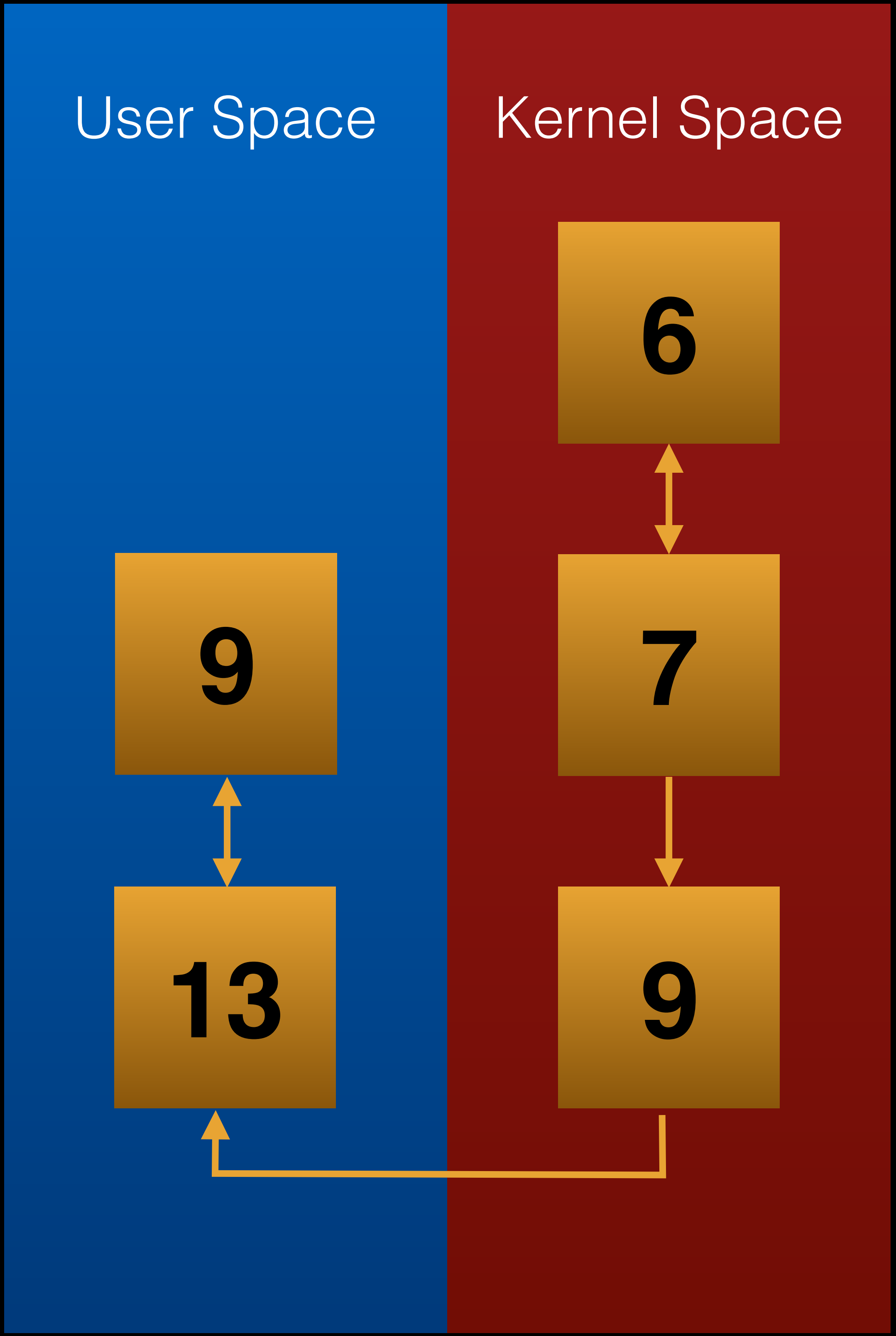
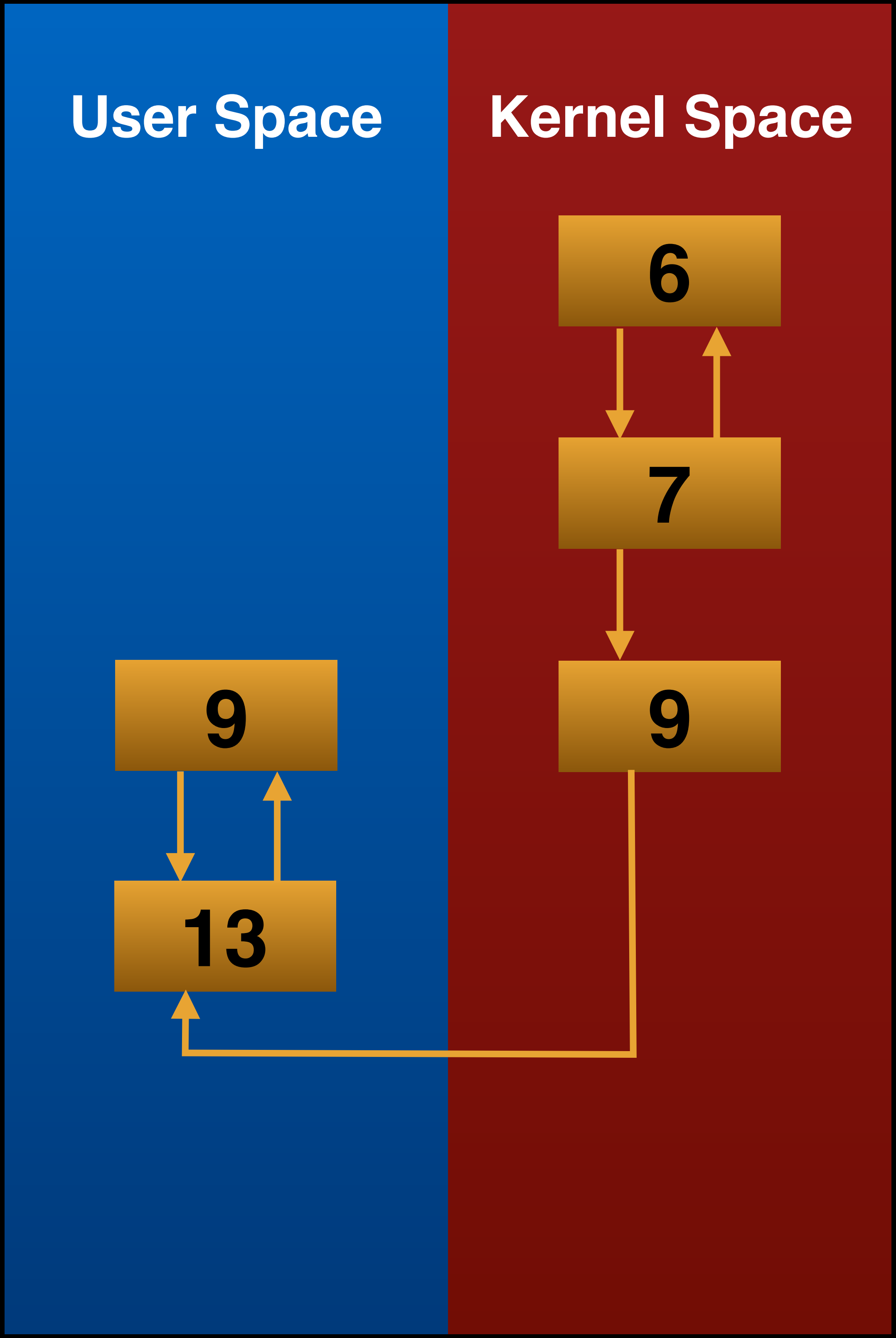
# TowelRoot

