北京高等教育精品教材建设项目立项

高等学校教材·计算机教学丛书

数字鉴别与认证

主　编：蔡永泉
编　写：周艺华　姜　楠　杨宇光

北京航空航天大学出版社
BEIHANG UNIVERSITY PRESS

高等学校教材·计算机教学丛书
北京高等教育精品教材建设项目立项

数字鉴别与认证

蔡永泉　主编
周艺华
姜　楠　编写
杨宇光

北京航空航天大学出版社
BEIHANG UNIVERSITY PRESS

内 容 简 介

数字鉴别与认证涉及理论与应用两方面的内容。第一篇以密码学为基础的数字鉴别与认证；第二篇以人的生理特性为特征的鉴别与认证；第三篇以量子密码学为基础的鉴别与认证。读者通过本书学习，不仅能掌握基本理论与方法，还能学到实际应用技巧。本书可以作为高校计算机专业及相关专业，高年级本科生和研究生的教材，也可以作为网络安全工程技术人员的参考书。

图书在版编目(CIP)数据

数字鉴别与认证 / 蔡永泉主编. --北京 :
北京航空航天大学出版社，2011.7
ISBN 978-7-5124-0262-1

Ⅰ. ①数… Ⅱ. ①蔡… Ⅲ. ①电子计算机—密码技术
Ⅳ. ①TP309.7

中国版本图书馆 CIP 数据核字(2011)第 222324 号

数字鉴别与认证

蔡永泉 主编

责任编辑 文幼章

*

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(邮编 100191) http://www.buaapress.com.cn

发行部电话：(010)82317024 传真：(010)82328026

读者信箱：bhpress@263.net 邮购电话：(010)82316936

涿州市新华印刷有限公司印装 各地书店经销

*

开本：787×1 092 1/16 印张：16.25 字数：416 千字

2011 年 7 月第 1 版 2011 年 7 月第 1 次印刷 印数：3 000 册

ISBN 978-7-5124-0262-1 定价：30.00 元

总 前 言

随着科学技术、文化、教育、经济和社会的发展，计算机教学进入了我国历史上最火热的年代，欣欣向荣。就计算机专业而言，全国开办计算机本科专业的院校在2004年之初有505所，到2006年已经发展到771所。另外，在全国高校中的非计算机专业，包括理工农医以及文科（文史哲法教、经管、文艺）等专业，按各自专业的培养目标都融入了计算机课程的教学。过去出版界出版了一大批计算机教学方面的各类教材，满足了一定时期的需求，但是还不能完全适应计算机教学深化改革的要求。

面对《国家科学技术中长期发展纲要（2006年—2020年）》制订的信息技术发展目标，计算机教学也要随之进行改革，以便提高培养质量。教学要改革，教材建设必须跟上。面对各层次、各类型的学校和各类型的专业都要开设计算机课程，就应有多样化的教材，以适应各专业教学的需要。北京航空航天大学出版社是以出版高等教育教材为主的，愿对计算机教学的教材建设做出贡献。

为计算机类教材的出版，北京航空航天大学出版社成立了“高等学校教材·计算机教学丛书”编审委员会。出版计算机教材，得到了北京航空航天大学计算机学院的大力支持。该院有三位教育部高等学校计算机科学与技术教学指导委员会（下称教指委）的成员参加编审委员会的工作。其他成员是北京航空航天大学、北京交通大学等6所院校和中科院计算技术研究所对计算机教育有研究的教指委成员、专家、学者和出版社的领导。

我们组织编写、出版计算机课程教材，以大多数高校实际状况为基点，使其在现有基础上能提高一步，追求符合大多数高校本科教学适用为目标。按照教指委制订的计算机科学与技术本科专业规范和计算机基础课教学基本要求的精神，我们组织身居教学第一线，具有教学实践经验的教师进行编写。在出书品种和内容上，面对两个方面的教学：一是计算机专业本科教学，包括计算机导论、计算机专业技术基础课、计算机专业课等；二是非计算机专业的计算机基础课程的本科教学，包括理工农医类、文史哲法教类、经管类、艺术类等的计算机课程。

