EE / CprE / SE 491 – sdmay21-09

Instruction Level Reverse Engineering through EM Side Channel

Week 3 Report

2/22/2021 - 3/1/2021

Client: Akhilesh Tyagi

Faculty Advisor: Akhilesh Tyagi

Team Members:

Noah Berthusen — *Data Analysis Engineer*

Matthew Campbell — *Test Engineer*

Cristian George — *Meeting Scribe*

Jesse Knight — *Signals Processing Engineer*

Evan McKinney — *Integration Engineer*

Jacob Vaughn — *Report Manager*

Weekly Summary

This week we worked on solving the problems that we found with our execution times last week.

Past Week Accomplishments

- New data
  - Collected more data using the new format for a variety of opcodes.
- Rewrote microcontroller firmware
  - Removing arduino support as arduino provides less control over hardware. Arduino did not allow compiling flags, and no way to get disassembled code.
  - Adding more instructions to the code, each instruction will be classified by a different letter code that Matlab can send
- Machine-Learning
  - Confirmed binary classification results with other machine learning, more advanced, machine learning models (such as CNN and DNN). This will be more scalable as we increase the dataset and complexity of the problem.
  - Created an environment in the high-performance computing cluster that we have access to. Should make data processing and training go much faster.
- Python
  - Wrote a simple oscilloscope-to-model pipeline to quickly transform raw data into the type needed for machine learning.

Pending Issues

- Execution time in between runs is inconsistent.
    - We have disabled compiler optimizations and are trying to generate an assembly file to observe how the compiler is interpreting our code.
    - After meeting with our advisor, we must also begin debugging using a separate software suite.

Individual Contributions

Team Member	Contribution	Weekly Hours	Total Hours
Noah Berthusen	Configuring training pipeline and more environments	4	14
Matthew Campbell	Reading data sheets	2	9
Cristian George	Stepped through Arduino code	3	11
Evan McKinney	Worked with Matched Filter, sktime package	2	15
Jacob Vaughn	Reading data sheets	3	9
Jesse Knight	Rewrote microcontroller code in STMCube	6	16

Plans for Coming Week

- Jesse: Data Collection
    - Collect minimum 10 new opcodes
    - Modify MATLAB code to accommodate controlling more opcodes
    - Redesign antenna
- Cristian: UART Branch Detection
    - Step through STM32 HAL calls for UART to locate any potential branches
    - Identify where a predictive branch may occur during the first iteration of our data collection.
- Jake: Finding opcodes
    - Go through data sheet to find the most relevant opcodes to test
    - Write code for hardware using new opcodes
- ML Team (Evan, Noah):
    - Attempt to achieve decent results for multiclass classification between a small number of opcodes
    - Compare machine learning methods with respect to time trained, accuracy, dataset size

needed, training hardware needed, etc.