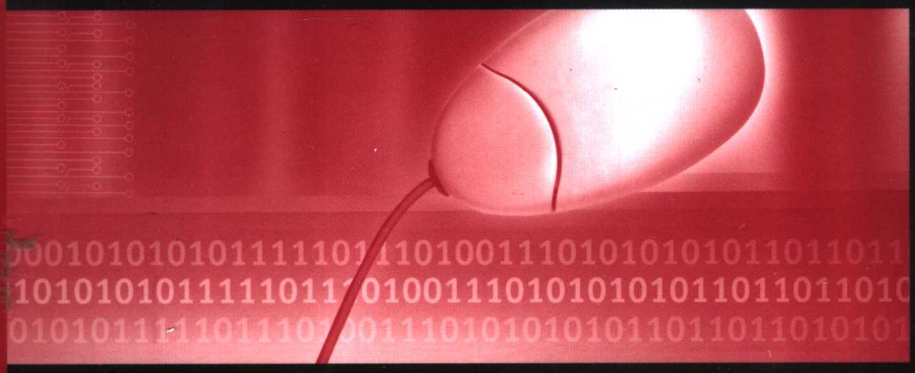
网·络·安·全·实·用·丛·书

PRACTICAL NETWORK SECURITY TECHNOLOGY



网络安全技术与应用

赵安军 曾应员 徐邦海 常春藤 编著

- 作者多年教学与科研工作经验总结
- 概念明晰，实例丰富，注重**技能训练**
- 适合作为**应用型院校教材**
- 简明易懂的写作风格，方便读者**自学**

人民邮电出版社
POSTS & TELECOM PRESS

网络安全实用丛书

网络安全技术与应用

赵安军　曾应员　徐邦海　常春藤　编著

人民邮电出版社

北　京

图书在版编目（CIP）数据

网络安全技术与应用/赵安军等编著. —北京：人民邮电出版社，2007.7
（网络安全实用丛书）
ISBN 978-7-115-16012-6

Ⅰ. 网… Ⅱ. 赵… Ⅲ. 计算机网络—安全技术 Ⅳ. TP393.08

中国版本图书馆 CIP 数据核字（2007）第 043620 号

内 容 提 要

本书共分 3 个部分。第 1 部分为网络安全基础篇，主要讨论了网络安全的基础知识，并从网络协议角度出发，阐述了当今计算机网络中存在的安全威胁；第 2 部分为密码学基础，简要介绍了网络安全中涉及的各种密码技术；第 3 部分为网络安全应用实践，也是本书的重点内容，主要介绍了网络安全实践中的一些比较重要的产品及其技术应用。

全书共分 11 章。其中第 1 章和第 2 章介绍了网络安全基础知识；第 3 章简要介绍了密码学基础；剩余的 8 章主要对现有的网络安全技术，包括身份认证、防火墙技术、入侵检测技术、加密技术、公钥基础设施、虚拟专用网络、恶意代码和病毒防治以及无线网络所涉及的网络安全技术进行了详细的讨论。

本书可以作为高等院校信息安全、通信、计算机等专业的本科生和研究生教材，也可以作为网络安全工程师、网络管理员的参考用书，或作为网络安全培训教材。

网络安全实用丛书

网络安全技术与应用

◆ 编　　著　赵安军　曾应员　徐邦海　常春藤
责任编辑　刘　洋

◆ 人民邮电出版社出版发行　　北京市崇文区夕照寺街 14 号
邮编　100061　　电子函件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
三河市海波印务有限公司印刷
新华书店总店北京发行所经销

◆ 开本：787×1092　1/16
印张：16.25
字数：385 千字　　2007 年 7 月第 1 版
印数：1－3 500 册　　2007 年 7 月河北第 1 次印刷

