21世纪全国应用人才培养规划教材

网络安全基础教程

WANGLUO ANQUAN JICHU JIAOCHENG

李 艇 编著

北京大学出版社
PEKING UNIVERSITY PRESS

21 世纪全国应用人才培养规划教材

网络安全基础教程

李 艇 编著

北京大学出版社
PEKING UNIVERSITY PRESS

内 容 提 要

在计算机网络发展过程中，网络安全技术是理论性和实践性都很强的一个新的发展方向和研究领域。本书对于网络安全基础、网络安全技术、操作系统的安全性等进行了较全面的介绍，并以任务驱动的方式，介绍网络安全工具的使用，使学生能够对 Windows 平台和 Linux 平台的安全管理问题进行初步的分析和解决。

通过本书的学习，读者可以掌握计算机网络安全的基本概念，熟悉现行的网络安全技术应用。本书适合应用本科和高职高专院校的计算机专业、电子商务专业及相关专业的学生使用。

图书在版编目（CIP）数据

网络安全基础教程/李艇编著. —北京：北京大学出版社，2006.1
（21 世纪全国应用人才培养规划教材）
ISBN 7-301-09940-1

I. 网… II. 李… III. 电子商务－高等学校：技术学校－教材 IV. FT13.36

中国版本图书馆 CIP 数据核字（2005）第 132715 号

书　　名：网络安全基础教程
著作责任者：李艇　编著
责 任 编 辑：王登峰
标 准 书 号：ISBN 7-301-09940-1/TP・0827
出　版　者：北京大学出版社
地　　址：北京市海淀区成府路 205 号　100871
电　　话：邮购部 62752015　发行部 62750672、编辑部 62765126
网　　址：http://cbs.pku.edu.cn
电 子 信 箱：xxjs@pup.pku.edu.cn
印　刷　者：北京飞达印刷有限责任公司
发　行　者：北京大学出版社
经　销　者：新华书店
787 毫米×980 毫米　16 开本　14.25 印张　307 千字
2006 年 1 月第 1 版　2006 年 1 月第 1 次印刷
定　　价：32.00 元（含光盘）

前　言

Internet 的发展使信息安全的概念发生了根本性的变化。信息安全从单机扩展到网络连接的世界范围，同时，安全技术也得到新的发展，其内容极为丰富，是我们从事计算机应用工作的人员应熟练掌握的一门技术。

另外，随着网络技术及其应用的深入和普及，电子商务、电子政务的开展、实施和应用，信息安全已经不再仅仅是科学研究人员和少数黑客的专利，日益庞大的网络用户群同样需要掌握信息安全知识。只有这样，才有可能构筑属于全社会的信息安全体系。

网络安全是指计算机和网络本身可能存在的安全问题，其内容包括计算机物理安全、系统安全、数据库安全、网络设备安全、网络服务安全等。

目前，无论企事业单位，还是 IT 运营公司，都迫切需要能够从事网络安全管理技术的人才。为适应这一需求，许多高校在一些学科中已经开设网络安全技术方面的课程。

本书是针对应用本科的特点而组织编写的。除了较完整的基础理论介绍外，通过一系列的相关实训以提高学生对网络安全管理方面的技能和解决实际问题的能力，为从事网络安全维护方面的应用打下良好的基础。

本书包括第 1 章网络安全概述、第 2 章网络安全技术、第 3 章基于公钥的安全服务基础设施 PKI、第 4 章防火墙技术、第 5 章 Windows 2000 系统安全和第 6 章 Linux 操作系统安全共六章，并提供教学光盘。本书选用了免费版的网络安全工具作为教学实训软件，并将每个实训内容进行了屏幕录像。读者可以通过观看相关的辅助教学演示软件进行操作，非常适合于教学和自学。

本书在编写过程中始终得到了天津职业大学经济与管理学院的领导和老师的支持与帮助，在此谨表衷心的感谢。

限于本人的学术水平，书中错误和不当之处一定不少，敬请读者批评指正。

编　者

E-mail:litingcn@sina.com

2005 年 10 月

目　录

第 1 章　网络安全概述

网络在为人们提供更多的机会和方便，更加绚丽多彩地将世界展现在人们面前的同时，也带来了一些新的问题。例如，人们的生活越来越依赖于网络及其存储的信息，一旦网络由于种种原因发生故障，陷于瘫痪，人们的生活也必然受到极大的影响。另外，计算机犯罪的日益增多也对网络的安全运行和进一步发展提出了挑战。因此，如何保证网络的安全，以及如何保证网络上数据的完整性等问题就越来越受到人们的高度重视。

