高等职业院校国家技能型紧缺人才培养培训工程规划教材
·计算机应用与软件技术专业

电子·教育

网络安全与管理

林 涛 主编　张建辉 黄瑾瑜 廖 朗 副主编

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

高等职业院校国家技能型紧缺人才培养培训工程规划教材·计算机应用与软件技术专业

网络安全与管理

林 涛 主 编
张建辉
黄瑾瑜 副主编
廖 朗

電子工業出版社
Publishing House of Electronics Industry
北京·BEIJING

内 容 简 介

本书是一本从实战出发，以应用为目的，防范手段为重点，理论讲述为基础的系统性、实战性、应用性较强的网络安全课程实用教材。教材摒弃了传统网络安全教材理论过多、实用性不强的问题，是一本紧密跟踪网络安全领域最新问题和技术运用的教材。教材从应用的角度，系统讲述了网络安全所涉及的理论及技术。以阶段能力培养为目的，每个能力阶段为一个章节，开始为问题的背景介绍，然后讲述处理手段和方法，最后系统讲述涉及的理论问题。在每章的最后设计了实训内容，规划了任务，通过实战演练使读者能够综合运用书中所讲授的技术进行网络信息安全方面的实践。

本书力求避免抽象的理论介绍，而是通过案例讲解相关的技术和知识。本书可作为高等职业院校计算机应用与软件技术专业的教材，也可作为自学和急需了解计算机网络安全相关技术和知识的技术人员的参考书，中等技校也可以参考部分内容教学。

图书在版编目(CIP)数据

网络安全与管理/林涛主编. —北京：电子工业出版社，2005.8
高等职业院校国家技能型紧缺人才培养培训工程规划教材·计算机应用与软件技术专业
ISBN 7-121-01571-4

Ⅰ. 网… Ⅱ. 林… 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 079716 号

责任编辑：洪国芬
印　　刷：北京铁成印刷厂
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　邮编 100036
经　　销：各地新华书店
开　　本：787×1 092　1/16　印张：17.75　字数：454 千字
印　　次：2005 年 8 月第 1 次印刷
印　　数：6 000 册　定价：25.00 元

凡购买电子工业出版社的图书，如有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系。联系电话：（010）68279077。质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

出 版 说 明

高等职业教育是我国高等教育体系的重要组成部分，也是我国职业教育体系的重要组成部分。社会需求是职业教育发展的最大动力。根据劳动市场技能人才的紧缺状况和相关行业人员资源需求预测，教育部会同劳动和社会保障部、国防科工委、信息产业部、交通部、卫生部启动了“职业院校制造业和现代服务业技能型紧缺人才培养培训工程”，明确了高等职业教育的根本任务是要从劳动力市场的实际需要出发，坚持以就业为导向，以全面素质为基础，以能力为本位，把提高学生的职业能力放在突出的位置，加强实践教学，努力造就数以千万计的制造业和现代服务业一线迫切需要的高素质技能型人才，并且优先确定了“数控技术应用”、“计算机应用与软件技术”、“汽车运用与维修”、“护理”等四个专业领域，在全国选择确定200多所高职院校作为承担技能型紧缺人才培养培训工程示范性院校，其中计算机应用与软件技术专业79所，软件示范性高职学院35所，数控技术应用专业90所，汽车运用与维修专业63所。为加快实施技能型人才培养培训工程，教育部决定，在3～5年内，高职院校学制要由3年逐步改为2年。

为了适应高等职业教育发展与改革的新形势，电子工业出版社在国家教育部、信息产业部有关司局的支持、指导和帮助下，进行了调研，探索出版符合高等职业教育教学模式、教学方法、学制改革的新教材的路子，并于2004年4月3日～13日在南京分别召开了“计算机应用与软件技术”、“数控技术应用”、“汽车运用与维修”等3个专业的教材研讨会。参加会议的150多名骨干教师来自全国100多所高职院校，很多教师是双师型的教师，具有丰富的教学经验和实践经验。会议根据教育部制定的3个专业的高职两年制培养建议方案，确定了主干课程和基础课程共60个选题，其中，“计算机应用与软件技术专业”30个；“数控技术应用专业”12个；“汽车运用与维修专业”18个。

