

Long Nguyen

Academic Perspective:

The main takeaway of the project is being an aid for reverse engineers to decipher obfuscated applications. From my perspective, it is a way for me to explore the field of reverse engineering and hone my existing skills from the Malware Analysis class. Additionally, this project has the biggest scope of any of my individual projects. This serves as a test and way for me to practice project management skills so that everything is completed on time and that roadblocks are addressed accordingly. Lastly, this project will be a culmination of all the software engineering and computer science principles that I have learned throughout my academic career. While the courses are a way for me to learn and have a preliminary practice of such principles, this project serves as a “real-world” way for me to apply them.

Curriculum

The courses most relevant to this project are Intro to Comp. Sys. (CS2011) and Malware Analysis(CS5138/6038). Through CS2011, I learned how low level computing works and how to debug and understand assembly level code. These skills will be used as a foundation for the system as understanding how programs/code work at a fundamental level is a prerequisite for reverse engineering. CS5138 taught me how to examine 3rd party executables and reverse engineer their functions and features. This insight can be brought into the project because the users will be examining executables using this system. The perspective learned in this class shows me what someone could want out of a system like the one we are developing.

Co-op

The most relevant co-op experience(3 rotations) for this project was my time as a Software Development R&D Co-op at Siemens. Through my time there, I experimented with the capabilities of cutting edge AI models and how far they can truly stretch. This experience is directly applicable to the ai-augmentation that the system is aiming to implement. Specifically, it allows me to set realistic expectations for the capability of AI and serves as a foundation on how to train/set up a more specialized AI for reverse engineering. Additionally, the project-based structure of my internship teaches me how to plan and implement features in a timely manner, which can be applied to the senior design project. Lastly, learning how to work with a team productively is another thing I learned through the shared projects in my experience. While the senior design project only consists of two people, my experiences can still be applied as expectations, roles, and communication methods can be set accordingly.

Motivation

The motivation behind this project is my interest in reverse engineering applications. There is a particular community I'm a part of where reverse engineering is used to modify video games. The issue is that reverse engineering a video game is difficult as you don't have the source code to work with and that the executable may be obfuscated. By pursuing this project, I aim to find a way to make reverse engineering less tedious and time-consuming. Additionally, the process of making a tool that can aid in reverse engineering will serve as an opportunity to learn more

about reverse engineering. Lastly, the specific point of reverse engineering malware is important because malware is obfuscated. If I can make a tool that aids in reverse engineering malware, that means the tool can also reverse engineer obfuscated applications.

Preliminary Approach

The preliminary approach will be broken down to two main components. The first component is the malware analysis component of the system. The starting point will be making a tool that can provide static and dynamic analysis. The second component is the ai-augmentation component of the system. The starting point for this component would be feeding an AI model low level code constructs to see how its malware analysis capabilities could be improved. The expected results and accomplishments are a functioning malware analysis system that utilizes ai-augmentation to reduce the tediousness and time-consuming nature of reverse engineering. The self-evaluation will be pretty straightforward as the contract will contain milestones that we should complete by a certain deadline. Whether we do a good job is also straightforward because there is only a set list of features that we want completed. If those features are completed, we have accomplished our goal.