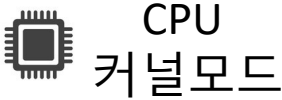


과제1. 시스템 콜 과정 이해하기



사용자 뿐만 아니라 커널 영역 메모리도 접근 가능

IDT(Interrupt Descriptor Table)

4.시스템 콜 테이블에서 실제 처리하는 sys_read 호출 (포인터 역할)

```
# The format is:
# <number> <abi> <name> <entry point>
#
# The abi is "common", "64" or "x32" for this file.
#
0 common read sys_read
1 common write sys_write
2 common open sys_open
```

```
50 #define IA32_SYSCALL_VECTOR 0x80
51
```

```
101 #if defined(CONFIG_IA32_EMULATION)
102     SYSG(IA32_SYSCALL_VECTOR, entry_INT80_compat),
103 #elif defined(CONFIG_X86_32)
104     SYSG(IA32_SYSCALL_VECTOR, entry_INT80_32),
105 #endif
```

6. 0x80이 발생하면 entry_INT80 관련 내용을 수행해라

7. 엔트리에는 인터럽트에 따라 처리할 일이 어셈블리 언어로 작성되어 있음 (eax system call number 확인하기, 여기서 0번)

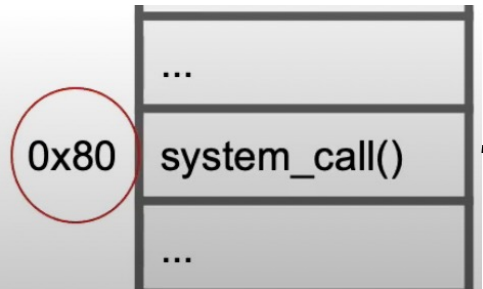
```
0 common read sys_read
```

9. 헤더 확인(선언된 함수) ./include/linux/syscalls.h

```
598 asmlinkage long sys_read(unsigned int fd, char __user *buf, size_t count);
599 asmlinkage long sys_readahead(int fd, loff_t offset, size_t count);
600 asmlinkage long sys_readv(unsigned long fd, struct iovec __user *iov, int iovcnt);
```



3. 128번 인터럽트 발생 (시스템콜 호출)



5. 리눅스 소스코드 확인

./arch/x86/include/linux/asm/irq_vectors.h

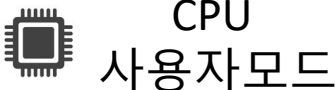
```
* Arguments:
* eax system call number
* ebx arg1
* ecx arg2
* edx arg3
* esi arg4
* edi arg5
* ebp user stack
* 0(%ebp) arg6
*/
```

```
main() 1.c언어로 작성된 프로그램 호출
{
    read()
}
```

```
read() (0을 %eax에 전달, sys_read의 고유번호)
{
    movl 0, %eax
    int $0x80
}
```

2.시스템 콜 호출 전, GNU C Library 에서 함수 호출

```
$ ldd --version
ldd (Ubuntu GLIBC 2.31-0ubuntu9.2) 2.31
Copyright (C) 2020 Free Software Foundation, Inc.
이 프로그램은 자유 소프트웨어입니다. 복사조건은 소스를 참조하십시오.
상품성이나 특정 목적에 대한 적합성을 비롯하여 어떠한 보증도 하지 않습니다.
만든 사람: Roland McGrath 및 Ulrich Drepper.
```



사용자 영역 메모리에만 접근 가능

과제2. 시스템 콜 실습

과제2-1. 새로운 시스템 콜 추가하기

(정답은 마지막 장에 2-2 정답과 함께 표기)

