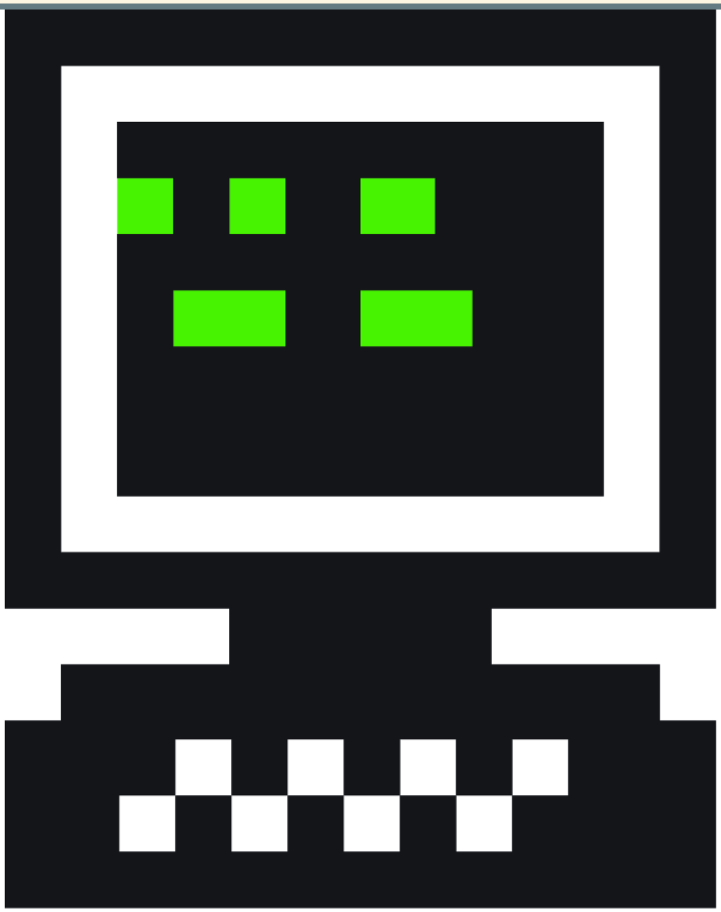
YOU CAN BE A KERNEL HACKER

by Julia Evans
twitter.com/b0rk
github.com/jvns
jvns.ca



Hacker School

WHERE WE'RE GOING

1. WTF is a kernel?
2. Why should you care?
3. Strategies for getting started with kernel programming
    1. Read some kernel code!
    2. Write a kernel module!
    3. Write your own operating system
    4. Do an internship

1. WTF IS A KERNEL?

KERNELS ARE JUST CODE!

When I go to http://google.com, kernel code runs for:

- Typing in the address
- Handling every network packet
- Writing history files to disk
- Allocating memory
- Communicating with the graphics card

HOW TO CALL KERNEL CODE

System calls!!!

SYSTEM CALLS: A KERNEL’S API

- open a file! (open)
- start a program! (execve)
- change a file's permissions! (chmod)

WHAT WE'VE LEARNED

- Your kernel does tons of stuff
- Programs tell it what to do using system calls