Tu Dang Nguyen, Chun-Yu Chuang

# Structure

- Thread 1
  - socket listener
- Thread 2
  - main thread, make rt_waiters
  - manage writing addr_limit
  - gaining root access
- Thread 3
  - make dangling waiter
  - sendmmsg()





User Space

Kernel Space

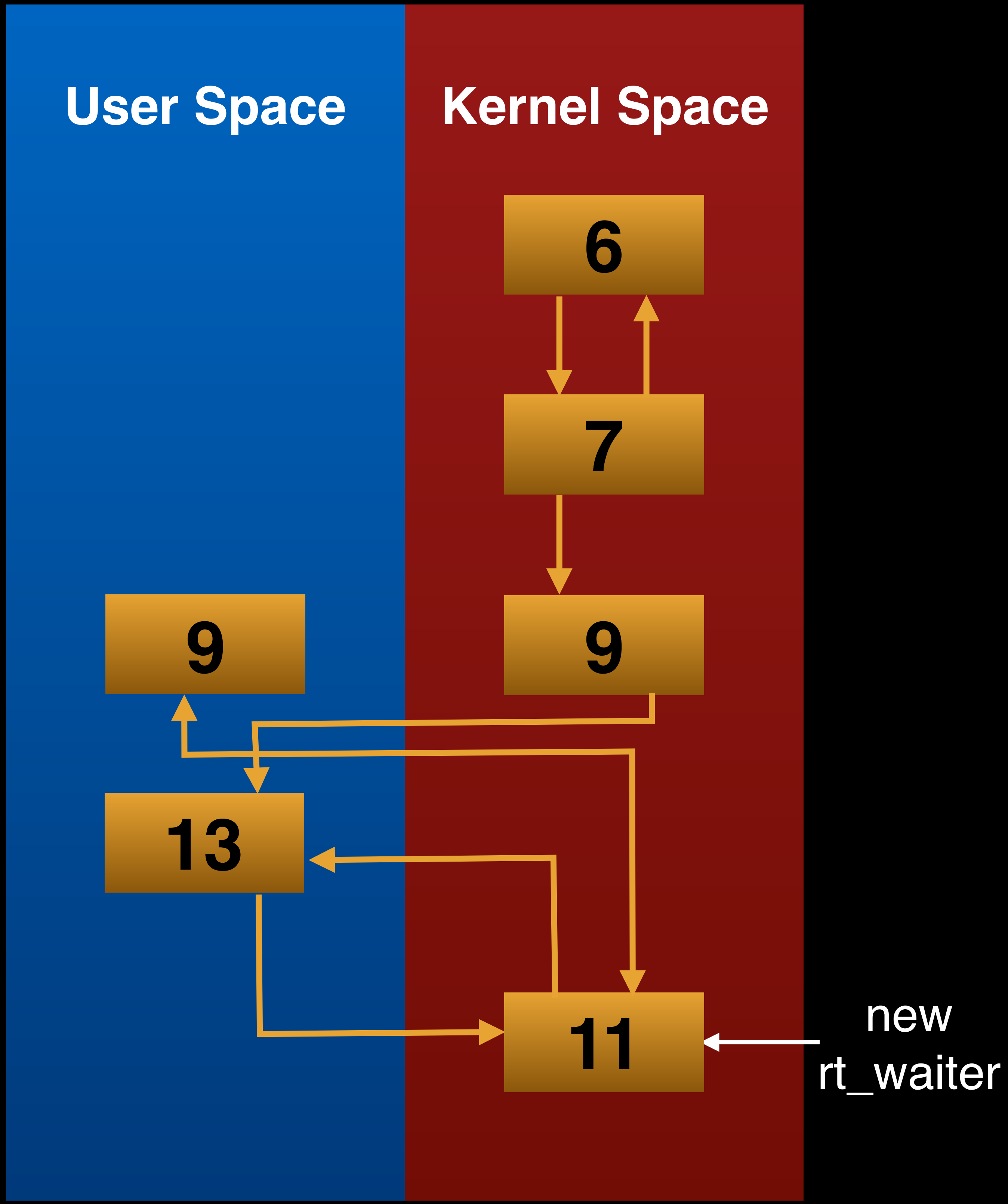
6

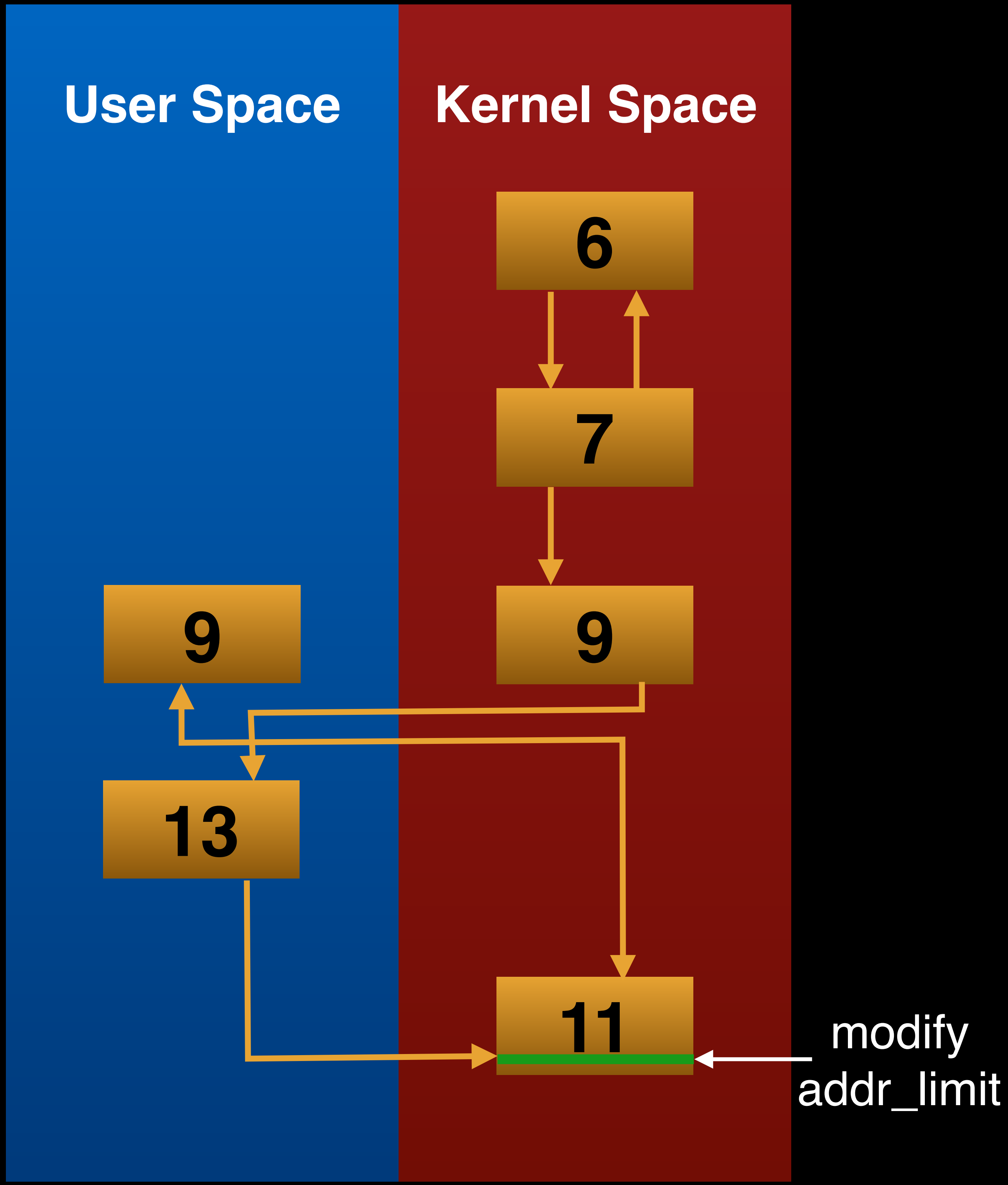
7

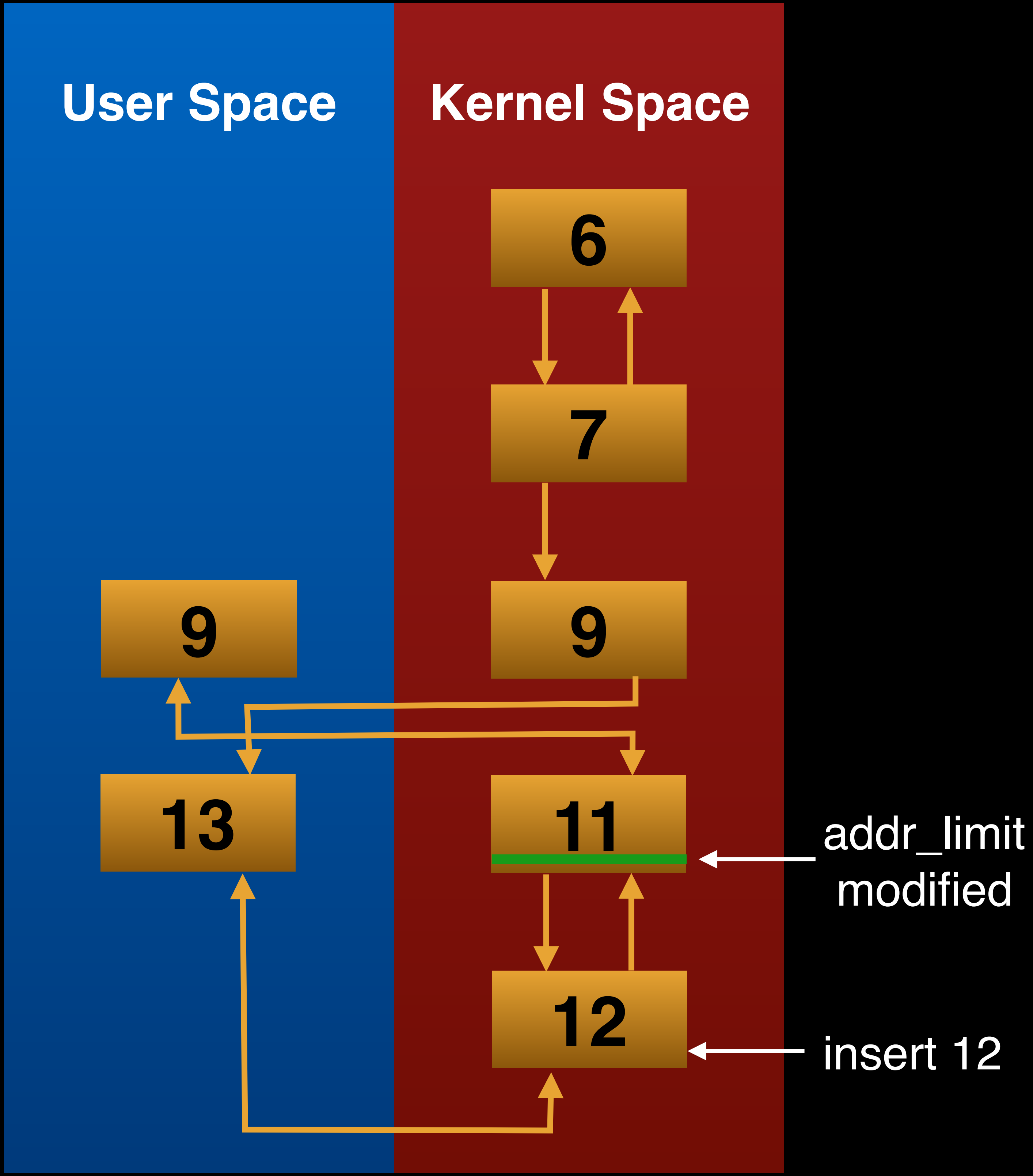
9

9

