高等学校计算机科学与技术教材

计算机网络安全应用基础

杨富国　主 编
于广海　邹良群　李德水　编
陈兰生　尹晓东

清华大学出版社
http://www.tup.tsinghua.edu.cn
北京交通大学出版社
http://press.bjtu.edu.cn

高等学校计算机科学与技术教材

计算机网络安全应用基础

杨富国　主编
于广海　邹良群　李德水
陈兰生　尹晓东　编

清华大学出版社
北京交通大学出版社
·北京·

内 容 简 介

本书共分为11章。主要内容有计算机网络安全概述、网络体系结构与网络协议、黑客攻击方法、计算机病毒及防范、网络安全设备——防火墙、入侵检测、安全漏洞扫描器、口令入侵者、加密技术、用户身份认证技术、网络安全性规划的设计与管理。

本书从安全角度出发，以基本理论为指导，重点介绍网络操作系统的安全设置，其可操作性和实用性较强。通过阅读本书，不仅呆以深刻理解网络操作系统安全机制，而且可以掌握常用网络操作系统的安全配置方法和安全管理技巧。

本书以网络安全管理人员为主要读者群体，同时兼顾广大计算机网络爱好者的需求，是一本进行网络操作系统安全管理的实用教材和必备的重要参考书。

图书在版编目(CIP)数据

计算机网络安全应用基础／杨富国主编；于广海等编. —北京：清华大学出版社；北京交通大学出版社，2005.2

（高等学校计算机科学与技术教材）

ISBN 7-81082-355-8

Ⅰ.计… Ⅱ.①杨… ②于… Ⅲ.计算机网络－安全技术－高等学校－教材 Ⅳ.TP393.08

中国版本图书馆CIP数据核字(2004)第133924号

责任编辑：孙秀翠　　特邀编辑：赵　娟

出 版 者：清华大学出版社　　邮编：100084　　电话：010-62776969

　　北京交通大学出版社　　邮编：100044　　电话：010-51686414

印 刷 者：北京鑫海金澳胶印有限公司

发 行 者：新华书店总店北京发行所

开　　本：185×260　　印张：18　　字数：446千字

版　　次：2005年2月第1版　　2005年2月第1次印刷

书　　号：ISBN 7-81082-355-8/TP·168

印　　数：1～4 000册　　定价：25.00元

编委会成员名单

前　言

当今世界信息技术迅猛发展，人类社会正进入一个信息社会，社会经济的发展对信息资源、信息技术和信息产业的依赖程度越来越大。在信息社会中，信息已成为人类宝贵的资源。近年来 Internet 正以惊人的速度在发展，Internet 技术已经广泛渗透到各个领域。然而，由 Internet 的发展而带来的网络系统的安全问题正变得日益突出，受到越来越多的人的关注。因此，网络安全已成为关系国家安全的重大战略问题。

网络是信息资源得以利用的基础，通过信息网络，商界和政府可以获得显著的效益并开拓新型服务。日益增长的系统依赖性使得国家的经济力量、众多的商业利润、生存能力及政府的职能运作都极大依赖于这些复杂网络的运行可靠性。然而，由于信息网络的脆弱性与对系统依赖性的矛盾，存在着潜在的威胁，这类信息安全威胁使安全事件屡屡发生、波及甚广、危害极大。因此，网络安全是当前一个很重要的研究课题和亟待解决的对象。