教材的编写注重以下几点。

1. 基础性。具有基础知识和基本理论，以使学生在专业发展上具有潜力，便于适应社会的需求。

2. 先进性。融入计算机科学与技术发展的新成果；瞄准计算机科学与技术发展的新方向，内容应具有前瞻性。这样，以使学生扩展视野，以便与科技、社会发展的脉络同步。

3. 实用性。一是适应教学的需求；二是理论与实践相结合，以使学生掌握实用技术。

编写、出版的教材能否适应教学改革的需求，只有师生在教与学的实践中做出评价，我们期望得到师生的批评和指正。

“高等学校教材·计算机教学丛书”
编审委员会

“高等学校教材·计算机教学丛书”
编审委员会成员

前 言

随着计算机网络的广泛应用，人们对网络的依赖性越来越大；因此如何在开放的互联网络中构建安全的应用环境就成为信息安全领域亟待解决的迫切问题。

数字鉴别与认证涉及理论与应用两方面的内容。本书始终把握理论与实践紧密结合，使读者通过本书的学习不但能够掌握到基本的理论与方法，还能学习到实际的应用技巧。本书分为三篇，共 10 章。第一篇以密码学为基础的数字鉴别与论证；第二篇以人生理特性为特征的鉴别与论证；第 3 篇以量子密码学为基础的鉴别与论证。

第 1 章绪论。介绍网络信息安全的基本知识、对网络攻击的主要形式、信息安全提供的服务及数字鉴别与认证的功能和用途。

第 2 章经典密码基础。介绍对称和非对称加密算法和密钥管理的有关内容。其中包括 DES 加密算法、IDEA 加密算法、RSA 加密算法、离散对数加密算法、ECC 加密算法、密钥的协商与分发等。

第 3 章报文鉴别的基本原理及方法。首先介绍报文鉴别的基本原理及方法，然后介绍基于加密算法的报文鉴别、基于报文鉴别码的报文鉴别、基于散列函数的报文鉴别。

第 4 章数字签名。首先介绍数字签名的基本原理及方法；然后介绍常规的数字签名算法，包括基于 RSA 的签名、基于离散对数的签名、基于椭圆曲线的签名等；最后介绍与应用密切相关的非常规签名技术，包括盲签名、代理签名、群签名、多重签名、不可否认签名、失败-终止签名等。

第 5 章身份认证。首先介绍身份认证的目标与基础；接着介绍身份认证协议中的信息新鲜性保证技术、基于口令的身份认证、相互认证、单向认证、群组认证、零知识证明技术、认证令牌技术、生物认证技术及身份认证协议中的典型攻击；最后介绍基于对称密钥的 Kerberos、基于公钥证书的认证框架和基于身份的认证框架。

第 6 章多媒体认证。首先介绍多媒体认证的概念及分类，接着详细阐述多媒体认证中的主动式图像认证与被动式图像认证技术。

第 7 章生物识别技术。首先介绍生物识别技术的特征、过程及系统设计方法；接着详细阐述常用的生物识别中的指纹识别技术、静脉识别技术、面像识别技术、虹膜识别技术、视网膜识别技术等；最后对生物识别技术存在的问题进行分析。

第 8 章量子密码基础。首先介绍了量子力学五大公设；然后介绍量子力学的基本原理，诸如量子 Heisenberg 测不准原理、量子不可克隆定理和非正交量子态不可区分定理等；最后介绍量子的信息特性，如量子位、量子门、量子隐形传态等。