1.1　安全服务及安全机制

计算机网络的安全性可以定义为：保障网络信息的保密性、完整性、网络服务可用性和可审查性。即要求网络保证其信息系统资源的完整、准确和具有一定的传播范围，并能及时提供所有用户所选择的网络服务。

ISO7498-2 从体系结构的观点描述了 OSI 基本参考模型之间的安全通信必须提供的安全服务和安全机制，以及安全服务及其相应机制在安全体系结构中的关系。

1.1.1　安全服务（Security services）

安全服务是指开放某一层所提供的服务，用以保证系统或数据传输有足够的安全性。根据 ISO7498-2 中提出的建议，一个安全的计算机网络应当能够提供以下的安全服务：

1. 认证（Authentication）

认证安全服务是防止主动攻击的重要措施。认证就是识别和证实，即识别一个实体的身份和证实该实体身份的真实性。身份认证是授权控制的基础，其必须是无二义性地将对方识别出来，同时还应提供双向认证。

对于单机状态下的身份认证一般有用户口令、一次性密码和生理特征等方法。而网络环境下的身份认证要采用高强度的密码技术，一般为对称密钥加密或公开密钥加密的方法。

2. 访问控制（Access Control）

访问控制是确定不同用户对信息资源的访问权限。也是针对越权使用资源的防御措

施。

3. 数据保密性（Data Confidentiality）

数据保密性的安全服务是针对信息泄漏的防御措施。是使系统只对授权的用户提供信息，对于未被授权的使用者，这些信息是不可获得或不可理解的。

4. 数据完整性（Data Integrity）

数据完整性的安全服务是针对被非法篡改的信息、文件和业务流设置的防范措施，以保证资源的可获得性。

5. 不可否认性（Non-reputation）

不可否认性的安全服务是针对对方进行抵赖的防范措施，可用于证实发生过的操作。一般有发送防抵赖、对递交防抵赖和公证。

1.1.2 安全机制（Security mechanisms）

安全机制分为实现安全服务和对安全系统的管理两种类型。ISO7498-2 建议的安全机制有：

1. 加密机制（Encipherment）

加密机制用于加密数据或流通中的信息，其可以单独使用，也可以同其他机制结合使用。具体到加密手段，一般有软件加密和硬件加密。软件加密成本低且应用灵活，但加解密效率较低；而硬件加密，加解密效率较高，但成本高，应用较不灵活。

2. 数字签名机制（Digital signature mechanisms）

数字签名机制是由对信息进行签字和对已签字的信息进行证实这样两个过程组成。其必须保证签字只能由签字者的私有信息产生。

3. 访问控制机制（Access control mechanisms）

访问控制机制是根据实体的身份及其有关信息来决定该实体的访问权限。一般采用访问控制信息库、认证信息（口令等）和安全标签等技术。

4. 数据完整性机制（Data integrity mechanisms）

在通信中，发送方根据要发送的信息产生一条额外的信息（如校验码），并将其加密后随信息本体一同发出；收方接收到信息本体以后，产生相应的额外信息，并与接收到的额

外信息进行比较，以判断在通信过程中信息本体是否被篡改过。

5. 认证机制（Authentication mechanisms）

认证机制可通过认证信息（如口令、指纹等）实现同级之间的认证。

6. 通信业务填充机制（Traffic padding mechanism）

通过填充冗余的业务流来防止攻击者进行业务流量分析，填充过的信息要进行加密保护方可有效。

7. 路由控制机制（Routing control mechanisms）

预先设置好网络中的路由策略和策略路由，以便提供安全的子网和链路。

8. 公证机制（Notarization mechanism）

公证机制是由第三方参与的签名机制。是基于通信双方对第三方的绝对信任，让公证方备有适用的数字签名、加密或完整性机制等。公证方可以利用公证机制对实体间的通信进行实时的或非实时的公证。

1.2　网络安全体系及评估标准

一个网络的整体由网络硬件、网络操作系统和应用程序构成。而若要实现网络的整体安全，还需要考虑数据的安全性问题。此外，无论是网络本身还是操作系统和应用程序，最终都是由人来操作和使用的，这样一个重要的安全问题就是用户的安全性。因此，在考虑网络安全问题的过程中，应主要对网络安全、操作系统安全、用户安全、应用程序安全以及数据安全这五个方面进行分析。

1983 年美国国家计算机安全中心（NCSC）发布的《桔皮书》，即“可信计算机系统评估标准”TSEC（Trusted Computer System Evaluation Criteria），规定了安全计算机系统的基本准则和评估标准。

