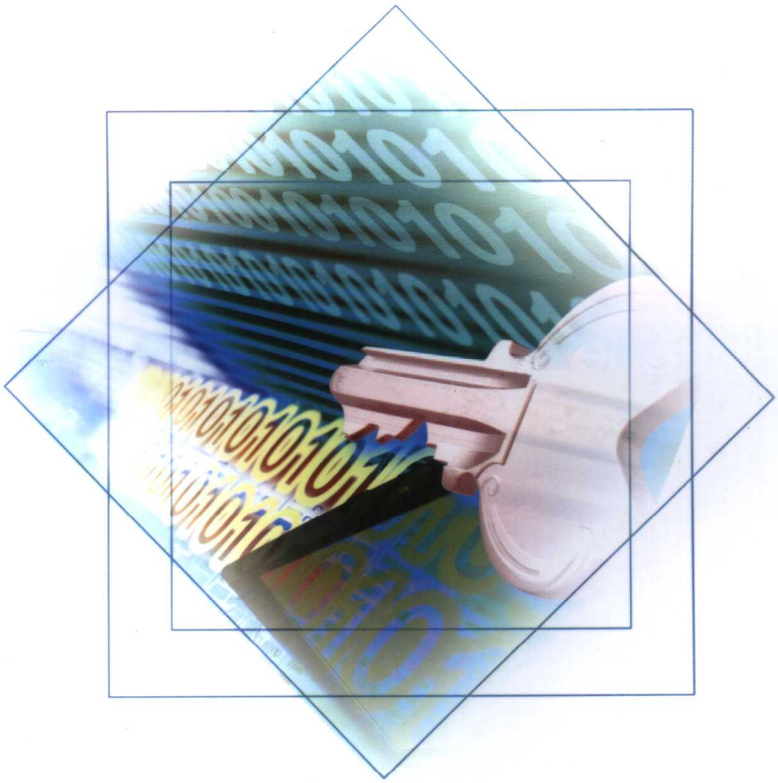
21世纪高等院校计算机系列规划教材

Computer

张友纯 主编

# 计算机网络安全



华中科技大学出版社
http:// www.hustp.com

21 世纪高等院校计算机系列规划教材

# 计算机网络安全

主　编　张友纯

副主编　向金海　宋　军

华中科技大学出版社

**图书在版编目(CIP)数据**

计算机网络安全/张友纯　主编
武汉:华中科技大学出版社,2006 年 2 月
ISBN 7-5609-3658-X

Ⅰ.计…
Ⅱ.张…
Ⅲ.计算机网络-安全技术
Ⅳ.TP393.4

**计算机网络安全**　　张友纯　主编

责任编辑:曾　光　张　毅　　封面设计:刘　卉
责任校对:刘　竣　　责任监印:张正林

出版发行:华中科技大学出版社
武昌喻家山　　邮编:430074　　电话:(027)87557437

录　　排:武汉万卷鸿图科技有限公司
印　　刷:武汉首壹印刷厂

开本:787×1092　1/16　　印张:20.75　　字数:463 000
版次:2006 年 2 月第 1 版　　印次:2006 年 2 月第 1 次印刷　　定价:29.80 元
ISBN 7-5609-3658-X/TP・600

# 内 容 简 介

本书共 14 章，分别介绍了网络安全模型，网络安全技术的研究内容；网络安全技术的理论基础，即数论、信息论和复杂度等相关概念；对称加密体制、公开密钥体制、数字签名与认证和密钥管理等信息安全基础；数据库的安全与加密、电子邮件安全、IP 安全、Web 安全和防火墙技术等安全技术以及网络攻击与防范、入侵检测系统和计算机病毒的诊断与清除等。

本书系统性较强，既介绍了网络安全技术，对安全技术的理论基础也作了简要介绍；内容较新，反映了当前网络与信息安全领域的一些新动向、新方法和新技术；篇幅适中，有一定的理论深度和参考价值。

本书既可作为除信息安全专业以外的信息学科的本科学生和研究生的使用教材，也可作为其他专业本科学生和研究生公选课教材，还可作为从事计算机网络工作人员的参考书和进修教材。

