高等学校计算机教材

网络安全原理与应用

沈苏彬　编著

人民邮电出版社
POSTS & TELECOM PRESS

高等学校计算机教材

网络安全原理与应用

沈苏彬　编著

人民邮电出版社

图书在版编目（CIP）数据

网络安全原理与应用 / 沈苏彬编著. —北京：人民邮电出版社，2005.5
高等学校计算机教材

ISBN 7-115-13437-5

Ⅰ. 网… Ⅱ. 沈… 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（2005）第 047453 号

内 容 简 介

本书系统地介绍网络安全原理及其典型应用。本书共包括 7 章：网络安全概述、密码学导论、身份验证技术及其应用、访问控制技术及其应用、网络攻击检测与网络蠕虫、网络数据安全技术以及网络应用安全技术。本书重点讨论了网络安全的基本概念和组成，传统密码学和公钥密码学，报文身份验证、身份验证协议和 Kerberos 身份验证系统，访问控制模型和网络防火墙技术，网络攻击检测原理和网络蠕虫的分类方法，安全 IP 技术和传送层安全技术，网络应用安全体系和万维网安全技术。

本书主要作为高等院校相关专业的本科生和研究生的网络安全课程教材，也可以作为相关专业科研和工程技术人员学习、研究和开发网络安全技术的入门书籍。

高等学校计算机教材

网络安全原理与应用

◆ 编　　著　沈苏彬
责任编辑　滑　玉

◆ 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

读者热线　010-67170985
北京隆昌伟业印刷有限公司印刷
新华书店总店北京发行所经销

◆ 开本：787×1092　1/16
印张：11.5
字数：275 千字　　2005 年 5 月第 1 版
印数：1－4 000 册　　2005 年 5 月北京第 1 次印刷

ISBN 7-115-13437-5/TP・4673

定价：16.00 元

编 者 的 话

从 1988 年 11 月 2 日晚在因特网上首次爆发“网络蠕虫”，计算机网络界开始重视网络安全的研究和开发。在将近 17 年的时间里，网络安全技术已经有了很大的发展，在此期间发明了网络防火墙技术、网络防病毒技术、网络身份验证技术、安全 IP 技术、传送层安全技术以及新型的网络攻击检测技术。

但是，目前网络安全形势依然十分严峻。这里主要原因在于：近 17 年来网络应用有了大幅度的发展，目前网络应用已经深入到我们社会的各个层面。其结果是，一方面，网络用户越来越多，越来越复杂，无法单纯通过道德准则的教育限制网络攻击和网络犯罪活动。另一方面，金融和商业等应用在网络上的普及，对安全要求越来越高，同时，网络攻击也越来越具有经济价值。另一个原因在于，目前基于 TCP/IP 协议簇的因特网本身就缺乏严密的安全机制，本质上难以提供高质量的安全服务。最后一个原因在于，我们目前的软件技术还不成熟，无法消除网络软件中的错误。而网络软件的错误产生了网络系统的安全漏洞。网络安全目前已经成为制约网络应用进一步发展的关键问题。

虽然我从 2000 年起就着手研究网络安全技术，但并没有考虑编写书籍。因为对于编著这类理论性和技术性太强的书籍，其巨大的工作量是令人望而生畏的。编写本书的动因来源于我的老朋友，南京邮电大学的郑会颂教授。2002 年郑教授在筹办成功南京邮电大学电子商务专业之后，邀请我为该专业的本科生开设一门“网络安全”的课程。由于网络安全正是我当时研究的主要内容之一，而且郑教授又是十多年的朋友，我欣然接受了邀请。在准备教案时，我才发觉当时国内图书市场难以找到一本完全符合我讲课要求的网络安全教材。这样，才考虑自己编著一本较为全面地介绍网络安全原理及其应用的教材，能够帮助本科生以及拟从事网络安全研究和开发的初学者尽快理解网络安全原理，具备实际研究、开发和设计网络安全系统所必备的知识。

