#### Minutes #2

Minutes for meeting of Group EEE-UG13352

**Location**: IW 3.15

**Date**: 22/03/2021

**Time:** 11:10

**Present:** Hong Gunn Chew (HGC), Kyle Millar (KM), Hung Nguyen (HN), Quang Huy Ngo (QHN), Anh Tuan Phu (ATP)

**Absent:** n/a

1. **Formally open the meeting**
2. **Review of previous minutes**
3. **Action items resulting from previous meeting**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Task** | **Assigned** | **Due** | **Status** | |
| Review on CMU-CERT data and DAPT2020 data | QHN |  | Completed | |
| Use GCN to detects on Insider threats on DAPT2020 data | ATP |  | Completed | |
|  |  |  |  | |
|  |  |  |  | |
|  |  |  |  | |
|  |  |  |  | |
|  |  |  |  | |
|  |  |  |  |  |

1. **Project status/progress during last period**
   1. Use GCN to detects malicious activity in reconnaissance/lateral movement stages
   2. Obtained and inspected the log files and DAPT2020 dataset
   3. Re-run the experiment of DAPT2020 paper
2. **Project goals for upcoming period**
   1. Implement One-class GCN on DAPT-2020
   2. Use Random Forest to check the importance of features.
   3. Validate the performance of GCN on DAPT-2020
3. **Individual reports**
   1. Anh Tuan Phu
      1. Impemented GCN to detects malicious activity in reconnaisance and lateral movement stages, using the similar setting as in the original DAPT2020 paper
   2. Quang Huy Ngo:
      1. inspected the log files from DAPT2020 datasets, pointing out the drawbacks of the logs
      2. Proposed new potential use of GCN for combined logs and netflows data
4. **Risks and dependencies**
   1. Overfitting with GCN:

**Risk:** The performance of GCN might be overfitting, showing a false sense of high performance.

**Mitigation:** use Random Forest to check the importance of features and see what features are actually used by the classifier

1. **Any other business**
2. **Formally close the meeting**
3. **Summary of actions items arisen from the meeting**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Meeting Item** | **Task** | **Assigned** | **Due** | **Status** | |
| 1 | Implement One-class GCN for detecting with DAPT2020 dataset, using netflows data | QHN |  | On Track | |
| 2 | Find out the importance of each features with RF | ATP |  | On track | |
|  |  |  |  |  | |
|  |  |  |  |  | |
|  |  |  |  |  | |
|  |  |  |  |  | |
|  |  |  |  |  | |
|  |  |  |  |  |  |