漏洞银行逆向工程系列课程（一） —— 暴力流学汇编

第七课_数据传送指令

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

数据传送指令

通用数据传送指令

堆栈操作指令

地址传送指令

标志寄存器传送指令

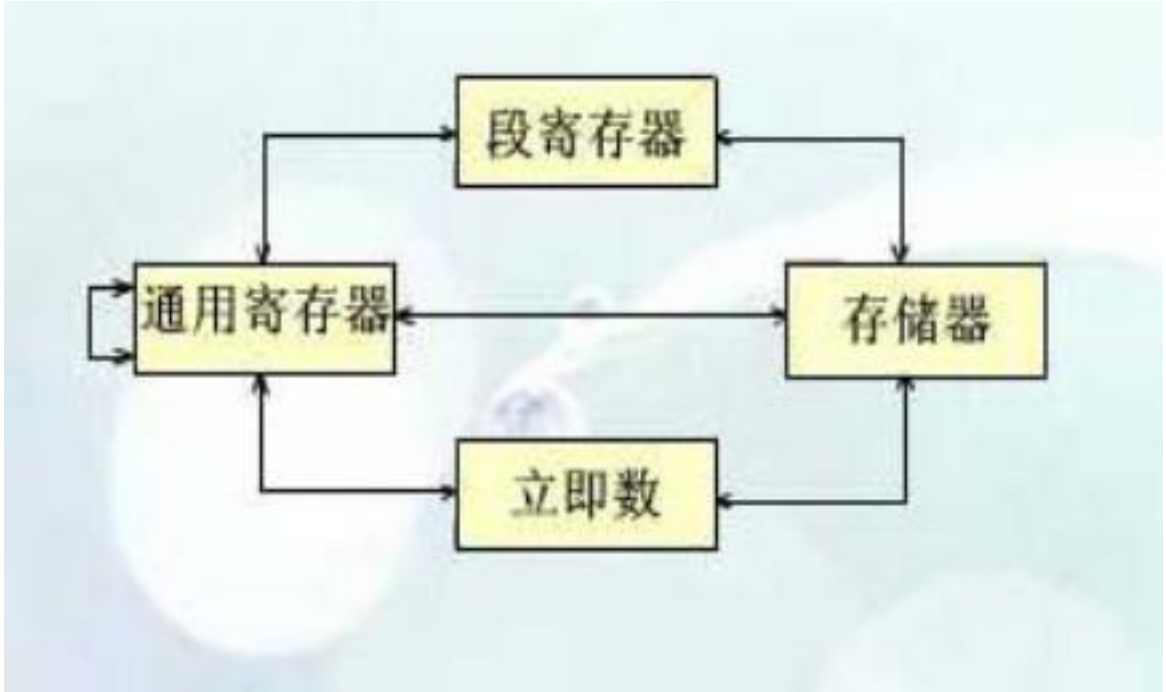
一、通用数据传送指令

1.传送指令是使用最频繁的指令，

格式：MOV DEST,SRC

功能：把一个字节，字或双字从源操作数SRC传送至目的操作数DEST。

传送指令允许的数据流方向见图 ⟶



MOV EAX，ESI；

EAX←ESI　　(32位)

一、通用数据传送指令

- **立即数送通用寄存器、存储器。**

```
MOV EAX，12345678H    ；EAX←12345678H        (32位)
MOV [BX]，12H         ；间接寻址             (8位)
MOV AX，1234H         ；AX←1234H(16位)
```

- **使用该指令应注意以下问题：**

源和目的操作数不允许同时为存储器操作数；

源和目的操作数数据类型必须一致；

源和目的操作数不允许同时为段寄存器；

目的操作数不允许为CS和立即数；

当源操作数为立即数时，目的操作数不允许为段寄存器；

传送操作不影响标志位。

一、通用数据传送指令

2 .扩展传送指令

格式：MOV SX　DEST，SRC

MOV ZX　DEST，SRC

功能：将源操作数由8位扩展到16位送目的操作数，或由16位扩展到32位送目的操作数。其中MOVSX是按有符号数扩展，MOVZX是按无符号数扩展。无符号数或正数高位扩展为0，负数高位扩展为全“1”。

