软件安全入门

第二课 软件安全分析基本知识

目录

CONTENTS

主要内容包括CPU的结构以及处理器设计的一些特性(保护模式、特权级、虚拟化支持)。

1.1 CPU结构介绍

CPU是计算机中央处理器的简称，控制着计算机的操作和执行数据处理功能。

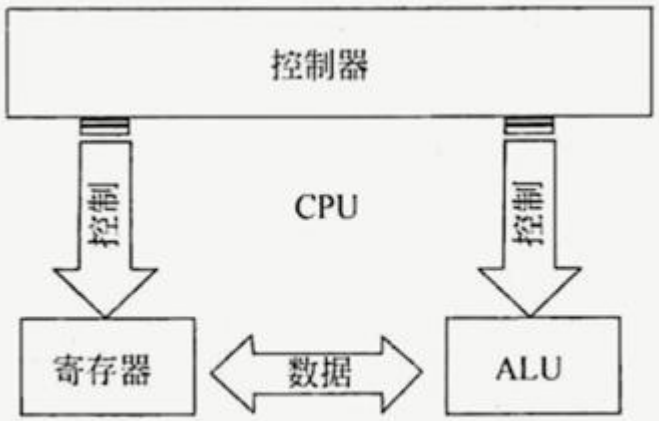


图 2-1　CPU 的结构

寄存器:提供CPU的内部存储，用来暂时存放参与运算的数据及运算结果。

算术逻辑单元(ALU): 执行计算机的运算功能。

控制区:控制计算机各部件工作，包括取指、译码、执行。

内部总线:将寄存器、ALU、控制器进行互连，提供通信机制。

实模式

CPU刚开始初始化后的工作模式

不支持多线程，不能实现权限分级。

保护模式

操作系统启动后的工作模式

引入内存的分页和分段管理机制，实现内存分页和权限分级。

CPU支持Ring0、Ring1、Ring2.

