漏洞银行逆向工程系列课程（一） —— 暴力流学汇编

第六课_80386寄存器组

主讲：K1ght（漏洞银行安全专家）

讲师互动丨课后交流丨资料共享 二进制学习圈：**542285506**

漏洞银行微信公众号：**BUG_BANK**

漏洞银行 | BUGBANK
www.bugbank.cn

主要内容

01
80386寄存器

02
内存寻址方式

80386都有哪些寄存器

通用寄存器(EAX、EBX、ECX、EDX、ESP、EBP、ESI、EDI)

段寄存器(CS、SS、DS、ES、FS、GS)

指令指针寄存器和标志寄存器(EIP、EFLAGS)

系统地址寄存器(GDTR、IDTR、LDTR、TR)

控制寄存器(CR0、CR1、CR2、CR3、CR4)

调试寄存器(DR0、DR1、DR2、DR3、DR4、DR5、DR6、DR7)

测试寄存器(TR6、TR7)

通用寄存器

EAX（累加器）

EBX（基址）

ECX（计数）

EDX（数据）

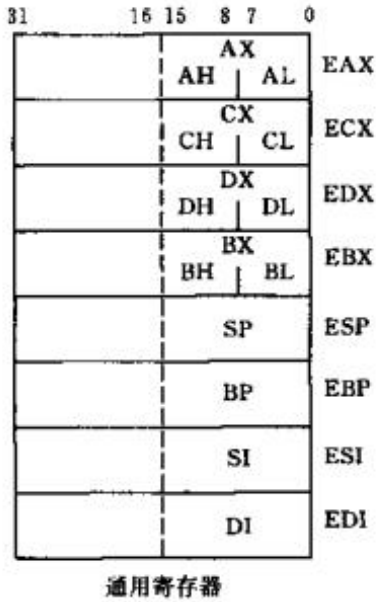
ESP（栈指针）

EBP（基址指针）

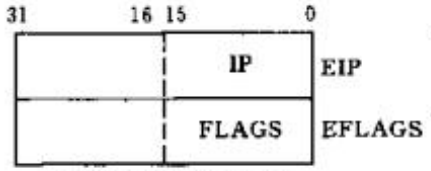
ESI（源变址）

EDI（目的变址）

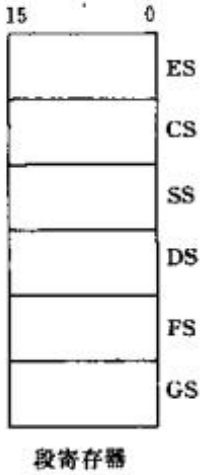
80386 寄存器的宽度大多是 32 位，可分为如下几组：通用寄存器、段寄存器、指令指针及标志寄存器、系统地址寄存器、控制寄存器、调试寄存器和测试寄存器。应用程序主要使用前三组寄存器，只有系统程序才会使用各种寄存器。这些寄存器是 x86 系列微处理器



通用寄存器



指令指针和标志寄存器



段寄存器

段寄存器

80386比8086/80286增加了两个段寄存器FS、GS。

CS：代码段寄存器

DS：数据段寄存器

SS：堆栈段寄存器

ES、FS 及GS：附加数据段寄存器

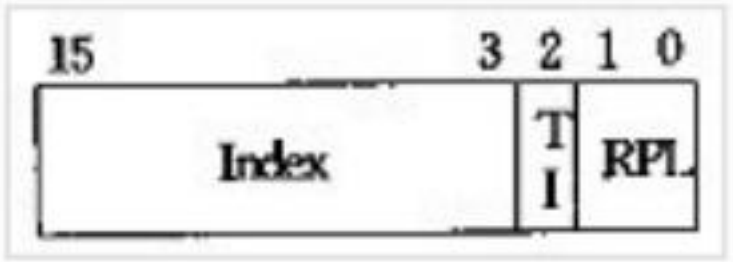
- 这些段寄存器中存放的不再是某个段的基地址，而是某个段的选择符（Selector）。因为16 位的寄存器无法存放32 位的段基地址，段基地址只好存放在段的描述符（Descriptor）中

