Race Condition

实验环境：Ubuntu 16.04 LTS amd64

实验工具：无

实验目的：本实验的目的是通过实验了解条件竞争产生的原因以及如何利用存在漏洞的特权程序获得root权限。

环境搭建：

```
gcc rc.c -o rc -lpthread
sudo chown root:root secret.txt
sudo chmod 700 secret.txt
mv common.txt /tmp/
sudo chown root:root rc
sudo chmod +s rc
```

执行程序

```
./rc
```

观察是否有flag之类的字样出现。

本次实验的内容为，通过rc程序读只有root用户才能读取的secret内容。

本节课任务要求：

1. 分析rc程序源代码，解释其中的漏洞原因。
2. 如果将源代码中的两处usleep函数去掉，结果会怎样，为什么?
3. 请你为上述程序打上补丁，避免此漏洞的发生
4. 解释race condition漏洞产生的根本原因以及比较通用的解决办法(选做)