78
3.5.4 网络防毒的整体方案 …… 79
3.6 网络病毒实例 …… 80
3.6.1 Nimda 病毒 …… 80
3.6.2 “震荡波”病毒 …… 82
练习题 …… 84

第 4 章 数据加密技术 …… 87

4.1 概述 …… 87
4.1.1 密码学的有关概念 …… 87
4.1.2 传统的加密技术 …… 88
4.2 对称加密算法 …… 91
4.2.1 DES 算法及其基本思想 …… 92
4.2.2 DES 算法的安全性分析 …… 93
4.2.3 DES 算法在网络安全中的应用 …… 94
4.3 公开密钥算法 …… 94
4.3.1 RSA 算法及其基本思想 …… 95
4.3.2 RSA 算法的安全性分析 …… 96
4.3.3 RSA 算法在网络安全中的应用 …… 96
4.4 数据加密技术的应用 …… 98
4.4.1 报文鉴别和 MD5 算法 …… 98
4.4.2 SSL 协议和 SET 协议 …… 100
4.4.3 PGP 加密系统 …… 102
练习题 …… 109

第 5 章 防火墙技术 …… 111

5.1 防火墙的概述 …… 111
5.1.1 防火墙的概述 …… 111
5.1.2 防火墙的概念 …… 111
5.1.3 防火墙的功能 …… 112
5.1.4 防火墙的发展历程 …… 113
5.2 防火墙实现技术原理 …… 113
5.2.1 包过滤防火墙 …… 113
5.2.2 代理防火墙 …… 116
5.2.3 动态包过滤防火墙 …… 118
5.2.4 自适应代理防火墙 …… 119
5.3 防火墙的体系结构 …… 119
5.4 防火墙的应用 …… 121

5.4.1 个人版防火墙的应用 …… 121
5.4.2 代理服务器的应用 …… 124
5.5 天融信网络卫士防火墙 …… 127
5.5.1 网络卫士防火墙概述 …… 127
5.5.2 网络卫士防火墙的基本设置 …… 128
5.5.3 网络卫士防火墙的通信策略 …… 131
5.5.4 网络卫士防火墙的访问策略 …… 134
5.5.5 网络卫士防火墙的日志 …… 138
5.6 防火墙的性能 …… 141
5.6.1 防火墙的性能 …… 141
5.6.2 选购防火墙的注意点 …… 144
练习题 …… 144

第 6 章 入侵检测技术 …… 147

6.1 入侵检测技术的作用与概念 …… 147
6.1.1 系统风险与入侵行为 …… 147
6.1.2 入侵检测概念 …… 147
6.2 入侵检测原理 …… 149
6.2.1 入侵检测分类 …… 149
6.2.2 入侵检测技术 …… 150
6.2.3 入侵检测过程 …… 151
6.3 入侵检测的应用 …… 152
6.3.1 网络卫士入侵检测系统特性 …… 152
6.3.2 入侵检测系统在网络中的应用 …… 153
练习题 …… 159

第 7 章 Windows 2000 的安全 …… 161

7.1 Windows 2000 的安全特性 …… 161
7.1.1 操作系统的安全 …… 161
7.1.2 Windows 2000 的安全特性 …… 161
7.1.3 Windows 2000 的安全架构 …… 162
7.1.4 Windows 2000 的登录和安全子系统结构 …… 163
7.1.5 安全标识符 …… 164
7.2 Windows 2000 的安全配置 …… 166
7.2.1 Windows 2000 的安装 …… 166
7.2.2 Windows 2000 系统账号的安全策略 …… 167
7.2.3 Windows 2000 系统的访问控制 …… 169
7.2.4 激活 Windows 2000 系统的安全策略 …… 170
7.2.5 Windows 2000 系统的日志 …… 172

7.3 Windows 2000 常用的系统进程和服务 …… 173
7.3.1 Windows 2000 常用的系统进程 …… 173
7.3.2 Windows 2000 的系统服务 …… 175
7.4 Windows 2000 注册表 …… 178
7.4.1 注册表由来 …… 178
7.4.2 注册表基本知识 …… 179
7.4.3 Windows 2000 注册表的备份与恢复 …… 180
7.4.4 注册表的操作 …… 182
7.4.5 注册表的应用 …… 183
练习题 …… 184

