Scribe Notes

Thursday, October 24, 2013 2:41 PM

Calling convention: compiler matches functions to instructions. "Convention" because can be customized, non-standard

- Example: %eax is return value
- Example: Stack frames are 16 byte aligned
- Example: First argument is at 4(%esp) when function begins
- Example: Return address is stored at (%esp)

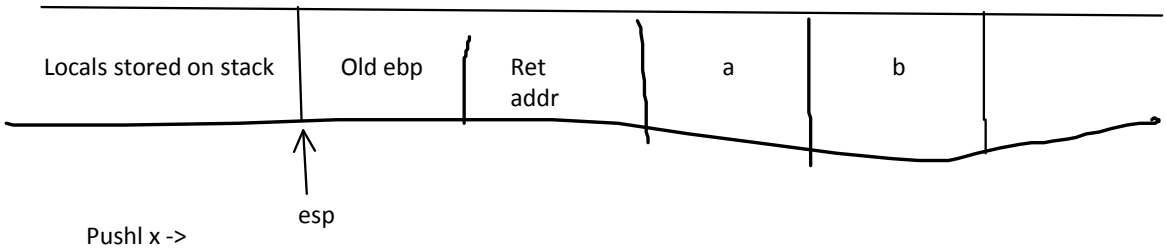
ebp: base pointer register. Boundary between params & locals. Does not change.

Callee Save Register: save old value on stack and restore the register if touched.

- Example: ebp, esp, ebx, esi, edi
- **Caller** Save: eax, edx

Pos offset off ebp is likely argument

f(int a, int)



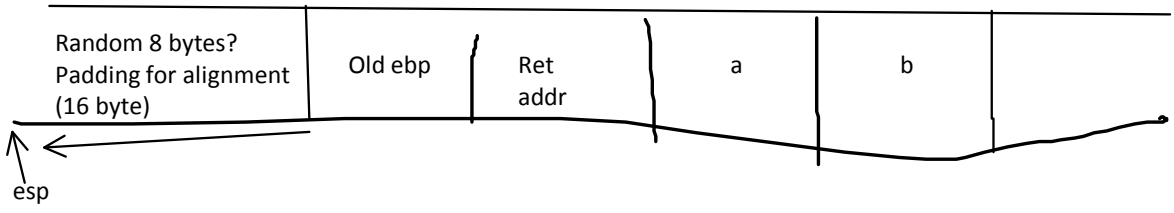
Popl x ->
movl %esp, x
addl $4, %esp

Pushl x ->
subl $4, esp
Movl x, esp

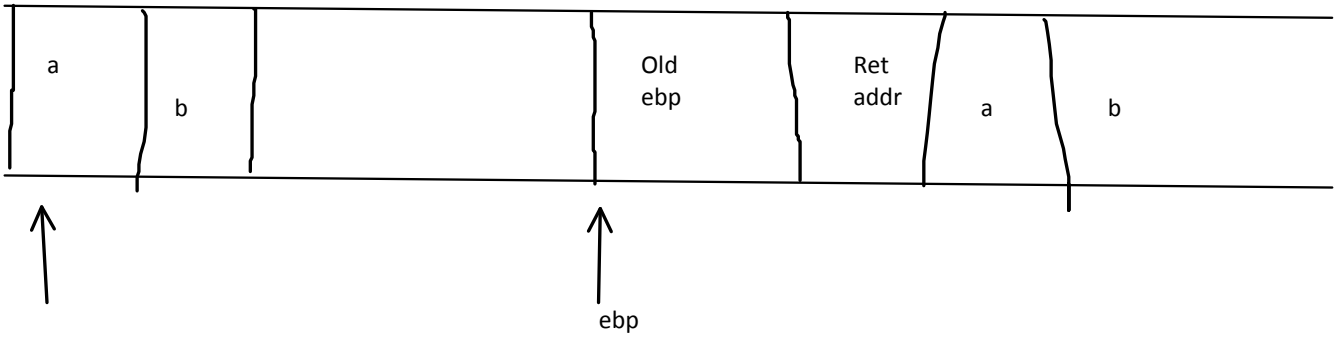
"dereference" register: (%reg)
Address of register: %reg

Leave ->
movl %ebp, %esp
popl %ebp

Compiler does this instead:



F46:



Movl(array, ??, size), destination

leal a, b
moves addr of a into b (**L**oad **E**ffective **A**ddress)