2. WHY SHOULD YOU CARE?

- People will think you're a badass
- You'll become a better programmer

USUAL STRATEGIES

- Read LKML
- Submit patches
- Linus yells at you for being dumb
- Cry

OUR STRATEGIES

1. Read some kernel code!
2. Write a kernel module!
3. Write your own operating system
4. Do an internship

3. STRATEGIES FOR GETTING STARTED

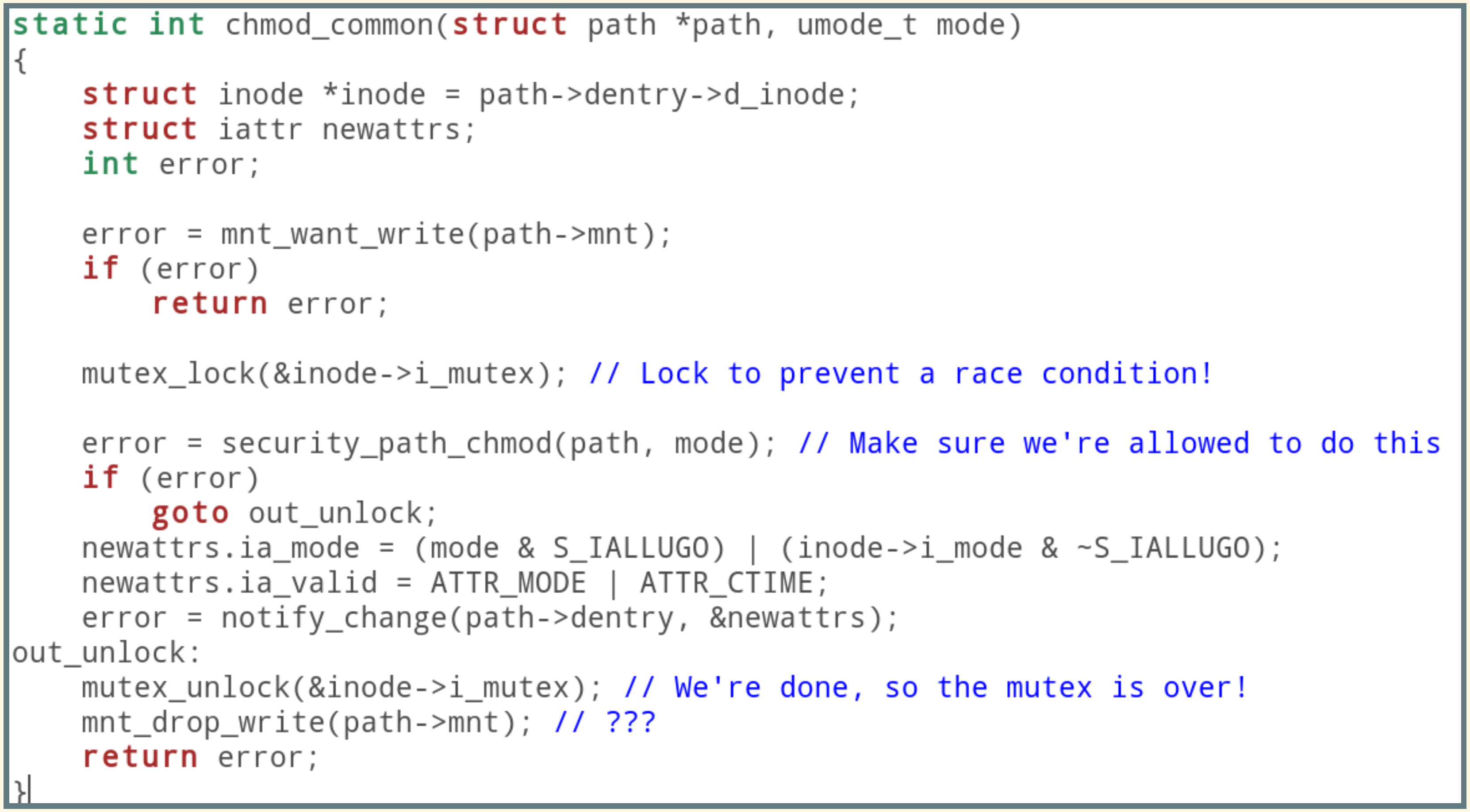
STRATEGY 1: READ SOME KERNEL CODE

BUT THAT’S TERRIFYING!!!!!

