"九五"国家重点电子出版物规划项目·计算机知识普及系列
21世纪计算机网络技术系列书

面向21世纪
网络安全与防护

北京希望电子出版社　总策划
胡昌振　李贵涛等　编　著

本书配套光盘内容包括：
1. "网络安全软件"
2. "Internet互联网即时通"
多媒体学习软件

北京希望电子出版社
Beijing Hope Electronic Press
www.bhp.com.cn

“九五”国家重点电子出版物规划项目，计算机知识普及系列

21 世纪计算机网络技术系列书

面向 21 世纪网络安全与防护

胡昌振　李贵涛　等编著

希望图书创作室　审校

本书配套光盘内容包括：

1. “网络安全软件”
2. “Internet 互联网即时通”
   多媒体学习软件

北京希望电子出版社
Beijing Hope Electronic Press
www.bhp.com.cn

内 容 简 介

本书全面地介绍了目前全球关注的网络系统安全及其防护体系问题。在介绍黑客对网络攻击过程的基础上，系统地阐述了如何用超越防火墙的网络安全技术——攻击检测技术的原理与方案，并对网络安全防护技术进行了系统的总结和建议。全书共分五个部分，第一部分介绍网络安全及其体系；第二部分介绍网络的安全漏洞；第三部分介绍网络技术攻击；第四部分介绍攻击检测技术；第五部分介绍黑客攻击的系统防护策略与措施。该书从实用角度，对网络安全与攻击检测技术进行了深入浅出的阐述，为从事网络攻击检测技术的研究和开发的科技人员，及网络管理员、广大的计算机网络爱好者提供了重要的参考学习资料。

本书和特别适合从事计算机网络安全、防护体系研发的广大科技人员借鉴与参考，同时也适合作为大专院校师生自学、教学参考书和社会相关领域的培训教材。

与本书配套光盘内容包括“网络安全软件”和“Internet 互联网即时通”多媒体学习软件。

“九五”国家重点电子出版物　　计算机知识普及系列

系　列　书	21 世纪计算机网络技术系列书
书　　名	面向 21 世纪网络安全与防护
文本著作/翻译	胡昌振　李贵涛　等编著
审校/责任编辑	周凤明
C D 制 作 者	希望天一工作室
C D 测 试 者	希望多媒体测试部
出 版 / 发 行 者	北京海淀路 82 号（100080）
地　　址	网址：www.bhp.com.cn E-mail：lwm@hope.com.cn 电话：010-62562329，62541992，62637101，62637102（图书发行，技术支持） 010-62633308，62633309（多媒体发行，技术支持） 010-62613322-215（门市） 010-62531267（编辑部）
经　　销	各地新华书店、软件连锁店
排　　版	北京希望图书照排中心
C D 生 产 者	文录激光科技有限公司
文 本 印 刷 者	北京双青印刷厂
规 格 / 开 本	787 毫米×1092 毫米　16 开本　16.25 印张　373 千字
版 次 / 印 次	1999 年 10 月第 1 版　　1999 年 10 月第 1 次印刷
印　　数	0001—5000 册
本　版　号	ISBN7-900024-92-1/TP・92
定　　价	34.00 元(1CD，含配套书)

说明：凡我社光盘配套图书若有自然破损、缺页、倒页、脱页者，本社发行部负责调换。

序

网络技术在国家防务、政府管理、电子商务乃至信用消费活动中的应用愈来愈广。伴随网络技术所带来的快速、方便、“天涯若比邻”的同时，通过网络犯罪而对国家安全、企业安全和个人安全造成的严重危害也日益显现。1999 年 8 月 18 日，美俄之间爆发了第一次“世界计算机大战”，互相指责黑客入侵网络“禁地”，窃取军事机密。我国有关部门也发出联合通知，要求作好网络安全工作，严防黑客入侵。“网络战争”正逐步从“预言”变为现实。

谈起网络安全，人们首先想到的就是病毒防治与防火墙技术。其实，从技术上讲，网络安全是一个病毒防治、防火墙和攻击检测的综合集成系统。攻击检测技术以探测与控制为技术本质，起着主动防御的作用，是网络安全的一个极其重要的部分。该技术 90 年代初期提出，已引起了广泛的重视，美国政府就曾打算建立一个网络检测系统来保护政府机构的数据网络免受黑客入侵。在我国，对该项技术的研究则刚刚起步。该书的出版，对促进这一领域工作的开展，无疑具有重要的意义。

