第5章

操作系统与数据库安全

本章主要讨论保护计算机操作系统和基于操作系统的其他信息系统的安全，内容涉及操作系统安全技术和数据库安全技术。首先介绍操作系统的基本功能和特征、当前主要的操作系统及其性能，重点介绍操作系统的安全机制，然后介绍数据库安全的基本概念、面临的安全威胁和安全需求以及实现数据库安全的主要技术，最后介绍经典的 SQL 注入攻击案例。

本章的知识要点、重点和难点包括：操作系统的主要功能、操作系统的安全机制、主要操作系统(Linux 和 Windows)采取的安全机制、数据库面临的安全威胁和需求、实现数据库安全的技术。

5.1 操作系统概述

5.1.1 基本概念

现代计算机系统都是由硬件和软件两大部分组成的。计算机硬件部分是指计算机物理装置本身，包括处理机、存储器、输入输出设备和各种通信设备，即硬件构成了系统本身和用户使用计算机的物质基础和工作环境。软件部分是指所有程序和数据的集合，它们由硬件执行，可以完成某种特定的任务。

计算机系统中的硬件和各种软件构成了层次关系。硬件部分是核心，通常称为裸机。从功能上看，裸机是有局限性的。软件的作用是在硬件的基础上对硬件的性能进行扩充和完善。计算机中的软件通常可分为系统软件和应用软件。系统软件与具体的应用领域无关，它主要用于计算机的管理、维护、控制和运行，并对运行的程序进行翻译、装载等服务工作。系统软件本身又可分为 3 部分，即操作系统、语言处理程序和支撑软件。应用软件是用户为解决某一特定问题而编制的程序。在各种软件中，一部分软件的运行往往需要另一部分软件作为基础，新增加的软件是对原有软件的扩充和完善，因此，在裸机之上每增加一个软件层次就变成一台功能更强的机器，称为虚拟机。

图 5-1 为计算机硬件和软件的层次关系，操作系统是最接近硬件的软件层，是对硬件的首次扩充，也是其他各种软件的运行基础。

总之，操作系统是计算机系统中最重要的一个系统软件，由一系列系统程序模块的集合组成。它们管理和控制整个计算机系统中的软硬件资源，并合理地组

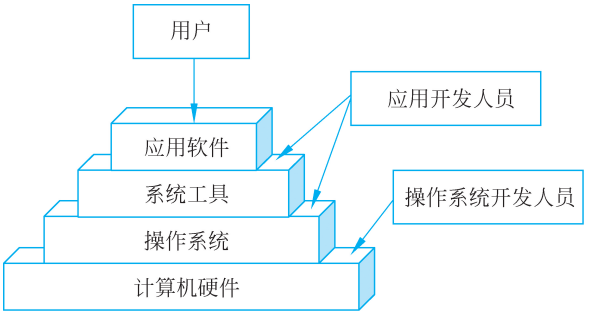


图 5-1　计算机硬件和软件的层次关系

织计算机工作流程，以便有效地利用资源，为使用者提供一个功能强大、方便实用、安全完整的工作环境，从而在最底层的软硬件基础上为计算机用户建立、提供一个统一的操作接口。

5.1.2　作用和目的

从用户的角度看，引入操作系统是为了给用户使用计算机提供一个良好的工作界面，用户无须了解许多有关硬件和系统软件的细节，就能方便灵活地使用计算机，因此操作系统是用户与计算机硬件之间的接口(interface)。

从资源管理的角度看，操作系统是计算机系统资源的管理者。用户使用计算机实际上是使用计算机系统的软硬件资源，操作系统的主要目的之一就是帮助用户管理系统资源，更好地为用户服务。

从任务组织的角度看，引入操作系统是为了合理地组织计算机工作流程，以提高资源的利用率。

从软件的角度看，操作系统是计算机系统中最重要的软件，是程序和数据的集合。

综上所述，操作系统是一组有效控制和管理计算机硬件和软件资源、合理组织计算机工作流程并方便用户使用计算机的程序的集合。它是配置在计算机上的第一层软件，是对硬件功能的首要扩充。