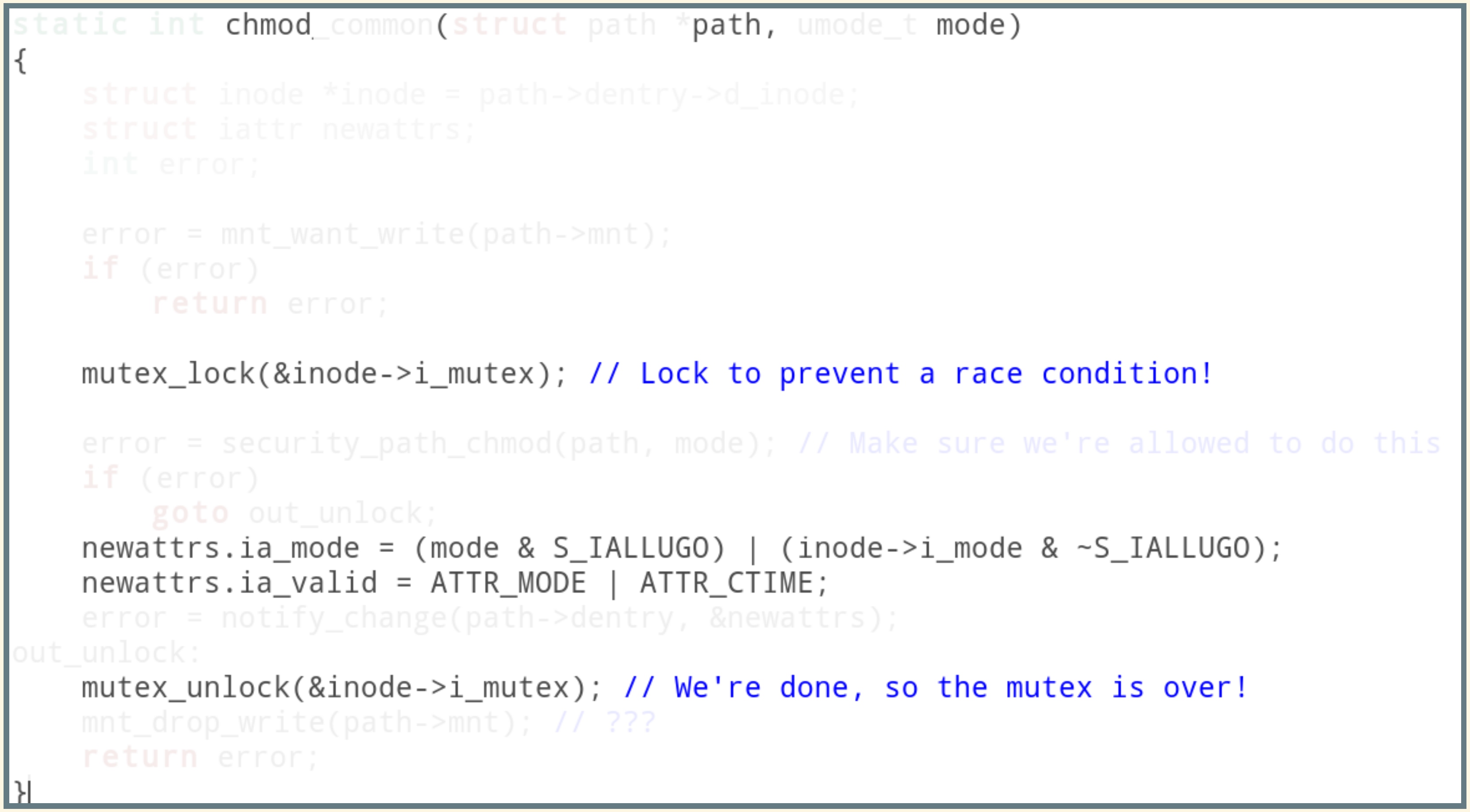
Pick one system call and try to understand one thing about it

