2008
考试专用

全国计算机等级考试

National Computer Rank Examination

考点分析、题解与模拟

(三级数据库技术)

飞思考试中心
Fecit Examination Center

Future
未来教育

全国计算机等级考试命题研究中心 编著
飞思教育产品研发中心
未来教育教学与研究中心 联合监制

新大纲

超媒体教学软件
精析最新考试大纲，重点难点及时巩固
名师演示，像看电影一样轻松学习

模拟考试软件
真考环境+智能评分，强化学习成果
带您提前“进入”考场

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

飞思考试中心

全国计算机等级考试考点分析、题解与模拟
（三级数据库技术）

全国计算机等级考试命题研究中心　　编著
飞思教育产品研发中心
未来教育教学与研究中心　　联合监制

電子工業出版社
Publishing House of Electronics Industry
北京·BEIJING

内 容 简 介

本书依据教育部考试中心最新发布的《全国计算机等级考试大纲（2007 年版）》，在《全国计算机等级考试考点分析、题解与模拟（2006 版）》的基础上修订而成。在编写过程中，一方面结合最新大纲和数套真卷，对重要考点进行了分析、讲解，并选取经典考题进行了深入剖析；另一方面配有同步练习、模拟试题和上机试题，以逐步向考生详尽透析考试中的所有知识要点。“一书在手，通关无忧”。

本书配有“全国计算机等级考试模拟软件”。其中智能化的答题系统按照本书的顺序循序渐进、逐步编排；模拟试卷和上机的内容与形式，完全模拟真实考试，考试步骤、考试界面、考试方式、题目形式与真实考试完全一致，并可以自动评分。“书+光盘，物超所值”。

本书适合作为全国计算机等级考试考前培训班辅导用书，也可作为应试人员的自学用书。

图书在版编目（CIP）数据
全国计算机等级考试考点分析、题解与模拟. 三级数据库技术 / 全国计算机等级考试命题研究中心编著.
北京：电子工业出版社，2007.11
(飞思考试中心)
ISBN 978-7-121-05208-8

I. 全… II.全… III.①电子计算机－水平考试－自学参考资料②数据库管理系统－水平考试－自学参考资料Ⅳ.TP3

中国版本图书馆 CIP 数据核字（2007）第 160318 号

责任编辑：王树伟 田 蕾
印 刷：北京中科印刷有限公司
装 订：三河市双峰印刷装订有限公司
出版发行：电子工业出版社
北京市海淀区万寿路 173 信箱 邮编：100036
开 本：880×1230 1/16 印张： 15.75 字数：504 千字
印 次：2007 年 11 月第 1 次印刷
定 价：29.80 元（含光盘 1 张）

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。
质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。
服务热线：（010）88258888。

Preface 前言

全国计算机等级考试自1994年由国家教育部考试中心推出以来，为评测全社会非计算机专业人员的计算机知识与技能，培养各行业的计算机应用人才开辟了一条新的道路，受到了用人单位和学习人员的热烈欢迎。全国计算机等级考试通过数年的发展，已经成为我国最大型的计算机类考试。

为了帮助更多的学习者顺利地通过考试，并掌握相应的操作技能，我们在深入调研、详尽分析考试大纲的基础上，组织国内著名高校的计算机专家和一线教师编写了本书。

本书共分为三大部分，同时配有一张学习软件光盘。

※ 考点分析/经典题解/同步练习

“考点分析”结合最新考试大纲、教材，对教材中考核的重点和难点进行了讲解，内容涵盖了大纲中所有的笔试和上机考试的考点。

“经典题解”选取极具代表性的经典例题。例题符合考试命题规律的特征，对题目的讲解深入、透彻，循序渐进，极有条理。

“同步练习”提供了大量习题，对前面所学的理论知识进行温习和巩固，以练促学、学练结合。

※ 笔试全真模拟试卷

结合最新考试大纲，筛选与演绎出的典型试卷集，不论在形式上还是难度上，都与真题类似，解析详尽、透彻。

※ 上机全真模拟试题

本部分对典型考试题目进行了讲解，使学习者熟悉整个考试过程，了解上机考试的题型、题量；并配有详细的解析，使学习者既能知其然，也能知其所以然。

※ 配套学习软件

本书配套光盘具有如下特色：

- 超大量仿真考试模拟试卷，自动组卷，即时评分，由专家对答题结果进行“现场指导”。
- 自动化上机评分功能，从抽题、答题到交卷完全模拟真实考试，唯一不同之处是可以对上机作答进行评分。
- 做题原始记录随时抽调，温故知新，导出、打印随心所欲。