本书特点

网络安全书籍可以分成两种类型，一种是介绍网络安全实用技术或技巧的书籍，用于设计和配置安全的网络系统、设计和配置安全的电子邮件系统、万维网应用系统等；另一种是介绍网络安全原理和典型应用的书籍，用于系统地学习、研究和开发网络安全技术或系统。前一类书籍比较简单、直观，很容易看懂，也知道如何使用；后一类书籍比较复杂、抽象，初看起来觉得比较费力，也不知道如何应用。前一类书籍仅仅介绍应用过程，知其然，不知其所以然；后另一类书籍侧重于内在的原理和方法，既知其然，又知其所以然。前一类书籍主要用于一般读者掌握网络安全的某些使用技巧；后一类书籍主要用于专业人员学习、研究和开发网络安全方法和技术。前一类书籍的读者群大；后一类书籍的读者群小。前一类书籍的内容容易过时；后一类书籍的内容具有较长时间的参考价值。本书是属于后一类网络安全的书籍，主要用于高等院校相关专业的本科生和研究生的网络安全课程教材，也可以作为相关专业科研人员学习、研究和开发网络安全技术的入门书籍。

本书试图采用一种“深入浅出”的风格，较为完整和严谨地描述网络安全中的基本原理

和方法，并且较为通俗地论述和分析这些原理和方法。这样，既能够满足希望基本了解网络安全原理，能够进行基本网络安全应用的初学者的需要。同时，也能满足希望较为全面、准确地掌握网络安全原理和方法，能够进一步从事网络安全研究和开发的初学者的需要。

本书试图将网络安全中最为本质的原理和方法介绍给读者。网络安全及其相关技术是近30年蓬勃发展的技术，相关的参考文献和专业书籍十分丰富。我一直认为，任何复杂的技术都有反映其本质的简单原理。所以，本书主要取材于在网络安全及其相关技术研究中，最有影响的研究论文和国际标准。这样，既可以保证对技术阐述的准确性，又可以保证对基本原理描述的简洁性。

本书试图介绍较为先进和实用的网络安全技术。网络安全技术是一门正在发展的技术，网络安全方面的新技术、新方法、新标准不断涌现；网络安全方面的国际性学术会议和学术刊物也在不断翻新。为了使得读者能够掌握较为先进的、较为实用的网络安全技术，本书也尽可能采用了一些近两年国际学术会议和学术刊物上发表的有关网络安全方面的研究成果。

本书试图采用科学的方法描述网络安全原理及其应用技术。网络安全技术是一门复杂的技术，要准确地描述这类复杂的技术，必须采用一些较为科学的方法。同样，要准确地掌握这类复杂的技术，也必须学习这些科学的描述方法。本书在关键的原理和技术论述方面，采用了一些形式化的描述方法。为了方面初学者阅读，本书对这些形式化描述方法进行了较为详细的说明，试图达到“深入浅出”的效果。

本书不是简单地汇总一些网络安全方面的研究报告或参考文献，而是根据我个人对网络安全技术的总体认识，对网络安全原理和网络安全应用进行系统阐述。在网络安全原理方面，着重阐述身份验证、访问控制和攻击检测的原理和方法；在网络安全应用方面，着重阐述网络数据安全技术和网络应用安全技术。根据我个人研究和开发体验，密码学知识是掌握网络安全原理不可缺少的基础知识，所以，本书从学习和研究网络安全的角度，较为系统地介绍了密码学。

本书不是网络安全技术大全。网络安全技术是一门理论性、综合性较强的技术，也是一门不断发展的技术，单凭一个的学识和精力是无法穷尽网络安全技术的全部内容。我虽然希望能够尽量完整、准确、清楚地阐述网络安全原理及应用，但是，由于自己研究阅历、时间和技术发展本身的限制，有些方面并不尽如人意，有些方面还存在不少遗憾。我期望今后有机会弥补这些不足和遗憾。

阅读建议

本书包括网络安全概述、密码学导论、身份验证技术及其应用、访问控制技术及其应用、网络攻击检测与网络蠕虫、网络数据安全技术，以及网络应用安全技术，共7章。各章的主要内容和重点如下：

