Syed Ahmed Farrukh

ProblemSet2

Exercise 1

```
syedahmedfarrukh@Hydrasd

kernel/syscall.c
      126 [SYS_link]    sys_link,
      127 [SYS_mkdir]   sys_mkdir,
      128 [SYS_close]   sys_close,
      129 };
      130
      131 void
      132 syscall(void)
B+>   133 {
      134   int num;
      135   struct proc *p = myproc();
      136
      137   num = p->trapframe->a7;
      138   if(num > 0 && num < NELEM(syscalls) && syscalls[num]) {
      139     // Use num to lookup the system call function for num, call it,
      140     // and store its return value in p->trapframe->a0
      141     p->trapframe->a0 = syscalls[num]();
      142   } else {
remote Thread 1.2 (src) In: syscall                                  L133   PC: 0x80001cde
(gdb) backtrace
#0  syscall () at kernel/syscall.c:133
#1  0x0000000080001a9c in usertrap () at kernel/trap.c:68
#2  0x0000003ffffff09c in ?? ()
(gdb)
```

```
syedahmedfarrukh@Hydrasd

kernel/syscall.c
      126 [SYS_link]    sys_link,
      127 [SYS_mkdir]   sys_mkdir,
      128 [SYS_close]   sys_close,
      129 };
      130
      131 void
      132 syscall(void)
B+    133 {
      134   int num;
      135   struct proc *p = myproc();
      136
  >   137   num = p->trapframe->a7;
      138   if(num > 0 && num < NELEM(syscalls) && syscalls[num]) {
      139     // Use num to lookup the system call function for num, call it,
      140     // and store its return value in p->trapframe->a0
      141     p->trapframe->a0 = syscalls[num]();
      142   } else {
remote Thread 1.2 (src) In: syscall                                  L137   PC: 0x80001cf0
(gdb) n
(gdb) p /x *p
$1 = {lock = {locked = 0x0, name = 0x80007118, cpu = 0x0}, state = 0x4, chan = 0x0,
  killed = 0x0, xstate = 0x0, pid = 0x1, parent = 0x0, kstack = 0x3fffffd000, sz = 0x5000,
  pagetable = 0x87f52000, trapframe = 0x87f56000, context = {ra = 0x800012fc,
    sp = 0x3fffffdc50, s0 = 0x3fffffdc80, s1 = 0x80007cb0, s2 = 0x80007880, s3 = 0x0,
    s4 = 0x80012dc0, s5 = 0x3, s6 = 0x80018950, s7 = 0x0, s8 = 0x80018a78, s9 = 0x182,
    s10 = 0xb0, s11 = 0x2}, ofile = {0x0 <repeats 16 times>}, cwd = 0x80015dc0, name = {
    0x69, 0x6e, 0x69, 0x74, 0x0 <repeats 12 times>}}
(gdb)
```

```
syedahmedfarrukh@Hydrasd
kernel/syscall.c
      126 [SYS_link]    sys_link,
      127 [SYS_mkdir]   sys_mkdir,
      128 [SYS_close]   sys_close,
      129 };
      130
      131 void
      132 syscall(void)
B+    133 {
      134   int num;
      135   struct proc *p = myproc();
      136
  >   137   num = p->trapframe->a7;
      138   if(num > 0 && num < NELEM(syscalls) && syscalls[num]) {
      139     // Use num to lookup the system call function for num, call it,
      140     // and store its return value in p->trapframe->a0
      141     p->trapframe->a0 = syscalls[num]();
      142   } else {
remote Thread 1.2 (src) In: syscall                                          L
  pagetable = 0x87f52000, trapframe = 0x87f56000, context = {ra = 0x800012fc,
    sp = 0x3fffffdc50, s0 = 0x3fffffdc80, s1 = 0x80007cb0, s2 = 0x80007880, s3 = 0x0,
    s4 = 0x80012dc0, s5 = 0x3, s6 = 0x80018950, s7 = 0x0, s8 = 0x80018a78, s9 = 0x182,
    s10 = 0xb0, s11 = 0x2}, ofile = {0x0 <repeats 16 times>}, cwd = 0x80015dc0, name =
    0x69, 0x6e, 0x69, 0x74, 0x0 <repeats 12 times>}}
(gdb) p /x p->trapframe->a7
$2 = 0xf
(gdb) p /x $sstatus
$3 = 0x200000022
(gdb)
```

```
syedahmedfarrukh@Hydrasd
no-builtin-strchr -fno-builtin-exit -fno-builtin-malloc -fno-builtin
mcpy -Wno-main -fno-builtin-printf -fno-builtin-fprintf -fno-builtin
pie -no-pie  -c -o kernel/syscall.o kernel/syscall.c
riscv64-unknown-elf-ld -z max-page-size=4096 -T kernel/kernel.ld -o
loc.o kernel/string.o kernel/main.o kernel/vm.o kernel/proc.o kernel
p.o kernel/syscall.o kernel/sysproc.o kernel/bio.o kernel/fs.o kerne
o kernel/pipe.o kernel/exec.o kernel/sysfile.o kernel/kernelvec.o ke
/start.o kernel/console.o kernel/printf.o kernel/uart.o kernel/spinl
riscv64-unknown-elf-ld: warning: kernel/kernel has a LOAD segment wi
riscv64-unknown-elf-objdump -S kernel/kernel > kernel/kernel.asm
riscv64-unknown-elf-objdump -t kernel/kernel | sed '1,/SYMBOL TABLE/
m
mkfs/mkfs fs.img README user/findtest.sh user/sixfive.txt user/_cat
er/_init user/_kill user/_ln user/_ls user/_mkdir user/_rm user/_sh
ind user/_wc user/_zombie user/_logstress user/_forphan user/_dorpha
nmeta 47 (boot, super, log blocks 31, inode blocks 13, bitmap blocks
balloc: first 956 blocks have been allocated
balloc: write bitmap block at sector 46
qemu-system-riscv64 -machine virt -bios none -kernel kernel/kernel -
-mmio.force-legacy=false -drive file=fs.img,if=none,format=raw,id=x0
=virtio-mmio-bus.0

xv6 kernel is booting

hart 1 starting
hart 2 starting
scause=0xd sepc=0x80001cee stval=0x0
panic: kerneltrap
```

