王爽汇编第17章,指令系统总结

1．指令系统总结图：

汇编指令总结　　指令系统总结

我们对 8086CPU 的指令系统进行一下总结。读者若要详细了解 8086 指令系统中的各个指令的用法，可以查看有关的指令手册。

8086CPU 提供以下几大类指令。

1. 数据传送指令

比如，mov、push、pop、pushf、popf、xchg 等都是数据传送指令，这些指令实现寄存器和内存、寄存器和寄存器之间的单个数据传送。

2. 算术运算指令

比如，add、sub、adc、sbb、inc、dec、cmp、imul、idiv、aaa 等都是算术运算指令，这些指令实现寄存器和内存中的数据的算数运算。它们的执行结果影响标志寄存器的 sf、zf、of、cf、pf、af 位。

3. 逻辑指令

比如，and、or、not、xor、test、shl、shr、sal、sar、rol、ror、rcl、rcr 等都是逻辑指令。除了 not 指令外，它们的执行结果都影响标志寄存器的相关标志位。

4. 转移指令

可以修改 IP，或同时修改 CS 和 IP 的指令统称为转移指令。转移指令分为以下几类。

(1) 无条件转移指令，比如，jmp；
(2) 条件转移指令，比如，jcxz、je、jb、ja、jnb、jna 等；
(3) 循环指令，比如，loop；
(4) 过程，比如，call、ret、retf；
(5) 中断，比如，int、iret。

5. 处理机控制指令

这些指令对标志寄存器或其他处理机状态进行设置，比如，cld、std、cli、sti、nop、clc、cmc、stc、hlt、wait、esc、lock 等都是处理机控制指令。

6. 串处理指令

这些指令对内存中的批量数据进行处理，比如，movsb、movsw、cmps、scas、lods、stos 等。若要使用这些指令方便地进行批量数据的处理，则需要和 rep、repe、repne 等前缀指令配合使用。

> 参考文章：
>
> https://blog.csdn.net/qq_39654127/article/details/88698911 王爽《汇编语言》笔记（详细）

最后，我是先学的逆向，当时没有学汇编 才发现原来汇编对逆向是那么的重要，了解汇编后 再回头来看OD动态调试 好多以前不懂的东西 豁然开朗了。

有兴趣的小伙伴可以加群：一起讨论逆向、PWN甚至是Web安全 群内有web大佬 ai大佬 pwn大佬，只有我这个re菜鸡哈哈

群名称:Pwn菜鸡学习小分队
群 号:1145528880