VICTORIA UNIVERSITY OF WELLINGTON
Te Whare Wānanga o te Ūpoko o te Ika a Māui

School of Engineering and Computer Science
Te Kura Mātai Pūkaha, Pūrorohiko

PO Box 600
Wellington
New Zealand

Tel: +64 4 463 5341
Fax: +64 4 463 5045
Internet: office@ecs.vuw.ac.nz

Why Do Programmers Do What They Do? A Theory on Influences on Security Practices

Lavanya Sajwan

Supervisors: James Noble, Craig Anslow

Submitted in partial fulfilment of the requirements for Bachelor of Engineering with Honours in Software Engineering.

Abstract

Technologies are continually adapting to match ever-changing trends, and as this occurs, new vulnerabilities are exploited by malignant attackers and can cause significant economic damage to companies. Programmers are therefore repeatedly having to expand knowledge and skills to protect software. Programmers do make mistakes and this is why we must understand the thinking behind the decisions and influences of programmers to interpret how they implement and adopt security practices. Understanding these decisions can help inform design decisions around improving programming language security. This preliminary report will cover the current progress of the project "Why Do Programmers Do What They Do?"

Acknowledgements

I would like to thank my supervisors James Noble and Craig Anslow for their ongoing support so far in this project.

I would also like to thank my friends for keeping me sane.

Contents

Chapter 1

Introduction

As software is now ubiquitous across industry and it is impossible not to have a presence in the tech sphere. Consequently, software security has become so significant, programmers have to ensure that the security processes that they implement are resilient to any attacks. Lack of attack prevention can cause leakage of sensitive information, massive economic damage and danger to massive numbers of users and employees, consequently opening business, clients and end-users to exploitation by external bodies. Unfortunately, every day, we hear of organisations that have been compromised [1]. Last year New Zealand experienced a significant security breach within the Tū Ora Compass Health (Tū Ora) Primary Health Organisation (PHO) [2]. Tū Ora is one of the largest PHO's in the country and it governs the greater Wellington region [2]. Personal information of up to one million New Zealander's was exposed and the effects of this are ongoing [2]. Ccosts have been great in attempts to mitigate any effects to the public. Dedicated call centres have had to be organised as well as dedicated mental health lines [3, 2]. Regular updates have had to be released in order to maintain communication transparency and assurance quality measures are ongoing [3, 2].

Qualitative research is often neglected and overlooked in favour of more quantitative reasoning and technical traits such as the security method used or the programmers task-completion rate [4]. Programmers provide a human aspect to a technical solution and therefore, there should be a shift towards understanding the more background 'soft' processes that occur when making decisions; why are the choices made based on past influences, and how they affect the programmers work in the present?

Past the research aspect, when security and privacy issues do occur in real-world scenarios, developers are blamed first as it is their projects that have allowed the vulnerabilities to be exploited [5]. While developers do make mistakes, they also do need the support to make better security decisions, and this support is currently lacking in the industry [5]. Education is limited past initial acceptance within organisations, and often developers have a blasé attitude to the matter expecting another team to fix the issue [6]. Furthermore, security mechanisms often have an increased complexity, which make them difficult to understand and to then use [7].

This project will investigate how software developers implement and adopt security practices in the work they do in order to develop an understanding of what influences and impact decisions surrounding their technical work. This project will be conducted using grounded theory which is a theory is a method which aims to establish a theory when there is none [8], and it is a commonly used method for data analysis. Interviews will take place to

collect the data, from which the answers will be analysed to draw conclusions on standard security practices in the professional workplace. This project builds upon works by Hala Assal, Charles Weir and Nathan Newton [9, 1, 10].

This project aims to implement a theory as to why programmers implement and adopt security practices in the work they do by interviewing professional developers and using the Grounded Theory Method to analyse the outcomes. Grounded theory is a research method to analyse qualitative data. There are several thorough steps which include; sampling, data collection, data analysis, theoretical note writing, identifying core categories, forming theoretical outlines and presenting a theory.

Participants will be recruited by posting on tech-related groups (i.e. From OWASP Meetup Group and LinkedIn) and mailing lists and also using mine and my supervisor contacts. At this point, I can then start semi-structured interviews with 10-20 interested individuals on their security practices while programming. These people will all be developers in New Zealand that are in varying stages of their careers and career paths to allow for a broader range of responses and a case study relevant to New Zealand. Examples of appropriate job titles include; DevOps engineer, front-end security developer, database administrator, developer, programmer and security architect.

This project will lead to a new, more in-depth understanding of the psychology of the decisions made by programmers. The research done by this project could lead to future qualitative research to be done on another under-developed topic on why programmers do what they do. Paired with this research, that future one could help build a profile of a programmer and their thought processes. Data collected could also be the foundation that allows a developer to build tools that helps other developers implement proper security practices; a Grammarly for security. It can also help the further development of existing static analysis tools such as Infer developed by Facebook, Tricorder used by Google, Coverity and Raygun [11, 12, 13, 14]. These tools all work by providing security detection modules and are used for quality assurance and security.

Exploring this topic is essential as it allows for a more comprehensive understanding of how and why programmers think the way they do, and of the human and social aspects of Software Engineering [15]. We want to understand what solutions developers are using to implement in their security practices, if at all. The findings from this can support developers in terms of education and the better design of security methods in programming [9] that have an emphasis on usability. The findings of this project can also be used to identify what security methods developers find as beneficial in their programming. This will allow programmers to complete their work to a high standard, by adhering to proper security protocols, thus overall making their work of a higher value both in a secure and professional sense.

1.1 Deviations from the Original Plan

There have been no deviations from the original plan.

Chapter 2

Background

Conceptually, this project aims to gather data in order to ultimately form a theory on the influences of security practices in New Zealand. Therefore, It is essential that I know enough information about the topic of security so that I am able to interview professional engineers in a manner which is knowledgeable. This chapter will include background on the importance of information security practices, what practices are widely used, summaries on existing research on similar subject matter, and a discussion on the chosen methodology.

2.1 Research Methodology

Grounded theory (GT) is the chosen methodology for this study. It was an appropriate choice as the study focuses on human aspects and GT is appropriate to study these as it is way of analysing qualitative data with the end-goal of defining a new theory from the sampled data [15]. There are several procedures in the GT methodology in order to make the final theory. The theory is expected to be explanatory, focusing on describing elements of the findings rather than stating. It should also be based on the collected responses and observations, rather than pre-conceived ideas. Avoidance of an extensive literature review should occur accordingly.

Initially, researchers must choose a topic and research whether the Grounded Theory method is the right one for the research project [15]. After contacting sample groups the iterative process of data collection occurs. Questions adapt between collection as analysis of the previous answers occurs. This refinement of questions happens to delve deeper into the traits of the emerging theory. When saturation is achieved, no more new findings are displayed which contribute to the final theory. This results in the "grounded" nature of the overall theory.

Similar projects at the university have been conducted using this methodology. Siva Dorairaj's, "The Theory of One Team: Agile Software Development with Distributed Teams"; Rashina Hoda's, "Self-Organising Agile Teams: A Grounded Theory"; Brendan Julian's, "Agile Practices: A Theory of Agile Adoption and Evolution"; Nathan Newton's, "Information Security in Agile Software Development: A Critical Success Factor Perspective"; and Aaron Pangs, "What Programming Languages Do Developers Use? A Theory of Static vs Dynamic Language Choice" [16].

2.2 Information Security in New Zealand

Information security is defined by three objectives; confidentiality, integrity and availability, most commonly referred to as the CIA triad. Confidentiality is the act of keeping information private to protect information, Integrity is the act of maintaining information validity and Availability is the act of ensuring reliable access to information. Any breach of those principles can result in significant negative impacts economically, and to personal emotional and physical well-being.

A study run by Aura Security showed showed a 10% increase in cyber-attacks on New Zealand businesses between the years of 2018-2019 [17]. In NZ the rise is attributed to the digitisation of day-to-day way-of-life; as new technologies are continuously developed there is an urgency to deploy products. There is a lot of pressure on programmers to finalise these products and the deviation of attention to the finished output means that there are many new threats to security [18]. Malicious attackers are also becoming more sophisticated. Individual threat attackers now seem to have the same knowledge and resources as nation-backed actors [18].

Areas of improvement identified by the New Zealand government are [18]:

1. **Cyber security aware and active citizens:** Increased regular awareness campaigns and education opportunities for the public in regards to best personal security practices.
2. **Strong and capable cyber security workforce and ecosystem:** Increased promotion and support of the development of the cyber industry in New Zealand.
3. **Internationally active:** Detect and prevent any breaches as well as proactively maintaining international relationships regarding information security and participating in any rule reforms.
4. **Resilient and responsive New Zealand:** Supporting infrastructure, businesses, charity organisations, community organisations, individuals in improving security capabilities and resilience.
5. **Proactively tackle cybercrime:** Increasing support to impacted parties, preventing and encouraging reporting of any cybercrimes.

These five principles are planned to continue to improve upon till 2023 [18]. It is expected that aspects of these will influence the security practices that programmers use in NZ industry.

2.3 Secure Programming Practices

Secure refers to protecting and deterring any security breaches due to vulnerabilities in program code. Without a focus of security while programming, there is a lack of confidence in the outputted security, resulting in the lack of use and waste of time, effort and money. If unsecured programs are used, it poses significant negative impacts to businesses and individuals.

The Open Web Application Security Project (OWASP) have outlined a checklist to ensure that code is secure. They have provided this document which spans various languages and

technologies as the nonprofit foundation aims to improve the security across all software. It is stated that it is "much less expensive to build software than to correct security issues" [19].

