DUBLIN CITY UNIVERSITY

ELECTRONIC AND COMPUTER ENGINEERING

An Evaluation of Distributed Denial of Service Attacks in IoT Networks

Project Design Plan

Author

Michael Lenehan michael.lenehan4@mail.dcu.ie

Student Number: 15410402

15/06/2020

Declaration

I declare that this material, which I now submit for assessment, is entirely my own work and has not been taken from the work of others, save and to the extent that such work has been cited and acknowledged within the text of my work. I understand that plagiarism, collusion, and copying are grave and serious offences in the university and accept the penalties that would be imposed should I engage in plagiarism, collusion or copying. I have read and understood the Assignment Regulations set out in the module documentation. I have identified and included the source of all facts, ideas, opinions, and viewpoints of others in the assignment references. Direct quotations from books, journal articles, internet sources, module text, or any other source whatsoever are acknowledged and the source cited are identified in the assignment references. This assignment, or any part of it, has not been previously submitted by me or any other person for assessment on this or any other course of study.

I have read and understood the DCU Academic Integrity and Plagiarism at `https://www4.dcu.ie/sites/default/files/policy/1%20-%20integrity_and_plagiarism_ovpaa_v3.pdf` and IEEE referencing guidelines found at `https://loop.dcu.ie/mod/url/view.php?id=448779`.

Signed: _____ Date: 15/06/2020

Michael Lenehan

Contents

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 avail-

able 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.

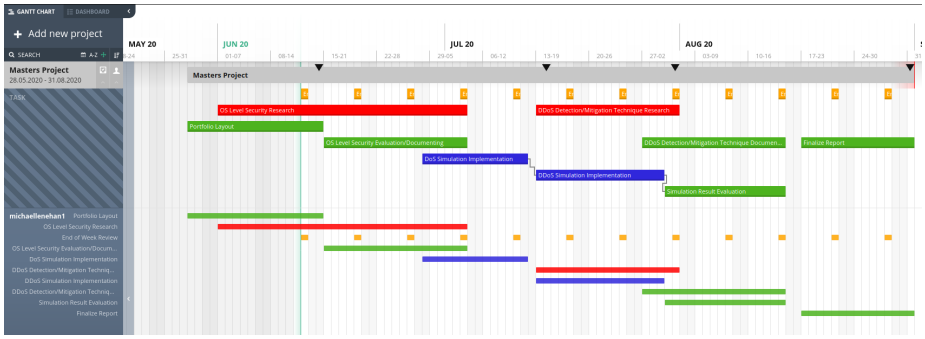

Figure 1: Project Gannt Chart

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.