21 世纪全国高职高专计算机系列实用规划教材

计算机网络安全技术

主　编　王其良　高敬瑜
副主编　吴冬燕　范荣真
参　编　顾　桢
主　审　宣仲良　曾瑶辉

北京大学出版社
PEKING UNIVERSITY PRESS

内 容 简 介

本书全面介绍了计算机网络安全的基础知识。全书共 9 章，包括：网络安全概述、操作系统安全、信息加密技术、数字签名与 CA 认证技术、防火墙技术与配置、网络病毒与防治、黑客攻击与防范、Web 服务安全、电子商务网络安全。

本书主要以网络安全技术实训为主，以操作应用软件来引导学生学习，可供计算机专业学生使用，也可供对网络安全技术感兴趣的读者参考使用。

图书在版编目(CIP)数据

计算机网络安全技术/王其良，高敬瑜主编. —北京：北京大学出版社，2006.8

(21 世纪全国高职高专计算机系列实用规划教材)

ISBN 7-301-10887-7

Ⅰ. 计… Ⅱ. ①王… ②高… 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(2006)第 078396 号

书　　名：计算机网络安全技术

著作责任者：王其良　高敬瑜　主编

责 任 编 辑：刘　丽

标 准 书 号：ISBN 7-301-10887-7/TP・0887

出 版 者：北京大学出版社

地　　址：北京市海淀区成府路 205 号　100871

网　　址：http://www.pup.cn　http://www.pup6.com

电　　话：邮购部 62752015　发行部 62750672　编辑部 62750667　出版部 62754962

电 子 信 箱：pup_6@163.com

印 刷 者：

发 行 者：北京大学出版社

经 销 者：新华书店

787 毫米×1092 毫米　16 开本　19.75 印张　450 千字

2006 年 8 月第 1 版　2006 年 8 月第 1 次印刷

定　　价：28.00 元

21世纪全国高职高专计算机系列实用规划教材

专家编审委员会

信息技术的职业化教育

(代丛书序)

刘瑞挺/文

北京大学出版社第六事业部组编了一套《21 世纪全国高职高专计算机系列实用规划教材》。为此，制订了详细的编写目的、丛书特色、内容要求和风格规范。在内容上强调面向职业、项目驱动、注重实例、培养能力；在风格上力求文字精练、图表丰富、脉络清晰、版式明快。

一、组编过程

2004 年 10 月，第六事业部开始策划这套丛书，分派编辑深入各地职业院校，了解教学第一线的情况，物色经验丰富的作者。2005 年 1 月 15 日在济南召开了“北大出版社高职高专计算机规划教材研讨会”。来自 13 个省、41 所院校的 70 多位教师汇聚一堂，共同商讨未来高职高专计算机教材建设的思路和方法，并对规划教材进行了讨论与分工。2005 年 6 月 13 日在苏州又召开了“高职高专计算机教材大纲和初稿审定会”。编审委员会委员和 45 个选题的主、参编，共 52 位教师参加了会议。审稿会分为公共基础课、计算机软件技术专业、计算机网络技术专业、计算机应用技术专业 4 个小组对稿件逐一进行审核。力争编写出一套高质量的、符合职业教育特点的精品教材。

二、知识结构

职业生涯的成功与人们的知识结构有关。以著名侦探福尔摩斯为例，作家柯南道尔在“血字的研究”中，对其知识结构描述如下：

- 文学知识——无；
- 哲学知识——无；
- 政治学知识——浅薄；
- 植物学知识——不全面。对于药物制剂和鸦片却知之甚详。对毒剂有一般了解，而对于实用园艺却一无所知；
- 化学知识——精深；
- 地质学知识——偏于应用，但也有限。他一眼就能分辨出不同的土质。根据裤子上泥点的颜色和坚实程度就能说明是在伦敦什么地方溅上的；
- 解剖学知识——准确，却不系统；
- 惊险小说知识——很渊博。似乎对近一个世纪发生的一切恐怖事件都深知底细；
- 法律知识——熟悉英国法律，并能充分实用；
- 其他——提琴拉得很好，精于拳术、剑术。

事实上，我国唐朝名臣狄仁杰，大宋提刑官宋慈，都有类似的知识结构。审视我们自己，每人的知识结构都是按自己的职业而建构的。因此，我们必须面向职场需要来设计教材。

三、职业门类

我国的职业门类分为 18 个大类：农林牧渔、交通运输、生化与制药、地矿与测绘、材料与能源、土建水利、制造、电气信息、环保与安全、轻纺与食品、财经、医药卫生、旅游、公共事业、文化教育、艺术设计传媒、公安、法律。