13

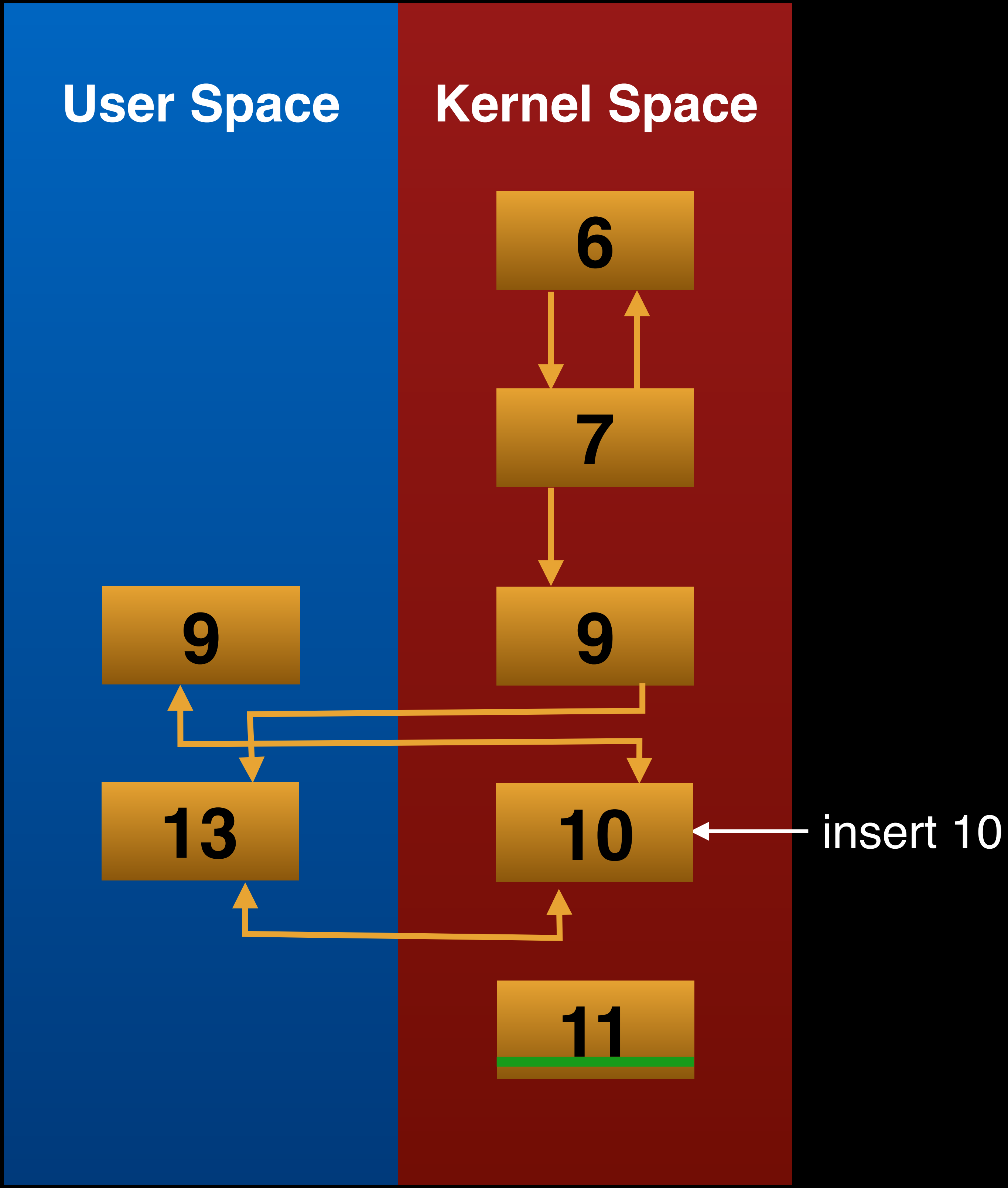

User Space
Kernel Space
6
7
9
9
13
11
new
rt_waiter


User Space
Kernel Space
6
7
9
9
13
11
modify
addr_limit



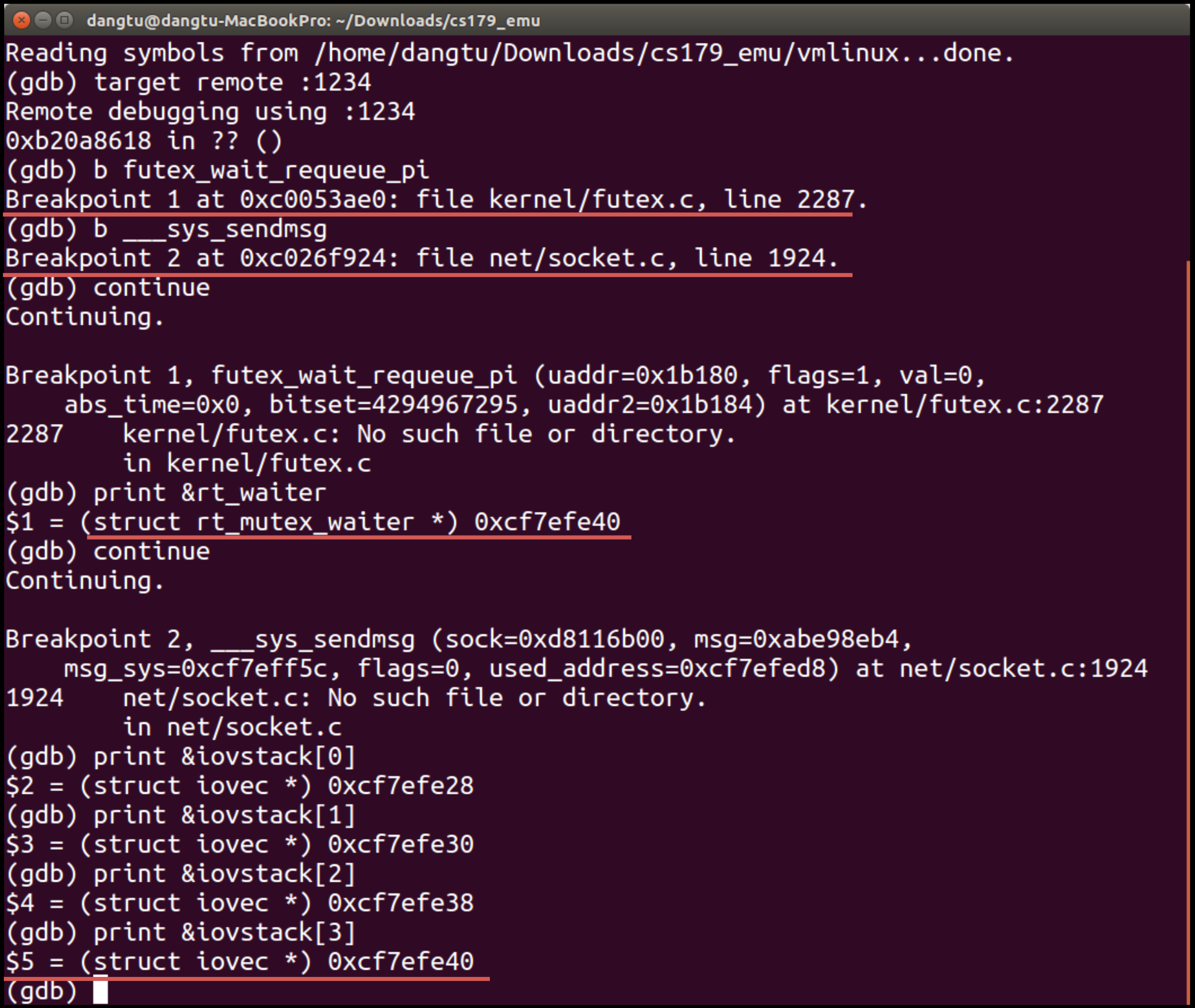
addr_limit modified

insert 12


User Space
Kernel Space
6
7
9
9
13
10
insert 10
11

# Address of rt_waiter

- breakpoints
  - futex_wait _requeue_pi()
  - __sys_sendmsg()
- address found