Significant items from the checklist include [19]:

- **Input Validation:** This is the act of validating that all inputs are trusted. Examples of inputs are data from databases, file streams, etc, as well as client provided data. If anything is classed as 'untrusted', it should fail and result in a rejection. The application should have one input validation routine, a specified common character set and all validation should occur on a preset trusted system.
- **Output Encoding:** When data is sent back to a client, the information needs to be output encoded. To make this secure, a started test routine has to be utilised, and similar to input validation; all encoding must occur on a preset trusted system.
- **Authentication and Password Management:** This is verifying whether a user is allowed to perform an action. Best practice is restricting all resources except the ones intended to be public. All authentication controls should be able to fail in order to maintain security and passwords should be hashed. In order to pass, authentication has to occur first and every detail has to match the protected records.
- **Session Management:** A session should only associate the same client ID. It can only occur after authentication.
- **Access Control:** Set users access based on system permissions. It should use only preset trusted systems.
- **Cryptographic Practices:** All assets should be protected by cryptography. A policy should be established in how to manage the public and private keys.
- **Error Handing and Logging:** All application errors must be 'caught' and handled. They should not disclose any information in the error responses, and instead only show in the logs. The logs themselves can only be accessed by a few and mechanisms should be in place to analyse the logs.
- **Data Protection:** Protect most assets, communications and caches. Encrypt any stored information that holds significant value.
- **Communication Security:** Encrypt any communication channels. Certificates should be valid and the protocol Transport Layer Security should be used.
- **System Configuration:** Ensure that everything is up to date. This includes servers, frameworks, components, languages, IDE's and libraries. Remove unnecessary information before deployment; test code, TODO's, HTTP methods and response headers.
- **Database Security:** Maintain short connections. Authentication needs to be checked prior use, and access control needs to be restricted.
- **File Management:** Require authentication and access control before any interaction with files. Validate file headers. Implement safe uploading by scanning for any malicious intent; viruses and malware.
- **Memory Management:** Check buffers. If larger than expected, potentially has malware or viruses. Avoid the use of vulnerable functions - *printf, strcpy*

- **General Coding Practices:**
  - Use tested and trusted components for tasks
  - Restrict users from altering code in any way
  - Review all third part components; code and libraries
  - Initialise all variables and fields

2.4 Related Work

This project expands upon ideas on the following works; A Survey with Software Developers - Think secure from the beginning; and Kirk and Tempero's, Software Development in New Zealand.

2.4.1 "Think secure from the beginning" – Assal and Chiasson

In "A Survey with Software Developers" [9], the authors pursue to understand the human behaviours and motivations which surround factors of software security. The authors specified a series of questions targeted towards software developers through an online survey. The research examined responses to further support the professional development of programmers, both in theory and practice. This aligns well with the research goals of "Why Do Programmers Do What They Do?", as it aims to form a theory on the influences and effects of decisions surrounding technical work.

The results outlined the following common groups:

1. **Work Motivation:** Developers did not lack motivation in their job. They performed based on self-determination.
2. **Understanding of software security:** Developers had a sound understanding of software security. They grasped the importance of securing technical work and the discussed various methods of doing so and specifying at what stages in the project lifecycle they should implement these based on "best practices".
3. **Security Issues:** Majority of the participants believed their software could be compromised, despite being comfortable with the approaches to protecting the software. The majority has also experienced a security issue, whether that be a breach, or vulnerable code.

From these common groups the overarching theme displayed was that the developers were not purposefully ignorant to maintaining security practices, the majority were proactive and willing to learn. However, it was the importance of functionality and lack of ongoing support from organisations which made working towards a more secure software challenging.

This paper was valuable to read as there are strong similarities between the research topic developed in this and the subject of the 489 topic. The methodologies are different, however, the findings of this display a programmers personal perspective rather than a theorised view. It is a direct comparison to our project, and we can further outline questions directed to the future work stated in the article's conclusion; "to explore potential relationships between motivations, deterrents and strategies for software security" and "investigate

security procedures and attitudes in companies that have experienced security breaches and compare it to others who have not".

Similar questions from the survey can be used for the interview process in this study. Important questions identified are:

- How does security fit in the development life-cycle in real life?
- What are the current motivators and deterrents to developers paying attention to security?

The differences can be easier understood in the table below:

This Research	**Assal and Chiasson's Research**
Interview	Survey
Any type of programmer involved with security practices	Software Developers
New Zealand based	North American based
Confidential Participants	Anonymous Participants
Results based on overall analysis of participant answers	Results based only on participant answers
Security	Security

2.4.2 "Software Development Practices in New Zealand" – Kirk and Tempero

In "Software Development Practices in New Zealand" [20], the report authors look to "developing and applying a range of software productivity techniques and tools to enhance the performance of the New Zealand software industry". Like Assal and Chiasson, the authors of this study outlined a series of questions in a survey targeted towards known Information Technology organisations. The aim of the survey was to understand the practices used by industry and in the findings can be used to make recommendations on best-use development practices for organisations. Kirk and Tempero's report is similar in output to the one research defined in this report as the findings of the theory can be used to make suggestions for teams adopting and developing security practices.

The key findings of this study were:

1. Organisations and individuals **do not follow** standard agile process models.
2. New Zealand is generally more **implementation-focused** in software development. There is an emphasis on this over other aspects of the software development life-cycle such as security and testing.
3. Decision-making is a **collaborative effort** with individuals involved in different stages and traits of the development life-cycle.
4. While most New Zealander's state they are "agile" this is not supported as frequent contact with clients and stakeholders is not upheld. However, there is a **highly iterative aspect** to the work individuals do on projects which does maintain agile principles.
5. There is a **weakness in requirements gathering** which results in a widely noticed lack of clarity on scope details.
6. A tie in to point 2, notices a severe **lack of code quality** whether this be in design, reviewing and testing stages, or with general coding best practices.
7. Most **do not develop around** tools such as libraries, rather they use them as a support. This can be derived as not being "best-practice" and can be more time consuming.

Not much was asked specific to security, but finding number 6 links to poor practices around secure programming.

The report had a limitation in which it did not make any recommendations at this stage, but it did mention that these findings can be used by organisations to obtain a view of the software practices in New Zealand. From here the organisations can make their own decisions on what to focus on to better their specific operations.

Comparing to the described ENGR489 project, the methodology is different, and while the topics too are differing, they are similar enough to make interesting comparisons between the two. Kirk and Tempero focus on software development practices, while this project will research security practices. A comparison that can be made could be between the findings, as much like the prior related work, the findings are that of personal perspective of the participants rather than an objective view which Grounded Theory supplies.

The differences are outlined in the table below:

This Research	Kirk and Tempero's Research
Interview	Survey
Any type of programmer involved with security practices	Those involved with developing software
New Zealand based	New Zealand based
Confidential Participants	Anonymous Participants
Results based on overall analysis of participant answers	Results based only on participant answers
Security	Software Best Practices

Chapter 3

Work Completed

As of yet, the progress made on this study has been predominately focused on the human ethics application as well as the steps in crafting appropriate interview questions. Before any contact with potential interview participants, the human ethics application has to be approved. This is to ensure that research follows responsible and robust processes involving people and their data, consequently, proceeding ethically. As this has been in a recursive stage of editing and sending back to be reviewed, there has been iterative work designing potential questions for the semi-structured interview. Processes which have involved pilot studies in order to focus on an area of my topic. As the human ethics application is yet to be approved, my data collection and analysis stages have not started. Each of the areas are discussed in detail in the following sections.

3.1 Human Ethics Application

There was an immediate pressure to complete the human ethics application as the rest of the project is highly dependent on the participant interviews. This meant that the research had to be planned quite quickly in order to provide the human ethics committee with all the relevant information needed to approve the application. The initial application was submitted 8th of April. It has since undergone pre-committee revisions and post-committee revisions and is currently pending a second committee review. This application outlined a series of multichoice and short-answer questions which had to be answered thoroughly and supporting documents had to be submitted. These supporting documents included the participant information sheet, consent to interview document, an interview guide, and as this research's recruitment will be done through mailing lists and Meetup and LinkedIn posts, a sample recruitment post was also supplied.

The human ethics application specified key methods for ethical data collection in order to maintain a research that followed ideal human ethics policy [21]. The application went into details of data collection and recruitment, conformation with the university Te Tiriti o Waitangi statute, project risks, and data management. Answering these sections meant that a lot of planning has gone into the interview process for data collection. In particular it was decided that the selection process will follow purposeful sampling for the interviews. This is because participants will need to be selected on whether they are professional programmers in industry. The study will ideally include participants with a range of job titles and years in the field in order to find interesting comparisons during the interview process in the way security practices are adopted in the developed software. Participants will consequently be filtered by appropriate job titles, and be older by the age of 18 to avoid complexities with

the Vulnerable Children Act 2014 [22].

Focus on the Te Tiriti o Waitangi was necessary as this is a research project run in New Zealand with participants who work in the domestic industry. Therefore, the recruitment of participants and the conducting of the interviews will be run in a way which respects the principles outline in the university statute, which derive directly from Te Tiriti o Waitangi. Specific care was taken to this as there is only a certain threshold that this study can pertain to. However, it was decided that through my recruitment, I should work under the principle of Whai wāhi (participation) and encourage the participation of tangata whenua by advertising it on accessible platforms and to organisations with more of an emphasis of Te Tiriti in their core values. An alum of Maori decent was also consulted on this and they mentioned that in the participant information and consent forms, it should be explicitly clear that participants still have ownership of their data and are able to edit and remove information as they wish.

Corresponding to the point above, the interviews will be confidential rather the anonymous to allow for participant edits and to also allow for follow up questions if necessary. They will in no way be able to be identified and in any report outputs of this study will not name participants and instead be either referred to by role or by pseudonyms. Data will also be aggregated to maintain confidentiality. Participants will also be reminded before the interview as well as in the information and consent documents, that they should not divulge any sensitive information.

Due to complications with COVID-19 the interviews will also be adapted to allow for online capabilities using applications such as Zoom. There were issues surrounding obtaining consent, and the application had to be amended to allow for electronic consent. This will be done by emailing the form to participants, and consent will be obtained by a simple email back of agreement. Electronic signing of the form was not applicable as not everyone may have access to software with the capabilities to do so. It was also decided that the interview will offer a $10 gift reward for participation for their time during the pandemic and this will be a supermarket voucher. Safety was consequently paramount in the planning of the pandemic for both the interviewer and the interviewee. In the case of any in-person interviews sanitiser and a box of tissues will be in hand as well as disinfection of the meeting rooms before and after interviews, and the interviews themselves will be conducted while maintaining social distancing practices. To thank participants for their time, they will be offered a gift voucher to a supermarket.

3.2 Interview Planning

In the ethics application planning had to occur well ahead of interviews and there was a focus on creating the questions. However, as grounded theory involves a semi-structured interview process, a guide was submitted alongside the application. This is because questions are meant to change dependent on the participant as well as the narrowing focus on the ultimate theory. The interviews will also include open-ended questions which allow for more personal, in-depth responses which can hold more information to be analysed. It is expected that the analysis will occur immediately after interviews in order to revise questions before the next participant. All interviews are expected to take a maximum of 60 minutes, and will be coded. The interview recordings will be available for participants at their request for any amending of content.

