sdmay23-16: Robustness of Microarchitecture Attacks/Malware Detection Tools against Advers
Week 8 Report
November 20 - November 27

Team Members

Kevin Lin — *Machine Learning Lead*
Liam Anderson — *Internal Logic Lead*
Shi Yong Goh — *Internal Logic Member*
Connor McLoud — *OS Lead*
Eduardo Robles — *Internal Logic Member*
Eduardo Robles — *UI Lead*

Summary of Progress this Report

Continuation of last week -adding more instructions into spectre source code. Comparison of benign application power set to spectre attack. Working on GUI.

Pending Issues

Figuring out how to get spectre attack to act directly/change pattern.

Plans for Upcoming Reporting Period

Work on modifying source code with instructions. Work on GUI.

Individual Contributions

Team Member	Contribution	Weekly Hours	Total Hours
Kevin Lin	Working on understanding the ML model trained with TensorFlow on the server.	7	0
Liam Anderson	Led analysis and insertion of x86 instructions to spectre code	8	0
Shi Yong Goh	Analysis of x86 instructions in spectre code.	7	0
Connor McLoud	Analysis of x86 instructions in spectre code.	7	0
Eduardo Robles	Analysis of x86 instructions in spectre code.	7	
Eduardo Robles	Worked on GUI.	7	

Gitlab Activity Summary

Nothing to report.