每个职业大类又分为二级类，例如电气信息大类又分为 5 个二级类：计算机、电子信息、通信、智能控制、电气技术。因此，18 个大类共有 75 个二级类。

在二级类的下面，又有不同的专业。75 个二级类共有 590 种专业。俗话说：“三百六十行，行行出状元”，现代职业仍在不断涌现。

四、IT 能力领域

通常信息技术分为 11 个能力领域：规划的能力、分析与设计 IT 解决方案的能力、构建 IT 方案的能力、测试 IT 方案的能力、实施 IT 方案的能力、支持 IT 方案的能力、应用 IT 方案的能力、团队合作能力、文档编写能力、项目管理能力以及其他能力。

每个能力领域下面又包含若干个能力单元，11 个能力领域共有 328 个能力单元。例如，应用 IT 方案能力领域就包括 12 个能力单元。它们是操作计算机硬件的能力、操作计算软件包的能力、维护设备与耗材的能力、使用计算软件包设计机构文档的能力、集成商务计算软件包的能力、操作文字处理软件的能力、操作电子表格应用软件的能力、操作数据库应用软件的能力、连接到互联网的能力、制作多媒体网页的能力、应用基本的计算机技术处理数据的能力、使用特定的企业系统以满足用户需求的能力。

显然，不同的职业对 IT 能力有不同的要求。

五、规划梦想

于是我们建立了一个职业门类与信息技术的平面图，以职业门类为横坐标、以信息技术为纵坐标。每个点都是一个函数，即 IT(Professional)，而不是 IT+Professional 单纯的相加。针对不同的职业，编写它所需要的信息技术教材，这是我们永恒的主题。

这样组合起来，就会有 IT((328)*(Pro(590)))，这将是一个非常庞大的数字。组织这么多的特色教材，真的只能是一个梦想，而且过犹不及。能做到 IT((11)*(Pro(75)))也就很不容易了。

因此，我们既要在宏观上把握职业门类的大而全，也要在微观上选择信息技术的少而精。

六、精选内容

在计算机科学中，有一个统计规律，称为 90/10 局部性原理(Locality Rule)：即程序执行的 90%代码，只用了 10%的指令。这就是说，频繁使用的指令只有 10%，它们足以完成 90%的日常任务。

事实上，我们经常使用的语言文字也只有总量的 10%，却可以完成 90%的交流任务。同理，我们只要掌握了信息技术中 10%频繁使用的内容，就能处理 90%的职业化任务。

有人把它改为 80/20 局部性原理，似乎适应的范围更广些。这个规律为编写符合职业教育需要的精品教材指明了方向：坚持少而精，反对多而杂。

七、职业本领

以计算机为核心、贴近职场需要的信息技术已经成为大多数人就业的关键本领。职业教育的目标之一就是培养学生过硬的 IT 从业本领，而且这个本领必须上升到职业化的高度。

职场需要的信息技术不仅是会使用键盘、录入汉字，而且还要提高效率、改善质量、降低成本。例如，两位学生都会用 Office 软件，但他们的工作效率、完成质量、消耗成本可能有天壤之别。领导喜欢谁？这是不言而喻的。因此，除了道德品质、工作态度外，必须通过严格的行业规范和个人行为规范，进行职业化训练才能养成正确的职业习惯。

我们肩负着艰巨的历史使命。我国人口众多，劳动力供大于求的矛盾将长期存在。发展和改革职业教育，是我国全面建设小康社会进程中一项艰巨而光荣的任务，关系到千家万户人民群众的切身利益。职业教育和高技能人才在社会主义现代化建设中有特殊的作用。我们一定要兢兢业业、不辱使命，把这套高职高专教材编写好，为我国职业教育的发展贡献一份力量。

刘瑞挺教授　曾任中国计算机学会教育培训委员会副主任、教育部理科计算机科学教学指导委员会委员、全国计算机等级考试委员会委员。目前担任的社会职务有：全国高等院校计算机基础教育研究会副会长、全国计算机应用技术证书考试委员会副主任、北京市计算机教育培训中心副理事长。

前　言

计算机网络成为当前社会发展的重要推动力。社会经济发展、国防信息建设以及与人们生活息息相关的各行各业，对计算机网络的依赖程度都不断增大。计算机网络给人们带来便利的同时，也带来了保证信息安全的巨大挑战。如何使信息不受黑客的入侵，如何保证计算机网络不间断地工作并提供正常的服务，是各个组织信息化建设必须考虑的重要问题。