本书所有上机试题都经过上机调试通过。由于时间仓促，书中难免有不当之处，敬请指正。

联系方式

电　　话：(010)82552266　68134545　88254160

电子邮件：support@fecit.com.cn　eduwin@sina.com

未来教育考试网：http://www.eduexam.cn

飞思在线：http://www.fecit.com.cn　http://www.fecit.net

通用网址：计算机图书、飞思、飞思教育、飞思科技、FECIT

全国计算机等级考试命题研究中心

飞思教育产品研发中心

未来教育教学与研究中心

Contents 目录

第 1 章 计算机基础知识

第 2 章 数据结构与算法

第 3 章 操 作 系 统

第 4 章 数据库系统基本原理

第 5 章 事务管理和新一代数据库

第 6 章 笔试全真模拟试卷

第 7 章 上机指导及上机全真模拟试题

附 录

第1章 计算机基础知识

考核知识点

- 计算机系统的组成和应用领域
- 计算机软件的基础知识
- 计算机网络的基础知识和应用知识
- 信息安全的基本概念

重要考点提示

根据对历年的试卷分析可知，本章考核内容约为10%。主要考核以下几个方面：

- 计算机系统的组成
- Internet基础及其提供的主要服务
- 信息安全基础

1.1 计算机系统组成与应用领域

考点 1 计算机系统组成

一个完整的计算机系统，包括硬件和软件两个部分。

硬件系统是指组成一台计算机的各种物理装置，它是计算机的物质基础，由各种器件组成，如主板、CPU、硬盘、显示器、内存和线路等。

软件系统是运行在计算机硬件设备上的各种程序及相关资料的总称。

以存储程序原理为基础的冯·诺依曼结构的计算机，一般由五大功能部件组成，它们是运算器、控制器、存储器、输入设备以及输出设备。

下面分别对各种设备进行介绍。

1 运算器

运算器是用于对数据进行加工的部件，它可以对数据进行算术运算和逻辑运算。算术运算包括加、减、乘、除、求余及复合运算。逻辑运算包括一般的逻辑判断和逻辑比较。

2 控制器

控制器是计算机的控制部件。它控制计算机各部分自动协调地工作，用于对程序的指令进行解释和执行，协调输入、输出设备，以实现数据输入、运算和输出等操作。

3 存储器

存储器的主要功能是存放程序和数据，是计算机的记忆存储装置。它分为内部存储器和外部存储器。

4 输入设备

输入设备是计算机从外部接收、获取信息的装置。其功能是将数据、程序及其他信息，从人们所熟知的形式转换成计算机能识别的信息形式，并输入到计算机内部。

常见输入设备有鼠标、键盘、扫描仪、纸带输入机、模/数转换器(A/D转换器)等。

5 输出设备

输出设备的主要功能是将计算机处理过的二进制形式的信息转换成人们所需要的形式或其他设备接受并可以识别的信息形式。常见的输出设备有显示器、打印机、声音合成输出、绘图仪和数/模转换器(D/A转换器)等。

一般把运算器和控制器合称为中央处理器(Central Processor Unit，简称CPU)，中央处理器与内存储器统称为主机，输入设备、输出设备和外存储器合称为外部设备，外部设备通过接口与主机相连。

TIPS小提示

模/数转换器为输入设备,而数/模转换器为输出设备。有些设备既有输入功能又有输出功能,如磁盘机、磁带机等。

考点 2 计算机的应用领域

1 科学和工程计算

主要是用数值方法对一些数学问题的求解。计算机不仅可以提高计算的速度,还可以使一些人工不能解决的数学问题得到解决。在科学实验和工程设计中,经常会遇到一些数学方程和函数问题,这些问题人们不能从理论上得出其准确解,但利用计算机可以得到它们的近似解。这种应用称为科学和工程计算,其特点是计算量大,而逻辑关系相对简单。

2 数据和信息处理

数据处理是指对数据的收集、存储、加工、分析和传送的一系列过程。

计算机的一个非常重要的应用领域就是对数据和信息的处理。数据的含义是相当广泛的,包括声、像、文字和图表等,它们都可以用计算机来进行处理。

3 过程控制

过程控制是自动化技术的重要技术内容和手段,指计算机对所采集到的数据按一定的方法经过计算,然后输出到指定的执行设备中去控制生产的过程。

4 辅助设计

计算机辅助设计(Computer Aided Design,简称 CAD)是用计算机来帮助设计人员进行产品、工程设计的重要技术手段,可以节省人力和物力,且速度快,质量高,能有效缩短产品的设计周期。