第1章“网络安全概述”主要介绍与网络安全相关的概念和技术，例如密码技术、通信安全技术、计算机安全技术、数据安全技术和信息安全技术，重点讨论了网络安全的组成和关键技术，介绍了目前网络安全技术面临的主要挑战及其发展的机遇。还介绍研究和开发网络安全技术通常依据的原则：网络安全研究和开发的5条公理。本章要求掌握网络安全内涵，它涉及到网络系统以及在网络系统中传递和存储数据的保密性、完整性和可用性。网络安全不仅仅是保护网络系统中数据的安全，还需要保护网络系统本身的安全。

第 2 章“密码学导论”主要介绍密码学相关的概念和知识，重点介绍传统密码学和公钥密码学，其中包括传统密码学和公钥密码学原理，DES 加密算法，ASE 加密算法，RC4 加密算法，RSA 公钥加密算法，Diffie-Hellman 密钥生成算法，以及加密操作模式。本章介绍的 DES 加密算法、RSA 公钥加密算法以及加密操作模式是必须掌握的内容。

第 3 章“身份验证技术及其应用”重点介绍报文身份验证、身份验证协议以及 Kerberos 身份验证系统。在报文身份验证中，主要介绍 MD5 报文摘要算法、SHA-1 安全哈希算法以及 HMAC 报文验证码算法；在身份验证协议中，主要介绍了 Needham-Schroeder 身份验证协议及其改进。本章也介绍基于身份验证的公钥基础设施（PKI）基本原理和结构。

第 4 章“访问控制技术及其应用”主要介绍传统计算机安全中常用的访问控制模型，以及基于访问控制模型的网络防火墙技术。其中在访问控制模型中，重点介绍军用 Bell-LaPadula 访问控制模型和商用 Clark-Wilson 访问控制模型，以及基于角色的访问控制模型；在网络防火墙技术中，重点介绍网络层防火墙和应用层防火墙技术。

第 5 章“网络攻击检测与网络蠕虫”主要介绍网络攻击的现状，网络攻击检测的基本原理，以及网络蠕虫的分类方法。其中重点介绍了网络攻击的分类、网络攻击检测的基本原理、以及网络蠕虫基本特征。本章介绍的网络攻击检测原理包括了网络入侵检测，而网络攻击检测不仅包括入侵检测，还包括以破坏网络系统可用性为目标的攻击检测。

第 6 章“网络数据安全技术”主要介绍安全 IP 技术和传送层安全技术。其中重点介绍了安全 IP 技术中的 AH 和 ESP 网络安全协议，ISAKMP 安全关联和密钥管理协议， IKE 密钥交换协议，以及 SSL 协议。网络数据安全技术是密码学和身份验证技术在网络安全中的具体应用，它是对现有网络系统的安全加固技术。

第 7 章“网络应用安全技术”主要介绍网络应用系统的安全应用体系结构，电子邮件系统的安全技术，以及万维网系统的安全技术。这是对网络安全技术的综合应用技术，涉及到前面介绍的主要网络安全技术，包括网络数据安全技术。

本书前后章节具有一定的关联性，但是，“身份验证技术及其应用”、“访问控制技术及其应用”和“网络攻击检测与网络蠕虫”这 3 章相互具有一定的独立性，可以根据读者需要，按照各自喜好的顺序阅读。

本书可以作为高等院校相关专业“网络安全”课程的本科生和研究生教材。对于本科生，重点在于掌握网络安全原理和基本应用方法，其中形式化算法描述和身份验证协议描述部分可以不作为具体考核的内容。对于研究生，重点在于掌握网络安全原理、主要算法和形式化描述方法，要求研究生掌握网络安全技术研究和开发的基本方法。每章后面所附的思考题仅仅作为复习时参考。

本书也可以作为相关专业科研人员学习、研究和开发网络安全技术的入门书籍。在作为入门书阅读过程中，可以根据自己科研工作的需要，有选择地阅读相关的章节；也可以从头到尾系统地阅读。每章后面所附的思考题，有助于读者归纳和总结每章所学的主要内容。

