面向21世纪高级应用型人才

中国高等职业技术教育研究会推荐

高职高专系列教材

网络安全技术

李卓玲 白雪峰 曲乐声 编著

胡建伟 主审

西安电子科技大学出版社

http://www.xduph.com

□ 中国高等职业技术教育研究会推荐

高职高专系列教材

网络安全技术

李卓玲　白雪峰　曲乐声　编著

胡建伟　主审

西安电子科技大学出版社

2004

内 容 简 介

随着网络应用的日益普及，网络安全防范的重要性和必要性也愈加突出。本书全面地介绍了计算机网络安全的基础知识，包括计算机网络安全的概念、网络安全机制、网络通信安全问题、操作系统的安全机制、密码技术和数据安全。同时，本书也介绍了网络安全实用技术，涉及到网络服务与应用安全、计算机网络病毒和防火墙技术、网络攻击及防范、主要网络设备的安全技术等网络安全知识与方法。本书旨在帮助计算机专业人员及相关专业人员了解计算机网络安全领域中相关方面的知识，建立安全意识，把握安全的衡量准则，对保证网络系统的安全具有实际的指导意义。

本书从实用的角度出发，内容详实，有章可循，行文流畅，讲解清晰，介绍全面，具有很强的可读性，必能让读者获益匪浅。各章配有适量的习题，特别是在可操作性的章节中还配有操作练习题。

本书可作为高职高专计算机专业及相关专业的教材，亦可作为计算机网络工程技术人员和网络管理人员的参考书。

★ 本书配有电子教案，需要的教师请与出版社联系，免费提供。

图书在版编目（CIP）数据

网络安全技术 / 李卓玲等编著.

—西安：西安电子科技大学出版社，2004.7

（高职高专系列教材）

ISBN 7-5606-1413-2

Ⅰ. 网… Ⅱ. 李… 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（2004）第 053168 号

策　　划　马武装

责任编辑　吴　奎　潘恩祥　马武装

出版发行　西安电子科技大学出版社(西安市太白南路 2 号)

电　　话　(029)88242885　88201467　　邮　编　710071

http: //www.xduph.com　　E-mail: xdupfxb@pub.xaonline.com

经　　销　新华书店

印刷单位　西安文化彩印厂

版　　次　2004 年 7 月第 1 版　2004 年 7 月第 1 次印刷

开　　本　787 毫米×1092 毫米　1/16　　印张　15.25

字　　数　354 千字

印　　数　1～4000 册

定　　价　17.00 元

ISBN 7-5606-1413-2/TP・0754(课)

XDUP 1684001-1

序

1999 年以来，随着高等教育大众化步伐的加快，高等职业教育呈现出快速发展的形势。党和国家高度重视高等职业教育的改革和发展，出台了一系列相关的法律、法规、文件等，规范、推动了高等职业教育健康有序的发展。同时，社会对高等职业技术教育的认识在不断加强，高等技术应用型人才及其培养的重要性也正在被越来越多的人所认同。目前，高等职业技术教育在学校数、招生数和毕业生数等方面均占据了高等教育的半壁江山，成为高等教育的重要组成部分，在我国社会主义现代化建设事业中发挥着极其重要的作用。

在高等职业教育大发展的同时，也有着许多亟待解决的问题。其中最主要的是按照高等职业教育培养目标的要求，培养一批具有“双师素质”的中青年骨干教师；编写出一批有特色的基础课和专业主干课教材；创建一批教学工作优秀学校、特色专业和实训基地。

为解决当前信息及机电类精品高职教材不足的问题，西安电子科技大学出版社与中国高等职业技术教育研究会分两轮联合策划、组织编写了“计算机、通信电子及机电类专业”系列高职高专教材共 100 余种。这些教材的选题是在全国范围内近 30 所高职高专院校中，对教学计划和课程设置进行充分调研的基础上策划产生的。教材的编写采取公开招标的形式，以吸收尽可能多的优秀作者参与投标和编写。在此基础上，召开系列教材专家编委会，评审教材编写大纲，并对中标大纲提出修改、完善意见，确定主编、主审人选。该系列教材着力把握高职高专“重在技术能力培养”的原则，结合目标定位，注重在新颖性、实用性、可读性三个方面能有所突破，体现高职教材的特点。第一轮教材共 36 种，已于 2001 年全部出齐，从使用情况看，比较适合高等职业院校的需要，普遍受到各学校的欢迎，一再重印，其中《互联网实用技术与网页制作》在短短两年多的时间里先后重印 6 次，并获教育部 2002 年普通高校优秀教材二等奖。第二轮教材预计在 2004 年全部出齐。