syedahmedfarrukh@Hydrasd

```
   0x80001cde <syscall>    addi    sp,sp,-32
   0x80001ce0 <syscall+2>  sd      ra,24(sp)
   0x80001ce2 <syscall+4>  sd      s0,16(sp)
   0x80001ce4 <syscall+6>  sd      s1,8(sp)
   0x80001ce6 <syscall+8>  addi    s0,sp,32
   0x80001ce8 <syscall+10> jal     0x80000d7a <myproc>
   0x80001cec <syscall+14> mv      s1,a0
B+>0x80001cee <syscall+16> lw      a3,0(zero) # 0x0
   0x80001cf2 <syscall+20> addiw   a4,a3,-1
   0x80001cf6 <syscall+24> li      a5,20
   0x80001cf8 <syscall+26> bltu    a5,a4,0x80001d16 <syscall+56>
   0x80001cfc <syscall+30> slli    a4,a3,0x3
   0x80001d00 <syscall+34> auipc   a5,0x6
   0x80001d04 <syscall+38> addi    a5,a5,-1448
   0x80001d08 <syscall+42> add     a5,a5,a4
   0x80001d0a <syscall+44> ld      a5,0(a5)
   0x80001d0c <syscall+46> beqz    a5,0x80001d16 <syscall+56>
   0x80001d0e <syscall+48> ld      s1,88(a0)
   0x80001d10 <syscall+50> jalr    a5
remote Thread 1.3 (asm) In: syscall
(gdb) c'
Not stopped at any breakpoint; argument ignored.
Continuing.
[Switching to Thread 1.3]

Thread 3 hit Breakpoint 1, syscall () at kernel/syscall.c:137
(gdb) p p->name
$1 = "init", '\000' <repeats 11 times>
(gdb) p p->pid
$2 = 1
(gdb)
```

