*EE/CprE/SE 491 BI-WEEKLY REPORT 07*

*09/13/2021-30/08/2021*

*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 developing the deep learning model, debugging it, and training it using already existing data. Also, worked on collecting more data.

- **Aaron Anderson:** Researched and Documented critical information about neural networks for team (wrote notes and posted them to slack for team to read)
- **Sean McClannahan:** Researched machine learning models and how our model in particular works, and looked into tools for developing Adversarial AI effectively.
- **Thane Storley:** Developed a few minor functions in the code for aggregating data. Researched machine learning, and where to potentially introduce noise into our program.

○ **Pending issues**

- **Ege Demir:** Model had problems, especially with validation loss showing NaN. Even though that is taken care of, we still have the problem of having low validation accuracy. One possibility that causes this is the fact that browser timer precision might be too low to actually convey enough information about website memorygram.
- **Aaron Anderson:** Utilization of Adversarial AI (Is it applicable to our project?)
- **Sean McClannahan:** No major complications, want to research further.
- **Thane Storley:** Finding where exactly to implement noise, and generating valid data

- **Individual contributions**

| **NAME** | **Individual Contributions**<br>*(Quick list of contributions. This should be short.)* | **Hours this bi-week** | **HOURS cumulative** |
|---|---|---|---|
| Ege Demir | Model debugging, research, data collection | 8 | 18 |
| Aaron Anderson | Research and theory | 7 | 20 |
| Sean McClannahan | Research | 6 | 14 |
| Thane Storley | Design, research | 6 | 15 |

- **Plans for the upcoming week**

  - **Ege Demir:** Work on understanding why validation accuracy of the model doesn't increase as we train the model. If it is because the dataset size is small, continue to collect more data. If it is not because of that, check if our dataset look similar to previous research's dataset, and try to debug how it differs.
  - **Aaron Anderson:**
    Assist Sean with the research and utilization of the ART adversarial AI code.
  - **Sean McClannahan:** Continue researching tools to develop Adversarial AI, and help with the development of the AI.
  - **Thane Storley:** Divert efforts to assisting with AI research and development, making sure to keep in mind where noise must be introduced.

- **Summary of weekly advisor meeting**

We discussed the current situation of our model, and the importance of finding an Adversarial AI tools we can use online. We've also discussed where we should focus as we try to find exploits that we can introduce noise in. We have discussed the importance of thinking about our model as a black box.