# 前　言

计算机网络的普及与发展正改变着人们的工作、学习和生活方式，计算机网络的发展和应用对整个社会的科学技术、经济发展、国防建设、文化思想带来了巨大的影响和推动，计算机网络的发展和应用水平也成为衡量一个国家或地区综合实力的重要标志。

计算机网络技术的本质就是信息共享，在人们享受 Internet 及其 E-Mail、Web 和 FTP 带来方便的同时，由于网络的开放性，信息安全的问题也随之摆在了人们面前。网络上的黑客和不法之徒利用一些安全漏洞可以取走用户的机密文件、窃取用户的银行存款、破坏用户的企业账目、公布用户的隐私信函、篡改和毁坏用户的数据库，甚至使用户的网络瘫痪或崩溃。因此，人们已清醒地认识到在发展计算机网络技术的同时，必须做好计算机网络安全方面的理论研究与应用技术开发，网络安全技术也是计算机网络技术的重要研究内容，网络安全问题的研究和技术的开发应用已成为当前和将来一个时期内的热点。

在除信息安全专业以外的信息学科的本科学生和研究生中开设网络安全课程，旨在让学生建立网络安全的基本概念，掌握网络安全的基本知识、基本方法和技术，了解计算机网络安全的应用系统设计原理和方法，为今后在从事信息技术工作中保障计算机网络安全、保障信息安全打下基础，也为今后从事计算机网络的研究和开发打下良好的基础。

本书共分 14 章。第 1 章介绍了网络安全模型及网络安全技术的研究内容；第 2 章对网络安全技术的理论基础，即数论、信息论和复杂度等相关概念进行了简单描述；第 3 章、第 4 章、第 5 章和第 6 章，分别介绍了对称加密体制、公开密钥体制、数字签名与认证和密钥管理等相关问题；随后在第 7 章、第 8 章、第 9 章、第 10 章和第 11 章中，分别介绍了数据库的安全与加密、电子邮件安全、IP 安全、Web 安全和防火墙技术；最后在第 12 章、第 13 章和第 14 章中，分别介绍了网络攻击与防范、入侵检测系统和计算机病毒的诊断与清除。

本书的第 1、2、3、4、5、6、11 章由张友纯编写，第 8、9、10、13 章由向金海编写，第 7、12、14 章由宋军编写。张友纯教授完成统稿。中国地质大学信息工程学院罗忠文教授审阅了全书内容并提出了宝贵意见。本书在编写过程中得到了中国地质大学教务处、研究生院和信息工程学院的支持。本书的编写参考了许多相关文献，在此一并表示感谢。

由于编者水平有限，编写时间仓促，书中难免出现错误和问题，殷切希望读者批评指正，也请各位专家给予指教。

编　者

2005 年 12 月

# 目　录

# 第 1 章　计算机网络安全概述

计算机网络技术的发展使得计算机应用日益广泛与深入，同时也使得计算机系统的安全问题日益复杂和突出。一方面，网络提供了资源的共享性，提高了系统的可靠性，通过分散工作提高了工作效率，并且还具有可扩充性。这些特点使得计算机网络深入到经济、国防、科技、文教等各个领域。另一方面，也正是这些特点，增加了网络安全的脆弱性和复杂性，资源共享和分布增加了网络受威胁和攻击的可能性。计算机的使用使机密和财富集中于计算机，计算机网络的使用也使这些机密和财富随时受到网络攻击的威胁。随着网络覆盖范围的扩大，以各种非法手段企图渗透计算机网络的黑客迅速增加，使得国内外屡屡发生严重的黑客入侵事件。

2000 年 2 月 7 日起的一周内，黑客对 Internet 网站发动了大规模的袭击，著名的美国雅虎、亚马逊等八大网站相继瘫痪，造成直接损失 12 亿美元。

2003 年 1 月 15 日，北美洲、欧洲和亚洲的 Internet 全部陷入瘫痪，其原因至今尚不清楚。据美国 FBI 的估计，大型计算机网络被攻破一次所造成的损失为 50 亿美元，而一个银行数据中心的计算机每停机一秒钟，其损失为 5 000 美元。