段寄存器

RPL 特权级字段：0~3

TI ：指定包含段描述符的描述符表是在GDT（TI=0），还是在LDT（TI=1）

Index ：14位的索引字段可以识别的段从0至16383，共16384个段。



80386比8086/80286增加了两个段寄存器FS、GS。

CS：代码段寄存器

DS：数据段寄存器

SS：堆栈段寄存器

ES、FS 及GS：附加数据段寄存器

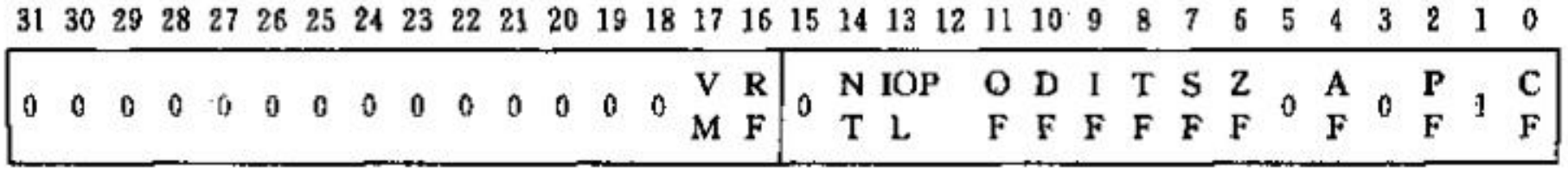
- 这些段寄存器中存放的不再是某个段的基地址，而是某个段的选择符（Selector）。因为16 位的寄存器无法存放32 位的段基地址，段基地址只好存放在段的描述符（Descriptor）中

指令指针寄存器

- 指令指针寄存器（EIP）中存放下一条将要执行指令的偏移量（offset ），这个偏移量是相对于目前正在运行的代码段寄存器（CS）而言的。偏移量加上当前代码段的基地址，就形成了下一条指令的地址。

标志寄存器

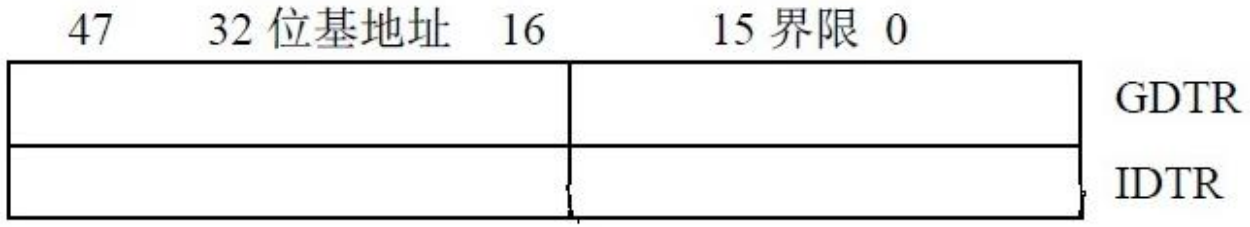
- OF、DF、IF、TF、SF、ZF、AF、PF和CF在8086中就已经存在
- VM（Virtual-8086 mode）表示虚拟8086模式，如果VM被置位且80386已出于保护模式下，则CPU切换到虚拟8086模式，此时，对段的任何操作又回到了实模式，如同在8086下运行一样



系统地址寄存器

- 全局描述符表寄存器GDTR（Global Descriptor Table Register ），是48 位寄存器，用来保存全局描述符表（GDT）的32位基地址和GDT 的大小（16位）。
- 中断描述符表寄存器IDTR（Interrupt Descriptor Table Register），是48 位寄存器，用来保存中断描述符表（IDT）的32位基地址和IDT 的大小（16位）。
- 局部描述符表寄存器LDTR（Local Descriptor Table Register ），是16 位寄存器，保存局部描述符表LDT 段的选择符。
- 任务状态寄存器TR（Task State Register）是16 位寄存器，用于保存任务状态段TSS 段的16 位选择符。

