高等学校**应用型特色**规划教材

计算机网络信息安全

刘永华 主 编
陈 茜 张淑玉 周金玲 副主编

赠 送
电子教案

清华大学出版社

高等学校应用型特色规划教材

计算机网络信息安全

刘永华　主　编

陈茜　张淑玉　周金玲　副主编

清华大学出版社
北京

内 容 简 介

本书的内容涵盖了计算机网络安全和管理的基本概念、原理和技术，全书共分为 10 章。主要内容包括计算机网络安全概述、数据加密与认证技术、操作系统安全技术、数据库与数据安全技术、计算机病毒防治技术、防火墙技术、入侵检测技术、VPN 与 NAT 技术及安全协议、计算机网络管理与维护技术、网络信息安全系统设计案例等内容。本书内容全面，取材新颖，既有网络安全和管理的理论知识，又有应用案例和实用技术，反映了计算机网络信息安全技术的最新发展。

本书可作为普通高等教育和成人高等教育计算机科学与技术、网络工程、软件工程、通信工程、自动化及相关专业本科教材使用，也可作为高职高专计算机网络安全技术教材使用，同时也是广大工程技术人员较好的科技参考书。

图书在版编目(CIP)数据

计算机网络信息安全/刘永华主编. --北京：清华大学出版社，2014
(高等学校应用型特色规划教材)
ISBN 978-7-302-35623-3

Ⅰ. ①计… Ⅱ. ①刘… Ⅲ. ①计算机网络—信息安全—高等学校—教材 Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字(2014)第 046701 号

责任编辑：桑任松
封面设计：杨玉兰
责任校对：周剑云
责任印制：何　芊

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦 A 座　　邮　　编：100084
社 总 机：010-62770175　　邮　　购：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质 量 反 馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
课 件 下 载：http://www.tup.com.cn,010-62791865

印 刷 者：北京富博印刷有限公司
装 订 者：北京市密云县京文制本装订厂
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　张**：19.75　　**字　数**：477 千字
版　　次：2014 年 7 月第 1 版　　**印　次**：2014 年 7 月第1 次印刷
印　　数：1～3000
定　　价：36.00 元

产品编号：050543-01

前　言

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受到破坏、更改、泄露，系统连续可靠地运行，网络服务不中断。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、信息论等多种学科的综合性学科。随着计算机网络技术的发展，网络的安全问题越来越受到关注，网络安全已超越其本身而达到国家安全的高度。

本书在介绍网络安全理论及其基础知识的同时，突出计算机网络安全方面的管理、配置及维护的实际操作手法和手段，并尽量跟踪网络安全技术的最新成果与发展方向，结合网络安全系统案例精心阐述。全书主要内容包括网络安全的基本概念、数据加密与认证技术、操作系统的安全与保护措施、数据库与数据安全、防火墙技术、黑客技术与防范措施、网络病毒技术、VPN 技术与安全协议、网络管理与维护技术、Internet/Intranet 的安全性、网络信息安全系统案例等。

全书共分为 10 章，各章内容安排如下。

第 1 章具体介绍计算机网络安全的相关基础知识，包括网络安全的概念及影响网络安全的主要因素，网络安全的组成以及网络安全常用的技术；第 2 章介绍网络安全中数据加密与认证技术，包括传统的加密方法、DES 加密标准、公开密钥体制和数字签名等技术；第 3 章主要介绍操作系统安全技术，包括 Windows 和 Linux 操作系统的安全机制、安全漏洞和安全配置方案；第 4 章介绍数据库与数据安全技术，数据库的安全特性、数据库的安全、保护数据的完整性、数据备份和恢复、网络备份、系统数据容灾等；第 5 章主要介绍病毒的原理、病毒的类型和计算机网络病毒，同时介绍了几种影响较大的网络病毒，并且介绍了病毒的清除及防护措施；第 6 章介绍访问控制技术中的防火墙的技术，包括防火墙的原理、种类和实现策略等；第 7 章主要介绍对入侵检测的概念和相关技术进行了全面介绍，并对入侵检测的未来发展进行了讨论；第 8 章主要介绍了 VPN 与 NAT 技术及安全协议，涉及 VPN 的原理与设置、NAT 的工作工程，以及网络安全的几个主要协议；第 9 章主要介绍计算机网络管理和维护技术。主要包括网络管理的基本概念、网络管理协议、网络管理工具和网络维护方法。介绍 Windows 自带的常用网络工具，讨论了网卡、集线器、交换机、路由器、网线和 RJ-45 接头等网络连接设备的维护，网络的性能优化等问题，重点介绍了常用网络故障及排除方法；第 10 章主要介绍网络信息安全系统设计案例。涉及需求分析、工程论证、总体设计与实体设计等内容。