ISBN 978-7-115-16012-6/TN

定价：28.00 元

读者服务热线：(010)67129258　印装质量热线：(010)67129223

前 言

Forward

随着计算机网络应用的广泛深入，网络安全问题变得日益复杂和突出。网络的资源共享、信息交换和分布处理提供的良好环境，使得网络深入到社会生活的各个方面，逐步成为国家和政府机构运转的命脉和社会生活的支柱。这一方面提高了工作效率，另一方面却由于网络自身的复杂性和脆弱性，使其受到威胁和攻击的可能性大大增加。众所周知，因特网是世界上最大的计算机网络，它连接了全球不计其数的网络与计算机，同时因特网也是世界上最开放的系统，任何地方的计算机，只要遵守共同的协议即可加入其中。因特网的特点就是覆盖的地理范围广，资源共享程度高。由于因特网网络协议的开放性，系统的通用性，无政府的管理状态，使得因特网在大量地传播信息的同时，也面临着不可预测的威胁和攻击。随着网络技术的发展，网络攻击的手段也变得越来越巧妙，越来越多样化。计算机网络的开放性和信息共享促进了网络的飞速发展，但也正是这种开放性以及计算机本身安全的脆弱性，导致了网络安全方面的诸多漏洞。可以说，网络安全问题将始终伴随着因特网的发展而存在。所以，网络的安全性同网络的性能、可靠性和可用性一起，成为组建、运行网络不可忽视的问题。

网络安全是一个综合的交叉学科领域，涉及数学、信息、通信和计算机等诸多学科的长期知识积累和最新发展成果。本书是一本系统论述网络安全理论与技术的书籍，书中总结了常见的网络安全理论与技术，主要内容包括：网络安全基础知识，主要讨论了网络安全的基本知识，并从网络协议角度出发，阐述了当今计算机网络中存在的安全威胁；密码学基础，简要介绍了网络安全中涉及的各种密码技术；网络安全应用实践，也是本书的重点内容，主要介绍了网络安全实践中的一些比较重要的产品及其技术应用。

全书共分 11 章。其中第 1 章和第 2 章介绍了网络安全基础知识；第 3 章简要地介绍了密码学基础。剩余的 8 章主要对现有的网络安全技术，包括身份认证、防火墙技术、入侵检测技术、加密技术、公钥基础设施、虚拟专用网络、恶意代码和病毒防治以及无线网络所涉及的网络安全技术进行了详细的讨论。

由于本书涉及的技术领域较广，而且编写较为仓促，尽管几位作者已是付出诸多努力，但最终书稿无论在结构还是内容方面，尚有许多不尽如人意的地方，欢迎读者批评指正。读者可与本书的责任编辑联系，联系邮箱为：liuyang@ptpress.com.cn。欢迎您提出自己的宝贵意见与建议。

目 录

CONTENTS

第 1 章
网络安全概述

CHAPTER 1

随着网络技术的飞速发展和网络时代的到来，网络安全问题变得越来越严重。现在，每年关于网络安全问题的报道层出不穷，由于网络不安全造成的损失越来越大，人们为解决网络安全问题投入的资金也越来越多。

网络安全问题严重影响了人们的生活和工作，以至整个国家的安全。它可能对国家的重大部门造成严重的后果，如金融部门、政府机构、军事设施、公共基础设施等。现在，由于大多数部门都实现了网络信息系统，这就为网络安全问题提供了可能产生的土壤。

本章主要介绍网络安全的一些基本概念，主要包括：网络安全的发展、威胁与防护、网络安全策略、网络攻击的种类和常见形式以及网络安全的体系结构。

1.1 网络安全的发展

1.1.1 网络安全的概念

信息技术的使用给人们的生活和工作带来了便捷，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了工作效率，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，造成了难以估量的损失。据统计，全球约 20s 就有一次计算机入侵事件发生；约 1/4 的网络防火墙被突破；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、社会稳定、民族文化的继承和发扬等的重要问题。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、数论和信息论等多种学科。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、更改或泄露；系统连续、可靠、正常地运行；网络服务不中断。从广义上来说，凡是涉及网络中信息的保密性、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破坏。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中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，本章所说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、管理机制和技术保障等多方面相互协调和配合，形成一个完整的安全保障体系。

1.1.2 网络安全的需求

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。可以用系统的观点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。第一，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，又是风险的根源，它会导致更多的用户（友好与不友好的）远程访问系统，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。第二，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、可控性和真实性。