这批教材的编写指导思想是以两年制高等职业教育技能型人才为培养目标，明确职业岗位对专业核心能力和一般专业能力的要求，重点培养学生的技术运用能力和岗位工作能力，并围绕核心能力的培养形成系列课程链路。教材编写注重技能性、实用性，加强实验、实训、实习等实践环节。教材的编写内容和学时数较以往教材有根本的变化，不但对教材内容系统地进行了精选、优化和压缩，而且适当考虑了相应的职业资格证书的课程内容，有利于学生在获得学历证书的同时，顺利获得相应的职业资格证书，增强学生的就业竞争能力。为了突出教学效果，这批教材将配备电子教案，重点教材将配备多媒体课件。

这批教材按照两年制高职教学计划编写。第一学期教学所用的基础教材将于2004年9月前出版。第二学期及之后的教材大部分将于2004年12月前出版。这批教材是伴随着高等职业教育的改革与发展而问世的，可满足当前两年制高等职业教育教学的需求，教材所存在的一些不尽如人意之处，将在今后的教学实践中不断修订、完善和充实。我们将在教育部和信息产业部的指导和帮助下，一如既往地依靠业内专家，与科研、教学、产业第一线人员紧密结合，加强合作，与时俱进，不断开拓，为高等职业教育提供优质的教学资源和服务。

电子工业出版社
高等职业教育教材事业部
2004年8月

参与编写“高等职业院校国家技能型紧缺人才培养培训工程规划教材”的院校及单位名单

吉林交通职业技术学院
长春汽车高等专科学校
山西交通职业技术学院
湖南交通职业技术学院
云南交通职业技术学院
南京交通职业技术学院
陕西交通职业技术学院
浙江交通职业技术学院
江西交通职业技术学院
福建交通职业技术学院
南京工业职业技术学院
浙江工贸职业技术学院
四川职业技术学院
郴州职业技术学院
浙江师范大学高等技术学院
辽宁铁岭农业职业技术学院
河北承德石油高等专科学校
邢台职业技术学院
保定职业技术学院
武汉工交职业学院
湖南生物机电职业技术学院
大庆职业学院
三峡大学职业技术学院
无锡职业技术学院
哈尔滨工业大学华德应用技术学院
长治职业技术学院
江西机电职业技术学院
湖北省襄樊机电工程学院
河南漯河职业技术学院
吉林电子信息职业技术学院
陕西国防工业职业技术学院
天津中德职业技术学院
河南机电高等专科学校
平原大学
苏州工业园区职业技术学院
九江职业技术学院
宁波大红鹰职业技术学院
无锡轻工职业技术学院
江苏省宜兴轻工业学院
湖南铁道职业技术学院
顺德职业技术学院
广东机电职业技术学院
常州机电职业技术学院
常州轻工职业技术学院
南京工程学院数控培训中心
上海市教育科学研究院
深圳职业技术学院
深圳信息职业技术学院
湖北轻工职业技术学院
上海师范大学
广东技术师范学院
包头职业技术学院
山东济宁职业技术学院
无锡科技职业学院
钟山学院信息工程系
合肥通用职业技术学院
广东轻工职业技术学院
山东信息职业技术学院
大连东软信息技术学院
西北工业大学金叶信息技术学院
福建信息职业技术学院
福州大学工程技术学院
江苏信息职业技术学院
辽宁信息职业技术学院
华北工学院软件职业技术学院
南海东软信息技术职业学院
天津电子信息职业技术学院
北京信息职业技术学院
安徽新华学院
安徽文达信息技术职业学院

杭州电子工业学院软件职业技术学院
常州信息职业技术学院
武汉软件职业学院
长春工业大学软件职业技术学院
淮安信息职业技术学院
上海电机高等专科学校
安徽电子信息职业技术学院
上海托普信息技术学院
浙江工业大学
内蒙古电子信息职业学院
武汉职业技术学院
南京师范大学计算机系
苏州托普信息技术学院
北京联合大学
安徽滁州职业技术学院
新疆农业职业技术学院
上海交通大学软件学院
天津职业大学
沈阳职业技术学院
南京信息职业技术学院
南京四开电子有限公司
新加坡 MTS 数控公司
上海宇龙软件工程有限公司
北京富益电子技术开发公司
安徽职业技术学院
河北化工医药职业技术学院
河北工业职业技术学院
河北师大职业技术学院
北京轻工职业技术学院
成都电子机械高等专科学校
广州铁路职业技术学院
广东番禺职业技术学院
桂林电子工业学院高职学院
桂林工学院
河南职业技术师范学院
黄冈职业技术学院
黄石高等专科学校
湖北孝感职业技术学院
湖南信息职业技术学院
江西蓝天职业技术学院
江西渝州科技职业技术学院
江西工业职业技术学院
柳州职业技术学院
南京金陵科技学院
西安科技学院
西安电子科技大学
上海新侨职业技术学院
四川工商职业技术学院
绵阳职业技术学院
苏州工商职业技术学院
天津渤海职业技术学院
宁波高等专科学校
太原电力高等专科学校
无锡商业职业技术学院
新乡师范高等专科学校
浙江水利水电专科学校
浙江工商职业技术学院
杭州职业技术学院
浙江财经学院信息学院
台州职业技术学院
湛江海洋大学海滨学院
天津滨海职业技术学院