5.1.3　操作系统的基本功能

计算机系统的主要硬件资源有处理机、存储器和外部设备。软件资源主要以文件的形式保存在外存储器中。因而形成了操作系统的五大功能，即处理器管理、存储器管理、设备管理、文件管理和用户接口。

处理器管理主要是对处理器的分配和运行进行管理。在传统的操作系统中，处理器的分配和运行都是以进程为基本单位的，因此通常将处理器管理归结为对进程的管理。

存储器管理主要是为多道程序的运行提供良好的环境，它的任务是对内部存储器进行分配、保护和扩充。

设备指的是计算机系统中除 CPU 和内存以外的所有输入输出设备。操作系统的设备管理主要是对这些设备提供相应的设备驱动程序、初始化程序和设备控制程序等，使用户不必详细了解设备及接口的技术细节，就可方便地对这些设备进行操作。

操作系统将所有的软件资源都以文件的形式存放在外存储器(磁盘)中，操作系统对软件资源的管理就是对文件的管理。

用户接口功能在上面已作了介绍。

5.1.4 操作系统的特征

各种类型的操作系统虽然各有特点，但它们都有如下共同的基本特征：

(1) 并发性。并发是指两个或多个事件在同一时间间隔内发生。在多处理器环境下，并发是指宏观上在一段时间间隔内有多道程序在同时运行；而在单处理器环境下，每一时刻仅能执行一道程序，故微观上这些程序是在交替执行。

(2) 共享性。共享是指操作系统程序与多个用户程序共用系统中的各种资源，这种共享是在操作系统控制下实现的。共享可分为两种：

① 互斥共享。系统某些资源，如打印机、扫描仪、重要系统数据等，虽然可供多个用户程序共同使用，但在一段特定时间内只能由某一个用户程序使用。

② 同时共享。系统中还有一类资源，在同一段时间内可以被多个程序同时访问。当然这是指宏观上的，微观上这些程序访问资源有可能还是交替进行的。硬盘就是一个典型的例子。

(3) 虚拟性。虚拟是指通过某种技术将一个物理实体变为若干逻辑上的对应物。用来实现虚拟的技术称为虚拟技术。

(4) 异步性。异步是指在多道程序的环境下，每个程序以不可预知的速度向前推进。但是，与此同时，操作系统应保证程序的执行结果是可再现的，即只要运行环境相同，程序结果就相同。

5.1.5 操作系统的分类

操作系统按机型可分为大型机、小型机和微型机的操作系统，按用户数目可分为单用户操作系统和多用户操作系统，按功能特征可分为批处理操作系统、实时操作系统和分时操作系统。

下面从功能特征角度对各类操作系统加以介绍。

1. 批处理操作系统

过去，在计算中心的计算机上配置的操作系统一般采用以下方式工作：用户把要计算的应用问题编成程序，连同数据和作业说明书一起交给操作员，操作员集中一批作业并输入计算机中，由操作系统调度和控制用户作业的执行。通常，采用这种批量化处理作业方式的操作系统称为批处理操作系统。

批处理操作系统根据一定的调度策略把要求计算的问题按一定的组合和次序执行，从而使系统资源利用率高，作业的吞吐量大。批处理系统的主要特性如下：

(1) 用户脱机工作。用户提交作业之后直至获得结果之前不再和计算机及其他的作业交互，因而作业控制语言对脱机工作的作业来说是必不可少的。这种工作方式对调试和修改程序是极不方便的。

