Modern Security Compliance with Zero-Knowledge Proofs

Victor Kuo

Supervisors: Prof. Stefan Williams
Dr. Qiang Tang

Industry Supervisor: Mr. Luke Higgins

THE UNIVERSITY OF SYDNEY

School of Aerospace, Mechanical and Mechatronic Engineering
The University of Sydney

A thesis submitted to The University of Sydney in fulfilment of the requirements for the degree of *Bachelor of Engineering Honours*

Jan 2022

Declaration

I, Victor Kuo, hereby declare that this thesis submission titled *Modern Security Compliance with Zero-Knowledge Proofs* is my own work and that, to the best of my knowledge and belief, it contains no material previously published or written by another person nor material which to a substantial extent has been accepted for the award of any other degree or diploma of the University or other institute of higher learning, except where due acknowledgement has been made in the text. Specifically, the work I contributed consists of:

1. Conducting the literature review;
2. Analysing and hypothesising solutions to Zero-Knowledge compliance issues.
3. Defining the requirements of ;
4. Developing , a complete end-to-end zk-SNARK application to generate and verify computational proofs for sanitization purposes;
5. Developing a generic, high level string library for arithmetic circuits for use in zk-SNARKs;
6. Contributing the algorithm for `Compare()` to the open-source project ;
7. Conducting the analysis of runtimes and memory usage for , and asserting the feasibility and viability of using zk-SNARKs in industry for security compliance requirements; and
8. Writing this thesis report.

Assistance was received from my supervisors in the areas of:

1. Identifying zk-SNARKs as a viable solution to the problem;
2. Identifying relevant literature to this thesis; and
3. Improving this thesis through their feedback.

Victor Kuo *Author*	Date
Prof. Stefan Williams *Supervisor*	Date

Acknowledgements

Modern Security Compliance with Zero-Knowledge Proofs

Abstract

Executive Summary

Table of contents

List of figures

List of tables

Chapter 1

Introduction

Listing 1.1 Example computation

```
// Calculate the multiplication of x and y by adding x, y number of
    ↪ times.
function multiply(x, y):
  output = 0

  for i = 0..y:
    output = output + x

  return output
```

Appendix A

Work Health and Safety

Work Health and Safety is a significant concern to all workers. Although seemingly simple in nature and low in risk, office jobs have their fair share of long-term health risks that must be considered. This section will analyse a number of Work Health and Safety concerns in the modern office that applies to this ESIPS placement at Accenture. Some that will be discussed include physical health, COVID-19, and mental health.

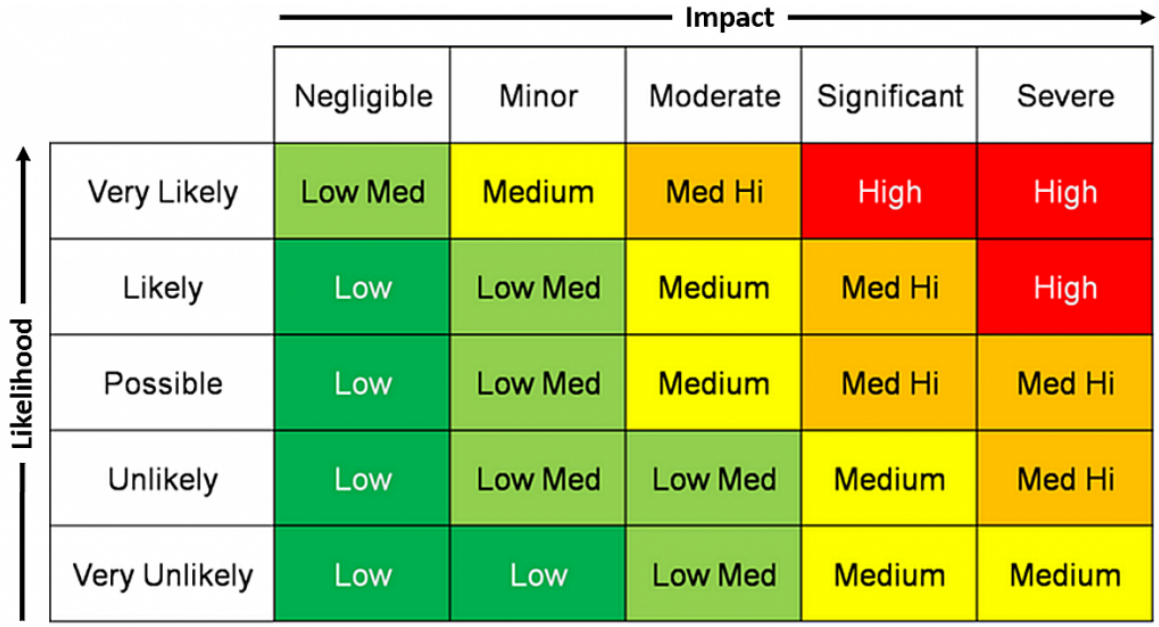

Fig. A.1 Risk matrix. From `https://www.armsreliability.com/page/resources/blog/beyond-the-risk-matrix`.