由于网络安全的内容非常丰富，本书按理论教学以“必需、够用”为度，加强实践性环节教学，提高学生的实际技能的原则组织编写。讲究知识性、系统性、条理性、连贯性。力求激发学生兴趣，注重提示各知识之间的内在联系，精心组织内容，做到由浅入深，由易到难，删繁就简，突出重点，循序渐进。本书既注重网络安全基础理论，又着眼培养读者解决网络安全问题的能力。

本书的特点是文字简明、图表准确、通俗易懂，用循序渐进的方式叙述网络安全知识，对计算机网络安全的原理和技术难点的介绍适度，内容安排合理，逻辑性强，重点介绍网

络安全的概念、技术和应用，在内容上将理论知识和实际应用紧密地结合在一起。本书共10章，适用于48学时左右的课堂教学。通过对本书的学习，可使读者较全面地了解网络系统安全的基本概念、网络安全技术和应用，培养读者解决网络安全问题的能力。

本书可作为普通高等教育和成人高等教育计算机科学与技术、网络工程、软件工程、通信工程、自动化及相关专业本科教材使用，也可作为高职高专计算机网络安全技术教材使用，同时也是广大工程技术人员较好的科技参考书。

本书由刘永华担任主编并完成全书的通稿整理，陈茜、张淑玉、周金玲担任副主编。其中第1～7章由刘永华编写，第8章由陈茜编写，第9章由张淑玉编写，第10章由董春平编写。孟凡楼、孙俊香、赵艳杰、解圣庆、周建梁、张宗云对本书的编写提供了帮助，在此向他们表示感谢。

由于作者水平有限，加之编写时间仓促，书中难免有疏漏和不足之处，恳请广大读者和同行批评指正。

编　者

目　录

第 1 章　计算机网络安全概述

学习目标

系统学习网络安全的概念，网络安全的现状，网络面临的主要威胁，影响网络安全的因素，保证网络安全的技术。通过本章的学习，读者应掌握及了解以下内容。

- 掌握网络安全的概念，网络安全的基本技术。
- 了解网络的安全威胁，影响网络安全的主要因素。

1.1　计算机网络安全简介

随着信息技术的迅速发展，网络已成为重要的信息传播工具。而随着互联网的飞速发展，网络安全问题也越来越受到广泛的关注，各种病毒花样繁多、层出不穷，系统、程序、软件的安全漏洞越来越多，黑客们常通过不正当手段侵入他人计算机，非法获得用户信息资料，给正常使用互联网的用户带来不可估计的损失。因此，网络安全越来越引起人们的重视。

1.1.1　网络安全的概念

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。计算机网络信息安全技术经过 10 多年的发展，在信息安全技术的研究基础上形成了两个完全不同的角度和方向：一个从正面防御角度考虑，研究加密、鉴别、认证、授权和访问控制等；另一个从反面攻击角度考虑，研究漏洞的扫描评估、入侵检测、紧急响应和病毒预防。网络安全从其本质上来讲就是网络上的信息安全。它涉及的领域相当广泛，这是因为在目前的公用通信网络中存在着各种各样的安全漏洞和威胁。下面给出网络安全的一个通用定义。

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，系统能连续、可靠正常地运行，使网络服务不中断。

广义来说，凡是涉及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，两者相互补充，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。

网络安全要考虑以下几个方面的内容。

1. 网络系统的安全

网络系统的安全主要包括以下几方面的问题。

(1) 网络操作系统的安全性。目前流行的操作系统(UNIX、Windows 2000/ NT/XP 等)

