CSE 543- Computer Security

Project 2: Implementing Integrity Access Control Monitor

Date: October 16, 2022

Student Name: Md Rafi Ur Rashid

Answers to Project Questions:

Q1.

Although p2 had a low integrity level initially, meanwhile it is changed to high (after its execution on f2) integrity level and on the other hand f1 has low integrity level. Since Biba policy doesn’t allow any read down, hence we don’t let process p2 read the file f1.

Q2.

Simply because MIC policy allows all reads.

Q3.

p11 has system(high) integrity level, where f1’s integrity level is user (low). Since MIC policy doesn’t allow any execution down, hence we don’t let process p11 execute the file f1.

Q4.

LOMAC policy allows a process’s integrity level be changed to the executed file’s level that has the lowest integrity level. Here, p11 has high integrity level, where f1’s integrity level is low. Hence, we allow p11 change its integrity level to low for executing f1.

Q5.

At the first write, both p2 and f3 had high integrity level, so p2 was allowed to write f3. Before the 2nd write, meanwhile p2’s integrity level is changed to low. However, according to LOMAC policy, file f3 now can not change its level to low. Thus, write is not allowed this time. Again, before the 3rd write, f3’s integrity level is changed to low. Since, p2 is already holding low level, now write is allowed.