第 8 章 Web 的安全性 …… 186

8.1 Web 安全性概述 …… 186
8.1.1 Internet 的脆弱性 …… 186
8.1.2 Web 的安全问题 …… 187
8.2 Web 服务器的安全性 …… 187
8.2.1 Web 服务器的作用 …… 187
8.2.2 Web 服务器存在的漏洞 …… 189
8.2.3 Web 服务器的安全设置 …… 189
8.3 脚本语言的安全性 …… 195
8.3.1 CGI 程序的安全性 …… 195
8.3.2 CGI 程序的常见漏洞实例 …… 196
8.3.3 ASP 的安全性 …… 197
8.4 Web 浏览器的安全性 …… 199
8.4.1 浏览器本身的漏洞 …… 199
8.4.2 ActiveX 的安全性 …… 201
8.4.3 Cookie 的安全性 …… 203
练习题 …… 205

第 9 章 网络安全工程 …… 207

9.1 网络安全策略 …… 207
9.1.1 网络安全策略的制定原则 …… 207
9.1.2 网络安全策略 …… 208
9.2 网络安全工程的规划与管理 …… 211
9.2.1 网络安全标准 …… 211
9.2.2 网络安全工程 …… 215
9.2.3 网络安全系统的设计原则 …… 216
9.2.4 网络安全系统的管理 …… 217
9.2.5 网络安全系统的风险评估 …… 218

9.3 网络安全整体解决方案实例 …… 219
9.3.1 网络安全需求分析 …… 220
9.3.2 网络安全系统设计和实施 …… 221
练习题 …… 222

附录1 部分练习题参考答案 …… 224

附录2 常用端口大全 …… 226

参考文献 …… 227

第 1 章

计算机网络安全概述

1.1 网络安全简介

1.1.1 网络安全的重要性

随着计算机技术的飞速发展，以 Internet 为代表的信息网络技术的应用正日益普及，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，信息网络已经深入到国家的政府、军事、文教、金融、商业等诸多领域，可以说网络无处不在，它正在改变我们的工作方式和生活方式。

伴随网络的普及，安全日益成为影响网络效能的重要问题。据上海艾瑞市场咨询有限公司调查结果显示（如图 1-1 所示），信息安全成为一个非常严重的社会问题，已经引起了人们的足够重视。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。据美国联邦调查局的报告，计算机犯罪是商业犯罪中最大的犯罪类型之一，每笔犯罪的平均金额为 4.5 万美元，美国每年因为计算机犯罪造成的经济损失高达 150 亿美元。近年来，国内的计算机犯罪案件也急剧上升，计算机犯罪已经成为普遍的国际性问题。

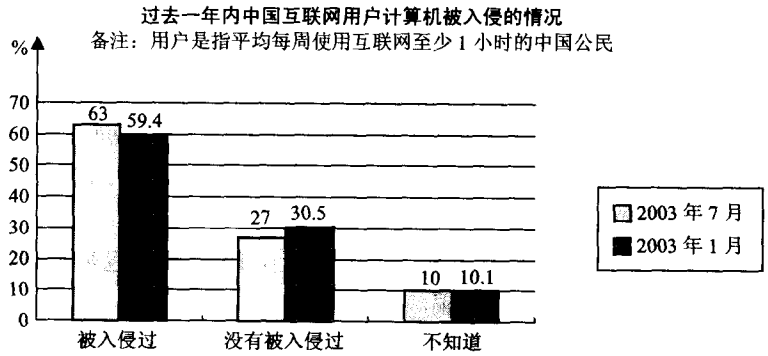


图 1-1 艾瑞市场公司调查计算机被入侵的结果

网络安全不仅关系到国计民生，还与国家安全息息相关，它涉及到国家政治和军事命脉，影响到国家的安全和主权。一些发达国家如英国、美国、日本、俄罗斯等都把国家网络安全纳入了国家安全体系。因此，网络安全不仅成为商家关注的焦点，也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话："Internet 的美妙之处在于你和每个人都能互相连接，Internet 的可怕之处在于每个人都能和你互相连接。"

