KV6003 Individual Computing Project - Terms of Reference

Carl Slatter

5th October 2020

1 Background

The modern technological landscape demands much from innovation. We must find new ways of solving exisitng and new problems in the world. This is amazing for convinience, and quality of life, but does pose a problem for security. There is a law in IOT that the more you add in terms of functionality, the more that must be secured. A concrete cube may be secure, but is not overly functional. I am incredibly interested in the duality between attack and defence. It seems to be a constant cat and mouse game of which defence is paramount. I hope that by looking at both sides with a purple team perspective, I can gain a deep understanding of the landscape we have currently and moving forwards.

Cybersecurity is really "Managed insecurity", I intend to discover where cyber attacks are at, and how they have innovated over the years. Cyber threats are growing, how can be detect them? How can we proactivly block them? These are questions that must be answered in order to get a good overview. I must be able to show my understanding in a theorectical and practical way to be able to potentially apply it to a real life scenario. I will have to develop my understanding of infrastructure, networking, semi low-level programming and penetration testing.

Developing realistic solutions for smaller buisnesses is really important. They are arguably more at risk, with less resources for security. I dispise the idea of security snakeoil and scareware, and value defence-in-depth rather than a supposed all-in-one solution. With the detection work, I hope to show the importance of the human element to security, how it can be the weakest link, or the strongest asset. I must look at current solutions with a critical eye with care to be realistic about defence.

Malware has evolved over time, what was once an excercise of freedom and curisolity, is now a platform for theft and crime. Defences catch up over time, it will be eye-opening to see the different methods historically that the two sides try to out-smart each other. Malware analysis is something I haven't really touched on before, though I have be interested for a long while now. It will benefit my defence greatly.

2 Proposed Work

I aim to create documentation in the form of my dissertation to describe the Cybersecurity landscape in regards to infrastructure. This will involve talking about infrastructure directly, it's use, inplementation and potential pitfalls, but more importantly, how it can be secured. On the other side, I will be looking at the common ways that infrastructure is compromised, in a network setting. I do think that a good comparison is important for this.

I will be investigating how threats have evolved as a whole, whether that be malware, offuscation and clever exflitration. I believe it is important to at least touch on how this was done in the past, to understand how the future may follow similar foundations. Naturally an investigation into threats would be pointless without a practical defence, I hope to compare both endpoint and infrastructure defences in relation to both a sample of threats, and to one another. I will then analyse this data and draw sensible conclusions based upon it.

I also hope to create a rudamentrary intrusion detection system written in C. This will be a proof of concept to show my understanding, rather than a product. My hopes are that by developing network defence myself, I can gain an even deeper understanding.

3 Aims and Objectives

3.1 Aims

To understand the theory behind defence in relation to common threat vectors To develop attack and defence to aid the theory, in a practical manner

3.2 Objectives

Explanation of entry vectors profiling

Explantaiton of expliotation

Analyis of historic threats malware

Explantaiton of obfuscation

Explantaiton of exflitration

Investigate IDS/IPS systems w/ comparison

Illustrate proof of concept IDS

Investigate antivirus systems w/ comparison

Analyse modern attack:defence landscape

Describe meaningfull defence (defence-in-depth, social engineering resilience)

The **enumerate** environment is useful here for generating a numbered list. You can put `\label{}` commands in with a keyword `\label{understand-problem}` and then refer to the label with a `\ref{understand-problem}` command, it puts the number of the objective in the text

```
See objective \ref{understand-problem}
```

See objective 1

1. **Classify the problem domain** this is where you develop an understanding of the nature of the problem/project
2. **Identify Techniques to solve** What Algorithms are you to use, how is a database structured,
3. **Select tools to use** What languages, software, hardware; are you using?
4. **Design the system to be build** Its requirements, the **test plan**, the architecture (Layer model/Model-View-Controller)
5. **Build the system** I'd include testing here, as the result is a *working wywtem*

4 Skills

This is where you can cover the skills you have relevant to the project and the new skills you are going to acquire during the project.

1. Programming in C, see module KFxxx
2. Hardware Design

5 Resources

This is an important section, it lists the hardware and software you are going to need for the project.

5.1 Hardware

For Hardware this is more critical, as we need to identify any hardware we have, or that you are going to buy. We do have an ordering mechanism in the Department, but time and budget are critical constraints here.

5.2 Software

In the case of software, there isn't usually an issue, unless you're needing huge amounts of run-time (we don't have a super-computer handy).

6 Structure and Contents of the Report

Here you set out the likely chapters you will have in your report. Usually each objective lends itself to one or more chapters. You can refer back to the objectives set.

6.1 Report Structure

Introduction Sets out the background and motivation for the project. Summarises the work done, the results, the conclusions, and the recommendations for future work. It is a one chapter summary of the *entire* project.

Defining the problem Objective 1 requires a precise definition of the problem you are solving. Don't forget to reference good source material [Schulzrinne, 2017] and [Talbot, 2013]. See section 2.

Possible Solutions Discuss the possible solutions, compare the alternatives, and select the one to use for the implementation.

6.2 List of Appendices

What Appendices you will include. A copy of the TOR should be the first, followed by the Ethics form and the Risk Assessment.

Others might include design documentation, code listings, tables of results (if too large to include in the main text).

7 Marking Scheme

The marking scheme sets out what criteria we are going to use for the project.

Project Type General Computing or Software Engineering projects

Project Report State which chapters constitute the *Analysis*, the *Synthesis*, and the *Evaluation*. This help me when marking to know when to stop reading one section and put a mark down for it.

