OSLAB2实验报告

余晨宁 151242062 匡亚明学院
151242062@smail.nju.edu.cn
2017.04.09

实验环境

ubuntu：64位16.04，gcc：5.3.1, 要先apt-get install gcc-4.8-multilib

实验进度

我完成了扁平模式+分页，并用系统调用重构了黑白棋游戏。游戏成功运行。

实验问题

一、

如果你参考jos的代码，在entry.S中，有这样2行代码：
_start = RELOC(entry)
...
jmp *%eax
请分别解释这2行代码的意义

答：RELOC(entry)的意思就是把entry的地址从虚拟地址映射到物理地址再赋值给_start。jmp *%eax的意思就是不再在低地址运行，跳转到kern的C程序里。

二、

这样做为什么可以，会不会带来什么问题?

答：因为kernel是所有进程都能用的，但想要用的话需要通过从用户态变为内核态或者系统调用，因此就算拷贝了，也是有特权等级的。kernel的物理地址是不变的，因此通过拷贝给所有的进程，kernel能够被共享。没看出什么问题。

实验心得和想法

实验一开始我是崩溃的，因为完全不知道自己要干什么，没有实现系统调用的思路，也完全忘记了关于分页的知识。但后来通过借鉴andsora前辈和JOS的代码（谢谢你们！），我逐渐懂得了oslab2是干嘛的，它相当于整理一下书桌的事情。

另外我深深体会到JOS的特别靠谱，除了能提高我熟练地阅读洋文的知识水平之外，它给了我很多方便的地方，比如很多的注释。

自然，我碰到了一些bug，比如说运行的时候一直卡在kernel代码不跳到game代码上，原因是我的game里的和kernel里的keyboard的按键筛选不一样；
再比如碰到了一个图案被依照颜色分离成九个图案打在了屏幕上，原因是我的屏幕大小搞错了，而且boot里面进入了VESA的图形模式。

这些地方都是由于我不深入理解代码导致的，这告诉我们写代码时一定要读懂原有的代码。

另外，make qemu的时候出现了如同**lib/printfmt.c:41: undefined reference to `__udivdi3'**的错误，查了一下是由于没有sudo apt-get install gcc-4.8-multilib，install花费了一个小时的时间（宿舍网速小水管），那时我的内心想法是：如果有下次的话我就直接跑ubuntu32位机子得了，编译的时候还不用加-m32。

总得来说，这次实验还算是比较轻松的，我成功在一个周末内完成了它。同时，我的间接体会告诉我git记录对于清楚自己要干什么很重要，有的时候我写代码，写着写着就会产生“咦？我在哪？我要干什么？”的疑问。提前在log当中写好我要干什么，也许会是解决自我困惑的重要途径。

助教玩游戏的时候要记得先按enter啊，不然游戏进不去的2333。