**CSE 2431 Team Project**

Jacob Grove

Henry Karagory

Ian Yang

**Objective:**

Our goal is to create a malware scanner. The user of the program will have the ability to trigger a scan of currently running processes to search for a “bad” process. These processes will be identified if they match a user supplied regular expression or match any of a series of user supplied tokens. The program will automatically attempt to kill any process identified by the search. Killing the process will only be performed if the process can be killed safely. Additionally, the program will support a few other features. The scanner will be able to search through files that are formatted to execute instructions on Linux, and quarantine them if they meet the above criteria. Additionally, the user will be able to schedule automatic searches to run in the background at set times.

**Progress:**

So far, we have created a program entirely in the user space that can loop through files and process and identify those with a name that matches a user provided regular expression. We have enabled the ability to specify where the search criteria come from and how they are created. Search criteria could be passed to through program through command line arguments, program prompts, or a configuration file. Also, we have started to research the implementation of system calls. We have identified several tutorials and online technical documents to teach ourselves how to develop new system calls for Linux.

**Goals:**

The next steps that the team will make in completing this project are to begin development of the system calls that will search through the running processes to identify processes specified by the user and perform user specified actions on those processes and to incorporate these system calls in the user space program. We are still trying to identify to some extent how the work should be split among the Linux kernel and the user space. Additionally, we are trying to design a program package to be able to easily inject test examples into the OS. We will be visiting office hours soon in order to discuss some implementation specifics and ensure that our ideas regarding system calls are correct and will work in the context of our project.