21世纪高等职业教育信息技术类规划教材
21 Shiji Gaodeng Zhiye Jiaoyu Xinxi Jishulei Guihua Jiaocai

网络安全技术与实训

（第2版）

WANGLUO ANQUAN JISHU YU SHIXUN

杨文虎 李飞飞 主编　刘志杰 平寒 副主编

- 内容实用
- 提供丰富教学资料
- 附有大量实训内容

人民邮电出版社
POSTS & TELECOM PRESS

21世纪高等职业教[illegible]材
21 Shiji Gaodeng Zhiye Jiac[illegible]cai

网络安全技术与实训

（第2版）

WANGLUO ANQUAN JISHU YU SHIXUN

杨文虎 李飞飞 主编　刘志杰 平寒 副主编

人民邮电出版社
北京

图书在版编目（CIP）数据

网络安全技术与实训 / 杨文虎，李飞飞主编. -- 2版. -- 北京 : 人民邮电出版社，2011.7
21世纪高等职业教育信息技术类规划教材
ISBN 978-7-115-24981-4

Ⅰ. ①网… Ⅱ. ①杨… ②李… Ⅲ. ①计算机网络－安全技术－高等职业教育－教材 Ⅳ. ①TP393.08

中国版本图书馆CIP数据核字(2011)第055791号

内 容 提 要

本书围绕网络安全的定义、标准、模型以及常见的网络安全威胁进行系统介绍和分析，从网络管理与安全防护入手，详细讲述和分析入侵检测、数据加密、身份验证、防火墙以及无线网安全等多方面的理论与技术，同时结合现场工程应用，将网络安全管理技术与主流系统软硬件结合，强调对实践能力的培养。

本书适合作为高职高专院校计算机网络技术专业、信息安全技术专业、计算机应用技术专业等的教材，也可作为广大网络管理人员及技术人员学习网络安全知识的参考书。

21 世纪高等职业教育信息技术类规划教材

网络安全技术与实训（第 2 版）

◆ 主　　编　杨文虎　李飞飞
副 主 编　刘志杰　平　寒
责任编辑　赵慧君

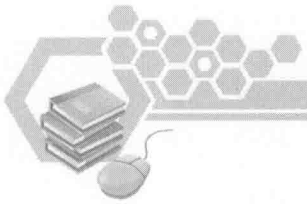
◆ 人民邮电出版社出版发行　　北京市崇文区夕照寺街 14 号
邮编　100061　　电子邮件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
北京鑫正大印刷有限公司印刷

◆ 开本：787×1092　1/16
印张：14.5　　2011 年 7 月第 2 版
字数：372 千字　　2011 年 7 月北京第 1 次印刷

ISBN 978-7-115-24981-4

定价：29.80 元

读者服务热线：(010)67170985　印装质量热线：(010)67129223
反盗版热线：(010)67171154



前言

本书第 1 版出版之后，受到广大读者的关注。为了更好地为读者服务，我们对该书部分内容进行了修订，具体如下。

1. 将第 1 章、第 2 章的内容进行了改写，加入了大量新的知识和实例内容。

2. 对第 7 章和第 8 章做了合并。

此外，为了使本书能够成为适合职业教育特色的实用型教材，我们对本书的体系结构进行了精心的设计，减少了枯燥难懂的理论，取而代之的是设备应用、防护技术等实际操作能力的培养与训练。本书内容的选取涉及面广泛，包含网络安全技术中网络攻击、病毒防护、加密技术、无线安全、入侵检测、防火墙等方面的内容。为了提高本书的实用性，我们引入了大量的实际案例，并设计了 13 个综合实训内容。

本书配套的教学大纲、课程设计、ppt 课件等资源可以到 http://web2.jnrp.cn/jbkc/security/或人民邮电出版社教学服务与资源网（http://www.ptpedu.com.cn）免费下载使用。

本书的参考学时为 96 学时，其中讲授环节为 60 学时，实践环节为 36 学时，各章的参考学时参见下面的学时分配表。

	课程内容	学时分配	
		讲授	实训
第 1 章	网络安全基础	4	
第 2 章	网络攻击与防范	16	8
第 3 章	拒绝服务与数据库安全	4	4
第 4 章	计算机病毒与木马	10	6
第 5 章	安全防护与入侵检测	4	4
第 6 章	加密技术与虚拟专用网	8	4
第 7 章	防火墙	10	6
第 8 章	无线局域网安全	4	4
课时总计		60	36