系统地址寄存器



- 全局描述符表寄存器GDTR（Global Descriptor Table Register ），是48 位寄存器，用来保存全局描述符表（GDT）的32 位基地址和GDT 的大小（16位）。
- 中断描述符表寄存器IDTR（Interrupt Descriptor Table Register），是48 位寄存器，用来保存中断描述符表（IDT）的32 位基地址和IDT 的大小（16位）。
- 局部描述符表寄存器LDTR（Local Descriptor Table Register ），是16 位寄存器，保存局部描述符表LDT 段的选择符。
- 任务状态寄存器TR（Task State Register）是16 位寄存器，用于保存任务状态段TSS 段的16 位选择符。

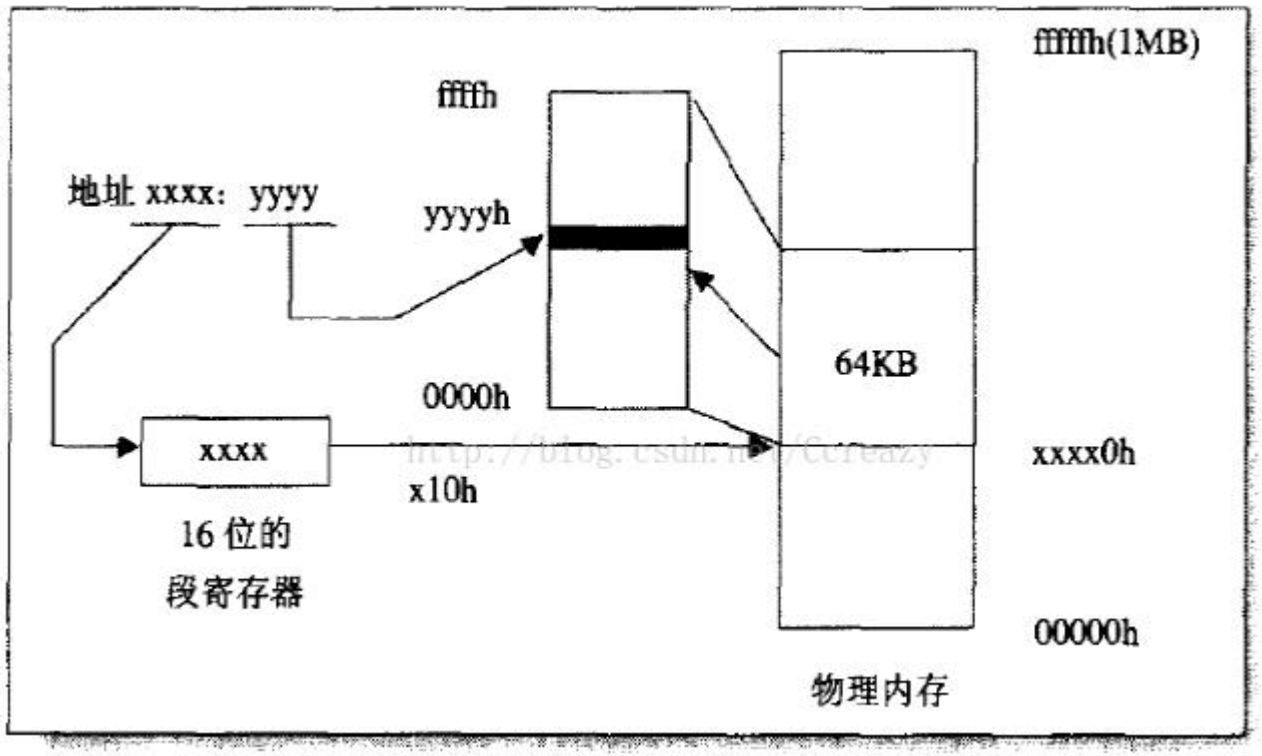
系统地址寄存器

- 全局描述符表寄存器GDTR（Global Descriptor Table Register ），是48 位寄存器，用来保存全局描述符表（GDT）的32 位基地址和GDT 的大小（16位）。
- 中断描述符表寄存器IDTR（Interrupt Descriptor Table Register），是48 位寄存器，用来保存中断描述符表（IDT）的32 位基地址和IDT 的大小（16位）。
- 局部描述符表寄存器LDTR（Local Descriptor Table Register ），是16 位寄存器，保存局部描述符表LDT 段的选择符。
- 任务状态寄存器TR（Task State Register）是16 位寄存器，用于保存任务状态段TSS 段的16 位选择符。