本书着重于从实训与应用的角度介绍计算机网络安全，使读者了解一般网络安全的基础理论及技术原理，从实训中认识、理解什么是网络安全，并掌握常用的安全应用技术。全书共 9 章，第 1 章主要介绍计算机网络安全的相关概念，计算机网络的安全体系结构。第 2 章主要介绍计算机操作系统的安全基础与防范措施，包括：操作系统的安全机制及安全级别、操作系统安全技术。第 3 章主要介绍信息加密与公钥架构(Public Key Infrastructure，PKI)技术，包括：加密体系；单钥加密和双钥加密算法；链路、节点、端到端加密；公钥架构。第 4 章主要介绍数字签名与 CA 认证技术，掌握个人数字凭证的申请、颁发和使用。第 5 章主要介绍防火墙技术，包括：防火墙体系结构、包过滤防火墙和应用代理防火墙，以及防火墙的应用。第 6 章主要介绍计算机病毒防范技术，包括：计算机病毒的工作原理和分类，计算机病毒的检测和防范技术，各种防治病毒的软件的使用。第 7 章主要介绍网络黑客的攻击与防范，包括：黑客常用的各种攻击工具及攻击步骤、各种常用的防黑客的方法与工具的使用。第 8 章主要介绍因特网中 Web 服务器的安全性，包括 FTP、电子邮件及 Web 可能的攻击技术及其安全保护措施。第 9 章主要介绍电子商务的安全性，包括电子商务的安全需求分析、电子商务采取的安全措施。本书涉及的内容操作性比较强，在学习时，可多安排学生的实训操作课时，加强实训的监督，并要求学生认真写好实训报告。对书中一些理论如需要进一步加深的，应该指导学生参阅相应的参考书。建议本课程的教学时间为 64 学时，其中 32 学时用于授课，32 学时用于实训。第 1 章安排 2 学时，第 2 章、第 3 章、第 4 章分别安排 6 学时，第 5 章、第 6 章、第 8 章、第 9 章分别安排 8 学时，第 7 章安排 12 学时。

本书由王其良，高敬瑜任主编，吴冬燕，范荣真任副主编，顾桢任参编。王其良编写第 1 章以及第 8 章，范荣真编写第 2 章、第 5 章、第 9 章，高敬瑜编写第 3 章、第 4 章，吴冬燕编写第 6 章，顾桢编写第 7 章。本书由苏州职业大学计算机工程系宣仲良主任，保险职业学院信息系曾瑶辉主任担任主审，他们对本书的修改提出了宝贵的意见，在此表示衷心的感谢！

本书是北京大学出版社组织的 21 世纪全国高职高专计算机系列实用规划教材之一，在取材上突出培养和强化学生的实践能力与应用能力，加强了实训内容的编写，在理论上取精而且简单明了。本书特别突出了各项技术的应用性，希望能贴近高职高专学生的学习特

点，从而激发起学习兴趣，在实践中提高其对计算机网络安全的应对与控制能力。

网络安全是一门涉及计算机科学、通信技术、密码技术、应用数学等多门学科的交叉学科，同时在应用上，网络安全技术和产品发展很快，因此这本书的编写思想是，理论讲解简洁化，应用实例新颖化，操作步骤详细化，以实训引导学生理解理论，从而达到应用的目的。当然，在采用本书做实验时，也可根据具体情况采用熟悉的实例。

由于编写水平及时间所限，书中难免有疏漏之处，恳请广大读者和专家批评指正。

编 者

2006 年 2 月

目　录

第 1 章　网络安全概述

本章要点

- 网络安全的概念、现状分析
- 网络不安全的主要因素及其造成的主要威胁
- 网络信息安全特征与保护技术的简述
- 保护网络信息安全采用的技术机制
- 网络安全威胁及相应对抗技术的发展趋势

1.1　网络安全的重要性

安全性是互联网技术中最关键也最容易被忽视的问题。许多组织都建立了庞大的网络体系，但在多年的使用中从未考虑过安全问题，直到网络安全受到威胁，才不得不采取安全措施。随着计算机网络的广泛使用和网络之间数据传输量的急剧增长，网络安全的重要性愈加突出。