本书的组织结构

本书内容共分 11 章，各章内容相对独立，读者可以根据自己的需要，选择阅读相关的章节，如果对前面的内容很熟悉，可以跳过这些主题继续阅读。

第 1 章概述了计算机网络安全的概念、计算机网络系统面临的威胁、网络安全技术策略模型及网络安全的基本措施。

第 2 章简要介绍网络体系结构与网络协议的基本知识，内容包括 OSI 参考模型、TCP/IP 协议，以及端口和网络服务的概念等。

第 3 章讨论黑客攻击方法，主要内容有：弱点扫描型攻击，拒绝服务攻击，分布式拒绝服务攻击和隐藏身份的技术。

第 4 章讲述计算机病毒及防范。从计算机病毒原理与起源到典型的计算机病毒分析；从计算机病毒的分类到常用防病毒软件都做了全面介绍。

第 5 章介绍网络安全设备——防火墙。首先介绍防火墙的基本知识，然后讲述了防火墙的主要功能，防火墙的基本原理和基本类型，最后介绍了防火墙的使用与配置方法。

第 6 章是入侵检测，介绍了入侵检测系统的概念，入侵检测技术，入侵检测系统的弱点和局限性，入侵检测系统面临的挑战，以及入侵检测系统的性能和功能测试，另外还介绍了几种典型的入侵检测系统。

第 7 章介绍安全漏洞扫描器。内容有扫描器的基本概念、主要功能、运行平台和工作方式，同时还介绍了几种常用的扫描器。

第 8 章是“口令入侵者”，介绍了口令入侵者是如何工作的，口令破解的过程及各种“口令入侵者”的常用程序。

第 9 章讨论加密技术。内容包括数据加密机制，对称与非对称加密机制，混合加密机制，DES 加密，RSA 加密及其他常用的加密算法，最后介绍了常用加密技术的应用。

第 10 章是用户身份认证技术，介绍了用户身份认证的必要性；数字签名的概念、特点、算法和数字签名的文件传输过程。另外还介绍了 Kerberos 认证的原理和特点。

第 11 章讲述网络安全性规划的设计与管理，网络系统安全性规划的主要内容、设计步骤、基本原则；网络系统的安全管理的内容、实现和网络系统安全事件的判定、处理原则和处理方法。

本书的读者对象

本书适合以下读者对象：

- 信息安全专业本科高年级学生；
- 计算机、通信及相关专业的本科生和硕士生；
- 网站设计开发和维护的程序员、分析员和项目管理人员；
- 需要建立、实现和管理因特网和企业内部网的网络管理人员；
- 对网络操作系统安全关注的技术人员；
- 关注网络安全的非专业人员和网络爱好者。

编　者

2005 年 2 月

目　　录

第 1 章　计算机网络安全概述

1.1　网络安全的概念

随着计算机应用的网络化和全球化，人们日常生活中的许多活动将逐步转移到网络上来。主要原因是由于网络交易的实时性、方便性、快捷性及低成本性。Internet 最大的优点是消除了地域上的障碍，使得地球上的每一个人均可方便地与另一端的用户通信。企业用户可以通过网络进行信息发布、广告、营销、娱乐和客户支持等，同时可以直接与商业伙伴进行合同签订和商品交易，用户通过网络可以获得各种信息资源和服务，如购物、娱乐、求职、教育、医疗、投资等。

信息技术的使用给人们的生活、工作带来了数不尽的便捷和好处。然而，计算机信息技术也和其他科学技术一样是一把双刃剑，当大部分人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。他们非法侵入他人的计算机系统窃取机密信息、篡改和破坏数据，给社会造成了难以估量的巨大损失。据统计，全球约 20 秒钟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，约有 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。

网络安全是一个关系国家安全和主权、社会的稳定、民族文化的 e 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。

网络安全从其本质上来讲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，系统连续、可靠、正常地运行，网络服务不中断。从广义来说，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，管理方面则侧重于防止内部人为因素对信息网络造成的损害。如何更有效地保护重要的信息、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。

计算机网络的安全不是绝对的。安全是有成本的，而且也有时间限制。因此，这里所谈的安全是指花多大成本在多长时间之内可以保证计算机网络安全。安全问题的解决依赖于法律、管理机制、技术保障等多方面相互协调配合，形成一个完整的安全保障体系。

1.1.1　网络安全的定义

国际标准化组织（ISO）对计算机系统安全的定义是：为数据处理系统建立和采用的技术和管理的安全保护，保护计算机硬件、软件和数据不因偶然和恶意的原因遭到破坏、更改

和泄露。由此可以将计算机网络的安全理解为：通过采用各种技术和管理措施，使网络系统正常运行，从而确保网络数据的可用性、完整性和保密性。所以，建立网络安全保护措施的目的是确保经过网络传输和交换的数据不会发生增加、修改、丢失和泄露等。