Linux kernel: LXR, `http://livegrep.com`

OS X kernel: `http://opensource.apple.com`



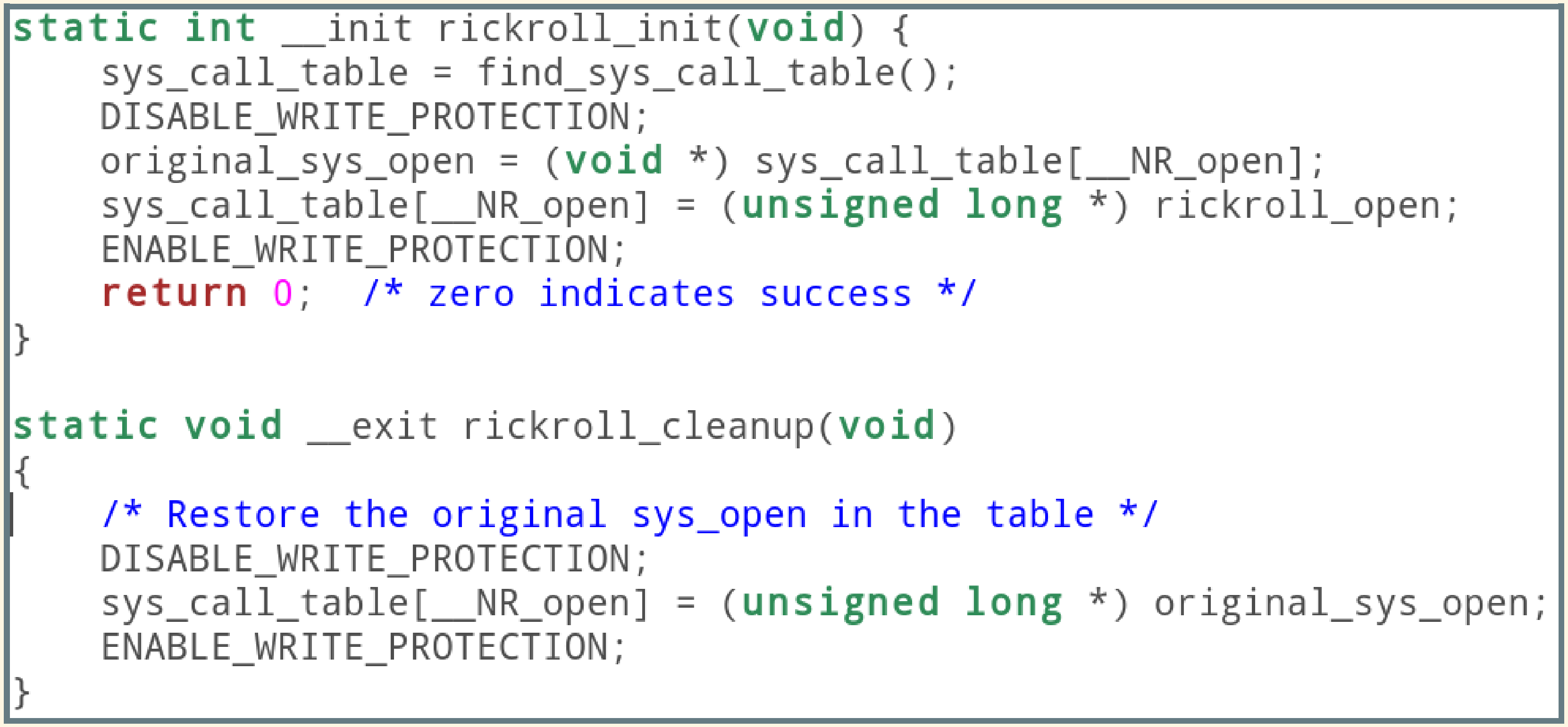
```c
static int chmod_common(struct path *path, umode_t mode)
{
    struct inode *inode = path->dentry->d_inode;
    struct iattr newattrs;
    int error;

    error = mnt_want_write(path->mnt);
    if (error)
        return error;

    mutex_lock(&inode->i_mutex); // Lock to prevent a race condition!

    error = security_path_chmod(path, mode); // Make sure we're allowed to do this
    if (error)
        goto out_unlock;
    newattrs.ia_mode = (mode & S_IALLUGO) | (inode->i_mode & ~S_IALLUGO);
    newattrs.ia_valid = ATTR_MODE | ATTR_CTIME;
    error = notify_change(path->dentry, &newattrs);
out_unlock:
    mutex_unlock(&inode->i_mutex); // We're done, so the mutex is over!
    mnt_drop_write(path->mnt); // ???
    return error;
}
```



