操作系统实习实验班

Lab 1: Booting a PC

陈向群 北京大学计算机科学技术系

2013 春季

实习相关

- 论文阅读
  - ***The UNIX Time-Sharing System***
  - ***The Origin of the VM/370 Time-sharing System***

- 代码和报告提交截止日期
  - **3月13日，23:55**

提纲

- 实习内容
- 知识要点
- 思考题

实习内容

第一周

1. 阅读实习指导文档
2. 自学本次实习中的知识要点
3. 搭建实习环境
4. 运行并感受JOS

第二周

1. 阅读JOS代码，熟悉JOS启动流程
2. 完成所有exercise和1个challenge
3. 撰写实习报告

知识要点

环境搭建与使用

- Linux的安装与使用
  - 基本的Shell语法：管道，重定向等
  - 常用Linux命令的使用：find，grep等
- JOS的编译生成
  - GNU make，JOS中的makefile
  - GNU binutils，汇编、反汇编和链接工具
  - gcc编译器的使用
- JOS的运行环境
  - QEMU虚拟机的编译，安装和使用

环境搭建与使用（续）

- JOS的调试
  - gdb的基本用法
- 代码的管理
  - git的基本用法

x86体系结构相关

- AT&T汇编语法
- x86指令系统
- x86 ABI （应用程序二进制接口）
  - 数据类型的大小、布局、对齐
  - 函数调用约定：参数、返回值传递，栈帧的结构
  - 通用寄存器的使用约定
- x86中的状态、控制寄存器
- 实模式和保护模式
- 虚拟地址，线性地址，物理地址

内核的加载运行

- **ELF文件格式**
- **链接地址和加载地址**
- **BIOS→Bootloader→内核的执行流程**

思考题

基础题

1. 脚本 **boot/sign.pl** 的作用是什么？
2. **printf**函数如何支持可变数量参数？参数的具体数量是如何确定的？
3. 解释从开机到**JOS**内核开始执行的整个流程

难题

1. 怎样使用GRUB等现有的bootloader加载JOS内核？
2. 在 boot/boot.S 中，`movl %eax, %cr0` 指令之后 CPU 已经进入保护模式，为何随后的 `ljmp` 指令却出现在 `.code32` 标志之前？能否移到 `.code32` 后面？

The End

Thanks