Ring3共4个权限级别。

Ring0通常赋予内核，Ring1和Ring2是一些系统

级服务，用户程序运行在Ring3。

虚拟化技术能够基于系统CPU、内存、磁盘等资源虚拟出多台主机提高资源利用率，最大化利用平台的硬件资源。

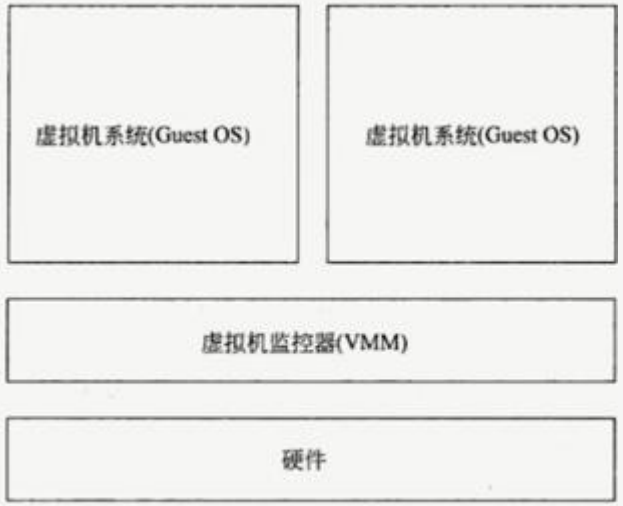


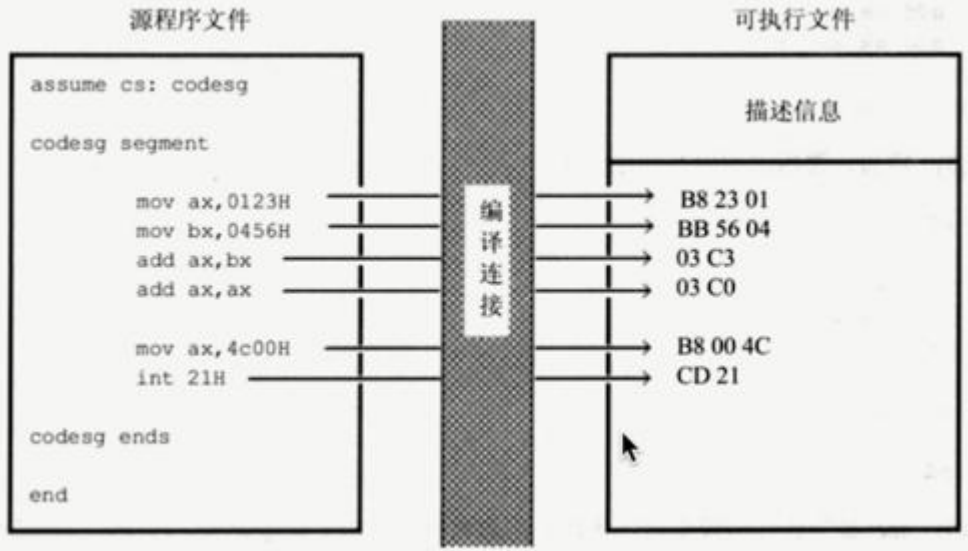
图 2-6　虚拟化架构图

主要内容包括汇编语言基础、反汇编、代码混淆、反调试等技术。

2.1汇编语言

汇编语言是一种用于计算机、微处理器、微控制器或其他可编程器件的低级语言，也称为符号语言。

不同的硬件架构对应不同的机器语言指令集。特定的汇编语言和特定的机器语言指令集是一一对应的不可直接移植。



2.2 反汇编

反汇编是将机器语言转换成汇编代码的过程。基本的反汇编流程如下:

确定反汇编的代码区域，即区分出程序的代码和数据段。

找到程序代码入口，读取该位置的二进制机器指令，提取它对应的汇编语言助记符和操作数。

获取指令并解码出所有操作数之后，对它的汇编语言等价形式进行格式化，输出反汇编代码。

重复上述过程，继续反汇编下一条指令，直到反汇编完程序文件的指令代码。

代码混淆是一种将计算机程序代码转换成一种功能上等价，但是难以阅读和理解的变形。

源代码混淆

将代码的变量、函数、类的名称改为毫无意义的名字；
修改代码部分逻辑，使其功能等价，但更难以理解……

VS

二进制代码混淆

分为两类：
其一是“反反汇编”的混淆，即针对反汇编缺陷进行设计使反汇编出错，或对代码加密混淆；
其二是指令控制流混淆，用来增加理解、分析反汇编代码的难度。

2.4 反调试

动态调试分析能够弥补静态分析中难以处理代码加壳及花指令等混淆的不足。与此同时，反调试技术也迅速发展，恶意代码用它识别是否被调试，或者让调试失败。

1

基于调试特征检测的反调试

当程序处于被调试状态时，PEB结构中有一个beingDebug标志会被置为非0，以此来判断程序是否处于调试状态

2

基于调试特征隐藏代码

异常中断指令int 3常被用来设置软件断点，在程序代码里植入int3指令是一个经典的反调试手段。

主要内容PE文件结构、系统进程管理、线程管理、内存管理等。

PE文件是微软公司的Windows操作系统上的可执行文件，全称为Portable Executable(可移植的可执行文件)。

图 2-14 PE 结构划分

PE文件头

DOS头：每个PE文件都以DOS MZ开头。

PE头：PE文件的主要定位信息所在。

PE数据区

区块表：是一个结构数组，每个结构包含了它所关联的区块信息，如位置、长度、属性等。

区块数据：包括代码区块、读写区块、导入表、导出表等。

进程是计算机中的程序关于特定数据集合上的一次运行活动，是系统进行资源调度和分配的基本单位。

Windows进程由一个执行体进程块EPROCESS来表示。

EPROCESS结构

EPROCESS结构包括内核进程块、进程标识、退出状态、创建和退出时间、进程优先级等属性信息。

内核进程块

也被称为进程控制块(PEB)，包含了Windows内核在调度线程时所需的基本信息，如页目录指针、内核时间、用户时间等。

进程环境块

该结构处于进程的用户态内存中，包含了映像基地址、模块列表、进程堆信息等。

线程是程序执行流的最小单元，是进程中的一个实体，是被操作系统独立调度和分派的基本单位。

线程块

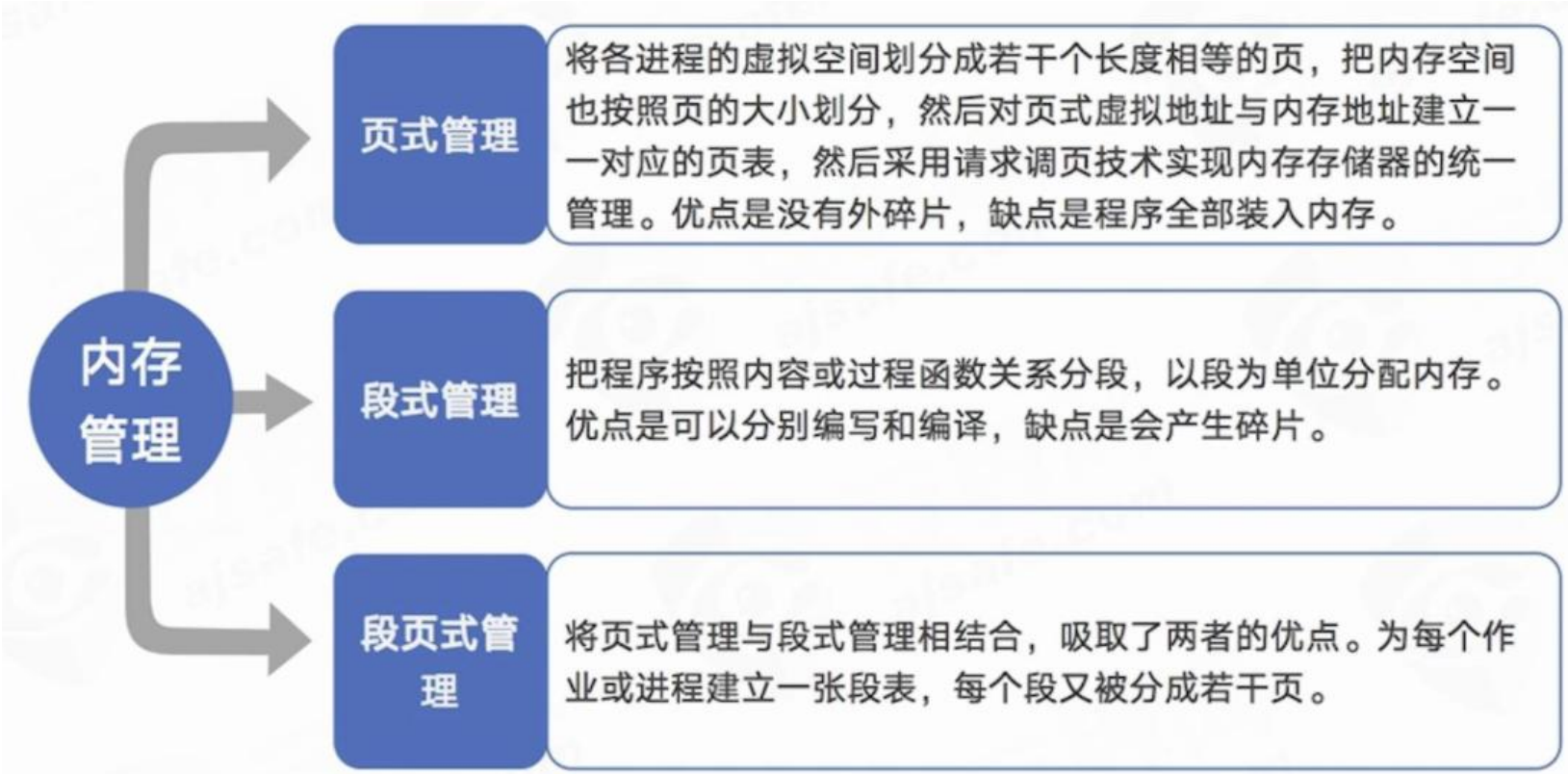
ETHREAD是线程的基本结构，包含了内核线程块指针、创建时间和退出时间、所属进程的ID标识、线程启动地址等属性。

内核线程块

位于系统内存内核空间，包含了Windows内核为正在运行的线程执行线程调度和同步而需要访问的信息。

线程环境块

TEB位于进程的用户地址空间，记录有关映像加载器和Windows DLL的环境信息。


内存管理
页式管理
将各进程的虚拟空间划分成若干个长度相等的页，把内存空间也按照页的大小划分，然后对页式虚拟地址与内存地址建立一一对应的页表，然后采用请求调页技术实现内存存储器的统一管理。优点是没有外碎片，缺点是程序全部装入内存。
段式管理
把程序按照内容或过程函数关系分段，以段为单位分配内存。优点是可以分别编写和编译，缺点是会产生碎片。
段页式管理
将页式管理与段式管理相结合，吸取了两者的优点。为每个作业或进程建立一张段表，每个段又被分成若干页。

课程小结

- 1.处理器硬件架构基础
- 主要内容包括：CPU的结构以及处理器设计的一些特性，包括保护模式、特权级、和虚拟化支持。
- 2.反汇编及对抗技术
- 主要内容包括：汇编语言基础、反汇编、代码混淆、反调试等技术。
- 3.Windows操作系统基础
- 主要内容包括：PE文件结构、系统进程管理、线程管理、内存管理等。

谢谢观赏