均存在网络安全漏洞。

(2) 来自外部的安全威胁。

(3) 来自内部用户的安全威胁。

(4) 通信协议软件本身缺乏安全性(如 TCP/IP 协议)。

(5) 计算机病毒感染。

(6) 应用服务的安全。许多应用服务系统在访问控制及安全通信方面考虑不周全。

2. 局域网安全

局域网采用广播方式，在同一个广播域中可以侦听到在该局域网上传输的所有信息包，这是一个不安全的因素。

3. Internet 互联安全

非授权访问、冒充合法用户、破坏数据完整性、干扰系统正常运行、利用网络传播病毒等都是在 Internet 上经常遇到的问题。

4. 数据安全

事实上，无论 Internet 还是其他专用网络，都必须注意数据的安全性问题，以保护本单位、本部门的信息资源不会受到外来的侵害。

从根本意义上讲，绝对安全的计算机是根本不存在的，绝对安全的网络也是不可能有的。只有存放在一个无人知晓的密室里，而又不通电的计算机才可以称得上安全。计算机只要投入使用，就或多或少地存在着安全问题，只是程度不同而已。因此，在探讨网络安全的时候，实际上指的是一定程度上的网络安全。而到底需要多大的安全性，要依据实际需要及自身能力而定。网络安全性越高，也就意味着网络的管理越复杂。网络的安全性与网络管理便利性是一对矛盾。

1.1.2 网络安全模型

典型的网络安全模型如图 1.1 所示。信息需要从一方通过网络传送到另一方。在传送中居主体地位的双方必须相互合作以便进行交换。通过通信协议(如 TCP/IP)在两个主体之间可以建立一条逻辑信息通道。

为防止对手对信息机密性、可靠性等造成破坏，需要保护传送的信息。保证安全性的所有机制包括以下两部分。

(1) 对被传送的信息进行与安全相关的转换。图 1.1 中包含了加密消息和以消息内容为基础的补充代码。加密消息使对手无法阅读，补充代码可以用来验证发送方的身份。

(2) 两个主体共享不希望对手得知的保密信息。例如，使用密钥链接，在发送前对信息进行转换，在接收后再转换回来。

为了实现安全传送，可能需要可信任的第三方。例如，第三方可能会负责向两个主体分发保密信息，而向其他对手保密，或者需要第三方对两个主体间传送信息可靠性的争端进行仲裁。

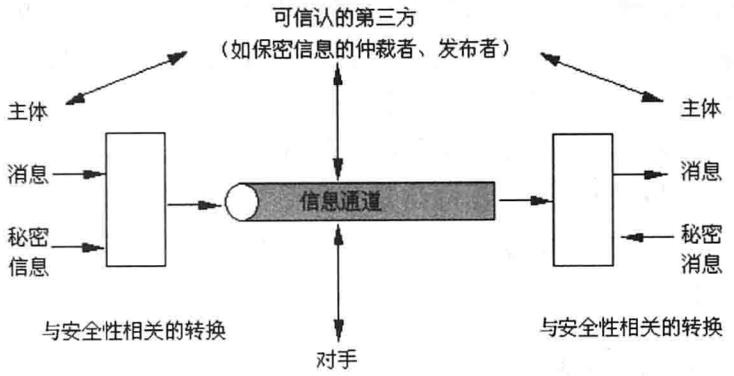

图 1.1　网络安全模型

这种通用模型指出了设计特定安全服务的 4 个基本任务。

(1) 设计执行与安全性相关的转换算法，该算法必须使对手不能对算法进行破解以实现其目的。

(2) 生成算法使用的保密信息。

(3) 开发分发和共享保密信息的方法。

(4) 指定两个主体要使用的协议，并利用安全算法和保密信息来实现特定的安全服务。

1.1.3　计算机安全的分级

计算机操作系统的安全级别在美国国防部发表的橘皮书——《可信计算机系统评测标准》中，把计算机系统分为 4 个等级、7 个级别，即 D(最低保护等级)、C(自主保护等级)、B(强制保护等级)、A(验证保护等级)4 等，细分为 D、C1、C2、B1、B2、B3、A1 等 7 级。

