15-213 Recitation
Bomblab

Your TAs

Friday, September 6th

Reminders

- **`datalab`** is due on ***Tuesday (Sep 10)***.
- **`bomblab`** is out! Due *September 19th*.
- Bootcamp 2: *Debugging & GDB* is pre-recorded. Watch Piazza for the link.

Agenda

- Assembly Refresher
- Preview: Calling Conventions
- Intro to `bomblab`
- `bomblab` defuse kit
- *If time*: `gdb` demo

Assembly Refresher

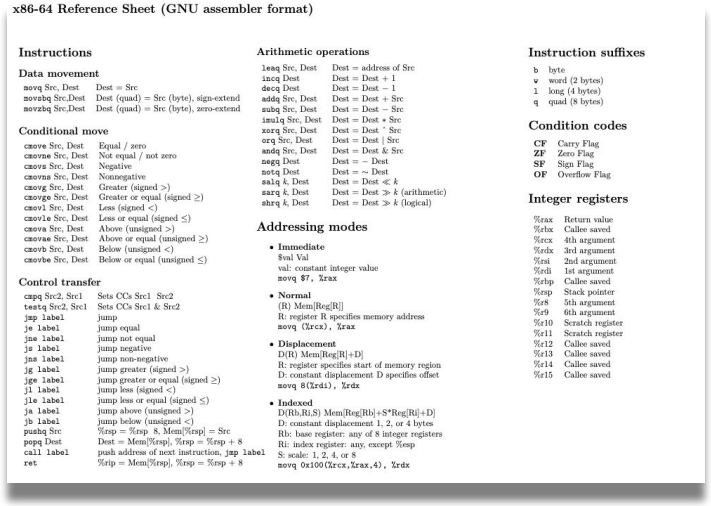
Reading Assembly

- We will use ***AT&T*** syntax in this class:

```
movq Src, Dest          movq Dest, Src
addq Src, Dest          addq Dest, Src
```

AT&T ***Intel***

- If you get stuck, refer to our assembly cheat sheet!



x86-64 Reference Sheet (GNU assembler format)

Instructions

Data movement

`movq` Src, Dest	Dest = Src
`movsbq` Src,Dest	Dest (quad) = Src (byte), sign-extend
`movzbq` Src,Dest	Dest (quad) = Src (byte), zero-extend

Conditional move

`cmove` Src, Dest	Equal / zero
`cmovne` Src, Dest	Not equal / not zero
`cmovs` Src, Dest	Negative
`cmovns` Src, Dest	Nonnegative
`cmovg` Src, Dest	Greater (signed >)
`cmovge` Src, Dest	Greater or equal (signed ≥)
`cmovl` Src, Dest	Less (signed <)
`cmovle` Src, Dest	Less or equal (signed ≤)
`cmova` Src, Dest	Above (unsigned >)
`cmovae` Src, Dest	Above or equal (unsigned ≥)
`cmovb` Src, Dest	Below (unsigned <)
`cmovbe` Src, Dest	Below or equal (unsigned ≤)

Control transfer

`cmpq` Src2, Src1	Sets CCs Src1 − Src2
`testq` Src2, Src1	Sets CCs Src1 & Src2
`jmp label`	jump
`je label`	jump equal
`jne label`	jump not equal
`js label`	jump negative
`jns label`	jump non-negative
`jg label`	jump greater (signed >)
`jge label`	jump greater or equal (signed ≥)
`jl label`	jump less (signed <)
`jle label`	jump less or equal (signed ≤)
`ja label`	jump above (unsigned >)
`jb label`	jump below (unsigned <)
`pushq` Src	%rsp = %rsp − 8, Mem[%rsp] = Src
`popq` Dest	Dest = Mem[%rsp], %rsp = %rsp + 8
`call label`	push address of next instruction, `jmp label`
`ret`	%rip = Mem[%rsp], %rsp = %rsp + 8

