

// Thread 1

```
sys_mmap(...) {  
    // Hold mmap_sem as mutex.  
    down_write(mm->mmap_sem);  
    do_map(...);  
    up_write(mm->mmap_sem);  
}
```

// Thread 2

```
sys_uselib(...) {  
    // Do not hold mmap_sem.  
    if (bss > len)  
        do_unmap(...); // Corrupt mm.  
}
```