EE/CPRE/SE 492 BI-WEEKLY REPORT 04

March 24 – April 7

Group number: 16

Project title: Robustness of Microarchitecture Attacks/Malware Detection Tools against Adversarial Artificial Intelligence Attacks

Client &/Advisor: Berk Gulmezoglu

Team Members:

Shi Yong Goh

Connor McLoud

Felipe Bautista Salamanca

Kevin Lin

Liam Anderson

Eduardo Robles

- **Bi-Weekly Summary:**
  - Since our last bi-weekly report submission, we have once again met with our advisor twice and have discussed how to proceed and what to prioritize as the semester draws to an end. As previously mentioned, finishing the original scope of our project is no longer possible and so we will be prioritizing additional error handling / console logging in the GUI, finish profiling x86 instructions utilizing other ports, changing the endpoint connection from the UI to the laptop we've been using to test the model, and beginning to assemble our final presentation.

- **Previous Week's Accomplishments:**
  - Shi Yong Goh:
    - □ Profiled the instructions that used different port to observe whether running these instructions can increase the power consumption
    - □ Tried to apply the instructions that used different port to run on the source code and observed the performance
  - Connor Mcloud:
    - □ Re-familiarized myself with where we at in the project after my time spent in hospital
    - □ Began looking into implementing console log in the GUI for error handling
  - Felipe Bautista:
    - □ Created a function which read the log file created by the attack executed
    - □ Began implementing an algorithm which searched for possible error keywords in the logs and extracts the message generated by the error and display it to the

user in the UI’s console.

- Kevin Lin:
    - □ Looked into using multiple different instructions in a row (utilizing different ports) to see if more power consumption could be used.
    - □ Presented results of this experimentation.
- Eduardo Robles:
    - □ Combined different instructions into the attack code and documented results and graphs
- Liam Anderson:
    - □ Started working on a python program to insert code and create C programs to generate test that will help profile x86 instructions
    - □ Tested using multiple ports on power consumption
    - □ Presented current progress on automated testing program to see if it is worth continue developing

- **<u>Pending Issues:</u>**
    - Shi Yong Goh: N/A
    - Connor Mcloud: N/A
    - Felipe Bautista: N/A
    - Kevin Lin: Ran into an issue where program took way too long to run after inserting ASM inline code.
    - Eduardo Robles: N/A
    - Liam Anderson:
        - □ Some issues with generated test (not compiling)
        - □ Receiving inconsistent data

Individual Contributions:

Team Member Names	**Individual Contributions**	**Hours** (this week)	**HOURS** (cumulative)
Shi Yong Goh	Used instruction profiling to observe the performance of difference instructions. Compared execution time.	10	58
Connor Mcloud	Work on error logging and tracking for the GUI.	5	48
Felipe Bautista	Implemented function to parse the attack's log file. Began working on an algorithm to extract error messages from the log file	8	52
Kevin Lin	Trying out consecutive x86 instructions in order to stimulate using various ports.	10	62
Eduardo Robles	Created multiple C codes to profile different x86 instructions	8	48
Liam Anderson	Worked on developing a python program that will can insert C code and generate programs to profile x86 power consumption	10	78

Plans for the Upcoming Week:

- Shi Yong Goh:
  - □ Continue trying to run some tests using the combination of the instructions that use different ports
  - □ Will try to use different registers and assign value to the registers
- Connor Mcloud:
  - □ Help Felipe with error handling and find out what needs to be implemented still.
- Felipe Bautista:
  - □ Continue working on the error searching logic. Continue to search and identify more error keywords that can be used by the algorithm
- Kevin Lin: Trying out more instructions and chaining them together to see if there is any more power consumption beyond the norm.
- Eduardo Robles:
  - □ Continue to profile different combination of instructions .
- Liam Anderson:
  - □ Continue to develop the automated testing script

Summary of Weekly Advisor Meeting:

Our advisor suggested that we begin working on the poster because he will be traveling in early May. Additionally, he wants us ensure nobody uses the laptop while collecting the data. To ensure this, we created a Teams channel to better communicate with the advisor and his teaching assistant (rather than email).