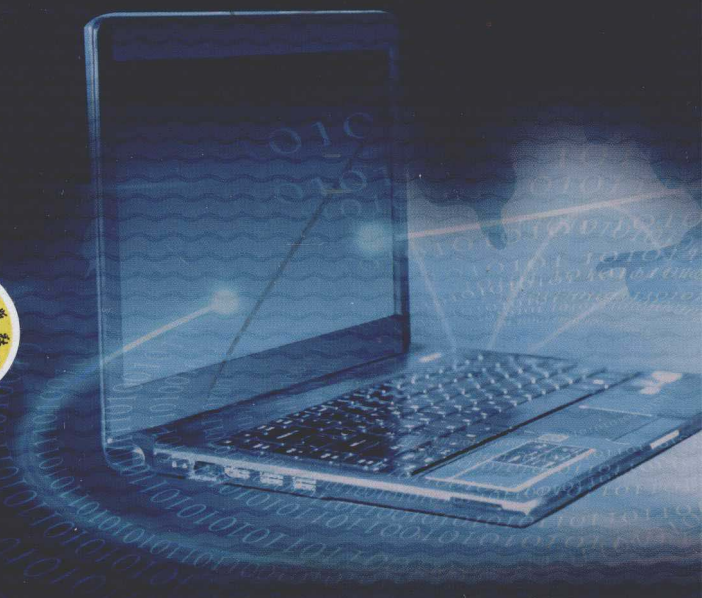
免费提供
电子教案

计算机网络安全

谭晓玲　蔡 黎　刘 毓　代妮娜　编著



机械工业出版社
CHINA MACHINE PRESS

计算机网络安全

谭晓玲　蔡　黎　刘　毓　代妮娜　编著

机械工业出版社

本书重点论述目前计算机网络安全中比较成熟的思想、结构和方法，着力介绍网络安全系统的实践操作方法。全书共10章，第1章引言，简单介绍计算机网络安全的产生和发展、主要功能、分类以及网络体系结构和ISO/OSI参考模型。第2、3章主要介绍网络安全攻击，内容包括计算机网络的入侵及检测和安全扫描。第4、5章介绍网络安全防御和防火墙技术。第6、7、8章介绍数据通信网的基本知识及数据安全、病毒防治技术。第9章介绍如何科学地管理广域/局域计算机网络的安全。第10章以案例的形式介绍计算机网络安全法规的相关知识。

本书可作为高等院校信息技术类专业高年级本科生或低年级硕士研究生的学习资料，也可以作为从事计算机网络工作的技术人员研读和参考用书。

本书配套授课电子课件，需要的教师可登录www.cmpedu.com免费注册、审核通过后下载，或联系编辑索取（QQ：241151483，电话：010-88379753）。

图书在版编目（CIP）数据

计算机网络安全/谭晓玲，蔡黎，刘毓，代妮娜编著．—北京：机械工业出版社，2012.3
ISBN 978-7-111-38537-0

Ⅰ．①计… Ⅱ．①谭… ②蔡… ③刘… ④代… Ⅲ．①计算机网络-安全技术-高等学校-教材 Ⅳ．① TP393.08

中国版本图书馆CIP数据核字（2012）第108989号

机械工业出版社（北京市百万庄大街22号 邮政编码100037）
责任编辑：郝建伟 罗子超
责任印制：乔 宇
三河市宏达印刷有限公司印刷

2012年8月第1版·第1次印刷
184mm×260mm·19印张·470千字
0001-3000册
标准书号：ISBN 978-7-111-38537-0
定价：39.00元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换

电话服务
社服务中心：（010）88361066
销售一部：（010）68326294
销售二部：（010）88379649
读者购书热线：（010）88379203

网络服务
门户网：http://www.cmpbook.com
教材网：http://www.cmpedu.com

封面无防伪标均为盗版

前　言

随着微电子技术、计算机技术和通信技术的迅速发展和相互渗透，计算机网络已成为当今最热门的学科之一。计算机网络尤其是 Internet 技术已经进入每一个现代社会人的生活，并在很大程度上影响和改变着人们的生活、学习、工作和思维方式，甚至对人类科技、政治、经济都产生了巨大的影响。因此，计算机网络的安全问题也日益得到重视。