Arithmetic operations

`leaq` Src, Dest	Dest = address of Src
`incq` Dest	Dest = Dest + 1
`decq` Dest	Dest = Dest − 1
`addq` Src, Dest	Dest = Dest + Src
`subq` Src, Dest	Dest = Dest − Src
`imulq` Src, Dest	Dest = Dest * Src
`xorq` Src, Dest	Dest = Dest ^ Src
`orq` Src, Dest	Dest = Dest | Src
`andq` Src, Dest	Dest = Dest & Src
`negq` Dest	Dest = − Dest
`notq` Dest	Dest = ~ Dest
`salq` *k*, Dest	Dest = Dest ≪ *k*
`sarq` *k*, Dest	Dest = Dest ≫ *k* (arithmetic)
`shrq` *k*, Dest	Dest = Dest ≫ *k* (logical)

Addressing modes

- **Immediate**
  $val Val
  val: constant integer value
  `movq $7, %rax`
- **Normal**
  (R) Mem[Reg[R]]
  R: register R specifies memory address
  `movq (%rcx), %rax`
- **Displacement**
  D(R) Mem[Reg[R]+D]
  R: register specifies start of memory region
  D: constant displacement D specifies offset
  `movq 8(%rdi), %rdx`
- **Indexed**
  D(Rb,Ri,S) Mem[Reg[Rb]+S*Reg[Ri]+D]
  D: constant displacement 1, 2, or 4 bytes
  Rb: base register: any of 8 integer registers
  Ri: index register: any, except %esp
  S: scale: 1, 2, 4, or 8
  `movq 0x100(%rcx,%rax,4), %rdx`

Instruction suffixes

`b`	byte
`w`	word (2 bytes)
`l`	long (4 bytes)
`q`	quad (8 bytes)

Condition codes

CF	Carry Flag
ZF	Zero Flag
SF	Sign Flag
OF	Overflow Flag

Integer registers

%rax	Return value
%rbx	Callee saved
%rcx	4th argument
%rdx	3rd argument
%rsi	2nd argument
%rdi	1st argument
%rbp	Callee saved
%rsp	Stack pointer
%r8	5th argument
%r9	6th argument
%r10	Scratch register
%r11	Scratch register
%r12	Callee saved
%r13	Callee saved
%r14	Callee saved
%r15	Callee saved

Reading Assembly: Operands

Constants ("Immediate" Values)