Interviews will be expected to start by collecting information on participant background. This means groupings can happen by education, roles and experience. The next section of the interview will cover their current security practices that they implement in their code. This will then lead on to the impacts of security and languages in the projects they have worked on, and any background in the testing of those practices and successes of some over others. These sections allow for the simplest of aggregations to occur when all data has been collected and analysed.

For a better understanding of the process, old alums; Nathan Newton and Brendan Julian, whom conducted grounded theory methodology studies were contacted on their approaches. Brendan stated that they did not know what their focus would be going into the interviews, and the idea slowly formed the more interviews and analysis he did. The Nathan stated that they was almost "over-prepared" in the sense that they had read many academic articles that none of the industry members knew specifics about. Both had the similarities that going into the interview stage, they had very broad questions that did not quite relate to each other. Those questions did not encourage the high-ended answers this study promotes.

Potential interview questions have been planned alongside these sections. However, much like the issues with the alums, they are too broad and are disjointed of each other; often focusing on several different aspects of security practices. More thought is going into these questions to having a specific focus, which will provide the semi-structured interview the flow it needs to collect concise data.

Time slots have been scheduled for interviews to take place in.

3.3 Pilot Study

After obtaining relevant feedback on the questions, a suggestion was made to run a small pilot study. The objective of a pilot study is to enhance the likelihood of success in the main study and to avoid any risks to completion [23]. The first pilot study conducted was to provide evidence on the level of efficiency of the outlined potential interview questions. The efficiency being that of the potential to obtain open answers with a ultimate focus in mind. This focus will allow for more detailed answers which can be analysed to draw closer comparisons to form a stronger theory. The participant of the pilot study was another alum of the university and a personal contact. This pilot solidified that the potential questions are definitely too broad in scope. It was also highlighted that a few questions were quite similar and can be condensed. The questions were also not as opened-ended as desired, which made the answers seem not very valuable. As this pilot study was about testing the questions the participant of the pilot study was asked every question. This meant that this interview did not follow a typical grounded theory approach in which questions are asked dependent on the participant.

For the following pilot interview, this was not an issue as with more clarity on questions. Therefore the typical grounded theory approach to interviews was followed and questions were dependent on the interviewee. The person being another personal contact. More concise questions were asked, but from this second interview, it is apparent that the questions need to be written in a way that promotes discussion. As an interviewer, there also needs to be more practice in continuing the conversation and adapting questions to the last answer.

Overall, this small pilot study was essential in providing some more clarity on the interview process. It also supplied practice in conducting interviews and has helped in the continuous process of defining questions.

3.4 Advertising

The study will need to be advertised through mailing lists and websites like OWASP Meetup and LinkedIn. A recruitment post has been made for this as well as the support of a simple web-page (https://homepages.ecs.vuw.ac.nz/ sajwanlava/) [24] to present this study as professional and legitimate – traits especially important to programmers interested in security practices. The advertising has not been released yet as the human ethics application is still pending approval. However, as everything has been planned and ready, as soon as the approval has been made, recruitment can begin.

Following the principle of Whai wāhi, the recruitment post and web-page include the use of Te Reo. This is simple way of respecting tangata whenua, and is also more welcoming.

Chapter 4

Future Work

This section outlines the remaining work to do for the completion and evaluation of this project. It will also provide a proposed timeline in which this will happen.

4.1 Work Remaining

The work completed this semester has laid the foundations to start work on the formal investigation as soon as the human ethics application is approved. The work remaining consists of outlining some more relevant interview questions, conducting interviews and analysing answers to find an overarching theory.

Defining relevant interview questions has been partially completed. By outlining sections in the interview guide that was submitted with the human ethics application the topics that the questions should fall under are known. After pilot testing there has been a better understanding of the types of questions to ask. Next steps for writing potential questions are to develop them into questions which focus on a specific topic, while also making sure they feature a majority of open-ended questions. These types of questions will motivate the participants to give longer and more concise responses which will allow for patterns to form when analysing the answers.

When the human ethics application is approved sampling can occur. As the recruitment methods have all been finalised, all that needs to be done is posting of the relevant information on mailing lists, Meetup and LinkedIn groups, and also using my own connections. They will be selectively chosen dependent on their role titles and other diversifying factors in order to find patterns across groups of people consequently avoiding any biases. It is important that recruitment occurs through different mediums, as it is not always that everyone will be interested in participating – especially with a topic related to security. Sampling then leads onto data collection.

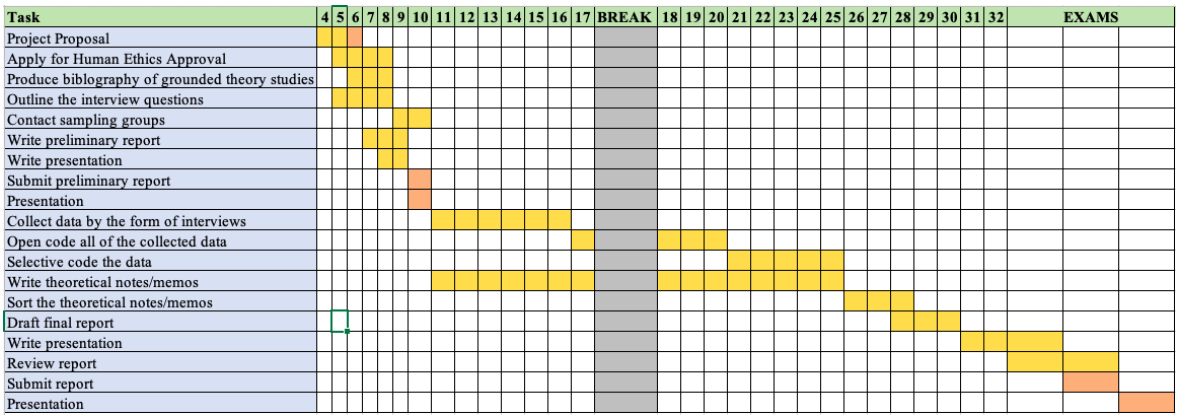
The form of data collection for this study is through interviews. They will be recorded to allow for focus to be on the participant and to mitigate a flow of conversation. This allows to concentration to be evenly distributed through the different steps of study. The interview will be semi-structured to allow for evolution in the questions [15].

Analysis will occur after each interview. This process will use open coding to analyse key points from the interview transcript [15]. Open coding is the process of keeping the mind free from any biases when sorting information. This means any assumptions should

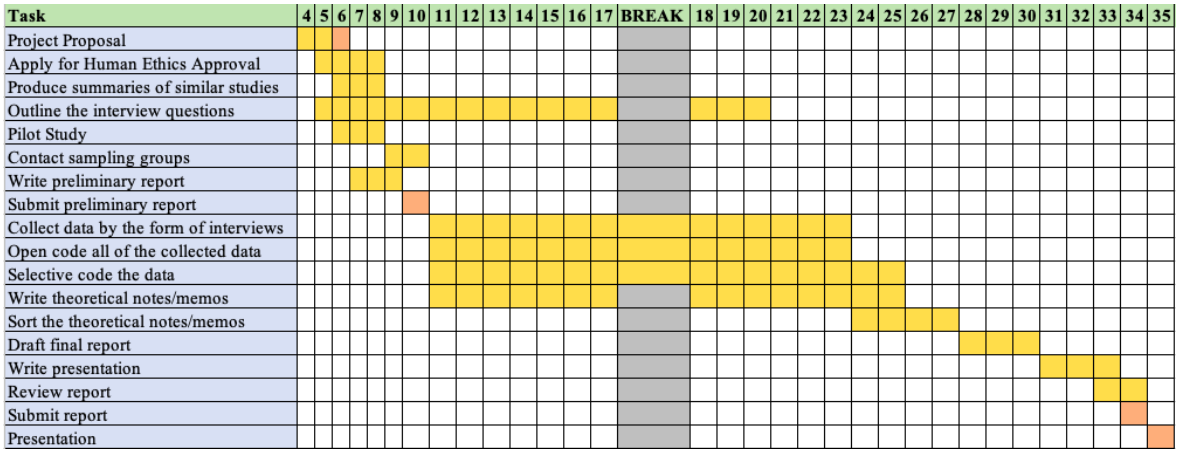
be ignored and ideas can only form from the data collected. This part of the remaining work is expected to take the longest. When concepts are identified these can influence the iterative nature of the interview and allow for the following interview to perhaps have different questions, target towards the found concepts. After the interviews and their following analysis, the core categories are found and then the theory can be presented in the final report and presentation.

There are limitations to evaluating the solution as the project does not produce a technical artefact. Pertaining to the method; there are two significant areas of evaluation that can be taken. These are the evaluation of the research process and theory and will occur after the generation of the final theory. By evaluating these two areas, it can be examined whether correct procedures have taken place, and determine whether project goals have been met. Past researchers; Aaron Pang, Nathan Newton and Brendan Julian, have evaluated their grounded theory research by either one of those areas or both [10, 8, 25].

4.2 Proposed Timeline



Above shows the Gantt chart which was outlined during the submission of the proposal. This outlined the timeline that the project would follow and what deadlines would fall within this course.



The above shows the now amended timeline. Not much has changed as I am following the proposed timeline quite closely. There have been additions of a pilot study which ran

across weeks 6 and 7. There are still details awaiting regarding the examination period in semester two so the "EXAM" columns are amended to being week columns. The initial analysis stage of this research has also been pulled back to starting alongside the interview process as analysis will ideally occur after each interview. Similarly, the theoretical notes will start to be written during the interview and analysis parts. The interview process has also been lengthened to allow for at least one interview a week in order to ensure that thorough analysis can take place and appropriate iteration of questions.

The entire timeline is dependent on whether the human ethics application obtains approval by the end of trimester one. If this does not occur, the entire timeline will have to shift back and tasks may have to be condensed.

Chapter 5

Feedback

Feedback on what would be an interesting area of focus would be much appreciated. I am currently focusing on education, but that almost seems like a overdone field. However, it is something of interest to me, so perhaps any input on how to make it more unique. Any feedback on the potential questions and one how to adapt questions to participants will also be much appreciated. Overall, interview and grounded theory feedback would also be helpful.