据有关部门统计，国内 90%以上的电子商务网站都存在严重的安全漏洞，网络的安全正面临着日益严重的威胁。

## 1.1　计算机网络面临的威胁

### 1.1.1　网络系统自身的脆弱性

所谓系统自身的脆弱性，是指系统的硬件资源、通信资源、软件及信息资源等，因可预见或不可预见甚至恶意的原因，可能导致系统被破坏、更改、泄漏和功能失效，从而使网络处于异常状态，甚至是导致系统崩溃、瘫痪的根源和起因。计算机网络本身由于系统主体和客体的原因可能存在不同程度的脆弱性，为各种动机的入侵、骚扰或破坏提供了可利用的途径和方法。

### 1.1.2　影响网络安全的因素

一个计算机网络进行通信时，一般要通过通信线路、调制解调器、网络接口、终端、转换器和处理机等部件。通信线路的安全令人担忧，通过通信线路与交换系统互联的网络是窃密者、非法分子威胁和攻击的重要目标。

对网络的威胁，影响网络安全的主要因素有以下五个方面。

1．硬件系统的因素

① Internet 的脆弱性。系统的易欺骗性和易被监控性，加上薄弱的认证环节，以及局域网服务的缺陷和系统主机的复杂设置与控制，使得计算机网络容易受到威胁和攻击。

② 电磁泄露。网络端口、传输线路和处理机都有可能因屏蔽不严或未屏蔽而造成电磁泄露。目前，大多数机房屏蔽和防辐射设施都不健全，通信线路也同样容易出现信息泄露。

③ 搭线窃听。随着信息传递量的不断增加，传递数据的密集度也不断提高，犯罪分子为了获取大量情报，可能通过监听通信线路而非法接收信息。

④ 非法终端。有可能在现有终端上并接一个终端，或合法用户从网上断开时，非法用户趁机接入并操纵该计算机端口，或由于某种原因使信息传到非法终端。

⑤ 线路干扰。在公共转接载波设备陈旧或通信线路质量低劣的情况下会产生线路干扰，从而导致超距攻击。超距攻击即为不接触进行攻击，如接收计算机工作时辐射的电磁波或利用电磁干扰计算机正常工作，使数据传输出错。调制解调器会随着传输速率的上升而使错误迅速上升。