- D 级。计算机安全的最低一级，不要求用户进行登录和密码保护，任何人都可以使用，整个系统是不可信任的，硬件和软件都易被他人侵袭。
- C1 级。自主安全保护级。要求硬件有一定的安全级(如计算机带锁)，用户必须通过登录认证方可使用系统，并建立了访问许可权限机制。
- C2 级。受控存取保护级。比 C1 级增加了几个特性，即：引进了受控访问环境，进一步限制了用户执行某些系统指令；授权分级使系统管理员给用户分组，授予他们访问某些程序和分级目录的权限；采用系统审计，跟踪记录所有安全事件及系统管理员的工作。
- B1 级。标记安全保护级。对网络上每个对象都给予实施保护；支持多级安全，对网络、应用程序工作站实施不同的安全策略；对象必须在访问控制之下，不允许拥有者自己改变所属资源的权限。
- B2 级。结构化保护级。对网络和计算机系统中所有对象都加以定义，分配给一个标签；为工作站、终端等设备分配不同的安全级别；按最小特权原则取消权力无限大的特权用户。
- B3 级。安全域级。要求用户工作站或终端必须通过可信任的途径链接到网络系统内部的主机上；采用硬件来保护系统的数据存储区；根据最小特权原则，增加了系统安全员，将系统管理员、系统操作员和系统安全员的职责分离，将人为因素对计算机安全的威胁降至最小。

- A1 级。验证设计级。这是计算机安全级别中最高的一级，本级包括了以上各级别的所有措施，并附加了一个安全系统的受监视设计；合格的个体必须经过分析并通过这一设计；所有构成系统的部件来源都必须有安全保证；这一级还规定了将安全计算机系统运送到现场安装所必须遵守的程序。

在网络的具体设计过程中，应根据网络总体规划中提出的各项技术规范、设备类型、性能要求及经费等，综合考虑来确定一个比较合理、性能较高的网络安全级别，从而实现网络的安全性和可靠性。

1.1.4 网络安全的重要性

在信息社会中，信息具有与能源、物源同等的价值，在某些时候甚至具有更高的价值。具有价值的信息必然存在安全性的问题，对于企业更是如此。例如，在竞争激烈的市场经济驱动下，每个企业对于原料配额、生产技术、经营决策等信息，在特定的地点和业务范围内都具有保密的要求，一旦这些机密被泄露，不仅会给企业，而且会给国家造成严重的经济损失。

经济社会的发展要求各用户之间的通信和资源共享，需要将一批计算机联成网络，这样就隐含着很大的风险，包含了极大的脆弱性和复杂性，特别是对当今最大的网络——Internet，很容易遭到别有用心者的恶意攻击和破坏。随着国民经济的信息化程度的提高，有关的大量情报和商务信息都高度集中地存放在计算机中，随着网络应用范围的扩大，信息的泄露问题也变得日益严重，因此，计算机网络的安全性问题就越来越重要。

1.2 计算机网络安全的现状

互联网与生俱有的开放性、交互性和分散性特征使人类所憧憬的信息共享、开放、灵活和快速等需求得到满足。网络环境为信息共享、信息交流、信息服务创造了理想空间，网络技术的迅速发展和广泛应用，为人类社会的进步提供了巨大推动力。正是由于互联网的上述特性，产生了许多安全问题。

(1) 黑客(Hacker)。这是指在 Internet 上有一批熟悉网络技术的人，经常利用网络上现存的一些漏洞，设法进入他人的计算机系统。有些人只是为了好奇，而有些人是心怀不良动机侵入他人系统，他们偷窥机密信息，或将其计算机系统破坏，这部分人就被称为“黑客”。尽管人们在计算机技术上做出了种种努力，但这种攻击却是愈演愈烈。从单一地利用计算机病毒破坏和用黑客手段进行入侵攻击转变为使用恶意代码与黑客攻击手段相结合，使得这种攻击具有传播速度迅猛、受害面惊人和穿透深度广的特点，往往一次攻击就会给受害者带来严重的破坏和损失。