Bibliography

[1] C. Weir, I. Becker, J. Noble, L. Blair, M. A. Sasse, and A. Rashid, "Interventions for long-term software security: Creating a lightweight program of assurance techniques for developers," *Software: Practice and Experience*, vol. 50, no. 3, pp. 275–298, 2020.

[2] M. of Health, "Cyber security incident." [Online]. Available: `https://www.health.govt.nz/our-work/emergency-management/cyber-security-incident`, [Accessed May 31 2020].

[3] M. of Health, "Update on tū ora cyber security incident at 8 october 2019." [Online]. Available: `https://www.health.govt.nz/system/files/documents/pages/health_report_8_october_20191935_redacted.pdf`, [Accessed May 31 2020].

[4] M. John, F. Maurer, and B. Tessem, "Human and social factors of software engineering: Workshop summary," *ACM SIGSOFT Software Engineering Notes*, vol. 30, pp. 1–6, 07 2005.

[5] Y. Acar, S. Fahl, and M. L. Mazurek, "You are not your developer, either: A research agenda for usable security and privacy research beyond end users," in *2016 IEEE Cybersecurity Development (SecDev)*, pp. 3–8, 2016.

[6] C. Weir, I. Becker, J. Noble, L. Blair, M. A. Sasse, and A. Rashid, "Interventions for long-term software security: Creating a lightweight program of assurance techniques for developers," *Software: Practice and Experience*, vol. 50, no. 3, pp. 275–298, 2020.

[7] S. G. Lorrie Faith Cranor, *Security and Usability*. O'Reilly Media, 2005.

[8] B. Julian, J. Noble, and C. Anslow, "Agile practices in practice: Towards a theory of agile adoption and process evolution," pp. 3–18, 04 2019.

[9] H. Assal and S. Chiasson, "think secure from the beginning," in *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems - CHI 19*, ACM Press, 2019.

[10] N. Newton, C. Anslow, and A. Drechsler, *INFORMATION SECURITY IN AGILE SOFTWARE DEVELOPMENT PROJECTS: A CRITICAL SUCCESS FACTOR PERSPECTIVE*, pp. 8–14. 06 2019.

[11] I. Facebook, "A tool to detect bugs in java and c/c++/objective-c code before it ships." [Online]. Available: `https://fbinfer.com/`, [Accessed May 31 2020].

[12] C. Sadowski, J. van Gogh, C. Jaspan, E. Soederberg, and C. Winter, "Tricorder: Building a program analysis ecosystem," in *International Conference on Software Engineering (ICSE)*, 2015.

[13] I. Synopsys, "Coverity scan static analysis." [Online]. Available: `https://scan.coverity.com/`, [Accessed May 31 2020].

[14] Raygun, "Raygun." [Online]. Available: https://raygun.com/, [Accessed May 31 2020].

[15] R. Hoda, J. Noble, and S. Marshall, "grounded theory for geeks," in *ACM International Conference Proceeding Series*, 2011.

[16] SPG, "Alumni." [Online]. Available: https://ecs.wgtn.ac.nz/Groups/SPG/Alumni, [Accessed May 31 2020].

[17] A. I. Security, "Cyber security market research report." [Online]. Available: https://www.kordia.co.nz/aura-cyber-security-market-research-2019, [Accessed May 25 2020].

[18] D. of the Prime Minister and Cabinet, "New zealand's cyber security strategy 2019." [Online]. Available: https://dpmc.govt.nz/sites/default/files/2019-07/Cyber\%20Security\%20Strategy.pdf, [Accessed May 25 2020].

[19] OWASP, "Owasp secure coding practices." [Online]. Available: https://owasp.org/www-pdf-archive/OWASP_SCP_Quick_Reference_Guide_v2.pdf, [Accessed May 25 2020].

[20] D. Kirk and E. Tempero, "Software development practices in new zealand," in *2012 19th Asia-Pacific Software Engineering Conference*, vol. 1, pp. 386–395, 2012.

[21] V. H. E. Committee, "Human ethics policy." [Online]. Available: https://www.wgtn.ac.nz/documents/policy/research-policy/human-ethics-policy.pdf, [Accessed May 22 2020].

[22] O. T. for Children and the Ministry of Education, "Children's act 2014." [Online]. Available: http://www.legislation.govt.nz/act/public/2014/0040/latest/DLM5501618.html?src=qs, [Accessed May 22 2020].

[23] L. Thabane, J. Ma, R. Chu, J. Cheng, A. Ismaila, L. P. Rios, R. Robson, M. Thabane, L. Giangregorio, and C. H. Goldsmith, "A tutorial on pilot studies: the what, why and how," *BMC medical research methodology*, vol. 10, no. 1, pp. 1–1o, 2010.

[24] L. Sajwan, "Why do programmers do what they do? recruitment webpage." [Online]. Available: https://homepages.ecs.vuw.ac.nz/~sajwanlava/, 2020.

[25] A. Pang, C. Anslow, and J. Noble, "What programming languages do developers use? a theory of static vs dynamic language choice," in *Conference: 2018 IEEE Symposium on Visual Languages and Human-Centric Computing (VL/HCC)*, pp. 239–247, 10 2018.

Appendix A

Proposal

VICTORIA UNIVERSITY OF WELLINGTON
Te Whare Wananga o te Upoko o te Ika a Maui

School of Engineering and Computer Science
Te Kura Mātai Pūkaha, Pūrorohiko

PO Box 600
Wellington
New Zealand

Tel: +64 4 463 5341
Fax: +64 4 463 5045
Internet: office@ecs.vuw.ac.nz

Why Do Programmers do What They Do?

Lavanya Sajwan

Supervisor(s): James Noble, Craig Anslow

Submitted in partial fulfilment of the requirements for
Bachelor of Engineering with Honours in Software Engineering

Abstract

Technologies are continually adapting to match ever-changing trends, and as this occurs, new vulnerabilities are exploited by malignant attackers and can cause significant economic damage to companies. Programmers are therefore repeatedly having to expand knowledge and skills to protect software. We must understand the thinking behind the decisions and influences of programmers to interpret how they implement and adopt security practices. This proposal will cover an overview of the project 'Why Do Programmers do What They Do?', regarding the security choices programmers make, and the output of the project will ultimately present a theory on the chosen topic.

1. Introduction

As software is now ubiquitous across industry and it is impossible not to have a presence in the tech sphere. Consequently, software security has become so significant, programmers have to ensure that the security processes that they implement are resilient to any attacks. Lack of attack prevention can cause leakage of sensitive information, massive economic damage and danger to massive numbers of users and employees, consequently opening business, clients and end-users to exploitation by external bodies. Unfortunately, every day, we hear of organisations that have been compromised [1].

This project will investigate how software developers implement and adopt security practices in the work they do in order to develop an understanding of what influences and impact decisions surrounding their technical work. This project will be conducted using grounded theory. Grounded theory is a method which aims to establish a theory when there is none [2], and it is a commonly used method for data analysis. Interviews will take place to collect the data, from which the answers will be analysed to draw conclusions on standard security practices in the professional workplace.

2. The Problem

Qualitative research is often neglected and overlooked in favour of more quantitative reasoning and technical traits such as the security method used or the programmers task-completion rate [3]. Programmers provide a human aspect to a technical solution and therefore, there should be a shift towards understanding the more background ‘soft’ processes that occur when making decisions; why are the choices made based on past influences, and how they affect the programmers work in the present?

Past the research aspect, when security and privacy issues do occur in real-world scenarios, developers are blamed first as it is their projects that have allowed the vulnerabilities to be exploited [4]. While developers do make mistakes, they also do need the support to make better security decisions, and this support is currently lacking in the industry [4]. Education is limited past initial acceptance within organisations, and often developers have a blasé attitude to the matter expecting another team to fix the issue [1]. Furthermore, security mechanisms often have an increased complexity as well, which make them difficult to understand to then use [5].

Exploring this topic is essential as it allows for a more comprehensive understanding of how and why programmers think the way they do, and of the human and social aspects of Software Engineering [6]. We want to understand what solutions developers are using to implement in their security practices, if at all. The findings from this can support developers in terms of education and the better design of security methods in programming [7] that have an emphasis on usability.

3. Proposed Solution

This project aims to implement a theory as to why programmers implement and adopt security practices in the work they do by interviewing professional developers and using the Grounded Theory Method to analyse the outcomes. Grounded theory is a research method to analyse qualitative data. There are several thorough steps which include; sampling, data collection, data analysis, theoretical note writing, identifying core categories, forming theoretical outlines and presenting a theory.

The findings of this project can be used to identify what security methods developers find as beneficial in their programming. This will allow programmers to complete their work to a high standard, by adhering to proper security protocols, thus overall making their work of a higher value both in a secure and professional sense.

The project will be an informative investigation on understanding the decisions programmers make, therefore obtaining data from actual programmers as soon as possible is essential for the smooth running of this project; human ethics approval will be needed quickly.

When the human ethics application is approved, participants will be recruited by posting on tech-related groups (i.e. From Meetups and Linkedin) and mailing lists and also using mine and my supervisor contacts [4]. At this point, I can then start semi-structured interviews with 10-20 interested individuals on their security practices while programming. These people will all be developers in New Zealand that are in varying stages of their careers and career paths to allow for a broader range of responses and a case study relevant to New Zealand. Examples of appropriate job titles include; DevOps engineer, front-end security developer, database administrator and security architect.

