

# ftz 10번 문제풀이

180726(목)  
안지현

# 문제

```
[level10@ftz level10]$ cat hint
```

두명의 사용자가 대화방을 이용하여 비밀스런 대화를 나누고 있다.  
그 대화방은 공유 메모리를 이용하여 만들어졌으며,  
key\_t의 값은 7530이다. 이를 이용해 두 사람의 대화를 도청하여  
level11의 권한을 얻어라.

- 레벨을 완료하셨다면 소스는 지우고 나가주세요.

# 키워드

# 문제

```
[level10@ftz level10]$ cat hint
```

두명의 사용자가 대화방을 이용하여 비밀스런 대화를 나누고 있다.  
그 대화방은 공유 메모리를 이용하여 만들어졌으며,  
key\_t의 값은 7530이다. 이를 이용해 두 사람의 대화를 도청하여  
level11의 권한을 얻어라.

- 레벨을 완료하셨다면 소스는 지우고 나가주세요.

# 공유 메모리란?

여러 프로세스가 함께 사용하는 메모리

공유 메모리를 이용하면 ~

- ① 기능 분할/참조 => 같은 데이터를 공유할 수 있다.
- ② 프로세스끼리 통신을 할 수 있다.

- 프로세스 A에서 공유 메모리 생성



- 프로세스 A에 공유 메모리 첨부 및 사용

★ 공유 메모리를 사용하기 위해서는 공유 메모리를 프로세스 안에 첨부하여 마치 자기 메모리를 사용하듯 사용합니다.



- 프로세스 B도 공유 메모리 첨부 및 사용



=> 프로세스 간의 통신0

# **ipcs** (Inter-Process Communication) 명령어

OS에서 프로그램이 사용하는 IPC, 공유 메모리,  
세마포어의 현황을 파악할 수 있다.

**ipcs -m**

공유 메모리 세그먼트만을 확인할 수 있다.

# 공유 메모리 정보 확인

```
[level10@ftz level10]$ ipcs
```

```
----- Shared Memory Segments -----
```

key	shmid	owner	perms	bytes	nattch	status
0x00001d6a	0	root	666	1028	0	

```
----- Semaphore Arrays -----
```

key	semid	owner	perms	nsems
-----	-------	-------	-------	-------

```
----- Message Queues -----
```

key	msqid	owner	perms	used-bytes	messages
-----	-------	-------	-------	------------	----------

# 16진수를 10진수로 변환하기

16진수

10진수

10진수 변환하기

다시 계산하기



헤더	#include <sys/ipc.h> #include <sys/shm.h>	
형태	int shmget(key_t key, int size, int shmflg);	
인수	key_t key	공유 메모리를 구별하는 식별 번호 7530
	int size	공유 메모리 크기 1028
	int shmflg	동작 옵션 IPC_CREATE 값을 입력후 ‘ ’ 연산자를 덧붙여 허용권한 설정 => IPC_CREATE   0666
	shmflg	옵션 내용
	IPC_CREATE	key에 해당하는 공유 메모리가 없다면 새로 생성한다. 만약있다면 무시하며 생성을 위해 접근 권한을 지정해 주어야 한다.
	IPC_EXCL	공유 메모리가 이미 있다면 실패로 반환하며 공유 메모리에 접근하지 못한다. 이 옵션이 없어야 기존 공유 메모리에 접근할 수 있다.
반환	-1 실패 -1 이외공유 메모리 생성 성공, 공유 메모리 식별자	

```
[level100ftz level101$ ipcs
```

```
----- Shared Memory Segments -----
```

key	shmid	owner	perms	bytes	nattch	status
0x00001d6a	0	root	666	1028	0	

```
----- Semaphore Arrays -----
```

key	semid	owner	perms	nsems
-----	-------	-------	-------	-------

```
----- Message Queues -----
```

key	msqid	owner	perms	used-bytes	messages
-----	-------	-------	-------	------------	----------

# 공유 메모리 관리 함수

`shmget(key_t key, int size, int flag)`

공유메모리 생성 or 생성된 공유메모리의 id 반환

=> `shmget(7530, 1028, IPC_CREAT | 0666)`

`shmat(int shmid, xshmatdr, int flag)`

생성된 공유메모리를 프로세스에 연결(attach)

=> `shmat(0, NULL, 0)`

```
[level10@ftz level10]$ cd /tmp/  
[level10@ftz tmp]$ cat > smemory.c  
#include <stdio.h>  
#include <sys/shm.h>  
#include <sys/ipc.h>  
  
int main() {  
    int a;  
    char *p  
  
    a = shmget(7530, 1028, IPC_CREAT | 0666);  
    p = shmat(a, NULL, 0);  
  
    printf("%s", p);  
    return 0;  
}
```

```
[level10@ftz tmp]$ gcc -o smemory smemory.c
[level10@ftz tmp]$ ls -al
total 32
drwxrwxrwt    2 root      root      4096 Jul 22 18:20 /
drwxr-xr-x   20 root      root      4096 Jul 22 17:56 /tmp
-rwxrwxr-x    1 level9    level9    391 Jul 22 12:44 bof
-rw-r--r--    1 level9    level9    364 Jul 22 12:39 bof.c
srwxrwxrwx    1 mysql     mysql      0 Jul 22 17:56 /tmp/mysql.sock
-rwxrwxr-x    1 level10   level10 11771 Jul 22 18:20 smemory
-rw-rw-r--    1 level10   level10 194 Jul 22 18:20 smemory.c
[level10@ftz tmp]$ ./smemory
```

flag

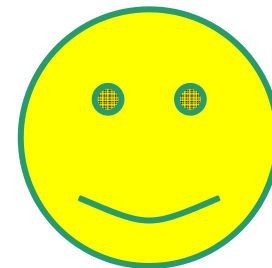
# # 아쉬운 점

속도를 내자

# # 만족한 점



애틀가 즐거웠다



감사합니다