前　言

网络技术和社会发展是辩证的关系，一方面它正在而且将更广泛和深刻地改变传统的生产、经营、管理和生活方式，成为21世纪新的经济增长点和资讯的重要传播工具；另一方面，网络国际化、社会化、开放化、个人化的特点，使网络成为一个国家的虚拟边界，如果在网络安全方面稍有不慎，一个国家的经济、军事、社会、科技、政治等多方面将遭受严重甚至是致命的后果。因此，网络信息安全保障能力已经成为新世纪综合国力、经济竞争力、生存与发展能力的重要标志。

本书从理论和技术两个方面对网络信息安全的相关知识进行全面和系统的介绍。首先，本书结合最新网络信息安全方面的案例，介绍网络安全领域面临的问题、出现安全问题的原因，解决网络安全问题的技术手段与方法，以及未来安全问题的发展趋势；第二，从全面安全的角度，介绍构造完整网络安全保障体系的几个方面；第三，详细分析主流操作系统Windows、Linux中的安全问题及解决手段；第四，从网络体系的角度分析黑客常见的攻击手段，网络OSI模型中的安全结构和问题，以及对付黑客的技术方法；第五，分析网络病毒的传播方式、机理和预防方法，介绍主流防病毒软件的工作原理和使用方法；第六，分析防火墙技术的理论和防火墙体系结构，介绍主流防火墙产品的工作原理及使用方法；第七，从网络管理的角度，介绍安全网络管理的系统构架，网络控制代理、检测代理和主机代理，讲述网络安全管理系统的规范、原则和流程，给出网络安全设计的具体应用实例。在每章最后，设计网络安全管理实训内容，使读者能够综合运用所学的知识进行网络安全管理的实际运用。

作者根据多年从事计算机网络安全科研和教学工作的实践编写了此书。在编写过程中，力求使本书具有以下特点：

1．在内容安排上，尽量适合学生学习的特点，循序渐进，深入浅出，注重计算机网络安全的应用方法和技能的传授。

2．注重教材的先进性，力求反映当前计算机网络安全技术发展的最新成果。

3．兼顾教材的系统性与科学性，既要考虑知识和技能的科学体系，又要遵循教育规律，注意内容的取舍与相关课程的衔接，尽量避免内容重复。

4．力求文字精练，语言流畅，并注重向学生传授灵活的学习方法。

5．习题具有思考性和启发性，注重培养学生的创新能力。

通过对本教材的学习，读者可以系统地掌握计算机网络安全的基础知识和技能。

深圳信息职业技术学院的林涛老师对本书的编写思路与大纲进行了总体策划，指导全书的编写，并编写了第1、2、7、8、9章。张建辉、廖朗和黄瑾瑜老师协助主编完成了全书的工作，并分别编写了第3章和第4章、第5章、第6章。彭开慧老师对第2章的编写提供了很多帮助。

