Release 0 , Week 2 |Minutes/Report

## 09/10/2019 | 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 (09/10/19)

To give an informal progress update of research findings thus far

Describe the known methods of attacks on image detection neural networks

Describe the ways to mitigate them

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

Questions to ask:

Between ShapeShifter and TrojanNN, which is better to use?

To propose scope of project

Decide which adversarial attack to focus on

Decide if mitigation should be in the scope

Propose hardware needed

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

* Second Milestone (Until Dec 2019)
  + Decided on TrojanNN
  + To setup RaspberryPi and RealVNC for remote access
  + To setup TrojanNN on that RaspberryPi
    - Replicate the model used in the research papers
  + Decide on ways to extend the attack/transferability
* Literature review
  + To be done by Dec 2019

|  |  |  |
| --- | --- | --- |
| 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