- Start with **$**

`$-15213`
Decimal

`$0x3b6d`
Hex

Registers

- Can store values or addresses
- Start with **%**

`%rax`
"Return" Register

`%eax`
Low 32 bits of `%rax`

Memory Locations

- Parentheses around a register, or an addressing mode

`(%rbx)`
Normal

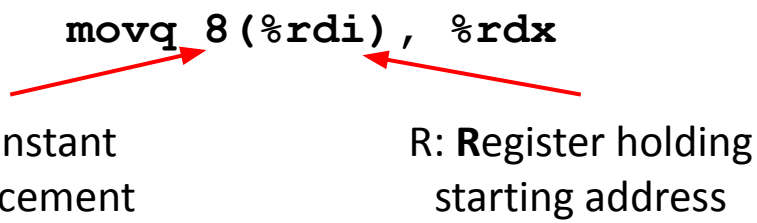
`0x1c(%rax)`
Displacement

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

Reading Assembly: Addressing Modes

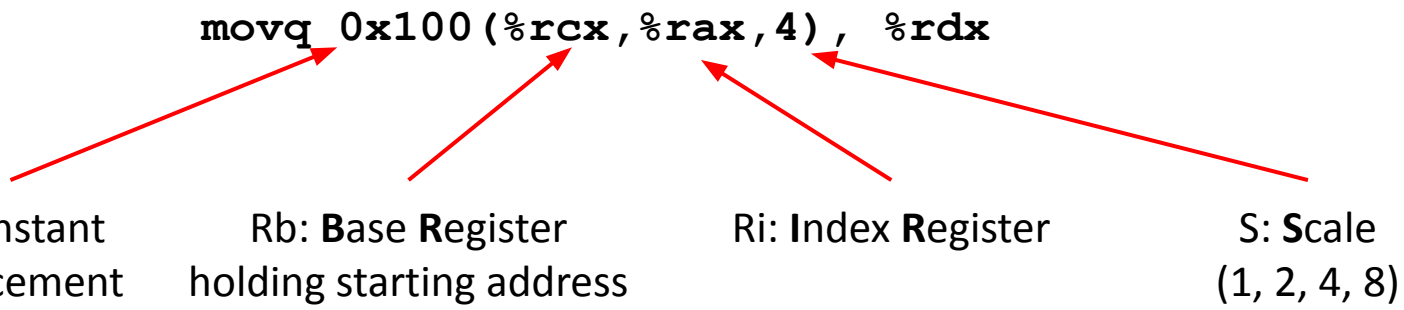
Displacement

- D(R) Mem[Reg[R] + D]



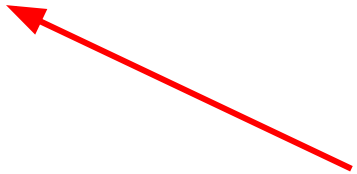
Indexed

- D(Rb, Ri, S) Mem[Reg[Rb] + S*Reg[Ri] + D]



Reading Assembly: Examples

Instruction	*Effect*
`mov %rbx, %rdx`	`rdx = rbx`
`add (%rdx), %r8`	`r8 += value at rdx`
`mul $3, %r8`	`r8 *= 3`
`sub $1, %r8`	`r8--`
`lea (%rdx, %rbx, 2), %rdx`	`rdx = rdx + rbx * 2`



No dereferencing!

Reading Assembly: Comparisons

Example

```
cmpl %r9, %r10
jg 8675309
```

- *"If the value of one register is greater than the value in the other, then jump to 8675309"*
- But which way around is it?
- Let's use the cheat sheet!

x86-64 Reference Sheet (GNU assembler format)

Instructions

Data movement

`movq` Src, Dest	Dest = Src
`movsbq` Src,Dest	Dest (quad) = Src (byte), sign-extend
`movzbq` Src,Dest	Dest (quad) = Src (byte), zero-extend

Conditional move

`cmove` Src, Dest	Equal / zero
`cmovne` Src, Dest	Not equal / not zero
`cmovs` Src, Dest	Negative
`cmovns` Src, Dest	Nonnegative
`cmovg` Src, Dest	Greater (signed >)
`cmovge` Src, Dest	Greater or equal (signed ≥)
`cmovl` Src, Dest	Less (signed <)
`cmovle` Src, Dest	Less or equal (signed ≤)
`cmova` Src, Dest	Above (unsigned >)
`cmovae` Src, Dest	Above or equal (unsigned ≥)
`cmovb` Src, Dest	Below (unsigned <)
`cmovbe` Src, Dest	Below or equal (unsigned ≤)

Control transfer

`cmpq` Src2, Src1	Sets CCs Src1 − Src2
`testq` Src2, Src1	Sets CCs Src1 & Src2
`jmp label`	jump
`je label`	jump equal
`jne label`	jump not equal
`js label`	jump negative
`jns label`	jump non-negative
`jg label`	jump greater (signed >)
`jge label`	jump greater or equal (signed ≥)
`jl label`	jump less (signed <)
`jle label`	jump less or equal (signed ≤)
`ja label`	jump above (unsigned >)
`jb label`	jump below (unsigned <)
`pushq` Src	%rsp = %rsp − 8, Mem[%rsp] = Src
`popq` Dest	Dest = Mem[%rsp], %rsp = %rsp + 8
`call label`	push address of next instruction, `jmp label`
`ret`	%rip = Mem[%rsp], %rsp = %rsp + 8

