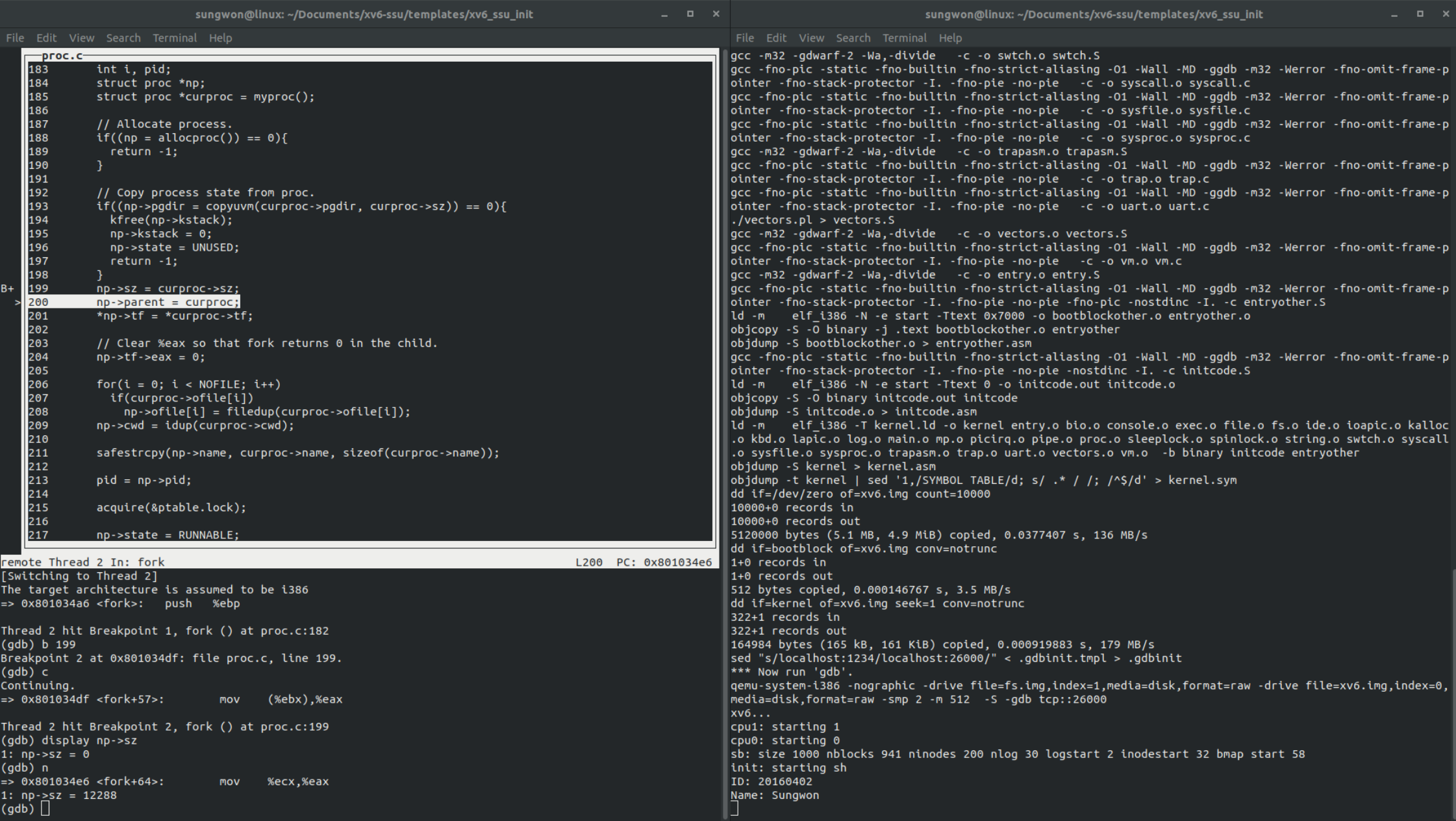
sungwon@linux: ~/Documents/xv6-ssu/templates/xv6_ssu_init
File Edit View Search Terminal Help
proc.c
183 int i, pid;
184 struct proc *np;
185 struct proc *curproc = myproc();
186
187 // Allocate process.
188 if((np = allocproc()) == 0){
189 return -1;
190 }
191
192 // Copy process state from proc.
193 if((np->pgdir = copyuvm(curproc->pgdir, curproc->sz)) == 0){
194 kfree(np->kstack);
195 np->kstack = 0;
196 np->state = UNUSED;
197 return -1;
198 }
B+ 199 np->sz = curproc->sz;
> 200 np->parent = curproc;
201 *np->tf = *curproc->tf;
202
203 // Clear %eax so that fork returns 0 in the child.
204 np->tf->eax = 0;
205
206 for(i = 0; i < NOFILE; i++)
207 if(curproc->ofile[i])
208 np->ofile[i] = filedup(curproc->ofile[i]);
209 np->cwd = idup(curproc->cwd);
210
211 safestrcpy(np->name, curproc->name, sizeof(curproc->name));
212
213 pid = np->pid;
214
215 acquire(&ptable.lock);
216
217 np->state = RUNNABLE;
remote Thread 2 In: fork L200 PC: 0x801034e6
[Switching to Thread 2]
The target architecture is assumed to be i386
=> 0x801034a6 <fork>: push %ebp
Thread 2 hit Breakpoint 1, fork () at proc.c:182
(gdb) b 199
Breakpoint 2 at 0x801034df: file proc.c, line 199.
