Farhan Khan, fkk2008
CS-UY 3923: Computer Security

Addressing Vulnerabilities and Enhancing Debugging in the RepyV2 Reference Monitor

In the assignment, I handled the vulnerabilities in 4 key areas:

1. Basic Functionality: My code had a lot of random log statements on errors, which I later understood was not meant to be logged but rather raised according to most other reference monitors and the assignment prompt. That had to be fixed first. The basic functions of the undo() and writeat() command were implemented in 2.1, in 2.3 I removed some of the redundant input validation checks that were already built in to the library functions.
2. Error Handling and Hierarchy: The primary problem I had was with managing the proper error hierarchies, and hence a lot of attack cases bypassed my code when testing for the appropriate errors. And a lot of errors were handled initially using the general Exception class, I changed it to more specific ones later.
3. Thread handling: This was the most difficult part, as I had zero experience with parallel computing, locks and thread synchronization. This is the first time I've learnt the concept, and therefore implementing locks in the final version of the reference monitor fixed the majority of the test cases that were bypassing my monitor.
4. Unhandled Problem: There is a specific threading problem, where each thread executes multiple functions. I could not identify a way of handling that without directly changing the thread structure itself. If I was expected to make sure that a thread executes **all** of the different functions inside it before another thread gets executed, that has been a problem. Case in point: kp3291_attackcase5