希望
Beijing Hope Electronic Press
www.bhp.com.cn

21世纪高等院校计算机科学与工程系列教材

北京希望电子出版社　总策划
李仁发　主　编
喻飞　朱淼良　周洲仪　等　编　著

计算机网络安全

科学出版社
www.sciencep.com

21世纪高等院校计算机科学与工程系列教材

北京希望电子出版社 总策划
李仁发 主 编
喻飞 朱淼良 周洲仪 等 编 著

计算机网络安全

科学出版社
www.sciencep.com

内 容 简 介

本书是“21 世纪高等院校计算机科学与工程系列教材”中的一本，它从两个不同的角度介绍了计算机网络安全的理论、技术和方法。一个角度从正面防御考虑，介绍了加密、数字认证、防火墙和访问控制等技术与方法；另一个角度从反面考虑，介绍了操作系统及网络协议的安全漏洞、入侵检测、信息安全测评与认证和计算机取证等，并对电子邮件安全作了详细的介绍。

本书注重理论与实践应用相结合，选材范围广泛、实例丰富、实用性强。既可作为高等院校计算机科学与技术专业及相关专业的本科高年级学生或研究生的教材，也可作为从事网络安全研究的工程技术人员的参考用书或作为进修培训教材。

需要本书或技术支持的读者，请与北京中关村 083 信箱（邮编：100080）发行部联系，电话：010-82702660，82702658，62978181（总机）转 103 或 238，传真：010-82702698，E-mail：yanmc@bhp.com.cn。

图书在版编目（CIP）数据

计算机网络安全/李仁发主编；喻飞等编著.—北京：科学出版社，2004.11

21 世纪高等院校计算机科学与工程系列教材

ISBN 7-03-014059-1

Ⅰ.计… Ⅱ.①李…②喻… 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 078304 号

责任编辑：李 峰 / 责任校对：肖 寒

责任印刷：列电 / 封面设计：王 翼

科 学 出 版 社 出版

北京东黄城根北街 16 号

邮政编码：100717

http://www.sciencep.com

列电印刷厂印刷

科学出版社发行 各地新华书店经销

*

2004 年 11 月第 一 版 开本：787×1092 1/16

2004 年 11 月第一次印刷 印张：20

印数：1~3000 册 字数：454 974

定价：29.00 元

21世纪高等院校计算机教材编委会名单

（排名不分先后）

主　任： 陈火旺 院士

副主任： 李仁发 教授　金茂忠 教授　陈　忠 教授　陆卫民 高工

委　员：

晏海华	教授	北京航空航天大学
邵秀丽	副教授	南开大学
刘振安	教授	中国科技大学
董玉德	副教授	合肥工业大学
倪志伟	教授	合肥工业大学
吕英华	教授	东北师范大学
杨喜权	副教授	东北师范大学
朱诗兵	副教授	装备指挥学院
樊秀梅	副教授	北京理工大学
徐　安	教授	上海同济大学
赵　欢	副教授	湖南大学
胡学钢	教授	合肥工业大学
林福宗	教授	清华大学
王家昕	教授	清华大学
郑　莉	教授	清华大学
朱淼良	教授	浙江大学
刁成嘉	副教授	南开大学
林和平	教授	东北师范大学
孙铁利	教授	东北师范大学
温子梅	讲师	广东教育学院
吕国英	副教授	山西大学
张广州	讲师	沈阳大学
何新华	教授	装甲学院
邱仲潘	副教授	厦门大学
曾春平	副教授	第二航空学院
姬东耀	教授	中科院计算所
赵宏利	教授	装备指挥学院
喻　飞	博士	浙江大学
徐建华	总编	北京希望电子出版社
郑明红	副总编	北京希望电子出版社
韩素华	编室主任	北京希望电子出版社

总　序

21世纪挑战与机遇并存，没有足够的知识储备必将被时代所抛弃。中国IT教育产业竞争日趋激烈，用户需求凸现个性，行业发展更需要理性。未来五年IT行业将以每年18%的速度连续增长，将引发IT产业新的发展高潮。实现信息产业大国的目标，应该依赖教育，要圆信息产业强国的梦想，依然要寄托于教育，IT教育事业任重道远，其产业也正面临着机遇与挑战。

我国的计算机教学长久以来一直重原理、轻应用。高等院校的计算机教学机制和教材对计算机本身的认识都存在误区。要改革高校计算机教学，教材改革是重要方面，用计算机教材的改革促进基础教育的改革势在必行。