带符号数扩展

```
MOV     BL，80H     ;   -12
MOV     SX AX，BL     ;   将80H扩展为FF80H后送AX中。
```

无符号数扩展

```
MOV     BL，80H     ;   128
MOV     ZX AX，BL     ;   将80H扩展为0080H后送AX中。
```

一、通用数据传送指令

3 交换指令

(1)**格式：**XCHG OPR1，OPR2

功能：交换操作数OPR1和OPR2的值，操作数数据类型为字节、字或双字。允许通用寄存器之间，通用寄存器和存储器之间交换数据。

XCHG AX，BX；通用寄存器之间交换数据(16位)

XCHG ESI，EDI；通用寄存器之间交换数据(32位)

使用该指令应注意以下问题：

·操作数OPR1和OPR2不允许同为存储器操作数；

·操作数数据类型必须一致；

·交换指令不影响标志位。

格式：BSWAP REG

功能：将32位通用寄存器中，第1个字节和第4个字节交换，第2个字节和第3个字节交换。

```
MOV EAX，44332211H
BSWAP EAX          ；EAX=11223344H
```

二、堆栈操作指令

1 压栈指令

(1)**格式：**PUSH SRC

功能：将源操作数压下堆栈，源操作数允许为16位或32位通用寄存器、存储器和立即数以及16位段寄存器。当操作数数据类型为字类型，压栈操作使SP值减2；当数据类型为双字类型，压栈操作使SP值减4。

```
PUSH AX                    ；通用寄存器操作数入栈(16位)
PUSH EBX                   ；通用寄存器操作数入栈(32位)
```

PUSHA、 PUSHAD

功能：PUSHA　　将16位通用寄存器压入堆栈，压栈顺序为AX，CX，DX，BX，SP，BP，SI，DI。

PUSHAD　将32位通用寄存器压入堆栈，压栈顺序为EAX，ECX，EDX，EBX，ESP，EBP，ESI，EDI。

二、堆栈操作指令

2 出栈指令

(1) **格式：**POP DEST

功能：从栈顶弹出操作数送入目的操作数。目的操作数允许为16或32位通用寄存器、存储器和16位段寄存器。当操作数数据类型为字类型，出栈操作使SP加2；当操作数数据类型为双字类型，出栈操作使SP加4。

```
POP AX          ；操作数出栈送寄存器(16位)
POP ECX         ；操作数出栈送寄存器(32位)
```

```
POPA、POPAD
```

功能：POPA从堆栈移出16字节数据，并且按顺序存入寄存器DI，SI，BP，SP，BX，DX，CX，AX中。

POPAD从堆栈移出32字节数据，并且按顺序存入寄存器EDI，ESI，EBP，ESP，EBX，EDX，ECX，EAX中。

使用堆栈操作指令应注意以下问题。

(1) 目的操作数不允许为CS以及立即数。

(2) 堆栈操作指令不影响标志位。

三、地址传送指令

格式：LEA REG，MEM

功能：将源操作数的有效地址传送到通用寄存器，操作数REG为16位或32位通用寄存器，源操作数为16位或32位存储器操作数。

LEA EAX，[EBX]；将EBX内容的有效地址传送到EAX中(32位)

四、标志寄存器传送指令

(1) **格式：**LAHF
SAHF
功能：LAHF将标志寄存器中低8位送AH中。SAHF将AH中内容送标志寄存器中低8位。

(2) **格式：**PUSHF
POPF
功能：PUSHF将标志寄存器低16位内容压入堆栈，SP←SP-2。POPF将当前栈顶一个字传送到标志寄存器低16位中，SP←SP+2。

(3) **格式：**PUSHFD
POPFD
功能：PUSHFD将标志寄存器32位内容压入堆栈SP←SP-4。POPFD将当前栈顶一个双字传送到32位标志寄存器中，SP←SP+4。

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