  - iovstack[3]



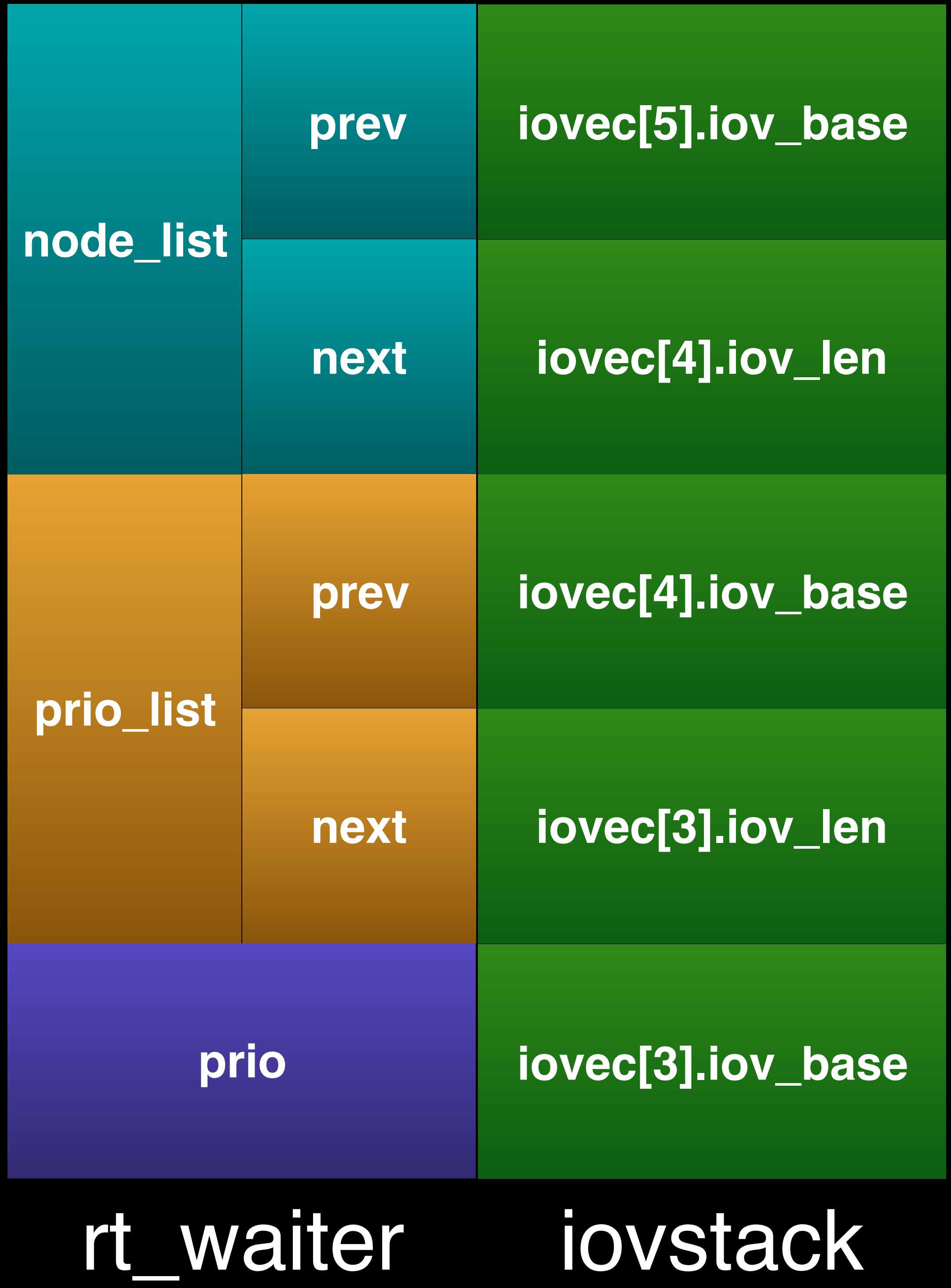
```
Reading symbols from /home/dangtu/Downloads/cs179_emu/vmlinux...done.
(gdb) target remote :1234
Remote debugging using :1234
0xb20a8618 in ?? ()
(gdb) b futex_wait_requeue_pi
Breakpoint 1 at 0xc0053ae0: file kernel/futex.c, line 2287.
(gdb) b ___sys_sendmsg
Breakpoint 2 at 0xc026f924: file net/socket.c, line 1924.
(gdb) continue
Continuing.

Breakpoint 1, futex_wait_requeue_pi (uaddr=0x1b180, flags=1, val=0,
    abs_time=0x0, bitset=4294967295, uaddr2=0x1b184) at kernel/futex.c:2287
2287    kernel/futex.c: No such file or directory.
        in kernel/futex.c
(gdb) print &rt_waiter
$1 = (struct rt_mutex_waiter *) 0xcf7efe40
(gdb) continue
Continuing.

Breakpoint 2, ___sys_sendmsg (sock=0xd8116b00, msg=0xabe98eb4,
    msg_sys=0xcf7eff5c, flags=0, used_address=0xcf7efed8) at net/socket.c:1924
1924    net/socket.c: No such file or directory.
        in net/socket.c
(gdb) print &iovstack[0]
$2 = (struct iovec *) 0xcf7efe28
(gdb) print &iovstack[1]
$3 = (struct iovec *) 0xcf7efe30
(gdb) print &iovstack[2]
$4 = (struct iovec *) 0xcf7efe38
(gdb) print &iovstack[3]
$5 = (struct iovec *) 0xcf7efe40
(gdb) 
```