这里有必要提一下这几个名词:计算机辅助制造(Computer Aided Manufacturing,简称 CAM)、计算机辅助测试(Computer Aided Testing,简称 CAT)和计算机辅助教学(Computer Aided Instruction,简称 CAI)。

5 人工智能

人们把用计算机模拟人脑思维的过程称为人工智能,并利用计算机程序来实现这些过程。

1.2 计算机软件

考点 3 计算机语言

计算机语言是面向计算机的人工语言,它是进行程序设计的工具,又称为程序设计语言。现有的程序设计语言一般可分为机器语言、汇编语言及高级语言,下面分别加以介绍。

1 机器语言

机器语言是最初级的计算机语言,它依赖于硬件,是由 0,1 组成的二进制编码形式的指令集合。不易被人识别,但可以被计算机直接执行。

2 汇编语言

汇编语言指使用助记符号和地址符号来表示指令的计算机语言,也称之为符号语言。每条指令有明显的标识,易于理解和记忆。

用汇编语言编写的程序,直观且易理解,这是汇编语言的优点。但是汇编语言仍是面向机器的,编程工作量大,程序可移植性差。计算机不能识别和直接运行汇编语言,必须翻译成机器语言程序后才能识别并

运行。这种翻译程序即称为汇编程序，其关系如图 1-1 所示。

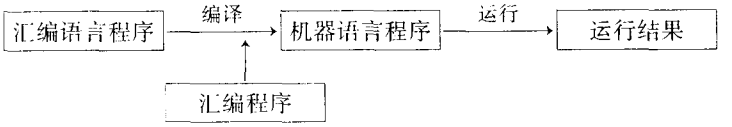

图 1-1 汇编过程

TIPS 小提示

用汇编语言编写的程序称为“汇编源程序”，而汇编程序是将汇编源程序翻译成机器语言的程序。

3 高级语言

高级语言是一类面向问题的程序设计语言，且独立于计算机的硬件，对具体的算法进行描述，所以又称为算法语言，它的特点介绍如下。

(1)脱离具体的计算机硬件。

(2)通用性及可移植性好。

下面介绍几种常用的高级语言。

(1)BASIC 语言：多用于教学及小型应用程序的开发工作。

(2)FORTRAN 语言：多用于科学及工程计算程序的开发工作。

(3)PASCAL 语言：多用于专业教学及应用程序的开发工作。

(4)C 语言：多用于系统程序的开发。

(5)C ++ 语言：多用于面向对象程序的开发。

(6)COBOL 语言：多用于商业、交通及银行等应用程序的开发。

(7)PROLOG 语言：多用于人工智能程序的开发。

(8)FoxPro 语言：多用于专业教学及应用程序的开发。

高级语言程序一般又称为源程序，不能直接在计算机上运行，需要翻译成机器语言程序(又称为目标程序)才可执行。这种翻译是由编译程序来完成的，翻译过程如图 1-2 所示。

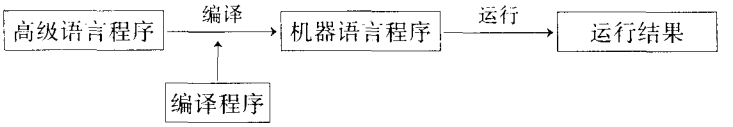

图 1-2 编译过程

考点 4 系统软件

系统软件指负责管理、监控和维护计算机资源(含硬件资源和软件资源)的程序。

1 操作系统

操作系统(Operating System，简称 OS)是系统软件的核心，也是用户同计算机之间的接口，是一组程序模块的集合。它们有效地控制和管理计算机系统中的硬件和软件资源；合理地组织计算机工作流程，以改善系统性能；提供一个易于使用、功能强大的工作环境，从而在计算机和其他用户之间起到接口的作用。

2 语言处理程序

语言处理程序就是将各种语言编写的源程序翻译成机器语言表示的目标程序。按处理方式的不同可分为解释型程序与编译型程序两大类。

3 数据库管理系统

数据库管理系统(DataBase Management System，简称 DBMS)是组织、管理和查询计算机中的存储数据并

提供一定处理功能的大型系统软件,是计算机信息系统和应用系统的基础,可分为两类:

(1)基于微型计算机的小型数据库管理系统。可解决数据量不大且功能要求较简单的数据库应用。

(2)大型的数据库管理系统。功能齐全,安全稳定,支持对大数据量的管理并提供相应开发工具。

4 服务性程序

服务性程序属于辅助性的程序,比如用于程序的装入、连接和编辑,调试用的装入程序、连接程序、编辑程序及调试程序,以及故障诊断程序、纠错程序等。

考点 5 应用软件

应用软件是指人们为了解决某个领域的实际问题而编制的计算机程序。除了系统软件以外的所有软件都称为应用软件。随着计算机应用在不同领域的深入发展,应用软件的类型也不断增多,如各种用于计算的软件包、字处理软件、CAD 软件、CAI 软件、CAM 软件,以及各种绘图软件等。

计算机硬件、软件及计算机系统的组成情况如图 1-3 所示。

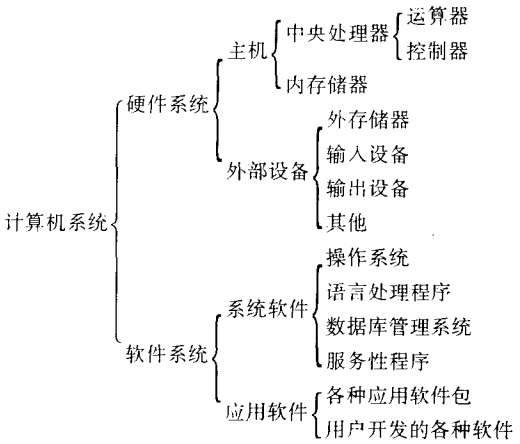

图 1-3 计算机系统组成

1.3 计算机网络基础

考点 6 计算机网络概述

1 计算机网络的基本概念

计算机网络是通信技术与计算机技术紧密结合的产物,通过通信线路及通信设备将分布在不同地点的具有独立功能的多个计算机系统连接起来,并在网络软件支持下实现相互的数据通信及资源共享的硬件系统。计算机网络按规模大小可分为局域网、城域网和广域网。

2 计算机网络的发展历史

(1)具有通信功能的单机系统阶段。

(2)具有通信功能的多机系统阶段。

(3)计算机网络阶段。

3 计算机网络的主要特点

在不同的发展阶段,人们对网络的定义是不同的,这些定义大致可分为 3 类:广义的观点、资源共享的观点和用户透明性的观点。从目前计算机网络的特点来看,资源共享观点能比较准确地描述计算机网络的基本特征。下面简单介绍一下资源共享的含义:

(1)资源共享。网络用户可以通过网络访问联网的远程计算机资源,也可以调用不同计算机共同完成任务。

(2)独立的计算机。网络中的计算机可以联网工作,也可以脱离网络独立工作。

(3)遵循共同的网络协议。为保证网络中的计算机能有序地工作,每台计算机在交换数据的过程中遵守共同的通信规则,一个网络协议主要由语法、语义与时序组成。

考点 7 计算机网络的分类

1 分类方法

(1)根据传输技术分类:可分为广播式网络与点-点式网络。

(2)根据网络的覆盖范围与规模分类:可分为局域网、城域网及广域网。

2 广域网

广域网(Wide Area Network,简称 WAN)也称为远程网,其覆盖范围从几十千米到几千千米甚至上万千米,广域网具有以下特点。

(1)适应大容量与突发性通信要求。

(2)适应综合业务服务要求。

(3)开放的设备接口与规范化的协议。

(4)完善的通信服务与网络管理。

随着通信技术的不断发展,数据通信的环境也发生了变化,主要表现在以下3个方面。

(1)传输介质由原有的电缆逐步走向误码率很低且带宽很宽的光纤。

(2)局域网内部的数据传输速率已经达到10Mb/s~1Gb/s,多个局域网之间高速互联的要求越来越强烈。

(3)用户设备性能大大提高,可以承担部分原来由数据通信网承担的通信处理功能。

3 局域网

局域网(Local Area Network,简称 LAN)指网络服务区域在一个局部的范围内,可以有一台或多台计算机及多个工作站通过其进行通信。它有以太网(Ethernet)、令牌总线(Token Bus)和令牌环(Token ring)3种工作原理。

局域网的技术特点主要表现在以下几个方面。

(1)覆盖范围有限,多用于公司、机关、校园等范围内的计算机终端与信息处理设备之间的联网需求。

(2)提供高数据传输速率、低误码率、高质量数据传输环境。

(3)易于建立、维护与扩展,一般为一个单位所有。

(4)决定局域网特性的主要技术要素为网络拓扑、传输介质与介质访问控制方法。

(5)从介质访问控制方法角度,可分为共享式与交换式局域网。

4 城域网

城域网(Metropolitan Area Network,简称 MAN)是介于广域网与局域网之间的一种高速网络。早期的城域网主要采用光纤分布式数据接口(Fiber Distributed Data Interface,简称 FDDI),它主要有以下几个技术特点。