第 9 章量子身份认证。首先介绍共享信息型量子身份认证和共享纠缠态型量子身份认证；然后介绍量子身份认证协议设计的基本要求和未来发展方向。

第 10 章量子数字签名。首先介绍了量子数字签名设计中涉及的几个概念，如量子一次一密、量子单向函数以及量子 Swap Test 等；接着介绍几种典型的量子数字签名方案，包括基于量子单向函数的量子数字签名方案、基于对称密码的针对量子态的量子数字签名和量子门限

签名等;最后介绍量子数字签名设计的基本要求和未来发展方向。

本书由蔡永泉主编。

第1、第2、第3、第4、第5章由周艺华编写;第6章、第7章由姜南编写;第8、第9、第10章由杨宇光编写。本书三篇相互独立,读者可根据需求任选某一篇。

本书是作者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讲课过程中形成的,可以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书,也可作为从事计算机网络安全工程技术人员的参考书籍。本书是北京高等教育精品教育建设项目,也得到了北京工业大学重点课程(群)优秀教学团队建设项目、国家自然科学基金、教育部博士点专项科研基金和北京市自然科学基金的资助。

在编写过程中不可避免出现这样或那样的错误,敬请读者指正。

作者 2010 年 10 月

目 录

第1章 绪 论

1.1 概 述

随着网络技术的飞速发展、信息系统商业化应用的进一步加快以及密码学研究的重大进展，各种新兴的网络应用层出不穷，电子商务、电子政务、网络金融、网络媒体、网络对抗迅速兴起，应用领域逐步扩大，涉及政府、军事、文教、商业、金融等各个领域。尤其是随着全球 Internet 的发展，人们能以最快的速度、最便利的方式以及最低廉的价格获得最新的信息，从某种意义上来讲，人们真正有了“千里眼”和“顺风耳”。人们可以自由地阅读世界新闻，毫无约束的同远在国外的朋友聊天，实时地了解股票行情等。

正如任何事物总有它的两面性一样，Internet 在给人们带来了开放、自由、便利的同时，也打开了“潘多拉之盒”。遍布全球的黑客，利用网络和系统的漏洞，肆意攻击各种业务应用系统和网站，造成巨大的经济损失，搅得全球不安。机密信息在网络上被泄漏、篡改和假冒，计算机病毒和垃圾邮件肆意传播，不良信息传播给青少年的成长带来负面影响，计算机犯罪呈上升趋势。Financial Times 做过的统计表明，平均 20 s 就有一个网络遭到入侵，网络安全事件时有发生。例如，1979 年，美国少年米尼克成功打入“北美防空指挥中心电脑系统”，偷看了美国瞄准前苏联所有核弹头的绝密数据资料；1990 年，在海湾战争中，美军首次把网络攻击手段应用于实战。早在战前，美军就在伊拉克进口的一批计算机散件中预置了带病毒的芯片。战争开始不久，伊拉克的整个防空指挥控制网络即遭受病毒感染，组织指挥陷入混乱，几乎丧失了防空作战能力。短短 42 天，伊拉克伤亡 10 多万人，而美军只损失 126 人；1995 年，俄罗斯黑客用笔记本电脑成功地从纽约花旗银行非法转移资金 370 万美元；1999 年，南联盟及俄罗斯计算机高手成功地侵入美国白宫网站，使该网站无法工作。如何在享受计算机网络给人们带来便利的同时，满足信息安全的需要，成为计算机网络亟待解决的迫切问题，如信息加密技术、数字鉴别(identification)与认证(authentication)技术、防火墙技术、病毒检测技术、入侵检测技术、漏洞扫描技术、量子计算技术应运而生。数字鉴别与认证是信息安全领域的研究热点，涉及数字鉴别与认证两个方面：数字鉴别又称为报文鉴别，在多媒体数字鉴别领域中又称为多媒体认证，指的是对数据完整性的鉴别；数字认证又称为身份认证或身份鉴别，指的是对用户身份真实性的核实或鉴别。随着计算机计算速度提高、功能增强和算法复杂度的加大，特别是量子并行算法的提出，基于数学复杂性的经典密码体制的安全性受到严峻挑战，因此人们将数字鉴别与认证的研究扩展到量子密码领域，利用量子力学的基本原理和量子效应可实现通信信息的完整性认证以及通信方身份真实性的认证。只有通过有效的数字鉴别与认证，才能核实用户身份的真实性、数据的完整性，有效地防止发送方对数据的抵赖。抵御网络犯罪分子的入侵，电子商务、网上银行、电子政务等业务才能有效地展开。因而，近年来与数字鉴别及认证相关的技术，如数字签名技术、PKI 技术、IBE 技术、交互式零知识证明技术、生物认证技术以