本书由杨文虎、李飞飞任主编，刘志杰、平寒任副主编。杨文虎负责全书的构思，并编写第 5 章、第 6 章、第 7 章、第 8 章，樊静淳编写第 1 章，李飞飞编写第 2 章，平寒编写第 3 章，刘志杰编写第 4 章，吴鹏编写实训 1、实训 3、实训 13 等。全书由杨文虎统稿、定稿。在编写本书的过程中，我们引用了部分书中的内容，在此对所有的作者表示衷心的感谢。

由于时间仓促，加之编者水平有限，书中难免存在错误和不妥之处，敬请广大读者批评指正。

编　者

2011 年 2 月

目 录

第1章 网络安全基础

本章学习要点

- 掌握网络安全的概念及安全模型
- 掌握安全服务及安全标准
- 了解我国计算机网络安全等级标准
- 掌握常见的安全威胁和攻击
- 了解网络安全的现状与发展趋势

1.1 引言

在社会日益信息化的今天，信息已成为一种重要的战略资源，信息的应用也从原来的军事、科技、文化和商业渗透到当今社会的各个领域，它在社会生产、生活中的作用日益显著。传播、共享和增值是信息的固有属性，与此同时，又要求信息的传播是可控的，共享是授权的，增值是确认的，因此信息的安全和可靠在任何状况下都是必须要保证的。

计算机网络是信息社会的基础，已经进入社会的各个角落。经济、文化、军事和社会生活越来越多地依赖计算机网络。然而，网络本身的开放性在给人们带来巨大便利的同时，也带来了一些不容忽视的问题，计算机网络的安全性成为信息化建设的一个核心问题。

许多在计算机网络中存储、传输和处理的信息是政府宏观调控决策、商业经济信息、银行资金转账、股票证券、科研数据等重要信息，其中很多是敏感信息，甚至是国家机密。由于网络安全的漏洞，导致敏感信息泄露、信息篡改、数据破坏、恶意信息发布、计算机病毒发作等，由此造成的经济损失和社会不良影响难以估计。全世界计算机犯罪正以每年大于100%的速度增长，网络的黑客攻击事件也以每年10倍的速度递增。首例计算机病毒自1988年发现以来，计算机病毒种类的数量正在呈几何级数的速度增长。利用计算机实施金融犯罪已经渗透到了我国金融行业的各项业务。近几年已经掌握和破获

了100多起金融犯罪，涉及金额几个亿。据有关部门统计，国内90%以上的电子商务网站存在着严重的安全漏洞，网络的安全问题正面临着日益严重的威胁。

1.2 网络安全概念

国际标准化组织（ISO）7498-2安全体系结构文献定义，安全就是最小化资产和资源的漏洞。资产可以指任何事物。漏洞是指任何可以造成破坏系统或信息的弱点。

网络安全（Network Security）是一门涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等多种学科的综合性科学。下面给出网络安全的一个通用定义。

网络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、泄露，系统连续可靠正常地运行，网络服务不中断。

从内容上看，网络安全大致包括以下4个方面的内容。

- 网络实体安全：如计算机硬件、附属设备及网络传输线路的安装及配置。
- 软件安全：如保护网络系统不被非法侵入，软件不被非法篡改，不受病毒侵害等。
- 数据安全：保护数据不被非法存取，确保其完整性、一致性、机密性等。
- 安全管理：运行时突发事件的安全处理等，包括采取计算机安全技术、建立安全制度、进行风险分析等。

从特征上看，网络安全包括5个基本要素。

- 机密性：确保信息不泄露给非授权的用户、实体。
- 完整性：信息在存储或传输过程中保持不被修改、不被破坏和不会丢失的特性。
- 可用性：得到授权的实体可获得服务，攻击者不能占用所有的资源而阻碍授权者的工作。
- 可控性：对信息的传播及内容具有控制能力。
- 可审查性：对出现的安全问题提供调查的依据和手段。

