
EE/CPRE/SE 492 BI-WEEKLY REPORT 1

January 17 – February

18 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

- **Bi-Weekly Summary:** After winter break, we started the senior design efforts again with a meeting on January 24th with everyone involved in the project. We discussed our current design and any changes made. We revisited the project's objectives, requirements, and schedule to decide the next steps needed to be made. From there, we spent the next three weeks working on the project. We further developed the GUI and got it to a state where it can successfully collect data, test it on the ML model, and show results. We created scripts to automate data collection and analysis to help with testing and instruction profiling. Lastly, we were able to alter an attack's power signature with various instructions and fool the ML model, which gave us more insight into how to create adversarial examples.

- **Previous Week's Accomplishments:**
  - Shi Yong Goh:
    - Worked on collecting power consumption data of specter attack source code.
    - Added instruction to the source code and observed the instructions code affects the accuracy of the ML model
    - Reported laptop connectivity issues to TA
  - Connor Mcloud:
    - Attempted to fix python3 and pyQt6 on ubuntu so I can access the GUI on my own computer again.
    - Worked on various elements of the GUI's implementation features & design. Currently looking for & researching more ways to improve the overall design & usability while building on top of the excellent foundation Felipe has provided.
  - Felipe Bautista:
    - Implement various GUI features such as attack definition dropdown, upload file Widget, Input boxes for number of executions of attack and time in between executions. Also run button which runs the attack uploaded.

        - Created various functions that allow the widget to do their job such as file upload, running the attack and format results files
        - Connected the GUI to the remote laptop and server using bash scripts
        - Implemented Results page which allows the users to see the results of the attack executed on the remote laptop and tested on the detection model
- Kevin Lin:
    - Work on testing instruction profiling by testing various x86 instructions
    - Compare results on ML model
- Eduardo Robles:
    - Worked on collecting and formatting power consumption data of the attack code.
    - Added x86 instructions to the attack code to affect the power consumption
    - Tested data with the ML model to check accuracy
- Liam Anderson:
    - Updated scripts to help with testing and instruction profiling efforts
    - Troubleshot power signature collection errors.
    - Tested attack code variants on ML model

- **Pending Issues:**
- Shi Yong Goh:
    - Have not found out the shortest sleep time affects the ML model, will continue find out next week
    - Have not successfully used the latest GUI to collect the data because was having issues on the ssh key. I will try again next week.
    - Tried to understand which instruction to put in the code.
- Connor Mcloud:
    - A persisting Python error is preventing the GUI from launching on personal workstation.
- Felipe Bautista:
    - N/A
- Kevin Lin:
    - MATLAB was forced to deactivate on my Linux machine, which prevented access to viewing .fig files to compare results in a time efficient way. Relatively minor inconvenience.
- Eduardo Robles:
    - Some of the x86 instructions where more difficult to understand and use properly
    - Had problems with GitHub which prevented my ability to push or pull from the repository
- Liam Anderson: N/A

- **Individual Contributions:**

Team Member Names	Individual Contributions	Hours (this week)	HOURS (cumulative)
Shi Yong Goh	Collected data and found the instructions affects the ML model results. Helped to test the GUI.	7	7
Connor Mcloud	GUI research, development, & debugging	6	6
Felipe Bautista	GUI development and fixes	10	10
Kevin Lin	Profiling x86 instructions (specifically add), testing of the new retrained ML model.	7	7
Eduardo Robles	Tested on different x86 instructions and checking the accuracy against the ML model	6	6
Liam Anderson	Created scripts for data collection and analysis. Progressed on instruction profiling	10	10

- **Plans for the Upcoming Week:**
  - Shi Yong Goh:
    - Finding out the shortest sleep time/ the minimum number of instructions affects the ML model
    - Trying different instruction code from the research paper
  - Connor Mcloud:
    - Assist Felipe further in GUI development process.
    - Research fixes/solutions to current issues in design, apperance, and usability.
    - Implement warnings & error reporting into the GUI's framework, most likely to be designed as some sort of notification or pop-up window.
  - Felipe Bautista:
    - Implement a feature which allows the user to select which run mode they want
    - Improve the GUI appearance
    - Refactor some areas of code to improve run time
  - Kevin Lin:
    - Testing out minimum number of instructions that creates a noticeable difference in the accuracy of the machine learning model.
    - Doing this with various instructions that use more power than arithmetic operations.
  - Eduardo Robles:
    - Working with vector x86 instructions alter the power consumption data
  - Liam Anderson:
    - Test other x86 instruction specifically ones that will have higher power consumption

- **Summary of Weekly Advisor Meeting:** According to Professor Berk, we will receive a new attack to focus on in the coming week, and going forward, two people will collaborate on each attack. In addition, he recommended a research paper to help us explore various code snippets for different Intel instructions. He encouraged us to experiment with the instructions he provided and

see what we can discover.