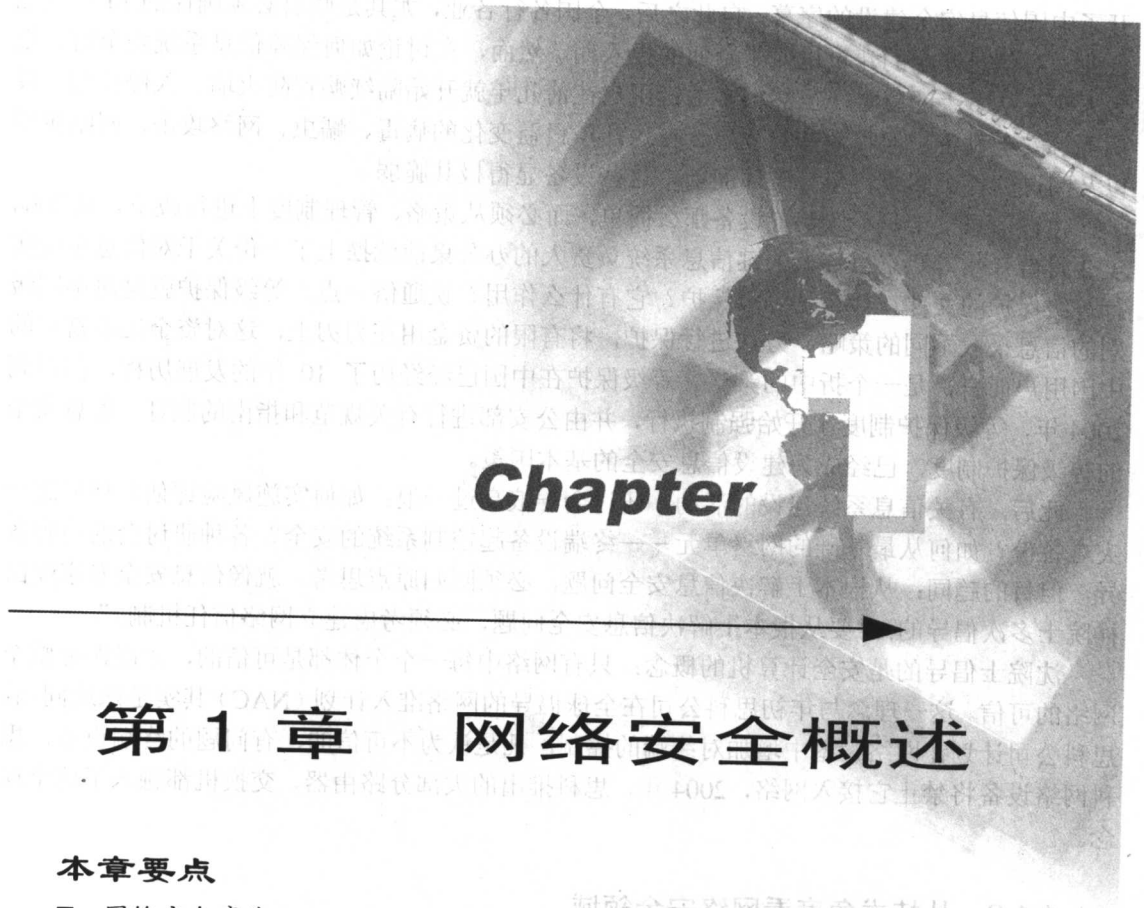
深圳信息职业技术学院张平安副教授审核并校对了全书。

由于时间仓促，加之作者水平有限，不当之处在所难免，恳请读者批评指正。作者的E-mail地址是lint@sziit.com.cn。

编　者

2005年2月

目　录



第 1 章　网络安全概述

本章要点

- 网络安全产业；
- 网络安全面临的威胁；
- 网络安全体系结构与模型；
- 网络安全策略。

1.1　引言

在回顾过去几十年众多安全问题的过程中，我们才醒悟：世界上没有绝对的安全。错误是所有安全漏洞的主要原因，正如那句谚语所说：人非圣贤孰能无过。防火墙、入侵检测系统或反病毒软件都不能保证绝对安全。用这种评论来介绍一本关于安全的书是不是使你觉得奇怪？其实并不奇怪，因为这是开始研究安全问题之前必须接受的残酷事实。

和传统教科书不同，我们没有从技术来讨论技术。因为技术本身并没有任何意义，只有当厂家利用该技术形成了产业，用户受益于该技术，技术才会有特别的意义。下面分别从用户、技术、产业角度来看网络安全领域。

1.1.1　从用户角度看网络安全领域

2004 年 1 月 8 日是个特别有意义的日子，在那天召开的全国信息安全保障工作会议，拉

开了中国信息安全建设的序幕。自此之后，全国各行各业，尤其是政府必须确保的14个重点行业，对信息安全的建设进入了全面的投入期。然而，在讨论如何保障信息系统安全时，很多人有无从下手的感觉。虽然很多关键用户在前几年就开始陆续购置防火墙、入侵检测、反病毒等安全设备，但收效并不理想。在这几年日益变化的病毒、蠕虫、网络攻击、网络犯罪以及间谍软件、网络钓鱼等破坏面前，这些设备显得极其脆弱。