1.1.2　网络安全的内容

计算机网络安全涉及个人权益、企业生存、金融风险防范、社会稳定和国家的安全，它是物理安全、网络安全、数据安全、信息内容安全、信息基础设施安全与公共、国家信息安全的总和。

1. 物理安全

物理安全是指用来保护计算机网络中的传输介质、网络设备和机房设施安全的各种装置与管理手段。物理安全包括防盗、防火、防静电、防雷击和防电磁泄漏等方面的内容。

物理上的安全威胁主要涉及对计算机或人员的访问。可用于增强物理安全的策略有很多：将计算机系统和关键设备布置在一个安全的环境中，销毁不再使用的敏感文档，保持密码和身份认证部件的安全性，锁住便携式设备等。物理安全的实施更多的是依赖于行政的干预手段并结合相关技术。如果没有基础的物理保护，例如带锁的开关柜、数据中心等，物理安全是不可能实现的。

2. 逻辑安全

计算机网络的逻辑安全主要通过用户身份认证 、访问控制、加密、安全管理等方法来实现。

● 用户身份认证：身份证明是所有安全系统不可或缺的一个组件。它是区别授权用户和入侵者的惟一方法。为了实现对信息资源的保护，并知道何人试图获取网络资源的访问权，任何网络资源拥有者都必须对用户进行身份认证。当使用某些更尖端的通信方式时，身份认证特别重要。

● 访问控制：访问控制是制约用户连接特定网络、计算机与应用程序、获取特定类型数据流量的能力。访问控制系统一般针对网络资源进行安全控制区域划分，实施区域防御的策略。在区域的物理边界或逻辑边界使用一个许可或拒绝访问的集中控制点。

● 加密：即使访问控制和身份验证系统完全有效，在数据信息通过网络传送时，企业仍可能面临被窃听的风险。事实上，低成本和连接的简便性已使 Internet 成为企业内和企业间通信的一个极为诱人的媒介。同时，无线网络的广泛使用也在进一步加大网络数据被窃听的风险。加密技术用于针对窃听提供保护。它通过使信息只能被具有解密数据所需密钥的人员读取来提供时信息的安全保护。它与第三方是否通过 Internet 截取数据包无关，因为数据即使在网络上被第三方截取，它也无法获取信息的本义。这种方法可在整个企业网络中使用，包括在企业内部（内部网）、企业之间（外部网）或通过公共 Internet 在虚拟专用网络（VPN）中传送私人数据。加密技术主要包括对称式和非对称式密钥，这两种方式都有许多不同的密钥算法来实现，在此不一一详述。

● 安全管理：安全系统应当允许由授权人进行监视和控制。使用验证的任何系统都需要

某种集中授权来验证这些身份，而无论它是 UNIX 主机、Windows NT 域控制器还是 Novell Directory Services（NDS）服务器上的 /etc/passwd 文件。由于能够查看历史记录，如突破防火墙的多次失败尝试，安全系统可以为那些负责保护信息资源的人员提供宝贵的信息。一些更新的安全规范（如 IPSec）需要包含策略规则数据库。要使系统正确运行，就必须管理所有这些要素。但是，管理控制台本身也是安全系统的另一个潜在故障点。因此，必须确保这些系统在物理上得到安全保护，并确保对管理控制台的任何登录进行验证。

3. 操作系统安全

计算机操作系统担负着自身庞大的资源管理、频繁的输入输出控制，以及不可间断的用户与操作系统之间的通信任务。由于操作系统具有“一权独大”的特点，所有针对计算机和网络的入侵及非法访问都是以攫取操作系统的最高权限作为入侵的目的。因此，操作系统安全的内容就是采用各种技术手段和采取合理的安全策略，降低系统的脆弱性。

