高校计算机规划系列教材

计算机网络安全

蔡永泉　编著

北京航空航天大学出版社

高校计算机规划系列教材

计算机网络安全

蔡永泉　编著

北京航空航天大学出版社

内 容 简 介

本书是作者在多年的教学和科研实践基础上撰写的。主要包括：计算机网络安全体系结构、对称加密体系和不对称加密体系、数字签名、报文完整性鉴别、密钥管理、身份认证、访问控制、虚拟专用网技术、网络入侵与安全检测、可信计算、计算机病毒及防范。特点是概念准确、论述严谨、内容完整；在既重视基本理论，又注重基本实践上，还力图反映一些最新知识。它可以帮助读者系统地了解网络安全基本理论和应用知识。本书可作为高等院校高年级本科生和研究生网络安全和密码学教材，也可供相关技术人员参考。

图书在版编目(CIP)数据

计算机网络安全/蔡永泉编著. —北京：北京航空航天大学出版社，2006.10

ISBN 7-81077-921-4

Ⅰ.计… Ⅱ.蔡… 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(2006)第 108883 号

计算机网络安全

蔡永泉 编著

责任编辑 许传安

*

北京航空航天大学出版社出版发行

北京市海淀区学院路 37 号[100083] 发行部电话：010-82317024 传真：010-82328026

http://www.buaapress.com.cn E-mail:bhpress@263.net

北京市松源印刷有限公司印装 各地书店经销

*

开本：787×1092 1/16 印张：14 字数：358 千字

2006 年 10 月第 1 版 2006 年 10 月第 1 次印刷 印数：5 000 册

ISBN 7-81077-921-4 定价：21.00 元

本书备有课件，供教师使用。需要的教师可向本社发行部索取。

前 言

随着计算机网络的广泛使用，人们对网络的依赖越来越大，但是如何在开放的互联网络中得心应手去做自己想做的工作，即如何在一个开放的计算机网络环境中构造一个适合自己的环境，这就是计算机网络安全所要解决的问题。

