EE/CprE/SE 491 BI-WEEKLY REPORT

09/27/2021-10/11/2021

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. Our deep learning model is now functioning how we want it to, so we're moving on to making our adversarial defense. We are splitting into two teams to accomplish this. One team will work on the javascript code, and the other will work on a saliency map.

- **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. Going to start work on a saliency map with Ege soon.
  - **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:** Gaining a clear understanding of saliency maps.
  - **Thane Storley:** Figuring out where to insert noise and how much so it doesn't completely hinder cache usage.

- **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	33
Aaron Anderson	Research and theory	5	30
Sean McClannahan	Research and theory	6	26
Thane Storley	Design, research	6	24

- **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:** Work with Thane on js.
  - **Sean McClannahan:** Work with Ege to start developing a saliency map for our project and continue research.
  - **Thane Storley:** Continue noise development, also plan to work on js.

Meeting with Advisor: We discussed the next steps to take following completion of our neural network.