(1)使用基于 IEEE 802.5 的单令牌的环网介质访问控制 MAC 协议。

(2)使用 IEEE 802.2 协议,与符合 IEEE 802 标准的局域网兼容。

(3)数据传输速率为 100 Mb/s,联网的节点数≤1 000,环路长度为 100 km。

(4)可以使用双环结构,具有容错能力。

(5)可以使用多模或单模光纤。

(6)具有动态分配带宽的能力,能支持同步和异步数据传输。

考点 8 Internet 基础

1 Internet 的形成与发展

(1)TCP/IP 协议与 ARPAnet 的结合,使 ARPAnet 成为 Internet 的主干网。

(2)NSFnet 从一开始就使用 TCP/IP 协议,是第一个使用 TCP/IP 协议的广域网。

(3)Internet 实现了 TCP/IP 协议参考模型与协议的结合。TCP/IP 协议使网络不受主机、用户微型计算机及所使用的操作系统的限制。

2 Internet 的结构与组成

从技术角度上来看,Internet 主要是由通信线路、路由器、主机、信息资源几个主要部分组成的。

(1)通信线路。将 Internet 中的路由器与路由器、路由器与主机连接起来。

(2)路由器。是 Internet 中最重要的通信设备之一,它的作用是将 Internet 中的各个局域网、城域网或广域网,以及主机互联起来。

(3)主机。是 Internet 中信息资源与服务的载体。

(4)信息资源。是用户最关心的问题,它会影响到 Internet 中站点受欢迎的程度。

3 TCP/IP 协议、域名与 IP 地址

TCP/IP 协议是为保证 Internet 正常工作而要求所有 Internet 中的主机都必须遵守的通信协议。它具有以下几个特点。

(1)开放的协议标准,独立于特定的计算机硬件与操作系统。

(2)独立于特定的网络硬件,可以运行在局域网和广域网,更适用于互联网中。

(3)标准化的高层协议,可以提供多种可靠的用户服务。

(4)统一的网络地址分配方字模,使得整个 TCP/IP 设备在网中都具有唯一的 IP 地址。

在 TCP/IP 参考模型中,应用层包括了所有的高层协议,且一直有新的协议加入。应用层协议主要有下面几种。

(1)网络终端协议 TELNET,实现网络互联中远程登录的功能。

(2)文件传送协议 FTP,实现因特网中交互式文件传送的功能。

(3)域名服务 DNS,实现网络设备名字与 IP 地址相互映射的网络服务。

(4)路由信息协议 RIP,网络设备间交换路由信息的协议。

(5)电子邮件协议 SMTP,实现网络中电子邮件的传送功能。

(6)HTTP 协议,用于 WWW 服务。

(7)网络文件系统 NFS,用来实现网络中不同主机间的文件共享。

域名与 IP 地址是 Internet 上计算机地址的两种表示形式。根据不同的取值范围,IP 地址可分为以下几类。

(1)A 类。网络地址空间长度为 7 位,主机地址空间长度为 24 位。

(2)B 类。网络地址空间长度为 14 位,主机地址空间长度为 16 位。

(3)C 类。网络地址空间长度为 21 位,主机地址空间长度为 8 位。

由于 IP 地址是数字形式,用户难于记录,TCP/IP 专门设计了一种字符型的主机名字机制,这就是 Internet 域名系统 DNS。DNS 是比 IP 地址更为高级的地址形式,但它同样要解决主机命名、主机域名管理、主机域名与 IP 地址映射等问题。

TIPS 小提示

每个 C 类网络主机地址数量最多为 256 个,适用于一些小公司与普通的研究机构。

考点 9 Internet 提供的主要服务

目前,Internet 上所提供的服务功能已达上万种,经常使用的 Internet 服务主要有:WWW 服务、电子邮件服务、文件传输、新闻与公告类服务等。

1 WWW 服务

WWW(World Wide Web,简称 WWW)服务是当今最受欢迎、最方便的信息服务类型之一。WWW 的信

息组织形式是超文本(Hypertext)与超媒体(Hypermedia)。以超文本标记语言 HTML(Hyper Text Markup Language)与超文本传输协议 HTTP(Hyper Text Transfer Protocol)为基础,向用户提供风格一致的信息浏览服务。