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。也就是说，保证只有授权用户才可以访问数据，而限制其他人对数据的访问。

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、重放及插入等破坏和丢失的特性。数据的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。要保证信息可用，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。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等。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，甚至使网络瘫痪等；后者有灾害事故（火灾、水灾、雷击等）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网络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，即是只能读取数据还是可以修改数据，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。通过握手协议和密码进行身份验证，以确保其确实是所声称的那个用户。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，指在网络信息系统的信息交互过程中参与者的真实同一性，即所有参与者都不可能否认或抵赖曾经完成的操作和承诺。利用信息源证据可以防止“发信方”否认已发送信息，利用递交接收证据可以防止“收信方”事后否认已经接收信息。必须以某种方式对通信双方进行确认和鉴别，以防止假冒和欺骗。当计算机网络用于电子商务和军事领域时，对用户账号的确认和鉴别是十分重要的问题。

1.1.3 网络安全的发展趋势

从管理和技术两个维度推进网络安全工作不仅是现阶段解决好网络安全问题的需要，也是今后网络安全发展的必然趋势。

从技术角度而言，可以采用以下技术。

（1）逻辑隔离技术。以防火墙为代表的逻辑隔离技术将逐步向大容量、高效率、基于内容的过滤技术，以及与入侵监测和主动防卫设备、防病毒网关设备联动的方向发展，形成具有统计分析功能的综合性网络安全产品。

（2）防病毒技术。防病毒技术将逐步实现由单机防病毒向网络防病毒方式过渡，而防病毒网关产品的病毒库更新效率和服务水平，将成为今后防病毒产品竞争的核心要素。

（3）身份认证技术。80%的攻击发生在内部，而不是外部。内部网的管理和访问控制相对外部的隔离来讲要复杂得多。在一般人的心目中，基于 Radius 的鉴别、授权和管理（AAA）系统是一个非常庞大的安全体系，它主要用于大的网络运营商，企业内部不需要这么复杂的东西。这种看法越来越过时，实际上，组织内部网同样需要一套强大的 AAA 系统。根据 IDC 的报告，内部的 AAA 系统是目前安全市场增长最快的部分。

（4）入侵监测和主动防卫技术。入侵监测和主动防卫（IDS、IPS）作为一种实时交互的监测和防卫手段，正越来越多地被政府和企业应用，但如何解决监测效率和错报、漏报率的

矛盾，需要继续进行研究。

（5）加密和虚拟专用网技术。在一个单位中，员工外出、移动办公、单位和合作伙伴之间、分支机构之间通过公用的互联网通信是必需的，因此，加密通信和虚拟专用网（VPN）有很大的市场需求。IPSec 已经成为市场的主流和标准。

（6）网管。网络安全越完善，体系架构就越复杂。管理网络的多台安全设备需要集中网管。集中网管是目前安全市场的一大趋势。

从管理角度讲，应遵循以下原则。

（1）整体考虑，统一规划。

网络安全取决于系统中最薄弱的环节。“一点突破，全网突破”，单个系统考虑安全问题并不能真正有效地保证安全，需要从整体 IT 体系层次建立网络安全架构，整体考虑，全面防护。

（2）战略优先，合理保护。

网络安全工作应服从组织信息化建设总体战略，滚动式实现系统安全体系的统一。在此前提之下，追求适度安全，合理保护组织信息资产，安全投入与资产的价值应相匹配。

（3）集中管理，重点防护。

统筹设计安全总体架构，建立规范、有序的安全管理流程，集中管理各系统的安全问题，避免安全“孤岛”和安全“短板”。

（4）七分管理，三分技术。

管理是网络安全的核心，技术是安全管理的保证。只有制定完善的规章制度、行为准则并和安全技术手段合理结合，网络系统的安全才会得到最大限度的保障。

1.2 安全威胁与防护

计算机网络系统面临的安全威胁有：网络中的主机可能会受到非法入侵者的攻击；网络中的敏感数据有可能泄露或被修改；从内网向公网传送的信息可能被他人窃听或篡改等。造成网络安全威胁的原因可能是多方面的，有的来自外部，有的可能来自机构（企业）网络内部。攻击者主要是利用了 TCP/IP 协议的安全漏洞和操作系统的安全漏洞来实施攻击。归纳起来，计算机网络系统的安全威胁常表现出以下特征：窃听、重传、伪造、篡改、拒绝服务攻击、行为否认和传播病毒等。