syedahmedfarrukh@Hydrasd

```
loc.o kernel/string.o kernel/main.o kernel/vm.o kernel/proc.o kernel/swtch.o kernel/tra
p.o kernel/syscall.o kernel/sysproc.o kernel/bio.o kernel/fs.o kernel/log.o kernel/slee
o kernel/pipe.o kernel/exec.o kernel/sysfile.o kernel/kernelvec.o kernel/plic.o kernel/
/start.o kernel/console.o kernel/printf.o kernel/uart.o kernel/spinlock.o
riscv64-unknown-elf-ld: warning: kernel/kernel has a LOAD segment with RWX permissions
riscv64-unknown-elf-objdump -S kernel/kernel > kernel/kernel.asm
riscv64-unknown-elf-objdump -t kernel/kernel | sed '1,/SYMBOL TABLE/d; s/ .* / /; /^$/d
m
mkfs/mkfs fs.img README user/findtest.sh user/sixfive.txt user/_cat user/_echo user/_fo
er/_init user/_kill user/_ln user/_ls user/_mkdir user/_rm user/_sh user/_stressfs user
ind user/_wc user/_zombie user/_logstress user/_forphan user/_dorphan  user/_memdump
nmeta 47 (boot, super, log blocks 31, inode blocks 13, bitmap blocks 1) blocks 1953 tot
balloc: first 956 blocks have been allocated
balloc: write bitmap block at sector 46
qemu-system-riscv64 -machine virt -bios none -kernel kernel/kernel -m 128M -smp 3 -nogr
-mmio.force-legacy=false -drive file=fs.img,if=none,format=raw,id=x0 -device virtio-blk
=virtio-mmio-bus.0

xv6 kernel is booting

hart 1 starting
hart 2 starting
scause=0xd sepc=0x80001cee stval=0x0
panic: kerneltra
QEMU: Terminated
syedahmedfarrukh@Hydrasden:~/xv6lab_syedahmedfarrukh_28543$ nano kernel/kernel.asm
syedahmedfarrukh@Hydrasden:~/xv6lab_syedahmedfarrukh_28543$ grep 80001cee kernel/kernel
    8000[illegible]: 00002683                lw      a3,0(zero) # 0 <_entry-0x80000000>
syedahmedfarrukh@Hydrasden:~/xv6lab_syedahmedfarrukh_28543$
```