WWW 服务系统采用客户/服务器模式。信息资源存储在 WWW 服务器中,用户通过浏览器向服务器发出请求,WWW 服务器根据请求将保存在服务器上的页面发送给客户端。

服务器中的主页通过统一资源定位器 URL(Uniform Resource Locator)来管理其他页面。标准 URL 由服务器类型、主机名、路径和文件名组成。

2 电子邮件服务

电子邮件是利用网络传输信息的非交互式服务。Internet 中的电子邮件系统设有邮件服务器、电子邮箱,以及相应规定的电子邮件书写规则。每个电子邮箱地址全球唯一。

3 文件传输

用 FTP 方式可以直接进行文字与非文字信息的双向传输,用户可以使用各种索引服务器查找各种信息资源。

考点 10 Internet 的基本接入方式

用户由 Internet 服务提供商 ISP(Internet Service Provider)提供的入口点接入网络。一般来说有以下两种方式。

1 通过局域网接入

所谓"通过局域网接入",是指用户的局域网使用路由器,通过数据通信网与 ISP 相接,再通过 ISP 的连接通道接入 Internet。

一般来说,采用这种方式接入的用户希望达到以下目的。

(1)在 Internet 上提供信息服务。

(2)通过 Internet 实现企业内部网的互联。

(3)在单位内部配置连接 Internet 的电子邮件服务器。

(4)获得更大的带宽,以保证传输的可靠性。

2 通过电话网接入

所谓"通过电话网接入",即用户计算机使用调制解调器,通过电话网与 ISP 相接,再通过 ISP 的连接通道接入Internet。

1.4 信息安全基础

考点 11 信息安全

信息安全就是要防止非法的攻击和病毒传播,保证计算机系统和通信系统的正常运转。概念上包括 4 方面的内容:保密性(Confidentiality)、完整性(Integrity)、可用性(Availability),以及可控性(Controllability)。

信息安全涉及到网络安全、操作系统安全、数据库系统安全和信息系统安全等。

考点 12 信息保密

信息系统中的机密信息要进行加密来保证其安全。加密是为防止破译信息系统中机密信息的技术手段,就是使用数学方法重新组织数据或信息,使非授权用户不能获取数据信息。

加密是通过加密算法来实现的。加密前的文件称为明文,加密后的文件称为密文。一个加密体制一般由 5 个部分组成。

(1)明文空间,即全体明文所组成的集合。

(2)密文空间,即全体密文所组成的集合。

(3)加密密钥空间,即全体加密密钥所组成的集合。

(4)解密密钥空间,即全体解密密钥所组成的集合。

(5)规则集,即加密算法集和解密算法集。

加密体制分为单钥加密体制(私钥或对称加密体制)和双钥加密体制(公钥或非对称加密体制)。

考点 13 信息认证

信息认证就是验证信息发送者的真实性及信息的完整性。认证是防止对系统进行主动攻击的重要技术手段。为了保证信息的可认证性,抵抗主动攻击,一个安全的认证体制应满足以下要求。

(1)消息的接收者能够检验和证实消息的合法性、真实性和完整性。

(2)消息的发送者对发送的信息不能抵赖,有时也要求消息的接收者不能否认所收到的消息。

(3)除合法消息发送者外,其他人不能伪造合法的消息。

1 数字签名

数字签名是实施身份认证的方法之一,通过签字算法来实现。一个签名算法至少应满足以下 3 个条件。

(1)签名者事后不能否认自己的签名。

(2)接收者能验证签名,但其他人都不能仿造签名。

(3)双方对签名的真伪发生争执时,有能解决争执的第三方存在。

2 身份识别

身份识别涉及计算机的安全访问、使用及出入境管理等内容。使用密码技术,特别是公钥密码技术,可以设计出安全性能高的识别方法。

基于密码识别技术的身份识别有两种方式,即通行字方式和持证方式。

通行字方式使用广泛的身份识别方式,通行字一般为数字、字母和特殊字符等组成的长度为 5 ~ 8 的字符串。其认证过程如下。

(1)识别者将它的通行字传送给计算机。

(2)计算机完成通行字的单项函数值的计算。

(3)计算机把单项函数值和机密存储值相比较。

持证方式是另一种身份识别方式,它是用一种持有物来启动电子设备的身份识别方式。常见的是嵌有磁条的磁卡,在磁条上记录用于机器识别的个人信息。

3 消息认证

消息认证是指接收者能检验收到消息真实性的方法,其检验内容如下。

(1)验证消息的源与宿。

(2)验证消息内容是否保持完整性,即未被篡改。

(3)消息的序号和时间性。

消息的序号和时间性的认证主要是阻止消息的重放攻击。常用方法有消息的流水作业号、链接认证符、随机数认证和时间戳等。

4 密钥管理

密钥管理影响到密码系统的安全性且会涉及到系统的可靠性、有效性及经济性。密钥管理包括密钥的产生、存储、装入、分配、保护、丢失、销毁及保密等内容,其中解决密钥的分配和存储是最关键和困难的问题。密钥管理与密钥分配协议和密钥协定有关。