该书从实用角度，对网络安全与攻击检测技术进行了深入浅出的阐述，是一本既适合于从事这一领域研究和开发的科技人员，也适合于网络管理员与广大网络爱好者的重要参考资料。

值此书出版之际，谨作此序，祝我国网络安全技术繁荣昌盛。

谭惠民

1999 年 9 月

前　言

Internet 的发展，正在引发一场人类文明的根本性变化。网络已成为一个国家最为关键的政治、经济、军事资源，成为国家实力的新象征。发展网络技术是国民经济现代化建设不可或缺的一个必要条件。能否把握网络给中国发展带来的机遇，将会直接影响 21 世纪中国的生存。

网络改变了人们的工作、生活方式，使信息的获取、传递、处理和利用更加高效、迅捷，同时，也使“黑客”侵犯和操纵一些重要信息和数据成为可能，因而引发出网络安全性问题。正如我国著名计算机专家沈昌祥院士指出的：“信息安全保障能力是 21 世纪综合国力、经济竞争实力和生存能力的重要组成部分，是世纪之交世界各国在奋力攀登的制高点。”

网络安全是一个系统的概念，完善的网络安全体系，必须合理协调法律、技术和管理三种因素，集成防护、监控和恢复三种技术。从技术层次上讲，网络安全包括防火墙技术、数据加密技术、攻击检测技术和数据恢复技术。防火墙是一种用来加强网络之间访问控制的特殊网络互连设备，该设备通常是软件和硬件的组合体。它能阻挡外部入侵者，但是，防火墙绝对不是坚不可摧的，即使是某些防火墙本身也会引起一些安全问题。数据加密技术是为提高信息系统及数据安全性、保密性和防止秘密数据被破解所采用的主要手段之一。任何数据加密的措施都有一定的限度，在现今的计算条件下，没有无法破译的密码。攻击检测技术是一种利用攻击者的蜘蛛马迹，如试图登录的失败记录，试图连接特定文件、程序和其他资源的失败记录，或者通过监视某些特定指标如 CPU、内存、磁盘的不寻常活动等，有效地发现来自外部或内部的非法攻击的技术。从网络安全防护上讲，防火墙技术和数据加密技术给出了一个静态防护的概念，而攻击检测技术则具有动态防御的意义。

我国计算机系统及网络是以国外产品为主，其操作系统的安全性基本上是最低层次的，即使最高的也只是美国标准的 C 级，同时，软硬件系统中难免也存在各种潜在威胁和安全“陷阱”（最近发现的 PIII芯片、WIN98 的安全问题及 Windows 操作系统的安全“后门”就映证了这一事实）。因此，利用这些设备建立的网络系统，即使采用了加密、防火墙等安全技术措施，其安全水平也不可能有根本性的提高。在我国计算机网络的安全现状下，基于防火墙、加密技术的安全防护固然重要，但是，要根本改善网络的安全现状，必须发展网络攻击检测技术。

本书全面地讲述了网络系统安全及其防护体系问题。在介绍网络攻击过程的基础上，系统地阐述了一种超越防火墙的网络安全技术——攻击检测技术的原理与方案，并对网络安全防护技术进行了系统的总结。为从事网络攻击检测技术的研究和应用工作的科技人员，及网络管理员与广大的计算机网络爱好者提供重要参考资料。

承蒙天一工作室的何敏男老师，为本书的出版提出了许多宝贵的具体意见，并进行了有效的策划。希望出版公司的秦人华老师、侯业勤老师和沈鸿老师仔细地审阅了全书并提出了修改意见。机电工程与控制国家重点实验室主任、博士生导师谭惠民教授对本书的编

