Pratham Gupta pg2441

CSGY 6813: Internet, Security and Privacy
Assignment 2 Part 3

Vulnerabilities

There were some vulnerabilities in the reference monitor such as:

1. Error Handling:

   Instead of raising valid exception, my reference monitor handled the error, but I did not raise any valid exception. Any exception handled by the code, was not thrown even if it was a valid exception. Exceptions such as RepyArgumentError or InvalidFilenameError, were handled by the code but not thrown correctly. This is a vulnerability as, if the reference monitor was not working properly by some valid user, they would not be able to properly verify where and what is wrong with the way they are using the reference monitor.

2. End of file error:

   Another error in my code was that if anyone wanted to write at a place which was after the file was ended or if they used writeat before another valid writeat we need to save the filesize for that as well, because if they give an offset which is greater than that of the writeat which has still not been written, it should be an error which was not handled by the case in my reference monitor.

Fixing Reference Monitor:

The vulnerabilities discussed above were fixed in the following manner:

1. Error Handling:

   In this case, I had previously used try, except, finally to completely bypass any errors thrown by the code, but instead of just bypassing the code, I used the except clause to raise valid exceptions regarding the error being given. All valid exceptions are being thrown in the code now and if a valid user encounters an error, they would be able to see the valid exceptions and see the trace for any valid error which would be given by the repy branch as well.

2. End of file error:

   I used a new variable named, future_filesize which would be able to save the offset which would be present when a writeat is not yet committed, this future_filesize would be able to help the reference monitor to remember where the offset limit should be for the next writeat function. This future_filesize resets to the filesize once undo functionality is called so that it is forgotten once the uncommitted writeat has been revoked.