ای نام تو بهترین سرآغاز

دستور کار پنجم آزمایشگاه سیستم عامل

حمید فدیشه‌ای، دانشگاه بجنورد

برنامه‌نویسی سطح کرنل

کرنل قسمتی از نرم‌افزار سیستم است که با قابلیت دسترسی کامل به منابع سیستم (Privileged Mode) اجرا می‌شود. سایر برنامه‌ها کاربردی هستند و برای دسترسی به امکانات سیستم از کرنل درخواست (System Call) انجام می‌دهند.

کرنل لینوکس کد حجیمی است. برنامه‌نویسی برای تغییرات یا افزودن قابلیت‌ها به آن اگر به روش معمولی برنامه‌نویسی انجام شود (کامپایل مجدد کد بعد از اجرا) کار سخت و زمان‌بری خواهد بود و ضمنا تغییر کرنل جاری سیستم نیاز به راه‌اندازی مجدد آن (Restart) خواهد داشت. برای رفع این دشواری‌ها در کرنل لینوکس مفهومی به نام ماژول (Module) وجود دارد. یک ماژول برنامه‌ای است که جداگانه کامپایل و اجرا می‌شود و قابلیت افزوده شدن به یک کرنل در حال اجرا را داراست.

افزودن یک ماژول به کرنل با دستور insmod و حذف آن از کرنل با دستور rmmod انجام می‌شود. با توجه به این که ماژول‌ها سلسله مراتب نیازمندی به یکدیگر دارند، دستور دیگری به نام modprobe وجود دارد که برای نصب یک ماژول به طور خودکار نیازمندی‌های آن را نیز نصب می‌کند.

هر ماژول وظیفه خاصی از وظایف سیستم عامل را پیاده سازی می کند. مثلا کنترل فرایندها، مدیریت حافظه، ایجاد ارتباط و راه‌اندازی وسایل جانبی نظیر کارت شبکه و غیره.

آزمایش ۵-۱. آشنایی با ماژول‌های موجود کرنل

ماژول‌ها به صورت فایل‌های با پسوند ko در مسیر /lib/modules/<kernel-version> ذخیره شده‌اند. فهرست آن‌ها را با دستور مناسب در خط فرمان لیست کنید:

```
find /lib/modules/<kernel-version> -name “*.ko” | less
```

فهرست ماژول‌هایی که هم اکنون در کرنل بارگذاری شده اند با دستور lsmod قابل مشاهده است. ببینید. تلاش کنید ماژول راه‌انداز کارت صوتی و کارت شبکه را در فهرست شناسایی کنید.

در صورت نیاز از دستور modinfo برای دریافت اطلاعات یک ماژول خاص استفاده کنید.

آزمایش ۵-۱. افزودن/ حذف یک ماژول از پیش موجود به/از کرنل

می‌خواهیم حذف کردن یا افزودن یک ماژول را امتحان کنیم و اثر آن بر کرنل را ببینیم. ماژول هدف آزمایش ما ماژول درایور کارت شبکه سیستم است.

سیستم شما یک کارت شبکه دارد. با دستور ifconfig –a نام کرنلی آن را احتمالا به صورت eth0 مشاهده خواهید کرد. نام ماژول آن را در قسمت قبل یافتید. مثلا e1000. سعی کنید آن را از کرنل حذف کنید:

rmmod e1000

اگر خطایی مبنی بر مشغول و تحت استفاده بودن ماژول گرفتید ابتدا رابط شبکه را با دستور ifconfig eth0 down غیر فعال کنید بعد ماژول را حذف کنید

بعد از حذف ماژول دوباره فهرست رابط‌های شبکه را با ifconfig –a بگیرید. چه می‌بینید؟

اگر ماژول در حین نصب پیامی تولید کند در Log کرنل ثبت می‌شود. Log کرنل با دستور dmesg قابل مشاهده است. بگویید حذف و نصب ماژول جدید چه پیام‌هایی تولید کرده است.

آزمایش ۵-۳. نوشتن یک ماژول جدید

هدف نوشتن ماژولی است که هیچ کاری نمی‌کند. فقط هنگام نصب و حذف یک پیام در Log تولید می‌کند.

برای نوشتن ماژول نیاز به فایل‌های Header کرنل دارید (چون برنامه ماژول آن‌ها را #include کرده است). این فایل ها به طور پیش فرض با سیستم عامل نصب نشده اند. پس نصبشان کنید:

apt-get install kernel-headers

اسکلت سورس یک ماژول به صورت زیر است. فایل hello.c را با محتوای زیر ایجاد کنید:

```
#define MODULE
#define LINUX
#define __KERNEL__

#include <linux/module.h>

int init_module()
{
	printk("<1>inserting module\n");
	return 0;
}

void cleanup_module()
{
	printk("<1>removing module\n");
}

MODULE_LICENSE("GPL");
```

دقت کنید کد کرنل به جای printf از printk استفاده می‌کند و خروجی به Log کرنل هدایت می‌شود.

برای کامپایل ماژول یک فایل به نام Makefile با محتوای زیر ایجاد کنید. سپس در همان مسیر دستور make را صادر نمایید:

```
obj-m += hello.o

all:
	make -C /lib/modules/$(shell uname -r)/build M=$(PWD) modules
```

```
clean:
	make -C /lib/modules/$(shell uname -r)/build M=$(PWD) clean
```

تمرین ۵

ماژول کرنلی بنویسید که هر ثانیه یک بار تعداد فرایندهای در حال اجرا روی سیستم را در Log ذکر نماید برای این منظور باید از امکان تعریف timer در کرنل استفاده کنید که با استفاده از آن تابعی که مشخص می کنید در فواصل مشخص زمانی اجرا می شود. برای تعریف و استفاده از این امکان، در مورد ساختار timer_list در کرنل جستجو کنید.

ضمنا برای شمارش تعداد فرایندها می‌توانید از قطعه کدی شبیه زیر استفاده نمایید:

```
#include <sched.h>
…

struct task_struct *task;
int n=0;
for_each_process(task)
	n++;
```