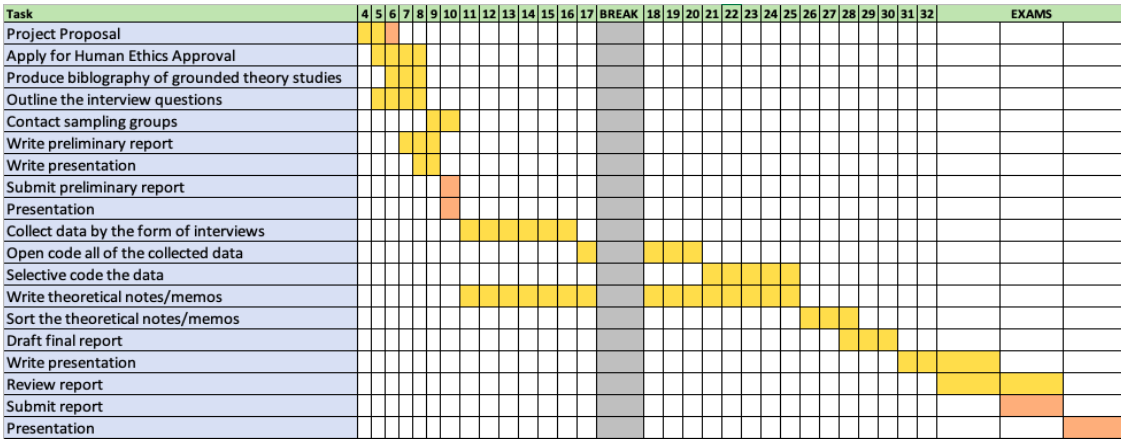
Potential questions include:

- What languages do you use?
- Are you changing languages based on what you do?
- Are you adding any specific security components?
- How are you managing security in languages; do you use libraries, toolkits and/or frameworks?
- When do you use security practices in your work; start, end or during a project?
- Do you do maintenance on security features afterwards?
- How many years experience do you have with security?
- What qualifications do you have (tertiary and industry)?
- How do you test the security features that you implement?
- What is your role in your project team?
- How did you get involved with security as a career?

This project will lead to a new, more in-depth understanding of the psychology of the decisions made by programmers. The research done by this project could lead to future qualitative research to be done on another under-developed topic on why programmers do what they do. Paired with this research, that future one could help build a profile of a programmer and their thought processes. Data collected could also be the foundation that allows a developer to build a tool that helps other developers implement proper security practices; a Grammarly for security.

Gantt Chart of the proposed timeline:

This has been edited to account for the COVID-19 lockdown that New Zealand is currently under, but it does not account for any future lockdowns. If future lockdowns occur, the project workflow should not be significantly affected as this project involves a lot of research and work that can be done outside of the physical engineering and computer science (ECS) school.



The break outlined is a hesitant gap as there has been a five-week halt on course work and a lack of communication from the broader university faculty about the university procedures after lockdown.

4. Evaluating your Solution

There are limitations to evaluating the solution as the project does not produce a technical artefact. Pertaining to the method; there are two significant areas of evaluation that can be taken [7]. These are the evaluation of the research process and the generation of the final theory.

Evaluation of the research process can occur by examining the interviewee recruitment process, whether the interview questions are connected to the overarching question being asked, and the relevance to the categories in the data collection [7]. Evaluation of the theory can be performed by using Glaser's four criteria of; fit, work, relevance and modifiability [8]. These criteria are often used to evaluate grounded theory work [7].

5. Ethics and Resourcing

5.1. Ethics

A human ethics application will need to be approved before any work with participants will occur. This will need to be done as soon as possible as a significant portion of this project is dependent on the interviews.

The interviews will be confidential rather than anonymous as they are done in-person and to also allow for follow up questions if necessary. Participants will be welcome to leave at any time during the interview, do not have to answer any questions they do not want to and can choose to withdraw data within a week after the interview if they would like.

5.2. Safety

Interviews should be done in safe and private environments, with all participants clear on earthquake and fire evacuation procedures relevant to their location. I will ensure that my own mental and physical wellbeing is taken into account, by mitigating any significant amounts of pressure, Repetitive

Strain Injury (RSI) and migraines. Working without breaks for extended periods will increase eye strain and encourage bad ergonomics which could cause RSI and migraine issues.

For both myself, as the surveyor, and for my interviewee's, I will ensure that interviews will be taken between the times 9 am and 5 pm to support work/life balance. Due to the recent COVID-19 outbreak, I will offer Zoom interviews for those who are unable or unwilling to meet directly. For in-person interviews, I will provide a box of tissues in the room and a bottle of sanitiser, while maintaining social distancing and sanitising the room between individuals (if I do happen to have two consecutive interviews).

5.3. Budget

Sanitiser, a box of tissues and disinfectant will be needed to promote healthy hygiene practices during in-person interviews.

All individuals who participate in the interviews will be given a $10 supermarket voucher, and all will go into the draw to win a $60 supermarket voucher.

Therefore, the estimated budget for this project will be approximately $180-$280, dependent on the number of participants and the inflated cost of sanitiser. This is within the approved course budget of $500.

5.4. Space and Access

Access to private ECS meeting rooms on campus will be necessary. Small rooms such as CO242A and CO242B will be ideal as they are relatively private, quiet and small enough to be comfortable locations for one-on-one interviews. The Kelburn campus is an excellent location as it is close to the central business district, so participants do not need to go too far out of their way to attend the interview.

If the lockdown persists, I will need access to a university Zoom account to allow for an unlimited time when interviewing via video.

5.5. Risks and Hazards

Risks	Likelihood	Severity	Mitigation
COVID-19 Lockdown	High	High	Have regular video call meetings with supervisors and communicate with participants via video.
Participants are ill/Access to participants are limited	Moderate	Moderate	Ask many people to participate, so if someone cannot make it, the saturation of available people will allow the development cycle to continue as planned. Want the research to have 10-20 participants to interview.

Ethics approval takes too long	Moderate	High	Start this as soon as possible to allow for any delays that revisions of the application may cause.
Underestimation of project life cycle	Moderate	High	Need to strictly timebox issues and break down tasks into reasonable blocks.
Failure to obtain relevant data	Low	High	Interview questions need to be planned and revised to ensure that they are relevant to the grounded theory question.

6. Bibliography

1. Weir Charles, Becker Ingolf, Noble James, Blair Lynne, Sasse M.Angela, Rashid Awais (2019). Interventions for long‐term software security: Creating a lightweight program of assurance techniques for developers. Software: Practice and ExperienceVolume 50, Issue 3. DOI: https://doi-org.helicon.vuw.ac.nz/10.1002/spe.2774
2. Julian, Brendan. 2018. Agile Practices: A Theory of Agile Adoption and Evolution. Final ENGR489 Honours Project Report.
3. Michael John, Frank Maurer, and Bjornar Tessem. 2005. Human and social factors of software engineering: workshop summary. SIGSOFT Softw. Eng. Notes 30, 4 (July 2005), 1-6. DOI:https://doi-org.helicon.vuw.ac.nz/10.1145/1082983.1083000
4. Y. Acar, S. Fahl and M. L. Mazurek, "You are Not Your Developer, Either: A Research Agenda for Usable Security and Privacy Research Beyond End Users," *2016 IEEE Cybersecurity Development (SecDev)*, Boston, MA, 2016, pp. 3-8. doi: 10.1109/SecDev.2016.013
5. Cranor, Lorrie Faith and Garfinkel Simson. (August 2005). Security and Usability. O'Reilly Media, Inc. ISBN: 9780596008277
6. Hoda, Rashina & Noble, James & Marshall, Stuart. (2011). Grounded Theory for Geeks. ACM International Conference Proceeding Series. 10.1145/2578903.2579162.
7. Assal, Hala and Chiasson, Sonia. 2019. "Think secure from the beginning": A Survey with Software Developers. CHI '19: Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems. DOI: https://doi.org/10.1145/3290605.3300519
8. Pang, Aaron (2018). Why Do Programmers Do What They Do. Final ENGR489 Honours Project Report.
9. GLASER, B. G. Theoretical sensitivity: Advances in the methodology of grounded theory. Sociology Pr, 1978.

Appendix B

Application

Human Ethics Application

Application ID :	0000028506
Application Title :	Why Do Programmers Do What They Do?
Date of Submission :	15/05/2020
Primary Investigator :	Lavanya Sajwan; Principal Investigator
Other Personnel :	Prof James Noble; Supervisor
	Dr Craig Anslow; Associate Investigator

Research Form

Application Type

Is this application for:*

◉ Research ○ Teaching only

Please select **'Research'** below and then select **'Save'** to access the rest of the form.

*

Research

Research Overview

Application Details

1. Application ID

0000028506

2. Title of project
*(Click the ? icon for more info)**

Why Do Programmers Do What They Do?

3. School or research centre*

Engineering and Computer Science

4. The following questions will help the committee assess whether your application is categorised as a Category A (more than low risk) or Category B (low risk).

Please check all of the boxes that apply. You will be asked for more information about some of these questions later in the application.

Check the box if your study:

4a Is health research*

○ Yes ◉ No

4b Is an intervention study*

○ Yes ◉ No

4c Involves the use, collection or storage of human tissue*

○ Yes ◉ No

4d Involves processes that use EEG, ECG, MRI, TMS, FMRI, EMG, radiation, invasive or surface recordings*

○ Yes ◉ No

4e Involves collection of information about illegal behaviour, or information that has been obtained illegally*

○ Yes ◉ No

4f Involves people who are not giving consent to be part of the study (other than observational research in a public place)*

○ Yes ◉ No

4g Involves participants under the age of 16*

○ Yes ◉ No

4g (i) Will a parent/guardian be asked to give consent for the child/young person to participate in research?*

○ Yes ○ No ◉ N/A

4g (ii) Will more than one meeting be held with the child/young people without others present? *

○ Yes ○ No ◉ N/A

4h Involves participants whose ability to consent freely is compromised due to context (e.g. people in prison), or a limited capability to make independent rational decisions (e.g. those with a serious intellectual disability).*

○ Yes ◉ No

4i Involves the use of concealment or covert observations, including those conducted online or conducted in social media. *
○ Yes ◉ No

4j Involves the use of previously collected personal information, other data, or biological samples for the collection of which there was no explicit consent for use in research.*
○ Yes ◉ No

4k Involves deception of the participants, including concealment of the true purpose of the research*
○ Yes ◉ No

4l Involves the use of highly sensitive information (see policy for definition)*
○ Yes ◉ No

4m Involves a focus on, has particular importance for, or impacts on Māori*
○ Yes ◉ No

4n Involves any other group (for example cultural or religious), other than Māori, and has the potential to cause discomfort or disruption to members of that group*
○ Yes ◉ No

4o Involves any direct financial interest in the outcome of the research by any member of the research team or external sponsor*
○ Yes ◉ No

4p Involve a conflict of interest or the appearance of a conflict of interest for the researcher (for example, where the researcher is also the lecturer/teacher/treatment provider/colleague/manager or employer of the participants)*
○ Yes ◉ No

4q Involve any situation which may put the researcher at risk of harm (e.g. overseas in politically unstable countries)*
○ Yes ◉ No

4r Involve a reasonable expectation that participants may experience (at a greater level than in everyday life) physical discomfort, emotional discomfort, or psychological or spiritual harm (e.g. asking participants to recall upsetting events)*
○ Yes ◉ No

Relationship to other Projects

5. Does this application relate to any previous applications submitted to an ethics committee (at VUW or other Institute)?*
◉ Yes
○ No

5a. If this was a Victoria University of Wellington human ethics applications, please search and add the related ethics applications from the below search window.