1994 年末，俄罗斯黑客弗拉基米尔·利文伙同朋友在圣彼得堡的一家小软件公司的联网计算机上，向美国花旗银行进行了一连串恶性攻击，以电子转账方式，从花旗银行在纽约的计算机主机里窃取了 180 万美元。

1996 年 8 月 17 日，美国司法部的网络服务器遭到黑客入侵，美国司法部主页被篡改，还留下大量攻击美国司法政策的文字，此事在当时成为轰动一时的新闻。

1996 年 2 月，刚开通不久的 Chinanet 网站就受到了攻击，且攻击得逞。1997 年初，北京某 ISP 运营商被黑客成功侵入，并在清华大学“水木清华”BBS 的“黑客与解密”论坛张贴如何免费通过该 ISP 进入 Internet 的文章。

据不完全统计，我国的网络安全问题近年来呈逐年上升趋势，1998 年公安部有关部门受理网络犯罪案件仅 80 多起，1999 年增至 400 多起，2000 年剧增为 2700 多起，2001 年增加到 4500 多起，比 2000 年上升约 70%，2002 年又上升到 6600 多起，而且仅 2003 年上半年就有 4800 多起，比同期上升 77.1%。

有关黑客威胁的报道已经屡见不鲜，而内部工作人员的疏忽甚至有意充当间谍对网络安全已构成更大的威胁。内部工作人员能较多地接触内部信息，工作中的任何大意都可能给信息安全带来威胁。无论是有意的攻击，还是无意的误操作，都会给系统带来不可估量的损失。虽然目前大多数的攻击者只是恶作剧似地使用篡改网站主页、拒绝服务等攻击，但当攻击者的技术达到某个层次后，他们就可以窃听网络上的信息，窃取用户密码、数据库等信息，还可以篡改数据库内容，伪造用户身份，否认自己的签名。更有甚者，可以删除数据库内容，摧毁网络结点，释放计算机病毒等。

综上所述，网络必须有足够强大的安全措施。无论是局域网还是广域网，无论是单位

还是个人，网络安全的目标是全方位地防范各种威胁以确保网络信息的保密性、完整性和可用性。

1.2　网络安全现状分析

20 世纪 90 年代初，英、法、德、荷 4 国针对传统的 TCSEC(Trusted Computer System Evaluation Criteria)准则只考虑保密性的局限性，联合提出了包括保密性、完整性、可用性概念的“信息技术安全评价准则 (nSFC) ”，但是该准则中并没有给出综合解决上述问题的理论模型和方案。近年来 6 国 7 方(美国国家安全局和国家技术标准研究所、加拿大、英国、法国、德国、荷兰)共同提出了“信息技术安全评价通用准则”，该准则综合了国际上已有的评审准则和技术标准的精华，给出了框架和原则要求。

然而，作为取代 TCSEC 用于系统安全评测的国际标准，它仍然缺少综合解决信息的多种安全属性的理论模型依据。更重要的是，他们的高安全级别的产品对我国是封锁禁售的。

作为信息安全的重要内容，安全协议的形式化方法分析始于 20 世纪 80 年代初，目前主要有基于状态机、模态逻辑和代数工具的 3 种分析方法，但仍有局限性和漏洞，处于发展提高阶段。

由于在广泛应用的因特网上，黑客入侵事件不断发生，不良信息在网上大量传播，所以网络安全监控管理理论和机制的研究就备受重视。黑客入侵手段的研究分析、系统脆弱性检测技术、报警技术、信息内容分级标识机制、智能化信息内容分析等研究成果已经成为众多安全工具软件的基础。

从已有的研究结果可以看出，现在的网络系统中存在着许多设计缺陷和情报机构有意埋伏的安全陷阱。例如在 CPU 芯片中，发达国家利用现有技术条件，可以加入无线发射接收功能，在操作系统、数据库管理系统或应用程序中能够预先安置从事情报搜集、受控激发的破坏程序。通过这些功能，可以接收特殊病毒；接收来自网络或空间的指令来触发 CPU 的自杀程序；搜集和发送敏感信息；通过特殊指令在加密操作中将部分明文隐藏在网络协议层中传输等。而且，通过唯一识别 CPU 的序列号，可以主动、准确地识别、跟踪或攻击一个使用该芯片的计算机系统，根据预先的设定搜集敏感信息或进行定向破坏。

