漏洞银行逆向工程系列讲座（一） —— 暴力流学汇编

8086指令系统之通用寄存器

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 **二进制群：542285506**

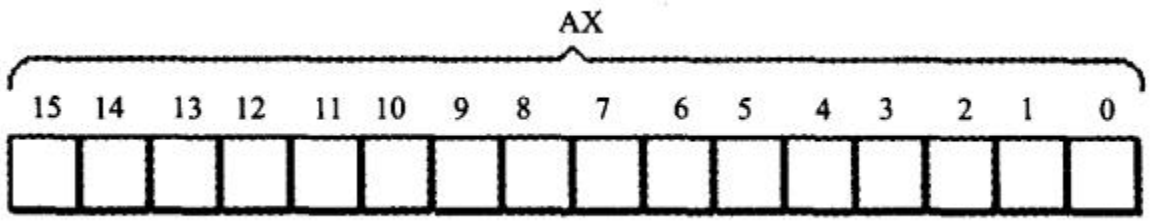
漏洞银行微信公众号：**BUG_BANK**

漏洞银行 | BUGBANK
www.bugbank.cn

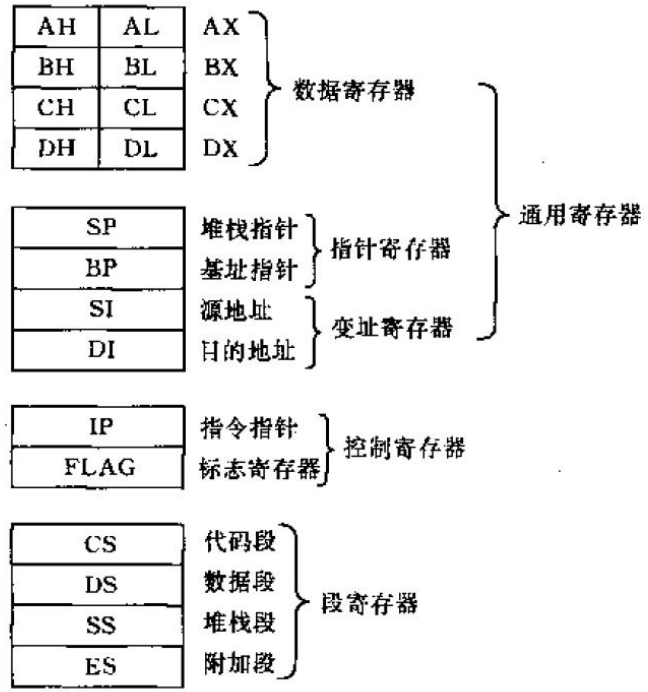
目录

数据寄存器

- AX、BX、CX、DX
- 1字节（3BH）=8位（0011 1100）
- AX=ABCDH
- AX可分为AH（ABH），AL（CDH）



通用寄存器



寄 存 器	用 途
AX	字乘法，字除法，字 I/O
AL	字节乘法，字节除法，字节 I/O，十进制算术运算
AH	字节乘法，字节除法
BX	存储器指针
CX	串操作或循环控制中的计数器
CL	移位计数器
DX	字乘法，字除法，间接 I/O
SI	存储器指针（串操作中的源指针）
DI	存储器指针（串操作中的目的指针）
BP	存储器指针（存取堆栈的指针）
SP	堆栈指针

介绍几条汇编指令

- mov　　ax,18
- mov　　ah,78
- add　　ax,bx
- add　　al,1(ax=00FFH,add运行之后ax是多少？)
- sub　ax,1

物理地址

- 在存储器里以字节为单位存储信息，为正确地存放或取得信息，每一个字节单元给以一个唯一的存储器地址，称为物理地址（Physical Address），又叫实际地址或绝对地址。
- 8086是16位cpu，地址总线是20位
- 物理地址=段地址*10H+偏移地址
- CS：2000H，IP：0033H
- 物理地址=2000Hx10H+0033H=20033H

DS和[address]

- mov ax,[1000H]
- mov ax,[bx]

栈

1000H	
1001H	
1002H	
1003H	

栈

- PUSH
- POP

- push ax
- push 1000h
- pop bx
- pop ax

SS和SP

SS:SP---->

1000H	
1001H	
1002H	
1003H	

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