建设信息安全，不像购置设备那么简单，而必须从策略、管理制度上进行改革。从2004年2月份开始，北京市各大关键信息系统负责人的办公桌前就摆上了一份关于对信息系统实行等级保护的文件。什么是等级保护？它有什么作用？说通俗一点，等级保护就是对不同级别的信息采取不同的策略、方法进行保护，将有限的资金用在刀刃上，这对资金还不富裕的中国用户而言，是一个折中的策略。等级保护在中国已经经历了10年的发展历程，但直到2004年，等级保护制度才开始强制执行，并由公安部进行有关规范和指南的制订。信息安全的等级保护制度，已经成为建设信息安全的基本国策。

此后，有关信息系统建设的活动、研讨会一浪高过一浪：如何实施风险评估？如何进行灾难备份？如何从最基础的网络单元——终端设备起控制系统的安全？各种研讨会的内容各异，但目的趋同：从根本上解决信息安全问题，必须回归原点思考。就像信息安全专家沈昌祥院士多次倡导的："要从根本上解决信息安全问题，必须考虑建立网络信任机制。"

沈院士倡导的是安全计算机的概念：只有网络中每一个个体都是可信的，才能保证整个网络的可信。这一理念与年初思科公司在全球倡导的网络准入计划（NAC）其实是殊途同归：思科公司计划在网络设备中增加对终端的控制，凡是认为不可信的、有问题的终端设备，思科网络设备将禁止它接入网络，2004年，思科推出的大部分路由器、交换机都融入了这个理念。

1.1.2 从技术角度看网络安全领域

从信息安全设备"老三样"防火墙、入侵检测和反病毒产品看，越来越多的厂商，将这三项功能集中在一个硬件盒子中，用一台设备解决多种难题。这种趋势在2003年已经抬头，但在2004年，几乎已经成为安全产品的"标配"，尤其是那些面对中小企业用户的整合安全产品，某些甚至增添了内容过滤、漏洞扫描、垃圾邮件过滤、SSL VPN、路由等各种功能：赛门铁克的综合网关整合了7项安全功能；网新易尚在其防火墙产品中，增添了反病毒、VPN功能；WatchGuard、ServeGate、SonicWall以及国内的瑞星公司等，都新推出了这类整合各种安全功能的硬件设备，虽然叫法不一，但实质一样。

这种融合不仅体现在安全功能的融合上，还体现在网络设备与安全设备的融合上：思科公司在其新推出的交换机和路由器产品中，增加了反病毒和入侵检测功能，并宣布，其未来的所有交换机中均增加安全模块。

与技术的融合相对应的是产品的多元化趋势。虽然出现了融合现象，但"老三样"依然活跃在市场上，并且呈急速上升趋势。联想信息安全事业部2004年一口气推出了45款防火墙，并在第三季度时，被IDC中国确认为国内防火墙销量第一，证明防火墙依然有很强的增长空间。但是，与此同时，随着攻击模式的多样化，安全技术和产品的发展也呈现出多样化的趋势。

垃圾邮件的泛滥成灾使反垃圾邮件产品成为2004年安全市场的主要角色。在一项反垃

圾邮件产品横向评测中，可以发现，市场上一下子出现了十多个品牌的反垃圾邮件产品；电子商务的发展使安全的远程办公环境成为迫切需求，在此情况下，SSL VPN 作为一种简单、方便、安全的远程接入设备成为市场新宠，同样地，厂商数量迅速增加到十几个；此外，对入侵检测技术和产品（IDS）的不满，导致了入侵防御技术（IPS）的出台；间谍软件和网络钓鱼的泛滥，催生出一种新的反间谍软件和反 Fishing 的行业；对漏洞的恐惧和对打补丁的厌倦催生出新的补丁分发工具市场；对海量日志文件头疼的分析催生出安全事件管理软件市场；对多种安全设备的管理难题催生出统一安全管理平台技术；对网上身份的认证催生出生物识别技术、双因素认证技术和各种智能卡技术；对灾难恢复又催生出一个巨大的产业——存储备份；对建立可信计算机环境的期望也许将产生一个巨大的行业——可信计算机。

这些新技术新产品，都活跃在 2004 年的安全设备大舞台上，安全技术和产品的多元化还将不断上演，也许，不久之后，随着病毒开始攻击手机等移动平台，在移动平台上，将照搬互联网上的全部安全大戏？

