Thesis Progress Report 3

Aytar Akdemir
150170115

December 1, 2021

1 Superviser Input - 17.11.2021

1.1 Multilevel Security Review

It was defined in the Rainbow series published by the United States Department of Defense. Trusted Computer System Evaluation Criteria that i found belongs in the Rainbow series.

What MLS essentially is the intersection of the Biba Integrity Model and the Bell-LaPadula Confidentiality Model. This leaves us with a system in which every subject can only access to its security level. There is no communication between security levels.

To perform that communication without leaving the system open to attacks, Policy Enfrocement Points are used between every security level. We assume that the PEPs are completely secure. The reason for privilege escalation is the need for communication between the security levels.

Even though we assumed PEP is completely secure, the programs used in the Operationg System generally have vulnerabilities. For example, a program might perform privilege escalationin order to function. If an attacker gains access to said program, they will access to the higher security level. In out simulation, we will assume that the system damage is caused by using insecure programs.

Insecure Program Example: On Linux, a daemon mail client named Sendmail had root access and it worked continuously on the background. In a case of intrusion to the Sendmail, the attacker might gain root privileges.

1.2 Formalizations

Subjects access to the objects using processes. Subject will transfer its privileges to the process it intends to run. When the process is trying to access to the subjects, OS applies PEP to the process. Newer OSes have their own PEPs while older OSes need PEPs developed on top of them.

We talked about four possible formalization techniques for the simulation.

- Clark Wilson - Graph based
- Take-Grant - Graph based
- State Machine - It allows certain states.
- Petri Net

Main problem with the graph based formalizations is the complexity. In order to compute all the access possibilites we also need to sacrifice a big chunk of memory. We need to use a combination to find a formalization technique with a reasonable complexity. Penetration testing that I mentioned in the literature review might be a key to this. Fuzzer is another option for detecting vulnerabilities.