感谢

本书的构思、编写和出版得到了许多领导、同事和朋友的关心和指导。本书的完成离不开他们的帮助和支持。我十分感谢这几年来一直支持我从事网络安全研究和教学的这些领导和朋友们。

本书所涉及内容的核心部分都是近5年来从事网络安全原理及其应用的研究和开发过程中积累的素材，所以，我首先要感谢最早资助我从事网络安全研究的东大金智软件系统公司，非常感谢金智公司的葛宁总经理、陈钢副总经理、徐兵副总经理、丁小异总会计师、以及陈弘毅总经理助理对我的帮助和支持！

有幸参与信息产业部十进制网络工作组资助的“新一代安全可控网络技术研究”项目，也使我有机会较为深入地研究网络安全理论和机制。我十分感谢信息产业部十进制网络工作组谢建平组长和中国科学院计算技术研究所网络中心张国清主任对我在网络安全研究方面的关心和支持！

没有郑教授的邀请，就不会触发我写本书的念头。我非常感谢郑教授这么多年来对我以及我领导的研究组的关心和支持！

我衷心地感谢南京邮电大学谢玲院长、张顺颐副院长对我研究和教学工作等多方面的关心、帮助和支持！感谢南京邮电大学科技处师崇群处长、谌进副处长对我以及我所领导的研究组的帮助和支持！感谢我所在的研究组各位成员对我的帮助和支持！这些关心、帮助和支持使我能够潜心研究，完成本书的编著工作。

编 者

2005年3月于南京

目　录

第 1 章　网络安全概述

系统地学习一门技术，必须了解这门技术的发展历史。任何技术都有其发展的历史，同样，网络安全技术也是在众多技术基础上发展起来的技术。网络安全技术实际上是传统通信安全技术和计算机安全技术在计算机网络环境下的融合和发展，网络安全在很大程度上继承了通信安全技术中的保密通信技术和身份验证协议模型、计算机安全技术中的访问控制和攻击检测模型，发展成为一种在网络分布处理环境下的，包括身份验证、访问控制和攻击检测的网络安全理论，以及在具体网络环境下的网络安全应用技术。

网络安全已经成为目前网络技术和应用发展过程中的一项关键问题，如果不能从根本上解决网络安全问题，则目前网络将难以发展成为无论在任何时间、任何地点、使用任何方式都能够提供信息服务的现代信息社会的基础设施。网络安全的严峻现实要求有社会责任心的网络研究者和网络应用者都能够关心和研究网络安全问题。

本章将介绍网络安全的相关理论和技术，网络安全的定义、目标和基本原理，并对本书介绍的网络安全理论及其应用提供一个总体概述。

1.1　信息安全基本概念

网络安全是近十多年来发展起来的一种在网络环境下的安全控制理论和技术，这是一门综合性的安全控制理论和技术。目前比较常用的网络安全技术包括安全 IP 报文传递技术、网络防火墙技术、网络入侵和攻击检测技术、安全万维网技术、安全电子邮件技术以及网络防攻击技术。

为了学习和研究这些网络安全技术，必须首先学习和理解与网络安全相关的理论和技术。这些理论和技术包括计算机网络理论和技术、密码学理论和密码技术、通信安全、计算机安全、数据安全和信息安全相关的理论和技术。

任何安全技术都是应对某种安全风险模型的技术，网络安全技术也是应对现代计算机网络和电信网环境下的安全风险模型而发展的一类技术。由于下一代电信网也是一种与计算机网络融合的网络系统，所以，学习和研究网络安全必须学习和理解现代计算机网络理论和技术，这样，才能正确理解现代网络面临的安全风险模型，把握当前网络安全技术研究的主要问题。考虑到篇幅的限制，本书不再专门论述计算机网络的基本概念和原理。

计算机网络技术是通信技术与计算机技术融合的产物，所以，计算机网络中面临的安全风险模型与通信和计算机中面临的风险模型具有一定的相关性。因此，通信安全和计算机安全中有关理论和技术可以直接应用于网络安全。