由于网络建立伊始只考虑方便性、开放性，并没有考虑总体安全构想。因此，开放性的网络，导致网络的技术是全开放的，任何一个人、团体都可能接入，因而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。

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。由于 Internet 是个虚拟的世界，我们不知道和我们相连的另一端是谁。图 1-2 所示是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，因此说，网络安全所面临的是一个国际化的挑战。

图 1-2 网上图片

2. 协议本身的缺陷

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，如 TCP/IP 等本身就存在着漏洞。针对 TCP/IP 协议栈各个层次的攻击有以下几方面。

① 网络应用层服务的安全隐患。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，攻击者可以假冒别的用户进行通信，即 IP 欺骗。

③ 局域网中以太网协议的数据传输机制是广播发送，使得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

使用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。而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的安全性是很差的，而进行安全配置又比较复杂并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。

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　典型的网络安全事件

网络安全事件不计其数，下面列举一些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，他们因其所居住的地区密尔沃基电话区号是 414，而被人称做“414 黑客”。这 6 名少年黑客被控侵入 60 多台电脑，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
1987 年	17 岁的高中学生赫尔伯特·齐恩（被执法当局称做“影子鹰”）承认侵入美国电话电报位于新泽西州贝特敏斯特市的电脑网络。美国联邦执法部门指控他（在芝加哥郊区的卧室里操纵一台电脑）闯入美国电话电报公司的内部网络和中心交换系统。齐恩是美国被判有罪的第一位黑客
1988 年	康奈尔大学研究生罗伯特·莫里斯（22 岁）向互联网上传了一个“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电脑并自我繁衍。当时使得美国 6000 多个系统（几乎占当时互联网的 1/10）陷入瘫痪，专家称他设计的“蠕虫”程序造成了 1500 万到 1 亿美元的经济损失
1990 年	“末日军团”（美国南方的一个黑客组织）的 4 名成员盗窃南方贝尔公司的 911 紧急电话网络的技术秘密。4 名黑客中有 3 人被判有罪
1995 年	米特尼克被逮捕。他被指控闯入许多电脑网络，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
1998 年	美国国防部宣布黑客向五角大楼网站发动了“有史以来最大规模、最系统性的攻击行动”。黑客打入了许多政府非保密性的敏感电脑网络，查询并修改了工资报表和人员数据。3 个星期后，美国警方宣布以色列少年黑客“分析家”被抓获
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 千万部的电脑受害
1999 年 5～6 月	美国参议院、白宫和美国陆军网络以及数十个政府网站都被黑客攻陷
1999 年 11 月	挪威黑客组织“反编译工程大师”破解了 DVD 版权保护的解码密钥，还编制了一个 DVD 解码程序公布在互联网上
1999 年	北京江民公司在杀毒软件 KV3000 的 L＋＋版中设置逻辑炸弹（逻辑锁），造成损失 260 万元，被多方控告，江民公司败诉
2000 年 2 月	以“雅虎”为首的美国一系列大型网站遭到了黑客的有组织的攻击，他们攻击的目标包括了雅虎、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
2000 年 5 月	5 月 4 日开始发作的“I Love You”电脑病毒如野火一般肆虐美国公司，进而袭击全球，使许多公司的生产大受影响。全球已造成 100 亿美元损失
2000 年 10 月 27 日	全球软件业龙头微软怀疑被一伙藏在俄罗斯圣彼得堡的电脑黑客入侵。这些黑客可能已经窃取了微软一些最重要的软件产品的源代码或设计蓝图，这些软件产品包括 Office、Windows Me、Windows 2000 和 Microsoft.NET。但微软公司在 10 月 27 日公布说，闯入其网络系统的黑客只是看到了一些未完成的源代码，而并没有看到现有产品的源代码