1. 시스템콜번호할당

2. 시스템콜함수구현

파일	머신	보기	입력	장치	도움말
317	common	seccomp	sys_seccomp		
318	common	getrandom	sys_getrandom		
319	common	memfd_create	sys_memfd_create		
320	common	kexec_file_load	sys_kexec_file_load		
321	common	bpf	sys_bpf		
322	64	execveat	sys_execveat/ptregs		
323	common	userfaultfd	sys_userfaultfd		
324	common	membarrier	sys_membarrier		
325	common	mlock2	sys_mlock2		
326	common	copy_file_range	sys_copy_file_range		
327	64	preadv2	sys_preadv2		
328	64	pwritev2	sys_pwritev2		
329	common	pkey_mprotect	sys_pkey_mprotect		
330	common	pkey_alloc	sys_pkey_alloc		
331	common	pkey_free	sys_pkey_free		
332	common	statx	sys_statx		
333	common	print_student_id	sys_print_student_id		
334	common	print_student_info	sys_print_student_info		
#					
# x32-specific system call numbers start at 512 to avoid cache impact					
# for native 64-bit operation.					
#					
512	x32	rt_sigaction	compat_sys_rt_sigaction		
513	x32	rt_sigreturn	sys32_x32_rt_sigreturn		
514	x32	ioctl	compat_sys_ioctl		
515	x32	readv	compat_sys_readv		
516	x32	writev	compat_sys_writev		
517	x32	recvfrom	compat_sys_recvfrom		
518	x32	sendmsg	compat_sys_sendmsg		
519	x32	recvmsg	compat_sys_recvmsg		
520	x32	execve	compat_sys_execve/ptregs		
521	x32	ptrace	compat_sys_ptrace		
522	x32	rt_sigpending	compat_sys_rt_sigpending		
523	x32	rt_sigtimedwait	compat_sys_rt_sigtimedwait		
524	x32	rt_sigqueueinfo	compat_sys_rt_sigqueueinfo		
525	x32	rt_sigprocmask	compat_sys_rt_sigprocmask		
526	x32	clock_gettime	compat_sys_clock_gettime		
527	x32	clock_getres	compat_sys_clock_getres		
528	x32	clock_nanosleep	compat_sys_clock_nanosleep		
529	x32	timer_create	compat_sys_timer_create		
530	x32	timer_delete	compat_sys_timer_delete		
531	x32	timer_getoverrun	compat_sys_timer_getoverrun		
532	x32	timer_settime	compat_sys_timer_settime		
533	x32	timerfd_create	compat_sys_timerfd_create		
534	x32	timerfd_gettime	compat_sys_timerfd_gettime		
535	x32	timerfd_settime	compat_sys_timerfd_settime		
536	x32	eventfd	compat_sys_eventfd		
537	x32	eventfd_read	compat_sys_eventfd_read		
538	x32	eventfd_write	compat_sys_eventfd_write		
539	x32	epoll_create	compat_sys_epoll_create		
540	x32	epoll_create1	compat_sys_epoll_create1		
541	x32	epoll_ctl	compat_sys_epoll_ctl		
542	x32	epoll_ctl_old	compat_sys_epoll_ctl_old		
543	x32	epoll_wait	compat_sys_epoll_wait		
544	x32	epoll_wait_old	compat_sys_epoll_wait_old		
545	x32	close_range	compat_sys_close_range		
546	x32	openat2	compat_sys_openat2		
547	x32	openat2_old	compat_sys_openat2_old		
548	x32	openat2_new	compat_sys_openat2_new		
549	x32	openat2_new2	compat_sys_openat2_new2		
550	x32	openat2_new3	compat_sys_openat2_new3		
551	x32	openat2_new4	compat_sys_openat2_new4		
552	x32	openat2_new5	compat_sys_openat2_new5		
553	x32	openat2_new6	compat_sys_openat2_new6		
554	x32	openat2_new7	compat_sys_openat2_new7		
555	x32	openat2_new8	compat_sys_openat2_new8		
556	x32	openat2_new9	compat_sys_openat2_new9		
557	x32	openat2_new10	compat_sys_openat2_new10		
558	x32	openat2_new11	compat_sys_openat2_new11		
559	x32	openat2_new12	compat_sys_openat2_new12		
560	x32	openat2_new13	compat_sys_openat2_new13		
561	x32	openat2_new14	compat_sys_openat2_new14		
562	x32	openat2_new15	compat_sys_openat2_new15		
563	x32	openat2_new16	compat_sys_openat2_new16		
564	x32	openat2_new17	compat_sys_openat2_new17		
565	x32	openat2_new18	compat_sys_openat2_new18		
566	x32	openat2_new19	compat_sys_openat2_new19		
567	x32	openat2_new20	compat_sys_openat2_new20		
568	x32	openat2_new21	compat_sys_openat2_new21		
569	x32	openat2_new22	compat_sys_openat2_new22		
570	x32	openat2_new23	compat_sys_openat2_new23		
571	x32	openat2_new24	compat_sys_openat2_new24		
572	x32	openat2_new25	compat_sys_openat2_new25		
