Kevin Chen

Assignment 2.3

My reference monitor had a number of different vulnerabilities that I had not really accounted for during initial design. Some of these vulnerabilities were design choices that I made that I didn't realize would cause a vulnerability. For example, one of the major flaws in my reference monitor was that I did not handle trying operations on a closed file correctly. My reference monitor avoided raising an exception while the correct behavior was to raise an exception, which I did not know. The fix for this vulnerability was to raise a file closed exception in the correct places when trying to perform an operation on a closed file.

Another major flaw that my reference monitor had was handling write inputs outside of the norm, which included negative offsets as well as offsets that were larger than the current file size. I had just not accounted for this during my initial design but this was easy to fix by keeping track of current file size and raising an exception in the event of negative offset input. Another similar vulnerability I had was handling read inputs outside of the norm which included negative bytes to be read, negative offsets as well as offsets that were larger than the current file size. This was fixed by tracking current file size like in the write issue previously mentioned as well as checking byte and offset input before starting any operations.

Another big vulnerability in my reference monitor is my handling of threads. I had not considered threads when I was initially designing my security layer so my reference monitor had some concurrency issues. This was fairly easily solved by adding locks into my reference monitor so that only 1 thread could be modifying or reading a file at a time.

Additionally, another flaw that I had also not accounted for was what happens if someone closes and then reopens the same file. The issue with this particular action is that I had not kept track of file size so I could not tell whether or not someone had a valid offset in a writeat operation so this issue was solved reading from the file at the time of creation to learn about the size of the file before any operations happen.