Search by title (partial or complete) or application ID (partial or complete):

This question is not answered.

5a (i). If you can't find the application above, please enter the application number here.

0000024839

5a (ii). If this was an ethics committee from another institution, please upload supporting documentation (such as a letter of approval) in the document section.

5a (iii). If your research has been assessed by a Health and Disability Ethics Committee (HDEC) and found to be Out of Scope, please upload a copy of the Scope of Review form submitted to HDEC and the Out of Scope letter on the Documents page.

Personnel

Personnel
To add other researchers, enter their user name, if known, or search for their first or last name (whichever is the most unusual). Click the search icon to run the search, and select the person from the list view. Click on '**OK**' at the bottom right corner to save the person record.

1	First Name	Lavanya
	Last Name	Sajwan
	Full Name	Lavanya Sajwan
	AOU system code	Engineering and Computer Science
	Position	Principal Investigator
	Primary Investigator?	Yes
2	First Name	Craig
	Last Name	Anslow
	Full Name	Dr Craig Anslow
	AOU system code	Engineering and Computer Science
	Position	Associate Investigator
	Primary Investigator?	No

6. Are any of the researchers from outside Victoria?*

- ○ Yes
- ◉ No

7. Is the principal investigator a student?*

- ◉ Yes
- ○ No

Student Researcher

7a. What is your course code (e.g. ANTH 690)?*

ENGR489

7b. Supervisor

To add your supervisor enter their user name, if known, or search for their first or last name (whichever is the most unusual). Click the search icon to run the search, and select the person from the list view. Click on '**OK**' at the bottom right corner to save the person record. *

1	Given Name	James
	Surname	Noble
	Full Name	Prof James Noble
	AOU	Engineering and Computer Science
	Position	Supervisor

7c. What is your email address? (this is needed in case the committee needs to contact you about this application)*

sajwanlava@myvuw.ac.nz

Scope of Research

Project Details

8. Describe the aims and objectives of this project
Provide a brief summary in plain language of the purpose, research questions/hypothesis, and objectives of your project. *

This project will investigate how software programmers may implement and adopt security practices in the work they do, in order to develop an understanding of the influences and impacts on decisions surrounding their technical work. Examples of influences can include, type of education, whether the organisation further educates the employees, and what programming languages have they had experiences with.

This project will be done by using grounded theory and interviews will to take place to collect the data, to which then analysis of answers will then need to occur.

9. Describe the benefits and scholarly value of the project
Briefly place the project in perspective, explaining its significance and worthwhile outcomes. Include how this project will build on relevant literature, including references if appropriate.
*

Qualitative research is often neglected and overlooked in favour of more quantitative reasoning and technical traits; the processing speed, the programmers task-completion rate. Programmers provide a human aspect to a technical solution and therefore, there should be a shift to understanding the more background 'soft' processes that occur when making decisions; why are the choices made based on past influences, and how they affect the programmers work in the present?

Exploring this topic is essential as it allows for more understanding on how and why programmers think the way they do, and it builds a more robust understanding of the human and social aspects of Software Engineering The findings of this can be used to identify what security methods developers find as beneficial in their programming. This will allow programmers to complete their work to a higher standard, thus overall making their work of a higher value.

10. Explain any ethical issues your research raises for participants, yourself as the researcher, or wider communities and institutions, and how you will address these. This is an opportunity to present what you think the key risks are in your project and show how you have taken them into account.*

The project aims to investigate how security practices are implemented and adopted in the work programmers in industry work on. Steps will need to be taken to ensure that the interview questions will be written in a way that does not reveal the individuals personal passwords or suggest any hints to it. As they will be professionals, the questions will also have to be worded in a way that does not expose specific business secrets. By doing both of these, the privacy of the person and the company can be maintained and protected. Participants will not require approval from organisations to partake in this study, as the participants will not be named in any produced texts, and therefore, will not be linked to any specific organisation. It will be explained to participants that they should not reveal any business secrets or passwords at the start of the interview, and this piece of information will also be stated in the supporting participant information sheet document.

There is also a risk of discovering an organisation's security practices, which means the interview data needs to be kept secure and confidential. For instance, any reports or publications should avoid including compromising information and allow interviewees to see their transcripts to comment and edit any information.

Key Dates

If approved, this application will cover this research project from the date of approval for up to 3 years.

11. Proposed start date for data collection*

06/07/2020

12. Proposed end date for data collection*

28/02/2021

13. Proposed end date for research project*

28/02/2021

Proposed source of funding and other ethical considerations

14. Indicate any sources of funding

- Internally: by a University grant, such as the University Research Fund
- Externally: funding from an external organisation for this project, or a scholarship awarded by an external organisation
- Self-funded: paying for research costs such as travel, postage etc. from your own funds

Tick all that apply:

- [x] Internally funded
- [ ] Externally funded
- [x] Self-funded

15. Is any professional code of ethics to be followed?*

- ( ) Yes
- (•) No

16. Do you require ethical approval from any other organisation, such as another tertiary institution in New Zealand or overseas, or a District Health Board?*

- ( ) Yes
- (•) No

Data Collection and Recruitment

Data Collection

17. Please select all forms of data collection you will use in your project*

- [x] Interviews
- [ ] Focus groups
- [ ] Questionnaires
- [ ] Observation
- [ ] Other

18. Provide an explanation of the sampling rationale for your study.
E.g. representative sampling of a particular population, purposive sampling, convenience sampling. Include here your eligibility criteria for potential participants -- will there be particular criteria for participants to be included in your study, or criteria that will exclude them? *

The study will follow purposeful sampling as the participants will be those working in the industry and ideally have a range of job titles associated with programming and years in the field in order to find interesting comparisons during the interview process in the way security practices are adopted in the developed software. They can be a part of any type of organisation; government, private, non-profit etc.

Examples of appropriate jobs associated with the individuals can be; devops engineers, front-end security developers, database administrators, security architects etc.

Participants will consequently be filtered by appropriate job titles and anyone younger than the age of 18.

19. How many participants will be involved in your research?
Please specify how many groups and how many participants in each group. *

Up to 30 participants from the industry who are familiar with security practices through the professional work they do.

20. What are the characteristics of the people you will be recruiting?*

The key characteristic of the individuals will be their programming experience, security education, and age. They will have a technical role within the organisation. The study hopes to capture a range of ages and levels experience in their role in order for in-depth comparisons for analysis. Therefore, there is no specific minimum or limit on the years of programming experience, or what kind of experience, and security education sought. However, participants do have to be at least 18 years old. Participants jobs will all be New Zealand based. Participants can also work across a range programming fields eg. gaming, education, financial, analysis.

21. Outline in detail the method(s) of recruitment you will use for participants in your study. Include here how potential participants will be identified, who will contact them and how. Please include copies of all advertisements, online posts or recruitment emails in the 'Documents' section. *

I will make contact with sample groups with a request of participation by posting on groups, mailing lists and by using supervisor and my own connections. Such groups could be security groups on the websites, Meetup and Linkedin. Mailing lists can consequently be obtained from those groups as well.

A pilot study will be conducted with 2-3 participants. These participants will be recruited directly by me and are all personal contacts; friends, and family friends.

22. Explain the details of the method of data collection. For example, describe the location of your research procedures, if appropriate (e.g. where your interviews will take place). If necessary, upload a research protocol in the 'Documents' section.*

The interviews will be confidential rather than anonymous as they are done in-person and to also allow for follow up questions if necessary. Participants will be welcome to leave at any time during the interview, do not have to answer any questions they do not want to and can choose to leave the study within a week after the interview if they would like.

Interviews, should be done in safe and private environments, with all participants clear on earthquake and fire evacuation procedures relevant to their location. Due to the recent COVID-19 outbreak, I will offer zoom interviews for those who are unable or unwilling to meet directly. Consent can be obtained over email by sending the information sheet and consent form content to the participant in an email body and they reply to that email with "I consent".

For in-person interviews, I will provide a box of tissues, a bottle of sanitiser, and maintain social distancing. The small meeting room will be wiped down and disinfected between interviews.

The interviews will be voice recorded, and will then be transcribed.

23. Will your research project take place overseas?*

- ○ Yes
- ◉ No

24. Does the research involve any other situation which may put the researcher at risk of harm (e.g. gathering data in private homes)?*

- ○ Yes
- ◉ No

Participants and Informed Consent

25. Does your research target members of a vulnerable population?
This includes, but is not limited to, children under the age of 16, people with significant mental illness, people with serious intellectual disability, prisoners, employees and students of a researcher, and people whose health, employment, citizenship or housing status is compromised. Vulnerability is a broad category and encompasses people who may lack the ability to consent freely or may be particularly susceptible to harm.*

- ○ Yes
- ◉ No

26. Have you undertaken any consultation with the groups from which you will be recruiting, regarding your method of recruitment, data collection, or your project more widely?*

- ○ Yes
- ◉ No

27. Will your participants receive any gifts/koha in return for participating?*

- ◉ Yes
- ○ No

27a. Describe the gifts/koha and the rationale.*

All individuals who participated in the interviews will be given a $10 supermarket voucher, and all will go into the draw to win a $60 supermarket voucher to thank them for their time and provide them with an incentive.

28. Will your participants receive any compensation for participation (for instance, meals, transport, or reimbursement of expenses)?*

- ○ Yes
- ◉ No

29. How will informed consent be obtained? (tick all that apply to the research you are describing in this application)*

- ☐ Informed consent will be implied through voluntary participation (anonymous research only)
- ☐ Informed consent will be obtained through a signed consent form
- ☑ Informed consent will be obtained by some other method

29a. Describe the other method*

Participants can consent over email by simply sending the consent form content to the participant in an email body and they reply to that email with "I consent".