573	x32	openat2_new26	compat_sys_openat2_new26		
574	x32	openat2_new27	compat_sys_openat2_new27		
575	x32	openat2_new28	compat_sys_openat2_new28		
576	x32	openat2_new29	compat_sys_openat2_new29		
577	x32	openat2_new30	compat_sys_openat2_new30		
578	x32	openat2_new31	compat_sys_openat2_new31		
579	x32	openat2_new32	compat_sys_openat2_new32		
580	x32	openat2_new33	compat_sys_openat2_new33		
581	x32	openat2_new34	compat_sys_openat2_new34		
582	x32	openat2_new35	compat_sys_openat2_new35		
583	x32	openat2_new36	compat_sys_openat2_new36		
584	x32	openat2_new37	compat_sys_openat2_new37		
585	x32	openat2_new38	compat_sys_openat2_new38		
586	x32	openat2_new39	compat_sys_openat2_new39		
587	x32	openat2_new40	compat_sys_openat2_new40		
588	x32	openat2_new41	compat_sys_openat2_new41		
589	x32	openat2_new42	compat_sys_openat2_new42		
590	x32	openat2_new43	compat_sys_openat2_new43		
591	x32	openat2_new44	compat_sys_openat2_new44		
592	x32	openat2_new45	compat_sys_openat2_new45		
593	x32	openat2_new46	compat_sys_openat2_new46		
594	x32	openat2_new47	compat_sys_openat2_new47		
595	x32	openat2_new48	compat_sys_openat2_new48		
596	x32	openat2_new49	compat_sys_openat2_new49		
597	x32	openat2_new50	compat_sys_openat2_new50		
598	x32	openat2_new51	compat_sys_openat2_new51		
599	x32	openat2_new52	compat_sys_openat2_new52		
600	x32	openat2_new53	compat_sys_openat2_new53		
601	x32	openat2_new54	compat_sys_openat2_new54		
602	x32	openat2_new55	compat_sys_openat2_new55		
603	x32	openat2_new56	compat_sys_openat2_new56		
604	x32	openat2_new57	compat_sys_openat2_new57		
605	x32	openat2_new58	compat_sys_openat2_new58		
606	x32	openat2_new59	compat_sys_openat2_new59		
607	x32	openat2_new60	compat_sys_openat2_new60		
608	x32	openat2_new61	compat_sys_openat2_new61		
609	x32	openat2_new62	compat_sys_openat2_new62		
610	x32	openat2_new63	compat_sys_openat2_new63		
611	x32	openat2_new64	compat_sys_openat2_new64		
612	x32	openat2_new65	compat_sys_openat2_new65		
613	x32	openat2_new66	compat_sys_openat2_new66		
614	x32	openat2_new67	compat_sys_openat2_new67		
615	x32	openat2_new68	compat_sys_openat2_new68		
616	x32	openat2_new69	compat_sys_openat2_new69		
617	x32	openat2_new70	compat_sys_openat2_new70		
618	x32	openat2_new71	compat_sys_openat2_new71		
619	x32	openat2_new72	compat_sys_openat2_new72		
620	x32	openat2_new73	compat_sys_openat2_new73		
621	x32	openat2_new74	compat_sys_openat2_new74		
622	x32	openat2_new75	compat_sys_openat2_new75		
623	x32	openat2_new76	compat_sys_openat2_new76		
624	x32	openat2_new77	compat_sys_openat2_new77		
625	x32	openat2_new78	compat_sys_openat2_new78		
626	x32	openat2_new79	compat_sys_openat2_new79		
627	x32	openat2_new80	compat_sys_openat2_new80		
628	x32	openat2_new81	compat_sys_openat2_new81		
629	x32	openat2_new82	compat_sys_openat2_new82		
630	x32	openat2_new83	compat_sys_openat2_new83		
631	x32	openat2_new84	compat_sys_openat2_new84		
632	x32	openat2_new85	compat_sys_openat2_new85		
633	x32	openat2_new86	compat_sys_openat2_new86		
634	x32	openat2_new87	compat_sys_openat2_new87		
635	x32	openat2_new88	compat_sys_openat2_new88		
636	x32	openat2_new89	compat_sys_openat2_new89		
637	x32	openat2_new90	compat_sys_openat2_new90		
638	x32	openat2_new91	compat_sys_openat2_new91		
639	x32	openat2_new92	compat_sys_openat2_new92		
640	x32	openat2_new93	compat_sys_openat2_new93		
641	x32	openat2_new94	compat_sys_openat2_new94		
642	x32	openat2_new95	compat_sys_openat2_new95		
643	x32	openat2_new96	compat_sys_openat2_new96		
644	x32	openat2_new97	compat_sys_openat2_new97		
645	x32	openat2_new98	compat_sys_openat2_new98		
646	x32	openat2_new99	compat_sys_openat2_new99		
647	x32	openat2_new100	compat_sys_openat2_new100		
648	x32	openat2_new101	compat_sys_openat2_new101		