计算机网络安全最终需要专业的计算机网络从业人员掌握，国内与计算机网络安全有关的著作一般都是沿袭国外 20 世纪 80 年代的体系，以介绍网络安全概念、结构、攻防理论为主，缺乏如网络安全软件的使用、网络安全案例等实践性知识的阐述。

本书重点论述目前计算机网络安全中比较成熟的思想、结构和方法，着力介绍网络安全系统的实践操作方法，并且力求做到深入浅出、通俗易懂。在内容选择上，我们一方面从理论上以 ISO/OSI 参考模型为引线介绍计算机网络安全的基本概念、原理和方法；另一方面以 TCP/IP 协议族线索详细探讨网络安全软件的使用、实例及案例。为了使未系统学习基础课程的读者也能读懂此书，我们还在本书中增加了有关数据通信网的基础知识。

全书共 10 章，分为 5 大部分。第 1 章简单介绍计算机网络安全的产生和发展、主要功能、分类以及网络体系结构和 ISO/OSI 参考模型。第 2、3 章构成第一部分——网络安全中的攻击，内容包括计算机网络的入侵及检测和安全扫描。第 4、5 章构成第二部分——网络防御，内容包括网络安全防御和防火墙技术。第 6、7、8 章构成第三部分——网络中的数据保密技术，内容包括数据通信网的基本知识及数据安全、病毒防治技术。第 9 章是第四部分——安全管理，内容包括如何科学地管理广域/局域计算机网络的安全。第 10 章是第五部分——网络法规，以案例的形式介绍计算机网络安全法规的相关知识。

本书作为一本计算机网络安全领域的著作，主要供专业和业余计算机网络专业人员研读，也可以作为高等院校电子信息类专业高年级本科生或低年级硕士研究生教材，同时也可作为计算机网络设计人员、开发人员以及管理人员的技术参考书。

本书由重庆三峡学院谭晓玲副教授带领计算机网络课程教研组编写，也是重庆市教育科学“十二五”规划教育考试规划课题成果：第 1、3、6、7 章由谭晓玲、蔡黎编写，第 2、5、10 章由谭晓玲、刘毓编写，第 4、8、9 章由谭晓玲、代妮娜编写，谭晓玲对全书进行了统稿。

计算机网络安全技术发展非常迅速，涉及的知识面广，加之作者水平有限，虽经编者艰苦努力，但书中难免错漏之处，欢迎广大读者批评指正。

编　者

目　录

第1章　网络安全概述

以 Internet 为代表的全球性信息化浪潮日益高涨，计算机以及信息网络技术的应用正日益普及和广泛，应用层次正在深入，信息的应用也从原来的军事、科技、文化和商业渗透到当今社会的各个领域，其在社会生产、生活中的作用日益显著。信息技术的使用给人们生活和工作带来了数不尽的便捷和好处。然而，当人们使用信息技术提高工作效率，为社会创造更多财富的同时，另外一些人却利用信息技术做着相反的事情。网上失密、泄密、窃密及传播有害信息的事件屡有发生。一旦网络中传输的用户信息被有意窃取、篡改，则对用户和企业本身造成的损失都是不可估量的。无论是庞大的服务提供商，还是一个企业的某一个业务部门的局域网，数据安全的实施均迫在眉睫。据统计，全球约 20 秒就有一次计算机入侵事件发生，Internet 上的网络防火墙约 1/4 被突破，70% 以上的网络信息主管人员报告因机密信息泄露而受到了损失。网络安全成为一个关系到国家的安全和主权、社会的稳定、民族文化的继承和发扬的重要问题，网络安全涉及计算机科学、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。