⑥ 意外原因。它包括人为地对网络设备进行破坏；设备出现故障；处理非预期中断过程中，留在内存中未被保护的信息段因通信方式意外弄错而传到别的终端。

2．软件系统因素

① 网络软件的漏洞及缺陷被利用，对网络进行入侵和破坏。

② 网络软件安全功能不健全或被安装了“特洛伊木马”软件。

③ 应加安全措施的软件可能未予标志和保护，关键的程序可能没有安全措施，使软件被非法使用或破坏，或产生错误结果。

④ 未对用户进行分类和标志，使数据的存取未受到限制和控制，导致非法窃取数据或非法处理用户数据。

⑤ 错误地进行路由选择，为一个用户与另一个用户之间的通信选择不合理的路径。

⑥ 拒绝服务，中断或妨碍通信，延误对时间需求较高的操作。

⑦ 信息重播，即把信息录下来准备过一段时间重播。

⑧ 对软件更改的要求没有充分理解，导致软件错误。

⑨ 没有正确的安全策略和安全机制，缺乏先进的安全工具和手段。

⑩ 不妥当的标定或资料，导致所修改的程序版本出错；程序员没有保存程序变更的记录，没有复制或未建立保存记录的业务。

3．工作人员因素

① 保密观念不强或不懂保密规则，随便泄露机密；打印、复制机密文件；随便打印系统保密字或向无关人员泄露机密信息。

② 业务不熟练，因操作失误导致文件出错或因未遵守操作规程而造成泄密。

③ 因规章制度不健全而造成人为泄密事故，如网络上的规章制度不严、对机密文件保管不善、各种文件存放混乱、违章操作等。

④ 素质差，缺乏责任心，没有良好的工作态度，明知故犯，或有意破坏网络系统和设备。

⑤ 熟悉系统的工作人员故意改动软件，或用非法手段访问系统，或通过窃取他人的口令字和用户标志码非法获取信息。

⑥ 否认参与过某一次通信或冒充别的用户获取信息或权限。

⑦ 担任系统操作的人员以超越权限的非法行为来获取或篡改信息。

⑧ 利用窃取系统的磁盘、磁带或纸带等记录载体，或利用废弃的打印纸、复写纸来窃取系统或用户的信息。

**4．外部的威胁与入侵**

① 否认或冒充。否认参与过某一次通信，或非法用户冒充为合法用户对系统进行非法的访问。冒充授权者发送和接收信息，造成信息的泄露和丢失。

② 篡改。通信网络中的信息在没有监控的情况下，都有可能被篡改，即对信息的标签、内容、接收者和始发者进行修改，以取代原信息，造成信息失真。

③ 窃取。盗窃信息可以通过多种途径，在通信线路中，通过电磁辐射侦截线路中的信息；在信息存储和信息处理中，通过非法访问达到窃取信息的目的。

④ 重放。将接受的信息重新修改和排序后，在适当的时机重放出来，从而造成信息的重放和混乱。

⑤ 推断。这是在窃取基础上的一种破坏活动，它的目的不在于窃取原信息，而是将窃取到的信息进行统计分析，了解信息流量大小的变化和信息交换频繁程度，再结合其他方面的信息，推断出有价值的内容。

⑥ 病毒入侵。在网络环境下，计算机病毒具有不可估量的威胁性和破坏力，计算机病毒可以通过多种方式侵入计算机网络，并不断繁殖，然后通过扩散到网上来破坏系统。轻则使系统出错，重则使整个计算机系统瘫痪或崩溃。

⑦ 黑客攻击。黑客采取多种手段，对网络及其计算机系统进行攻击，侵占系统资源，或对网络和计算机设备进行破坏，窃取或破坏数据和信息。根据攻击者到计算机系统的距离，可分为超距攻击、远距攻击和近距攻击。超距攻击是利用 Internet 进行攻击，其攻击方式具有极大的隐蔽性，必须严加防范，特别要警惕国外情报机关利用这种方式进行窃密和破坏；远距攻击是通过电话线侵入计算机网络，注册登录到网内某一主机，进行非法存取，要注意外部人员，尤其是黑客和国外敌对分子进行的攻击；近距攻击，即同一单位的人利用合法身份越权存取计算机中的数据或干扰其他用户使用，要注意内部人员的非法攻击。

**5．环境因素**

除了上述因素之外，环境因素也威胁着网络的安全，如地震、火灾、水灾、风灾等自然灾害或断电、停电等事故。上述因素能威胁到网络，主要由于网络存在以下几个方面的问题：

- 局域网存在的缺陷和 Internet 的脆弱性；
- 网络软件的缺陷和 Internet 服务中的漏洞；
- 薄弱的网络认证环节；
- 没有正确的安全策略和安全机制；
- 缺乏先进网络安全技术和工具；

• 对网络安全没有引起足够的重视，没有采取得力的措施，以致造成重大的经济损失，这是最重要的一个原因。

## 1.2 计算机网络安全策略和安全机制

在建立系统的网络安全之前，必须要明确需要保护的资源和服务类型、重要程度和防护对象等。安全策略是由一组规则组成的，对系统中所有与安全相关元素的活动做出一些限制性规定。系统提出的安全服务，其规则基本上都来自于安全策略。

### 1.2.1 网络安全的内容

网络安全的内容包括了系统安全和信息安全两个部分。系统安全主要指网络设备的硬件、操作系统和应用软件的安全；信息安全主要指各种信息的存储、传输的安全，具体体现在保密性、完整性及不可抵赖性等方面。

从内容上看，网络安全大致包括以下四个方面。

网络实体安全：如计算机机房的物理条件、物理环境及设施的安全标准，计算机硬件、附属设备、网络传输线路的安装及配置等。

软件安全：如保护网络系统不被非法侵入，系统软件与应用软件不被非法复制、篡改、不受病毒的侵害等。

数据安全：保护数据不被非法存取，确保其完整性、一致性、机密性等。

安全管理：运行时突发事件的安全处理等，包括采取计算机安全技术、建立安全管理制度、开展安全审计、进行风险分析等。

### 1.2.2 网络安全的特征

计算机网络的发展使信息的共享和应用日益广泛和深入，但是信息在通信网络上存储、共享和传输，会被非法窃取、截获或篡改而导致不可估量的损失。在现实中，计算机网络主要有以下三类不同的安全威胁：