Product List the deliverables that make up the *Product*. Code, design, requirements specifications, test plans, etc.

For the *Fitness for Purpose* and *Build Quality* list the critera used to asses the product by

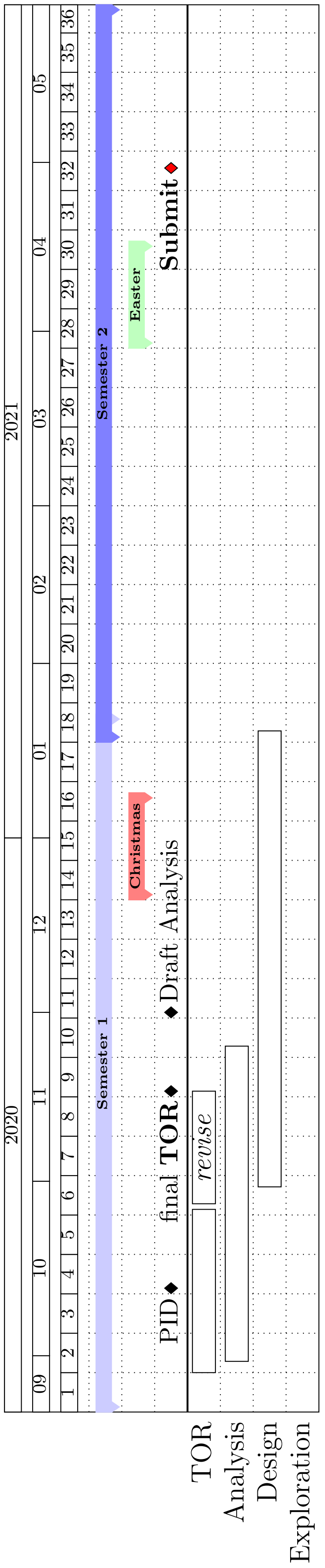
Fitness for Purpose

- meet requirements identified
- other appropriate measures

Build Quality

- Requirements specification and analysis
- Design Specification
- Code quality
- Test plan and Results

8 Project Plan



9 Bibliography

Henning Schulzrinne. Writing systems and networking articles, 2017. URL `http://www.cs.columbia.edu/~hgs/etc/writing-style.html`.

Nicola L. C. Talbot. *Using LaTeX to Write a PhD Thesis*, volume 2 of *Dickimaw LaTeX Series*. Dickimaw Books, Norfolk, UK, 2013. ISBN 978-1-909440-02-9. URL `http://www.dickimaw-books.com/latex/thesis/`.

A Ethics Form

```
\includepdf[pages=1-3]{ethics.pdf}
```

Ethical category of project
[Complete after approval]

Red	□
Amber	□
Green	□

northumbria
UNIVERSITY NEWCASTLE

Department of Computer Science and Digital Technologies

UNDERGRADUATE COMPUTING PROJECTS: ETHICS REGISTRATION AND APPROVAL FORM

Section One: Registration *[To be completed by student]*

Title of research project/dissertation	
Researcher's name	
Programme of study	
Academic Year	
Module code	
Supervisor's name	
Second marker's name	
Start Date of Project	

Brief outline of research topic:

Short description of proposed research methods including identification of participants:

Ethical considerations in the research project	YES	NO
1. Does your research involve an external organisation or partner?	□	□
2. Does your research involve human participants?	□	□
3. If yes to Q.2, will you inform the participants about the research?	□	□
4. Will you obtain their consent using the standard consent form?	□	□
5. Is any deception involved?	□	□
6. Do any participants constitute a 'vulnerable group'? (refer to definition of Vulnerable People)	□	□
7. Will the research involve the following information?		
Commercially sensitive	□	□
Personally sensitive	□	□
Politically sensitive	□	□
Legally sensitive	□	□
8. Is the research likely to have any significant environmental impacts?	□	□
9. Are there likely to be any risks for the participants in your research?	□	□
10. Are there likely to be any risks for you in conducting the research?	□	□
11. If yes [to 5, 6, 7, 8, 9 or 10 above] have you identified steps to address the issues and mitigate any risks to participants, yourself or the environment?	□	□

Statement to explain how any issues identified above will be addressed and what steps will be taken to mitigate such risks or adverse impacts

Ethical category of research project

Based on the above Ethical Considerations and with reference to the University's Ethical Scrutiny Risk Assessment tool identify the Ethical category of your research project (refer to http://www.northumbria.ac.uk/static/5007/respdf/riskassesmenttool for further guidance):

[Please tick as appropriate]

Red	□	vulnerable participants; human tissue; sensitive data; risks to participants & researchers etc.
Amber	□	human participants requiring informed consent; commercially sensitive information etc.
Green	□	no participants involved; secondary data only; no sensitive data

I have read the University and the Faculty Ethics Policy and Procedures and confirm that the answers I have given above are correct. Where issues arise under items 5, 6, 7, 8, 9 or 10 [above] I have described in writing how I intend to approach these issues in the research.

Researcher's signature ....

Date ....

Section 1 Ethics Registration to be submitted to Principal Supervisor or Module Tutor and allocated to a reviewer as follows:

Green risk - may be approved by Supervisor
Amber risk - to be submitted for approval by one independent reviewer (second marker)
Red risk - to be submitted for approval by two independent members of Faculty Research Ethics Committee

B Risk Assessment Form

```
\includepdf[pages=1-3]{risk-assesment.pdf}
```