1.1　网络安全的基础知识

根据中国因特网信息中心（CNNIC）2011 年 1 月 19 日公布的《第 27 次中国因特网络发展状况统计报告》显示，截至 2010 年 12 月底，我国网民规模达到 4.57 亿，较 2009 年底增加 7330 万人。网络用户和网络主机的数量仍然在持续增长，与此同时，电子政务、电子商务、网络游戏、网络博客等因特网业务正在快速扩展，新的操作系统、新应用软件不断投入使用，这些都导致大量人为主观疏忽和网络系统客观漏洞的存在。而黑客攻击动机已经从单纯地追求“荣耀感”向获取多方面实际利益和表达政治情绪的方向转移，黑客技术的发展也将重点放在网上木马、间谍程序、恶意网站、网络仿冒、僵尸网络等方面。因此，网络安全问题变得更加错综复杂，涉及范围将不断扩大。

1.1.1　网络安全的定义

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，不受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，网络服务不中断。网络安全就其本质而言是网络上的信息安全。从广义上讲，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，都是网络安全的研究领域。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，两方面相互补充，缺一不可。

1.1.2　网络安全的特征

一个安全的计算机网络应该具备以下几个特征。

（1）可靠性

可靠性是网络系统安全最基本的要求。可靠性主要是指网络系统硬件和软件无故障运行的性能。提高可靠性的具体措施包括提高设备质量，配备必要的冗余和备份，采取纠错、自愈和容错等措施，强化灾害恢复机制，合理分配负荷，保护软、硬件资源不被非法占有，免受病毒的侵害等。

（2）可用性

可用性是指网络信息可被授权用户访问的特性，即网络信息服务在需要时，能够保证授权用户使用。这里包含两个含义：一是当授权用户访问网络时不致被拒绝；二是授权用户访问网络时要进行身份识别与确认，并且对用户的访问权限加以规定的限制。

（3）保密性

保密性是指网络信息不被泄露的特性。保密性是在可靠性和可用性的基础上保证网络信息安全的非常重要的手段。保密性可以保证信息即使泄露，非授权用户在有限的时间内也不能识别真正的信息内容。常用的保密措施包括防监听、防辐射、信息加密和物理保密（限制、隔离、隐蔽、控制）等。

（4）完整性

完整性是指网络信息未经授权不能进行改变的特性，即网络信息在存储和传输过程中不被删除、修改、伪造、乱序、重放和插入等操作，保持信息的原样。影响网络信息完整性的主要因素包括设备故障、误码、人为攻击以及计算机病毒等。

（5）可控性

可控性是指对信息的传播及内容具有控制能力，可以控制授权范围内的信息流向及行为方式。

（6）可审查性

不可抵赖性也称为不可否认性，主要用于网络信息的交换过程，保证信息交换的参与者都不可能否认或抵赖曾进行的操作，类似于在发文或收文的签名和签收的过程。对出现的安全问题提供调查的依据和手段，用户不能抵赖曾做出的行为，也不能否认曾经接到对方的信息。概括起来讲，网络信息安全就是通过计算机技术、通信技术、密码技术和安全技术保护在公用网络中存储、交换和传输信息的可靠性、可用性、保密性、完整性、可控性和可审查性的技术。

1.1.3 网络安全的内容

从技术角度看，网络安全的内容大体包括 4 个方面，如图 1-1 所示。

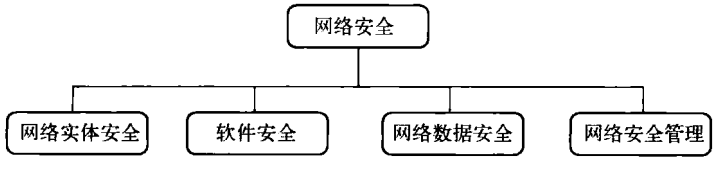


图 1-1　网络安全的内容

（1）网络实体安全

网络实体安全如机房的物理条件、物理环境及设施的安全标准，计算机硬件、附属设备

及网络传输线路的安装及配置等。

（2）软件安全

软件安全包括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。

（3）网络数据安全

网络数据安全包括保护网络信息的数据不被非法存取，保护其完整、一致等。

（4）网络安全管理

网络安全管理包括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、进行风险分析等内容。

从不同的角度来说，网络安全具有不同的含义。从一般用户的角度来说，他们希望涉及个人隐私或商业利益的信息在网络上传输时受到机密性、完整性和真实性的保护，避免其他人或对手利用窃听、冒充、篡改等手段对用户信息的损害和侵犯，同时也希望用户信息不受非法用户的非授权访问和破坏。