下面是 CA（美国 Computing Associates 公司，全球著名的最大软件公司之一）公司关于网络安全事件的预算计算公式，如图 1-3 所示。

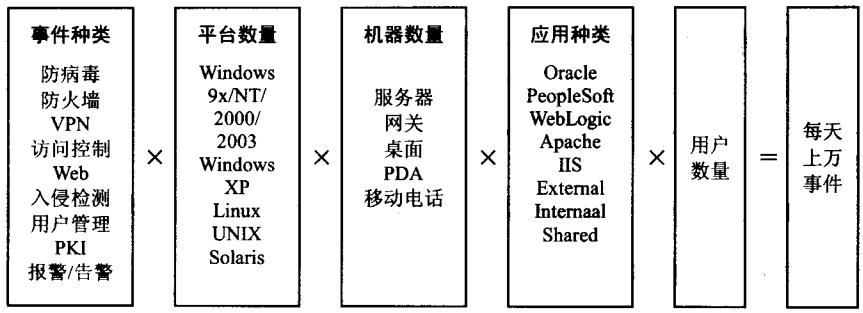


图 1-3　网络安全事件的预算计算公式

通过这个公式我们也可以预想，现在系统平台越来越多，应用更加多种多样，网络安全设备也逐渐增多，这么多因素，我们将来面临的网络安全事件将会更多。

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，发展到今天的各种各样的信息安全产品、技术手段等多方面。总的来说，信息安全技术在其发展过程中经历了以下 3 个阶段。

1.2.1　通信保密阶段

早在 20 世纪初期，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，人们强调的主要是信息的保密性，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称为通信安全，即 COMSEC（Communication Security）。

该阶段的标志是 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。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，涉及了数据的保密性和完整性，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，再加上美国政府把它当做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　信息安全阶段

20 世纪 60 年代后，半导体和集成电路技术的飞速发展推动了计算机软硬件的发展，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信息安全阶段，即 INFOSEC（Information Security）。

这一时期的标志就是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）和美国国防部在 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。

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，应用范围不断扩大。人们利用通信网络把孤立的计算机系统连接起来，资源共享。随之而来的信息安全问题也越来越受到重视。

该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。这时的安全威胁已经扩展到了非法访问、恶意代码、口令攻击等。

美国国防部 1985 年再版的《可信计算机系统评价准则》（又称橘皮书），使计算机系统的安全性评估有了一个权威性的标准。

1.2.3　信息保障阶段

20 世纪 90 年代，由于互联网技术的飞速发展，信息无论是对内还是对外都得到极大开放，由此产生的信息安全问题跨越了时间和空间。信息安全的焦点已经不仅仅是传统的保密性、完整性和可用性 3 个原则了，由此衍生出了诸如可控性、抗抵赖性、真实性等其他的原则和目标。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，也称网络信息系统安全阶段。

该阶段的主要安全威胁已经发展到网络入侵、病毒破坏和信息对抗的攻击等。随着电子商务等的发展，对安全性有了新的需求：可控性（Controllability），即对信息及信息系统实施安全监控管理；不可否认性（Non-Repudiation），即保证行为人不能否认自己的行为。

此时期，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。

1.3　网络安全的定义

1.3.1　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是这样的：安全就是最大程度地减少数据和资源被攻击的可能性。

《中华人民共和国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，网络安全就是网络上的信息安全，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，凡是涉及到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，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、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，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“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，避免机要信息泄露，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。数据可以单独保存，也可以分开保存。

1.3.2 网络安全的基本要素

网络安全的基本要素，实际上也就是网络安全的目的，即机密性（Confidentiality）、完整性（Integrity）、可用性（Availability）、可控性（Controllability）与不可否认性（Non-Repudiation）。

1. 机密性

机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，还通过加密变换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

完整性是只有得到允许的人才能修改实体或者进程，并且能够判别出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

可用性是信息资源服务功能和性能可靠性的度量，涉及到物理、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。即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。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，使得攻击者、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。

1.4 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