- 未经授权访问，指非授权的侵入；
- 信息泄漏，造成有价值的或高度机密的信息泄漏；
- 拒绝服务，使任务难于或不可能继续执行。

要保证网络信息安全，计算机网络必须具有以下特性。

① 保密性。信息不泄漏给非授权用户、实体或过程，仅供授权用户、实体或过程利用的特性。

② 完整性。在存储或传输的过程中，信息保持不被篡改、破坏和丢失的特性。

③ 可用性。可被授权实体访问并要求使用的特性，即当需要时应能够存取所需要的信息。

④ 可控性。对信息的传播及其内容具有控制能力。

⑤ 可审查性。对出现的网络安全问题提供调查的依据和手段。

### 1.2.3　网络安全的策略与安全机制

使用安全策略，目的是决定一个计算机网络的组织机构怎样来保护自己的网络及其信息。一般来说，保护的政策包括两个部分：一个总的策略和一个具体的规则。

总的策略用于阐明安全政策的总体思想，而具体的规则用于说明什么是被允许的、什么是被禁止的。

总的安全策略是制定一个组织机构的战略性指导方针，并为实现这个方针分配必须的人力和物力。一般由网络组织领导机构和高层领导来主持制定这种政策，以建立该机构的安全计划和基本的框架结构。

**1．网络安全政策的作用**

网络安全政策的作用包括：定义该安全计划的目的和在该机构中涉及的范围；把任务分配给具体的部门和人员，并且实施这个计划；明确违反政策的行为及其处理措施。

针对互联网的系统情况，可以作以下一些考虑。

① 根据全系统的安全性，做统一规划，对安全设备统一选型。

② 以网络作为安全系统的基本单元。

③ 以网络的安全策略统一管理。

④ 对网络采取访问控制措施。

⑤ 负责安全审计跟踪与安全警告报告。

⑥ 对网间的数据传输，可以采用加密技术进行保护。

⑦ 整个系统采用统一的密钥管理措施。

⑧ 采用防电磁泄漏措施，特别注意电磁辐射。

⑨ 采用抗病毒入侵和检测消毒措施。

⑩ 采用一切技术和非技术手段来保证系统的安全。

**2．网络安全策略的等级**

网络安全策略可分为以下四个等级。

① 不把内部网络与外部网络相连，因此一切被禁止。

② 除那些被明确允许之外，一切都被禁止。

③ 除那些被明确禁止之外，一切都被允许。

④ 一切都被允许，当然包括那些本来被禁止的。

可以根据实际情况，在这四个等级之间找出符合自己的安全策略。当系统自身的情况发生变化时，必须注意及时修改相应的安全策略。

**3．网络安全策略的内容**

(1) 网络管理员的安全责任

该策略可以要求在每台主机上使用专门的安全措施、登录用户名称、检测和记录过程等，还可以限制连接中所有的主机不能运行应用程序。

(2) 网络用户的安全策略

该策略可以要求用户每隔一段时间改变口令，使用符合安全标准的口令形式，执行某些检查，以了解其账户是否被别人访问过。

(3) 正确利用网络资源

该策略规定谁可以利用网络资源，他们可以做什么、不应该做什么。对于 E-mail 和计算机活动的历史，应受到安全监视，告知有关人员。

(4) 检测到安全问题的策略

该策略要求当检测到安全问题时，应该做什么、应该通知什么部门，这些问题都要明确。

### 1.2.4 网络安全的机制

具体的安全规则就是根据安全策略规定的各种安全机制。如身份认证机制、授权机制、访问控制机制、数据加密机制、数据完整性机制、数据签名机制、报文鉴别机制、路由控制机制、业务流填充机制等。

如授权机制是针对不同用户的信息资源的访问权限。对授权用户的控制有以下要求。

① 一致性。对信息资源的控制没有二义性，各种定义之间不冲突。

② 统一性。对所有信息资源进行集中管理，安全政策统一。

③ 审计功能。对所有授权用户进行跟踪检查。

④ 尽可能提供相近粒度的检查。

### 1.2.5 网络安全的实现

实现网络安全，不仅要靠先进的技术，而且也要靠严格的安全管理和安全法律的约束。

(1) 先进的网络安全技术

用户对自身面临的威胁进行风险分析和评估，决定其所需要的安全服务种类，选择相应的安全机制，然后用先进的安全技术形成全方位的安全系统。先进的网络安全技术是网络安全的根本保证。