计算机网络安全涉及到理论与技术两方面内容。本书始终把握住这两方面内容，让读者通过本书的学习，能够掌握其理论及方法，并得到应用。本书整体结构安排如下。

第 1 章概述，介绍计算机网络面临的威胁，ISO 网络安全体系结构和计算机网络存在安全漏洞及其有关概念。

第 2 章数论初步，包括素数、同余或按模计算、一次同余方程、欧拉定理、孙子定理等一些与本书有关算法。

第 3 章信息加密技术，介绍对称和不对称加密算法。其中包括 DES 加密算法、IDEA 加密算法、RSA 加密算法、ALGMA 加密算法以及 ECC 加密算法。

第 4 章报文完整性鉴别，首先介绍报文完整性鉴别的基本原理及方法，最后介绍与报文完整性鉴别有关的单向函数。

第 5 章数字签名，首先介绍数字签名原理及其算法，然后介绍多重签名和盲签名算法。

第 6 章密钥管理，包括基于阈值的密钥分割管理、基于几何特性密钥管理和具有等级密钥管理。

第 7 章身份验证，首先介绍验证的基本原理及其方法，最后介绍 Needhanm 方法、Kerberos 标准和 CCITT X. 509 标准。

第 8 章访问控制，包括隔离法、矩阵法以及防火墙的基本原理及实现。

第 9 章虚拟专用网技术，主要介绍虚拟专用网的构成和虚拟专用网的协议。

第 10 章网络入侵与安全检测，首先介绍入侵的原理及其方法，最后介绍对其入侵的检测方法。

第 11 章计算机病毒及防范，包括计算机病毒定义、计算机病毒分类、计算机病毒的机制、计算机病毒检测方法、计算机病毒的防范。

第 12 章可信计算初步，主要包括可信计算原理、可信计算机系统结构、可信计算硬件系统、可行计算软件系统。

本书是在多次给计算机专业和信息安全专业的高年级本科生和研

究生的讲课过程中形成的，所以可作为高等院校计算机专业及其相关专业的高年级本科生和研究生教材和参考用书，也可以作为从事计算机网络安全工程技术人员的参考书籍。

在编写过程中不可避免出现这样、那样的错误，敬请读者指正。

作　者

2006 年 8 月

目 录

第1章 综 述

1.1 概 述

当今，计算机网络所带来的信息共享和资源共享等优点，日益受到人们的注目，并获得广泛的应用。同时，随着全球互联网络 Internet 应用范围的扩大，使得网络应用进入到一个崭新的阶段。一方面，入网用户能以最快的速度、最便利的方式及最廉价的开销和最新的信息，在国内、国际范围内进行交流；另一方面，随着网络规模越来越大和越来越开放，网络上的许多敏感信息和保密数据难免受到各种主动和被动的人为攻击。也就是说，计算机网络在为人们提供益处的同时，人们也必须考虑如何对待网络上日益泛滥的信息垃圾和非法行为，即必须研究网络安全问题。

众所周知，利用计算机环境进行全球通信已成为时代发展的必然趋势。但是，如何在一个开放式的计算机网络物理环境中构造一个封闭的逻辑环境来满足国家、集团和个人实际需要，已成为必须考虑的实际问题。互联的计算机网络常常由于节点分散、难以管理等特点，而易受到攻击和蒙受分发操作带来的损失，若没有安全保障，则给系统会带来灾难性的后果。

1.2 计算机网络安全的基本概念

1.2.1 信息系统中安全性的作用

计算机网络系统可以表现为各种各样的形态，信息系统则是其中主流之一。由于信息系统在实际中的安全保护有着丰富的内容，因而人们过去对计算机安全性问题的研究总是围绕着信息系统进行。

对任一信息系统，安全性的作用在于：防止未经授权的用户（包括程序在内）来动用（甚至破坏）系统中的信息，或干扰（甚至破坏）系统的正常工作。

上述安全性作用给新系统带来了以下“四性”：

1）保密性（confidentiality）：即系统只向已被授权者开放。

2）完整性（integrity）：使系统只允许有权的用户或已被授权的用户修改信息。

3）可获得性（availability）：使系统不会发生因瘫痪等不正常现象而不能向已授权的用户提供服务。

4）可审查性（accountability）：使系统内所发生的与安全有关的动作均有说明性记录可查。

1.2.2 计算机网络信息的构成

当今，计算机网络信息系统已从以局域网为基础的形式发展为广域网为基础的形式。后一形式的计算机网络信息系统在逻辑上可抽象为由域(domain)和互联两者构成，如图 1.1 所示。

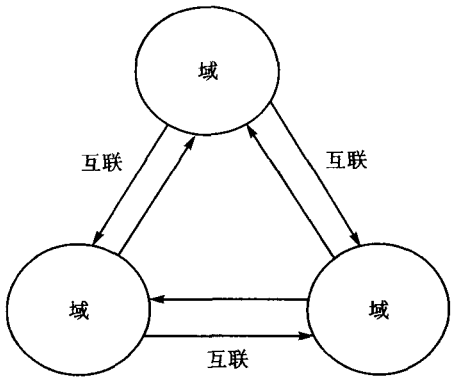

图 1.1 系统安全模型

为了确保计算机网络整个信息系统的安全性，图 1.1 中各组成成分也应是安全的，即它们分别将采用安全域和安全互联。由此可见，要实现计算机网络信息系统的安全性，应从两方面的问题考虑：端系统的安全性与网络系统的安全性。