写给予了热情的鼓励与关怀。在此，对他们表示诚挚的谢意。

研究生危胜军、牛兰杰、王瑞刚等为本书也作了大量的工作。

本书的编写过程中，参阅了许多网络安全论著，在此向这些作者表示衷心的感谢。

由于编者的水平所限，书中不足乃至谬误在所难免，恳请各位专家、学者及读者批评指正。

编 者

1999 年 9 月 10 日

目　录

第一篇　网络安全及其体系

第一章　网络安全 3

1.1　网络安全的基本概念 3
1.2　网络的安全威胁 6
1.3　网络的安全问题及其原因 11
1.4　网络的安全标准 14

第二章　网络安全防护体系 17

2.1　网络安全策略 17
2.2　网络安全体系 19

第二篇　网络的安全漏洞

第三章　网络和数据通讯安全 27

3.1　UUCP 系统概述 27
3.2　UUCP 的安全问题 28
3.3　HONEYDANBER UUCP 30
3.4　通信安全 37
3.5　SUN OS 系统的网络安全 40

第四章　人员安全 48

4.1　管理员安全 48
4.2　用户安全漏洞 65
4.3　程序员安全漏洞 71

第五章　Windows NT 安全漏洞及对策 80

5.1　NT 服务器和工作站的安全漏洞及防范技术 80
5.2　NT 与浏览器有关的安全漏洞及防范措施 89

第六章　TCP/IP 网络安全漏洞及解决对策 93

6.1　Internet 层的安全性 93
6.2　传输层的安全性 95
6.3　应用层的安全性 96

第三篇　网络技术攻击

第七章　网络攻击的概念 101

7.1　网络攻击及其原因 101
7.2　网络攻击使用的操作系统 106
7.3　黑客攻击策略 107

第八章　黑客攻击技术与防范 109

8.1　目标分析 109
8.2　密码文件的获得 110
8.3　文档的获取 112
8.4　日志清除 114

第九章　安全“后门”与堆栈溢出 119

9.1　安全“后门” 119
9.2　堆栈溢出（Buffer Overflow） 124

第四篇　攻击检测技术

第十章　网络攻击检测基础 141

10.1　系统日志 141
10.2　进程记帐 148
10.3　审计工具 150
10.4　其他操作系统的审计跟踪 154
10.5　使用 System Log 发现入侵者 156

第十一章　攻击检测方法 159

11.1 攻击检测系统构成.....159
11.2 基于审计信息的攻击检测技术.....162
11.3 攻击检测方法.....163
11.4 攻击检测系统的测试.....165
11.5 网络入侵跟踪方法.....166
11.6 几种常用的攻击检测工具.....171