一本好书，是人生前进的阶梯；一套好教材，就是教学成功的保证。为缓解计算机技术飞速发展与计算机教材滞后落伍的矛盾，我们通过调查多所院校的师生，并多次研讨，根据读者认识规律，开创出一种全新的方式，打破过去介绍原理——理论推导——举例说明的模式，增加实用操作性，通过上机实验与课上内容结合来增强可读性，用通俗易懂的语言和例子说明复杂的概念。

本套教材的特点一是“精”，精选教学内容；二是“新”，捕捉最新资讯；三是“特”，配备电子课件，力争达到基础性、先进性、全面性、典型性和可操作性的最大统一。

为保证教材质量，我们同时聘请了一批学术水平较高的知名专家、教授作为本套教材的主审和编委。全套教材包括必修课教材二十多种，选修课教材和学习配套用书10余种，基本上涵盖了目前高等院校（含高等职业技术学院、高等专科学校、成人高等学校）计算机科学与技术专业所必修或选修的内容。各种教材编写时既注意到内容上的连贯性，又保证了教学上的相对独立性。

本套教材在内容的组织上，大胆汲取当今计算机领域最新技术，摒弃了传统教材中陈旧过时的内容。这些变化在各本教材中都得到了不同程度的体现。本套教材编写时既参照了教育部有关计算机科学与技术专业的教学要求，又参考了“程序员考试大纲”和“全国计算机水平等级考试大纲”的内容，因此既适合作为高等学校计算机科学与技术专业教材，也可作为计算机等级考试学习用书。

考虑到各校教学特点和计算机设备条件，我们本着“学以致用”的理念，在本套教材编写中自始至终贯彻“由浅入深，理论联系实际”的原则，以阐明要义为主，辅之以必要的例题、习题和上机实习，能够使学生尽快领悟和掌握。

在本套教材编写过程中，作者们付出了艰辛的劳动，教材编委会的各位专家、教授进行了认真的审定和悉心的指导。书中参考、借鉴了国内外同类教材和专著，在此一并表示感谢。

我们希望更多的优秀教师参与到教材建设中来，真诚希望广大教师、学生与读者朋友在使用本丛书过程中提出宝贵意见和建议。

若有投稿或建议，请发至本丛书出版者电子邮件：hansuhua@163bj.com

21世纪高等院校计算机教材编委会

前　言

人类进入了信息时代，信息安全问题已成为人类社会发展面临的新问题。交通安全、生产安全一直是人们无法回避的重大难题，而信息安全除了具有交通安全、生产安全一样的特性外，还与经济繁荣、社会稳定、国家安全有着千丝万缕的联系。因此，信息安全不仅是我们无法回避的重大研究课题，而且正在形成一个巨大产业，催生了一个新兴行业。

国内许多高校近年来陆续开设信息安全专业，相关研究也十分深入。本书根据网络信息安全技术近十年来的发展，从两个完全不同的角度进行了系统的介绍。一个角度从正面防御考虑，论述鉴别、加密、认证、授权和访问控制等；另一个角度从反面攻击考虑，论述网络信息系统漏洞、入侵检测、防火墙等。

本书在选材、内容组织及描述等方面力求做到：

系统性。系统介绍网络安全的基本理论、方法及技术。

新颖性。在介绍网络安全的传统理论及方法的同时，着眼于国内外的最新研究，使读者了解当前提出的新理论、新方法，跟踪该领域发展的趋势。

实用性。理论与实践相结合，既注重于理论之间的探讨，又注重理论在实践中的应用。

全书共 9 章。第 1 章是对网络安全的概述；第 2 章介绍操作系统安全的相关知识；第 3 章介绍了网络协议安全相关知识；第 4 章系统地介绍了电子邮件安全，并以作者所承担的科研项目为实例，给出了一个较为完整的电子邮件安全解决方案；第 5 章介绍了数字加密与认证，并以作者所参与的科研项目为实例，给出了一个较为简单的认证应用方案；第 6 章介绍了访问控制相关技术和访问控制模型的实现；第 7 章介绍了防火墙的相关知识并以作者所承担的科研项目为实例，给出了一个较为完整的嵌入式防火墙的实现方案；第 8 章介绍了入侵检测的相关知识，并以作者所承担的科研项目为实例，实现了一个较为完整的入侵检测系统；第 9 章首先介绍了当前计算机犯罪和计算机取证，接着介绍了信息安全测评与认证，然后对我国计算机安全立法作评述，最后探讨与计算机安全相关的道德问题。