(2) 成批处理作业。操作员集中一批用户提交的作业，输入计算机成为后备作业。后备作业由批处理操作系统一批批地选择并调入内存执行。

(3) 多道程序运行。按预先规定的调度算法，从后备作业中选取多个作业进入内存，并启动它们运行，实现多道批处理。

（4）作业周转时间长。由于作业进入计算机成为后备作业后要等待操作员选择，因而，作业从进入计算机开始到完成并获得最后结果为止所经历的时间一般相当长，一般需等待数小时至几天。

2. 分时操作系统

在批处理系统中，用户不能干预程序的运行，无法得知程序运行情况，对程序的调试和排错不利。为了克服这一缺点，便产生了分时操作系统。

允许多个联机用户同时使用一台计算机系统进行计算的操作系统称分时操作系统。其实现思想如下：每个用户在各自的终端上以问答方式控制程序运行，系统把 CPU 的时间划分成时间片，轮流分配给各个联机终端用户，每个用户只能在极短时间内执行，若时间片用完，而程序还未执行完，则挂起并等待下次分得时间片。这样一来，每个用户的每次要求都能得到快速响应，每个用户获得的印象都是独占了这台计算机。本质上，分时系统是多道程序的一个变种，不同之处在于每个用户都有一台联机终端。

分时的思想于 1959 年由麻省理工学院正式提出，并在 1962 年开发出了第一个兼容分时操作系统——CTSS，成功地运行在 IBM 7094 机上，能支持 32 个交互式用户同时工作。1965 年 8 月，IBM 公司公布了 360 机上的分时系统 TSS/360，这是一个失败的系统，因为它太大而且太慢，没有任何用户愿意使用。

分时操作系统的主要特性如下：

（1）同时性。若干终端用户同时联机使用计算机，分时就是指多个用户分享使用同一台计算机。

（2）独立性。终端用户彼此独立，互不干扰，每个终端用户都感觉独占了这台计算机。

（3）及时性。终端用户的立即型请求（即不要求大量 CPU 时间处理的请求）能在足够快的时间之内得到响应。这一特性与计算机 CPU 的处理速度、分时系统中联机终端用户数和时间片的长短密切相关。

（4）交互性。人机交互，联机工作，用户直接控制其程序的运行，便于程序的调试和排错。

分时操作系统和批处理操作系统虽然都基于多道程序设计技术，但存在以下不同点：

（1）目标不同。批处理操作系统以提高系统资源利用率和作业吞吐率为目标，分时操作系统则要满足多个联机用户的快速响应要求。

（2）适合的作业不同。批处理操作系统适合已经调试好的大型作业，而分时操作系统适合正在调试的小型作业。

（3）资源使用率不同。批处理操作系统可合理安排不同负载的作业，使各种资源利用率较高；在分时操作系统中，多个终端作业使用相同类型的编译系统和公共子程序时，系统调用它们的开销较小。

（4）作业控制方式不同。批处理操作系统由用户通过批处理的语句书写作业控制流，预先提交，脱机工作；分时操作系统采用交互型作业，由用户从键盘输入操作命令控制作业执行，联机工作。

3. 实时操作系统

虽然多道批处理操作系统和分时操作系统获得了较高的资源利用率和快速的响应时间，从而使计算机的应用范围日益扩大，但它们难以满足实时控制和实时信息处理领域的需

要。于是，便产生了实时操作系统。

目前有 3 种典型的实时系统：实时过程控制系统、实时信息处理系统和实时事务处理系统。计算机用于生产过程控制时，要求系统能现场实时采集数据，并对采集的数据进行及时处理，进而能自动地发出控制信号控制相应的执行机构，使某些参数（压力、温度、距离、湿度）能按预定规律变化，以保证产品质量。导弹制导系统、飞机自动驾驶系统、火炮自动控制系统都是实时过程控制系统。计算机还可用于控制实时信息处理，情报检索系统是典型的实时信息处理系统。计算机接收成千上万从各处终端发来的服务请求和提问，系统应在极快的时间内做出回答和响应。事务处理系统不仅要对终端用户及时做出响应，而且要对系统中的文件或数据库频繁地进行更新。例如，每次银行与客户发生业务往来，银行业务处理系统均需修改文件或数据库。要求这样的系统响应快、安全保密、可靠性高。