Exercise 2

```
syedahmedfarrukh@Hydrasd
riscv64-unknown-elf-ld -z max-page-size=4096 -T user/user.ld -o user/_sandbox user/sandbox.o user/ulib.o user/usys.o use
r/printf.o user/umalloc.o
riscv64-unknown-elf-objdump -S user/_sandbox > user/sandbox.asm
riscv64-unknown-elf-objdump -t user/_sandbox | sed '1,/SYMBOL TABLE/d; s/ .* / /; /^$/d' > user/sandbox.sym
riscv64-unknown-elf-gcc -Wall -Werror -O -fno-omit-frame-pointer -ggdb -gdwarf-2 -DSOL_UTIL -DLAB_UTIL -MD -mcmodel=meda
ny -ffreestanding -fno-common -nostdlib -fno-builtin-strncpy -fno-builtin-strncmp -fno-builtin-strlen -fno-builtin-memse
t -fno-builtin-memmove -fno-builtin-memcmp -fno-builtin-log -fno-builtin-bzero -fno-builtin-strchr -fno-builtin-exit -fn
o-builtin-malloc -fno-builtin-putc -fno-builtin-free -fno-builtin-memcpy -Wno-main -fno-builtin-printf -fno-builtin-fpri
ntf -fno-builtin-vprintf -I. -fno-stack-protector -fno-pie -no-pie   -c -o user/memdump.o user/memdump.c
riscv64-unknown-elf-ld -z max-page-size=4096 -T user/user.ld -o user/_memdump user/memdump.o user/ulib.o user/usys.o use
r/printf.o user/umalloc.o
riscv64-unknown-elf-objdump -S user/_memdump > user/memdump.asm
riscv64-unknown-elf-objdump -t user/_memdump | sed '1,/SYMBOL TABLE/d; s/ .* / /; /^$/d' > user/memdump.sym
mkfs/mkfs fs.img README user/findtest.sh user/sixfive.txt user/_cat user/_echo user/_forktest user/_grep user/_init user
/_kill user/_ln user/_ls user/_mkdir user/_rm user/_sh user/_stressfs user/_usertests user/_grind user/_wc user/_zombie
user/_logstress user/_forphan user/_dorphan user/_sandbox  user/_memdump
nmeta 47 (boot, super, log blocks 31, inode blocks 13, bitmap blocks 1) blocks 1953 total 2000
balloc: first 993 blocks have been allocated
balloc: write bitmap block at sector 46
qemu-system-riscv64 -machine virt -bios none -kernel kernel/kernel -m 128M -smp 3 -nographic -global virtio-mmio.force-l
egacy=false -drive file=fs.img,if=none,format=raw,id=x0 -device virtio-blk-device,drive=x0,bus=virtio-mmio-bus.0

xv6 kernel is booting

hart 2 starting
hart 1 starting
init: starting sh
$ sandbox 32768 - cat README
cat: cannot open README
$
```

```
syedahmedfarrukh@Hydrasd

qemu-system-riscv64 -machine virt -bios none -kernel kernel/kernel -m 128M -smp 3 -nographic -global virtio-mmio.force-legacy=false -drive file=fs.img,if=none,format=raw

xv6 kernel is booting

hart 1 starting
hart 2 starting
init: starting sh
$ ls
.              1 1 1024
..             1 1 1024
README         2 2 2425
findtest.sh    2 3 91
sixfive.txt    2 4 19
cat            2 5 36584
echo           2 6 35440
forktest       2 7 17160
grep           2 8 40824
init           2 9 35896
kill           2 10 35360
ln             2 11 35176
ls             2 12 38720
mkdir          2 13 35424
rm             2 14 35408
sh             2 15 58424
stressfs       2 16 36296
usertests      2 17 186328
grind          2 18 51824
wc             2 19 37576
zombie         2 20 34760
logstress      2 21 37360
forphan        2 22 36184
dorphan        2 23 35632
sandbox        2 24 35496
memdump        2 25 36800
console        3 26 0
$ cat README
xv6 is a re-implementation of Dennis Ritchie's and Ken Thompson's Unix
Version 6 (v6).  xv6 loosely follows the structure and style of v6,
but is implemented for a modern RISC-V multiprocessor using ANSI C.

ACKNOWLEDGMENTS

xv6 is inspired by John Lions's Commentary on UNIX 6th Edition (Peer
to Peer Communications; ISBN: 1-57398-013-7; 1st edition (June 14,
2000)).  See also https://pdos.csail.mit.edu/6.1810/, which provides
pointers to on-line resources for v6.

The following people have made contributions: Russ Cox (context switching,
locking), Cliff Frey (MP), Xiao Yu (MP), Nickolai Zeldovich, and Austin
Clements.

We are also grateful for the bug reports and patches contributed by
Abhinavpatel00, Takahiro Aoyagi, Marcelo Arroyo, Hirbod Behnam, Silas
Boyd-Wickizer, Anton Burtsev, carlclone, Ian Chen, clivezeng, Dan
Cross, Cody Cutler, Mike CAT, Tej Chajed, Asami Doi,Wenyang Duan,
echtwerner, eyalz800, Nelson Elhage, Saar Ettinger, Alice Ferrazzi,
Nathaniel Filardo, flespark, Peter Froehlich, Yakir Goaron, Shivam
Handa, Matt Harvey, Bryan Henry, jaichenhengjie, Jim Huang, Matúš
```

```
syedahmedfarrukh@Hydrasd
riscv64-unknown-elf-gcc -Wall -Werror -O -fno-omit-frame-pointer -ggdb -gdwarf-2 -DSOL_UTIL -DLAB_UTIL -MD -mcmodel=meda
ny -ffreestanding -fno-common -nostdlib -fno-builtin-strncpy -fno-builtin-strncmp -fno-builtin-strlen -fno-builtin-memse
t -fno-builtin-memmove -fno-builtin-memcmp -fno-builtin-log -fno-builtin-bzero -fno-builtin-strchr -fno-builtin-exit -fn
o-builtin-malloc -fno-builtin-putc -fno-builtin-free -fno-builtin-memcpy -Wno-main -fno-builtin-printf -fno-builtin-fpri
ntf -fno-builtin-vprintf -I. -fno-stack-protector -fno-pie -no-pie   -c -o user/memdump.o user/memdump.c
riscv64-unknown-elf-ld -z max-page-size=4096 -T user/user.ld -o user/_memdump user/memdump.o user/ulib.o user/usys.o use
r/printf.o user/umalloc.o
riscv64-unknown-elf-objdump -S user/_memdump > user/memdump.asm
riscv64-unknown-elf-objdump -t user/_memdump | sed '1,/SYMBOL TABLE/d; s/ .* / /; /^$/d' > user/memdump.sym
mkfs/mkfs fs.img README user/findtest.sh user/sixfive.txt user/_cat user/_echo user/_forktest user/_grep user/_init user
/_kill user/_ln user/_ls user/_mkdir user/_rm user/_sh user/_stressfs user/_usertests user/_grind user/_wc user/_zombie
user/_logstress user/_forphan user/_dorphan user/_sandbox  user/_memdump
nmeta 47 (boot, super, log blocks 31, inode blocks 13, bitmap blocks 1) blocks 1953 total 2000
balloc: first 993 blocks have been allocated
balloc: write bitmap block at sector 46
qemu-system-riscv64 -machine virt -bios none -kernel kernel/kernel -m 128M -smp 3 -nographic -global virtio-mmio.force-l
egacy=false -drive file=fs.img,if=none,format=raw,id=x0 -device virtio-blk-device,drive=x0,bus=virtio-mmio-bus.0

xv6 kernel is booting

hart 1 starting
hart 2 starting
init: starting sh
$ sandbox 32768 - cat README
cat: cannot open README
$ QEMU: Terminated
syedahmedfarrukh@Hydrasden:~/xv6lab_syedahmedfarrukh_28543$ ./grade-lab-syscall sandbox_mask
```