1.2.1 安全模型

通信双方想要传递某个信息，需建立一个逻辑上的信息通道。通信主体可以采取适当的安全机制，包括以下两个部分。

- 对被传送的信息进行与安全相关的转换，包括对消息的加密和认证。
- 两个通信主体共享不希望对手知道的秘密信息，如密钥等。

图1.1所示为网络安全的基本模型。

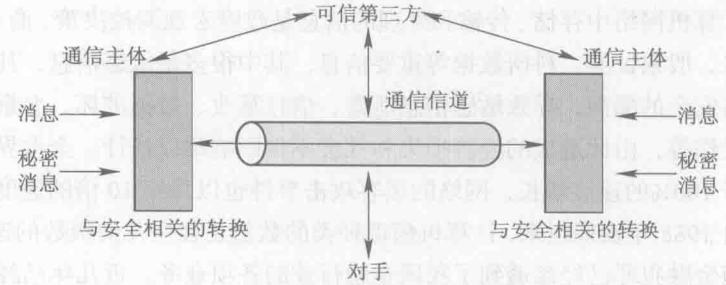


图1.1 网络安全的基本模型

为了获得消息的安全传输，还需要一个可信的第三方，其作用是负责向通信双方分发秘密消息或者在通信双方有争议时进行仲裁。

并非所有的同安全相关的情形都可以用上述安全模型来描述，如目前万维网（WWW）的安全模型就应当另当别论。由于其通信方式大都采用客户/服务器方式来实现，由客户端向服务器发送信息请求，然后服务器对客户端进行身份认证，根据客户端的相应权限来为客户端提供特定的服务，因此，其安全模型可以采用如图 1.2 所示的安全模型来描述。其侧重点在于如何有效地保护客户端对服务器的安全访问，以及如何有效地保护服务器的安全性。

图 1.2　网络安全访问模型

这种安全模型同现实中的黑客入侵相吻合，客户端本身就可以是对手或者敌人，他可以利用大量的网络攻击技术来对服务器系统构成安全威胁，这些攻击可以利用网络服务的安全缺陷、通信协议的安全缺陷、应用程序或者网络设备本身的安全漏洞来实施。

为了有效地保护模型中信息系统的各种资源以及对付各种网络攻击，在模型中加入了守卫（Guard）功能。守卫可以有效地利用安全技术对信息流进行控制，如对客户端进行身份认证、对客户端对服务器的请求信息进行过滤、对服务器的资源进行监视审计等，从而可以抵御大部分的安全攻击。

下面介绍几种常见的网络安全模型。

（1）P^2DR 安全模型

美国国际互联网安全系统公司（ISS）提出的 P^2DR 安全模型是指策略（Policy）、防护（Protection）、检测（Detection）和响应（Response），如图 1.3 所示。

图 1.3　P^2DR 安全模型

P^2DR 安全模型可以描述为

安全=风险分析+执行策略+系统实施+漏洞监视+实时响应

P^2DR 安全模型认为没有一种技术可以完全消除网络中的安全漏洞，必须在整体安全策略的控制、指导下，在综合运行防护工具的同时，利用检测工具了解和评估系统的安全状态，通过适当的反馈将系统调整到相对安全和风险最低的状态，才能达到所需的安全要求。P^2DR 依据不同等级的系统安全要求来完善系统的安全功能、安全机制，是整体的、动态的安全模型，也称为可适应安全模型（Adaptive Network Security Model，ANSM）。

① 策略。安全策略具有一般性和普遍性。一个恰当的安全策略总会把关注的核心集中到最高决策层认为必须值得注意的那些方面。概括地说，当设计所涉及的那个系统在进行操作时，必须明确在安全领域的范围内，什么操作是明确允许的，什么操作是一般默认允许的，什么操作是明确不允许的，什么操作是默认不允许的。建立安全策略是实现安全的最首要的工作，也是实现安全技术管理与规范的第一步。目前，如何能使安全策略与用户的具体应用紧密结合是计算机网络安全系统面临的最关键

问题。因此，安全策略的制定实际上是一个按照安全需求，依照应用实例不断精确细化的求解过程。

安全策略是 P^2DR 安全模型的核心，所有的防护、检测、响应都是依据安全策略实施的，安全策略为安全管理提供管理方向和支持手段。策略体系的建立包括安全策略的制定、评估、执行等。只有对计算机网络系统进行了充分的了解，才能制定出可行的安全策略。

② 防护。防护就是采用一切手段保护计算机网络系统的保密性、完整性、可用性、可控性和不可否认性，预先阻止攻击可以发生的条件产生，让攻击者无法顺利地入侵。因此，防护是网络安全策略中最重要的环节。