# Data Alignment

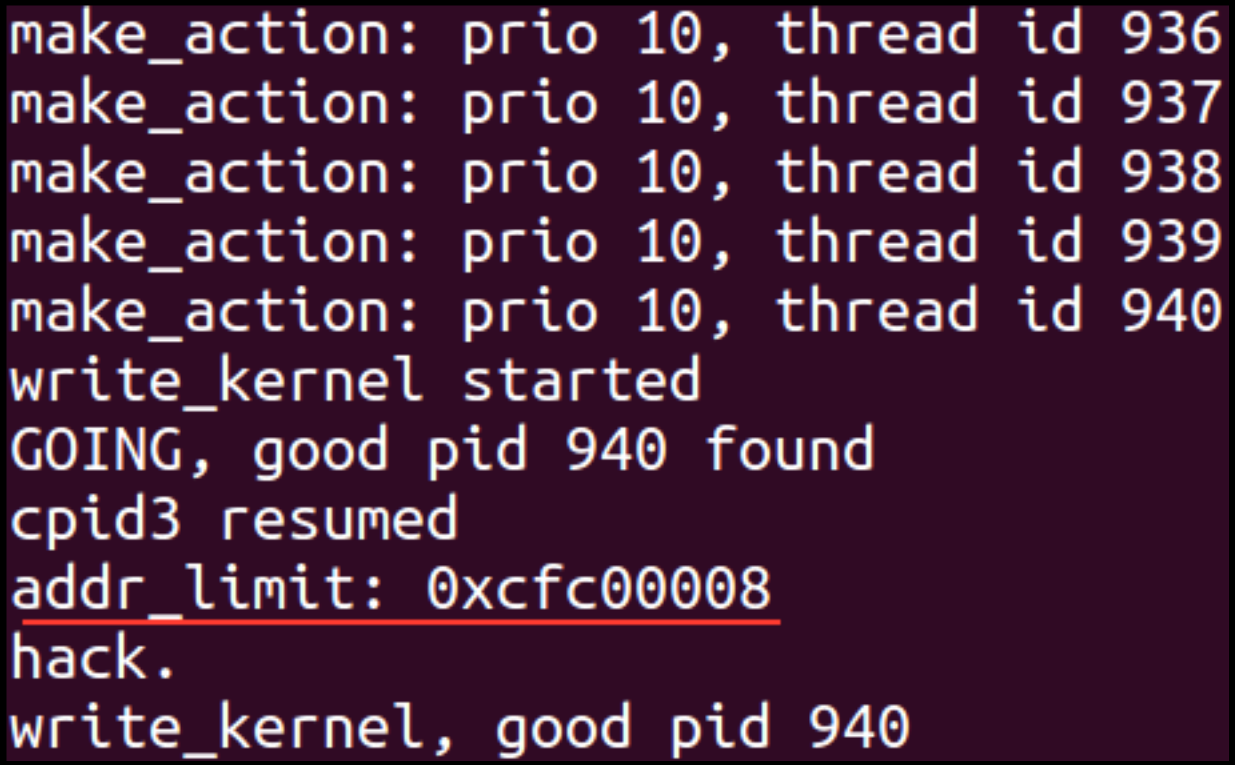
- iov_base is address
  - iovec[3].iov_base = (void *) val;
- iov_len is integer
  - iovec[3].iov_len = val;