教材建设是高等职业院校基本建设的主要工作之一，是教学内容改革的重要基础。为此，有关高职院校都十分重视教材建设，组织教师积极参加教材编写，为高职教材从无到有，从有到优、到特而辛勤工作。但高职教材的建设起步时间不长，还需要做艰苦的工作，我们殷切地希望广大从事高等职业教育的教师，在教书育人的同时，组织起来，共同努力，编写出一批高职教材的精品，为推出一批有特色的、高质量的高职教材作出积极的贡献。

中国高等职业技术教育研究会会长 李宗尧

IT类专业系列高职高专教材编审专家委员会名单

主　任：高　林　（北京联合大学副校长，教授）

副主任：温希东　（深圳职业技术学院电子通信工程系主任，教授）

李卓玲　（沈阳电力高等专科学校信息工程系主任，教授）

李荣才　（西安电子科技大学出版社总编辑，教授）

计算机组：组长：李卓玲(兼)　（成员按姓氏笔画排列）

丁桂芝　（天津职业大学计算机工程系主任，教授）

王海春　（成都航空职业技术学院电子工程系副教授）

文益民　（湖南工业职业技术学院信息工程系主任，副教授）

朱乃立　（洛阳大学电子工程系主任，教授）

李　虹　（南京工业职业技术学院电气工程系副教授）

陈　晴　（武汉职业技术学院计算机科学系主任，副教授）

范剑波　（宁波高等专科学校电子技术工程系副主任，副教授）

陶　霖　（上海第二工业大学计算机学院教授）

徐人凤　（深圳职业技术学院计算机应用工程系副主任，高工）

章海鸥　（金陵科技学院计算机系副教授）

鲍有文　（北京联合大学信息学院副院长，副教授）

电子通信组：组长：温希东(兼)　（成员按姓氏笔画排列）

马晓明　（深圳职业技术学院电子通信工程系副主任，副教授）

于　冰　（宁波高等专科学校电子技术工程系副教授）

孙建京　（北京联合大学教务长，教授）

苏家健　（上海第二工业大学电子电气工程学院副院长，高工）

狄建雄　（南京工业职业技术学院电气工程系主任，副教授）

陈　方　（湖南工业职业技术学院电气工程系主任，副教授）

李建月　（洛阳大学电子工程系副主任，副教授）

李　川　（沈阳电力高等专科学校自动控制系副教授）

林训超　（成都航空职业技术学院电子工程系主任，副教授）

姚建永　（武汉职业技术学院电子信息系主任，副教授）

韩伟忠　（金陵科技学院龙蟠学院院长，高工）

项目总策划：梁家新

项目策划：马乐惠　云立实　马武装　马晓娟

电子教案：马武装

前　言

随着计算机网络技术的迅猛发展，网络已经影响到社会生活的各个方面，给现代人类生活带来了深远的影响。当网络为整个社会带来了巨大的推动与冲击的同时，也给信息安全工作带来了极大的挑战。计算机网络犯罪事件已屡见不鲜，且呈上升趋势。随着网络上电子商务、电子现金、数字货币和网络银行等业务的兴起以及各种专用网(如金融网)的建设，网络和信息系统的安全与保密工作也就显得越来越重要。

网络安全是一个综合、交叉的学科领域。它要利用数学、电子、信息、通信、计算机等诸多学科的长期积累的知识和最新发展成果。本书将计算机网络安全的理论与实践相结合，讲解中注意实例的介绍，使读者能真正做到学以致用。

