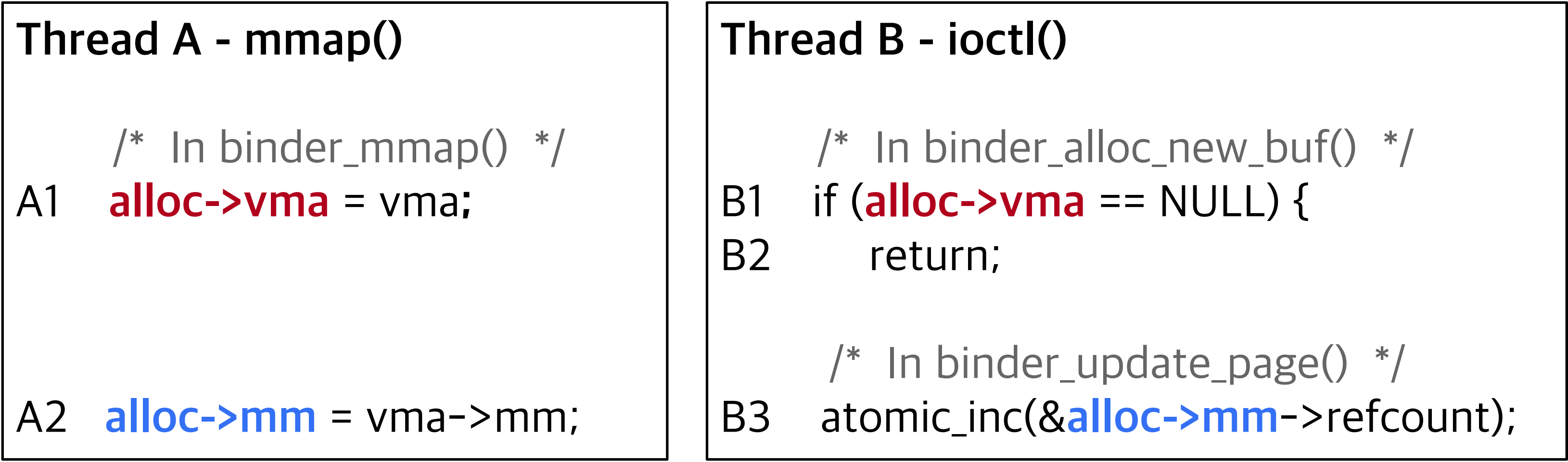

Thread A - mmap()

```
     /*  In binder_mmap()  */
A1   alloc->vma = vma;



A2   alloc->mm = vma->mm;
```

Thread B - ioctl()

```
     /*  In binder_alloc_new_buf()  */
B1   if (alloc->vma == NULL) {
B2       return;

     /*  In binder_update_page()  */
B3   atomic_inc(&alloc->mm->refcount);
```