649	x32	openat2_new102	compat_sys_openat2_new102		
650	x32	openat2_new103	compat_sys_openat2_new103		
651	x32	openat2_new104	compat_sys_openat2_new104		
652	x32	openat2_new105	compat_sys_openat2_new105		
653	x32	openat2_new106	compat_sys_openat2_new106		
654	x32	openat2_new107	compat_sys_openat2_new107		
655	x32	openat2_new108	compat_sys_openat2_new108		
656	x32	openat2_new109	compat_sys_openat2_new109		
657	x32	openat2_new110	compat_sys_openat2_new110		
658	x32	openat2_new111	compat_sys_openat2_new111		
659	x32	openat2_new112	compat_sys_openat2_new112		
660	x32	openat2_new113	compat_sys_openat2_new113		
661	x32	openat2_new114	compat_sys_openat2_new114		
662	x32	openat2_new115	compat_sys_openat2_new115		
663	x32	openat2_new116	compat_sys_openat2_new116		
664	x32	openat2_new117	compat_sys_openat2_new117		
665	x32	openat2_new118	compat_sys_openat2_new118		
666	x32	openat2_new119	compat_sys_openat2_new119		
667	x32	openat2_new120	compat_sys_openat2_new120		
668	x32	openat2_new121	compat_sys_openat2_new121		
669	x32	openat2_new122	compat_sys_openat2_new122		
670	x32	openat2_new123	compat_sys_openat2_new123		
671	x32	openat2_new124	compat_sys_openat2_new124		
672	x32	openat2_new125	compat_sys_openat2_new125		
673	x32	openat2_new126	compat_sys_openat2_new126		
674	x32	openat2_new127	compat_sys_openat2_new127		
675	x32	openat2_new128	compat_sys_openat2_new128		
676	x32	openat2_new129	compat_sys_openat2_new129		
677	x32	openat2_new130	compat_sys_openat2_new130		
678	x32	openat2_new131	compat_sys_openat2_new131		
679	x32	openat2_new132	compat_sys_openat2_new132		
680	x32	openat2_new133	compat_sys_openat2_new133		
681	x32	openat2_new134	compat_sys_openat2_new134		
682	x32	openat2_new135	compat_sys_openat2_new135		
683	x32	openat2_new136	compat_sys_openat2_new136		
684	x32	openat2_new137	compat_sys_openat2_new137		
685	x32	openat2_new138	compat_sys_openat2_new138		
686	x32	openat2_new139	compat_sys_openat2_new139		
687	x32	openat2_new140	compat_sys_openat2_new140		
688	x32	openat2_new141	compat_sys_openat2_new141		
689	x32	openat2_new142	compat_sys_openat2_new142		
690	x32	openat2_new143	compat_sys_openat2_new143		
691	x32	openat2_new144	compat_sys_openat2_new144		
692	x32	openat2_new145	compat_sys_openat2_new145		
693	x32	openat2_new146	compat_sys_openat2_new146		
694	x32	openat2_new147	compat_sys_openat2_new147		
695	x32	openat2_new148	compat_sys_openat2_new148		
696	x32	openat2_new149	compat_sys_openat2_new149		
697	x32	openat2_new150	compat_sys_openat2_new150		
698	x32	openat2_new151	compat_sys_openat2_new151		
699	x32	openat2_new152	compat_sys_openat2_new152		
700	x32	openat2_new153	compat_sys_openat2_new153		
701	x32	openat2_new154	compat_sys_openat2_new154		
702	x32	openat2_new155	compat_sys_openat2_new155		
703	x32	openat2_new156	compat_sys_openat2_new156		
704	x32	openat2_new157	compat_sys_openat2_new157		
705	x32	openat2_new158	compat_sys_openat2_new158		
706	x32	openat2_new159	compat_sys_openat2_new159		
707	x32	openat2_new160	compat_sys_openat2_new160		
708	x32	openat2_new161	compat_sys_openat2_new161		
709	x32	openat2_new162	compat_sys_openat2_new162		
710	x32	openat2_new163	compat_sys_openat2_new163		
711	x32	openat2_new164	compat_sys_openat2_new164		
712	x32	openat2_new165	compat_sys_openat2_new165		
713	x32	openat2_new166	compat_sys_openat2_new166		
714	x32	openat2_new167	compat_sys_openat2_new167		
715	x32	openat2_new168	compat_sys_openat2_new168		
716	x32	openat2_new169	compat_sys_openat2_new169		
717	x32	openat2_new170	compat_sys_openat2_new170		
718	x32	openat2_new171	compat_sys_openat2_new171		
719	x32	openat2_new172	compat_sys_openat2_new172		
720	x32	openat2_new173	compat_sys_openat2_new173		
721	x32	openat2_new174	compat_sys_openat2_new174		
722	x32	openat2			

