CPS499-Frida

Computer Security Course Final Project -- This topic involves using a JavaScript framework called Frida to do in-line reference monitoring on lower-level code (at the assembly and C level). The JS framework will be used in a Python script.

Project Proposal

0. CPS499-Frida | Evan Krimpenfort and Anna Duricy

1. Summary of Background

This final project is a case study of an injection framework called Frida. Their website https://frida.re has explicit documentation on use cases and documents on their APIs. We are going to be examining AOP inside of in-line reference monitors, similarly to the Shopping Cart Problem seen in Lab I and Assignment I. Since Frida is more focused on the the lower-level works, we will be writing a program in C that has vulnerabilities similar to ShoppingCart.java. Then, like Assignment I, we will fix the program with Frida.

2. Project objectives

This program will be graded on a few things.

- Was Frida easier to use than AspectJ?
- Does it have the same capabilities as AspectJ?
- Does it work well as a reference monitor? And...
- Are there things that Frida can do better?

3. Expected contributions and the relevance to the course topics

Our contributions to the course will be in regards to be *IRMs, AOP, Data Races,* and *Protection in Software*.

4. Your group plan: how your group members contribute to the project, the work plan.

Anna and Evan will work together through each of these sections. The work plan will be as such:

- **A.** Recreate a program like *ShoppingCart.java*.
    - **A.1** Lay out the data race vulnerability while creating the program.
- **B.** Create the Python script that will run the Frida script.
- **C.** Design the Frida script and see if it can completely fix the problems that ShoppingCart.java had (Assignment I).
    - **C.1** If Frida *can't*, we will both go back and make any necessary changes to the code so that Frida **can** fix the code.
    - **C.2** If Frida *can*, then we will show how it completely fixed the program.
- **D.** Write the final report on our solution.

5. Timeline: Particular intermediate tasks and timeframe to complete the task. The time starts from proposal approval to the final report deadline.

- Task A should take 3 weeks.
- Task B should take 1 week.
- Task C should take 2-3 weeks (depending on Frida's capabilities).
- Task D should take 1 week.