嵌入式Linux驱动开发简介

主要内容

- Linux内核与驱动的关系
- Linux内核中驱动的分类
- 驱动开发的两前题：模块、节点
- Linux下驱动程序的基本框架
- Linux下驱动程序的调试方法
- Linux中驱动编程的高级接口

FARSIGHT

Linux设备驱动的概念

- 驱动程序为硬件提供一个定义良好的内部接口
- 驱动程序封装了硬件细节
- 驱动程序为应用程序提供了访问设备的机制

FARSIGHT

设备驱动健壮性和安全性

- 驱动程序是内核的一部分
- 驱动程序的漏洞和缺陷直接危及内核
- 留心未初始化的指针，恶意用户程序，缓冲区溢出

FARSIGHT

驱动程序与内核的关系

- 字符设备驱动与块设备驱动由内核中的文件系统来管理
- 网络设备驱动由内核中的协议栈来管理

FARSIGHT

Linux设备和模块的分类

- 设备和模块的分类：字符设备，块设备，网络接口以及提供公共服务的特定类型设备
  - 例如Dma驱动
  - 系统时钟驱动
  - 终端控制器驱动

FARSIGHT

Linux下构建和运行模块

- 为什么用模块?
- 模块和应用程序有什么不同
- #ifdef __KERNEL__
- #ifdef MODULE
- Kernel 和 user space