安全防护就是采用一切手段保护信息系统的保密性、完整性、可用性、可控性和不可否认性。防护是预先阻止可以发生攻击的条件的产生，让攻击者无法顺利入侵。防护可以减少大多数的入侵事件，因此，它是网络安全中最重要的一个环节。

1.2.1 安全威胁

威胁是一种对组织及其资产构成潜在破坏的可能性因素，是客观存在的。威胁可以通过威胁主体、资源、动机和途径等多种属性来描述。造成威胁的因素可分为人为因素和环境因素。根据威胁的动机，人为因素又可分为恶意和非恶意两种。环境因素包括自然界不可抗拒的因素和其他物理因素。威胁作用的形式可能是对信息系统直接或间接的攻击，在机密性、

完整性或可用性等方面造成损害，也可能是偶发的或蓄意的事件。

在对威胁进行分类前，应考虑威胁的来源。如表 1-1 所示，列出了一种威胁来源的分类方法。

表 1-1 威胁来源列表

来　源	描　述
环境因素	断电、静电、灰尘、潮湿、温度、鼠蚁虫害、电磁干扰、洪灾、火灾、地震等环境条件或自然灾害，意外事故或软件、硬件、数据、通信线路方面的故障
恶意人员	不满的或有预谋的内部人员对信息系统进行恶意破坏，采用自主或内外勾结的方式盗窃机密信息或进行篡改，以获取利益；外部人员利用信息系统的脆弱性，对网络或系统的机密性、完整性和可用性进行破坏，以获取利益或炫耀能力
非恶意人员	内部人员由于缺乏责任心，或者由于不关心和不专注，或者没有遵循规章制度和操作流程而导致故障或信息损坏；内部人员由于缺乏培训，专业技能不足，不具备岗位技能要求而导致信息系统故障或被攻击

对威胁进行分类的方式有多种，针对表 1-1 所示的威胁来源，可以根据其表现形式将威胁分类，如表 1-2 所示。

表 1-2 一种基于表现形式的威胁分类表

种　类	描　述	威 胁 子 类
软硬件故障	由于设备硬件故障、通信线路中断、系统本身或软件缺陷造成对业务实施、系统稳定运行的影响	设备硬件故障、传输设备故障、存储媒体故障、系统软件故障、应用软件故障、数据库软件故障、开发环境故障
物理环境影响	断电、静电、灰尘、潮湿、温度、鼠蚁虫害、电磁干扰、洪灾、火灾、地震等环境问题或自然灾害	
无作为或操作失误	由于应该执行而没有执行相应的操作，或无意地执行了错误的操作，对系统造成的影响	维护错误、操作失误
管理不到位	安全管理无法落实，不到位，造成安全管理不规范，或者管理混乱，从而破坏信息系统正常有序运行	
恶意代码和病毒	具有自我复制、自我传播能力，对信息系统构成破坏的程序代码	恶意代码、木马后门、网络病毒、间谍软件、窃听软件
越权或滥用	通过采用一些措施，超越自己的权限访问了本来无权访问的资源，或者滥用自己的职权，做出破坏信息系统的行为	
网络攻击	利用工具和技术、如侦察、密码破译、安装后门、嗅探、伪造和欺骗、拒绝服务等手段，对信息系统进行攻击和入侵	网络探测和信息采集、漏洞探测、嗅探（账户、密码、权限等）、用户身份伪造和欺骗、用户或业务数据的窃取和破坏、系统运行的控制和破坏
物理攻击	通过物理的接触造成对软件、硬件和数据的破坏	物理接触、物理破坏、盗窃
泄密	信息泄露给不应了解的他人	内部信息泄露、外部信息泄露
篡改	非法修改信息，破坏信息的完整性，使系统的安全性降低或信息不可用	篡改网络配置信息、系统配置信息、安全配置信息、用户身份或业务数据信息
抵赖	不承认收到的信息和所做的操作与交易	原发抵赖、接收抵赖、第三方抵赖