Treaty of Waitangi

Treaty of Waitangi

30. How does your research conform to the University's Treaty of Waitangi Statute? (you can access the statute from Victoria's Treaty of Waitangi page)*

The study does not involve knowledge directly related to Te Āo Māori but care should be taken to encourage the participation of Māori under the principle of Whai wāhi (participation). To encourage this, the study will be advertised to organisations where there is more emphasis on using Te Tiriti o Waitangi as part of their core values.

Pre-interview forms should include the use of Te Reo where appropriate, and participants need to know that they are able to edit/append/remove details after the interview has been undertaken as they have ownership of their information and as Te Tiriti o Waitangi states, I am just protecting their right of ownership.

Project Risks

Minimisation of Harm

31. Is it possible that participants may experience any physical discomfort as a result of the research?*

- ○ Yes
- ◉ No

32. Is it possible that participants may experience any emotional or psychological discomfort as a result of the research? (E.g. asking participants to recall upsetting events, viewing disturbing imagery.)*

- ○ Yes
- ◉ No

33. Will your participants experience any deception as a result of the research?*

- ○ Yes
- ◉ No

34. Is any third party likely to experience any special hazard/risk including breach of privacy or release of commercially sensitive information? This may occur in the instance participants are asked to discuss identifiable third parties in the research.*

- ◉ Yes
- ○ No

34a. Give details and indicate how you will manage this*

As this study involves questioning individuals on the security practices they implement in the software they develop there is a risk of exposing the company they work for. However, as outlined in question 10 of this application, there will be steps to prevent this happening by being careful of how questions are phrased. These include not publishing the interviewee and corresponding organisation name in any texts that are the result of this research.

35. Do you have any professional, personal, or financial relationship with prospective research participants? *

- ○ Yes
- ◉ No

36. What opportunity will participants have to review the information they provide? (tick all that apply)*

- ☑ Will be given a full transcript of their interview and given an opportunity to provide comments
- ☐ Will be given a full transcript of their interview and NOT given an opportunity to provide comments
- ☐ Will be given a summary of their interview
- ☐ Other opportunity
- ☐ Will not have an opportunity to review the information they provide

Confidentiality and Anonymity

37. Will participation in the research be anonymous?
'Anonymous' means that the identity of the research participant is not known to anyone involved in the research, including researchers themselves. It is not possible for the researchers to identify whether the person took part in the research, or to subsequently identify people who took part (e.g., by recognising them in different settings by their appearance, or being able to identify them retrospectively by their appearance, or because of the distinctiveness of the information they were asked to provide).*

- ○ Yes
- ◉ No

38. Will participation in the research be confidential?
'Confidential' means that those involved in the research are able to identify the participants but will not reveal their identity to anyone outside the research team. Researchers will also take reasonable precautions to ensure that participants' identities cannot be linked to their responses in the future.*

- ◉ Yes
- ○ No

38a. How will confidentiality be maintained in terms of access to the identifiable research data? (tick all that apply)*

- ☐ Access to the research will be restricted to the investigator
- ☑ Access to the research will be restricted to the investigator and their supervisor
- ☐ Focus groups will have confidentiality ground rules
- ☐ Transcribers will sign confidentiality forms
- ☐ Other

38b. How will confidentiality be maintained in terms of reporting of the data? (tick all that apply)*

- ☑ Pseudonyms will be used
- ☑ Data will be aggregated
- ☑ Participants will be referred to by role rather than by name
- ☐ Other

38b (i). Please provide details*

Participants in the study will not be named in any reports or summaries produced. The study uses grounded theory methodology so the people and the answers will be grouped to form a final theory on what influences programmers to make the decisions they do. The purpose of the study is not to focus on the individuals, but rather draw conclusions and similarities from their responses. Instead, the study will likely compare different groups of people based on key variables such as computing experience. Participants will not be directly quoted, and will be referred to by role or pseudonyms.

39. Will participation in the research be neither confidential nor anonymous, and participants will be identifiable in any outputs or publications relating to the research? *

- ○ Yes
- ◉ No

Data Management

Access, Storage, Use, and Disposal of Data

40. Which of the following best describes the form in which data generated in your study will be stored during the study?
See help text for guidance on these terms. Further info available on human ethics website.*

- ○ Identifiable
- ○ Potentially identifiable
- ◉ Partially de-identified
- ○ De-identified
- ○ Anonymous
- ○ Other

41. Which of the following best describes the form in which data generated in your study will be stored after the study is completed?
See help text for guidance on these terms. Further info available on human ethics website.*

- ○ Identifiable
- ○ Potentially identifiable
- ○ Partially de-identified
- ◉ De-identified
- ○ Anonymous
- ○ Other

42. Proposed date for destruction of identifiable research data (i.e. the date when data will be de-identified and personal information on participants destroyed)

*

31/12/2021

43. Proposed date for destruction of de-identified research data, including anonymous data

*

31/12/2021

44. Will any research data be kept for longer than 5 years after the conclusion of the research?*

- ○ Yes
- ◉ No

45. Who will have access to identifiable, de-identified or anonymous data, both during and at the conclusion of the research?*

- ○ Access restricted to the researcher only (whoever is named as PI)
- ◉ Access restricted to researcher and their supervisor
- ○ Access restricted to researcher and immediate research team, e.g. co-investigators, assistants
- ○ Other

46. Are there any plans to re-use either identifiable, de-identified or anonymous data?*

- ○ Yes
- ◉ No

47. What procedures will be in place for the storage of, access to and disposal of data, both during and at the conclusion of the research? (Check all that apply)
Information regarding appropriate data storage is available on the human ethics website. Note that storing research data on USB drives is strongly discouraged for security reasons. *

- ☑ All hard copy material will be stored securely e.g. in a locked filing cabinet
- ☑ All electronic material will be held securely, e.g. only on University servers, password protected
- ☑ All hard copy material will be appropriately destroyed (e.g. shredded) on the dates given above
- ☑ All electronic data will be deleted on the dates given (ITS should be consulted on proper method)

Dissemination

Dissemination

48. How will you provide feedback to participants?*

I will offer a summary of the results to be shared with the participants upon their request.

49. How will results be reported and published? Indicate which of the following are appropriate. The proposed form of publications should be indicated to participants on the information sheet and/or consent form*

- ☑ Publication in academic or professional journals
- ☑ Dissemination at academic or professional conferences
- ☑ Availability of the research paper or thesis in the University Library and Institutional Repository
- ☐ Other

50. Is it likely that this research will generate commercialisable intellectual property?
*(Click the ? icon for more info)**

○ Yes
◉ No

Supporting Documents

Documents

51. Please upload any documents relating to this application. Sample documents are available on the Human Ethics web page.

- Ensure that your files are small enough to upload easily, and in formats which reviewers can easily download and review.
- To upload a document click on the green arrow to the right of the named document. Follow the on screen instructions which will be displayed to upload a document.
- To replace a document, click the tick in the column to the right of the document you want to replace, and follow the screen instructions to continue.
- To add a new document click on 'New Document', at top right of the documents table. You **must** enter the document name in the box that appears. Click on 'OK'. Click on the green arrow which appears to the right of the file name to continue.
- Collate all your documents into one PDF or Word file, and upload as a new document. This should be labelled as 'Combined Documents'.

*

Description	Reference	Soft copy	Hard copy
Participant information sheet(s)	Participant_Information_Sheet.pdf	✓	
Participant consent form(s)	Consent_to_Interview.pdf	✓	
Interview questions or guide	Interview_Guide.pdf	✓	
Recruitment Posts	Recruitment_Post.pdf	✓	
RO Pre-Review Letter 21/04/2020	28506_Sajwan_Pre-review.docx	✓	

Application Sign Off

Application Feedback

Feedback

This page will be used to provide feedback between the Research Office and the researcher/s during the application review process.

Committee response to your application

Date

15/05/2020

Comments

Hi,
Please refer doc attached.
Thanks

Documents

28506_Sajwan_Revise and Resubmit.docx

Researcher response to requirements: please enter your comments below and then save.

This question is not answered.

If you have been asked to provide a response to the committee's comments in a document, please upload that document here and then **save**.

Changes_Summary.docx

Further required changes

Date

This question is not answered.

Comments

This question is not answered.

Documents

This question is not answered.

Researcher response to requirements: please enter your comments below and then save.

This question is not answered.

If you have been requested to respond to further feedback by uploading documentation here, please upload and then **save**.

This question is not answered.

Final Review Outcome

Final Review Outcome

This question is not answered.

Formal Notice of Approval

This question is not answered.

Risk Category

Based on answers to the screening questions (Q4), your application will be assessed as either Category A (higher than low risk), or Category B (low risk). The risk category will be reviewed by the Research Office before it is processed by the committee.

The risk assessment for this application is currently:

Category B (LOW RISK)

Appendix C

Participant Information Sheet

Why do Programmers Do What They Do?

INFORMATION SHEET FOR PARTICIPANTS

You are invited to take part in this research. Please read this information before deciding whether or not to take part. If you decide to participate, thank you. If you decide not to participate, thank you for considering this request.

Who am I?

Kia ora koutou! My name is Lavanya Sajwan and I am an Honours student in the school of engineering and computer science at Victoria University of Wellington. This research project is work towards partial fulfilment of the requirements for Bachelor of Engineering with Honours in Software Engineering.

What is the aim of the project?

This project is an informative investigation on how software programmers implement and adopt security practices in the work they do in order to develop an understanding of what influences and impact decisions surrounding their technical work. Your participation will support this research by providing insight to the solutions that programmers are using to implement in their security practices. Essentially this research aims to gather your experiences and compare them with those of your peers to understand the use of security practices in the New Zealand industry. This research has been approved by the Victoria University of Wellington Human Ethics Committee (Research Master Application ID: 0000028506).

How can you help?

You have been invited to participate because you are a professional programmer in the industry, familiar with working with security practices, and are over the age of 18 and this project aims to develop a theory as to why programmers implement and adopt security practices in the work, they do by interviewing professional programmer. It is important to gather data from individuals with varying career timelines and progressions as the data can be thoroughly analysed to form connections. I will interview you at Victoria University of Wellington's Kelburn campus, via Zoom or at another venue of your choice. I will ask you questions about your security practices and habits in your day-to-day work and how you make decisions regarding your methods of choice. It is advised that you refrain from naming any 3rd parties. If you agree to take part the interview will take 30-60 minutes of your time. I will audio record the interview with your permission and write it up later. You can choose to not answer

any question or stop the interview at any time, without giving a reason. You can withdraw from the study by contacting me at any time before the 20th of July 2020. If you withdraw, the information you provided will be destroyed. You may also choose to receive a copy of the interview transcript which will be emailed to you, and you will have the opportunity to add comments to the interview up to 2 weeks after receiving the transcript. You will be given a $10 supermarket voucher and go into the draw for a $60 supermarket voucher as koha to thank you for your time.