1.1.3 从产业角度看网络安全领域

2004 年 12 月 17 日，信息安全产业内最大的一桩并购案发生了：赛门铁克公司以 135 亿美元的天价收购了维尔公司。虽然对信息安全产业内的收购、兼并早有预期，心理早有准备，但如此巨大数额的兼并还是让产业界人士非常吃惊！

回顾这几年发生在信息安全产业内的兼并、收购事件，可以看到，许多安全厂商在这种兼并中迅速从小公司长大，形成信息安全领域内新的强品牌。以赛门铁克为例，从 2002 年开始，该公司一共收购了十几家安全公司，获得了从入侵检测到综合网关到安全服务的所有技术，而年营业额也从几亿美元迅速增长到去年的 18 亿美元，预计收购 Veritas 后，将达到 50 亿美元。而该公司，也从一个仅提供桌面防毒软件的公司，不仅迅速成长为信息安全产业内的毫无争议的“巨无霸”，也成为全球新的巨型 IT 公司。

思科对信息安全的发展思路同样如此，在 2004 年的 3 个月内，它就收购了 3 家公司，几年下来，收购的安全小厂商也不下十几种，获得了多种产品和技术；而年初时，Juniper 收购 NetScreen 的案例也曾轰动一时。

收购与兼并一定会长期在信息安全产业内进行下去，原因有几个方面：一是信息安全目前还是新兴的产业，其中大多数是正在成长的新兴公司，而作为信息安全这样一个独特、关键的领域，小公司很难获得用户的信赖，在 2004 年 9 月份《InfoWorld》对全球信息安全用户的一份报告中称，用户还是信赖像微软这样的大公司，虽然它的产品经常会有漏洞。另一方面的原因正如前述，产业内技术和产品多元化趋势明显，安全的木桶原理说明缺少哪一块都不行，作为大厂商而言，从头开发一项新技术显然是不可能的，最好的方式就是将它买下。

合作同样如此，思科收购了很多小型技术公司后，惟独对反病毒技术厂商趋势科技是个例外，不是收购它而是与它合作。道理很简单：购买产品容易，购买服务难。在思科的网络准入（NAC）计划中，不得不采取与趋势科技合作的态度。

1.2 网络安全面临的威胁

在网络出现以前，信息安全指对信息的机密性、完整性和可获性的保护，即面向数据的

安全。互联网出现以后，信息安全除了上述概念以外，其内涵又扩展到面向用户的安全。综合而言，网络安全包括物理安全威胁、操作系统的安全缺陷、网络协议的安全缺陷、应用软件的实现缺陷、用户使用的缺陷和恶意程序等6个方面的安全威胁。

1.2.1 物理安全威胁

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。

对于运行在任何操作系统下的计算机系统，物理安全都是一个必须要考虑的重要问题。但这个问题中的大部分内容与网络安全无关，例如，服务器被盗窃了，里面的硬盘就可能被窃贼使用物理读取的方式进行分析读取。这是一个极端的例子，更一般的情况可能是非法使用者接触了系统的控制台，重新启动计算机系统并获得控制权，或者通过物理连接的方式窃听网络信息。

在物理安全方面，与网络相关的问题主要在于传输数据的安全性。由于 TCP/IP 是一种分组交换协议，各个分组在网络上都是透明传输的，并经过不同的网络，由那些网络上的路由器转发，最后才能到达目的计算机。由于分组都是直接经过这些网络，所以这些网络上的计算机都有可能将其捕获，从而窃听到正在传输的数据。物理上的传输安全问题对网络安全非常重要。

由于物理网络的传输限制，并不是在网络上的任何位置都捕获分组信息。对于最常用的以太网，较老的共享式以太网能在任何一个位置窃听所有流经网络的分组信息，而新式的交换式以太网能够在交换机上隔离流向不同计算机的数据，因此安全性更高。然而，无论何种类型的网络，路由器总是一个非常关键的设备，所有流入和流出网络的数据都经过它，如果攻击者在路由器上窃听就会造成非常严重的安全问题。

目前主要的物理安全威胁包括以下3大类。

（1）自然灾害（例如地震、水灾和火灾等）、物理损坏（例如硬盘损坏、设备使用寿命到期和外力破损等）和设备故障（例如停电或电源故障造成设备断电和电磁干扰等）。特点是突发性、自然因素性、非针对性。这种安全威胁只破坏信息的完整性和可用性，无损信息的秘密性。