第十二章 典型网络攻击检测系统分析 174

12.1 有关网络攻击检测系统的一般描述...174
12.2 基于主机的攻击检测系统.....177
12.3 基于网络的侵入检测系统.....185

第五篇 黑客攻击的系统防护策略与措施

第十三章 黑客攻击的风险分析 199

13.1 黑客攻击的风险分析原则.....199
13.2 黑客攻击的风险分析方法.....199
13.3 风险分析工具的选择.....207

第十四章 黑客攻击防护系统的安全策略 ... 214

14.1 黑客攻击防护的基本概念.....214
14.2 黑客攻击防护的基本内容.....215
14.3 黑客攻击防护系统的安全策略.....218

第十五章 网络安全防护措施 223

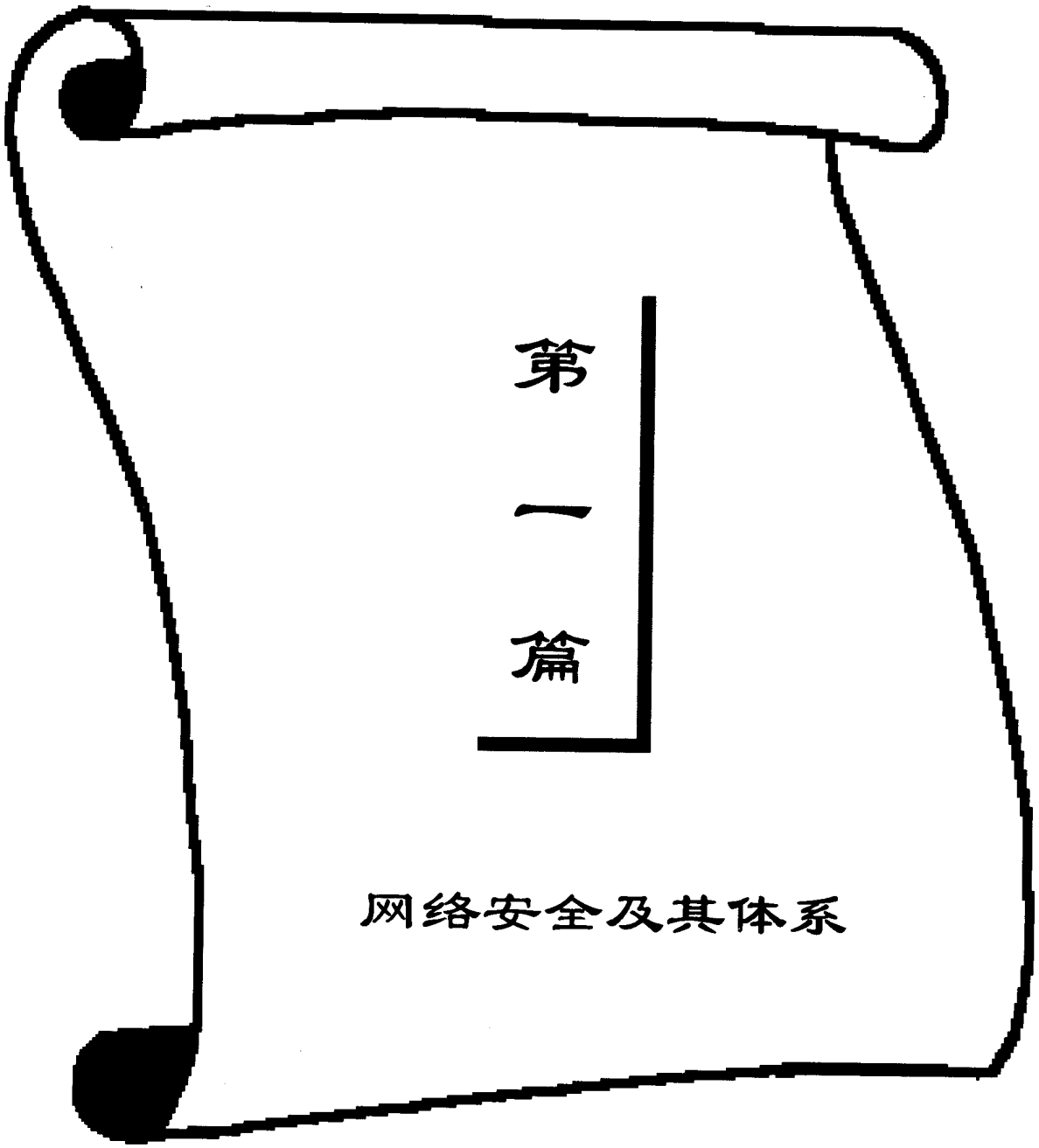
15.1 网络安全的常规防护措施.....223
15.2 网络安全控制措施.....227
15.3 网络安全实施过程中需要注意的一些问题.....231

附录 A 有关网络安全的的名词术语及缩略语汇编 236

A.1 网络安全的名词术语.....236
A.2 缩略语.....242

附录 B 黑客攻击途径、工具及防范策略 ... 245

B.1 黑客的界定.....245
B.2 黑客攻击网络的途径.....246
B.3 黑客获取口令的手段及管理员的应对策略.....246
B.4 远程控制黑客程序 BO2K 的防范.....248
B.5 电子邮件炸弹美莉莎（Melissa）及类似黑客攻击手段.....251



第一篇

网络安全及其体系

第一章 网 络 安 全

本章从系统的角度探讨了网络安全问题，大致包含如下内容：

- 网络安全的基本概念
- 网络的安全威胁
- 网络的安全问题及其原因
- 网络的安全标准

1.1 网络安全的基本概念

作为一种战略资源，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，在社会生产、生活中的作用日益显著。传播、共享和自增殖是信息的固有属性，与此同时，又要求信息的传播是可控的、共享是授权的、增殖是确认的。因此在任何情况下，信息的安全和可靠必须是保证的。Internet 是一种开放和标准的面向所有用户的技术，其资源通过网络共享。资源共享和信息安全是一对矛盾，随着 Internet 的飞速发展，计算机网络的资源共享程度进一步加强，随之而来的信息安全问题便日益突出，网上的犯罪活动、网上的侵权纠分加速增长：