本书的参考教学时数为 50 学时，其中上机实践参考教学时数为 20 学时。本书第 1 章介绍了计算机网络安全技术概论，第 2 章介绍了网络通信安全，第 3 章介绍了操作系统安全，第 4 章介绍了网络服务与应用系统的安全，第 5 章介绍了计算机网络病毒及其防范，第 6 章介绍了网络攻击及防范措施，第 7 章介绍了防火墙技术，第 8 章介绍了网络设备安全技术，第 9 章介绍了密码技术，第 10 章介绍了数据安全。

本教材编写分工为：李卓玲负责了全书的规划和统稿，包括各章节的详细设计；白雪峰编写了第 1、4、6、7、8 章；曲乐声编写了第 2、3、5、9、10 章。编者借本书出版之际，向所有为此书作出贡献的同志们表示感谢！

由于编者的水平和学识有限，加上时间仓促，疏漏甚至错误之处在所难免，恳请广大读者不吝指正。

编　者

2004 年 3 月

目　录

第 1 章　计算机网络安全技术概论

[本章的学习目标]

- 掌握计算机网络安全的定义和特征
- 掌握计算机网络面临的安全威胁、采用的安全机制和网络安全的设计原则
- 了解产生计算机网络安全威胁的原因和计算机网络安全的评价标准

计算机网络的作用从初期的信息传送和交换，扩展到信息的查询、共享和电子商务等，在人们的工作与生活中起着越来越重要的作用。随着计算机网络技术的高速发展和网络作用的扩大，计算机网络安全问题越来越受到人们的关注，也要求网络具有更高的安全性，相应的安全防御工作的难度也变得越来越大。网络安全问题已成为当今网络技术的一个重要研究课题。

在计算机网络上出现过非常多的安全性问题，这些问题源于计算机网络的开放性、自身缺陷和黑客的攻击。虽然计算机网络不是一个安全性非常高的系统，但是只要正确地使用计算机网络，也是可以保证它的安全的。

1.1　计算机网络安全简介

网络安全涉及的内容既有技术方面的问题，又有管理方面的问题，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。除传统的安全保密理论、技术及单机安全问题外，计算机网络安全包括计算机安全、通信安全、操作安全、控制安全、实体安全、电磁安全、系统平台与网络站点的安全，以及安全管理和法律制裁等诸多内容，这些内容结合，逐渐形成了独立的学科体系。如何更有效地保护重要信息和数据、提高计算机网络系统的安全性已经成为所有计算机网络应用必须考虑和解决的一个重要问题。

1.1.1　计算机网络安全定义

计算机网络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，不因偶然的或者恶意的原因而遭到破坏、更改、泄露，确保系统能连续、可靠、正常地运行，使网络服务不中断。网络安全从本质上讲就是网络上信息的安全。

从狭义的保护角度来说，计算机网络安全是指计算机及其网络系统资源及信息资源不受自然和人为有害因素的威胁与危害。从广义来说，凡是涉及到计算机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理论都是计算机网络安全研究的领域。广义的计算机网络安全还包括信息设备的物理安全，如场地环境保护、防盗措施、防火措

施、防雷击措施、防水措施、防静电措施、电源保护、空调设备、计算机及网络设备的辐射和计算机病毒等。

网络安全是一门涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论和信息论等多种学科的综合性学科。

1.1.2 计算机网络安全的特征

计算机网络安全应具有以下四个方面的特征。

1. 保密性

保密性是指信息不泄漏给非授权的用户、实体或过程，或供其利用的特性。即防止信息泄漏给非授权个人或实体，信息只为授权用户使用。

2. 完整性

完整性是指数据未经授权不能进行改变，信息的存储或传输过程中保持不被修改、不被破坏和丢失的特征。完整性是一种面向信息的安全性，它要求保持信息的原样，即信息的正确生成和正确存储与传输。

3. 可用性

可用性是指可被授权实体访问并按需求使用的特性。即网络信息服务在需要时，允许授权用户或实体使用的特性，或者是网络部分受损或需要降级使用时，仍能为授权用户提供有效服务的特性。