과제2. 시스템 콜 실습

과제2-2. 시스템 콜에 매개변수 전달하기

시스템콜함수선언 ➡ 사용자영역프로그램작성 ➡ 작성한 프로그램 실행 ➡ dmesg 명령어로 결과 확인
(2-1, 2-2 정답 함께 출력)

```
/*  
*_my code  
*/  
asmlinkage void sys_print_student_id(void);  
asmlinkage void sys_print_student_info(char *name, char *major);  
  
#endif  
"include/linux/syscalls.h" 949L, 40939C
```

```
int main(void)  
{  
    // TODO: Write your code here  
    const char* arr[2];  
    arr[0] = "SEUNG TAE KIM";  
    arr[1] = "English Language and Literature";  
    syscall(333);  
    syscall(334, arr[0], arr[1]);  
    return 0;  
}
```

```
[ 9.734565] RAPL PMU: hw unit of domain pp1-gpu 2^0 Joules  
[ 9.734565] RAPL PMU: hw unit of domain psys 2^0 Joules  
[ 39.908108] snd_intel8x0 0000:00:05.0: white list rate for 1028:0177 is 48000  
[ 39.969959] EXT4-fs (sda2): mounted filesystem with ordered data mode. Opts: (null)  
[ 40.210385] audit: type=1400 audit(1617337001.156:2): apparmor="STATUS" operation="profile_load"  
profile="unconfined" name="/usr/lib/snapd/snap-confine" pid=779 comm="apparmor_parser"  
[ 40.210392] audit: type=1400 audit(1617337001.156:3): apparmor="STATUS" operation="profile_load"  
profile="unconfined" name="/usr/lib/snapd/snap-confine//mount-namespace-capture-helper" pid=779 comm="apparmor_parser"  
[ 40.214499] audit: type=1400 audit(1617337001.160:4): apparmor="STATUS" operation="profile_load"  
profile="unconfined" name="/usr/bin/lxc-start" pid=777 comm="apparmor_parser"  
[ 40.235583] audit: type=1400 audit(1617337001.180:5): apparmor="STATUS" operation="profile_load"  
profile="unconfined" name="/usr/bin/man" pid=778 comm="apparmor_parser"  
[ 40.235588] audit: type=1400 audit(1617337001.180:6): apparmor="STATUS" operation="profile_load"  
profile="unconfined" name="man_filter" pid=778 comm="apparmor_parser"  
[ 40.235590] audit: type=1400 audit(1617337001.180:7): apparmor="STATUS" operation="profile_load"  
profile="unconfined" name="man_groff" pid=778 comm="apparmor_parser"  
[ 40.239525] audit: type=1400 audit(1617337001.184:8): apparmor="STATUS" operation="profile_load"  
profile="unconfined" name="lxc-container-default" pid=775 comm="apparmor_parser"  
[ 40.239533] audit: type=1400 audit(1617337001.184:9): apparmor="STATUS" operation="profile_load"  
profile="unconfined" name="lxc-container-default-cgns" pid=775 comm="apparmor_parser"  
[ 40.239536] audit: type=1400 audit(1617337001.184:10): apparmor="STATUS" operation="profile_load"  
profile="unconfined" name="lxc-container-default-with-mounting" pid=775 comm="apparmor_parser"  
[ 40.239540] audit: type=1400 audit(1617337001.184:11): apparmor="STATUS" operation="profile_load"  
profile="unconfined" name="lxc-container-default-with-nesting" pid=775 comm="apparmor_parser"  
[ 42.377593] IPv6: ADDRCONF(NETDEV_UP): enp0s3: link is not ready  
[ 42.384692] e1000: enp0s3 NIC Link is Up 1000 Mbps Full Duplex, Flow Control: RX  
[ 42.385212] IPv6: ADDRCONF(NETDEV_CHANGE): enp0s3: link becomes ready  
[ 45.141756] new mount options do not match the existing superblock, will be ignored  
[ 84.679806] My Student ID is 2013130890  
[ 84.679807] My Name is SEUNG TAE KIM  
[ 84.679808] I major in English Language and Literature
```

```
os-practice: ~  
➔ gcc -o assignment assignment.c  
assignment.c: In function 'main':  
assignment.c:9:2: warning: implicit declaration of function 'syscall' [-Wimplicit-function-declaration]  
    syscall(333);  
    ~~~~~  
os-practice: ~  
➔ ./assignment  
os-practice: ~  
➔ dmesg_
```

```
[ 84.679806] My Student ID is 2013130890  
[ 84.679807] My Name is SEUNG TAE KIM  
[ 84.679808] I major in English Language and Literature
```