在计算机网络系统的端系统中包括：

1）单机系统：对于用户主要是应用和提供应用数据，如图 1.2 所示。

2）分时系统：它是在单机系统的基础上接入多个终端，并分时为各个终端服务，如图 1.3 所示。

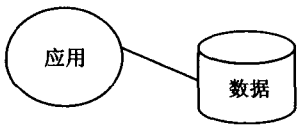

图 1.2 单机系统

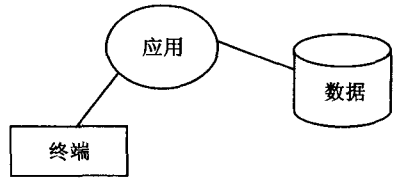

图 1.3 分时系统

上述两个系统正向更复杂的形态转换发展，主要有：

1）客户机/服务器系统：如图 1.4 所示，在此系统中，存在用于提供数据的服务器，为用户提供服务的客户端系统。

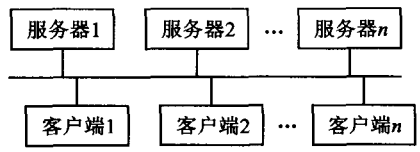

图 1.4 客户机/服务器系统

2）共享设备局域网系统：在此系统中又提供共享的硬件、软件、数据库等和多个用户终端系统，如图 1.5 所示。

3）对等合作系统：这个系统在网络环境下都是对等的，所有的系统都是在相同的环境下工作，如图 1.6 所示。

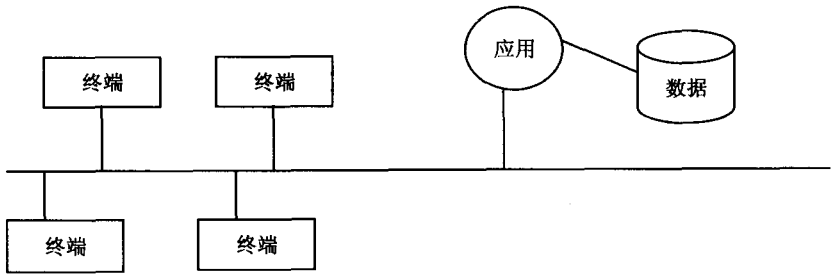

图 1.5 共享设备局域网系统

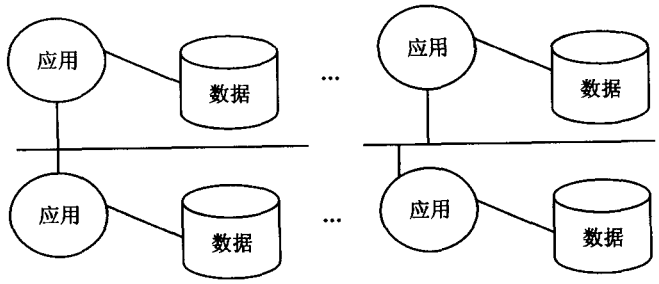

图 1.6 对等合作系统

在同一个计算机网络系统中允许存在异种计算机系统(如不同的计算机、不同的操作系统等)。

1.2.3 端系统的安全设计

一个域(端系统)的安全性必须统一设计,这样才能保证域内的全局安全性。安全设计可按以下步骤设计。

1) 明确安全设计要求:这主要涉及到脆弱性分析、威胁评估和后果分析。

2) 制定安全策略:这主要涉及到要防止何种威胁、要保护何种资源、靠何种手段实现安全、估计实现的代价。

3) 选择安全服务:这主要涉及到选择合适的安全服务、组织安全机制来实现、配以相应的安全管理。

一个安全域内应具有统一的安全策略。实际上,进行的种种有关安全保障的活动就是安全策略的具体体现。

1.2.4 端系统的安全管理系统概念模型

端系统的安全管理应包括:安全管理信息库、安全管理工具、安全管理员。这个模型如图 1.7所示。

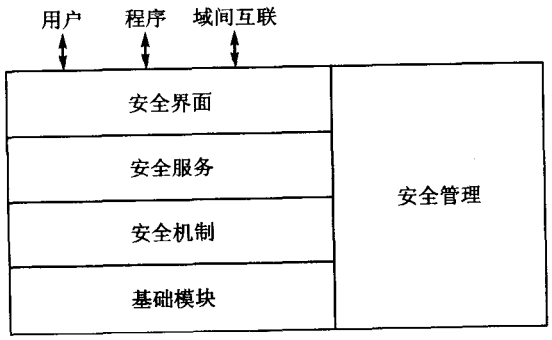

图 1.7 安全保障模型

1.3 计算机网络的安全体系

国际标准化组织 ISO 对开放计算机网络互连环境的安全性通过深入地研究，在 1989 年提出了安全体系结构，为计算机网络的安全提出了一个比较完整的安全框架。它包括安全服务、安全机制和安全管理及其它有关方面。它仍是一个概念，有待于进一步研究开发，才能适应计算机网络安全技术发展的要求。