(gdb) c
Continuing.
=> 0x801034df <fork+57>: mov (%ebx),%eax
Thread 2 hit Breakpoint 2, fork () at proc.c:199
(gdb) display np->sz
1: np->sz = 0
(gdb) n
=> 0x801034e6 <fork+64>: mov %ecx,%eax
1: np->sz = 12288
(gdb)
sungwon@linux: ~/Documents/xv6-ssu/templates/xv6_ssu_init
File Edit View Search Terminal Help
gcc -m32 -gdwarf-2 -Wa,-divide -c -o swtch.o swtch.S
gcc -fno-pic -static -fno-builtin -fno-strict-aliasing -O1 -Wall -MD -ggdb -m32 -Werror -fno-omit-frame-pointer -fno-stack-protector -I. -fno-pie -no-pie -c -o syscall.o syscall.c
gcc -fno-pic -static -fno-builtin -fno-strict-aliasing -O1 -Wall -MD -ggdb -m32 -Werror -fno-omit-frame-pointer -fno-stack-protector -I. -fno-pie -no-pie -c -o sysfile.o sysfile.c
gcc -fno-pic -static -fno-builtin -fno-strict-aliasing -O1 -Wall -MD -ggdb -m32 -Werror -fno-omit-frame-pointer -fno-stack-protector -I. -fno-pie -no-pie -c -o sysproc.o sysproc.c
gcc -m32 -gdwarf-2 -Wa,-divide -c -o trapasm.o trapasm.S
gcc -fno-pic -static -fno-builtin -fno-strict-aliasing -O1 -Wall -MD -ggdb -m32 -Werror -fno-omit-frame-pointer -fno-stack-protector -I. -fno-pie -no-pie -c -o trap.o trap.c
gcc -fno-pic -static -fno-builtin -fno-strict-aliasing -O1 -Wall -MD -ggdb -m32 -Werror -fno-omit-frame-pointer -fno-stack-protector -I. -fno-pie -no-pie -c -o uart.o uart.c
./vectors.pl > vectors.S
gcc -m32 -gdwarf-2 -Wa,-divide -c -o vectors.o vectors.S
gcc -fno-pic -static -fno-builtin -fno-strict-aliasing -O1 -Wall -MD -ggdb -m32 -Werror -fno-omit-frame-pointer -fno-stack-protector -I. -fno-pie -no-pie -c -o vm.o vm.c
gcc -m32 -gdwarf-2 -Wa,-divide -c -o entry.o entry.S
gcc -fno-pic -static -fno-builtin -fno-strict-aliasing -O1 -Wall -MD -ggdb -m32 -Werror -fno-omit-frame-pointer -fno-stack-protector -I. -fno-pie -no-pie -fno-pic -nostdinc -I. -c entryother.S
ld -m elf_i386 -N -e start -Ttext 0x7000 -o bootblockother.o entryother.o
objcopy -S -O binary -j .text bootblockother.o entryother
objdump -S bootblockother.o > entryother.asm
gcc -fno-pic -static -fno-builtin -fno-strict-aliasing -O1 -Wall -MD -ggdb -m32 -Werror -fno-omit-frame-pointer -fno-stack-protector -I. -fno-pie -no-pie -nostdinc -I. -c initcode.S
ld -m elf_i386 -N -e start -Ttext 0 -o initcode.out initcode.o
objcopy -S -O binary initcode.out initcode
objdump -S initcode.o > initcode.asm
ld -m elf_i386 -T kernel.ld -o kernel entry.o bio.o console.o exec.o file.o fs.o ide.o ioapic.o kalloc.o kbd.o lapic.o log.o main.o mp.o picirq.o pipe.o proc.o sleeplock.o spinlock.o string.o swtch.o syscall.o sysfile.o sysproc.o trapasm.o trap.o uart.o vectors.o vm.o -b binary initcode entryother
objdump -S kernel > kernel.asm
objdump -t kernel | sed '1,/SYMBOL TABLE/d; s/ .* / /; /^$/d' > kernel.sym
dd if=/dev/zero of=xv6.img count=10000
10000+0 records in
10000+0 records out
5120000 bytes (5.1 MB, 4.9 MiB) copied, 0.0377407 s, 136 MB/s
dd if=bootblock of=xv6.img conv=notrunc
1+0 records in
1+0 records out
512 bytes copied, 0.000146767 s, 3.5 MB/s
dd if=kernel of=xv6.img seek=1 conv=notrunc
322+1 records in
322+1 records out
164984 bytes (165 kB, 161 KiB) copied, 0.000919883 s, 179 MB/s
sed "s/localhost:1234/localhost:26000/" < .gdbinit.tmpl > .gdbinit
*** Now run 'gdb'.
qemu-system-i386 -nographic -drive file=fs.img,index=1,media=disk,format=raw -drive file=xv6.img,index=0,media=disk,format=raw -smp 2 -m 512 -S -gdb tcp::26000
xv6...
cpu1: starting 1
cpu0: starting 0
sb: size 1000 nblocks 941 ninodes 200 nlog 30 logstart 2 inodestart 32 bmap start 58
init: starting sh
ID: 20160402
Name: Sungwon