国防科大计算机学院杨超群教授，对本书提出了许多宝贵的意见，在此表示衷心的感谢。浙江大学人工智能研究所的鲁东明教授、董亚波博士、郭晔博士、黄金钟博士、陈宇峰博士对本书提出了许多宝贵的意见，在此表示衷心的感谢。本书引用了中科院软件所石文昌博士和湖南大学计算机与通信学院郭媛妮硕士学位论文的部分研究成果，在此表示衷心的感谢。本书书稿由湖南宁乡创智电脑培训中心谢芬、谢静等学员录入与排版，在此谨表示衷心感谢。

感谢国家信息工作领导小组、计算机网络安全与信息化办公室（合同号：2001－研－041）、国家计算机网络与信息安全管理中心（合同号：2001－研 2B－003）、湖南省自然科学基金委（项目号 03JJY3103）对本书的相关研究工作的资助。

本书由李仁发主编，喻飞、朱淼良、周洲仪、徐成、刘晖编写。在编写本书的过程中，参阅了大量的国内外相关著作与文献，并引用了其中部分内容。在此，谨向相关作者表示衷心的感谢。

由于作者的学术水平有限，所以书中难免有不妥和错误之处，恳请读者与同行批评指正。

编　者

目　录

第 1 章　网络安全概述

在网络环境中，国家机密和商业秘密的保护，特别是政府上网后对涉密信息和敏感信息的保护，网上各种行为者的身份确认与权责的确认，高度网络化的各种业务（商务、政务等）信息系统运行的正常，网络银行、电子商务中的支付与结算的准确真实和金融机构数据保护与管理系统的稳定运行，都将成为国家主权、政治、经济、安全和社会稳定的焦点。为了有效地解决这些问题，网络安全成为信息化进程中的一个重要领域，受到各界人士的广泛关注。

1.1　网络安全基础

20 世纪 90 年代中期以来，随着网络技术突飞猛进的发展，特别是 Internet 的迅猛发展和美国政府率先推动的建设全球信息高速公路，使各国的信息化进程急剧加快。我国的信息化热潮也随之日益高涨，有关电子政务、电子商务乃至电子军务的讨论日益频繁。信息技术和网络空间，给社会的经济、科技、文化、教育和管理的各个方面都注入了新的活力。人们在享受信息化带来的众多好处的同时，也面临着日益突出的信息安全与保密的问题。

网络信息安全技术经过近十年来的发展，在信息安全技术的研究上形成了两个完全不同的角度和方向。一个角度从正面防御考虑，研究加密、鉴别、认证、授权和访问控制等；另一个角度从反面攻击考虑，研究漏洞扫描评估、入侵检测、紧急响应和防病毒。

1.1.1　网络安全的含义

网络安全的具体含义会随着“角度”的变化而变化。比如，从用户（个人、企业等）的角度来说，用户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，避免其他人尤其是竞争对手利用窃听、冒充、篡改、抵赖等手段侵犯用户的利益和隐私，同时也避免其他用户的非授权访问和破坏。

从网络服务提供商和管理者角度来说，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、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及对国家造成巨大的损失。

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。

从本质上来讲，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。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和理论都是网络安全所要研究的领域。网络安全涉及的内容既有技术方面的问题，也有管理方面的问题，两方面相互补充，缺一不可。技术方

面主要侧重于防范外部非法用户的攻击，管理方面则侧重于内部人为因素的管理。

因此网络安全包括以下几部份：

（1）运行系统安全。即保证信息处理和传输系统的安全。它侧重于保证系统正常运行，避免因为系统的崩溃和损坏而对系统存储、处理和传输的信息造成破坏和损失，避免由于电磁泄漏，产生信息泄露，干扰他人，受他人干扰。

（2）网络上系统信息的安全。包括用户口令鉴别，用户存取权限控制，数据存取权限、方式控制，安全审计，安全问题跟踪，计算机病毒防治，数据加密。

（3）网络上信息传播安全。即信息传播后果的安全，包括信息过滤等。它侧重于防止和控制非法、有害的信息进行传播。避免公用网络上大量自由传输的信息失控。

（4）网络上信息内容的安全。它侧重于保护信息的保密性、真实性和完整性。避免攻击者利用系统的安全漏洞进行窃听、冒充、诈骗等有损于合法用户的行为。本质上是保护用户的利益和隐私。