防护可以分为三大类：系统安全防护、网络安全防护和信息安全防护。

- 系统安全防护是指操作系统的安全防护，即各个操作系统的安全配置、使用和打补丁等。
- 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数据本身的保密性、完整性和可用性。

③ 检测。安全策略的第二个安全屏障是检测。检测是动态响应和加强防护的依据，是强制落实安全策略的工具，通过不断地检测和监控网络及系统来发现新的威胁和弱点，通过循环反馈来及时作出有效的响应。

网络的安全风险是实时存在的，检测的对象主要针对系统自身的脆弱性及外部威胁，主要包括检查系统本身存在的脆弱性；在计算机系统运行过程中，检查、测试信息是否发生泄露、系统是否遭到入侵，并找出泄漏的原因和攻击的来源。

在安全模型中，防护（P）和检测（D）之间有互补关系。如果防护部分做得很好，绝大多数攻击事件都被阻止，那么检测部分的任务就很少了；反过来，如果防护部分做得不好，检测部分的任务就很多。

④ 响应。响应就是在检测到安全漏洞或一个攻击（入侵）事件之后，及时采取有效的处理措施，避免危害进一步扩大，目的是把系统调整到安全状态，或使系统提供正常的服务。通过建立响应机制和紧急响应方案，能够提高快速响应的能力。

（2）PDRR 安全模型

网络安全的整个环节可以用一个最常用的安全模型——PDRR 模型来表示，如图 1.4 所示。PDRR 是防护（Protection）、检测（Detection）、响应（Response）、恢复（Recovery）4 个英文单词的头一个字母。

PDRR 安全模型中安全策略的前 3 个环节与 P^2DR 安全模型的后 3 个环节的内涵基本相同。最后一个环节“恢复”，是指系统被入侵之后，把系统恢复到原来的状态，或者比原来更安全的状态。系统的恢复过程通常需要解决两个问题：一是对入侵所造成的影响进行评估和系统的重建；二是采取恰当的技术措施。系统的恢复主要有重建系统、通过软件和程序恢复系统等方法。

PDRR 安全模型阐述了一个结论：安全的目标实际上就是尽可能地增加保护时间，尽量减少检测时间和响应时间，在系统遭受到破坏后应尽快恢复，以减少系统暴露时间。也就是说，及时的检测和响应就是安全。

（3）MPDRR 安全模型

MPDRR 安全模型是对 PDRR 模型的进一步完善，如图 1.5 所示。MPDRR 中的 M（Management）是管理。

MPDRR 安全模型是对防护、检测、响应、恢复这 4 个环节进行统一的安全管理和协调，使系统更加安全。

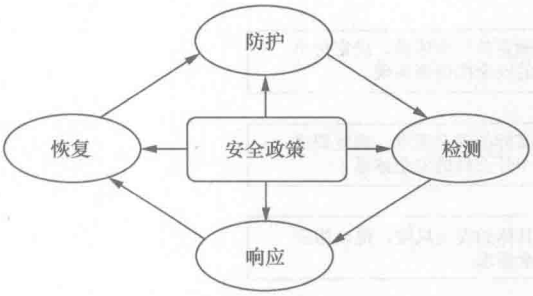


图 1.4　PDRR 网络安全模型

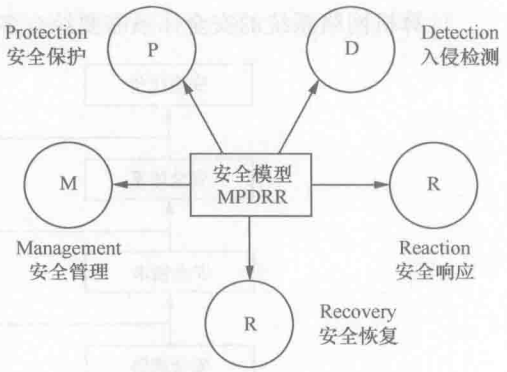


图 1.5　MPDRR 网络安全模型

1.2.2　安全体系

ISO（国际标准化组织）1989 年制定的 ISO/IEC 7498-2，给出了 ISO/OSI 参考模型的安全体系结构，在 OSI 参考模型中增设了安全服务、安全机制和安全管理，并给出了 OSI 网络层次、安全服务和安全机制之间的逻辑关系，定义了 5 大类安全服务，提供这些服务的 8 大类安全机制以及相应的与开放系统互连的安全管理。