4. 可控性

可控性是指对信息的传播及信息的内容具有控制能力。

1.1.3 网络安全的结构层次

网络安全的结构层次主要包括：物理安全、安全控制和安全服务。

1. 物理安全

物理安全是指在物理介质层次上对存储和传输的网络信息的安全保护。也就是保护计算机网络设备、设施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过程。物理安全是网络信息安全的最基本保障，是整个安全系统不可缺少和忽视的组成部分。它主要包括以下三个方面的内容：

1) 环境安全

环境安全是指对系统所在环境的安全保护，如区域保护和灾难保护。关于环境安全国家制定了一系列的国家标准。比如，GB 50173—93《电子计算机机房设计规范》、GB 2887—89《计算站场地技术条件》和 GB 9361—88《计算站场地安全要求》等。

2) 设备安全

设备安全主要包括设备的防盗、防毁、防电磁信息辐射泄漏、防止线路截获、抗电磁干扰及电源保护等。

3) 媒体安全

媒体安全包括媒体数据的安全及媒体本身的安全。

2. 安全控制

安全控制是指在网络信息系统中对存储和传输的信息操作及进程进行控制与管理，重点是在网络信息处理层次上对信息进行初步的安全保护。安全控制可以分为以下三个层次。

1) 操作系统的安全控制

操作系统的安全控制包括对用户的合法身份进行核实(比如，开机时要求键入口令)、对文件的读写存取的控制(比如，文件属性控制机制)等。此类安全控制主要保护被存储数据的安全。

2) 网络接口模块的安全控制

网络接口模块的安全控制是指在网络环境下对来自其他机器的网络通信进程进行安全控制，主要包括身份认证、客户权限设置与判别以及审计日志等。

3) 网络互联设备的安全控制

网络互联设备的安全控制是指对整个子网内的所有主机的传输信息和运行状态进行安全监测与控制，主要通过网管软件或路由器配置实现。

安全控制主要通过现有的操作系统或网管软件、路由器配置等实现。安全控制只提供了初步的安全功能和网络信息保护。

3. 安全服务

安全服务是指在应用程序层对网络信息的保密性、完整性和信源的真实性进行保护及鉴别，满足用户的安全需求，防止并抵御各种安全威胁和攻击手段。安全服务可以在一定程度上弥补和完善现有操作系统及网络信息系统的安全漏洞。安全服务的主要内容包括安全机制、安全连接、安全协议和安全策略等。

1) 安全机制

安全机制是利用密码算法对重要而敏感的数据进行处理的机制。比如，以保护网络信息的保密性为目标的数据加密和解密；以保证网络信息来源的真实性和合法性为目标的数字签名与签名验证；以保护网络信息的完整性，防止和检测数据被修改、插入、删除以及改变的信息认证等。安全机制是安全服务乃至整个网络信息安全系统的核心和关键。现代密码学在安全机制的设计中扮演着重要的角色。

2) 安全连接

安全连接是在安全处理前与网络通信方之间的连接过程。安全连接为安全处理进行了必要的准备工作。安全连接主要包括会话密钥的分配、生成和身份验证。后者旨在保护信息处理和操作的对等双方的身份真实性与合法性。

3) 安全协议

安全协议是使网络环境下互不信任的通信方能够相互配合，并通过安全连接和安全机制的实现来保证通信过程的安全性、可靠性和公平性的协议。

4) 安全策略

安全策略是安全体制、安全连接和安全协议的有机组合方式，是网络信息系统安全性的完整的解决方案。安全策略决定了网络信息安全系统的整体安全性和实用性。不同的网

络信息系统和不同的应用环境需要不同的安全策略。

1.1.4 对待计算机网络安全问题的态度

一般对待计算机网络安全问题通常有两种不同的态度。

第一种是保守的态度。这种态度认为将安全问题隐藏起来才是最好的解决办法。表面上看，隐藏就可以避免网络安全问题，但是不能证明不会被人发现安全漏洞，也不能阻止掌握了这种漏洞的人去利用这些网络安全问题。目前有些软件采用了这种态度，事实上这些安全性比较低的软件在攻击者或网络安全专家面前，漏洞就很容易被发现。