1.1.2 网络所面临的安全威胁

1. 互联网骨干网络面临的安全威胁

Internet 主要由两大基本架构组成：路由器构成 Internet 的主干，DNS 服务器将域名解析为 IP 地址。攻击互联网骨干网络最直接的方式就是攻击互联网主干路由器和 DNS 服务器。

如果一个攻击者能成功地破坏主干路由器用来共享路由信息的边界网关协议（BGP），或者更改网络中的 DNS 服务器，将能使 Internet 陷入一片混乱。为了寻找一些能够使主干路由器和 DNS 服务器彻底崩溃或者能够取得其系统管理权限的缓冲溢出或其他安全漏洞，恶意的高级攻击者通常会从头到尾，非常仔细地检查一些主流路由器和 DNS 服务器的服务程序代码和它们之间的通信协议的实现代码。路由代码非常复杂，目前已经发现并已修复了许多重要的安全问题，但是仍旧可能存在许多更严重的问题，并且很可能被黑客发现和利用。DNS 软件过去经常发生缓冲溢出这样的问题，在以后也肯定还可能发生类似的问题。如果攻击者发现了路由、DNS 或通信协议的安全漏洞，并对其进行大举攻击的话，大部分因特网将会迅速瘫痪。2002 年 8 月，互联网赖以运行的基础通信规则之一，ASN N0.1 信令的安全脆弱性就严重威胁互联网骨干网基础设施的安全。黑客可以利用 ASN N0.1 信令的安全漏洞开发相应的攻击程序，关闭 ISP 的骨干路由器、交换机和众多的基础网络设备，可最终引起整个互联网瘫痪。由于 ASN No.1 信令的安全脆弱性，超过 100 家计算机网络设备的提供商将要付出沉重代价。弥补这些缺陷的投入将超过 1 亿美金。数百家网络设备提供商在 2002 年早期就获得警告。由于多个 Internet 通信协议都是基于 ASN No.1 计算机网络语言，ASN No.1 的脆弱性将广泛威胁通信行业。最为显著的例子就是造成 SNMP 协议多个安全漏洞。相同的问题还影响至少其他三个互联网协议，在这里不做详细叙述。另外，随着黑客技术的发展，超级网络蠕虫、复杂的 DDoS 攻击等无不威胁着整个互联网的安全。

为防止骨干网基础设施遭到攻击，对于一般用户来说为确保自己的系统不会被作为攻击他人的跳板，需要对公共路由器和外部 DNS 服务器进行安全加固。如果公司的 DNS 服务器是为安全敏感的机器提供服务，则应为 DNS 服务器配置防火墙和身份验证服务器；确

保 DNS 服务器安装了最新补丁，对 DNS 服务器严格监控；如果认为是由 ISP 的安全缺陷造成的威胁，迅速和 ISP 取得联系，共同对付这种大规模的网络攻击。

2. 根域名服务器面临的安全威胁

什么是根域名服务器？全球共有 13 台根域名服务器。这 13 台根域名服务器中名字分别为“A”至“M”，其中 10 台设置在美国，另外各有一台设置于英国、瑞典和日本。下表是这些机器的管理单位、设置地点及最新的 IP 地址：

名称	管理单位及设置地点	IP 地址
A	INTERNIC.NET（美国，弗吉尼亚州）	198.41.0.4
B	美国信息科学研究所（美国，加利弗尼亚州）	128.9.0.107
C	PSINet 公司（美国，弗吉尼亚州）	192.33.4.12
D	马里兰大学（美国马里兰州）	128.8.10.90
E	美国航空航天管理局（美国加利弗尼亚州）	192.203.230.10
F	因特网软件联盟（美国加利弗尼亚州）	192.5.5.241
G	美国国防部网络信息中心（美国弗吉尼亚州）	192.112.36.4
H	美国陆军研究所（美国马里兰州）	128.63.2.53
I	Autonomica 公司（瑞典，斯德哥尔摩）	192.36.148.17
J	VeriSign 公司（美国，弗吉尼亚州）	192.58.128.30
K	RIPE NCC（英国，伦敦）	193.0.14.129
L	IANA （美国，弗吉尼亚州）	198.32.64.12
M	WIDE Project（日本，东京）	202.12.27.33