1.2.1　网络安全五层体系

从体系上看，Internet 网络安全问题可分为以下五个层次，即用户层、应用层、操作系统层、数据链路层和网络层。如图 1-1 所示。

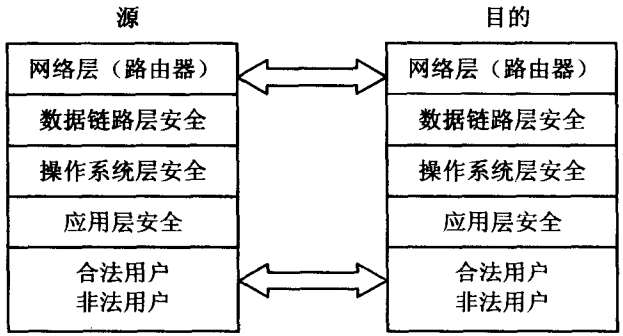

图 1-1 网络系统安全体系

1. *用户层安全*

对于用户的安全性问题，主要考虑的是使用系统中资源和数据的用户是否是真正被授权的用户。一般是对用户进行分组管理，即根据不同的安全级别将用户分为若干等级。如 Windows 操作系统中的用户（user）、组（groups）和管理员（administrator）。其每一等级的用户只能访问与其等级相对应的系统资源和数据。用户层安全包括保护合法用户安全权限及限制非法用户的不安全进入途径。其主要涉及对用户的识别、认证和数字签名等问题。

由于网络的目的是便于资源访问，而网络的安全又与用户密切相关。人们通常关心如何保护网络资源，以确保非法用户不能访问它们。所以，商用网络操作系统都提供了一些安全系统来限制对共享文件、打印机等资源及系统本身的访问。如：

（1）授权：用户访问系统前必须提供用户名和口令。

（2）访问特定许可的资源：操作系统检查文件、目录等的访问列表以确定一个用户是否有权访问它。

（3）受口令保护的共享资源：该资源受口令保护，操作系统只检查用户口令的正确性。

2. *应用层安全*

应用层安全是指合法的用户对特定数据进行合法的操作。应用层安全与应用系统直接相关，即包括不同用户的访问权限设置和用户认证，数据加密的完整性确认以及对不良信息的过滤等。

3. *操作系统层安全*

操作系统的安全问题主要是用户口令的设置与保护以及同一 LAN 或 VLAN 内的共享

文件和数据库的访问控制权限的设置等。无论是服务还是客户机，目前常用的操作系统主要是 UNIX 系列和 Windows 系列。由于用户的应用系统都在操作系统上运行，大部分的安全工具或软件也都在操作系统上运行。因此，操作系统的安全性直接影响网络安全。

为了安全级别的标准化，美国国防部（DOD）技术标准将操作系统的安全等级由低到高分成了 D、C1、C2、B1、B2、B3、A1 四类七个级别。这些标准发表在一系列的标准文献中，因为每本书的封面颜色不同，人们通常称之为“彩虹系列”。其中最重要的是桔皮书，它定义了上述一系列标准。

目前主要操作系统的安全等级都是 C2 级，其特征为：

（1）系统识别用户必须通过用户注册名和口令；

（2）系统可以根据用户注册名决定用户访问资源的权限；

（3）系统可以对其发生的每一事件进行审核并记录；

（4）可以创建其他具有系统管理权限的用户。

4. 数据链路层安全

数据链路层的安全主要涉及到传输过程中的数据加密及数据完整性问题。此外，还涉及到物理地址盗用的问题。解决的方法有：

（1）加强内部管理人员的法律意识；

（2）采用防火墙技术；

（3）交换设备的安全性。

5. 网络层安全

网络层安全问题的核心是网络是否能得到控制。这也是 Internet 网络安全中最重要的部分。其涉及三个方面：

（1）IP 协议本身的安全性；

（2）网络管理协议的安全性；

（3）对数据和 IP 地址进行加密后传输。

1.2.2　网络安全评估标准

许多政府与组织通常不会与未经第三方标准证实其安全性的另一方进行交流。也就是说安全性往往是一个局部的概念。对于不同的生产商、组织、国家政府，彼此也具有不同的安全措施与标准体系。近些年，人们试图建立一个全球性的 ISO 安全档案。下面的标准档案并不专门针对 UNIX 或 Windows NT，仅旨在为不同类型的网络提供一个框架。

1. 欧洲信息技术安全评估标准（ITSEC）文献 BS 7799

在欧洲，ITSEC BS 7799 列出了网络威胁的种类以及各种可以降低攻击危害的方法。要了解关于 ITSEC 的更多情况，请访问www.itsec.gov.uk。BS 7799 档案于 1999 年重写，增加了以下内容：