Arithmetic operations

`leaq` Src, Dest	Dest = address of Src
`incq` Dest	Dest = Dest + 1
`decq` Dest	Dest = Dest − 1
`addq` Src, Dest	Dest = Dest + Src
`subq` Src, Dest	Dest = Dest − Src
`imulq` Src, Dest	Dest = Dest * Src
`xorq` Src, Dest	Dest = Dest ^ Src
`orq` Src, Dest	Dest = Dest | Src
`andq` Src, Dest	Dest = Dest & Src
`negq` Dest	Dest = − Dest
`notq` Dest	Dest = ~ Dest
`salq` *k*, Dest	Dest = Dest ≪ *k*
`sarq` *k*, Dest	Dest = Dest ≫ *k* (arithmetic)
`shrq` *k*, Dest	Dest = Dest ≫ *k* (logical)

Addressing modes

- **Immediate**
  $val Val
  val: constant integer value
  `movq $7, %rax`
- **Normal**
  (R) Mem[Reg[R]]
  R: register R specifies memory address
  `movq (%rcx), %rax`
- **Displacement**
  D(R) Mem[Reg[R]+D]
  R: register specifies start of memory region
  D: constant displacement D specifies offset
  `movq 8(%rdi), %rdx`
- **Indexed**
  D(Rb,Ri,S) Mem[Reg[Rb]+S*Reg[Ri]+D]
  D: constant displacement 1, 2, or 4 bytes
  Rb: base register: any of 8 integer registers
  Ri: index register: any, except %esp
  S: scale: 1, 2, 4, or 8
  `movq 0x100(%rcx,%rax,4), %rdx`

Instruction suffixes

`b`	byte
`w`	word (2 bytes)
`l`	long (4 bytes)
`q`	quad (8 bytes)

Condition codes

CF	Carry Flag
ZF	Zero Flag
SF	Sign Flag
OF	Overflow Flag

Integer registers

%rax	Return value
%rbx	Callee saved
%rcx	4th argument
%rdx	3rd argument
%rsi	2nd argument
%rdi	1st argument
%rbp	Callee saved
%rsp	Stack pointer
%r8	5th argument
%r9	6th argument
%r10	Scratch register
%r11	Scratch register
%r12	Callee saved
%r13	Callee saved
%r14	Callee saved
%r15	Callee saved

Control transfer

`cmpq` Src2, Src1	Sets CCs Src1 − Src2
`testq` Src2, Src1	Sets CCs Src1 & Src2
`jmp label`	jump
`je label`	jump equal
`jne label`	jump not equal
`js label`	jump negative
`jns label`	jump non-negative
`jg label`	jump greater (signed >)
`jge label`	jump greater or equal (signed ≥)

- **`Src1`** is **`%r10`**, **`Src2`** is **`%r9`**
- Set CCs based on **`Src1 <op> Src2`**
- **`<op>`** is **`>`**

```
cmpl %r9, %r10
jg 8675309
```

- So we jump if: **`%r10 > %r9`**
- *"If the value of* **`%r10`** *is greater than the value in* **`%r9`***, then jump to 8675309"*

Reading Assembly: Jumps

Instruction	Condition	Description
`jmp`	`1`	Unconditional Jump
`je/jz`	`ZF`	Equal/Zero
`jne/jnz`	`~ZF`	Not Equal/Not Zero
`js`	`SF`	Negative
`jns`	`~SF`	Non-negative
`jg`	`~(SF^OF)&~ZF`	Greater (Signed)
`jge`	`~(SF^OF)`	Greater or Equal (Signed)
`jl`	`(SF^OF)`	Less (Signed)
`jle`	`(SF^OF)|ZF`	Less or Equal (Signed)
`ja`	`~CF & ~ZF`	Above (unsigned)
`jb`	`CF`	Below (unsigned)

Reading Assembly: Jumps

```
cmp $0x15213, %r12
jge deadbeef
```

If **%r12 >= 0x15213**, then jump to **0xdeadbeef**.

```
cmp %rax, %rdi
jae 15213b
```

If the *unsigned* value in **%rdi** is greater than the *unsigned value* in **%rax**, jump to **0x15213b**.