1.1.1　密码技术

密码技术是一种对数据进行编码处理的过程，经过该过程处理的数据可以使得非授权者

难以获取数据表示的信息，而授权者较为容易地获取该数据表示的信息。这种对数据的编码处理过程称为数据加密/解密过程。

例如对于数学中常用的常数π的近似值 3.1415926 中的每位数以 10 为模进行加 5 处理，例如(3 + 5)mod 10 = 8，(5 + 5)mod 10 = 0，经过这种简单的编码处理，π的近似值就变成为 8.6960471。这样，不知道该编码方法的非授权者就难以知道这个数就是π的近似值。而被授予可以读取该数据中信息权限的用户可以通过对该数每位数以 10 为模进行减 5 处理，例如(8 – 5)mod 10 = 3，(0 – 5)mod 10 = 5，这样，就可以将 8.6960471 还原成为 3.1415926，从而知道这是π的近似值。

与密码技术相关的理论是密码学，密码学不仅研究如何进行加密/解密数据的处理过程，还研究在不知晓加密/解密数据的处理过程的前提下，如何破译加密的数据，获取加密数据表示的信息。密码破译技术的研究具有双重目的：其一是可以检验加密/解密算法的安全性；其二是可以破译敌方的密码技术，窃取敌方的保密信息。

目前设计难以破译的密码技术通常有两种标准：（1）计算复杂度过高，使得为破译该密码技术花费的时间超出了数据保密的期限。例如，在战场上传递的作战计划所采用的保密技术如果能够保证敌方在战役开始之前无法破译，则就是一种安全的密码技术。又例如，现在民用的密码技术，如果采用目前可以的计算技术和方法，在 100 年之内也无法破译，则该密码技术就是一种安全的密码技术。（2）计算成本过高，如果花费在破译该密码技术的成本高于加密数据包含信息本身的价值，则这种密码技术从商业角度看，也是一种安全的密码技术。但是，对于国家安全所采用的密码技术而言，就不太适合采用第二种标准。

网络安全技术仅仅是利用密码技术，而不是研究密码技术。学习和研究网络安全技术虽然需要学习一些常用的密码技术，但并不需要专门去研究密码技术。因此，虽然某个密码技术的设计和验证通常涉及到较为复杂的数学理论和计算复杂性理论，但是，学习和使用该密码技术相对比较容易。

有的研究者认为，网络安全是基于密码技术之上的一种技术。这种说法有一定道理，但是，很不完整。正如国家安全确实需要基于一套保密体系，但是，这不代表一个国家的整个安全体系一样，网络安全有其自身一套完整的安全控制体系。密码技术仅仅是整个体系的一个环节。

1.1.2 通信安全技术

通信安全技术是一种保证通信过程中数据传递保密性和完整性的技术，它包括通信双方的身份标识和验证、数据在通信信道上加密传输技术，以及数据在通信信道上完整传输技术。

通信安全技术面临的第一个问题是如何识别远程由通信信道连接的另一方的身份，在确定对方真实身份之后才能进行数据的保密、完整地传输。早在第二次世界大战期间，为了识别我方和敌方的飞机，通信专家就开始研究身份验证协议[1]；在 20 世纪 70 年代，随着电信网应用发展，通信专家进一步研究在电信网环境下的身份验证协议。

身份验证协议就是通过通信双方的报文交互，相互识别并且验证对方身份的一组规则。著名的 Needham-Schroeder 身份验证协议就是 1978 年提出的安全身份验证协议。

身份验证协议构成了通信安全技术的主要内容，也是网络安全技术研究中的重要内容。

由于通信安全中研究身份验证协议的环境与网络安全中身份验证环境基本类似，所以，通信安全中的身份验证协议可以直接应用于网络安全中。

一旦通信双方验证了对方身份之后，双方就可以进行数据保密传递。通过数据加密传输技术可以实现数据保密传递，数据加密传输技术实际上就是密码技术在数据传输中的应用。这种技术也可以直接应用于网络安全。