从网络运行和管理者角度来说，使用者希望对本地网络信息的访问、读/写等操作受到保护和控制，避免出现病毒、非法存取、拒绝服务和网络资源的非法占用及非法控制等威胁，制止和防御网络“黑客”的攻击。

对安全保密部门来说，他们希望对非法的、有害的或涉及国家机密的信息进行过滤，避免其通过网络泄露，避免由于这类信息的泄密对社会产生危害，给国家造成巨大的经济损失，甚至威胁到国家安全。

从社会教育和意识形态角度来讲，网络上不健康的内容，会对社会的稳定和人类的发展造成阻碍，必须对其进行控制。

1.1.4 网络安全的目标

计算机网络安全不仅要保护计算机网络设备安全，还要保护数据安全等。其特征是针对计算机网络本身可能存在的安全问题，实施网络安全保护方案，以保证计算机网络自身的安全性为目标。

网络安全措施的目标体现在以下几个方面。

1）访问控制（Access Control）：确保会话对方（人或计算机）有权做他所声称的事情。

2）认证（Authentication）：确保会话对方的资源（人或计算机）同他声称的一致。

3）完整性（Integrity）：确保接收到的信息同发送的一致。

4）审计（Accountability）：确保任何发生的交易在事后可以被证实，发信者和收信者都认为交换发生过，即所谓的不可抵赖性（Non - repudiation）。

5）保密（Privacy）：确保敏感信息不被窃听。

所有这些目标同所要传输的信息是密切相关的。

网络信息安全主要包括两个方面：信息存储安全和信息传输安全。

信息存储安全是指信息在静态存放状态下的安全，如是否会被非授权调用等，一般通过设置访问权限、身份识别、局部隔离等措施来保证。针对“外部”的访问、调用而言的访问控制技术是解决信息存储安全的主要途径。

在网络系统中，任何调用指令和任何信息反馈均是通过网络传输实现的，所以网络信息

传输上的安全就显得特别重要。信息传输安全主要是指信息在动态传输过程中的安全。为确保网络信息的传输安全，尤其需要防止以下问题：

1）截获（Interception）。对网上传输的信息，攻击者只需在网络的传输链路上通过物理或逻辑的手段，就能对数据进行非法的截获与监听，进而得到用户或服务方的敏感信息。

2）伪造（Fabrication）。对用户身份仿冒这一常见的网络攻击方式，传统的对策一般采用身份认证方式防护，但是用于用户身份认证的密码在登录时常常是以明文的方式在网络上进行传输的，很容易被攻击者在网络上截获，进而可以对用户的身份进行仿冒，使身份认证机制被攻破。身份认证的密码90%以上是用代码形式传输的。

3）篡改（Modification）。攻击者有可能对网络上的信息进行截获并且篡改其内容（增加、截去或改写），使用户无法获得准确、有用的信息或落入攻击者的陷阱。

4）中断（Interruption）。攻击者通过各种方法，中断用户的正常通信，达到自己的目的。

5）重发（Repeat）。“信息重发”的攻击方式，即攻击者截获网络上的密文信息后，并不将其破译，而是把这些数据包再次向有关服务器（如银行的交易服务器）发送，以实现恶意攻击的目的。

网络安全不仅仅是一个纯技术问题，单凭技术因素确保网络安全是不可能的。网络信息因为其自身的特点，在复制、获取上的便捷性使得网络安全问题成为涉及法律、管理和技术等多方因素的复杂系统问题。