实时操作系统是指当外界事件或数据产生时，能够接收并以足够快的速度予以处理，其处理的结果又能在规定的时间内用于控制生产过程或对系统做出快速响应，并控制所有执行任务协调一致运行的操作系统。由实时操作系统控制的过程控制系统较为复杂，通常由数据采集、加工处理、操作控制和反馈处理 4 部分组成。

（1）数据采集。收集、接收和记录系统工作必需的信息或进行信号检测。

（2）加工处理。对进入系统的信息进行加工处理，获得控制系统工作必需的参数或做出决定，然后进行输出、记录或显示。

（3）操作控制。根据加工处理的结果采取适当措施或动作，达到控制或适应环境的目的。

（4）反馈处理。监督执行机构的执行结果，并将该结果反馈至信号检测或数据接收部件，以便系统根据反馈信息采取进一步措施，达到控制的预期目的。

在实时系统中通常存在若干个实时任务，它们常常通过队列驱动或事件驱动开始工作。当系统接收到来自某些外部事件的消息后，分析这些消息，驱动实时任务完成相应的处理和控制。可以从不同角度对实时任务加以分类。例如，按任务执行是否呈现周期性可分成周期性实时任务和非周期性实时任务，按实时任务截止时间可分成硬实时任务和软实时任务。

5.2 常用操作系统简介

目前最常用的操作系统是 Windows、UNIX 和 Linux。其他比较常用的操作系统还有 Apple 公司的 macOS、Novell 公司的 NetWare、IBM 公司的 OS/2 以及 64 位的 zOS（OS/390）、OS/400 等。

5.2.1 MS-DOS

第一个微型计算机的操作系统是 CP/M，诞生于 20 世纪 70 年代。它是 Digital Research 公司为 8 位机开发的操作系统，能够进行文件管理，控制磁盘的输入输出、显示器的显示以及打印输出，是当时 8 位机操作系统的标准。

微软公司的 MS-DOS 陆续推出了 1.1、1.25 等版本后，逐渐得到了业界同行的认可。1983 年 3 月，微软公司发布了 MS-DOS 2.0，可以灵活地支持外部设备，同时引进了 UNIX 系统的目录树文件管理模式。自此 MS-DOS 开始超越 CP/M。

1987 年 4 月，微软公司推出了 MS-DOS 3.3，它支持 1.44MB 的磁盘驱动器，支持更大容量的硬盘等。它的流行确立了 MS-DOS 在个人计算机操作系统中的霸主地位。

MS-DOS 的最后一个版本是 6.22，这以后的 DOS 就和 Windows 相结合了。

5.2.2　Windows 操作系统

1. Windows 简介

Windows 操作系统最初的研制目标是在 MS-DOS 的基础上提供一个多任务的图形用户界面。不过，第一个取得成功的图形用户界面系统并不是 Windows，而是 Windows 的模仿对象——Apple 公司于 1984 年推出的 Mac OS。Macintosh 计算机及其上的操作系统当时已风靡美国多年，是 IBM-PC 和 MS-DOS 操作系统在当时市场上的主要竞争对手。但是 Macintosh 计算机和 Mac OS 是封闭式体系（硬件接口不公开、操作系统源代码不公开等），与 IBM-PC 和 MS-DOS 的开放式体系（硬件接口公开、允许并支持第三方厂家做兼容机、操作系统源代码公开等），使得 IBM-PC 后来者居上，销量超过了 Macintosh 计算机，也使 MS-DOS 成为个人计算机市场上占主导地位的操作系统。