作为信息安全关键技术的密码学近年来空前活跃。美、欧、亚各洲频繁举行密码学和信息安全学术会议。1976 年美国学者提出的公开密钥密码体制克服了网络信息系统密钥管理的困难，同时解决了数字签名问题，并可用于身份认证，它是当前研究的热点。目前处于研究和发展阶段的电子商务的安全性是人们普遍关注的焦点，它带动了认证理论、密钥管理等方面的研究。随着计算机运算速度的不断提高，各种密码算法面临着新的密码体制，如量子密码、DNA 密码、混沌理论等的挑战。1977 年美国颁布使用的国家数据加密标准越来越不能满足安全需要，美国正在征集 21 世纪使用的新数据加密标准。

我国信息安全研究经历了通信保密及计算机数据保护两个发展阶段，现正进入网络信息安全的研究阶段。虽然通过学习、吸收、消化 TCSEC 的原则进行了安全操作系统、多级安全数据库的研制，但由于系统安全内核受控于人，以及国外产品的不断更新升级，所以基于具体产品的增强安全功能的成果很难保证没有漏洞，也很难得到推广应用。现在虽然在学习借鉴国外技术的基础上，国内一些部门也开发研制了一些防火墙、安全路由器、安全

网关、黑客入侵检测、系统脆弱性扫描软件等，但是，这些产品安全技术的完善性、规范化和实用性还存在许多不足。特别是在多平台的兼容性、多协议的适应性、多接口的满足性方面与国际水平相比存在很大差距，而且，理论基础和自主的技术手段也需要发展和强化。

总的来说，我国的网络信息安全研究起步晚，与技术先进国家相比有差距，特别是在系统安全和安全协议方面的工作与国外差距较大。在我国研究和建立创新性安全理论及系列算法，仍是一项艰巨的任务。然而我国的网络信息安全研究已具备了一定的基础和条件，尤其是在密码学研究方面积累较多，基础较好，可以期待取得实质性进展。

1.3　网络不安全的主要因素

计算机网络安全的脆弱性是伴随计算机网络一同产生的，换句话说，安全脆弱是计算机网络与生俱来的致命弱点。在网络建设中，网络特性决定了不可能无条件、无限制地提高其安全性能。要使网络方便快捷，又要保证安全，这是一个非常棘手的“两难选择”，而网络安全只能在“两难选择”所允许的范围中寻找支撑点。因此，可以说任何一个计算机网络都不是绝对安全的。

1.3.1　互联网具有的不安全性

最初，互联网仅用于科研和学术组织内，它的技术基础存在不安全性。现在互联网是对全世界所有国家开放的网络，任何团体或个人都可以在网上方便地传送和获取各种各样的信息，具有开放性、国际性和自由性的特征，这就对网络安全提出了挑战。互联网的不安全性主要表现在如下方面。

(1) 网络互联技术是全开放的，使得网络所面临的破坏和攻击来自各方面。可能来自物理传输线路的攻击，也可能来自对网络通信协议的攻击，以及对软件和硬件设施的攻击。

(2) 网络的国际性意味着网络的攻击不仅来自本地网络的用户，而且可以来自互联网上的任何一台机器，也就是说，网络安全面临的是国际化的挑战。

(3) 网络的自由性意味着最初网络对用户的使用并没有提供任何的技术约束，用户可以自由地访问网络，自由地使用和发布各种类型的信息。

另外，互联网使用的基础协议 TCP/IP(传输控制协议/网际协议)，FTP(文件传送协议)、E-mail(电子邮件)、RPC(远程进程调用)，以及 NFS(网络文件系统)等不仅是公开的，而且都存在许多安全漏洞。

1.3.2　操作系统存在的安全问题

操作系统软件自身的不安全性，以及系统设计时的疏忽或考虑不周而留下的“破绽”，都给网络安全留下了许多隐患。

操作系统的体系结构造成的不安全性是计算机系统不安全的根本原因之一。操作系统的程序是可以动态链接的，例如：I/O 的驱动程序和系统服务，这些程序和服务可以通过打“补丁”的方式进行动态链接，许多 UNIX 操作系统的版本升级也都是采用打补丁的方式进行的。

这种动态链接的方法容易被黑客所利用，并且也是计算机病毒产生的环境。另外，操作系统的一些功能也会带来不安全因素，例如支持在网络上传输可以执行的文件映像、网络加载程序等。

操作系统不安全的另一原因在于它可以创建进程，支持进程的远程创建与激活，支持被创建的进程继承创建进程的权限，这些机制提供了在远端服务器上安装“间谍”软件的条件。若将间谍软件以打补丁的方式“打”在一个合法的用户上，尤其“打”在一个特权用户上，黑客或间谍软件就可以使系统进程与作业的监视程序都监测不到它的存在。