- 1995 年 8 月 21 日，设防严密的美国某银行网络系统，被黑客通过 Internet 入侵，损失现金高达 1160 万元，为弄清楚原因并防患于未然，该银行不惜用上亿美元让入侵者讲述入侵的秘密和详细策略。
- 1996 年 12 月 29 日，黑客将美国空军网页修改为两只鲜血直流的红眼球，并书写上“欢迎了解真相”，对美国政府大肆攻击。
- 1997 年佛罗里达州的警察应急系统被黑客通过 Internet 入侵，使应急警务和消防部队无所适从。
- 根据权威机构统计，平均每 20 秒就发生一起入侵 Internet 的计算机事件。
- 美国每年 Internet 安全问题造成的损失，高达 75 亿美元。

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 12000 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。

Internet 是跨时空的，其安全问题也是跨越时空的，尽管我国的网络不发达，但我们遭到的安全危险却同国外是一样的，其安全威胁也是客观存在的。我国的网络也曾被人入侵，多次发生过私设帐号和网络瘫痪的事故。

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，国家与国家之间、集团与集团之间、甚至个人与个人之间展开着尖锐激烈的斗争。

谁掌握了信息，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。立足于本国，制定我国的安全策略，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，信息安全技术都是大有所为的。

网络安全是指网络系统的部件、程序、数据的安全性，它通过网络信息的存储、传输和使用过程体现。所谓的网络安全性就是保护网络程序、数据或者设备，使其免受非授权使用或访问，它的保护内容包括：

- 保护信息和资源
- 保护客户和用户
- 保证私有性

网络安全包括物理安全和逻辑安全。对于物理安全，需要加强计算机机房管理，如门卫、出入者身份检查、下班锁门以及各种硬件安全手段等预防措施；而对于后者，则需要用口令字、文件许可和查帐等方法来实现。

1.1.1 网络安全的目的

确保网络系统的信息安全是网络安全的目标，对网络系统而言，信息安全主要包括两个方面：信息的存储安全和信息的传输安全。

信息的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，无论是任何调用指令，还是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。信息的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，尤其需要防止如下问题：

（1）对网络上信息的监听

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）对用户身份的仿冒

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，很容易就能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）对网络上信息的篡改

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）对发出的信息予以否认

某些用户可能对自己发出的信息进行恶意的否认，例如否认自己发出的转帐信息等。

（5）对信息进行重发

“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。

基于网络安全目标的网络安全防护，具有如下两方面的意义：

（1）在安全与通信方便之间的平衡

当把安全性能设计得越完善时，系统的效率也就越低，即要求网络系统越安全，则对通信的限制和使用的难度就越大。因此，建立网络安全系统的真正有效的途径是用户本身应对安全作出恰当的评估，即用户应针对自己的具体信息存取需求，对自身的能力（尤其是管理能力）、可容忍的风险、增加安全的代价和网络的体系结构等作出折衷。

（2）以人为主，技术、管理和法律的综合

网络安全问题是一个典型的人—机关系问题，所有的各种安全保密功能是人设计和实现的，因此人也能破坏和干扰各种安全和保险功能。对于计算机安全，最重要的起点是从涉及计算机的人员（即用户、系统管理员以及超级管理员）开始。安全的最薄弱环节是人们的粗心大意，如登录和使用计算机后，不退出系统就离开终端不管；与他人共用计算机存取口令；将重要机密的信息存入不适当的计算机文件中等。

网络信息，即电子信息，本身具有特殊性质。当窃取信息时，并不需要从计算机文件中移走信息，只需要执行一个简单的文件拷贝。这一特点增大了信息被窃取事实识别的难度，也使得道义、道德和法律上的问题复杂化。

1.1.2 网络安全需求与安全机制

网络安全设计首先需考虑网络的安全需求和网络的安全机制。

网络安全需求包括：

(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。安全机制在 ISO/OSI 互联参考模型的七层体系结构中的分布如图 1.1。