在根域名服务器中虽然没有每个域名的具体信息，但储存了负责每个域（如 COM、NET、ORG 等）的解析的域名服务器的地址信息，如同通过北京电信用户问不到广州市某单位的电话号码，但是北京电信可以告诉用户去查 020114。世界上所有互联网访问者的浏览器将域名转化为 IP 地址的请求（浏览器必须知道数字化的 IP 地址才能访问网站）理论上都要经过根服务器的指引后去该域名的权威域名服务器（Authoritative Name Server，如 haier.com 的权威域名服务器是 dns1.hichina.com）上得到对应的 IP 地址。当然现实中提供接入服务的 ISP 的缓存域名服务器上可能已经有了这个对应关系（域名到 IP 地址）的缓存。

根域名服务器是架构因特网所必须的基础设施。在国外，许多计算机科学家将根域名服务器称作“真理”（TRUTH），足见其重要性。攻击整个因特网最有力、最直接，也是最致命的方法恐怕就是攻击根域名服务器了。早在 1997 年 7 月，这些域名服务器之间自动传递了一份新的关于因特网地址分配的总清单，然而这份清单实际上是空白的。这一人为失误导致了因特网出现最严重的局部服务中断，造成数天因特网无法访问，电子邮件也无法发送。在 2002 年的 10 月 21 日美国东部时间下午 4:45 开始，这 13 台服务器又遭受到了有史以来最为严重的也是规模最为庞大的一次网络袭击。此次受到的攻击是 DDoS 攻击，超过常规数量 30 至 40 倍的数据猛烈地向这些服务器袭来并导致其中的 9 台不能正常运行。7 台丧失了对网络通信的处理能力，另外两台也紧随其后陷于瘫痪。

2002 年 10 月 21 日的这次攻击对于普通用户来说可能根本感觉不到受到了什么影响。如果仅从此次事件的“后果”来分析，也许有人认为“不会所有的根域名服务器都受到攻

击，因此可以放心”，或者认为“根域名服务器产生故障也与自己没有关系”。因为他们并不清楚的根本原因是：

（1）并不是所有的根域名服务器都受到了影响。

（2）攻击在短时间内便告结束。

（3）攻击比较单纯，因此易于采取相应措施。

由于目前对于 DDoS 攻击还没有什么特别有效的解决方案，设想一下如果攻击的时间再延长，攻击再稍微复杂一点，或者再多有一台服务器瘫痪，全球互联网将会有相当一部分网页浏览以及 E-mail 服务彻底中断。

虽然此次事故发生的原因不在于根域名服务器本身，而在于因特网上存在很多脆弱的机器，这些脆弱的机器被植入 DDoS 客户端程序（如特洛伊木马），然后同时向作为攻击对象的根域名服务器发送信息包，从而干扰对象服务器的服务甚至直接导致其彻底崩溃。但是这些巨型服务器的漏洞是肯定存在的，即使现在没有被发现，以后也肯定会被发现。而一旦被恶意攻击者发现并被成功利用的话，将会使整个互联网处于瘫痪之中。

1.1.3 网络攻击发展动向

1. 近年来五种影响最大的攻击

（1）红色代码。2001 年 7 月的某天，全球的 IDS 几乎同时报告遭到不名蠕虫攻击。信息安全组织和专业人士纷纷迅速行动起来，使用蜜罐（Honeypots）技术从因特网上捕获数据包进行分析，最终发现这是一利用微软 IIS 缓冲溢出漏洞进行感染的变种蠕虫。其实这一安全漏洞早在一个月以前就已经被 eEye Digital Security 发现，微软也发布了相应的补丁程序，但是却很少引起组织和企业系统管理员的足够重视，下载并安装了该补丁。在红色代码首次爆发的短短 9 个小时内，这一小小蠕虫以迅雷不及掩耳之势迅速感染了 250，000 台服务器，其速度和深入范围之广也马上引起了全球媒体的注意。最初发现的红色代码蠕虫还只是篡改英文站点的主页，显示“Welcome to http://www.worm.com! Hacked by Chinese!”等信息。但是随后的红色代码蠕虫便如同洪水般在互联网上泛滥，发动 DoS（拒绝服务）攻击以及格式化目标系统硬盘，并会在每月 20～28 日对白宫的 WWW 站点的 IP 地址发动 DoS 攻击，使白宫的 WWW 站点不得不全部更改自己的 IP 地址。之后，红色代码又不断的变种，其破坏力也更强，在红色代码 II 肆虐时，有近 2 万服务器、500 万网站被感染。从红色代码的肆虐中网络用户可以得到启示，只要注意及时更新补丁和修复程序，对于一般的蠕虫传播是完全可以避免的。因此作为系统管理员在平时应该多注意自己的系统和应用程序所出现的最新漏洞和修复程序，对于提供了修复程序和解决方案的应立即安装和实施；在网络遭到攻击时，为进行进一步的分析，使用蜜罐技术是一种非常行之有效的方法；红色代码猛攻白宫之所以被成功扼制，是因为 ISP 们及时将路由表中所有白宫的 IP 地址都清空了，在这一蠕虫代码企图阻塞网络之前，在因特网边界就已被丢弃。另外，白宫网站也立即更改了所有服务器的 IP 地址。