Windows 系列操作系统包括个人、商用和嵌入式 3 条产品线。个人操作系统包括 Windows Me、Windows 98/95 及更早期的版本 Windows 3.x/2.x/1.x 等，主要在 IBM-PC 系列上运行。商用操作系统是 Windows 2000 和其前身版本 Windows NT，主要在服务器、工作站等上运行，也可以在 IBM 个人机系列上运行。嵌入式操作系统有 Windows CE 和手机用操作系统 Windows Phone 等。Windows XP 将家用和商用两条产品线合二为一。

Windows 早期为 MS-DOS 的虚拟环境，后采用图形用户界面（Graphical User Interface，GUI），其操作界面先后在 1995 年（Windows 95）、2001 年（Windows XP）、2006 年（Windows Vista）、2012 年（Windows 8）进行了大幅整改。Windows 更新推送系统 30 余个，普通版本已更新至 Windows 11；服务器版本已更新至 Windows Server 2022；手机版本已终止研发，最后版本为 Windows 10 Mobile；嵌入式版本为 Windows CE（后被 Windows for IoT 取代）。此外，还有提供线上 Web 服务的 Windows 365。

Windows PE 是一个小型操作系统，用于安装、部署和修复 Windows 桌面版、Windows Server 和其他 Windows 操作系统。

2. Windows 操作系统的特点

Windows 操作系统的优点主要表现以下几方面：

（1）界面图形化。操作可以说是“所见即所得”，只要移动并点击鼠标即可完成。

（2）多用户、多任务。Windows 可以让多个用户使用同一台计算机而不会互相影响。Windows 2000 在这方面做得比较完善，管理员可以添加、删除用户，并设置用户的权限。

（3）网络支持良好。Windows 9x 和 Windows 2000 以后产品内置了 TCP/IP 和拨号上网软件，只需一些简单的设置就能上网浏览、收发电子邮件等。

（4）出色的多媒体功能。在 Windows 中可以进行音频、视频的编辑和播放工作，支持高级的显卡、声卡，使其声色俱佳。

（5）硬件支持良好。Windows 95 以后的版本都支持即插即用（Plug and Play，PnP）技术，这使得新硬件的安装更加简单。几乎所有的硬件设备都有 Windows 下的驱动程序。

（6）众多的应用程序。Windows 下众多的应用程序可以满足用户各方面的需求。此

外，Windows NT、Windows 2000 系统还支持多处理器，这对大幅度提升系统性能有很大的帮助。

当然，作为一种集成了多种功能的庞大系统，Windows 操作系统也存在以下不足：

（1）由于设计时集成了多种功能，导致 Windows 操作系统非常庞大，程序代码烦冗。

（2）系统在使用过程中不是十分稳定。目前已知的多种不同版本的 Windows 操作系统都存在多种安全漏洞，这些安全漏洞虽然不一定会影响用户的正常使用，但是有可能对用户的信息安全带来安全隐患，因为这将使得计算机病毒入侵系统和人为攻击系统的机会大幅增加。

5.2.3 UNIX 操作系统

1. UNIX 简介

UNIX 是一种多用户操作系统，是目前的三大主流操作系统之一。它可以应用于各种不同的计算机上。它在推出之初就以简洁、易于移植等特点很快受到关注，并迅速得到普及和发展，是从微型机到巨型机都可以使用的唯一的操作系统。

UNIX 自诞生以来已被移植到数十种硬件平台上，许多大学、公司都发行了自己的 UNIX 版本。目前的主要变种有 SUN Solaris、IBM AIX 和 HPUX 等，不同变种间的功能、接口、内部结构与过程基本相同而又各有特色。此外，UNIX 还有一些克隆系统，如 Mach 和 Linux。

2. UNIX 操作系统的特点

UNIX 操作系统是一种多用户的分时操作系统，其主要特点如下：

（1）可移植性好。硬件的迅速发展，迫使依赖于硬件的基础软件特别是操作系统不断地发展。由于 UNIX 几乎全部是用移植性好的 C 语言编写的，其内核极小，模块结构化，各模块可以单独编译。当硬件环境发生变化时，只要对内核中有关的模块进行修改，编译后与其他模块装配在一起，即可构成一个新的内核，而上层完全可以不动。