数据完整性传递是为了防范数据在传递过程中被有意或者无意地篡改。数据完整性传递可以采用加密的报文校验和实现。报文校验和通常用于检测报文传递过程中发生的差错，如果对校验和进行加密，则可以防范报文传递过程中人为地篡改报文内容。

这里会产生这样的疑问：数据加密传输技术不是也可以保证数据传输过程中的完整性吗？为什么还需要单独研究数据完整性传递的问题？实际上对具有校验和的整个报文进行加密确实可以同时提供数据的保密性和完整性传递。但是，数据保密性传递和数据完整性传递是可以分离的两种不同类型的安全需要。例如某个供应商希望向其用户发送一个产品优惠活动的通告，他不希望保密性传递，仅仅希望完整地将该通告传递给他的用户。如果这时还是对整个报文进行加密，就会毫无必要地消耗发送方和接收方的计算资源，降低网络数据传递的性能。

数据加密传输技术和数据完整传输技术也可以直接应用于网络安全中。但是，在网络环境下不仅涉及到通信双方之间的数据传输，还会涉及到多方之间的数据传输。这样，就使得数据加密传输技术变得更加复杂。

1.1.3　计算机安全技术

计算机安全技术是一种在多用户环境下，保证用户数据处理和存储保密性、完整性和计算系统可用性的技术。它包括用户身份标识和验证技术、对计算资源的访问控制技术，以及数据加密存储技术。

数据加密存储技术是密码技术在数据存储方面的应用，多用户计算机系统中的用户身份标识和验证技术通常采用的是用户名和用户口令管理系统。计算机安全技术中最具有特色的内容是访问控制模型及其实现机制。

为了保证存放在计算机系统中的数据安全，美国军方从 20 世纪 60 年代就开始资助计算机系统访问控制的研究，包括对计算机系统中文件进行创建、删除、读、写、执行的权限控制研究。计算机安全技术的研究在 20 世纪 70 年代和 80 年代取得了丰硕的成果，提出了诸如 Bell-LaPadula 模型、Biba 模型等一系列著名的访问控制模型，以及相应的实现机制。这些访问控制模型和机制可以直接应用于网络安全中。

网络安全中的防火墙技术实际上并没有涉及全新的理论，它是访问控制模型及其实现机制在网络环境下的具体应用。

1.1.4　数据安全技术

数据安全技术是一种保证数据在采集、存储、传递、加工和访问过程中的保密性、完整性和可用性的技术。这是以数据为核心的安全技术，是密码技术、计算机安全和网络安全技术的应用技术。

数据安全技术是以数据为主体构造的安全风险模型作为防范目标的一类安全技术。数据

安全与处理数据过程中涉及的系统相关。如果数据仅仅存储在多用户计算机环境下，则数据安全技术只涉及到计算机安全技术，以及数据存储介质的安全技术，例如磁带防电磁干扰、防潮湿霉变技术等。

如果数据需要在网络环境下传递和存储，这样，数据安全就需要涉及到网络安全技术。从这个角度看，数据安全技术与网络安全技术具有共同关心的安全问题。

1.1.5 信息安全技术

信息安全技术是一种保证信息在采集、存储、传递、加工和访问过程中的保密性、完整性和可用性的技术。这是以信息为核心的安全技术，广义上讲，它是密码技术、通信安全技术、计算机安全技术、网络安全技术的应用技术；狭义上讲，它仅仅是研究信息安全编码的技术。

根据信息载体的不同，信息可以分成纸面信息和电子信息。从有文字开始起，人类就开始涉及纸面信息的安全问题。放在信封中传递书信就是一种信息安全传递方法，而恺撒密码（见“传统密码学概述”一节）是一种较为古老的数据编码的信息安全传递方法。现在信息安全技术通常是针对电子信息的安全控制技术。

在学术研究领域，“信息安全”主要侧重于信息安全编码的研究；在国家科技发展的战略规划中，“信息安全”主要是指广义的信息安全技术，其中包括了密码技术、通信安全技术、计算机安全和网络安全技术。