1. 安全体系

一般把计算机网络安全看成一个由多个安全单元组成的集合。其中，每一个安全单元都是一个整体，包含了多个特性。可以从安全机制的安全问题、安全服务的安全问题以及开发系统互连（ISO/OSI）参考模型结构层次的安全问题等 3 个主要特性去理解一个安全单元。所以安全单元集合可以用一个三维的安全空间去描述，如图 1.6 所示。图中描述了一个三维的计算机网络安全空间，反应了计算机网络安全中 OSI 模型、安全服务和安全机制之间的关系。

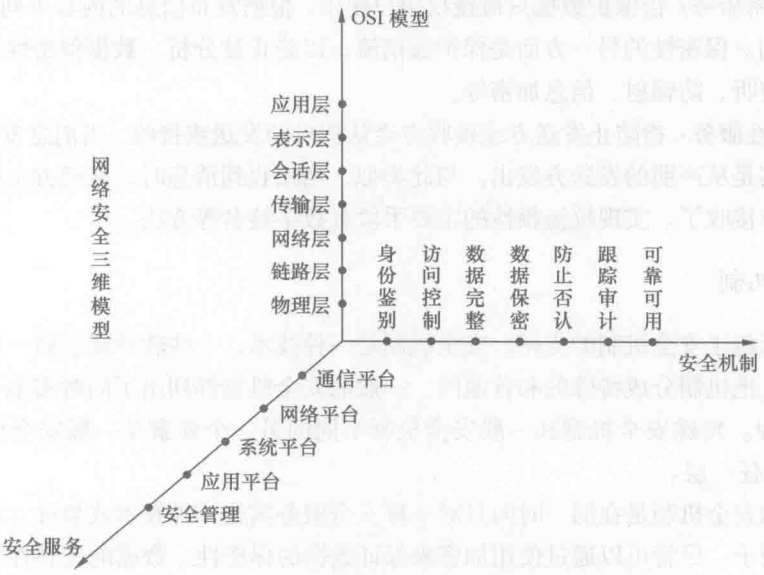


图 1.6　计算机网络系统的安全空间

计算机网络系统的安全体系需要综合多方面去考虑，如图 1.7 所示。

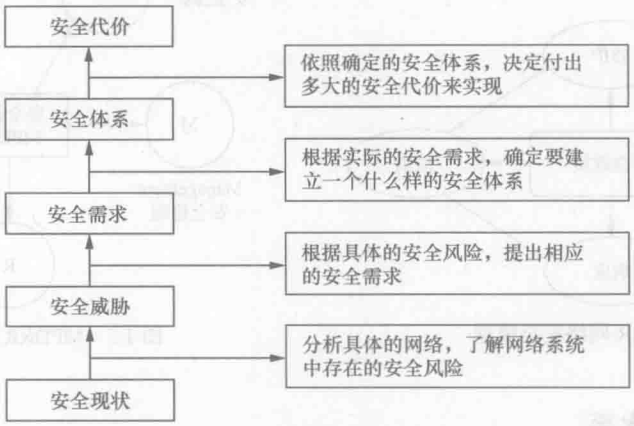


图 1.7　计算机网络系统的安全体系

2. 安全服务

针对网络系统受到的威胁，为了确保系统的安全保密性，ISO 安全体系结构定义了 5 种类型的安全服务，并在物理层、网络层、传输层和应用层上配置安全服务。

① 鉴别服务：它的目的在于保证信息的可靠性。实现身份认证的主要方法包括口令、数字证书、基于生物特征（比如指纹、声音等）的认证等。

② 访问控制服务：确定一个用户或服务可能用到什么样的系统资源，是查看还是改变。一旦一个用户通过认证，操作系统上的访问控制服务确定此用户将能做些什么。

③ 数据完整性服务：指网络信息未经授权不能进行改变的特性，它要求保持信息的原样，即信息的正确生成、正确存储和正确传输。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受到各种原因的破坏。

④ 数据保密服务：指保护数据只被授权用户使用。根据发布信息的内容不同，可以使用几个不同的保护级别。保密性的另一方面是保护通信流，以防止被分析。数据保密性实现的手段包括物理加密、防窃听、防辐射、信息加密等。

⑤ 抗抵赖性服务：指防止发送方或接收方否认消息的发送或接收。当消息发出时，接收方可以证实消息确实是从声明的发送方发出。与此类似，当接收到消息时，发送方也能证实消息确实由声明的接收方接收了。实现抗抵赖性的主要手段有数字签名等方法。