第二种是比较积极的态度。这种态度认为网络安全问题不应该隐藏，只有不断地去发现和解决这些安全问题，才能让计算机网络系统变得更安全。这种态度可以让用户知道哪些是安全的，哪些是存在问题的。对于存在安全问题的事务应该及时发现，并及时进行修补。如果一个系统经受住众多使用者的考验，那么开发者和使用者就不用担心严重的安全问题了。

对于计算机网络安全问题，应该采用比较积极的态度，不断地学习与研究，及时获取网络安全的新技术，修补网络安全上的漏洞，保障网络的安全。事实上，很多网络安全问题是因为网络管理员没有及时地弥补安全漏洞而导致的。

1.2 计算机网络安全面临的威胁

计算机网络所面临的威胁包括针对网络中信息的威胁和针对网络中设备的威胁。

1.2.1 计算机网络安全威胁的来源

影响计算机网络安全的因素很多，有些因素可能是有意的，也可能是无意的；可能是天灾，也可能是人为的。计算机网络安全威胁的来源主要有三个。

1. 天灾

天灾是指不可控制的自然灾害，如雷击、地震等。天灾轻则造成正常的业务工作混乱，重则造成系统中断和无法估量的损失。

2. 人为因素

人为因素可分为有意和无意两种类型。

人为的无意失误和各种各样的误操作都可能造成严重的不良后果。如文件的误删除、输入错误的数据、操作员安全配置不当；用户的口令选择不慎，口令保护得不好；用户将自己的账号随意借给他人或与别人共享等都可能会对计算机网络带来威胁。

有意因素是指人为的恶意攻击、违纪、违法和犯罪，它是计算机网络面临的最大威胁。人为的恶意攻击又可分为两种：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；另一种是被动攻击，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，将导致机密数据的泄露。

人为的威胁往往是由于系统资源和管理中的薄弱环节被威胁源(入侵者或其入侵程序)利用而产生的。

3. 系统本身原因

1) 计算机硬件系统及网络设备的故障

由于设计、生产工艺、制造、设备运行环境等原因，计算机硬件系统及网络设备会出现故障。如电路短路、断路、接触不良、器件老化和电压的波动干扰等引起的网络系统不稳定。

2) 软件的漏洞

软件不可能百分之百的无缺陷和漏洞，软件系统越庞大，出现漏洞和缺陷的可能性也越大。这些漏洞和缺陷就成了攻击者的首选目标。

3) 软件的“后门”

软件的“后门”是软件公司的程序设计人员为了方便而在开发时预留设置的。这些“后门”一般不为外人所知，但是一旦“后门洞开”，其造成的后果将不堪设想。

1.2.2 威胁的具体表现形式

威胁具体表现为物理威胁、系统漏洞造成的威胁、鉴别威胁、线缆连接威胁、有害程序威胁和管理上的威胁等六种形式。

1. 物理威胁

1) 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。如果偷窃者想偷的信息在计算机里，那他们一方面可以将整台计算机偷走，另一方面可以读取、复制计算机中的信息。

2) 恶劣的运行环境

恶劣的运行环境是指计算机网络系统的运行环境不符合标准，主要包括防火、防水、防雷击、防静电、电源保护、环境温度、环境湿度和抗电磁干扰等不符合安全技术要求。恶劣的运行环境可能加速设备的老化，造成设备的损坏、信息的错误或丢失。

3) 废物搜寻

废物搜寻是指在废物(如打印出来的材料或废弃的软盘、光盘)中搜寻所需要的信息。废物搜寻可能包括未从安全角度彻底删除信息的软盘或硬盘上获得有用资料。

4) 间谍行为

间谍行为是一种以获取有价值的机密信息为目的，采用不道德的、不合法的行为盗取信息的过程。

5) 身份识别错误

身份识别错误是指非法建立文件或记录，企图把它们作为有效的、正式生产的文件或记录。如对具有身份鉴别特征物品(如加密的安全卡、护照、执照等)进行伪造就属于身份识别发生错误的范畴。

