20200702

Thursday, July 2, 2020 09:56

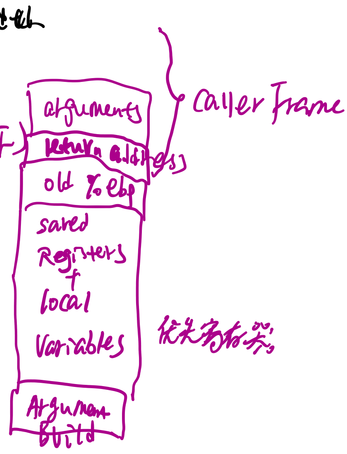
程序运行栈的基本操作 -2

call label

leal 跳转已找到返回地址

栈帧内容（自顶向下）

子过程参数.



寄存器使用惯例

ebx

调用者负责保存寄存器的状态

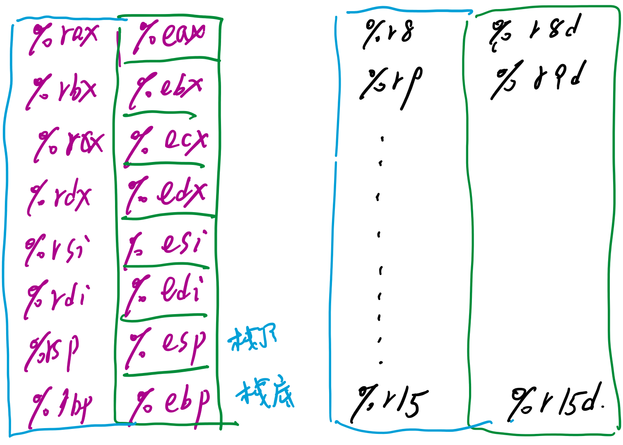
被调用者负责保存寄存器的状态

Caller eax, edx, ecx

Call ebx, esi, edi

ebp, esp

x86-64 通用寄存器



%rsp 指向栈顶

其它寄存器通用

%ebp 也被释放出来

寄存器使用惯例

%rax return value

%rbx Callee saved

%rcx Argument #4

%rdx Argument #3

%rsi Argument #2

%rdi Argument #1

%rsp 硬性指向栈顶

%rbp

%r8 Argument #5

%r9 Argument #6

%r10

%r11 used for linker

%r12

%r13

%r14

%r15

lea：取偏移地址 leaq a(b, c, d), %rax

⇒ a+b+c*d → %rax

80x86 汇编与 C 语言 一 四