1.1.5 网络安全需求与安全机制

1. 网络安全的需求

1）解决网络的边界安全问题。

2）保证网络内部的安全。

3）实现系统安全及数据安全。

4）建立全网通行的身份识别系统，并实现用户的统一管理。

5）在用户和资源之间进行严格的访问控制。

6）实现信息传输时数据的完整性和保密性。

7）建立一整套审计、记录的机制。

8）融合技术手段和行政手段，形成全局的安全管理。

网络安全机制包括访问控制机制、加密机制、认证交换机制、数字签名机制、业务流分析机制、路由控制机制。

2. 网络安全机制

1）物理层信息安全，主要防止物理通路的损坏、物理通路的窃听和对物理通路的攻击如干扰等。

2）链路层的网络安全需要保证通过网络链路的数据不被窃听。

3）网络层的安全需要保证网络只给授权的用户使用授权的服务，保证网络路由正确，避免被拦截或监听。

4）操作系统安全要求保证用户资料、操作系统访问控制的安全，同时能够对该操作系统上的应用进行审计。

5）应用平台指建立在网络系统之上的应用软件服务，如数据库服务器、电子邮件服务器、Web 服务器等。由于应用平台的系统非常复杂，通常采用多种技术（如 SSL 等）来增强应用平台的安全性。

6）应用系统完成网络系统的最终目的——为用户服务，应用系统的安全与系统设计和实现关系密切。

综上所述，在一般情况下，分布在网络层的安全机制，主要保护网络服务的可用性，解决系统安全问题；分布在应用层的安全机制，主要保护合法用户对数据的合法存取，解决数据安全问题。通过网络层和应用层，集成系统安全和数据安全，可构成立体的网络安全防护体系。通常，网络层的安全措施包括防火墙和安全检测手段，防火墙主要是限制访问，安全检测主要是预防黑客的攻击。应用层的安全措施包括建立全局的电子身份认证系统；实现全局资源的统一管理；为实现数据完整性和数据保密性的信息传输加密；实现通信记录和统计分析等。

1.2 网络拓扑与安全性

拓扑逻辑是构成网络的结构方式，是连接在地理位置上分散的各个节点的几何逻辑方式。拓扑逻辑决定了网络的工作原理及网络信息的传输方法。一旦网络的拓扑逻辑被选定，必定要选择一种适合这种拓扑逻辑的工作方式与信息的传输方式。如果这种选择和配置不当，将为网络安全埋下隐患。事实上，网络的拓扑结构本身就有可能给网络的安全带来问题。

网络可以依照不同的方法进行多种多样的分类。本节按照通常的分类方法——字母顺序法进行分类，重点讨论每一种网络类型涉及的安全问题。注意，网络的类型并不是只能按照某一个标准划分，所以网络可以属于下面的两种或两种以上的类型。

1.2.1 总线网

图 1-2 是一个总线网（Bus Network）的布局，它从网络服务器中引出一根电缆，所有的工作站依次接在电缆的各个节点上。这种网络有时也叫多点网络，它在安全问题上和网状网络有一些相似之处，它的组织性和安全性相对简单一些。如果发生了未经授权的改动，则可知道大约的地点，但具体的位置很难确定。安全性的焦点集中在信息的证实、验证和完整性上。

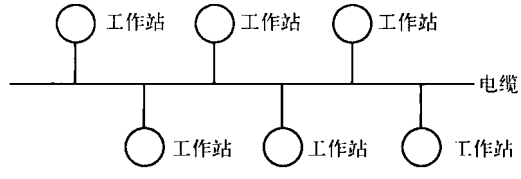


图 1-2 总线网

1.2.2 拨号网

由于交换和拨号功能的加入，本节所述的任何一种类型的网络均可以是拨号网（Dial up Network）。这一特点影响并降低了网络的安全性。对于拨号网络，需要解决下面一些问题：

1）如何决定双方通信时呼出方（给谁记账，如何跟踪，谁被授权发起这次呼叫等）和呼入方（是否能接受被叫用户付费等）的长途电话费。

2）如何证实授权用户的身份（采用口令或其他方法），如何校验（如用反向拨号等）。使用拨号线路来组建计算机网络时，被拨入方难以确认拨号方的身份，容易形成安全漏洞。