The *first* Master of Computing and innovation Group Project weekly meeting will be held in **Room 464** at **3.00pm on Tuesday 28 Feb 2018**.

Meeting minutes on 28th Feb

Attendance: Zheng Xu, Junjie Guo

1 Apologies

None

2 Questions to ask

2.1 About the topic

1. Question1: What is the purpose of this project? As for this system, does it like the firewall?

   Answer: Detecting different cyber-attacks, training model to detect cyber-attacks in testing data.

2. Question 2: How can we capture and record the network events? (eg. WireShark: collect the IP address, account name or private data?)

   Answer: The dataset is from the KDD competition database.

3. Question 3: How to define some network events belong to the cyber attack? (eg.malicious website, phishing website, trojan and virus)?

   Answer: Signature-based detection will be used in our system. There may be more than 30 parameters in one type of cyber activity.

4. Question 4: What are the specific problems we need to solve(capture, store data and analyze)? How to collect various data effectively? How to analyze the data we capture?(eg. analyze the characteristic of the IP/Port)

   Answer: Analyzing part. Do not need to collect dataset by ourselves, it is from KDD database.

5. Question 5: Which books can we refer to based on this topic?

   Answer: Some relevant papers are offered by tutor.

2.2 About the requirements

1. Question 1: functional requirements:

   Answer: Accuracy and response time.

2. Question 2: non-functional requirements:

   Answer: reliability, availability and scalability.

2.3 About the tools

1. Question 1: Which data tools and platforms we could use?(eg. hadoop?)

   Answer: Hadoop platform, Java language.

Note: Next meeting to be held on 13 March 2018.