及量子签名与认证技术等得到了深入的研究和发展。

1.2 网络信息安全的根源

产生网络信息安全问题的根源可以从以下几个方面分析：网络自身的缺陷、网络的开放性、技术发展和人为的因素。

1.2.1 网络自身的安全缺陷

网络自身的安全缺陷主要是指协议的不安全。导致协议不安全的主要原因：Internet 从建立开始就缺乏安全的总体构想和设计；Internet 起源的初衷是方便学术交流和信息流通，并非商业目的；Internet 所使用的 TCP/IP 协议是在假定的可信环境下，为网络互联专门设计的，本身缺乏安全措施的考虑。具体表现在 TCP/IP 协议的各层中。

① 互联层：在 IP 层 TCP/IP 只根据 IP 地址进行数据包的寻址，没有安全认证和保密机制。

② 传输层：TCP 连接是建立在“三次握手”的基础上的，也没有认证和保密机制，能被欺骗、截取、操纵。

如图 1.1 所示，设发起方 A 和被发起方 B 进行通信，主机 A 的 TCP 向主机 B 的 TCP 发出连接请求报文段。其首部的同步比特 SYN 应置 1，同时选择一个序号 X，表明在后面传送数据时的第一个数据字节的序号是 X。

主机 B 的 TCP 收到连接请求报文段后，如同意，则发回确认。在确认报文段中应将 SYN 置为 1，确认序号应为 $X+1$，同时也为自己选择一个序号 Y。主机 A 的 TCP 收到此报文后，还要向 B 给出确认，其确认序号为 $Y+1$。这个过程就叫做三次握手。通过这样一个简单的过程，发起方 A 与接收方 B 之间就建立起了一个有效的连接。

在这个连接过程中，如果发起方 A 发送的连接信息不是被合法的用户 B 收到，而是被一个非法的用户 C 收到，发起方就会和一个非法的用户 C 建立连接。这样就造成了一个非法的连接过程，使信息发往一个非法的用户。这是由于在开始建立 TCP/IP 协议时只考虑建立有效连接问题，而没有考虑安全问题造成的。造成上述安全隐患在当时的安全条件下是不能预料到的。另外，UDP 也容易受到 IP 源路由攻击和拒绝服务攻击的影响。

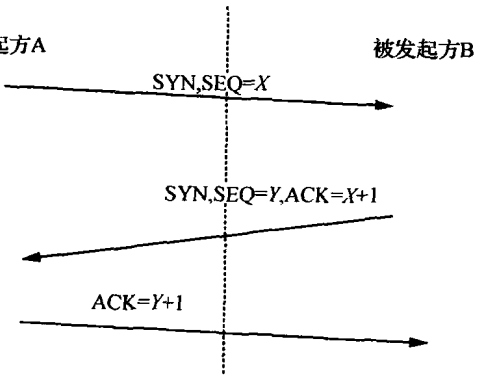

图 1.1 TCP 连接的三次握手

应用层：应用层在认证、访问控制、完整性、保密性等很多安全问题上都存在安全隐患。如 finger：在 TCP/IP 协议中，finger 只需要一个 IP 地址便可以提供许多关于主机的信息。谁在登录、登录时间、登录地址等，这对于一个训练有数的黑客来讲 finger 命令就可以成为进入主机的一把利刃。如匿名 FTP，虽然是一个合法的账号，但它不应具有创建文件和目录的权限；否则，黑客完全可以在一个具有写权限的目录内设置一个“特洛依木马”。再如远程登录在网

