Appendix B:

Project Design Plan

1 Research Question

This project aims to critically and technically evaluate the susceptibility of IoT networks to DDoS attacks, focusing on the devices, networks, and operating systems associated with IoT.

2 Project Scope

The following list describes the topics and technologies which will be utilized in the completion of this project.

- Susceptibility to Attack
  - Networks
    - ns-3 Network Simulations
  - Operating Systems
    - OS Level Security Feature Implementations
    - Known
- Mitigation/Detection

3 Design Approach

The proposed approach to this project is to present a detailed technical evaluation of the security features available at the operating systems level. These will include features such as networking security - i.e. firewalls, and software security - i.e. secure boot.

Simulations will be run using ns-3 in order to evaluate the effects of common DDoS attacks on networks consisting of IoT devices. These simulations will utilize the available IoT related protocols in ns-3, including IPv6 and 6LoWPAN. The results of these simulations will be evaluated to determine points of failure within the networks.

Finally, a technical evaluation will be done into the available detection and mitigation techniques. This will include recommendations of techniques which could have specific benefits in IoT networks.

4 Timeline

The Gannt chart below describes the proposed timeline for the project. All items within the Gannt chart are colour coded as follows; green represents documentation - i.e. work on the final report, red represents background research - i.e. background research required for understanding the topic, blue represents testing - i.e. simulation testing, orange represents end of week reviews, during which time the goals of the past week and following week will be assessed.

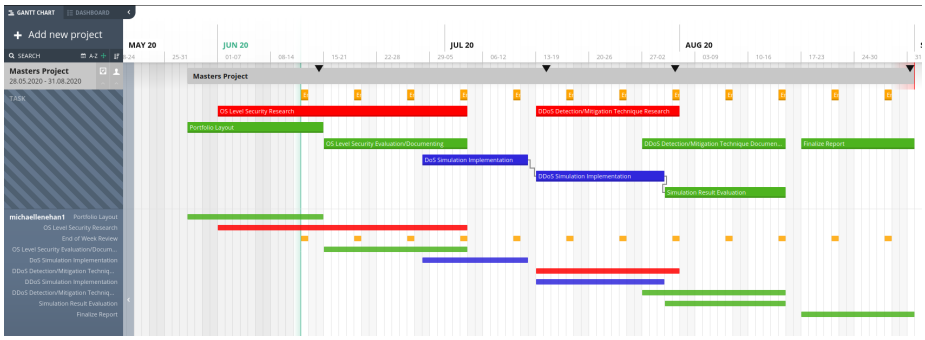

Figure 1: Project Gannt Chart

This project plan can be viewed at the following link: `https://app.agantty.com/#/sharing/d595b7c64d314f5788834d0ed8614ccc/de`

Not included in this design plan are working hours, which, for the duration of the project, will be 8 a.m. to 5 p.m Monday to Friday. All project work must be completed outside of these times.

5 Success Criteria

This project will be considered successful if the following criteria are met:

1. The completion of a literature review
2. The completion of a project project presentation
3. The completion of a Masters project research log
4. The completion of a technical evaluation of OS level security implementations
5. The completion of an investigation into known security vulnerabilities of IoT operating systems
6. The completion of a number of DDoS simulations on simulated IoT networks

7. The completion of a technical evaluation of DDoS detection and mitigation techniques

8. The completion of a list of recommendations of detection/mitigation techniques specifically applicable to IoT networks.

6 Remote Arrangements

It has been confirmed with the project supervisor, Liam Meany, that this project can be successfully completed remotely, i.e. with no access to on-campus resources.