1.2 网络安全基本概念

网络安全是在通信安全、计算机安全和密码技术的基础上建立的一种网络环境下的安全可控技术体系，其目的是保证网络系统本身，以及网络系统内部存储和传递的数据的保密性、完整性和可用性。

网络安全不同于通信安全和计算机安全技术，它是在网络环境下提供数据安全的功能，而不是在某个通信环境、或者某个计算机系统内提供数据安全功能。另外，网络安全还提供对网络系统自身的安全防护功能。

1.2.1 网络安全目标

根据网络安全的定义，网络安全的目标主要涉及两个方面的内容：数据在网络系统中传递和存储的安全性，网络系统本身的安全性。

安全性是一个比较抽象的特性，为了理解网络安全，必须进一步了解“安全性”的内涵。在网络安全中，安全性通常表示保密性、完整性和可用性[1]。

保密性通常指网络系统中信息的隐藏性。网络系统内传递的数据具有保密性就是指即使传递的数据中途被截获，截获方也无法获取数据中表示的信息。网络系统结构以及配置具有保密性是指非授权网络用户无法通过嗅探网络中传递的分组等非法手段，获取有关网络结构及其配置数据等网络系统信息。

完整性通常指网络系统中信息的不可篡改性。网络系统内传递的数据具有完整性就是指

该数据在传递过程中具有防范非法篡改的特性，这样，可以保证接收方完整地接收到发送方发送的数据。网络系统结构以及配置具有完整性是指非授权网络用户无法篡改网络结构和配置信息的特性。

可用性通常指网络系统及其存储在网络中的数据始终处于可以访问、可以使用的状态。可用性是网络安全中一个十分重要的指标。目前在网络安全中最大的威胁是“拒绝服务（英文缩写 DOS）”攻击。这种攻击不是窃取网络中的信息，也不是篡改网络中的存储或传递的信息，而是通过恶意使用网络，使得网络处于不可使用状态。

从网络用户角度看，网络安全目标就是保证在网络系统中传递和存储数据的保密性和完整性，保证网络系统的可用性。为了保证网络系统的可用性，网络管理员必须保证网络系统结构和配置文件的保密性和完整性。

在信息安全中，“安全性”还包括可鉴别性和不可抵赖性。可鉴别性是指对用户的身份可以标识和验证特性，而不可抵赖性是指用户对自己完成的操作具有不可隐藏、不可否认的特性。我们认为，在网络安全环境下，这两个特性都可以是保密性和完整性中隐含的特性。例如，如果系统提供了保密性，则系统必须首先明确哪些用户是合法阅读保密数据的用户，这样，系统必须对用户具有可鉴别性。如果系统提供了完整性，则系统可以保证数据确实是经过身份验证的数据源端发送给接收端的，而且没有被篡改的数据。这样，系统在某种意义上具备了不可抵赖性。

这里不可抵赖性是一个比较复杂的问题，在某种程度上的限制条件比“完整性”更加严格。不可抵赖性要求双方交互的数据必须具有第三方可以验证的“完整性”，这里涉及到网络安全中的信任域的划分问题。网络交互双方如果确定身份之后，就成为相互信任的交互方，则相互进行完整性验证就可以满足安全要求。如果双方不信任，则需要具有除了数据发送方之外任何人都无法篡改的“完整性”。不可抵赖性是指在后一种假设条件下的强“完整性”，所以，单独强调“不可抵赖性”在实际网络应用中也具有一定的价值。数字签名（见“数字签名”一节）就是提供这种“不可抵赖性”的安全技术。

1.2.2　网络安全技术组成

由于计算机网络可以看作是基于通信系统之上的计算机互连系统，所以，网络安全技术包括了通信安全技术和计算机安全技术，还包括了数据安全在网络环境下的应用技术。

从一方面看，不安全的计算机系统连接到网络之后，可能会导致不安全的网络系统。同样，基于不安全的通信系统之上的网络系统，也可能成为不安全的网络系统。从另一方面看，一个真正安全的网络系统可以构架在不安全的通信系统，也可以连接不安全的计算机系统。从这个意义上讲，网络安全又超越了通信安全和计算机安全技术。

