EE/CprE/SE 491 BI-WEEKLY REPORT

10/25/2021-11/08/2021

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 we have worked on saliency maps and cache noise creating code as two different groups.

- **Past 2 week accomplishments**

  Ege Demir: Modified saliency map creator program to generate difference between class saliencies. Created python testing code for saliency map, created different noise simulations

  - **Aaron Anderson:** Testing noise generation prototype
  - **Sean McClannahan:** Helped Ege with research on saliency maps.
  - **Thane Storley:** Have a prototype in testing for noise injection

- **Pending issues**

  - **Ege Demir:** More simulations are required to find exploits in DL model.

  Aaron Anderson: creating high amounts of noise for short time then repeating.

  - **Sean McClannahan:** Gaining a clear understanding of saliency maps.
  - **Thane Storley:** Implementing Saliency map into the noise injection

- **Individual contributions**

NAME	**Individual Contributions** *(Quick list of contributions. This should be short.)*	**Hours this bi-week**	**HOURS cumulative**
Ege Demir	Research & Implementation of Saliency Map & Generation of noise simulators	8	49
Aaron Anderson	JS coding and Research	5	40
Sean McClannahan	Research and theory	6	38
Thane Storley	Design and development of noise JS	7	36

- **Plans for the upcoming week**

• **Ege Demir:** More simulations are required to find exploits in DL model.

• **Aaron Anderson:** finish up noise generation

• **Sean McClannahan:** Continue working with Ege on saliency maps and how to apply them to our project.

• **Thane Storley:** Meet with Aaron to implement saliency data into JS

Meeting with Advisor: Discussed next steps on inducing noise, and results of noise simulations.