络上运行 telnet，rlogin 等远程登录命令，可以跨越网络传输口令；而 TCP/IP 对所有传输的信息又不加密，所以黑客只要在所攻击的目标主机的 IP 包所经过的一条嗅探器程序，就可以截获目标命令。

1.2.2 网络的开放性因素

网络的开放性使得计算机网络的触角伸向了地球的各个角落，渗透到每个领域。它正在对人们的生活和工作方式产生前所未有的影响，日渐成为人们生活中不可缺少的组成部分。

网络的开放性主要表现为：业务基于公开的协议；连接是基于主机上的社团彼此信任的原则；远程访问使得各种攻击无须到现场就能得手。

1.2.3 技术发展因素

随着计算机网络的飞速发展，各种新技术层出不穷，比如分布式计算、网格计算、云计算、量子计算等，大大提高了网络的计算能力。原来被认为是安全的密码算法在多年之后就会变得不再安全。比如，1994 年 Bellcore 公司的阿杰恩、伦斯特拉等人，通过 Internet 使用 1 600 台计算机，历时 8 个月成功破译了 RSA 最初发表时使用的密钥。

量子信息科学的研究和发展导致了量子计算机、量子通信和量子密码的出现。而量子计算机最直接的应用领域之一就是密码破译。一旦量子计算机成为现实，目前使用的公钥密码将被攻破，现有基于经典密码学的数字鉴别与认证方案的安全性将大打折扣，因此各种抗量子密码技术及量子签名与认证技术在近几年得到了广泛的关注和研究，并取得了较快的发展。原则上，以数学为基础的密码体制终究会被攻破，而基于物理规律的密码体制是不可能被攻破的。量子密码学作为密码学和量子力学结合的产物。它以量子力学为基础，利用系统所具有的量子性质，使得“一次一密”密码真正能应用于实际，且成本低廉。量子密码学的安全性是由“海森堡测不准原理”或“量子相干性”及“单量子不可克隆定理”来保证的，这一点不同于以往的以数学为基础的密码体制。量子密码学具有可证明的安全性，而且还具有其他密码体制所没有的特性：对窃听者存在的可检测性。这些特性使得量子密码学具有以往密码体制所没有的优势，因而受到密码学界和物理学界的高度重视。

无论是经典密码体制自身的缺陷，还是量子计算机带来的潜在威胁，两者都迫使人们必须设计出不受攻击者计算能力影响的、具有无条件安全性的密码体制，因此各种抗量子计算攻击能力的密码技术及量子签名与认证技术在近几年得到了广泛的关注和研究，并取得了较快的发展。随着光通信的不断发展，量子密码通过光纤传输将成为现实，量子密码学有可能成为光通信网络中信息安全的有力工具。而且在将来，要对付拥有量子计算能力的密码破译者，量子密码学将可能是唯一的选择。

1.2.4 人为因素

人是信息活动的主体，是引起网络信息安全问题的最主要的因素。主要包括以下三方面的内容。

1. 人为的无意失误

人为的无意失误主要是指用户安全配置不当造成的安全漏洞，包括用户安全意识不强、用户的口令设置不当，用户将自己的账号信息与别人共享、用户在使用软件时未按要求进行正确

的设置。

2. 黑客攻击

这是人为的恶意攻击，是网络信息安全的最大威胁。黑客一词来源于20世纪60年代的美国麻省理工学院，大意是电脑系统非法入侵者。这是一类闯入计算机网络系统盗取信息、故意破坏他人财产、使服务中断或仅仅为了显示他们可以做什么的人。黑客们对电脑非常着迷，自认为比他人有更高的才能，因此，只要他们愿意，就闯入某些信息禁区，开玩笑或恶作剧，有时干出违法的事。他们常以此作为一种智力上的挑战，好玩、刺激可能是他们最初的动机。但当有利可图时，很多人往往抵制不住诱惑而走上犯罪的道路。