（2）可靠性强。UNIX 是一个成熟而且比较可靠的系统。在应用软件出错的情况下，虽然其性能有所下降，但工作仍能可靠进行。

（3）开放式系统。UNIX 具有统一的用户界面，使得用户的应用程序可在不同环境下运行。

5.2.4 Linux 操作系统

1. Linux 简介

1991 年年初，年轻的芬兰大学生 Linus Torvalds 在学习操作系统设计时自行设计了一个操作系统。他只花了几个月的时间就在一台 Intel 386 微机上完成了一个类似于 UNIX 的操作系统，这就是最早的 Linux 版本。1991 年年底，Linus Torvalds 首次在 Internet 上发布了基于 Intel 386 体系结构的 Linux 源代码。由于 Linux 具有结构清晰、功能简洁等优点，很快就使得许多研究者把它作为学习和研究的对象。他们在更正原有 Linux 版本中错误的同时，也不断为 Linux 增加新的功能。在众多研究者的努力下，Linux 逐渐成为一个稳定可靠、功能完善的操作系统。一些软件公司，如 RedHat、InfoMagic 等，也不失时机地推出了以 Linux 为核心的操作系统，从而极大地推动了 Linux 的商业化进程。使得 Linux 的

使用日益广泛，其影响力也日益提升。Linux 是一个免费的类似 UNIX 的操作系统，用户可以获得其源代码，并能够随意修改。它是在共用许可证(General Public License，GPL)保护下的自由软件。Linux 有上百种不同的发行版，如基于社区开发的 Debian、Arch Linux 以及基于商业开发的 Red Hat Enterprise Linux、SUSE、Oracle Linux、XteamLinux 等。

Linux 具有 UNIX 的许多功能和特点，能够兼容 UNIX，但无须支付 UNIX 高额的费用。Linux 的应用也十分广泛。Sony 公司的 PS2 游戏机就采用了 Linux 作为系统软件，使 PS2 摇身一变，成为一台 Linux 工作站。对 Linux 进行适当的修改和剪裁就能够在嵌入式系统上使用，也就是嵌入式 Linux 操作系统。因其开源和免费，Linux 越来越成为许多嵌入式产品的首选操作系统。

2022 年 11 月，Linux 6.2 开始支持 Intel 公司锐炫独立显卡。

2. Linux 操作系统的特点

Linux 是一个以 UNIX 为基础的操作系统，它的主要特点如下：

(1) 基本思想。Linux 的基本思想有两点：一切都是文件；每个文件都有确定的用途。也就是说，系统中的命令、硬件和软件设备、操作系统、进程等对于操作系统内核而言都被视为拥有各自特性或类型的文件。

(2) 完全免费。Linux 是一款免费的操作系统，用户可以通过网络或其他途径免费获得，并可以任意修改其源代码。这是其他的操作系统做不到的。正是由于这一点，来自全世界的无数程序员参与了 Linux 的修改、编写工作，程序员可以根据自己的兴趣和灵感对其进行改变，这让 Linux 吸收了无数程序员的编程精华，不断壮大。

(3) 完全兼容 POSIX 1.0 标准。Linux 大部分代码是用 C 语言写的，完全兼容 POSIX 1.0 标准，这使得在 Linux 下可以通过相应的模拟器运行常见的 DOS、Windows 程序。这为用户从 Windows 转到 Linux 奠定了基础。许多用户在考虑使用 Linux 时，以前在 Windows 下常见的程序仍然能正常运行是非常重要的一个因素。

(4) 多用户、多任务。Linux 支持多用户，各个用户对于自己的文件设备有特殊的权限，保证了各用户之间互不影响。多任务则是现代计算机最主要的特点之一，Linux 可以使多个程序同时独立地运行。

