Department of Electrical Engineering and Computer Science
Syracuse University

Reference Monitor Lab

Overview

Since its 1972 introduction in the "Anderson Report", the Reference Monitor (RM) concept has proved itself to be a useful tool for computer security practitioners. It has been the only effective tool we know of for describing the abstract requirements of secure system design and implementation. By learning the Reference Monitor concept, students are equipped with an essential tool for constructing and assessing the effectiveness and assurance of security policy enforcement in automated systems.

A Reference Monitor should have the following properties:

- It must be always invoked, i.e., every access is mediated.
- It must be tamperproof. It is impossible for a penetrator to attack the access mediation mechanism such that the required access checks are not performed and authorizations not enforced.
- It must be small enough to be subject to analysis and test, the completness of which can be assured.

The goal of this lab is to help students understand the Reference Monitor concept, see how a real Reference Monitor is implemented, and evaluate the Reference Monitor. We have designed 3 sub-labs, each with a different focus and a different difficulty level.

Sub-Lab 1: Analyzing and Playing with Reference Monitor

The goal of this lab is to understand the Reference Monitor concept and its properties. We use Minix's reference monitor as an example system. Students need to accomplish the following tasks:

1. Find out where the RM is and how RM works in Minix. Try the followings:
    a. Disabling some access controls, and see how that affect the security of Minix.
    b. Add some ad hoc mandatory access control.
2. Derive the security policies for the Minix operating system.
3. Find out the security policies enforced by Minix's Reference Monitor. Are these enforced security policies the same as the one you derived? Are there other places where part of the security policies are enforced? Can we consolidate them into the Reference Monitor?
4. What security policies are not enforced by the Minix Reference Monitor (hint: memory protection, etc.)?
5. Evaluate whether the RM in Minix possesses the three properties or not. How are these properties satisfied? Are there ways to bypass access control? Students need to exam both software and hadware.
6. Justify whether Minix's RM design is good or not.

Submission: Students need to submit a detailed report to describe their findings, analysis, and conclusions. In the report, students also need to propose how to improve the Reference Monitor in

Minix.

Sub-Lab 2: Testing Reference Monitor

Students are given a RM implementation and the security policy. They need to conduct black-box testing (they do not have source code) on this RM to find out whether it correctly enforced the policy. Students need to develop their testing hypothesis and scenarios. We will inject the following well-known vulnerabilities into RM:

- Incomplete Mediation: there are holes in the RM; some policies are not enforced and some policies can be bypassed.
- Not Tamperproofing: we will introduce holes into Minix to make the RM not tamperproofing.
- The vulnerabilities we introduced should include both design errors and implementaiton errors. Some potential mplementation errors are the following:
  - boundary values
  - buffer overflow
  - loophole

After the black-box testing, we will give the source code to students, so students can further test the RM using white-box testing methods.

This project is a suitable project for Computer Security, Software Engineering, and Operating System courses.

Sub-Lab 3: Improving Reference Monitor

There are many places in Minix where access control is conducted. For instance, chmod, chroot, etc., Please find them out. Is this a good design? If not, please modify the RM of Minix, and make it better. (hint: more general, policy should be in one place, rather than scattering all over the places)

Helpful Documents

- The Anderson Report (1972)