CS 208

Wednesday

26 Jan 2022
Where are my local vars?
where is my code?
malloc'd mem?
"Hello"
local vars: 0x7fFfCd... (48 bits)

functions: 0x556...
           0x559...
           558...
           564

"Hello"  —  0x55F...
           557

malloc  —  0x558...
           560...
           562
0x556
  code
  0x3760
  string literals
  0x562
  malloc
  // mem
  ...
  ...
  0x7FC
  local vars

for OS use

3 fixed size
3 expandable
3 "heap"

3 "system stack"
<table>
<thead>
<tr>
<th>n</th>
<th>x</th>
<th>buf</th>
<th>z</th>
</tr>
</thead>
</table>

**4 bytes**

**4 bytes**

**4 bytes**

**8 bytes**

\[ \text{int } n \]
\[ \text{int } x \]
\[ \text{char buf[8]} \]
\[ \text{main's locals} \]
int n;  // "automatic" memory allocation (stack)

char **p = malloc(100);

*p = dynamic mem. (heap)
mor — copy data from one place to a register

Learn about
- addressing modes
- q, d, w, b

movq — move a quad word (64)
movl — move a double word (32)
word — move a word (16)
test edi, edi
AND the two operands

EFLAGS

SF = sign bit of result
ZF = 1 if result is $\emptyset$
PF = 1 if # of 1 bits in result is even
test edi, edi
jz SOME LABEL

jump if the ZF bit is 1
don't jump otherwise
START:

mov
add
test
jz
mov
add

L1:

L2:

sub
ret

Program Counter (PC)

lad
CMP a, b
compute a - b
(or is it b - a?)

Sets EFLAGS

ZF
SF
PF

CF
OF
AF
CMP edi, 50
23 - 50 < 0
SF = 1
So JLE jumps