10/5/2024

BOMB LAB RECITATION:-

→ If you blow up your bomb, it notifies AutoLAB.
  — 0.5 pts everytime you blow up.

→ Revision of Registers

%rax → that's where the return value is stored

- First six arguments stored in register, above six goes to stack
- In IA32 machines all of the arguments were stored in the stock. Good we have X86 Machines with 16 regs.
- %rsp → stores reference to the head of stack.
- Registers are fast, accessing something from stack is slower.
- If you just wont to use the lower 32-bit we use the '%e' identifier for the register.
- Constants start with '$' sign.
- %esi is lower 32 bit of %rsi, same convention holds for all regs.
- Register can store a value or they can store an address (referencing a location in memory)
- Paranthesis around a register, → Go get me that value from the memory

Example (%rbx) → addressing mode.

- Memory math; for example;- Look slides

  0x4(%rcx, %rdi, 0x1)

Instructions

```
mov   %rbx, %rdx      =>  rdx = rbx.
add   (%rdx), %r~~dx~~ r8  =>  r8 += value at rd x.
```

→ First (%rdx) is dereferenced i.e the original value is brough in from the memory and added into whatever was in reg %r8.

Lea instruction = Load effective address. It can also do the memory arithomatic and more the result to the destination Register

Lea → do not ~~fe~~ dereference

- derefrencing means fetching the original value that lives in that memory ~~reference~~ location
- Lea (%rdr, rbx, 2), %rdx    rdx = rdx + rbx * 2
- The %rdx still holds the memory address ~~and~~ as lea do not dereference.
- In easy word lea do not get the value living at that addrees. it only copies the memory location from src to dest

⟷

- (Cmp(l)) → suffix l indicates the word size is 4 bytes (32 bits)

↓

- Compare instruction
- Compare instructions set the flag registers

→ ~~Comp~~ Cmpl %r9, %r10 will check if %r10>%r9
If its true it will set the condition flag to 1

→ Remember there were ft. registers which only hold flags

✓ This is an addrees not a value

Jg $\boxed{\text{'8675309}}$

→ jg → jumpgreater than. This instruction will kick in only if the condition flag set by cmpl instruction is 1.

- test instructions ,

test %r8, %r8
jnz (%rsi)

test instruction looks for values in %r8 and %r8 and set the flag to 1 if they are not zero. If flag is set to 1 by test jnz kicks in and jumps to address stored in %rsi.

## BOMB LAB

objdump -E bomb

↳ flag for symbol table.

-d

↳ flag for dissassembled program

Explore the symbol table and Assembly code

Open gbb

└ Continue in Class