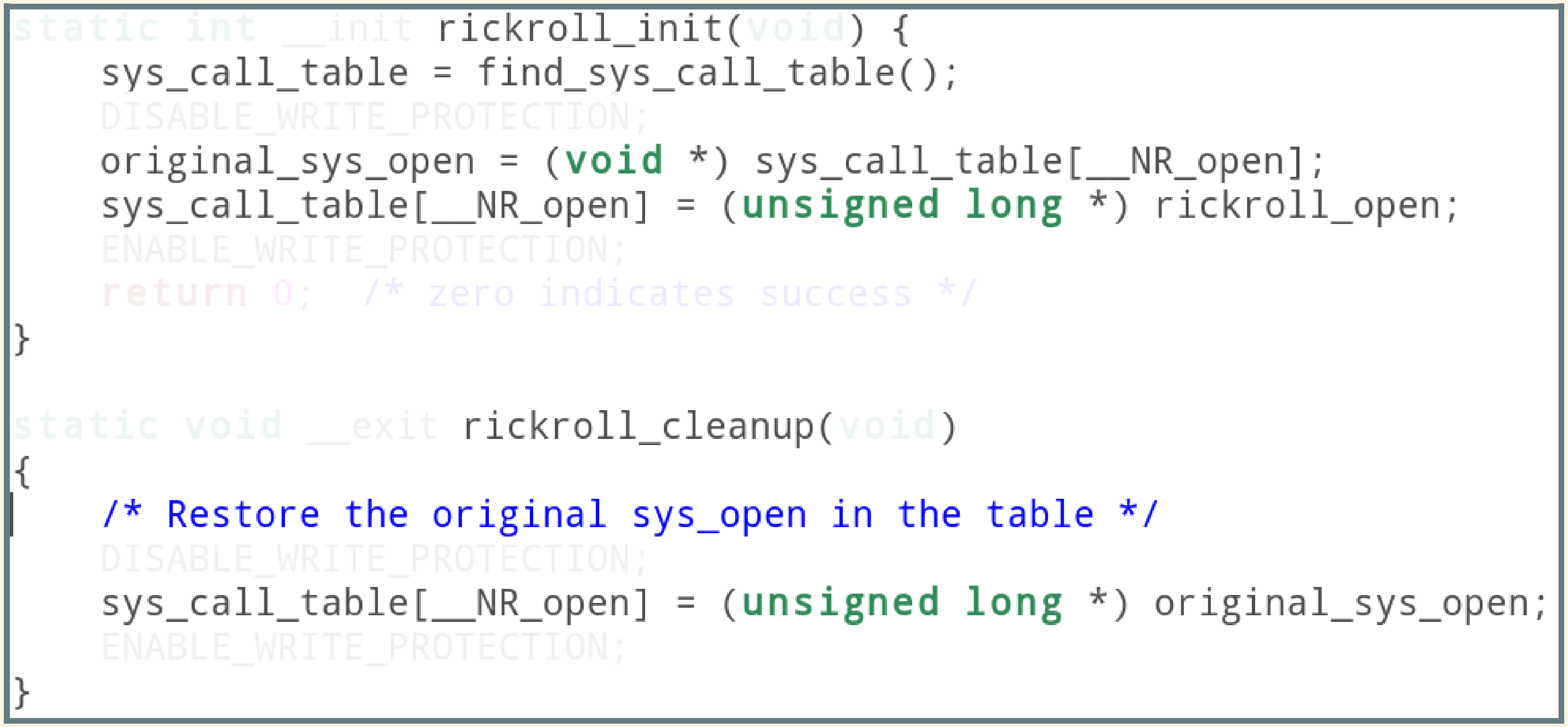
```
static int chmod_common(struct path *path, umode_t mode)
{
    struct inode *inode = path->dentry->d_inode;
    struct iattr newattrs;
    int error;

    error = mnt_want_write(path->mnt);
    if (error)
        return error;

    mutex_lock(&inode->i_mutex); // Lock to prevent a race condition!

    error = security_path_chmod(path, mode); // Make sure we're allowed to do this
    if (error)
        goto out_unlock;
    newattrs.ia_mode = (mode & S_IALLUGO) | (inode->i_mode & ~S_IALLUGO);
    newattrs.ia_valid = ATTR_MODE | ATTR_CTIME;
    error = notify_change(path->dentry, &newattrs);
out_unlock:
    mutex_unlock(&inode->i_mutex); // We're done, so the mutex is over!
    mnt_drop_write(path->mnt); // ???
    return error;
}
```