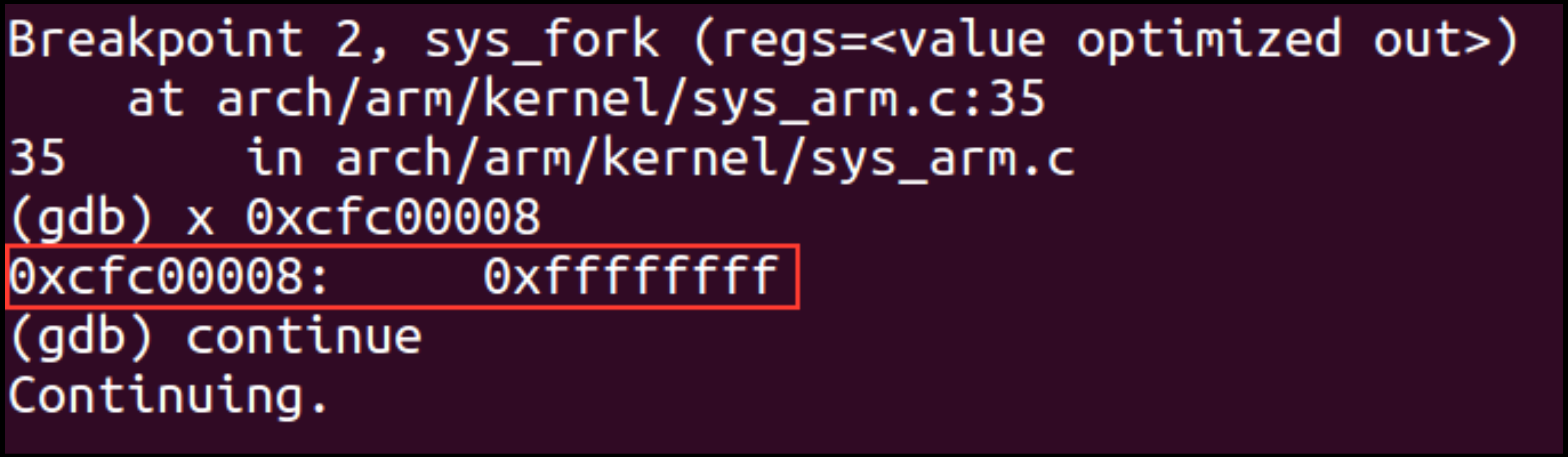
| | | |
|---|---|---|
| node_list | prev | iovec[5].iov_base |
| | next | iovec[4].iov_len |
| prio_list | prev | iovec[4].iov_base |
| | next | iovec[3].iov_len |
| prio | | iovec[3].iov_base |
| rt_waiter | | iovstack |

# Value in addr_limit

- addr_limit is in kernel space
  - no privilege to access
  - gdb can show the value



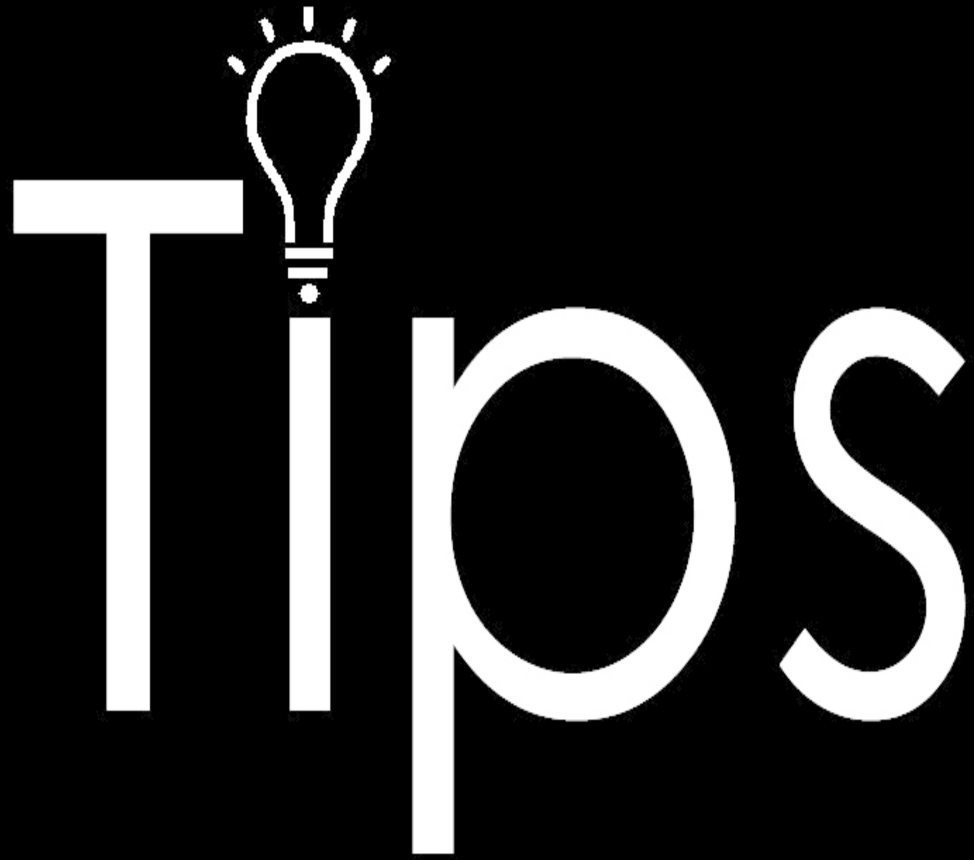
```
make_action: prio 10, thread id 936
make_action: prio 10, thread id 937
make_action: prio 10, thread id 938
make_action: prio 10, thread id 939
make_action: prio 10, thread id 940
write_kernel started
GOING, good pid 940 found
cpid3 resumed
addr_limit: 0xcfc00008
hack.
write_kernel, good pid 940
```



```
Breakpoint 2, sys_fork (regs=<value optimized out>)
    at arch/arm/kernel/sys_arm.c:35
35      in arch/arm/kernel/sys_arm.c
(gdb) x 0xcfc00008
0xcfc00008:     0xffffffff
(gdb) continue
Continuing.
```

# Q & A

- many printf() change behavior
    - using putchar() and puts()
- not stable gaining the root
    - modify the **pi_list** of rt_waiter
- slowly gaining the root
    - consume the kernel stack



# Reference

- http://blog.topsec.com.cn/ad_lab/cve2014-3153/
- https://github.com/timwr/CVE-2014-3153
- http://blog.idhyt.com/2016/02/26/exploit-cve-2014-3153/