2. 系统漏洞造成的威胁

1) 乘虚而入

例如，用户 A 停止了与某个系统的通信，但由于某种原因仍使该系统上的一个端口处于激活状态，这时，用户 B 通过这个端口开始与这个系统通信，这样就不必通过任何申请

使用端口的安全检查了。

2) 不安全服务

操作系统的一些服务程序有时可以绕过机器的安全系统，成为不安全服务。比如，互联网蠕虫就是利用了一些操作系统中的可绕过机器进行攻击的。

3) 配置和初始化

当关掉一台服务器以维修它的某个系统时，在重新启动服务器后，可能会有些用户说他们的文件丢失了或被篡改了，这就有可能是在系统重新初始化时，安全系统没有被正确地初始化，从而留下了安全漏洞让人利用。

3. 鉴别威胁

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。常见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，它一般被插入到正常的登录过程之前。最终用户看到的将是先后两个登录屏幕，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，第一次登录并没有失败，它将登录数据(如用户名和口令)写入某个数据文件中，留待使用，第二次登录屏幕才是正常的登录屏幕。

2) 口令破解

口令破解这种威胁主要是由于用户口令设置比较简单造成的。破解口令就像是猜测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。比如在计算密码的程序中使用多线程、密码字典等。一般比较安全的口令应该在六位以上，包括字母、数字、符号等。网络上已经出现了针对使用比较简单口令的操作系统进行口令破解、攻击的网络蠕虫病毒。

3) 算法考虑不周全

一般来说，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来实现。在一些入侵案例中，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

编辑口令一般需要依靠内部漏洞，如某单位内部的人建立了一个虚设的账户或修改了一个隐含账户的口令，这样，任何知道那个账户的用户名和口令的人便可以访问该机器了。

4. 线缆连接威胁

1) 窃听

对通信过程进行窃听可达到收集信息的目的，这种电子窃听可以将窃听设备安装在通信线缆上，也可以通过检测从连线上发射出来的电磁辐射来拾取所要的信号。

2) 拨号进入

拥有一个调制解调器和一个电话号码，每个人都可以通过拨号远程访问网络，但当别有用心的人拥有所期望攻击的网络的用户账户时，就会对网络造成很大的威胁。

3) 冒名顶替

冒名顶替是指通过使用别人的密码和账号，获得对网络及其数据、程序的使用能力。

5. 有害程序威胁

1) 计算机病毒

计算机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，病毒可以进行自我复制，并随着它所附着的程序在机器之间传播。

2) 代码炸弹

代码炸弹是一种具有杀伤力的代码，其原理是在到达设定的时间，通过网络向被攻击者发送特定代码或在机器中发生了某种操作时，代码炸弹就被触发并开始产生破坏性操作。代码炸弹不像病毒那样四处传播，一般是程序员有意或无意造成的软件安全漏洞。

3) 特洛伊木马

特洛伊木马程序一旦被安装到机器上，便可按编制者的意图行事。特洛伊木马有的伪装成系统上已有的程序，有的创建新的用户名和口令，有的窃取用户信息，甚至破坏数据。

4) 更新或下载

有些网络系统允许通过网络进行固件和操作系统更新，于是非法闯入者便可以通过这种更新方法，对系统进行非法更新。

6. 管理上的威胁

管理上的威胁主要来自单位的内部，但对网络安全的威胁非常大，这方面的威胁单靠计算机和网络技术是无法解决的。

1) 规章制度不健全

规章制度不健全会造成人为泄密事故。如网络方面的规章制度不严，出现网络安全问题不能及时响应、及时处理，对机密文件管理不善，文件存放混乱和违章操作等。

2) 网络管理员自身问题

网络管理员自身问题包括保密观念不强，不懂保密规则，不遵守规章制度，随便泄密；业务不熟练，不能及时发现并修补网络上的安全漏洞；操作失误造成信息出错、误发；素质不高，缺乏责任心，没有良好的工作态度，明知故犯甚至有意破坏网络系统和设备等。

