Jia Lin Weng
CS-UY 3923

Rationale on Vulnerabilities

In the updated version of my reference monitor, I added checks, locks and error handling while maintaining accuracy and efficiency. Firstly, I added four new globals, file_size, pending_filesize, lock, and is_closed. File_size and pending_filesize are checked after opening a file using the length of bytes read by readat and setting the initial pending_filesize to that as well so that writeat can be performed without problems. Locks are implemented to prevent race conditions. Before an operation can start, it must obtain the lock and release it after it's done with the lock. This is done by using the try and finally blocks. Is_closed ensures that no modifications can be made after a file is closed.

In writeat, I modified where offset < 0 to raise AurgumentError as expected then check if the offset is greater than the pending offset handling EOF errors. Then I made sure that the file size is updated to the correct size.

In undo, I made sure that the pending offset was reverted back to the previous file size as well.

In close, after committing the writeat, I removed all previously stored data on a file when it’s closed to ensure attackers cannot recreate a file with the same name and obtain the states.