STRATEGY 2: WRITE A LINUX KERNEL MODULE

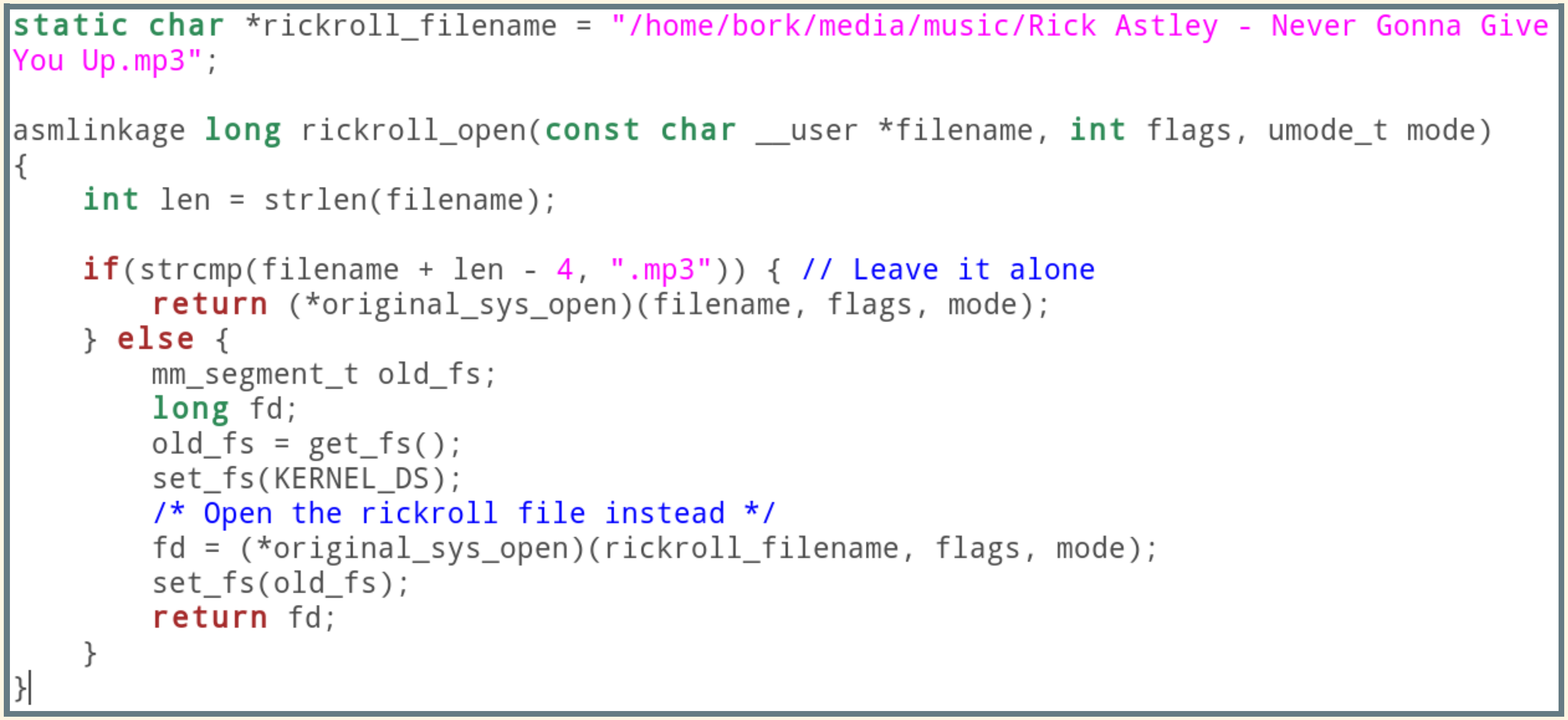
DEMO DEMO DEMO



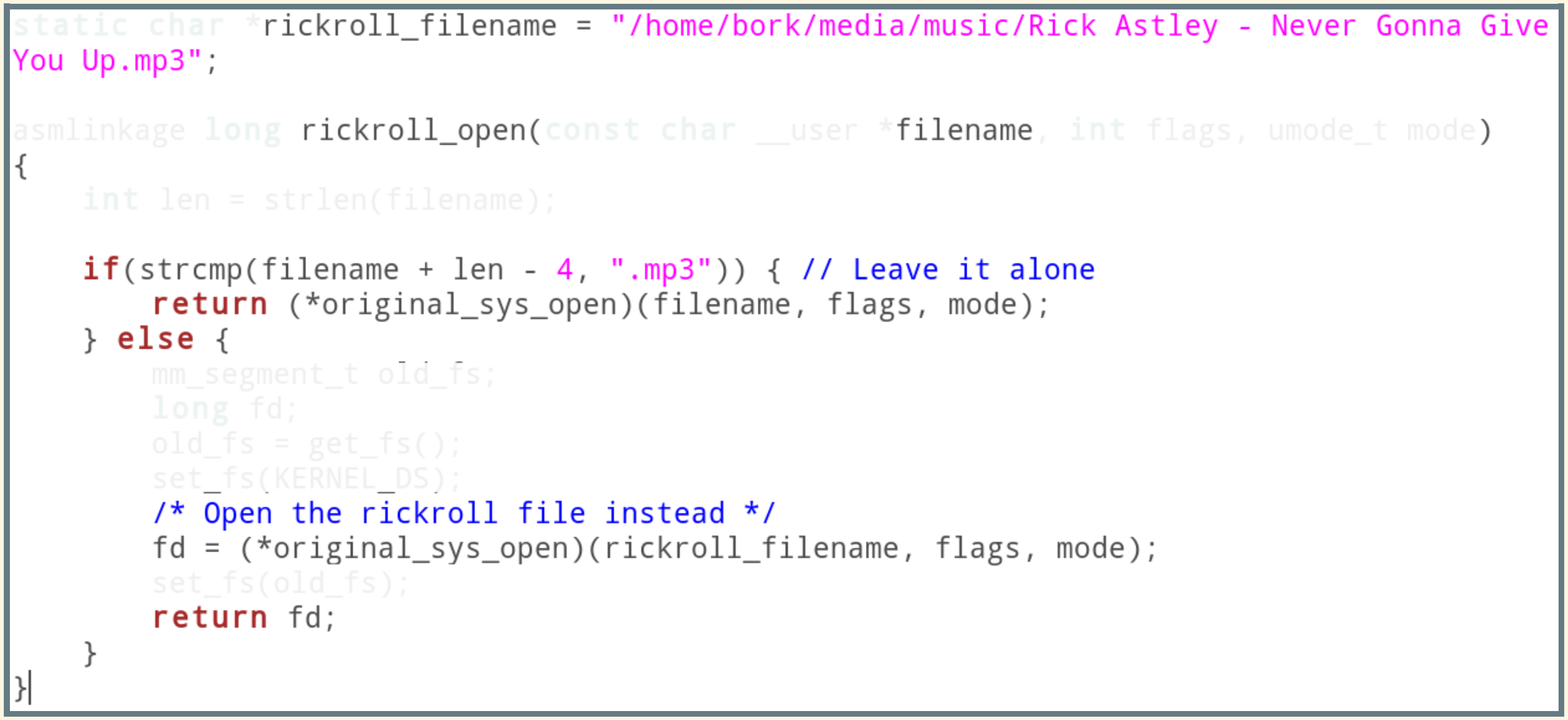
```
static int __init rickroll_init(void) {
    sys_call_table = find_sys_call_table();
    DISABLE_WRITE_PROTECTION;
    original_sys_open = (void *) sys_call_table[__NR_open];
    sys_call_table[__NR_open] = (unsigned long *) rickroll_open;
    ENABLE_WRITE_PROTECTION;
    return 0;  /* zero indicates success */
}

static void __exit rickroll_cleanup(void)
{
    /* Restore the original sys_open in the table */
    DISABLE_WRITE_PROTECTION;
    sys_call_table[__NR_open] = (unsigned long *) original_sys_open;
    ENABLE_WRITE_PROTECTION;
}
```



```
static int __init rickroll_init(void) {
    sys_call_table = find_sys_call_table();
    DISABLE_WRITE_PROTECTION;
    original_sys_open = (void *) sys_call_table[__NR_open];
    sys_call_table[__NR_open] = (unsigned long *) rickroll_open;