3. 安全机制

安全服务依赖于安全机制的支持。安全机制是一种技术，一些软件或实施一个或更多安全服务的过程。ISO 把机制分成特殊的和普遍的。一般的安全机制都列出了同时实施一个或多个安全服务的执行过程。特殊安全机制和一般安全机制不同的另一个要素是一般安全机制不能应用到 OSI 参考模型的任一层。

一个特殊的安全机制是在同一时间只对一种安全服务实施一种技术或软件。加密就是特殊安全机制的一个例子。尽管可以通过使用加密来保证数据的保密性、数据的完整性和不可否定性，但实施每种服务时都需要不同的加密技术。

ISO 安全体系结构提出了 8 种基本的安全机制，将一个或多个安全机制配置在适当层次上以实现安全服务。

- 加密机制。
- 数字签名机制。
- 访问控制机制。
- 数据完整性机制。
- 认证（鉴别）机制。
- 通信业务填充机制。
- 路由选择控制机制。
- 公证机制。

我们知道，TCP/IP 刚出现时，协议设计者对网络安全方面考虑得较少。随着 Internet 的快速发展，它的各种安全脆弱性逐步体现出来，但是又不能设计一种全新的协议来取代 TCP/IP，因此，相对于 ISO/OSI 的网络安全体系结构，Internet 的安全体系结构有点类似于打补丁，它是在各个层次上加上相应的安全协议来进行处理的，如表 1.1 所示。

表 1.1　　因特网安全体系结构

层次	安全协议
应用层	MOSS　PEM　PGP　S/MIME　SSH　SHTTP　Kerberos
传输层	TCP　SSL
网络层	UDP　IPv6　IPSec　ISAKMP

因特网各层与 ISO/OSI 安全服务的对应关系如表 1.2 所示。

表 1.2　　TCP/IP 各层与 ISO/OSI 安全服务的对应关系

层次	安全协议	鉴别	访问控制	机密性	完整性	抗抵赖性
网络层	IPSec	Y	–	Y	Y	–
传输层	SSL	Y	–	Y	Y	–
应用层	PEM	Y	–	Y	Y	–
	MOSS	Y	–	Y	Y	Y
	PGP	Y	–	Y	Y	Y
	S/MIME	Y	–	Y	Y	Y
	SHTTP	Y	–	Y	Y	Y
	SSH	Y	–	Y	Y	–
	Kerberos	Y	Y	Y	Y	Y
	SNMP	Y	–	Y	Y	–

注：Y=提供　–=不提供。

4. 安全服务和安全机制的关系

安全服务与安全机制有着密切的联系，安全服务是由安全机制来实现的，体现了安全系统的功能。一个安全服务可以由一个或几个安全机制来实现；同样，同一个安全机制也可以用于实现不同的安全服务，安全服务和安全机制并不是一一对应的。它们的关系如表 1.3 所示。

表 1.3　　安全服务和完全机制的关系

服务 \ 机制	数据加密	数字签名	访问控制	数据完整	鉴别交换	业务填充	路由控制	公正机制
鉴别服务	√	√	×	×	√	×	×	×
访问控制	×	×	√	×	×	×	×	×
数据完整	√	√	×	√	×	×	×	×
数据保密	√	×	×	×	×	×	×	×
抗抵赖性	×	√	×	√	×	×	×	√

注：√为该机制可以提供此项安全服务，或与其他机制结合提供安全服务；×为该机制一般不提供此项安全服务。

1.2.3　安全标准

安全标准按照制定的组织和实施的国家不同存在多种标准，一般有 OSI 安全体系技术标准、可信任计算机标准评估准则（TCSEC）和我国的计算机网络安全等级标准。OSI 安全体系技术标准属于国际标准，可信任计算机标准评估准则是由美国制定的，为实现对网络安全的定性评价，该标准认为要使系统免受攻击，对应不同的安全级别，硬件、软件和存储的信息应实施不同的安全保护，而安全级别对不同类型的物理安全、用户身份验证、操作系统软件的可信任性和用户应用程序进行了安全描述。