(2) 信息泄露、信息污染、信息不易受控。例如，资源未授权侵用、未授权信息流出现、系统拒绝信息流和系统否认等，这些都是信息安全的技术难点。

(3) 在网络环境中，一些组织或个人出于某种特殊目的，进行信息泄密、信息破坏、信息侵权和意识形态的信息渗透，甚至通过网络进行政治颠覆等活动，使国家利益、社会公共利益和各类主体的合法权益受到威胁。

(4) 网络运用的趋势是全社会广泛参与，随之而来的是控制权分散的管理问题。由于

人们的利益、目标及价值观产生分歧，使信息资源的保护和管理出现脱节和真空，从而使信息安全问题变得广泛而复杂。

(5) 随着社会重要基础设施的高度信息化，社会的“命脉”和核心控制系统有可能面临恶意攻击而导致损坏和瘫痪，包括国防通信设施、动力控制网、金融系统和政府网站等。

近年来，人们的网络安全意识逐步提高，很多企业根据核心数据库和系统运营的需要，逐步部署了防火墙、防病毒和入侵监测系统等安全产品，并配备了相应的安全策略。虽然有了这些措施，但并不能解决一切问题。我国网络安全问题日益突出，其主要表现在以下几个方面。

1. 安全事件不能及时、准确发现

网络设备、安全设备、系统每天生成的日志可能有上万条甚至几十万条，这样人工地对多个安全系统的大量日志进行实时审计、分析流于形式，再加上误报(如网络入侵检测系统 NIDS、互联网协议群 IPS)、漏报(如未知病毒、未知网络攻击、未知系统攻击)等问题，造成不能及时、准确地发现安全事件。

2. 安全事件不能准确定位

信息安全系统通常是由防火墙、入侵检测、漏洞扫描、安全审计、防病毒、流量监控等产品组成的，但是由于安全产品来自不同的厂商，没有统一的标准，所以安全产品之间无法进行信息交流，于是形成许多安全孤岛和安全盲区。由于事件孤立，相互之间无法形成很好的集成关联，因而一个事件的出现不能关联到真实问题。

如入侵监测系统事件报警，就需关联同一时间防火墙报警、被攻击的服务器安全日志报警等，从而了解是真实报警还是误报；如是未知病毒的攻击，则分为两类，即网络病毒、主机病毒。网络病毒大都表现为流量异常，主机病毒大都表现为中央处理器异常、内存异常、磁盘空间异常、文件的属性和大小改变等。要发现这个问题，需要关联流量监控(网络病毒)、服务器运行状态监控(主机病毒)、完整性检测(主机病毒)来发现。为了预防网络病毒大规模爆发，则必须在病毒爆发前快速发现中毒机器并切断源头。如服务器的攻击，可能是安全事件遭病毒感染；分布式拒绝服务 DDoS(Distributed Denial of Service)攻击，可能是服务器 CPU 超负荷；端口某服务流量太大、访问量太大等，必须将多种因素结合起来才能更好地分析，快速知道真实问题点并及时恢复正常。

DDoS 是一种基于 DoS 的特殊形式的拒绝服务攻击，是一种分布、协作的大规模攻击方式，主要瞄准比较大的站点，像商业公司、搜索引擎和政府部门的站点。DDoS 攻击是利用一批受控制的机器向一台机器发起攻击，这样来势迅猛的攻击令人难以防备，因此具有较大的破坏性。

3. 无法做集中的事件自动统计

它包括某台服务器的安全情况报表、所有机房发生攻击事件的频率报表、网络中利用次数最多的攻击方式报表、发生攻击事件的网段报表、服务器性能利用率最低的服务器列表等。需要管理员人为地对这些事件做统计记录，生成报告，从而耗费大量人力。

4. 缺乏有效的事件处理查询

没有对事件处理的整个过程做跟踪记录，信息部门主管不了解哪些管理员对该事件进行了处理，对处理过程和结果也没有做记录，使得处理的知识和经验不能得到共享，导致下次再发生类似事件时，处理效率的低下。