实模式寻址方式

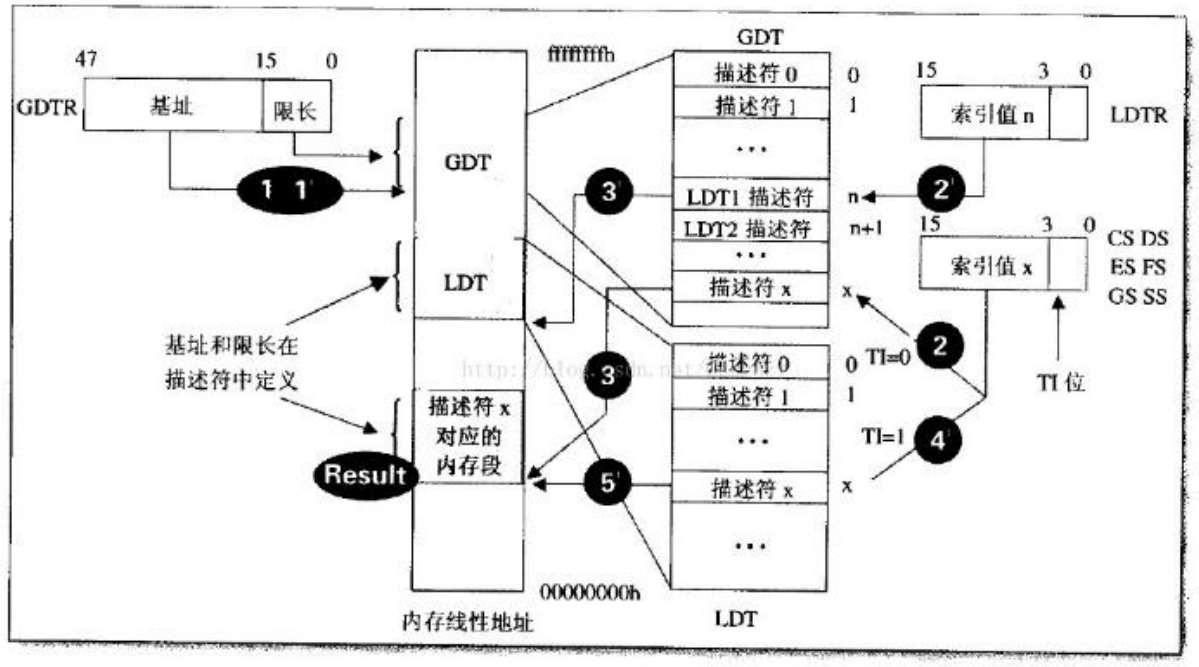
CS：IP

DS：[bx]



保护模式寻址方式

- 段描述符：地址空间的可读，可写，可执行等保护问题和地址空间的安全属性。要用64位的数据才能显示，这64位的属性数据叫做段描述符，



- 通过段寄存器来提供索引从段选择表中选择接收到的索引来找到相应的段描述符。

- 全局描述符表寄存器GDTR，局部描述符表寄存器LDTR两个分别指向全局描述符表GDT和局部描述符表LDT

80386存储器寻址

```
MOV     AL,[EBX+EBP*2]          ;默认的段寄存器是 DS
MOV     AL,[EBX+EBP]            ;默认的段寄存器是 DS
MOV     AL,[EBP+EBX]            ;默认的段寄存器是 SS
MOV     AL,GS:[EBP*2]           ;显式指定段寄存器 GS
MOV     EAX,[ESP]               ;默认的段寄存器是 SS
MOV     AL,CS:[ESP+2]           ;显式指定段寄存器 CS
MOV     [ESP+EBP*2],ECX         ;默认的段寄存器是 SS
MOV     AL,DS:[ESP+EDI+12]      ;显式指定段寄存器 DS
```

加入漏洞银行二进制学习圈　**QQ群号：542285506**

获取**免费课件**｜结交**讲师伙伴**｜紧跟**后续课程**

微信公众号：BUG_BANK

漏洞银行 | BUGBANK
www.bugbank.cn