1.3.1 计算机网络所面临的威胁

根据国际化标准组织定义的计算机网络面临的威胁，实际上是对计算机网络安全的潜在破坏。一个系统可能遭受到各种各样的威胁，只有知道了系统受到的威胁以后，才能对其进行有效的防范。

计算机网络所面临的威胁可分为两大类型，即主动威胁和被动威胁。主动威胁是指威胁者对计算机网络信息进行修改、删除等非法操作。被动威胁是指威胁者通过非法手段获取信息和分析信息，而不修改它。

探明威胁可通过以下三个方面来进行。

1）脆弱性分析：辨认出环境中存在哪些有脆弱性的成分。

2）威胁估计：评定由于威胁性的存在而可能会出现的问题。

3）危险分析：分析出现的问题可能导致的后果。

破坏系统的安全主要有四种类型：中断(interruption)、窃取(interception)、更改(modification)和伪造(fabrication)。

- 中断是指威胁源使系统的资源受损或不能使用，从而使数据的流动或服务的提供中止。
- 窃取意味着某个威胁源成功地获取了一个资源的访问，从而成功地盗窃有用的数据或服务。
- 更改就是未经授权的某个威胁源，成功地访问，并改动了某些资源从而篡改了系统所提供的数据或服务。
- 伪造是指未经授权的威胁源，能成功地在系统中制造假源，从而产生虚假的数据或服务。

国际标准化组织对具体的威胁定义如下。

- 伪装(pseudonym)：某个具有合法身份的威胁源成功地假扮另一实体，随后滥用这个实体的权利。其威胁源可以是用户，也可以是程序。
- 非法连接(illegal association)：威胁源以非法的手段形成合法的身份，使得网络资源之间建立非法的连接。威胁源可以是用户，也可以是程序。被威胁的对象是各种网络资源。
- 非授权访问(no-authorized access)：威胁源成功地破坏了访问控制服务(如修改了访问控制文件的内容)，实现了越权访问。威胁源可以是用户也可以是程序。被威胁的对象则是网络各种资源。
- 重放(replay)：威胁源通过截获信息，然后根据需要，将截获的信息再次重放。威胁源

主要是用户，被威胁的对象也是用户。

- 拒绝服务(denial of service)：是指阻止合法的网络用户或其他执行其合法的权限者的访问，如出现妨碍执行服务或信息传递。威胁源可以是用户，也可以是程序。
- 抵赖(repudiation)：主要是指使网络用户虚假的否认递交过信息或接收到信息。威胁源可以是用户，也可以是程序。被威胁的对象是用户。
- 信息泄漏(leakage of information)：是指未经授权的实体(用户或程序)获取了传递中或存放的信息，造成了失密。威胁源可以是用户，也可以是程序。受威胁对象是通信系统中的信息或数据库中的数据。
- 业务流量分析(traffic analysis)：是指威胁源观察通信协议中的控制信息，或对传送中的信息的长度、频率、源或目的进行分析。威胁源可以是程序，也可以是用户。受威胁的对象是通信系统中的信息。
- 改变信息流(invalid message sequencing)：是指通过对正确的通信信息序列进行非法修改、删除、重排序或重复。威胁源可以是用户，也可以是程序。被威胁的对象是通信系统中的信息。
- 篡改或破坏数据(data modification or destruction)：是针对传送的信息或存放的数据进行有意的非法修改或删除。威胁源可以是用户，也可以是程序。被威胁的对象是通信系统中的信息或数据库中数据。
- 推断或演绎信息(deduction of information)：由于统计信息数据含有原始的信息踪迹，非法用户利用公布的统计数据，推导出某个信息源是从何处来的值。威胁源可以是用户，也可以是程序。被威胁的对象是数据库中的数据或通信系统中的信息流。
- 非法篡改(illegal modification of programs)这种威胁具有三种形式：病毒、特洛尹木马和蠕虫。它们破坏操作系统、通信软件或应用程序。威胁源可以是程序，也可以是用户，威胁的对象是程序。