5. 缺乏专业的安全技能

管理员发现问题后，往往因为安全知识的不足导致事件迟迟不能被处理，从而影响网络的安全性，延误网络的正常使用。

1.3 计算机网络安全威胁

安全威胁是指某个人、物、事件或概念对某一资源的机密性、完整性、可用性或合法性所造成的危害。某种攻击就是某种威胁的具体实现。

安全威胁可分为故意的(如黑客渗透)和偶然的(如信息被发往错误的地址)两类。故意威胁又可进一步分为被动和主动两类。

1.3.1 安全攻击

对于计算机或网络安全性的攻击，一般是通过在提供信息时查看计算机系统的功能来记录其特性。当信息从信源向信宿流动时，图 1.2 中列出了信息正常流动和受到各种类型的攻击的情况。

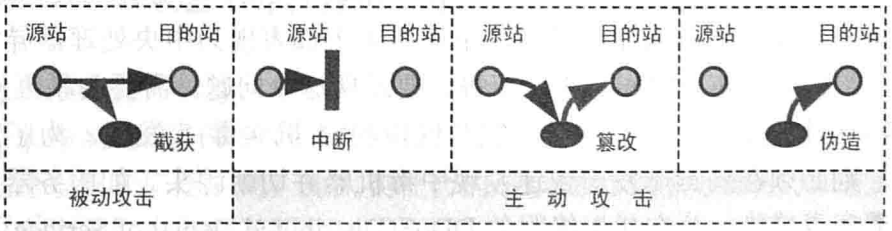

图 1.2 安全攻击

(1) 中断是指系统资源遭到破坏或变得不能使用。这是对可用性的攻击。例如，对一些硬件进行破坏、切断通信线路或禁用文件管理系统。

(2) 截获是指未授权的实体得到了资源的访问权，这是对保密性的攻击。未授权实体可能是一个人、一个程序或一台计算机。

(3) 篡改是指未授权的实体不仅得到了访问权，而且还篡改了资源，这是对完整性的攻击。

(4) 伪造是指未授权的实体向系统中插入伪造的对象，这是对真实性的攻击。

1. 被动攻击与主动攻击

以上这些攻击类型还可分为被动攻击和主动攻击两种，下面详细介绍。

(1) 被动攻击的特点是偷听或监视传送，其目的是获取正在传送的消息。被动攻击有泄露信息内容和通信量分析等。①泄露信息内容容易理解，包括电话对话、电子邮件消息

以及可能含有敏感的机密信息，要防止对手从传送中获得这些内容。②通信量分析则比较微妙，是用某种方法将信息内容隐藏起来，常用的技术是加密，这样即使对手捕获了消息，也不能从中提取信息。对手可以确定位置和通信主机的身份，可以观察交换消息的频率和长度。这些信息可以帮助对手猜测正在进行的通信特性。

(2) 主动攻击涉及修改数据或创建错误的数据流，它包括假冒、重放、修改消息和拒绝服务等。①假冒是一个实体假装成另一个实体，假冒攻击通常包括一种其他形式的主动攻击；②重放涉及被动捕获数据单元及其后来的重新传送，以产生未经授权的效果；③修改消息意味着改变了真实消息的部分内容，或将消息延迟或重新排序，导致未授权的操作；④拒绝服务是指禁止对通信工具的正常使用或管理，这种攻击拥有特定的目标；另一种拒绝服务的形式是整个网络的中断，可以通过使网络失效而实现，或通过消息过载使网络性能降低。主动攻击具有与被动攻击相反的特点。虽然很难检测出被动攻击，但可以采取措施防止它的成功。相反，很难绝对预防主动攻击，因为这样需要随时对所有的通信工具和路径进行完全保护。防止主动攻击的做法是对攻击进行检测，并从它引起的中断或延迟中恢复过来。因为检测具有威慑的效果，也可以起到预防作用。

2. 服务攻击与非服务攻击

另外，从网络高层协议的角度，攻击方法可以概括地分为两大类，即服务攻击与非服务攻击。

(1) 服务攻击(Application Dependent Attack)是针对某种特定网络服务的攻击，如针对 E-mail 服务、Telnet、FTP、HTTP 等服务的专门攻击。目前 Internet 应用协议集(主要是 TCP/IP 协议集)缺乏认证、保密措施，是造成服务攻击的重要原因。现在有很多具体的攻击工具，如 Mailf Bomb(邮件炸弹)等，可以很容易地实施对某项服务的攻击。

