
EE/CPRE/SE 492 BI-WEEKLY REPORT 03

February 18 – March 4

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, we have met with our advisor twice and discussed our current progress as well as what we'll be working on next. This past two weeks the team prioritize profiling different x86 instructions and see how it affected the laptop's power consumption. We have determined this task is taking way longer than expected and we have been having discussion with our client to see which instructions to prioritize as our project is quickly coming to an end. The UI is also on its last stages of development and testing. Our client has informed the UI team that he wants to change the current endpoint of connection from the UI to the testing laptop but he will reveal more details in the upcoming weeks.

- **Previous Week's Accomplishments:**
  - Shi Yong Goh:
    - Tested the instruction profiling and used instruction profiling to observe various instructions performance, including the power consumption and execution time.
    - Compared the attack code's execution time, instructions 'execution time and the attack code's execution time after adding the instructions as noise.
  - Connor Mcloud:
    - Worked on error logging for the GUI.
  - Felipe Bautista:
    - Implemented the console that will display the logs that occurred during executing an attack. Using the log file and implement some error catching conditions that will tell the users if any error cause the attack to not execute and fail.

- Kevin Lin:
    - Testing instruction profiling in order to further observe power consumption and time difference. Reporting results to advisor to view next steps.
- Eduardo Robles:
    - Added more C codes to profile different x86 instructions.
- Liam Anderson:
    - Worked on instruction profiling. Generated scripts to automate process. Created various C codes. Ran tests and reported results back to advisor / client

- **Pending Issues:**
    - Shi Yong Goh: Having issues to run the attack code on instruction profiling.
    - Connor Mcloud: N/A
    - Felipe Bautista:
        - Our client mentioned he wants to make changes to the UI to connect to a sever that will run the attacks and collect the power measures instead of the laptop we are currently using. I'm currently waiting on his approval to begin making the changes to the connect and change the communication endpoints.
    - Kevin Lin: N/A
    - Eduardo Robles: N/A
    - Liam Anderson: N/A

- **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.	6	48
Connor Mcloud	Work on error logging and tracking for the GUI.	6	43
Felipe Bautista	Implemented console display widget on the UI which displays the runtime logs of an attack. Implemented error handling conditions.	6	44
Kevin Lin	Profiled various instructions to observe power consumption of different instruction. Focus on floating point instructions.	6	52
Eduardo Robles	Created multiple C codes to profile different x86 instructions	6	40
Liam Anderson	Created script to automate data collection and created 9 C codes for 9 different instructions profiling testes	10	68

- **Plans for the Upcoming Week:**
  - Shi Yong Goh:
    - Planning to create an execution time report of various instruction and the attack code.
  - Connor Mcloud:
    - Continue working on error logging for the GUI.
  - Felipe Bautista:
    - Integrate the error handling logic created by Connor with the UI console widget
  - Kevin Lin:
    - Working on creating more C codes to add to new instruction profiling efforts. Look into using various ports in x86 instruction as they may generate more power usage.
  - Eduardo Robles:
    - Continue to add C codes and create a spreadsheet with the results of testing.
  - Liam Anderson:
    - Specific instructs where suggested by our advisor to try testing next so I plan on doing that this week. Also, would like see if it is possible to automate the C code creation. There is lots of instructions to test and doing it all by hand is very time consuming

- **Summary of Weekly Advisor Meeting:**

During the weekly advisor meeting, we delved into a stimulating discussion on how to streamline the process of creating instruction C codes. With an aim to optimize efficiency, the team explored potential avenues for automating this process. Additionally, we identified the key instructions that we should prioritize for development in the upcoming weeks, as they move closer towards the project's completion. As the discussion progressed, the team also shared their experiences and highlighted some of the challenges we were facing while working with x86 assembly. With only a couple of months left until the project's conclusion, the we mapped out a plan on how to efficiently allocate our time and resources to achieve our goals.