TCSEC 将网络安全性等级划分为 A、B、C、D 这 4 类共 7 级，如表 1.4 所示，其中，A 类安全等级最高，D 类安全等级最低。

表 1.4　　TCSEC 安全等级

类别	名称	描述	举例
D1	最小保护	该标准规定整个系统都是不可信任的。对硬件来说，没有任何保护；操作系统容易受到损害；对存储在计算机上信息的访问权限没有身份认证	MS-DOS、MS-Windows 3.1、Macintosh System 7.X
C1	选择安全保护	确定每个用户对程序和信息拥有什么样的访问权限	早期的 UNIX 系统
C2	访问控制保护	进一步限制用户执行某些命令或访问某些文件的能力。这不仅基于许可权限，而且基于身份验证级别。另外，这种安全级别要求对系统加以审核	UNIX、XENIX、Novell 3.X 及 Windows NT
B1	标签安全保护	除 C2 的保护外，把用户隔离成各个单元以提高进一步保护	AT&T System V
B2	结构保护	要求计算机系统中所有对象都加标签，而且给设备分配单个或多个安全级别	XENIX、Honeywell MULTICS
B3	安全域级别	使用安装硬件的办法来加强域管理	Honeywell、Federal
A	验证设计	包含了一个严格的设计、控制和验证过程。与前面提到的各级别一样，这一级包含了较低级别的所有特性。其设计必须是从数学上经过验证的，而且必须进行对秘密通道和可信任分布的分析	Honeywell SCOMP

1. D1 级

D1 级是最低的安全形式，整个计算机是不可信任的。拥有这个级别的操作系统就像一个门户大开的房子，任何人可以自由进出，是完全不可信的。对于硬件来说，是没有任何保护措施的，操作系统容易受到损害，没有系统访问限制和数据限制，任何人不需要任何账户就可以进入系统，不受任何限制就可以访问他人的数据文件。

属于这个级别的操作系统有 DOS、Windows、Apple 的 Macintosh System 7.1。

2. C1 级

C 级有两个安全子级别：C1 和 C2。

C1 级，又称有选择地安全保护或称酌情安全保护（Discretionary Security Protection）系统，它要求系统硬件有一定的安全保护（如硬件有带锁装置，需要钥匙才能使用计算机），用户在使用前必须登记到系统。另外，作为 C1 级保护的一部分，允许系统管理员为一些程序或数据设立访问许可权限等。

它描述了一种典型的 UNIX 系统上的安全级别。用户拥有注册账号和口令，系统通过账号和口令来识别用户是否合法，并决定用户对信息拥有什么样访问权。

C1 级保护不足之处在于用户直接访问操作系统的根用户。C1 级不能控制进入系统的用户访问级别，所以用户可以将系统中的数据任意移走，他们可以控制系统配置，获取比系统管理员允许的更高权限。

3. C2 级

C2 级又称访问控制保护，能够实现受控安全保护、个人账户管理、审计和资源隔离。

C2 级针对 C1 级的不足之处增加了几个特征，引进了访问控制环境（用户权限级别）的特征，该环境具有进一步限制用户执行某些命令或访问某些文件的权限，而且还加入了身份验证级别。另外，系统对发生的事情加以审计（Audit），并写入日志当中。审计可以记录下系统管理员执行的活动，同时还附加有身份验证。审计的缺点在于它需要额外的处理器时间和磁盘资源。

使用附加身份认证就可以让一个 C2 系统用户在不是根用户的情况下有权执行系统管理任务。不要把这些身份验证和应用于程序的 SGID 和 SUID 相混淆，身份认证可以用来确定用户是否能够执行特定的命令或访问某些核心表。

授权分级是系统管理员能够给用户分组，授予他们访问某些程序的权限或访问分级目录。

用户权限可以以个人为单位授权用户对某一程序所在的目录进行访问。如果其他程序和数据也在同一目录下，那么用户也将自动得到访问这些信息的权限。

能够达到 C2 级的常见操作系统有 UNIX 系统、XENIX、Novell 3.x 或更高版本、Windows NT。

4. B1 级

B 级中有 3 个级别，B1 级即标号安全保护（Labeled Security Protection），是支持多级安全（如秘密和绝密）的第一个级别，这个级别说明一个处于强制性访问控制之下的对象，系统不允许文件的拥有者改变其许可权限。

B1 级安全措施的计算机系统随操作系统而定。政府机构和系统安全承包商是 B1 及计算机系

统的主要拥有者。

5. B2级

B2级又叫做结构保护（Structured Protection），要求计算机系统中所有的对象都加标签，而且给设备（磁盘、磁带和终端）分配单个或多个安全级别。这里提出了较高安全级别的对象与另一个较低安全级别的对象通信的第一个级别。

