Release 0 , Week 5 |Minutes/Report

## 23/10/2019 | 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 (23/10/19)

To give an informal progress update of research findings thus far

Describe FGSM and TGSM attacks on image detection models

Describe defence distillation as a form of mitigation

Decide on subsequent steps to take

To propose timeline of development/writings

Literature Review to be started now and done by Dec 2019

Development to be done ASAP

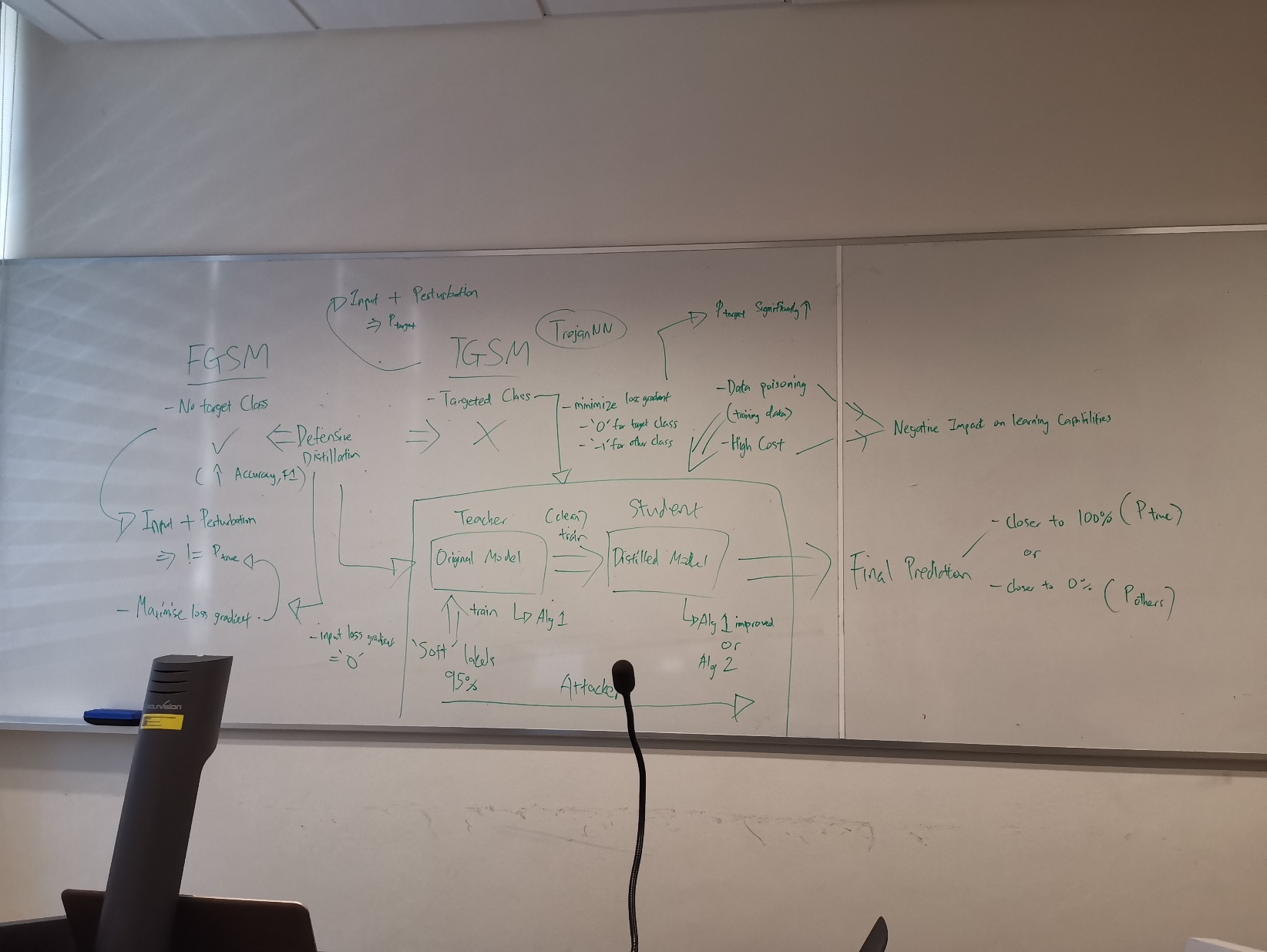
|  |  |  |
| --- | --- | --- |
| Notes and Suggestions |  |  |

* Second Milestone (Until Dec 2019)
  + To setup TrojanNN on Ubuntu Virtual Machine upon approval
    - 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 |
| Request of VM | Rech Leong | 24/10/2019 | 5:00pm |
| Literature Review on TrojanNN and other adversarial attacks against image detection neural networks | Rech Leong | 30/11/2019 | 5:00pm |
|  |  |  |

**PICTURES OR ANY OTHER RELEVANT RESOURCES**

****