KF7004 – MComp Computing Research Project Reflection

16018262

Sept 22

Word count:

Contents

1 group vs individual

Although I was primarily working alone, I did receive a lot of assistance from academic staff. This worked quite well due to the fact that the academic does not have any knowledge of cybersecurity, which meant that I was free to experiment and he was able to advise all the methods used without getting caught up in the smaller details, due to his knowledge of algorithms. Furthermore, the academic staff had prior knowledge of the project, due to supervision at undergraduate level and therefore understood the project and its complexities. This resulted in a more comprehensive approach to the problem; Thurow et al. argues that multidisciplinary settings allows individuals from different disciplines to contribute their disciplinary perspectives in an attempt to solve complex problems. An example of this is, when analysing the user agents, I had originally tried to implement a Levenshtein distance to try and find the nearest user agent. However, the academic suggested doing a bag of words approach, which was ultimately a stronger and more accurate methodology.

Throughout the year myself and my supervisor tried to get into a regular habit of meeting. It also kept us both informed as to where the research was at and what needed to be undertaken for the following week. This

also prevented delays in the research if I got stuck on something. This worked well to keep the momentum going and I was able to establish if a method was working or not. One of the downsides of this was if there had been a slow progress week it felt like I hadn't done anything, which negatively impacted my motivation. Also, some of our meetings involved brainstorming on whiteboards, this was sometimes difficult to read if the meeting was on Teams, due to bad internet connection. This would have been avoidable if my support had been properly arranged in advance of my return to University.

As there is a lack of research in the area I was researching, it may have made it challenging for someone to join the project and be able to completely understand the complexity of the project. Theoretically by working alone it made the ethics application easier, as I relied on getting data from customer websites. They already knew who I was and as a result were more willing to share their data with me for this project as well. However, there were times when having more than one dedicated researcher would have been beneficial. For example, when classifying the accuracy of the program it might have been beneficial to have someone to classify the data as well. This would help to remove any bias that I might have had.

The work for this module was meant to be undertaken as a group research project, however it was decided early on that I would complete it as an individual. Primarily due to the fact that the work was heavily linked to the work carried out for my undergrad dissertation. Most of the underlying software was written as a part of my dissertation, therefore most of the work was identifying small improvements that could be made. Then developing a methodology to prove that accuracy of the program. It may have been useful to get new ideas in, which may have led to a better outcome. If I were to have worked in a group the collaboration would have been beneficial as Robert E. Levasseur (2010) states, "to initiate and... the high level of two-way communication" (Levasseur 2010). Despite not being in a group I was still able to have effective communication with a lecturer in the department. Although they did not have any knowledge of cyber-security, they did know a lot about programming algorithms. I was able to take ideas to them and they would know how to implement them, without disagreement over the direction the project took. It can be shown that the more collaboration that exists in research projects, the higher the quality of the research (Figg et al. 2006). Therefore the collaboration within this project led to a better output but other collaborators would have increased this further.

If this had been an entirely new project it would have been beneficial to collaborate with more than one person. To bring in new ideas and a different point of view. However due to the fact that it was a continuation I believe it was the right decision to do it on my own.

2 Background, Motivation, Sources of Knowledge

Throughout this project, there have been many stages where reflection has been needed in order to understand the progress that has been made. At times, progress has felt limited and non-existent. However, these periods have allowed for reflection. By regularly putting my research on hold and taking a step back, I was able to develop a regular reflective habit (Dyment and O'connell 2010). However, at other times throughout the year, there have been ongoing issues with a lack of available support in order to complete work. There have been periods where reflection in action have been required. Often when reflection in action, we are often unaware that we have derived meaning from an experience, however we find ourselves doing the same action again, as it has a positive outcome (Schon 1983). By reflecting in action, it allows me to reflect on where I was in the project, and what I needed to do to progress thus resulting in more effective decision making and problem solving. This was mainly evident by last minutes changes made to my proposal, meaning I had to reflect on how to get this done. This meant having to do an online zoom session, so that someone was able to assess me to get changes done. The positive outcome here was that I got the work done and I was able to

learn that doing work on zoom, although not ideal, still contributed to the success of the project.