1.2.2 安全防护措施

安全防护分为系统安全防护、网络安全防护和信息安全防护。系统安全防护指的是操作

系统的安全防护，即各种操作系统的安全配置、使用和补丁等；网络安全防护指的是网络管理的安全以及网络传输的安全；信息安全防护指的是保证网络中数据的保密性、完整性和可用性。下面介绍可用于安全防护的相关技术与措施。

1．风险评估——缺陷扫描

为了实施网络防护，首先需要知道网络在哪些方面需要防护。扫描器在本质上是一种程序，用来检测和评估网络中某台主机的安全状况，是找出防护对象的一种工具。按照功能的强弱，它大致可以划分为两类：TCP 端口扫描器和普通扫描器。

真正的扫描器是 TCP 端口扫描器，这种程序可以选择 TCP/IP 端口和服务，如 Telnet 或 FTP，并记录目标的回答。通过这种方法，可以搜集到关于目标主机的有用信息，如一个匿名用户是否可以登录等。

普通扫描器仅仅是 UNIX 网络应用程序，这些程序一般用于观察某一服务是否正在一台远程计算机上正常工作，它们不是真正的扫描器，但也可以用于收集目标主机的信息。

所以，扫描器就是自动检测远程或本地主机安全性弱点的程序。通过使用一个扫描器，中国的用户几乎可以不留痕迹地发现远在日本的一台服务器的安全性弱点。Internet 本身是一个非常大的资源库，现代“入侵者”面临的问题是如何快速高效地找出那些目标，扫描器无疑非常适合这一用途。同时，扫描器还可以对目标主机进行分析，从而发现其潜在的漏洞。所以，在 Internet 安全领域，扫描器是最出名的破解工具。一个好的 TCP 端口扫描器的价值更是无法估量。

尽管扫描器能够发现目标主机某些内在的弱点，而这些弱点可能是破坏目标主机安全性的关键性因素。但是，要做到这一点，就必须了解如何识别漏洞。由于扫描器本身就是出自黑客之手，不像一般的商业软件，许多扫描器没有提供多少指南手册和指令，因此理解数据并能解释数据非常重要。

最后，讨论一下扫描器的合法性问题。总的来说，扫描器的使用是合法的，至少根据中国目前的法律规定，开发、设计、公布及使用扫描器在法律上还没有被明确地规定为非法。安全工作人员和开发人员经常设计、编写、公布扫描器，以便系统管理员能够检查自己系统的弱点。然而，尽管拥有和使用扫描器不违法，但如果不是系统管理员，却使用扫描器检查目标主机，将遇到目标主机管理员的强烈反对。而且，某些扫描器在调查远程服务时具有侵略性，未经授权而使用这些扫描器会被认为是非法进入计算机网络。

2．访问控制及防火墙

访问控制策略隶属于系统安全策略，它迫使在计算机系统和网络中自动地执行授权。对于不同的权限分别映射不同的访问控制策略。如基于身份的策略，该策略允许或者拒绝对明确区分的个体或群体进行访问；基于任务的策略，它是基于身份的策略的一种变形，它给每一个实体分配任务，并基于这些任务来使用授权规则；多等级策略，它是基于信息敏感性的等级及工作人员许可证等级而制定的一般规则的策略。

访问控制策略有时也被分为指令性访问控制策略和选择性访问控制策略两类。指令性访问控制策略是由安全区域权力机构强制实施的，任何用户都不能回避它；指令性安全策略在军事上和其他政府机密环境中最为常用。选择性访问控制策略为一些特殊用户提供了对资源（如信息）的访问权，这些特殊用户可以利用此权限控制对资源的访问。

在机密环境中，无条件访问控制策略用于强制执行最小权益策略（按主体执行任务所需