（2）尼姆达（Nimda）。尼姆达（Nimda）是在 9·11 恐怖袭击一个星期后出现的。不少人现在还清楚地记得因为美国的网络常常成为恐怖组织和对其怀有敌意的黑客的攻击目标。另外，地区之间的冲突和摩擦也会导致双方黑客互相实施攻击。当时传言是中国为了试探美国对网络恐怖袭击的快速反应能力而散布了尼姆达病毒，一些安全专家甚至喊出

了“我们现在急需制定另一个‘曼哈顿计划’，以随时应对网络恐怖主义”的口号，由此可见尼姆达在当时给人们造成的恐慌。尼姆达病毒是在早上 9：08 发现的，它明显地比红色病毒更快、更具有摧毁能力，半小时之内就传遍了整个世界。随后在全球各地侵袭了 830 万部电脑，总共造成将近 10 亿美元的经济损失。同“红色代码”一样，“尼姆达”也是通过网络对 Windows 操作系统进行感染的一种蠕虫型病毒。但是它与以前所有的网络蠕虫的最大不同之处在于，“尼姆达”通过多种不同的途径进行传播，而且感染多种 Windows 操作系统。“红色代码”只能够利用 IIS 的漏洞来感染系统，而“尼姆达”则利用了至少 4 种微软产品的漏洞来进行传播。从 Nimda 蠕虫病毒播发的全程和特点来看，网络用户又可以深刻地认识到，对网络攻击事件的紧急响应能力以及和安全专家们建立良好的关系是非常重要的。为阻断恶意蠕虫的传播，往往需要在和广域网的接口之间设置过滤器，或者干脆暂时断开和广域网的连接，在电子邮件客户端和网络浏览器中禁止任意脚本的执行对网络安全性来说也是很关键的。

（3）Melissa（1999）和 Love Letter（2000）。在 1999 年 3 月爆发的 Melissa 病毒和 2000 年 5 月爆发的 Love Letter 病毒因为它们能够迅速蔓延，给网络造成了极大的危害。Melissa 是 MicrosoftWord 宏病毒，LoveLetter 则是 VBScript 病毒，二者除了都是利用 Outlook 电子邮件附件进行传播外，都是利用 Microsoft 公司开发的 Script 语言缺陷进行攻击，因此二者非常相似。用户一旦在 Microsoft Outlook 里打开这个邮件，系统就会自动复制恶意代码并向地址簿中的所有邮件地址发送带有病毒的邮件。由于 Outlook 用户数目众多，其病毒又可以很容易地被复制，很快许多公司的邮件服务器就被洪水般的垃圾邮件塞满而中断了服务。一些公司在发现遭到攻击或可能遭到攻击后立即将自己内部网络与因特网断开，在内部网遭到蠕虫感染的机器清除或隔离，等病毒风暴过后才连接到 Internet 上，因此才免受其危害。当时的各大防病毒厂商在病毒爆发后不久立即向他们的客户分发病毒签名文件，但是由于用户太多却要在同一时间下载和更新病毒库，使得要想及时更新签名文件变得非常困难，这无疑更加助长了病毒的肆虐。也正是因为这个原因使得 Melissa 和 LoveLetter 病毒所产生的危害仅次于红色代码和尼姆达。Melissa 和 LoveLetter 的爆发可以说是信息安全的唤醒警钟，它引起了当时人们对信息安全现状的深思，并无形中对信息安全的设施和人才队伍的发展起了很大的促进作用。Melissa 和 LoveLetter 促进了企业和公司对网络安全的投资，尤其是对防病毒方面的投入。许多公司对网络蠕虫病毒的紧急响应表现出来的无能为力促进了专业网络安全紧急响应小组的空前壮大。