(5) 良好的界面。Linux 同时具有字符界面和图形界面。在字符界面中，用户可以通过键盘输入相应的指令进行操作。它同时也提供了类似 Windows 图形界面的 X-Window 环境，用户可以使用鼠标对其进行操作。X-Window 环境和 Windows 很相似，可以说是一个 Linux 版的 Windows。

(6) 支持多种平台。Linux 可以运行在多种硬件平台上，如具有 x86、680x0、SPARC、Alpha 等处理器的平台。此外，Linux 还是一种嵌入式操作系统，可以运行在掌机、机顶盒或游戏机上。2001 年 1 月份发布的 Linux 2.4 版内核已经能够完全支持 Intel 64 位芯片架构。同时 Linux 也支持多处理器技术。多个处理器同时工作，使系统性能大大提高。

(7) Linux 可以提供广泛的网络功能，支持大多数互联网通信协议和服务。但是 Linux 和 UNIX 还是有各自的特点。UNIX 属于商业化的操作系统，多年来一直在昂贵的专业硬件设备上运行。Linux 可以在几乎任何设备上运行。UNIX 的使用是受限制的，需要销售商提供技术支持。Linux 是一个免费的、自由的操作系统，可以自己检查代码，建立系统安全机制。但要充分发挥 Linux 技术自由的全部优势，需要的技术水平要比使用面向消费者

的操作系统高。有些 Linux 安全工具实际上已经成为工具箱，其中包含了许多独立的安全模式。Linux 可以提供和实现内容广泛的各种客户安全解决方案，但也需要用户放弃简单化的操作习惯。

5.3 操作系统安全

操作系统是连接硬件与其他应用软件的桥梁。数据库通常是建立在操作系统之上的，如果没有操作系统安全机制的支持，就不可能保障数据访问控制的安全性和可信性。在网络环境中，网络的安全可信依赖于各个主机系统的安全可信，没有操作系统的安全，就不会有主机和网络系统的安全。因此，操作系统的安全在信息系统整体安全中起着至关重要的作用，没有操作系统的安全，就不可能有信息系统的安全。

5.3.1 操作系统安全机制

操作系统安全的主要目标是监督、保障系统运行的安全性，保障系统自身的安全性，标识系统中的用户，进行身份认证，依据系统安全策略对用户的操作行为进行监控。为了实现这些目标，在进行操作系统设计时，需要建立相应的安全机制，主要包括硬件安全机制、标识与认证机制、访问控制机制、最小特权管理机制等。

1. 硬件安全机制

绝大多数实现操作系统安全的硬件机制也是传统操作系统要求的，优秀的硬件保护性能是高可靠的操作系统的基础。计算机硬件安全的目标是保证其自身的可靠性和为系统提供基本的安全机制，包括存储保护、运行保护和 I/O 保护等。

1）存储保护

存储保护主要是指保护用户在存储器中的数据安全。保护单元为存储器中的最小数据范围，可为字、字块、页面或者段。保护单元越小，则存储保护的精度越高。在允许多道程序并发执行的操作系统中，除了防止用户程序对操作系统的影响外，还进一步要求存储保护机制对进程的存储区域实行相互隔离措施。

对于一个安全的操作系统，存储保护是最基本的要求。存储保护与存储器管理是紧密联系的，存储保护负责保证整个系统各个任务之间互不干扰，存储器管理则是为了更有效地利用存储空间。

（1）基于段的存储保护。

当系统的地址空间分为两个段（系统段和用户段）时，应该禁止在用户模式下运行的非特权进程对系统段进行写操作；而当在系统模式下运行时，则允许进程对所有的虚存空间进行读写操作。用户模式到系统模式的转换应该由一个特殊的指令完成，该指令将限制进程只对部分系统空间进程进行访问。这些访问限制一般由硬件根据该进程的特权模式实施，从系统灵活性的角度看，还是希望由系统软件明确地说明该进程对系统空间的哪一页是可读的和可写的。