信息战也是开展黑客攻击的一个非常重要的理由。为了减少投入、共享信息、增加迂回路由，军网与民网逐步走向融合，但有极少数核心部分完全独立以外。如美国有95%的军用网络与民用网络相连，由此推动了黑客和网络安全防护的较量，不但敌对双方为了成功进入对方的军事系统培养了大批黑客，也由此引起了许多业余黑客研究网路攻击的兴趣。

在英文中，黑客有两个概念：Hacker和Cracker。Hacker是这样一类人，他们对钱财和权利蔑视，而对网络本身非常专注。他们在网上进行探测性的行动，帮助人们找到网络的漏洞，可以说他们是这个领域的绅士。但是，Cracker不一样，他们要么为了满足自己的私欲，要么受雇于一些商业机构，具有攻击性和破坏性。从简单的修改网页到窃取机密数据，甚至破坏整个网络系统。因其危害性较大，Cracker已称为网络安全真正的、主要的防范对象。

3. 管理不善

安全需求通常不能单靠密码算法和协议来满足，还需要某些程序的制定和法律的遵守才能达到期望的效果。例如，信件的隐私是通过一个被认可的邮件服务发送封装的信封来提供的。信封的物理安全是有限的，因此，还需要制定法律以规定未授权打开信封的行为是违法的。对网络信息系统的严格管理是避免受到攻击的重要措施。据统计，美国90%以上的IT企业对黑客攻击准备不足，75%～85%的网站都抵挡不住黑客的攻击。总之，管理的缺陷也可能使系统内部人员泄漏机密，为一些不法分子的利用制造可乘之机。

1.3 网络安全服务与机制

1.3.1 安全服务

安全服务就是加强数据处理系统和信息传输的安全性的一类服务。其目的在于利用一种或多种安全机制阻止安全攻击。对网络信息系统而言，通常需要以下几个方面的安全服务。

1. 机密性(confidentially)

机密性是指信息不泄露给非授权的用户、实体或过程，或不供其利用的特性。它确保在一个计算机系统中的信息和被传输的信息仅能被授权的各方得到。机密性可保护数据免受被动攻击。

① 防止对信息内容的析出。机密性能够确定不同层次的保护，如广义保护可以防止一段时间内两个用户之间传输的所有用户数据被泄漏；狭义保护可以保护单一信息中某个特定字段的内容。

② 防止对于通信量分析。机密性要求一个攻击不能在通信设备上观察到通信量的源端

和目的端、通信频率、通信长度或其他特征。

2. 完整性(integrity)

完整性是数据未经授权不能进行改变的特性,即信息在存储或传输过程中不被修改、不被插入或删除的特性。它保证收到的数据确实是授权实体所发出的数据。

完整性服务旨在防止以某种违反安全策略的方式改变数据的价值和存在的威胁。改变数据的价值是指对数据进行修改和重新排序;而改变数据的存在则意味着新增、删除或替代它。与机密性一样,完整性能够应用于一个信息流、单个信息或一个信息中的所选字段。

面向连接的完整性服务用于处理单个无连接信息,通常只保护信息免受篡改。

对完整性的破坏通常只关注检测而不关注防止,一旦检测到完整性破坏就报告并采取适当的恢复措施。

3. 鉴别(identification)与认证(authentication)

鉴别与认证用于确保一个信息的来源或信息本身被正确地标识,同时确保该标识没有被伪造。在本书中鉴别服务是指对信息内容完整性的甄别,又称为报文鉴别。认证是指对于通信双方而言,确保在连接发起时两个实体是可信的,即每个实体的确是他们宣称的那个实体。认证服务还必须确保该连接不被干扰,使得第三方不能假冒这两个合法方中的任何一方来达到未授权传输或接收的目的。