What will happen to the information you give?

This research is confidential, but may be limited due to small sample and nature of the research. You and your organisation will not be named in the final report, but title may be named and persons within or familiar with your organisation and title may be able to identify you and your organisation based on the distinctiveness of the information you provide. However, you may choose to not have any potential identifying information published.

Please do not name any 3rd parties and reveal any business secrets and passwords.

Your name and email address will be used to contact you in the event of winning the overall prize, and when a full transcript of your interview is sent if you choose to receive it.

Only my supervisors and I will read the notes or transcript of the interview. The interview transcripts, summaries and any recordings will be kept securely and destroyed on the 31st of December 2021.

What will the project produce?

The information from my research will be used in my Honours report and presentation. You will not be identified in either of these materials or in any supplementary reports such as publications in academic or professional journals.

If you accept this invitation, what are your rights as a research participant?

You do not have to accept this invitation if you don't want to. If you do decide to participate, you have the right to:

- choose not to answer any question;
- ask for the recorder to be turned off at any time during the interview;
- withdraw from the study up to 1 week after the interview has taken place;
- ask any questions about the study at any time;
- receive a copy of your interview recording;
- receive a copy of your interview transcript;
- edit/append/remove any details after the interview.

- be able to read any reports of this research by emailing the researcher to request a copy.

If you have any questions or problems, who can you contact?
If you have any questions, either now or in the future, please feel free to contact any of either one of the people listed:

Student Researcher:

Name: Lavanya Sajwan
University email address: sajwanlava@myvuw.ac.nz

Primary supervisor:

Name: James Noble
Role: Professor of Computer Science, Associate Dean (Postgraduate Research)
School: Engineering and Computer Science, Victoria University of Wellington
Phone: 04 463 6736
kjx@ecs.vuw.ac.nz

Secondary supervisor:

Name: Craig Anslow
Role: Senior Lecturer
School: Engineering and Computer Science, Victoria University of Wellington
Phone: 04 463 6449
craig.anslow@ecs.vuw.ac.nz

Human Ethics Committee information

If you have any concerns about the ethical conduct of the research you may contact the Victoria University HEC Convenor: Dr Judith Loveridge. Email hec@vuw.ac.nz or telephone +64-4-463 6028.

Appendix D

Participant Consent Form

Why do Programmers Do What They Do?

CONSENT TO INTERVIEW

This consent form will be held for 5 years.

Researcher: Lavanya Sajwan, School of Engineering and Computer Science, Victoria University of Wellington.

- I have read the Information Sheet and the project has been explained to me. My questions have been answered to my satisfaction. I understand that I can ask further questions at any time. The end research date is: 28th of February 2021.
- I agree to take part in an audio recorded interview.

I understand that:

- I may withdraw from this study up to 1 week after the interview has taken place and any information that I have provided will be returned to me or destroyed.
- Any information gathered will be securely stored on an ECS lab machine and any information I have provided will be destroyed on the 31st of December 2021.
- Any information I provide will be kept confidential to the researcher and the supervisors.
- I understand that the findings may be used for an Honours report and a summary of the results may be used in academic reports and/or presented in conferences.
- I understand that the any information I provide will be kept confidential to the researcher and the supervisor.
- My name and my organisation name will not be used in reports, but persons within or familiar with the organisation practices may be able to identify me based on distinctiveness of the information I provide.
- I have the right to edit/append/remove details after the interview.
- I would like a copy of the recording of my interview: Yes ☐ No ☐
- I would like a copy of the transcript of my interview: Yes ☐ No ☐
- I would like to receive a copy of the final report and have added my email address below. Yes ☐ No ☐

Signature of participant: _____

Name of participant: _____

Date: _____

Contact details: _____

Appendix E

Interview Guide

Why do Programmers Do What they Do?

INTERVIEW SCHEDULE

Lavanya Sajwan
8 April 2020

Researcher: Lavanya Sajwan (sajwanlava@myvuw.ac.nz)
Supervisors: James Noble (kjx@ecs.vuw.ac.nz; +64 4 463 6736), Craig Anslow (crag.anslow@ecs.vuw.ac.nz, +64 4 463 6449)
Research Topic: Why Do Programmers Do What They Do? Investigation of security practices in workplaces.

This research project is being conducted towards partial fulfilment of the requirements for Bachelor of Engineering with Honours in Software Engineering .

General Information

This study is examining how programmers choose to implement security practices in their software programs. I will be interviewing programmers from various backgrounds and job titles ranging from devops-engineer, front-end developer, database administrators and security architects as examples. Participants jobs will all be New Zealand based. Participants can also work across a range programming fields eg. gaming, education, financial, analysis. We will discuss the decisions and influences around the choices of security protocols, how they find working with them, and how they may be improved.

Interview Schedule

This interview will be semi-structed and will include the following topics and types of questions:

1. Participant background – this can include their education, their roles within their organisation and teams, and an overview of the security practices they have previously used, and a discussion on previous experiences with security and privacy protocols.

2. A description of their current security protocols that they regularly use and adopt. Are they adding to them in any way? Do they change languages based on the security practice they use?
3. For the current particular language and security used, how has it impacted the projects they have worked on?
4. How are the security measures that have been implemented tested?
5. What are some success in using the security practice over others? Any lessons learned, or changes made in personal projects and style?
6. What have been problems in projects due to choosing the specific protocol.
7. Any other issues or comments?

Appendix F

Recruitment Post

Groups/Mailing List Post:

Kia ora koutou!

My name is Lavanya Sajwan and I am a Software Engineering student at Te Herenga Waka - Victoria University of Wellington. I am working on an honours project this year which is about security practices in industry and investigating the influences impacting the decisions of the choice that developers make. This research has been approved by the Victoria University of Wellington Human Ethics Committee (Research Master Application ID: 0000028506).

I am looking to interview professional programmers who work with security practices, and will need to be over 18 years old and New Zealand based. Participants can also work across a range programming fields eg. gaming, education, financial, analysis.

If this is you and are interested in participating in this study please send me an email stating your interest including name and job title.

If you participate in the interview, you will be given koha of a $10 voucher, and go into the draw to win a $60 supermarket voucher to thank you for your time!

If you are interested in participating or hearing more about the study please contact me over email – sajwanlava@myvuw.ac.nz

Ngā mihi

Appendix G

Recruitment Webpage

Why Do Programmers Do What They Do?

VUW Honours Project 2020

Research Master Application ID: 0000028506

Who Am I?

Kia ora koutou! My name is Lavanya Sajwan and I am an Honours student in the school of engineering and computer science at Victoria University of Wellington. This research project is work towards partial fulfilment of the requirements for Bachelor of Engineering with Honours in Software Engineering.

What is the Aim of the Project?

This project is an informative investigation on how software developers implement and adopt security practices in the work they do in order to develop an understanding of what influences and impacts decisions surrounding their technical work. Your participation will support this research by providing insight to the solutions that developers are using to implement in their security practices. Essentially this research aims to gather your experiences and compare them with those of your peers to understand the use of security practices in the New Zealand industry.

How Can You Help?

The process that I will be following is through using Grounded Theory as a framework. Therefore, I need to interview many participants in order to gain enough information to form a theory around my findings. Participants should be professional programmers in industry and are over the age of 18 whom implement and adopt security practices at work.

Interested?

Get in contact with any of the people listed below

Researcher

Lavanya Sajwan
sajwanlava@myvuw.ac.nz

Supervisors

James Noble
kjc@ecs.vuw.ac.nz

Craig Anslow
craig@ecs.vuw.ac.nz

Appendix H

Initial Interview Questions

Why do Programmers Do What they Do? – Interview Questions

Participant Background

- What is your role within your organisation/teams?
- Please describe any security education you got before working at your current job?
- What prior work experience do you have with security and privacy protocols?
- Would you like to tell me anything more about your background/experience in the industry?

Current Work

- What security protocols do you regularly use and adopt?
- Can you give brief overviews of the security protocols for someone who may have never used them before?
- How do you choose what security practices to use and disregard? What factors are taken into consideration?
- Are you adding to the protocols in any way?
- Do you give other teams/individuals feedback on their security practices?
- Do you change languages based on the security practice you use? Why?
- What decision makings and actions have arisen surrounding security in your programming from covid19/working from home.
- Does your work provide any training, or is it expected that you how to program "securely"?
- How did you learn about your chosen practices in order to adopt them?
- If you have obtained training, has that continued? How has it changed since when you first started.
- How are the security practices you have used/are using been tested?
- Do your security practices have any influences from OWASP. If not, why? If yes, how?
- How well do your teams chosen methods fit your current work?
- Please share if you and your team have adapted any of the approaches to suit your work better?
- How well do your team's security practices fit into the organisations overarching practices?

- What changes over time, if any, has your team enacted? Why?
- How important would you consider security needs to be for the quality/success of your work?
- What practices have been extremely valuable?
- What are some difficulties in joining a team with an established process? What was the induction process like?
- Do security practices change based on the requirements of the project? How are they identified?
- How are security requirements prioritised in relation to functional requirements?
- What work do you do in a project on a day-to-day basis to ensure system security? Or if not daily, how often is attention given to security?
- At what stages of the project/how often is attention given to security? What approaches/techniques are used at each stage?
    - Planning
    - Requirement Gathering
    - Design/Development
    - Testing
    - Implementation
    - Iterations

Experience-Based

- What recommendations would you generally give to teams looking to adopt your security practice of choice?
- What differences do you see between new and experienced teams?
- What common “mistakes” do you see?
- What factors contribute to a successful education on how to use security practices?
- What difficulties did the teams you have worked with share? Which ones were unique? Why?
- What changes have you observed in the security programming landscape in New Zealand?

Impacts

- For your current particular languages and security used, how has it impacted the projects you have worked on?
- Have there been successes of using some security practices over others?

- Have there been any lessons learned in your own personal projects and style?
- What have been problems in projects due to choosing specific protocols?
- How have your chosen practices affected your ability to deliver within constraints?

Any other issues or comments?