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；实现审讯记录和统计分析等。

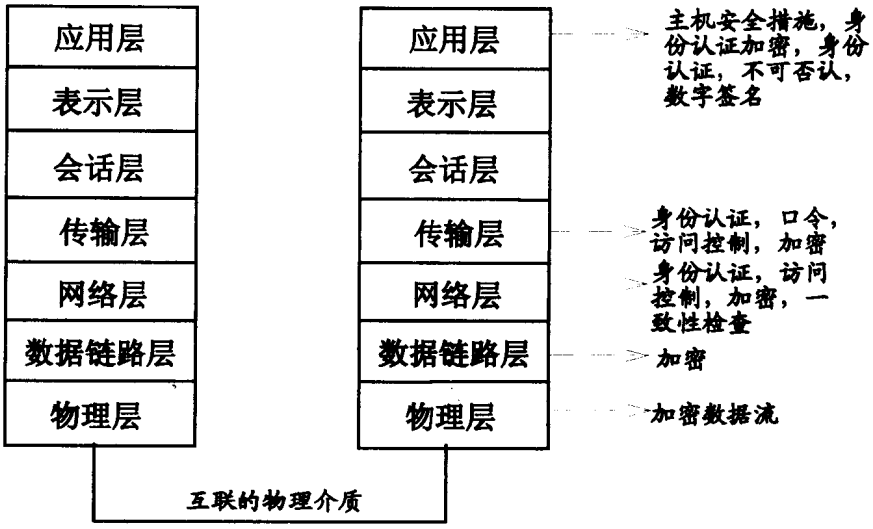


图 1.1　安全机制在七层体系结构中的分布

1.2　网络的安全威胁

对一个企业而言，保护网络的安全，就意味着保护企业。然而随着联网 PC 数量的增加，网络安全事故数量也在逐渐增加，如图 1.2 为美国 Internet 安全组织 CERT（计算机紧急情况处理小组）对 1989-1994 年网络安全事故数量的统计。

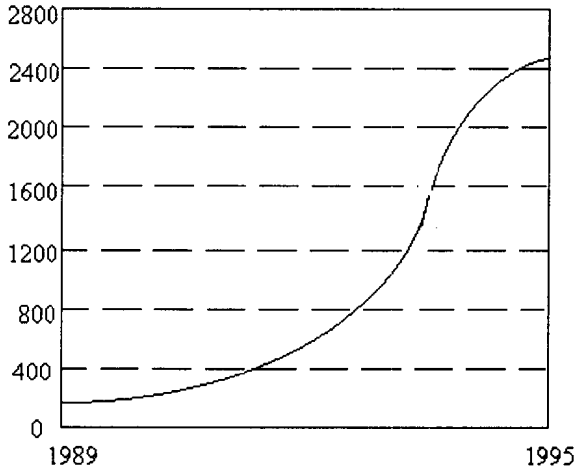
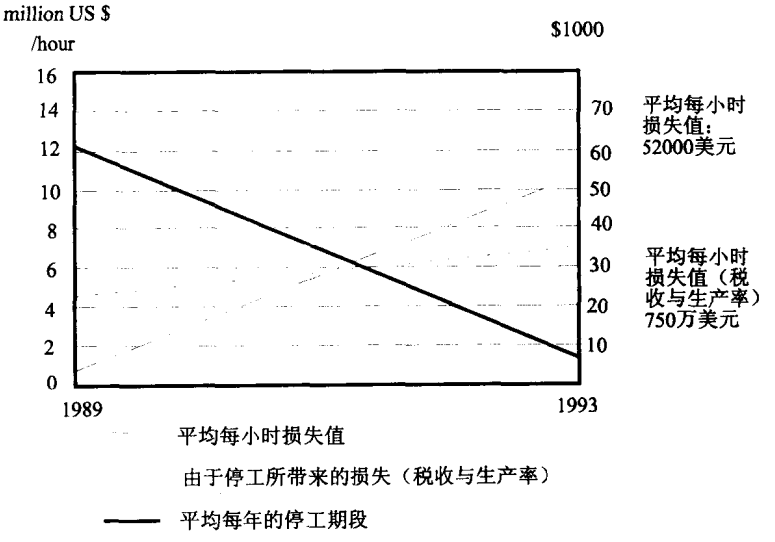