与过去相比，如今的操作系统性能更先进、功能更丰富，因而对使用者来说更有用，但同时也增加了安全漏洞。要减少操作系统的安全漏洞，需要对操作系统予以合理配置、管理和监控。做到这点的秘诀在于集中、自动管理机构（企业）内部的操作系统安全，而不是分散、人工管理每台计算机。

实际上，如果不集中管理操作系统安全，相应的成本和风险就会非常高。我们所知道的安全入侵事件，一半以上缘于操作系统根本没有合理配置，或者没有经常核查及监控。操作系统都是以默认安全设置来配置的，因而极容易受到攻击。

那些人工更改了服务器安全配置的用户，把技术支持部门的资源过多地耗于帮助用户处理口令查询上，而不是处理更重要的网络问题。考虑到这些弊端，难怪许多管理员任由服务器操作系统以默认状态运行。这样一来，服务器可以马上投入运行，但这却大大增大了安全风险。

现有技术可以减轻管理负担。要加强机构（企业）网络内操作系统的安全，需要做到以下三方面。

首先，对网络上的服务器进行配置应该在一个地方进行，大多数用户大概需要数十种不同的配置。然后，这些配置文件的一个镜像或一组镜像在软件的帮助下可以通过网络下载。软件能够自动管理下载过程，不需要为每台服务器手工下载。此外，即使有某些重要的配置文件，也不应该让本地管理员对每台服务器分别配置，这样做是很危险的，最好的办法就是一次性全部设定。一旦网络配置完毕，管理员就要核实安全策略的执行情况，定义用户访问权限，确保所有配置正确无误。你可以在网络上运行（或远程运行）代理程序，不断监控每台服务器。代理程序不会干扰正常操作。

其次，账户需要加以集中管理，以控制对网络的访问，并且确保用户拥有合理访问机构（企业）资源的权限。策略、规则和决策应在一个地方进行，而不是在每台计算机上进行，然后为用户系统配置合理的身份和许可权。身份生命周期管理程序可以自动管理这一过程，减少手工过程带来的麻烦。

第三，操作系统应该配置成能够轻松、高效地监控网络活动，可以显示谁在进行连接、谁断开了连接，以及发现来自操作系统的潜在安全事件。

4. 联网安全

联网安全指的是保证计算机联网使用后的操作系统安全运行和计算机内部信息的安全。联网安全性可以通过以下3个方面的安全服务来达到。

① 联网计算机用户必须很好地采取措施，确保自己计算机不会受到层出不群、传播迅速的计算机病毒的侵袭。

② 访问控制服务：用来保护计算机和联网资源不被非授权使用。

③ 通信安全服务：用来认证数据机密性与完整性，以及通信的可信赖性。

5. 其他形式的安全

多数计算机系统的价值是由系统的性能、安全管理所需的时间、实用性和复杂性决定的。许多政府系统设有专职的“安全管理员”，他们的工作是管理和监控计算机设备的安全运转。许多大学极为关心网络安全与计算机黑客攻击的威胁，因为他们是计算机黑客攻击的目标。然而，由于缺少经验，多数的商业机构在计算机安全方面非常脆弱。

安全工作有许多种形式：比如操作系统被设计得能阻止用户读取未授权数据；使操作系统有报警和日志功能；在操作人员接触秘密数据前，进行全面的安全教育。最后也许是物理安全形式，如安装锁和报警系统以防设备和存储介质失窃。

在安全的环境中，许多类型的安全工作是互相加强的，防止入侵或者最大限度地减少损失。

1.1.3　网络安全的基本需求

计算机网络安全是随着计算机网络的发展和广泛应用而产生的，是计算机安全的发展与延伸。用系统的观点，可以把计算机网络看成一个扩大了的计算机系统，因此许多关于计算机安全的概念和机制也同样适用于计算机网络。