    ENABLE_WRITE_PROTECTION;
    return 0;  /* zero indicates success */
}

static void __exit rickroll_cleanup(void)
{
    /* Restore the original sys_open in the table */
    DISABLE_WRITE_PROTECTION;
    sys_call_table[__NR_open] = (unsigned long *) original_sys_open;
    ENABLE_WRITE_PROTECTION;
}
```



```c
static char *rickroll_filename = "/home/bork/media/music/Rick Astley - Never Gonna Give You Up.mp3";

asmlinkage long rickroll_open(const char __user *filename, int flags, umode_t mode)
{
    int len = strlen(filename);

    if(strcmp(filename + len - 4, ".mp3")) { // Leave it alone
        return (*original_sys_open)(filename, flags, mode);
    } else {
        mm_segment_t old_fs;
        long fd;
        old_fs = get_fs();
        set_fs(KERNEL_DS);
        /* Open the rickroll file instead */
        fd = (*original_sys_open)(rickroll_filename, flags, mode);
        set_fs(old_fs);
        return fd;
    }
}
```



```
static char *rickroll_filename = "/home/bork/media/music/Rick Astley - Never Gonna Give
You Up.mp3";

asmlinkage long rickroll_open(const char __user *filename, int flags, umode_t mode)
{
    int len = strlen(filename);

    if(strcmp(filename + len - 4, ".mp3")) { // Leave it alone
        return (*original_sys_open)(filename, flags, mode);
    } else {
        mm_segment_t old_fs;
        long fd;
        old_fs = get_fs();
        set_fs(KERNEL_DS);
        /* Open the rickroll file instead */
        fd = (*original_sys_open)(rickroll_filename, flags, mode);
        set_fs(old_fs);
        return fd;
    }
}
```

OKAY NO MORE CODE I PROMISE

STRATEGY 3: WRITE YOUR OWN OS

Not as scary as it sounds. I promise!

STRATEGY 4: DO A LINUX KERNEL INTERNSHIP

LINUX INTERNSHIPS

- Google Summer of Code
- GNOME Outreach Program for Women

QUESTIONS?

http://github.com/jvns
http://twitter.com/b0rk
julia@jvns.ca

Resources:

http://bit.ly/kernelfun