1.3　计算机网络出现安全威胁的原因

即使有着良好安全措施的网络也会面临着网络安全方面的威胁。计算机网络的安全威胁主要表现在操作系统、网络系统和数据库管理系统等九个方面。

1. 操作系统的原因

操作系统不安全是计算机网络不安全的根本原因，目前流行的许多操作系统均存在网络安全漏洞。操作系统不安全主要表现为以下七个方面。

(1) 操作系统结构体制本身的缺陷。操作系统的程序是可以动态连接的。I/O 的驱动程序与系统服务都可以用打补丁的方式进行动态连接，有些操作系统的版本升级采用打补丁的方式进行。虽然这些操作需要被授予特权，但这种方法厂商可用，黑客也可用。操作系统支持程序动态连接与数据动态交换是现代系统集成和系统扩展的需要，这显然与安全有矛盾。

(2) 创建进程也存在着不安全因素。进程可以在网络的节点上被远程创建和激活，更为

重要的是被创建的进程还可继承创建进程的权利。这样可以在网络上传输可执行程序，再加上远程调用的功能，就可以在远端服务器上安装“间谍”软件。另外，还可以把这种间谍软件以打补丁的方式加在一个合法用户上，尤其是一个特权用户上，以便使系统进程与作业监视程序都看不到间谍软件的存在。

(3) 操作系统中，通常都有一些守护进程，这种软件实际上是一些系统进程，它们总是在等待一些条件的出现，一旦这些条件出现，程序便继续运行下去，这些软件常常被黑客利用。这些守护进程在 UNIX、Windows 2000 操作系统中具有与其他操作系统核心层软件同等的权限。

(4) 操作系统提供的一些功能也会带来一些不安全因素。例如，支持在网络上传输文件、在网络上加载与安装程序，包括可以执行文件的功能；操作系统的 debug 和 wizard 功能。许多精通于 patch 和 debug 工具的黑客利用这些工具几乎可以做成想做的所有事情。

(5) 操作系统自身提供的网络服务不安全。如操作系统都提供远程过程调用(Remote Processor Cal—RPC)服务，而提供的安全验证功能却很有限；操作系统提供网络文件系统(Network Files System—NFS)服务，NFS 系统是一个基于 RPC 的网络文件系统，如果 NFS 设置存在重大问题，则几乎等于将系统管理权拱手交出。

(6) 操作系统安排的无口令入口，是为系统开发人员提供的便捷入口，但这些入口也可能被黑客利用。

(7) 操作系统还有隐蔽的信道，存在着潜在的危险。

尽管操作系统的缺陷可以通过版本的不断升级来克服，但系统的某一个安全漏洞就会使系统的所有安全控制毫无价值。

2. 网络系统的原因

随着 Internet/Intranet 的发展，TCP/IP 协议被广泛地应用到各种网络中，但采用的 TCP/IP 协议族软件本身缺乏安全性，使用 TCP/IP 协议的网络所提供的 FTP、E-mail、RPC 和 NFS 都包含许多不安全的因素，存在着许多漏洞。

网络的普及使信息共享达到了一个新的层次，信息被暴露的机会大大增多。特别是 Internet 网络是一个开放的系统，通过未受保护的外部环境和线路可能访问系统内部，发生随时搭线窃听、远程监控和攻击破坏等事件。另外，数据处理的可访问性和资源共享的目的性之间是矛盾的，它造成了计算机系统保密性难，拷贝数据信息很容易且不留任何痕迹。如一台远程终端上的用户可以通过 Internet 连接其他任何一个站点，在一定条件下可以随意进行拷贝、删改乃至破坏该站点的资源。

3. 数据库管理系统的原因

大量的信息存储在各种各样的数据库中，然而，有些数据库系统在安全方面考虑很少。数据库管理系统的安全必须与操作系统的安全相配套。例如，数据库管理系统的安全级别是 B2 级，那么操作系统的安全级别也应该是 B2 级，但实践中往往不是这样做的。

4. 防火墙的局限性

利用防火墙可以保护计算机网络免受外部黑客的攻击，但它只是能够提高网络的安全性，不可能保证网络绝对安全。事实上仍然存在着一些防火墙不能防范的安全威胁，甚至