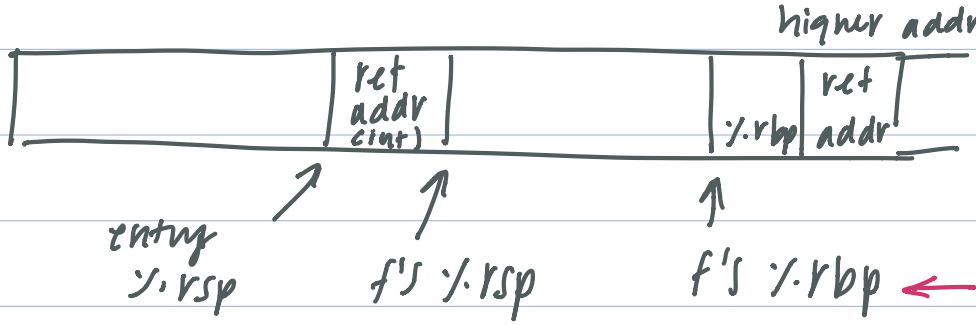
Review Session



entry seq
pushq y.rbp
pushq y.rsp, y.rbp

← callee-saved (call at beginning and save at end)

rsp is a multiple of 16 (stack frames are always aligned)

callq: decrease stack pointer by 8

sets instr. pointer to called address

retq: pops return addr off the stack
jumps to addr

Modification to local 6 can overwrite return addr

```
g(int x) {
  long buf[8]
~~ set buf to 0 ~~
buf[x] = ...
```

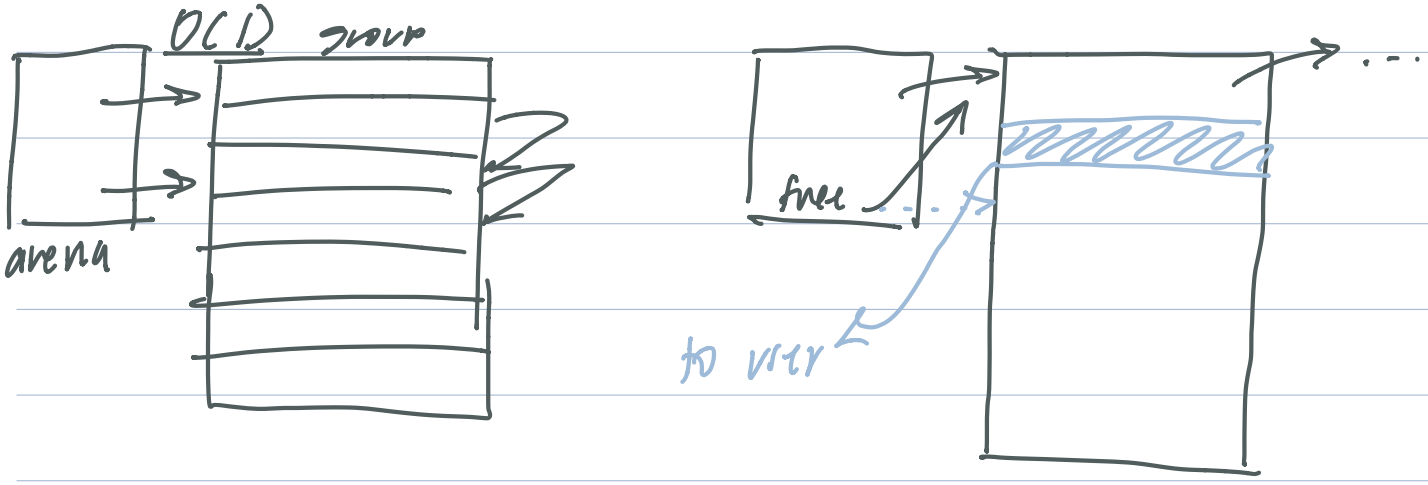
subq $0x40, %rsp

buf[8] = ... can overwrite the return address

* return addr + local variables must be mult. 16

leaf functions don't need to be 16-aligned

datarep 3 and arena allocator




```
g->nodes[0].key = 1024;
g->nodes[0].next = nullptr
a->frees = &g->nodes[0]

n= a->frees;
if (n->key >1) {
    n[1].key = n->key-1
    n[1].next =n->next
    a->frees = &n[1]
}
else {
    a->frees = n->next
}
```

Datarep-5

~ operation: 0→1 and 1→0