密钥一般通过签发证书来表明其合法性,即公钥证书。它包括持证人姓名、地址等信息,并有可信机构的签名。

考点14 计算机病毒

计算机病毒是一种破坏性程序，可进行自我复制并通过非授权侵入而隐藏在可执行程序或数据文件中。含有病毒的计算机运行时病毒会影响和破坏正常程序的执行和数据的正确性。

1 计算机病毒的特征

(1)传染性。传染性是所有病毒都具有的共同特性。

(2)破坏性。病毒程序一旦侵入当前的程序体内，就有可能中断一个系统的正常工作，极端的情况下会使一个计算机网络系统瘫痪。

(3)隐蔽性。计算机病毒的隐蔽性表现在两个方面：一是传染的隐蔽性，二是存在的隐蔽性。

(4)潜伏性。病毒具有依附于其他媒体而寄生的能力。

(5)可激发性。在一定的条件下，通过外界刺激可使病毒活跃起来。

2 病毒的破坏作用

(1)破坏磁盘文件分配表，使文件无法使用。

(2)删除磁盘上的可执行文件或数据文件。

(3)病毒程序的自身多次复制使内存可用空间减小。

(4)对磁盘的磁道或扇区进行格式化。

(5)将非法数据写入内存参数区，造成死机甚至引起系统崩溃。

(6)破坏磁盘扇区，使磁盘空间减小。

(7)修改或破坏文件中的数据。

(8)更改或重写磁盘卷标。

(9)改变磁盘分配表，造成数据写入错误。

(10)在系统中产生新的信息。

(11)改变系统正常运行过程。

3 病毒的来源

所有病毒都是掌握计算机技巧的人人为制造的。可能的来源有以下几个方面。

(1)黑客有意制造的病毒，原因可能是恶作剧、报复，从而达到某种经济、政治甚至军事目的。

(2)计算机企业或一些机构，为了某种防范目的，采用了埋藏病毒的不正当手段。

(3)一些计算机领域的研究或实验工作，因某种原因泄露或释放出病毒。

4 病毒的防治

对待病毒要以预防为主，主要是截断病毒的传播途径。目前计算机病毒传播的途径是通过网络和软件。一般认为，病毒的防治应从以下3方面着手。

(1)加强思想教育。

(2)组织管理。

(3)加强技术措施。

考点15 网络安全

计算机网络安全已经成为信息化社会的一个重要问题，各种计算机系统、资源都通过网络被连在一起，这样就使网络安全问题受到格外的关注。

1 构成对网络安全威胁的主要因素及相关技术

研究网络安全技术，首先要研究对网络安全构成威胁的主要因素，大致有以下6点。

(1)网络攻击、攻击检测与防范。

(2)网络中的信息安全保密。

(3)网络安全漏洞与安全对策。

(4)网络内部安全防范。

(5)网络防病毒。

(6)网络数据备份与恢复、灾难恢复。

网络中的信息安全保密主要包括信息存储安全与信息传输安全。保证信息安全与保密的核心技术是密码技术。

2 网络安全服务的主要内容

网络安全技术研究主要涉及以下3个方面的问题。

(1)安全攻击。是指所有有损于网络信息安全的操作。

(2)安全机制。是指用于检测、预防或从安全攻击中恢复的机制。

(3)安全服务。是指提高数据处理过程中的信息传输安全性服务。

一个功能完备的网络系统应该提供以下基本的安全服务功能:

(1)保密性。其目的是防止传输的数据被截获与篡改。

(2)认证。用于解决网络中信息传送的源节点用户与目的节点用户身份的真实性。

(3)数据完整性。用于保证发送信息与接收数据的一致性,防止出现信息在传输过程中被插入、删除的问题。

(4)防抵赖。用于保证源节点用户与目的节点用户不能对已发送或已接收的信息予以否认。

(5)访问控制。用于控制与限定网络用户对主机、应用程序、数据与网络服务的访问类型。

考点16 操作系统安全

操作系统是与计算机硬件最密切的软件系统,是计算机运行的基础。操作系统应提供的安全服务应包括内存保护、文件保护、存取控制和存取鉴别。

1 操作系统安全方法

操作系统的安全措施一般可从隔离、分层和内控3个方面来进行考虑。其中隔离又可分为以下几点。

(1)物理隔离。使不同安全要求的进程使用不同物理实体。

(2)时间隔离。使不同进程在不同时间运行。

(3)逻辑隔离。限制程序存取。

(4)密码隔离。进程以其他进程不知的方式隐蔽数据和计算。

2 操作系统安全控制方法

操作系统的安全控制措施包括访问控制、存储保护及文件保护与保密。

访问控制是保障信息安全的有效措施,访问控制的目的如下:

(1)保护存储在计算机内主要信息的秘密性。通过对访问进行控制,使机密信息保密。

(2)保护存储在计算机内个人信息的保密性。

(3)维护计算机内信息的完整性。拒绝非授权用户,减少非法用户对重要文件进行修改的机会。

(4)减少病毒感染机会,从而减少和延缓病毒的传播。

访问控制的基本任务和实现方法如下:

(1)规定要保护的资源。

(2)规定可以访问该资源的实体,它可以是一个人,也可以是一段程序。

(3)规定可对该资源执行的操作,如读、写、执行或禁止访问等。

(4)确定每个实体权限的安全方案。

最广泛使用的安全方案包括两步:首先是针对该资源确认用户身份,其次是同意或拒绝用户对该资源执行某些动作。

实施安全方案包括硬件、软件及相关的物理设备，主要有以下几个方面。

(1)认证。在访问资源之前用户应证明身份。确认身份的方法可以用诸如磁卡、密钥、证书或口令、指纹、掌纹或视网膜等。

(2)访问权限。对用户的访问权限进行规划，如可将用户分为特殊用户、一般用户、审计用户和作废用户。对不同的用户给予不同的权限，包括所具有的访问操作权利和可使用的资源。

(3)文件保护。对文件提供附加保护，使非授权用户不可读或对某些文件进行加密。

(4)审计。记录用户使用安全系统的过程，它可记录造成违反安全规定的时刻、日期及用户活动。

一般对文件的存取设置为两级控制：第一级是对访问者的识别，第二级是存取权限的识别。第一级控制将用户分为3类：文件创建者、文件主合作者和其他用户。第二级控制的基本存取权限有：R(只读)、W(可写)、E(可执行)和N(不允许任何操作)。

考点17 数据库安全

数据库安全性一般指保护数据库不受恶意访问，而完整性指由于意外而破坏数据的一致性。数据库存储的数据应防止未受权用户的访问、恶意破坏或修改等操作。

1 安全性措施的层次

防止对数据库的恶意访问比防止意外破坏数据一致性要困难。下面是一些恶意访问的形式：

(1)未经授权读取数据。

(2)未经授权修改数据。

(3)未经授权删除数据。

为了数据库的安全，应从以下几个层次上对数据库采取措施：

(1)物理层。计算机系统所位于的节点(一个或多个)必须在物理上受到保护，以防止入侵者强行闯入或暗中潜入。

(2)人员层。对用户的授权必须格外小心，以减少授权用户接受贿赂或其他好处而给入侵者提供访问机会的可能性。

(3)操作系统层。不管数据库系统多安全，操作系统安全性方面的弱点总是可能成为对数据库进行未授权访问的一种手段。

(4)网络层。由于几乎所有的数据库系统都允许通过终端或网络进行远程访问，网络软件的软件层安全性和物理安全性一样重要，不管在Internet上还是在企业私有的网络内。

(5)数据库系统层。数据库系统的某些用户获得的授权可能只允许他访问数据库中有限的部分，而另外一些用户获得的授权可能允许他查询，但不允许他修改数据。保证这样的授权限制不被侵犯是数据库系统的责任。

2 权限和授权

用户对数据库可以有多种不同形式的访问权限，其中包括read权限、insert权限、update权限、deleted权限、index权限、resource权限、alteration权限及drop权限。

3 在SQL中进行安全性说明

SQL数据定义语言中包含了权限授予和回收的命令。SQL标准包括delete、insert、select和update权限。

SQL-92标准定义了数据库模式的基本授权机制：只有模式属主才能对模式进行修改。因此，模式的修改(如关系的创建和删除，增加或去掉关系中的属性，以及增加或去掉索引)只能由模式属主来执行。