1.3.2 安全服务

设计和使用一个安全系统的最终目的，就是设法消除系统中的部分或全部威胁，探明系统中的威胁。根据安全需求和规定的保护级别，选用适当的服务来实现安全保护，为此国际标准组织对此定义了五种安全服务。

1. 对象认证(entity authentication)安全服务

对象认证安全服务是防止主动攻击的重要防御措施。它对计算机网络系统环境中的各种信息安全有重要的作用。认证就是识别和证实。识别是对一个对象的身份进行判明。

2. 访问控制(access control)安全服务

访问控制安全服务是针对越权使用资源的防御措施。访问控制可分为自主访问控制和强制访问控制两类。其实现机制可以是基于访问控制的属性访问控制表(或访问控制矩阵)，或基于安全标签、用户分类和资源分档的多级控制等。

3. 数据保密性(data confidentiality)

数据保密性安全服务是针对信息泄漏的防御措施。它又可分为以下几种。

- 信息保密：保护通信系统中的信息或数据库中的数据，而对于通信系统中的信息，又可进一步分为连接保密和无连接保密。

- 选择保密：保护信息中被选择的数据段。
- 业务流保密：防止攻击者通过观察业务流（如信源、信宿、传送时间、频率和路由等）来得到这些信息等。

4. 数据完整性（data intergrity）安全服务

数据完整性安全服务是针对非法篡改信息、文件和业务流而设置的防范，以保证资源可获得性的措施。它可分为如下几种。

- 连接的完整性（包括有恢复和无恢复的）：为一个连接上的所有信息提供完整性办法，探测是否对信息进行了非法篡改、插入、删除或重访。
- 选择字段有连接的完整性：为一个连接所传送的信息中所选择的信息段提供完整性，目的是判断所选择的信息段是否被进行了非法篡改、插入、删除或重放。
- 无连接的完整性：为无连接的各个信息提供完整性。目的是鉴别所收到的信息是否被篡改过。
- 选择字段无连接完整性：为在各个无连接的信息中所选择的信息段提供完整性。目的是鉴别所选择的信息段是否被非法篡改过。

5. 防抵赖（no-repudiation）安全服务

防抵赖安全服务是针对对方进行抵赖的防范措施，可用来证实已发生过的操作。其操作可分为如下几种。

- 发送防抵赖：用来防止信息发送者否认发送的信息。
- 递交防抵赖：用来防止接收信息的对象否认接收到的信息。
- 公证：通信双方互不信任，但对第三方（公证方）则绝对信任，于是依靠第三方来证实已发生的操作。

1.3.3 安全机制

安全机制可分为两类：一类是与安全服务有关，是用来安全服务的；另一类是与管理功能有关，被用于加强对安全系统的管理。

1. 与安全服务有关的安全机制

（1）加密机制

加密机制可用来加密存放着的数据或数据流中的信息。它既可以单独使用，也可以同其它机制结合起来使用。加密算法可分为对称密钥（单密钥）加密算法和不对称密钥（公开密钥）加密算法 。

（2）数字签名机制

数字签名由两个过程组成：对信息进行签字的过程和对已签字的信息进行证实的过程。前者使用私有密钥，后者使用公开密钥。它是由已签字是否与签字者的私有密钥有关信息而产生的。数字签名机制必须保证签字只能是签字者私有密钥信息。

（3）访问控制机制

访问控制机制根据实体的身份及其有关信息，来决定该实体的访问权限。访问控制实体常采用以下的某一或几个措施：访问控制信息库、证实信息（如口令）、安全标签等。