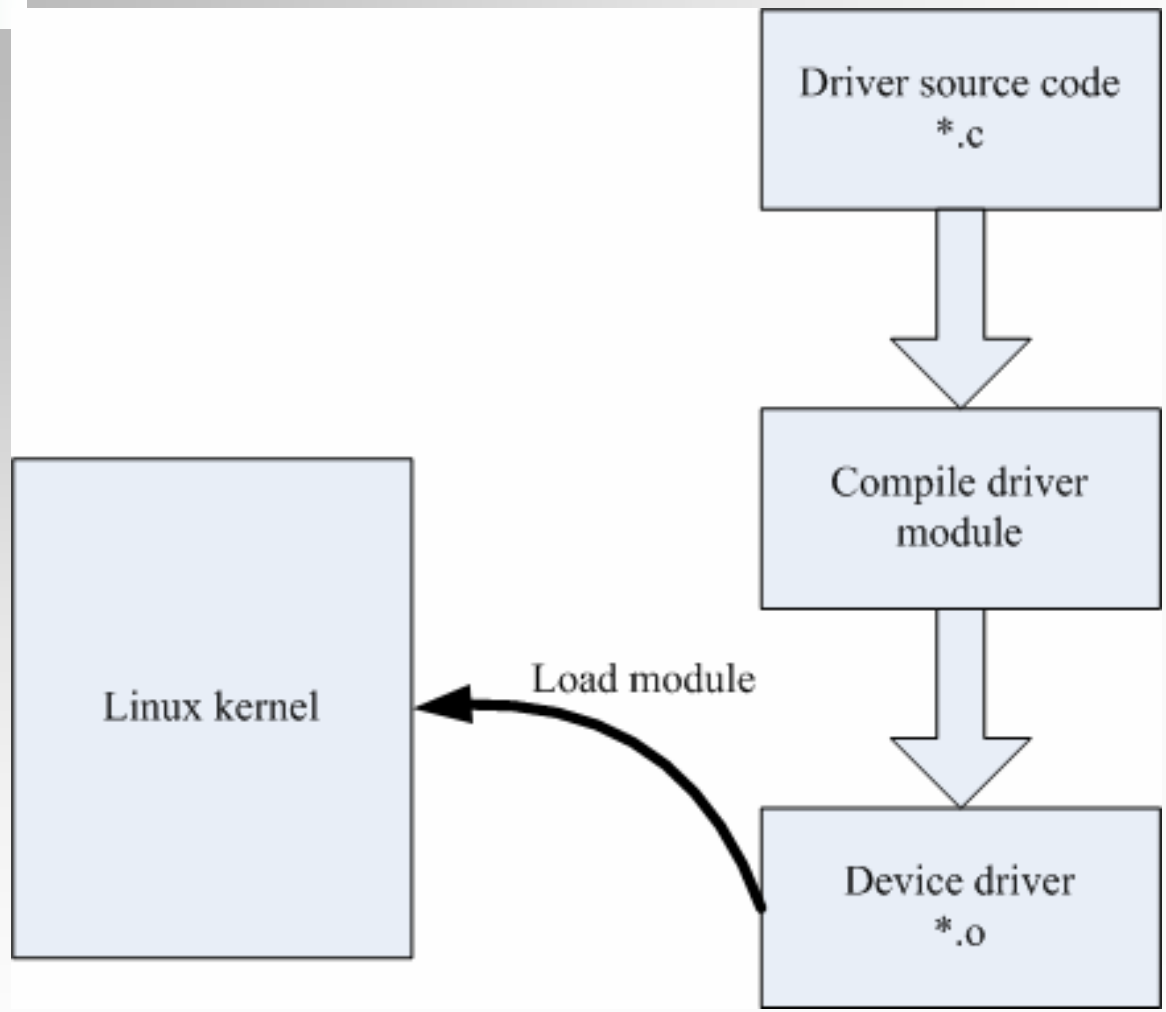
FARSIGHT

模块的编译和装载

- 编译模块都需要什么
- 编译模块相关的宏
- 模块工具insmod,rmmod

FARSIGHT

Linux驱动程序模块加载



设备访问－设备节点

- mknod 创建设备文件
- 字符设备文件例子
- crw-rw---- 1 root uucp 4, 64 2005-03-20 03:36 /dev/ttyS0
- 主设备号区分设备驱动程序
- 用户程序调用open close等操作，内核根据主设备号找到对应的驱动程序

设备访问－主设备号和次设备号

- 次设备号区分同一个驱动程序创建的多个设备
- 常见于多个串口，硬盘分区等
- 次设备号通常依次对应同类型多个设备

	主设备号	次设备号
hda1	3	1
hda2	3	2
hda3	3	3

设备驱动的框架

- 设备的注册－驱动程序的开始
- 注册的结构体
- 注册的fop指针

FARSIGHT

三类设备驱动程序的结构框架

- 字符设备驱动框架
- 块设备驱动框架
- 网络设备驱动框架

FARSIGHT

设备驱动程序的调试方法

- Printk/printascii
- kgdb
- 看系统崩溃信息
- 用硬件调试器
- 使用proc或sysfs文件系统

FARSIGHT

设备驱动高级接口－内存管理

- kmalloc
- slab
- 基于页的内存分配
- vmalloc
- Bootmem的分配

FARSIGHT

内核内存分配

- 内核程序员获得内存的方法kmalloc，使用方法类似于用户空间的malloc版本
- kmalloc传递不同标志，导致该函数的不同行为
  - GFP_KERNEL
  - GFP_ATOMIC
  - GFP_USER
  - __GFP_DMA

后备高速缓存

- 设备驱动程序如果常常反复使用同样大小的内存块，可以自己创建一个内存池
- 在大量使用固定大小内存块，使用后备高速缓存比kmalloc更快速，同时也节省空间
- /proc/slabinfo入口提供内存池的状态信息，方便我们跟踪

FARSIGHT

分页式内存

- 当需要在驱动程序中使用大块的内存，直接使用面向页的内存分配方式比较适合
- 使用get_free_page函数族申请整数倍于页大小的内存空间
- free_page函数用来释放不用的页面
- 分配、释放多个页面时，传递的参数为order，表示2的order次幂个页面

FARSIGHT

Vmalloc和相关函数

- vmalloc函数用来分配虚拟地址空间的连续区域
- vmalloc函数获得的连续虚拟地址空间在物理地址上可能是不连续的
- vmalloc函数获得的地址是平台相关的

FARSIGHT

内核引导时的内存分配

- 如果需要连续的大块内存区域，就需要在内核引导时分配
- 使用引导时分配的方式跳过了linux内存管理，直接保留需要的内存区域
- 调用alloc_bootmem函数族可以在boot time分配大块的连续区域，绕过了get_free_page等函数对分配内存大小的限制

FARSIGHT

www.FarSight.com.cn

谢谢！