汇编

2019年9月9日　　11:14

09.10

1、理解、调试计算机语言

2、破解 cracker、黑客hacker

zjusec.com 浙大信息安全小组 AAA

Defcon比赛 腾讯科恩实验室

3、混合语言编程

4、汇编语言常用于编写操作系统、设备驱动程序以及病毒

5、软件加密-磁盘加密、软件狗dongle加密、序列号加密

调试器破解sum.exe示例 OD

代码窗：地址栏 机器语言 汇编语言

F8 执行程序 F2设置/取消断点 F7跟踪调用

Alt+backspace 恢复修改

寄存器register CPU内部的全局变量

EAX-C语言函数的返回值

数据窗/代码窗：Ctrl-G＋地址/函数名

09.17

Password.exe 是控制台程序，没有菜单、按钮等界面，只有一个黑的输入/输出窗口

regtest是一个标准的Windows程序，其输入/输出是通过消息循环实现的，并非调用scanf()、printf()函数

弹框会调用MessageBoxA()，其中MessageBoxA是Windows操作系统的内核，称为API()Application Program Interface)

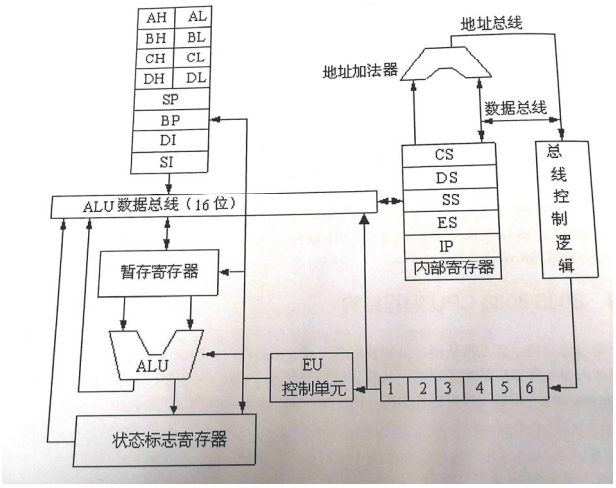
Keygen.exe 注册机

书

数据表示及运算

十六进制数以H、h结尾，字母开头则需要加前缀0

CPU编程结构



指令＝操作码+操作数

操作数寻址

立即数-常数

寄存器

直接寻址-常数表示偏移地址（e.g. ds:[10ABh]）

间接寻址-偏移地址[基址(BX/BP)或变址(SI/DI)寄存器+常数](e.g. word ptr ds:[bx+2])

编译步骤

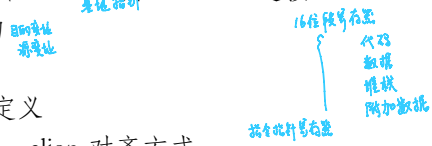
编辑Edit、汇编Assemb、连接Link

间接寻址-偏移地址[基址(BX/BP)或变址(SI/DI)寄存器+常数](e.g. word ptr ds:[bx+2])

编译步骤

编辑Edit、汇编Assemb、连接Link

程序结构



段

段定义

align-对齐方式

byte字节 word字 dword双字 para节/16字节 page页

db dw dd

combine-合并类型

public stack common memory at

段假设

建立段寄存器与段的对应关系

assume cs:code, ds:data, es:extra, ss:stk//ds、es仍需在程序段中赋值

段引用

mov ax, seg xx//访问段地址

mov di, offset xx//访问偏移地址

程序结束

end labelname//源程序到此结束，程序运行时从label段开始

程序段前缀PSP

Program segment prefix, 长度为100h字节的一段内存

程序运行时 ds/es = PSP段址

ss:sp=堆栈段段址和最后一个字节偏移地址+1

cs:ip=代码段段址和end指定标号偏移地址，程序从此处开始运行

示例 程序.exe的内存布局

起始地址	结束地址	长度（字节为单位）	内容
1432：0000	1432：00FF	100h	PSP
1442：0000	1442：000F	10h	data数据段
1443：0000	1443：000F	10h	code代码段
1444：0000	1444：01FF	200h	stk堆栈段

符号常数定义/可置于data segment之前

=（常数表达式）

equ（常数表达式、字符串、汇编语句，但不能重复定义）

变量引用

数据段中，xx 或 offset xx 都可作为变量的偏移地址

代码段中，xx 或 [x]都可作为变量的值

位置计数器

代码段中数据偏移地址

可访问数组元素个数 $ - offset xx

$ - 得到位置计数器的值

Org 0000h-改变位置计数器即偏移地址的值

CMO可执行程序

程序只定义代码段，程序入口偏移地址为100h(伪指令org设置)

近远过程调用

call-retn/retf（堆栈原理）

寄存器的保存与恢复（入栈出栈，注意顺序）

传递参数-寄存器、变量

软件中断调用DOS功能

初始化入口参数、功能号传入ah，执行中断指令int 21h

Ah = 01h-输入字符