（4）分布式拒绝服务攻击。在 2000 年新千年到来之际，信息安全领域的人们都以为可以长长地嘘一口气了，因为他们以为由于存在千年虫的问题，在信息网络安全领域中应该暂时还不会出现什么风波。然而，一月之后却来了一场谁也意想不到的“大洪水”。在全球知名网站雅虎第一个宣告因为遭受分布式拒绝服务攻击而彻底崩溃后，紧接着 Amazon.com、CNN、E*Trade、ZDNet、Buy.com、Excite 和 eBay 等其他七大知名网站也几乎在同一时间彻底崩溃。这无疑又一次敲响了因特网的警钟。在这以前人们其实已经接触过来自数以千计的机器的 Flood 攻击，但是像雅虎遭受的这样如此大规模的攻击却从未见过甚至想象过。DDoS 闪电般的攻击使人们认识到英特网远比他们想象的更加脆弱，分布式地拒绝服务攻击产生的影响也远比他们原来想象中的要大得多。利用因特网上大量的机器进行 DDoS 攻击，分布式扫描和分布式口令破解等，一个攻击者能够达到许多意想不到

的强大效果。从雅虎遭到强大的 DDoS 攻击中人们又获得了启示，要阻止这种攻击关键是网络出口反欺骗过滤器的功能强大。也就是说如果用户的 Web 服务器收到的数据包的源 IP 地址是伪造的话，用户的边界路由器或防火墙必须能够识别出来并将其丢弃，网络安全事件响应小组们认识到他们必须和他们的 ISP 共同去阻止数据包的 Flood 攻击。如果失去 ISP 的支持，即使用户的防火墙功能再强大，用户网络出口的带宽仍旧可能被全部占用。最有效的也是最快速的方法就是和 ISP 联手一起来通过丢包等方法阻挡这一庞大的 Flood 攻击。不幸的是 DDoS 攻击即使在目前也仍旧是互联网面临的主要威胁，当然这主要是因为 ISP 在配合阻断 DDoS 攻击上速度太慢引起的，从而使事件紧急响应的效果大打折扣。

（5）特洛伊木马后门（1998～2000）。在 1998 年 7 月，黑客 Cult of the Dead Cow（cDc）推出的强大后门制造工具 Back Orifice（或称 BO）使庞大的网络系统轻而易举地陷入了瘫痪之中。安装 BO 主要目的是，黑客通过网络远程入侵并控制受攻击的 Win95 系统，从而使受侵机器“言听计从”。BO 以多功能、代码简洁而著称。并且由于 BO 操作简单，只要简单地点击鼠标即可，即使最不熟练的黑客也可以成功地引诱用户安装 Back Orifice。只要用户安装了 Back Orifice，黑客几乎就可以为所欲为了，可以非法访问敏感信息，修改和删除数据，甚至改变系统配置。如果仅仅从功能上讲，Back Orifice 完全可以和市场上最流行的商业远程控制软件，像赛门铁克的 pcanywhere，CA 的 ControlIT 和免费软件 VNC 等相媲美。因此，许多人干脆拿它来当作远程控制软件来进行合法的网络管理。由于其简单易用和大肆地宣传，BO 迅速被众多的初级黑客用来攻击系统。BO 的成功后来也迅速地带动和产生了许多类似的远程控制工具，像 SubSeven，NetBus，Hack-a-Tack 和 Back Orifice 2000（BO2K）等。这些攻击工具和方法甚至一直保留到现在，作为黑客继续开发新的和更加强大的特洛伊木马后门，以避开检测，绕过个人防火墙和伪装自己的设计思路。Back Orifice 和其他类似的木马后门工具使人们从根本上认识到了对用户进行一定的安全方面的培训，使他们不要随意运行不信任软件和广泛地配置防病毒软件是多么的重要。

