EE/CprE/SE 491 BI-WEEKLY REPORT

09/13/2021-09/27/2021

Group number: 13

Project title: Adversarial AI to Prevent Microarchitectural Website Detection Attacks

Client &/Advisor: Berk Gulmezoglu

Team Members/Role: Ege Demir, Sean McClannahan, Aaron Anderson, Thane Storley

○ **Bi-Weekly Summary** These past two weeks, our overall goal was to research and think about our plan for this half of the project. We've gained a better understanding of what we want our project to do, and how we want it to work. We've also been working on setting up the deep learning model, and collecting data. Over the next two weeks, we want to do more research into machine learning and understand tools that could help make our project do better.

○ **Past 2 week accomplishments**·

Ege Demir: Worked on debugging the deep learning model, and training it using already existing data. Also, worked on collecting more data. Solved low validation accuracy problem. Increased datapoint period from 2ms to 5 ms, which lowered the size of the dataArray from 15000 to 6000(Due to total measurement time staying same)

- **Aaron Anderson:** Assisted Sean in research and utilization of adversarial AI tools
- **Sean McClannahan:** Continued research on adversarial tools. Currently looking into how Tensorflow.js can be utilized as an adversarial tool, as seen with "Adversarial.js" created by Kenny Song.
- **Thane Storley:** Continued research and noise investigation.

○ **Pending issues**

- **Ege Demir:** Even though validation accuracy has increased substantially, we now have the problem of validation accuracy being too high. I need to collect more websites to see whether this is actually a problem.

Aaron Anderson: Figuring out how to apply image related adversarial AI tools to our linear data set

- **Sean McClannahan:** Can Tensorflow.js and/or Adversarial.js be applied to our project?
- **Thane Storley:** Recovering from a concussion, still limited in my capability to participate.

Project related issues are involving noise insertion and AI research.

- **Individual contributions**

NAME	**Individual Contributions** *(Quick list of contributions. This should be short.)*	**Hours this bi-week**	**HOURS cumulative**
Ege Demir	Model debugging, research, data collection	7	26
Aaron Anderson	Research and theory	5	25
Sean McClannahan	Research and theory	6	20
Thane Storley	Design, research	3	18

- **Plans for the upcoming week**

- **Ege Demir:** Work on understanding and verifying why validation accuracy of the model is this high (almost %100).

- **Aaron Anderson:**

Look into implementation of Kenny Song's adversarial AI library

- **Sean McClannahan:** Continue researching tools to develop Adversarial AI, and help with the development of the AI.
- **Thane Storley:** Continue to research AI and its implementation. Also continuing efforts to implement noise.