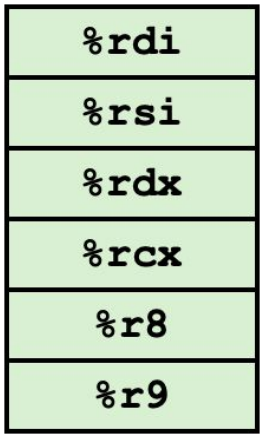
```
test %r8, %r8
jnz *%rsi
```

If **%r8** is not zero, jump to the address stored in **%rsi**.

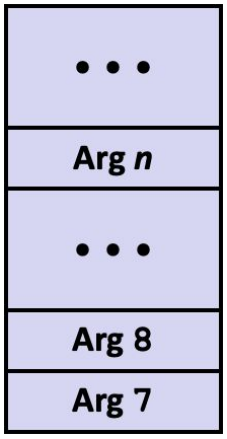
Preview: Calling Conventions

Calling Conventions: Passing Data

- How can we pass arguments to a procedure?



First 6 arguments passed in ***registers***.



Remaining arguments put at the end of the ***caller's stack frame***.

Calling Conventions: Passing Data

- How can we access the return value?

Return value placed in %rax
by convention.

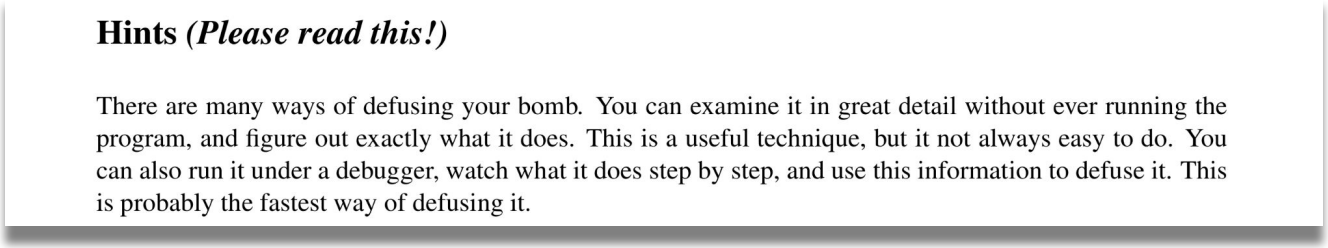
Bomblab

Bomblab: Premise

- ***Dr. Evil*** has planted *binary bombs* on our shark machines!
- Your task: defuse your bomb by passing the correct strings on **`stdin`**.
- You get:
  - A C source file for the *main program*
  - An executable (no C source code for the phases!)
- Have to reverse engineer the bomb using only **`gdb`** and the assembly code!

Bomblab: Getting Started

- Download your bomb from Autolab
- You must use the **Shark Machines** to extract (untar) and work on your Bomb.
- Run **`autolab setup`**
- 6 Progressively Harder Phases
  - Enter the correct string to move on to the next phase
- Read the write up! It has an entire page dedicated to hints!



Hints ***(Please read this!)***

There are many ways of defusing your bomb. You can examine it in great detail without ever running the program, and figure out exactly what it does. This is a useful technique, but it not always easy to do. You can also run it under a debugger, watch what it does step by step, and use this information to defuse it. This is probably the fastest way of defusing it.

Bomblab: Detonating Your Bomb

- Solving a phase automatically notifies Autolab and applies points to your score.
- If you let the bomb explode, Autolab will **deduct 0.5 points** *each time*.
- ***Do <u>not</u>*:**
  - Use gdb to jump between phases
  - Solve the phases out of order
  - Tamper with the bomb
  - Otherwise the bomb will explode!