6. B3级

B3级又称安全域级别（Security Domain），使用安装硬件的方式来加强域。B3级可以实现以下功能。

① 引用监视器参与所有主体对客体的存取，以保证不存在旁路。

② 审计跟踪能力强，可以提供系统恢复过程。

③ 支持安全管理员角色。

④ 用户终端必须通过可信通道才能实现对系统的访问。

⑤ 防止篡改。

7. A级

A级也称为验证保护级或验证设计（Verity Design），是当前的最高级别，包括一个严格的设计、控制和验证过程。与前面提到的各级别一样，这一级别包含了较低级别的所有特性。设计必须是从数学角度上经过验证的，而且必须进行秘密通道和可信任分析的分布。可信任分布（Trusted Distribution）的含义是硬件和软件在物理传输过程中已经受到保护，以防止破坏安全系统。

由公安部主持制定、国家质量技术监督局发布的中华人民共和国国家标准 GB 17895—1999《计算机信息系统安全保护等级划分准则》已经正式颁布，并于2001年1月1日起实施。该准则将信息系统安全分为如下5个等级。

- 自主保护级。
- 系统审计保护级。
- 安全标记保护级。
- 结构化保护级。
- 访问验证保护级。

主要的安全考核指标有自主访问控制、身份鉴别、数据完整性、客体重用、审计、强制访问控制、安全标记、隐蔽信道分析、可信路径和可信恢复等，这些指标涵盖了不同级别的安全要求。如表1.5所示。

表1.5　　信息系统的5个级别

	第一级	第二级	第三级	第四级	第五级
自主访问控制	√	√	√	√	√
身份鉴别	√	√	√	√	√
数据完整性	√	√	√	√	√

续表

	第一级	第二级	第三级	第四级	第五级
客体重用		√	√	√	√
审计		√	√	√	√
强制访问控制			√	√	√
安全标记			√	√	√
隐蔽信道分析				√	√
可信路径				√	√
可信恢复					√

注：某级别下的√表示该级别可以提供的安全服务。

在此标准中，一个重要的概念是可信计算基（TCB）。可信计算基是一个实现安全策略的机制，包括硬件、固件和软件，它们将根据安全策略来处理主体（如系统管理员、安全管理员、用户等）对客体（如进程、文件、记录、设备等）的访问。

（1）自主访问控制

计算机信息系统可信计算基定义和控制系统中命名客体的访问。实施机制运行命名用户和用户组的身份规定，控制客体的共享阻止非授权用户读取敏感信息，并控制权限扩散。自主访问控制机制根据用户指定方式或默认方式，阻止非授权用户访问客体。

（2）身份鉴别

计算机信息系统可信计算基初始执行时，首先要求用户标识自己的身份，并使用保护机制来鉴别用户的身份，阻止非授权用户访问用户身份鉴别数据。通过为用户提供唯一标识，计算机信息系统可信计算基能够使用户对自己的行为负责。

（3）数据完整性

计算机信息系统可信计算基通过自主和强制完整性策略，阻止非授权用户修改或破坏敏感信息。在网络环境中，使用完整性敏感标记来确信信息在传输中未受损。

（4）客体重用

在计算机信息系统可信计算基的空闲存储空间中，对客体初始指定、分配或再分配一个主体之前，撤销该客体所含信息的所有授权。当主体获得对一个已被释放的客体的访问权时，当前主体不能获得原主体活动所产生的任何信息。

（5）审计

计算机信息系统可信计算基能创建和维护受保护客体的访问审计跟踪记录，并能阻止非授权的用户对它的访问或破坏。

计算机信息系统可信计算基能记录下述事件：使用身份鉴别机制将客体引入用户地址空间（如打开文件、程序初始化）；删除客体；由操作员、系统管理员或（和）系统安全管理员实施的动作，以及其他与系统安全有关的事件。对于每一事件，其审计记录包括事件的日期和时间、用户、事件类型、事件是否成功。对于身份鉴别事件，审计记录包含来源（如终端标识符）；对于客体引入用户地址空间的事件及客体删除事件，审计记录包含客体名。

对不能由计算机信息系统可信计算基独立分辨的审计事件，审计机制提供记录接口，可由授权主体调用。