（2）电磁辐射（例如监听微机操作过程）、乘虚而入（例如进入安全进程后半途离开）和痕迹泄露（例如口令、密钥等保管不善，易于被人发现）。特点是难以察觉性、人为实施的故意性和信息的无意泄露性。这种安全威胁只破坏信息的秘密性，无损信息的完整性和可用性。

（3）操作失误（例如删除文件、格式化硬盘和线路拆除等）和意外疏忽（例如系统掉电、操作系统死机等系统崩溃）。特点是人为实施的无意性和非针对性。这种安全威胁只破坏信息的完整性和可用性，无损信息的秘密性。

1.2.2 操作系统的安全缺陷

操作系统介于用户和硬件之间。任何操作系统都自带一系列的系统应用程序，为用户使

用计算机提供有效和方便的操作。实际上，这些应用程序也是一种软件。不同于用户应用程序的是，操作系统的应用程序在用户安装操作系统时都是默认安装的。如果这些应用程序有安全缺陷，那么就会使系统处于不安全的状态。因此，了解操作系统经常出现的安全缺陷是很有必要的。

目前，人们使用的操作系统分为两大类：UNIX/Linux 系列和 Windows 系列。下面分别举例说明这两大类操作系统中存在的安全缺陷。

1．安全缺陷的检索

大多数信息安全工具都包含一个信息安全缺陷的数据库，例如，CERT 安全公告和 Bugtraq ID 等。但是，这些数据库对信息安全缺陷的描述格式各不相同。有时，很难确定在不同数据库中所描述的缺陷是否是同一个缺陷。每一个数据库都使用自己的编号以及描述格式，这样会给使用者带来很多不便。

CVE（Common Vulnerabilities and Exposures，公共缺陷检索）是信息安全确认的一个列表或者词典。它对不同信息安全缺陷的数据库之间提供一种公共的索引，是信息共享的关键。有了 CVE 检索之后，一个缺陷就有了一个公共的名字，从而可以通过 CVE 的条款检索到包含该缺陷的所有数据库。

2．UNIX 操作系统的安全缺陷

（1）远程过程调用（Remote Procedure Calls，RPC）。远程过程调用允许一台机器上的程序执行另一台机器上的程序。它们被广泛地用于提供网络服务，如 NFS 文件共享和 NIS。很多 UNIX 操作系统的 RPC 软件包中包含具有缓冲区溢出缺陷的程序。

（2）Sendmail。Sendmail 是在 UNIX 和 Linux 操作系统中用得最多的发送、接收和转发电子邮件的程序。

Sendmail 在 Internet 上的广泛应用，使它成为攻击者的主要目标，过去的几年里曾被发现若干个缺陷。事实上，第一个建议是 CERT/CC 在 1988 年提出的，指出了 Sendmail 中一个易受攻击的缺陷。其中最为常用的是攻击者可以发送一封特别的邮件消息给运行 Sendmail 的机器，Sendmail 会根据这条消息要求受劫持的机器把它的口令文件发送给攻击者的机器，这样口令就会被破解。UNIX 和 Linux 的大部分版本都会受到该漏洞的影响。Sendmail 有很多易受攻击的弱点，必须定期地检查 Sendmail 最新版本和补丁版本，并予以更新。如果没有更新版本或安装补丁文件，就可能受攻击。

3．Windows 系列操作系统的安全缺陷

（1）Unicode。Unicode 是 ISO 发布的统一全球文字符号的国际标准编码。它是一种双字节的编码。不论何种平台、何种程序、何种语言，Unicode 为每一个字符提供了惟一的序号。Unicode 标准被包括 Microsoft 在内的很多软件开发商所采用。通过向 IIS（Internet Information Server）服务器发出一个包含非法 Unicode UTF-8 序列的 URL，攻击者可以迫使服务器逐字“进入或退出”目录并执行任意脚本，这种攻击称为目录转换（Directory Traversal）攻击。

Unicode 用“% 2f”和“% 5c”分别表示“/”和“\”，但也可以用所谓的“超长”序列来代表这些字符。“超长”序列是非法的 Unicode 表示符，它们比实际代表这些字符的序列要长。“/”和“\”均可以用一个字节来表示。例如，“%c0%af”代表“/”用了两个字节，就是