Research Progress Report

Topic: **seL4 Emulation on Linux**

Student Name: Jiawei Gao

ZID: z5242283

Date: **Mar.5 (Week 3)**

Summary of this week

For week3, I mainly focused on two tasks:

- Collecting some useful resources for to gain some ideas:

  So far, I found:

  1. WSL (Windows Subsystem for Linux) version 1 does a similar job but unfortunately this is a close-source project.
  2. Qemu has a user-space emulation mode and is open source as well. I'm trying to understand how does Qemu works. Although Qemu is a big and complex project, eventually I will need to analyze the advantages and disadvantages of Qemu comparing to my emulation framework.
  3. Wine which is a compatibility layer translates WinAPI to POSIX/Linux APIs. This is another useful reference project. To gain some idea, I started looking at Wine's architecture design and how does it translate the syscalls.

- Thinking of a very basic implementation:

  After getting some ideas from Wine, the first step I'd like to try is to find a way to redirect the syscall from seL4 to Linux syscall. To achieve this, I came out with three approaches so far: 1) Change the seL4 source code, and make it directly call the emulation framework. 2) Using `ptrace()` to trace to syscall from seL4 then try to emulate it with Linux syscall. 3) Developing a kernel module to redirect the syscall from seL4. (I won't try this approach unless the previous two don't work, as developing a kernel module is very difficult).

Plan for next week

For the next coming week, I will focus on the following tasks (the order is from the most important to the least important task):

1. Reviewing the seL4 Documentation and trying to understand some details about the syscall routine in seL4.
2. Continue collecting some test suits which can be useful for monitoring syscall behavior from seL4Test, AOS project, etc.
3. Continue studying the `ptrace()` syscall of Linux to see if I can leverage that to the syscall redirection.
4. Continue learning some internal implementation of Qemu.

Time Table

(This will be my ideal timetable, the real progress will be assessed in the next week's report).

Day	Task
Sat	Reviewing seL4 Doc about syscalls + Collecting useful applications
Sun	Continue Sat task
Mon	Continue Sat task + All Hands Meeting
Tue	Learning `ptrace()` syscall
Wed	Continue Tue task
Thu	Writing the progress Report + learning Qemu + Weekly Sync Meetings with Axel
Fri	System meeting + Progress Report