2. 未来的攻击机制

（1）超级蠕虫。无论是手段的高明性，还是破坏的危害性，计算机网络受到蠕虫的威胁都在激增。民意调查中显示人们仍旧将这一威胁看作是计算机网络将面临的最大威胁之一，有超过 36%的人认为超级蠕虫的威胁应该摆在第一位。超级蠕虫一般被认为是混合蠕虫，它通常能自我繁殖，并且繁殖速度会越来越快，传播的范围会越来越广。更可怕的是它的一次攻击就能针对多个漏洞。例如，超级蠕虫潜入系统后，不是仅仅攻击某个漏洞，而是会尝试某个已知漏洞，然后再尝试一个又一个漏洞。超级蠕虫的一枚弹头针对多个漏洞发动攻击，所以总有一个会有效果。如果它发现用户未打补丁的地方，那用户就在劫难逃了。而事实上没有哪家公司的系统完全打上了所有的补丁。很多安全专家逐渐看到的通过 IM（即时消息）进行传播的蠕虫就可以说是一种超级蠕虫。黑客将一个链接发给 IM 用户后，如果用户点击链接，蠕虫就会传播给该用户的 IM 地址簿上的所有人。有了 IM，用户将随时处于连接状态，所以也随时会受到攻击。

（2）隐秘攻击。现在越来越多的黑客把攻击后成功地逃匿 IDS 的检测看作是一种艺术。有许多新工具能使他们在攻击用户的系统后不留下任何蛛丝马迹，有多种高级黑客技术将能使之成为可能，而这些技术已经广泛地被专业黑客所采用。

多变代码：这些恶意软件其本身可能是一种病毒、蠕虫、后门或漏洞攻击脚本。它

通过动态地改变攻击代码可以逃避入侵检测系统的特征检测（Signature-based detection，即模式匹配）。攻击者常常利用这种多变代码侵入因特网上带有入侵检测的系统或入侵警告系统。

逃避检测：攻击者利用反侦测手段进行攻击来逃避 IDS 的检测。例如，通过利用 Burneye，可以掩盖黑客对系统的攻击企图；使用 Defiler 的工具 Toolkit 可以覆盖攻击者对目标文件系统所做的修改而留下的蛛丝马迹。

隐蔽通道：为了和后门或者恶意软件进行通讯，攻击者建立一条非常隐蔽的通信通道。攻击者常常将通讯端口建立在一些不常用的通信协议端口上，如 HTTPS 或者 SSH。

内核级后门：通过从系统内核控制一个系统，攻击者获得对目标系统的完全控制权限，而对受害者来说一切都似乎风平浪静。

嗅探式后门：通过将后门和用户使用的嗅探器捆绑在一起，攻击者能够巧妙地绕过通过查看正在监听的端口来发现后门这一传统的检测方法，使受害者被安了后门却还一直蒙在鼓里。

反射式/跳跃式攻击：与其直接向目标系统发送数据，很多攻击者觉得利用 TCP/IP 欺骗技术能隐蔽攻击者的真实地址，误导正常的检测。如反射式的 DoS 攻击。

1.2　影响网络安全的主要因素

Internet 在其早期是一个开放的为研究人员服务的网际网，是完全非赢利性的信息共享载体，所以几乎所有的 Internet 协议都没有考虑安全机制。这点从 Internet 上最通用的应用 FTP、Telnet 和电子邮件中的用户口令的明文传输以及 IP 报文在子网段上的广播传递能充分地体现出来。只是近些年来，Internet 的性质和使用人员的情况发生了很大的变化，使得 Internet 的安全问题显得越来越突出。随着 Internet 的全球普及和商业化，用户越来越私人化，如信用卡号等和其自身利益相关的信息也通过 Internet 传输，而且越来越多的信息放在网上是为了赢利，并不是完全免费的信息共享，所以其安全性也成为人们日趋关注的问题。

1.2.1　操作系统因素

操作系统是计算机重要的系统软件，它控制和管理计算机所有的软、硬件资源。如果操作系统被攻破，即使里面其他应用软件的安全措施非常完美，也是徒劳。由于操作系统的重要地位，所以攻击者常常以操作系统为主要攻击目标。入侵者所做的一切，也大都是围绕着这个中心目标的。

操作系统的脆弱性主要表现在以下一些方面：

操作系统的程序是可以动态连接的。I/O 的驱动程序和系统服务都可以用打补丁的方式进行动态链接。Linux 操作系统的版本升级都是采用打补丁的方式进行的。虽然这些操作需要被授予特权，但这种方法厂商可用，黑客也可以用。动态链接也是计算机病毒产生的环境。一个靠打补丁改进和升级的操作系统是不可能从根本上解决安全问题的。然而，操作系统支持程序的动态链接与动态数据交换是现代系统集成和系统扩展的需要，显然这与安全是矛盾的。

操作系统支持在网络上传输文件，包括可执行文件，即在网络上加载和安装程序。