A.1 Physical Health

In a standard office, work is often long, repetitive, and stationary. Bad posture, uncomfortable chairs, mispositioned monitors, wrist strain over cramped keyboards, poor lighting or glare are just a few of the most common risks and hazards to physical health.

At Accenture and home, the following precautions were observed:

1. Education on the proper position to work in was studied from **??**. Notably, the height of the chair is set to the appropriate height to allow feet to rest in an almost 90 deg angle, the top of the monitor edge at eye level, and the monitor slightly tilted up to equalise the distance to all corners of the screen.
2. Good chairs were selected. I purchased a Herman Miller Aeron chair for work at home, known for its world-renowned ergonomics.
3. Used a second external monitor to relieve neck strain, as it is possible to adjust the monitor's position to the optimal position. This also provided a significant productivity boost. The brightness was also adequately adjusted to bring the most comfort to the eyes.
4. A standing desk was purchased for working at home.
5. Regular breaks were taken with the team during the time at the office.
6. An ergonomic keyboard, the Kinesis Advantage 2, was used to relieve wrist strain and improve productivity with the features such as macros.

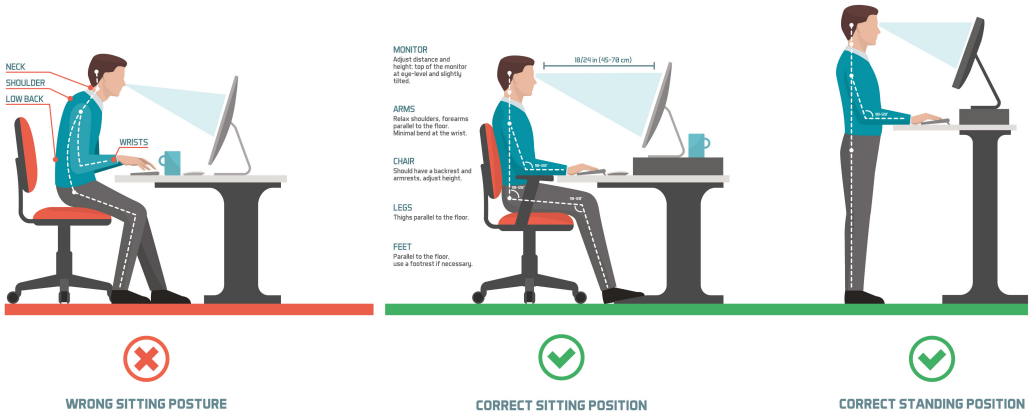

Fig. A.2 Best posture at a desk. From: `https://healthandbalance.com.au/workstation-desk-posture-ergonomics/`

Although there are many sources of long-term physical issues, these can be easily managed with awareness and mitigated effectively, resulting in a low level of risk.

A.2 Covid-19 precautions

Covid-19 has undeniably impacted the world in many ways. This highly infectious disease caused major lockdowns and shifted work from the office to the home for extended periods. In order to follow national and state requirements, Accenture and employees worked remotely and suspended office visits. Return to the office was first announced in mid-November, where a number of precautions were followed:

1. All state and national requirements were followed, including masks in public indoor areas and on transport, QR code check-ins in all locations required, and mandatory bookings for visits to the office.
2. Social distancing in all public areas.
3. Sanitising hands on every entry to the office.
4. Disallowing guest visits to the office.

Although the severity of symptoms one suffers from contracting Covid-19 vary wildly in the younger age group, the potential to be sick for a week or more, in addition to the mandatory self-isolation period, is highly disruptive to work and the greater population. As such, the threat of Covid-19 results in high risk.

A.3 Mental health

Mental health is an often under-looked part of one's health. It varies greatly from person to person, and many factors play into one's overall mental health, including social health, work-life balance, and financial status. Without careful consideration, planning and awareness of one's mental health, the employee's productivity may drop sharply.

A number of precautions were taken to care for my mental health:

1. Ensuring I was enjoying the work I was doing. I transferred internally between teams to find more exciting work that I could grow and learn in while also finding a more relevant thesis topic aligned with my interests.
2. Coming into the office when practical. Although there were many days where I was the only team member in the office, being able to experience the office, grab hot drinks in the morning with colleagues, and work in an environment separate from home was very beneficial.
3. Preventing work hours from extending into my personal time too often.

Mental health is a complex risk to quantify since it is difficult to measure and includes many factors. Overall the onus is mainly on the employee to ensure they take the proper precautions and use the available resources such as sick leave or personal time off. Particularly with the challenging program that is ESIPS, this risk is categorised as a moderate risk.