

Project 3 Write Up

Lawrence Chau

November 10, 2014

What do you think the main point of this assignment is?

I think the main point of this assignment is to learn about block devices, device drivers, and Linux Crypto API.

How did you personally approach the problem? Design decisions, algorithm, etc.

To implement the encrypted block device, we had to start off by breaking the project into two bits. First, we have to write a RAM Disk device driver which allocates a chunk of memory as a block device. Second, we need to make sure the block device encrypts and decrypts data. Although we had no idea how to write a device driver, the link to the *Linux Device Driver* proved to be a useful resource as it lead us to the source code for simple block driver. The code contained the instructions for initializing the block, setup of the generic disk, the requesting method, and the shutting down. Upon compilation, we recieved a few errors and warnings which were easily fixed by referring to a blog post written by Pat Paterson. His fixes were meant to port the source to Linux versions greater than 2.6.0. Finally, we had to a little more research to find out how to implement the cipher. After looking at a few examples, we were able to implement it in *sbd_transfer* and tried using "Blowfish" as our encryption method, to no success. We ended up using a for loop to have the cipher be encrypted and decryped a byte at a time.

How did you ensure your solution was correct? Testing details, for instance.

To ensure that our solution was correct, we inserted printk statements in our code that would display unsigned characters before and after the encryption process. The encrypted data was a jumble of unsigned characters that became more jumbled after the decryption.

What did you learn?

We learned how the importance of reusing kernel code and the simplest part of the encryption process.