(2) 非服务攻击(Application Independent Attack)不针对某项具体应用服务，而是基于网络层等低层协议而进行的。TCP/IP 协议(尤其是 IPv4)自身的安全机制不足为攻击者提供了方便之门。

与服务攻击相比，非服务攻击与特定服务攻击无法相比，它往往利用协议或操作系统实现协议时的漏洞来达到攻击的目的，更为隐蔽，而且目前也是常常被忽略的方面，因而被认为是一种更为有效的且更具危险性的攻击手段。

1.3.2 基本的威胁

网络安全的基本目标是实现信息的机密性、完整性、可用性和合法性。以下 4 个基本的安全威胁直接反映了这 4 个安全目标。

(1) 信息泄露或丢失。它指敏感数据在有意或无意中被泄露出去或丢失，通常包括信息在传输中丢失或泄露、信息在存储介质中丢失或泄露、通过建立隐蔽通道等窃取敏感信息等。

(2) 破坏数据完整性。这是指以非法手段窃得对数据的使用权，删除、修改、插入或重发某些重要信息，以取得有益于攻击者的响应；恶意添加、修改数据，以干扰用户的正常使用。

(3) 拒绝服务攻击。它不断对网络服务系统进行干扰，改变其正常的作业流程，执行

无关程序使系统响应减慢甚至瘫痪，影响正常用户的使用，甚至使合法用户被排斥而不能进入计算机网络系统或不能得到相应的服务。

(4) 非授权访问。没有预先经过同意，就使用网络或计算机资源，被看作是非授权访问，如有意避开系统访问控制机制，对网络设备及资源进行非正常使用，或擅自扩大权限，越权访问信息。它主要有假冒、身份攻击、非法用户进入网络系统进行违法操作、合法用户以未授权方式进行操作等几种形式。

1.3.3 主要可实现的威胁

这些威胁可以使基本威胁成为可能，所以十分重要。它包括两类，即渗入威胁和植入威胁。

1. 渗入威胁的几种形式

主要的渗入威胁有：假冒、旁路控制、授权侵犯。

(1) 假冒。这是大多数黑客采用的攻击方法。某个未授权实体使守卫者相信它是一个合法的实体，从而攫取该合法用户的特权。

(2) 旁路控制。攻击者通过各种手段发现本应保密却又暴露出来的一些系统“特征”，利用这些“特征”，攻击者绕过防线守卫者渗入到系统内部。

(3) 授权侵犯。也称为“内部威胁”，授权用户将其权限用于其他未授权的目的。

2. 植入威胁的主要形式

主要的植入威胁有：特洛伊木马、后门。

(1) 特洛伊木马。攻击者在正常的软件中隐藏一段用于其他目的的程序，这段隐藏的程序段常常以安全攻击作为其最终目标。

(2) 后门。后门是在某个系统或某个文件中设置的“机关”，使得当提供特定的输入数据时允许违反安全策略。

1.3.4 病毒

病毒是能够通过修改其他程序而“感染”它们的一种程序，修改后的程序里面包含了病毒程序的一个副本，这样它们就能够继续感染其他程序。编制或者在计算机程序中插入的破坏计算机功能或者破坏数据，影响计算机使用并且能够自我复制的一组计算机指令或者程序代码被称为计算机病毒(Computer Virus)。具有破坏性、复制性和传染性。

通过网络传播计算机病毒，其破坏性大大高于单机系统，使用户很难防范。由于在网络环境下，计算机病毒有不可估量的威胁性和破坏力，因此，计算机病毒的防范是网络安全性建设的重要内容。

网络防病毒技术包括预防病毒、检测病毒和清除病毒 3 种技术。

(1) 预防病毒技术。它通过自身常驻系统内存，优先获得系统的控制权，来监视和判断系统中是否有病毒存在，进而防止计算机病毒进入计算机系统和对系统进行破坏。这类技术有加密可执行程序、引导区保护、系统监控与读写控制(如防病毒卡等)。

(2) 检测病毒技术。它是通过对计算机病毒的特征来进行判断的技术，如自身校验、