图 1.2　1989-1994 年网络安全事故数量

网络安全事故之所以能经常发生，主要原因有：

- 现有网络系统具有内在的安全脆弱性。
- 思想麻痹，没有正视黑客入侵所造成的严重后果，因而舍不得投入必要的人力、财力、物力来加强网络的安全性。
- 没有采用正确的安全策略和安全机制。
- 缺乏先进的网络安全技术、工具、手段和产品。
- 缺乏先进的系统恢复、备份技术和工具。

80 年代末以来，公司对数据通信技术的依赖程度日益增大，几乎所有公司的重要数据都存储在计算机上，而且，越来越多的公司借助于网络化 PC 开展业务，安全的网络通信基础设施对几乎所有的公司来讲，



都是生死攸关的问题，计算机网络系统一旦出现问题或崩溃，不管怎样，会立即造成极大的损失。最近几年内，伴随着信息基础设施投资的提高，每次网络瘫痪所造成的损失呈逐年增加趋势。如图 1.3 为 CERT 对 1989 年以来公共网络停工期的损失价值统计结果。

图 1.3 1989 年以来公共网络停工期的损失价值

尽管网络非常有用而且充满生机，但它的安全性是非常脆弱的，极易遭受攻击，尤其是连在 Internet 上的局域网（站点），随时都面临着很大的被袭击的危险。危险程度受以下一些因素的影响：

- 网络系统的数量
- 网络使用的服务
- 网络与 Internet 的连接方式
- 网络知名度
- 网络对安全事故的准备情况

计算机网络所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。影响计算机网络的因素很多，有些因素可能是有意的，也可能是无意的；可能是人为的，也可能是非人为的；可能是外来黑客对网络系统资源的非法使用，归结起来，针对网络安全的威胁主要有三：

（1）人为的无意失误 如操作员安全配置不当造成的安全漏洞，用户安全意识不强，用户口令选择不慎，用户将自己的帐号随意转借他人或与别人共享等都会对网络安全带来威胁。

（2）人为的恶意攻击 这是计算机网络所面临的最大威胁，敌手的攻击和计算机犯罪就属于这一类。此类攻击又可以分为以下两种：一种是主动攻击，它以各种方式有选择地破坏信息的有效性和完整性；另一类是被动攻击，它是在不影响网络正常工作的情况下，进行截获、窃取、破译以获得重要机密信息。这两种攻击均可对计算机网络造成极大的危害，并导致机密数据的泄漏。

（3）网络软件的漏洞和“后门”　网络软件不可能是百分之百无缺陷和无漏洞的，然而，这些漏洞和缺陷恰恰是黑客进行攻击的首选目标。曾经出现过的黑客攻入网络内部的事件大部分就是因为安全措施不完善所招致的苦果。另外，软件的“后门”都是软件公司的设计编程人员为了自便而设置的，一般不为外人所知，但一旦“后门”洞开，其造成的后果将不堪设想。

总的来说，网络安全的威胁包括如图 1.4 所示的几种基本类型。

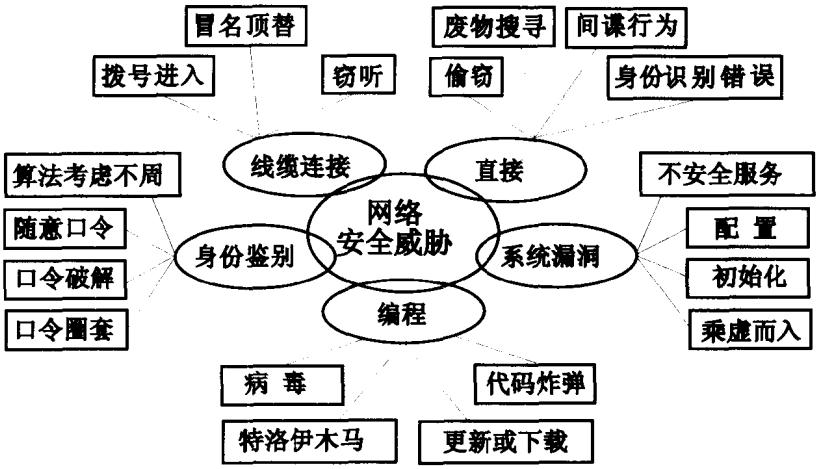


图 1.4　网络安全威胁的几种基本类型

1.2.1　物理威胁

物理安全的防护在概念上相当简单，即不要让别人拿到你的东西，也不让他们窥视你的东西。最常见的物理威胁包括如图 1.4 所示的偷窃、废物搜寻、间谍行为与身份识别错误等内容。