The project undertaken was a continuation of my undergraduate project, looking at a new way to detect attacks on websites. The motivation of this was to solve a challenge that I faced, running my own website. The lack of literature in this area to do with cyber security was surprising, however this led to freedom in creating a new methodology. Due to the fact that there was no existing methodology, apart from my own, I had to combine some existing techniques and test some new ones. Due to the lack of relevant literature, the literature review was challenging to construct. Therefore it became more about identifying gaps in previous work. Hertz (1997) points out that 'the reflective researcher does not merely report the findings of the research but at the same time questions and explains how those findings are constructed'. (CITE) This shows that I was be able to reflect on the available literature and ask questions that led to my hypothesis. A lot of these questions were not complicated in nature, but came from a working knowledge of websites and servers, the key lesson that I learned in this was that just by asking simple questions about the research, it was easy to identify flaws

3 Relevance

This work was relevant due to the fact that all previous cyber security work in regards to low rate DDoS attacks could be seen as deeply flawed. For example, Tripathi generated their own data to validated their own hypothesis and methods. One of my goals was to show that cyber security work needs to be validated by real data. The work is also relevant due to an increasing reliance on websites and the internet in general. If there aren't effective ways to check attacks, then they have the potential to disrupt daily life. I saw this actualise itself when, after helping a Newcastle University Researcher I was able to reduce the running cost of their web severs by fifty percent. This shows the real world effect that the software has, along with the harm that attacks can cause if they are able to go undetected. The work was also relevant to me on a personal level; as it allowed me to create some research that has never been done before and go on to develop it as a product to sell to other websites.

4 Scope, Objectives and Risk

4.1 Scope

The scope of this work was to continue the work started in my undergraduate project.

4.2 Objectives

I had to remove an objective, which would have been to develop a better way to assign risk to a country. I intended to look at the number of attacks coming from IP addresses within a country compared to the size of the population. However, due to time constraints I encountered due to a lack of support from the University, I kept the current methodology. This was just looking at the number of attacks from within a country.

4.3 Risk

The biggest risk associated with this project was the lack of previous work. Because, there was a question in my mind that this methodology seemed so simple and obvious, why had nobody tried this before? Was it because it did not work? This risk was mitigated due to the fact that, even if the conclusion was that this methodology did not work it would still be a valid conclusion to make.

5 Ethics, Legal, Social, Security and Professional Issues

5.1 Ethics

Due to the ambiguity of user consent in the collection of website log data, and whether users had given informed consent about the collection. Websites say that data can be analysed however due to the university policy of expressed consent, there were questions about whether the data could be used. However, due to the study wanting real-world data, this might have changed user behaviour, knowing that they would've been tracked. This was done to mitigate the effects of possible confounding variables, such as social desirability. Studies have suggested that individuals online behaviour changed when they are being monitored.

Another ethical implication of the work may be the fact that entire country is given a risk. This is mainly done to give the software an idea of context, however a user from a high risk country can still get a low overall risk score.

6 Legal Issues

There was a potential legal issue as people could not opt out of the data analysis. This is due to the fact that as soon as they went on to the website their IP address was logged. Most websites privacy policy state that IP addresses will be logged and used for analysis, therefore most users should be aware of how their data will be used.

7 bibliography

References

Dyment, Janet E and Timothy S O'connell (2010). "The quality of reflection in student journals: A review of limiting and enabling factors". In: *Innovative Higher Education* 35, pp. 233–244.

Figg, William D et al. (2006). "Scientific collaboration results in higher citation rates of published articles". In: *Pharmacotherapy: The Journal of Human Pharmacology and Drug Therapy* 26.6, pp. 759–767.

Levasseur, Robert E (2010). "People skills: Ensuring project success—A change management perspective". In: *Interfaces* 40.2, pp. 159–162.

Schon, D (1983). *The reflective practitioner. How professionals think in action.* London: Temple Smith.

Thurow, Amy Purvis et al. (1999). "The dynamics of multidisciplinary research teams in academia". In: *The review of higher education* 22.4, pp. 425–440.