操作系统的无口令入口以及隐蔽通道(原是为系统开发人员提供的便捷入口)也是黑客入侵的通道。

1.3.3　数据的安全问题

在网络中，数据是存放在数据库中的，供不同的用户共享。然而，数据库存在许多不安全因素。例如：授权用户超出了访问权限进行数据的更改活动；非法用户绕过安全内核窃取信息资源等。对于数据库的安全而言，就是要保证数据的安全可靠和正确有效，即确保数据的安全性、完整性和并发控制。数据的安全性就是防止数据库被故意地破坏和非法地存取；数据的完整性是防止数据库中存在不符合语义的数据，以及防止由于错误信息的输入、输出而造成无效操作和错误结果；并发控制就是在多个用户程序并行存取数据时，保证数据库的一致性。

1.3.4　传输线路的安全问题

尽管在光缆、同轴电缆、微波、卫星通信中窃听其中指定一路的信息是很困难的，但是从安全的角度来说，没有绝对安全的通信线路。

1.3.5　网络安全管理问题

网络系统缺少安全管理人员，缺少安全管理的技术规范，缺少定期的安全测试与检查，缺少安全监控，是网络最大的安全问题之一。

1.4　网络安全的主要威胁

网络系统的安全威胁主要表现在主机可能会受到非法入侵者的攻击，网络中的敏感数据有可能泄露或被修改，从内部网向公共网传送的信息可能被他人窃听或篡改等。表 1-1 列出典型的网络安全威胁。

影响计算机网络安全的因素很多，如有意的或无意的、人为的或非人为的等，外来黑客对网络系统资源的非法使用更是影响计算机网络安全的重要因素。归结起来，网络安全的威胁主要有以下几个方面。

表 1-1　典型的网络安全威胁

威　　胁	描　　述
窃听	网络中传输的敏感信息被窃听
重传	攻击者事先获得部分或全部信息，以后将此信息发送给接收者
伪造	攻击者将伪造的信息发送给接收者
篡改	攻击者对合法用户之间的通信信息进行修改、删除、插入，再发送给接收者

续表

威　　胁	描　　述
非授权访问	通过假冒、身份攻击、系统漏洞等手段获取系统访问权，从而使非法用户进入网络系统读取、删除、修改、插入信息等
拒绝服务攻击	攻击者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
行为否认	通信实体否认已经发生的行为
旁路控制	攻击者发掘系统的缺陷或安全脆弱性
电磁/射频截获	攻击者从电子或机电设备所发出的无线射频或其他电磁辐射中提取信息
人员疏忽	已授权人为了利益或由于粗心将信息泄漏给未授权人

1.4.1　人为的疏忽

人为的疏忽包括：失误、失职、误操作等。例如操作员安全配置不当所造成的安全漏洞，用户安全意识不强，用户密码选择不慎，用户将自己的账户随意转借给他人或与他人共享等都会对网络安全构成威胁。

1.4.2　人为的恶意攻击

这是计算机网络所面临的最大威胁，敌人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。这两种攻击均对计算机网络造成极大的危害，并导致机密数据的泄漏。人为恶意攻击具有下述特性。

1. 智能性

从事恶意攻击的人员大都具有相当高的专业技术和熟练的操作技能。他们的文化程度高，在攻击前都经过了周密预谋和精心策划。

2. 严重性

涉及到金融资产的网络信息系统被恶意攻击，往往会由于资金损失巨大，而使金融机构、企业蒙受重大损失，甚至破产，同时也给社会稳定带来动荡。如美国资产融资公司计算机欺诈案涉及金额达亿美元之巨，犯罪影响惊动全美。在我国也发生过数起计算机盗窃案，金额从数万到数百万人民币不等，给相关部门带来了严重的损失。

3. 隐蔽性

人为恶意攻击的隐蔽性很强，不易引起怀疑，作案的技术难度大。一般情况下，其犯罪的证据存在于软件的数据和信息资料之中，若无专业知识很难获取侦破证据。而且作案人可以很容易地毁灭证据，计算机犯罪的现场也不像传统犯罪现场那样明显。

4. 多样性

随着计算机互联网的迅速发展，网络信息系统中的恶意攻击也随之发展变化。由于经济利益的强烈诱惑，近年来，各种恶意攻击主要集中于电子商务和电子金融领域。攻击手