Release 0 , Week 2 |Minutes/Report

## 02/10/2019 | 09:00am//14:00pm | Location: NYP@SIT L4E / NYP@SIT UoG Office

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  | | --- | --- | | Meeting called by | Rech Leong | | Type of meeting | Requirements Gathering | | Note taker | Rech Leong | |  |  | | Attendees Rech Leong  Prof. Sye Loong |

# Agenda topics

* + - Requirements Gathering
      * Meeting with Prof. Sye Loong at 2pm (02/10/19)

To give an informal progress update of research findings thus far

Describe the known methods of attacks on neural networks

Describe the ways to mitigate them

Perhaps decide on a scope to focus on for attack and mitigation

Questions to ask:

Should the research findings be documented formally or informally? (latex or word)

To what extent should the research be done

To propose scope of project

Decide which adversarial attack to focus on

Decide if mitigation should be in the scope

|  |  |  |
| --- | --- | --- |
| Notes and Suggestions |  |  |

* First Milestone (4 to 5 weeks)
  + Decide on a model to work on (object/image prediction)
    - Look into Carma AV Dataset
  + Attack chosen should try to be that of data poisoning or something that involves programming work rather than simply manually altering
  + Narrow down research scope to existing attacks rather than coming up with a new one
  + Perhaps have tinyml run on raspberry pi
  + If decided on AV, make a list of hardware needed and do more research on the different ways AV systems are compromised
  + Still read up on mitigation and evaluate the difficulty before deciding if it should be part of scope

|  |  |  |
| --- | --- | --- |
| Decisions |  |  |

|  |  |  |
| --- | --- | --- |
| Action items | Person responsible | Deadline |
| Setup of Raspberry Pi | Rech Leong | 18/10/2019 | 5:00pm |
| Literature Review on TrojanNN and other adversarial attacks against image detection neural networks | Rech Leong | 30/11/2019 | 5:00pm |
|  |  |  |
| Research on operation of raspberry pi and relevant python libraries that can be used | Rech Leong | 14/10/2019 | 5:00pm |

**PICTURES OR ANY OTHER RELEVANT RESOURCES**

NIL