（1）偷窃　偷窃是一个与法律有关的概念。偷窃者所做的就是：如果他们想要什么他们负担不起的东西，他们就把它偷来，例如他们需要钱，他们就会偷点什么东西并把它卖掉，他们想要的在保险箱里，他们偷保险箱。网络安全意义的偷窃包含两方面的含义：如果他们想到偷的信息在计算机里，他们就一方面可以将整台计算机偷走，另一方面通过监视器读取计算机中的信息。

由于偷窃而引起的网络安全涉及保护硬件、软件和存取文件免受偶然的破坏、蓄意的偷窃。网络安全中的偷窃包括偷窃设备、偷窃信息和偷窃服务等内容。

（2）废物搜寻　就是在废物（如一些打印出来的材料或废弃的软盘）中搜寻所需要的信息。在微机上，废物搜寻可能包括从未抹掉有用东西的软盘或硬盘上获得未抹掉的存取资料。在主机上，暂存的磁带通常不是直接由用户或系统操作员来抹掉的，他们可能成为攻击者感兴趣的信息。

（3）间谍行为　是一种为了省钱或获取有价值的机密、什么不道德的行为都会采用的商业过程。

（4）身份识别错误　非法建立文件或记录，企图把他们作为有效的、正式生产的文

件或记录，如对具有身份鉴别特征物品如护照、执照、出生证明或加密的安全卡进行伪造，属于身份识别发生错误的范畴。这种行为对网络数据构成了巨大的威胁。

1.2.2 线缆连接

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。

（1）窃听 分布式计算机的特征是各种分立的计算机通过一些媒介相互通信，因此对通信过程进行窃听可达到收集信息的目的。这种电子窃听甚至不一定需要窃听设备一定安装在线缆上，可以通过检测从连线上发射出来的电磁辐射就能拾取所要的信号，为了使机构内部的通信有一定的保密性，可以使用加密手段来防止信息被解密。

（2）拨号进入 拥有一个调制解调器和一个电话号码，每个人都可以试图通过远程拨号访问网络，尤其是拥有所期望攻击的网络的用户帐户时，就会对网络造成很大的威胁

（3）冒名顶替 通过使用别人的密码和帐号，获得对网络及其数据、程序的使用能力。这种办法实现起来并不容易，而且一般需要有机构内部的，了解网络和操作过程的人参与。

1.2.3 身份鉴别

身份鉴别是指计算机借以决定你是否有权在服务器上要求或提供某些服务的过程，如果没有身份鉴别，在 LAN 系统上就不会有安全，常见的身份鉴别安全威胁如图 1.4。

（1）口令圈套 口令圈套是网络安全的一种诡计，与冒名顶替有关。常用的口令圈套通过一个编译代码模块实现，它运行起来和登录屏幕一模一样，被插入到正常有登录过程之前，最终用户看到的只是先后两个登屏幕，第一次登录失败了，所以用户被要求再输入用户名和口令。实际上，第一次登录并未失败，它将登录数据，如用户名和口令写入到一个数据文件中。

（2）口令破解 破解口令就象是猜测自行车密码锁的数字组合一样，在该领域中已形成许多能提高成功率的技巧。

（3）算法考虑不周 口令输入过程必须在满足一定条件下才能正常地工作，这个过程通过某些算法实现。在一些攻击入侵案例中，入侵者采用超长的字符串破坏了口令算法，成功地进入了系统。

（4）编辑口令 编辑口令需要依靠内部漏洞，如果公司内部的人建立了一个虚设的帐户或修改了一个隐含帐户的口令，这样，任何知道那个帐户的用户名和口令的人便可以访问该机器了。

1.2.4 编程

许多安全漏洞源于代码，多数情况下，这些漏洞是毁灭性的，会摧毁数据，因此，计算机病毒同时威胁到系统安全和数据完整性。

（1）病毒 病毒是一种把自己的拷贝附着于机器中的另一程序上的一段代码。通过这种方式病毒可以进行自复制，并随着它所附着的程序在机器之间传播。这种传播既可以通过从 BBS 进行，也可以通过磁盘