（2）基于物理页的访问控制。

在计算机系统提供透明的内存管理之前，访问判决是基于物理页号的识别进行的。每个物理页号都被标以一个称为密钥的秘密信息，系统只允许拥有该密钥的进程访问该物理

页，同时利用一些访问控制信息指明该物理页是可读的还是可写的。每个进程相应地分配一个密钥，该密钥由操作系统装入进程的状态字中。进程每次访问内存时，硬件都要对该密钥进行验证，只有当进程的密钥与内存物理页的密钥相匹配，并且相应的访问控制信息与该物理页的读写模式相匹配时，才允许该进程访问该页内存，否则禁止访问。

这种对物理页附加密钥的方法是比较烦琐的，因为一个进程在它的生存期内可能多次受到阻塞而被挂起。当该进程重新启动时，它占有的全部物理页与挂起前所占有的物理页不一定相同。每当物理页的所有权改变一次，相应的访问控制信息就得修改一次。同时，如果两个进程共享一个物理页，但一个用于读而另一个用于写，那么相应的访问控制信息在进程转换时就必须修改，这样就会增加系统开销，影响系统性能。

(3) 基于描述符的访问控制。

采用基于描述符的地址解析机制可以避免上述管理方式中的困难。在这种方式下，每个进程都有一个私有的地址描述符，进程对系统内存某页或某段的访问模式都在该描述符中说明。可以有两类访问模式集，一类用于在用户状态下运行的进程，另一类用于在系统模式下运行的进程。

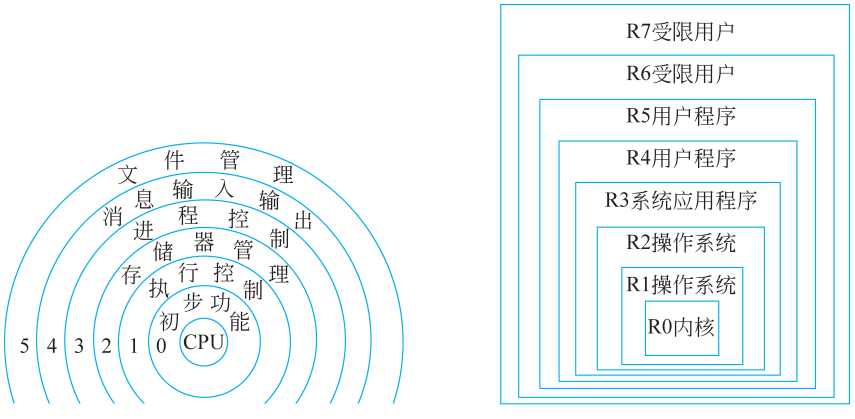
描述符 W、R、E 各占一位，它们用来指明是否允许进程对内存的某页或某段进行写、读和执行的访问操作。由于在地址解析期间地址描述符同时也被系统调用检验，因此，这种基于描述符的内存访问控制方法在进程转换、运行模式(系统模式和用户模式)转换以及进程调出/调入内存等过程中不需要或仅需要很少的额外开销。

2) 运行保护

安全的操作系统很重要的一点是进行分层设计，而运行域正是这种基于保护环的等级式结构。运行域是进程运行的区域。在最内层，保护环号最小，具有最高特权；而在最外层，保护环号最大，具有最低特权。一般的系统至少有三四个环。

设计两环系统是很容易理解的，它只是为了隔离操作系统程序与用户程序。多环结构的最内层是操作系统环，它控制整个计算机系统的运行；操作系统环之外的是受限使用的系统应用环，如数据库管理系统或者事务处理系统；最外层则是控制各个不同用户的应用环。

分层域的结构如图 5-2 所示，主要有两类层次结构：操作系统层次结构和分层域程序结构。



(a) 操作系统层次结构　　(b) 分层域程序结构

图 5-2　分层域的结构