4. 不可否认性(non-reputiation)

不可否认性是防止发送方或接收方抵赖所传输的信息,要求无论发送方还是接收方都不能抵赖所进行的传输。因此,当发送一个信息时,接收方能证实该信息的确是由所宣称的发送方发来的(源不可否认性)。当接收方收到一个信息时,发送方能够证实该信息的确送到了指定的接收方(宿不可否认性)。

5. 访问控制(access control)

在网络环境中,访问控制是限制或控制通信链路对主机系统和应用程序等系统资源进行访问的能力。防止对任何资源(如计算资源、通信资源或信息资源)进行未授权的访问,即未经授权地使用、泄漏、修改、销毁及颁发指令等。访问控制直接支持机密性、完整性以及合法使用等安全目标。对信息源的访问可以由目标系统控制。控制的实现方式是鉴别或认证。

访问控制是实施授权的一种方法。通常有两种方法用来组织非授权用户访问目标。①访问请求过滤:当一个发起者试图访问一个目标时,需要检查发起者是否被准予访问目标(由控制策略决定)。②隔离:从物理上防止非授权用户有机会访问到敏感的目标。

6. 可用性(availability)

可用性是可被授权实体访问并按需求使用的特性,也就是说,要求网络信息系统的有用资源在需要时可为授权各方使用,保证合法用户对信息和资源的使用不会被不正当地拒绝。例如,网络环境下拒绝服务、破坏网络和有关系统的正常运行等都是对可用性的攻击。网络服务的目标之一就是防止各种攻击对系统可用性的损害。

1.3.2 安全机制

安全机制可分为两类:一类与安全服务有关,是用来实现安全服务的;另一类与管理功能有关,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，也可以同其他机制结合起来使用。加密算法可分为对称密钥(单密钥)加密算法和非对称密钥(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，用来验证已有签字是否与签字者的私有密钥相关。数字签名机制必须保证签字只能使用签字者的私有密钥。

(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。访问控制实体常基于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。

(4) 数据完整性机制

在通信中，发送方根据发送的信息产生一额外的信息(如校验码)，将额外信息加密以后，随信息本体一同发送出去，接收方接收到本信息后，产生额外信息并与接收到的额外信息进行比较，以判断在信息传输过程中信息本体是否被篡改过。

(5) 认证交换机制

用来实现同级之间的认证，可以使用认证的信息，如由发方提供一口令，收方进行验证，也可以利用实体所具有的特征，如指纹、视网膜等来实现。

(6) 路由控制机制

为了使用安全的子网、中继站和链路，既可预先安排网络的路由，也可对其动态地进行选择。安全策略可以禁止带有某些安全标签的信息通过某些子网、中继站和链路。

(7) 防止业务流分析机制

通过填充冗余的业务流来防止攻击者进行业务流分析。填充过的信息要加保密保护才能有效。

(8) 公证机制

公证机制是第三方(公证方)参与数字签名的机制，是基于通信双方对第三方的绝对信任。让公证方具备相应的数字签名、加密或完整性机制等。当实体间互通信息时，由公证方利用所提供的上述机制进行公证。有的公证机制可以在实体连接期间进行实时认证，有的则在连接后进行非实时认证。公证机制既可防止收方伪造签字，或否认收到的信息，又可戳穿发送方对所签发信息的抵赖。

2. 与管理有关的安全机制

(1) 安全标签机制

可以让信息中的资源带上安全标签，以标明其在安全方面的敏感程度或保护级别。可以是显露式或隐藏式的，但都应以安全的方式与相关的对象结合在一起。

(2) 安全审核机制

审核的任务是指探测出和查明与安全有关的事件。要进行审核，必须具备与安全有关的信息记录设备，以便对这些信息进行分析和报告。安全审核机制指的是与安全有关的信息记录设备，分析和报告功能则属于安全管理功能。