Bomblab: Defuse Kit

Defuse Kit: Getting the Assembly

- Use **`objdump`** to get assembly code from your executable:
  - Then open and annotate in your favorite text editor!

```
objdump -d act1 > act1.asm
```

For syntax highlighting!

```
0000000000401620 <main>:
  401620:   f3 0f 1e fa             endbr64
  401624:   53                      push   %rbx
  401625:   48 63 ff                movslq %edi,%rdi
  401628:   48 89 f3                mov    %rsi,%rbx
  40162b:   31 c0                   xor    %eax,%eax
  40162d:   48 8b 54 fe f8          mov    -0x8(%rsi,%rdi,8),%rdx
  401632:   48 8d 35 6f d5 0a 00    lea    0xad56f(%rip),%rsi        # 4aeba8 <__PRETTY_FUNCTION__.0+0x78>
  401639:   bf 01 00 00 00          mov    $0x1,%edi
  40163e:   e8 4d 85 04 00          call   449b90 <___printf_chk>
  401643:   48 c7 03 00 00 00 00    movq   $0x0,(%rbx)
  40164a:   5b                      pop    %rbx
  40164b:   c3                      ret
  40164c:   0f 1f 40 00             nopl   0x0(%rax)
```

Defuse Kit: Figuring out Input Format

- Phases use **`sscanf`** to parse input strings:

```
char *example_string = "123, 456";
int a, b;
sscanf(example_string, "%d, %d", &a, &b);
```

```
...
1189: 48 8d 35 74 0e 00 00  lea  0xe74(%rip),%rsi # 2004 <_IO_stdin_used+0x4>
1190: 48 8d 3d 74 0e 00 00  lea  0xe74(%rip),%rdi # 200b <_IO_stdin_used+0xb>
1197: e8 d4 fe ff ff        call   1070 <__isoc99_sscanf@plt>
...
```

We know that the format string is the second argument (**`%rsi`**)

`0x2004` is the address of that string!

Defuse Kit: Figuring out Input Format

```
...
1189: 48 8d 35 74 0e 00 00  lea  0xe74(%rip),%rsi # 2004 <_IO_stdin_used+0x4>
1190: 48 8d 3d 74 0e 00 00  lea  0xe74(%rip),%rdi # 200b <_IO_stdin_used+0xb>
1197: e8 d4 fe ff ff        call   1070 <__isoc99_sscanf@plt>
...
```

- If we can examine that memory address, we can recover the format string!
- Enter ***gdb***:

```
(gdb) break main
Breakpoint 1 at 0x1169
(gdb) x /s 0x2004
0x2004: "%d, %d"
```

Examine memory address as a *string*.

We need two integers!

Defuse Kit: gdb

- **gdb** = GNU Debugger
- Fully-featured debugger:
  - For bomblab, lets you trace the execution of assembly
  - Useful for future labs, and well beyond 213.
  - Expand your debugging toolkit beyond **printf**!

Defuse Kit: gdb

Examining Program State

`print (p)`

```
print $rdi
```

Print contents of %rdi

```
(gdb) print /d 0x3b6d
$2 = 15213
```

Print with format

`info`

```
info registers
```

Print all register contents

`x` (For e**X**amine)

- **`x /[num][size][format]`**
- **`x /s 0x`**… Examine contents of address as a string
- **`x /64bx 0x`**… View 64 bytes starting at the given address in Hex Format

Warning: TUI Mode

TUI Mode

- Is very cool (can view assembly alongside **`gdb`** prompt).
- But can unexpectedly ***explode your bomb.***
- You will not get these points back.
- Can use **`vim`**/VSCode splitting instead.

GDB Demo

GDB Demo

If you want to follow along…

- Download today's activity handout from the *Schedule* page.

```
$ wget http://www.cs.cmu.edu/~213/activities/rec4.tar
$ tar xvpf rec4.tar
$ cd rec4
$ make
$ gdb act1
```