总体看，网络安全技术包括身份验证、访问控制、攻击检测、网络数据安全技术以及网络应用安全技术。虽然密码技术在网络安全技术中也扮演一个十分关键的、不可缺少的角色，但是，密码技术并不是网络安全中研究的内容。密码学只是学习、研究和开发网络安全技术中需要学习和应用的一种理论和方法。这些技术的相互依赖关系以及与密码技术的依赖关系如图 1.1 所示，这些技术共分成 3 层，上层技术依赖于下层技术。

身份验证是源于通信安全的一种技术，主要是验证网络环境下交互双方的身份，并且保证合法交互双方数据传递的完整性。身份验证技术是网络安全中的一项最为基本的技术，它

是网络安全应用中的不可缺少的一项技术，也是目前研究和应用较为成功的一项技术。

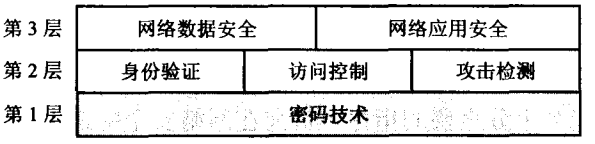

图 1.1 网络安全技术的组成

访问控制是源于计算机安全的一种技术，主要是在网络环境下控制对某些区域或者某些资源的访问。访问控制技术是具体实现网络安全控制策略的技术，它是网络安全应用中的一项关键技术，也是一项不可缺少的技术。

攻击检测技术是网络安全中最具有特点的一种技术，它包括网络环境下的入侵和攻击检测技术、网络蠕虫病毒防范技术。虽然计算机安全技术也研究安全检测和病毒防范技术，但是，网络安全中研究的网络攻击检测和网络病毒防范技术的深度和复杂程度都远远超出了计算机安全研究的范围。网络环境下的病毒防范技术主要是针对通过网络传递的蠕虫病毒，网络蠕虫已经成为目前计算机系统中危害最大的病毒。攻击检测技术应该是网络安全应用中不可缺少的一项技术，但是，目前这方面研究和开发并不完善。

网络数据安全技术是身份验证、访问控制等网络安全技术在网络传送系统上的具体应用，其目的是对已有的网络传送系统进行安全加固，使得已有网络中的数据传递具有保密性和防御攻击的能力。

网络应用安全技术是身份验证、访问控制、攻击检测等网络安全技术在网络应用系统中的具体应用，例如安全电子邮件技术、安全万维网服务技术等等。由于网络应用必须涉及到网络数据的传送，所以，某些网络应用安全技术需要基于网络数据安全技术。

密码技术是网络安全中不可缺少的一项应用技术，但它不是网络安全中研究和开发的一项技术。所以，在图中采用阴影模块表示。

下面一节将简要介绍网络安全中的三大基础技术：身份验证、访问控制和攻击检测技术，以及两类应用技术：网络数据安全技术和网络应用安全技术。

1.2.3 网络安全关键技术

目前网络环境下主要的安全威胁可以分成以下几种类型[4]：假冒型威胁、窃听型威胁、篡改型威胁、重播报文攻击、分布式拒绝服务攻击以及网络蠕虫攻击。

假冒型威胁，是指假冒网络主机或者假冒网络用户访问某机构内部网络系统或内部网络服务器（如图 1.2（a）所示）。例如在因特网应用初期常常通过 IP 地址限制主机对公共因特网的访问，这时，有人就假冒有权限访问公共因特网的 IP 地址，获得公共因特网的访问权限。

窃听型威胁，是指窃听网络上传递的报文（如图 1.2（b）所示）。例如攻击者可能窃听网上交易的报文，获取他人的信用卡信息。这样，就可以盗用他人信用卡在网上进行消费。

篡改型威胁，是指篡改网络上传递的报文（如图 1.2（c）所示）。例如攻击者可能截获网上交易传递的报文，更改报文中的关键数据（例如更改银行账户信息，将转入的账户更改为攻击者的账户），进行网络犯罪活动。