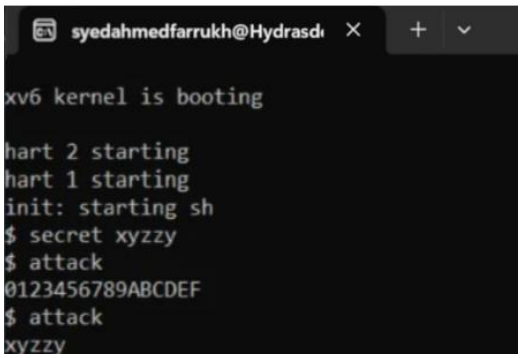
Exercise 3

```
syedahmedfarrukh@Hydrasd

riscv64-unknown-elf-objdump -t user/_sandbox | sed '1,/SYMBOL TABLE/d; s/ .* / /; /^
riscv64-unknown-elf-gcc -Wall -Werror -O -fno-omit-frame-pointer -ggdb -gdwarf-2 -DS
ny -ffreestanding -fno-common -nostdlib -fno-builtin-strncpy -fno-builtin-strncmp -f
t -fno-builtin-memmove -fno-builtin-memcmp -fno-builtin-log -fno-builtin-bzero -fno-
o-builtin-malloc -fno-builtin-putc -fno-builtin-free -fno-builtin-memcpy -Wno-main -
ntf -fno-builtin-vprintf -I. -fno-stack-protector -fno-pie -no-pie   -c -o user/memd
riscv64-unknown-elf-ld -z max-page-size=4096 -T user/user.ld -o user/_memdump user/m
r/printf.o user/umalloc.o
riscv64-unknown-elf-objdump -S user/_memdump > user/memdump.asm
riscv64-unknown-elf-objdump -t user/_memdump | sed '1,/SYMBOL TABLE/d; s/ .* / /; /^
mkfs/mkfs fs.img README user/findtest.sh user/sixfive.txt user/_cat user/_echo user/
/_kill user/_ln user/_ls user/_mkdir user/_rm user/_sh user/_stressfs user/_usertest
user/_logstress user/_forphan user/_dorphan user/_sandbox  user/_memdump
nmeta 47 (boot, super, log blocks 31, inode blocks 13, bitmap blocks 1) blocks 1953
balloc: first 993 blocks have been allocated
balloc: write bitmap block at sector 46
qemu-system-riscv64 -machine virt -bios none -kernel kernel/kernel -m 128M -smp 3 -n
egacy=false -drive file=fs.img,if=none,format=raw,id=x0 -device virtio-blk-device,dr

xv6 kernel is booting

hart 2 starting
hart 1 starting
init: starting sh
$ sandbox 32768 README grep xv6 README
xv6 is a re-implementation of Dennis Ritchie's and Ken Thompson's Unix
Version 6 (v6).  xv6 loosely follows the structure and style of v6,
xv6 is inspired by John Lions's Commentary on UNIX 6th Edition (Peer
(kaashoek,rtm@mit.edu).  The main purpose of xv6 is as a teaching
```

MAKE GRADE

```
syedahmedfarrukh@Hydrasd
== Test answers-syscall.txt ==
answers-syscall.txt: OK
== Test sandbox_mask ==
$ make qemu-gdb
sandbox_mask: OK (7.3s)
== Test sandbox_fork ==
$ make qemu-gdb
sandbox_fork: OK (1.0s)
== Test sandbox_path ==
$ make qemu-gdb
sandbox_path: OK (2.0s)
== Test sandbox_most ==
$ make qemu-gdb
sandbox_most: OK (0.7s)
== Test sandbox_minus ==
$ make qemu-gdb
sandbox_minus: OK (0.8s)
== Test attack ==
$ make qemu-gdb
attack: OK (0.7s)
== Test time ==
time: OK
Score: 45/45
syedahmedfarrukh@Hydrasden:~/xv6lab_syedahmedfarrukh
```

Exercise 4


syedahmedfarrukh@Hydrasd
xv6 kernel is booting
hart 2 starting
hart 1 starting
init: starting sh
$ secret xyzzy
$ attack
0123456789ABCDEF
$ attack
xyzzy