(2) 严格的安全管理

各计算机网络使用机构、企业和单位应建立相应的网络管理办法，加强内部管理，建立适合的网络安全管理系统，建立安全审计和跟踪体系，提高整体网络的安全意识。

(3) 严格的法律、法规

计算机网络是一种新生事物，好多行为无法可依、无章可循，因此导致网上计算机犯罪处于无序状态。面对日益严重的网络犯罪、计算机犯罪，必须严格执行法律、法规，并加强执法力度，坚决、严厉打击计算机犯罪和网上犯罪活动，保护国家国防机密和网民的合法权益，使犯罪分子慑于法律，不敢轻举妄动。

## 1.3　网络安全模型

大多数的网络安全模型如图 1.1 所示。通信一方要通过网络将消息传送给另一方，通信双方(称为交易的主体)必须协调努力共同完成消息变换。通过定义网络上从源到宿主的路由，然后在该路由上执行通信主体共同使用的通信协议(如 TCP/IP)来建立逻辑信息通道。

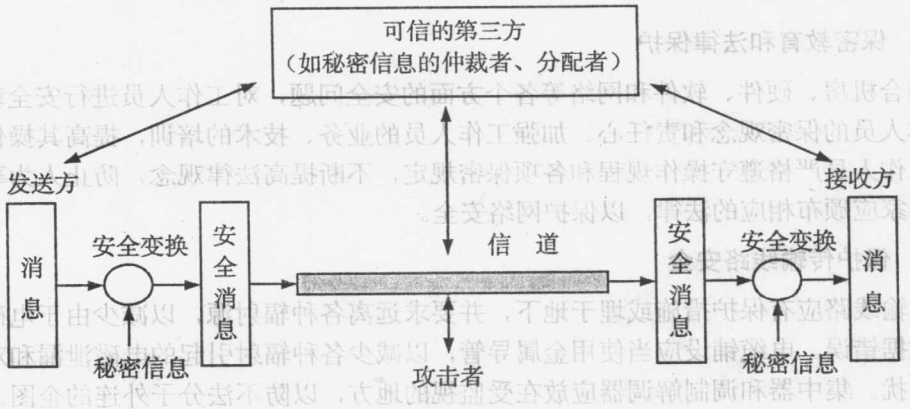



图1.1　网络安全模型

如果需要保护信息传输以防攻击者危害信息的保密性、真实性，则需要考虑通信的安全性。安全传输技术包括以下两个基本部分。

① 消息的安全传输，如对消息的加密和认证。加密的目的是将消息按照一定的方式重新编码以使攻击者无法获得真正的消息内容；认证的目的用于验证发送者的身份。

② 发送双方共享的某些秘密信息，如加密密钥。

为了获得信息的安全传输，需要有可信的第三方，其作用是负责向通信双方发送秘密信息而对攻击者保密，或者在通信双方有争议时进行仲裁。

上述模型说明，一个安全的网络通信必须考虑以下四个方面：设计执行安全相关的加密算法；用于加密算法的秘密信息(如密钥)；秘密信息的发布和共享；使用加密算法和秘密信息以获得安全服务所需的协议。

以上适用的主要是安全机制和服务的模型，还有一些不符合该模型的情况，图 1.2 所示为保护信息系统未授权访问模型。

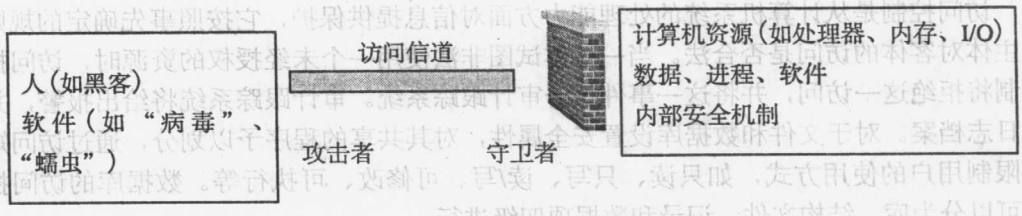



图 1.2　未授权访问模型