（1）审计过程；

（2）对文件系统审计；

（3）评估风险；

（4）保持对病毒的控制；

（5）正确处理日常事务及安全保护的 IT 信息。

2. 可信计算机系统评估标准（TCSEC）

在美国，National Computer Security Center（NCSC）负责制定关于可信的计算机产品的安全标准。NCSC 创立了 Trusted Computer Systems Evaluation Criteria（TCSEC）、Department of Defense（DOD）Standard 5200.28 用于建立信任级别。这一标准用于标明一个系统的安全特性和安全防护能力。

在标准中，系统安全程度分为四类，每类又分为若干等级。如 A1、B1、B2、B3、C1、C2，数字越大，表示的安全性越好。D 级系统的安全程度最低，通常为无密码保护的个人计算机系统。A 级别最高，用于军队计算机。具体描述如下：

（1）D 级为安全保护欠缺级。凡经检测安全性能达不到 C1 级的均划分为 D 级。

（2）C1 级为自主安全保护级。实施机制允许命名用户和用户组的身份规定并控制资源共享，防止非授权用户读取敏感信息。提供基本的访问控制。

（3）C2 级为受控存取保护级。与 C1 级相比，计算机处理系统安全保护策略的机制实施了粒度更细的自主访问控制。系统级的保护主要在资源、数据、文件和操作上。通过登录规程，系统不仅要识别用户，还要考虑其唯一性。并通过审计安全性相关事件以及隔离资源，使用户能对自己的行为负责。Windows NT 属于 C2 级的系统。

（4）B1 级为标记安全保护级。除具有 C2 级的所有功能外，系统还提供更多的保护措施。UNIX 的 MLS 及 IBM 的 MVS/ESA 属于 B1 级系统。

（5）B2 级为结构化保护级。支持硬件保护，加强了鉴别机制，并增强了配置管理控制。系统具有相当的抗渗透能力。Honeywell MULTICS 和 XENIX 属于 B2 级系统。

（6）B3 级为安全域级。提出数据隐藏和分层，扩充审计机制，提供系统恢复机制。系统具有很高的抗渗透能力。Honeywell XTS-200 属于 B3 级系统。

（7）A1 级为验证设计级。其安全功能与 B3 相同，同时可以严格而准确地证明系统安全功能的正确性。Honeywell SCOMP 属于 A1 级系统。

1.3　密码学基本原理

1.3.1　密码学基本概念

密码学是以研究数据保密为目的，对存储或传输的信息采取秘密的交换以防止第三者对信息的窃取。其基本术语如下：

（1）明文（Plaintext）：被变换的信息，其可以是一段有意义的文字或数据。

（2）密文（Ciphertext）：信息变换后的一串杂乱排列的数据，从字面上无任何含义。

（3）加密（Encryption）：从明文到密文的变换过程为加密。

（4）eK（p）：以加密密钥 k 为参数的函数。

（5）解密（Decryption）：将密文 C 还原为明文 P 的变换过程。

（6）dK'（C）：以解密密钥 k'为参数的函数。

密码学加密解密模型如图 1-2 所示。

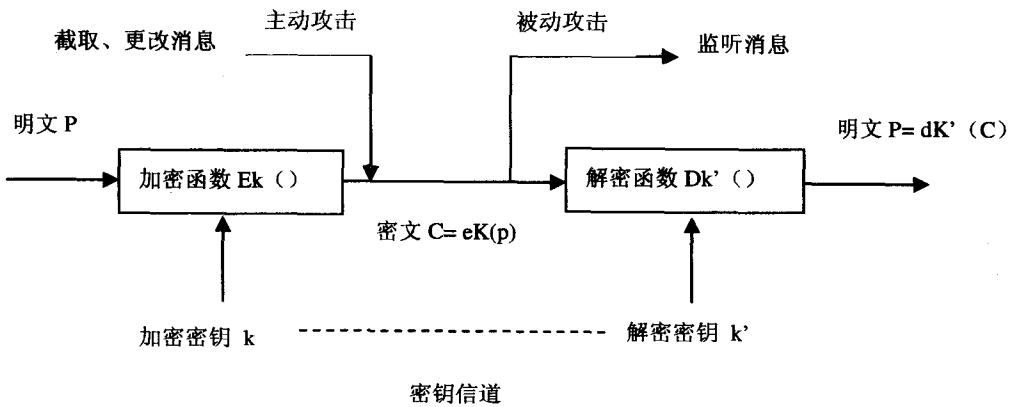

图 1-2　密码学加密解密模型

为了信息的保密性，抗击密码分析，保密系统应当满足以下要求：

（1）系统在实际上为不可破的。即从截获的密文中确定密钥或任意明文在计算上是不可行的。

（2）系统的保密性不依赖于对加密体制或算法的保密，而是依赖于密钥。

（3）加密和解密算法适用于所有密钥空间中的元素。

（4）系统便于实现和使用。