

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](mailto: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.

Task	4	5	6	7	8	9	10	11	12	13	14	15	16	17	BREAK	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	EXAMS
Project Proposal																															
Apply for Human Ethics Approval																															
Produce bibliography of grounded theory studies																															
Outline the interview questions																															
Contact sampling groups																															
Write preliminary report																															
Write presentation																															
Submit preliminary report																															
Presentation																															
Collect data by the form of interviews																															
Open code all of the collected data																															
Selective code the data																															
Write theoretical notes/memos																															
Sort the theoretical notes/memos																															
Draft final report																															
Write presentation																															
Review report																															
Submit report																															
Presentation																															

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 Experience* Volume 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.