虽然网络安全同单个计算机安全在目标上并没有本质区别，但由于网络环境的复杂性，网络安全比单个计算机安全要复杂得多。首先，网络资源的共享范围更加宽泛，难以控制。共享既是网络的优点，也是风险的根源，它会导致更多的用户（友好与不友好的）从远地访问系统，使数据遭到拦截与破坏，以及对数据、程序和资源的非法访问。其次，网络支持多种操作系统，这使网络系统更为复杂，安全管理与控制更为困难。第三，网络的扩大使网络的边界和网络用户群变得不确定，对用户的管理较计算机单机困难得多。第四，单机用户可以从自己的计算机中直接获取敏感数据，但网络中用户的文件可能存放在远离自己的服务器上，在文件传送过程中，可能经多个主机的转发，因而沿途可能受到多处攻击。第五，由于网络路由选择的不固定性，很难确保网络信息在一条安全通道上传输。

基于对上述5个特点的分析可知，保证计算机网络的安全，就是要保护网络信息在存储和传输过程中的保密性、完整性、可用性、真实性和可控性。

1. 数据的保密性

数据的保密性是网络信息不被泄露给非授权的用户和实体，信息只能以允许的方式供授权用户使用的特性。也就是，保证只有授权用户可以访问数据，而限制其他人对数据的访

问。在网络环境下，保密性不仅应包括数据存储保密性，而且还应包括数据传输保密性。保密性是在可靠性和可用性的基础上，保障网络信息安全的重要手段。

2. 数据的完整性

数据的完整性是网络信息未经授权不能进行改变的特性，即网络信息在存储或传输过程中保持不被偶然或蓄意地删除、修改、伪造、乱序、重放、插入等破坏和丢失的特性。完整性是一种面向信息的安全性，其目的是要保持信息的原貌，使信息处于一种完整和未受损害的状态，即信息的正确生成、存储和传输，不会因有意或无意的事件，在存储或传输时被改变或丢失。

完整性与保密性不同。保密性要求信息不被泄露给未授权的人，而完整性则要求信息不会受到各种原因的破坏。影响网络信息完整性的主要因素有：设备故障和失效、误码、人为攻击、计算机病毒和自然灾害等。信息完整性的丧失会直接影响到信息的可用性。

3. 数据的可用性

数据的可用性是网络信息可被授权实体访问并按需求使用的特性。即需要网络信息服务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。可用性是网络信息系统面向用户的安全性能。网络信息系统最基本的功能是为用户提供服务，而用户的需求是随机的、多方面的，有时还有时间要求。可用性一般用系统正常使用时间和整个工作时间之比来度量。保证信息可用，首先要保证信息是完整的，其次要保证系统是正常运转的，网络上不会出现严重的阻塞，以便用户请求信息时，能及时地获取之。

网络可用性对用户的影响，包括合法的用户不能正常访问网络的资源、有严格时间要求的服务不能得到及时的响应。影响网络可用性的因素包括人为和非人为两种。前者有非法占用网络资源，切断或阻塞网络通信，通过病毒、蠕虫或拒绝服务攻击降低网络性能，甚至使网络瘫痪；后者有灾害事故（火灾、水灾、雷击）和系统死锁、系统故障等。

4. 数据的可控性

数据的可控性是控制授权范围内的信息流向和行为方式的特性，如对信息的访问、传播及内容具有控制能力。首先，系统要能够控制谁能够访问系统或网络上的数据，以及如何访问，即是否可以修改数据还是只能读取数据。这要通过采用访问控制等授权方法来实现。其次，即使拥有合法的授权，系统仍需要对网络上的用户进行验证。通过握手协议和口令进行身份验证，以确保他确实是所声称的那个人。最后，系统还要将用户的所有网络活动记录在案，包括网络中计算机的使用时间、敏感操作和违法操作等，为系统进行事故原因查询、定位，事故发生前的预测、报警，以及为事故发生后的实时处理提供详细、可靠的依据或支持。审计对用户的正常操作也有记载，可以实现统计、计费等功能，而且有些诸如修改数据的“正常”操作恰恰是攻击系统的非法操作，同样需要加以警惕。

5. 数据的真实性

数据的真实性又称不可抵赖性或不可否认性。在网络信息系统的信息交互过程中，确信