TOWARDS A THREAT ASSESSMENT FRAMEWORK FOR CONSUMER HEALTH WEARABLES

A thesis submitted in fulfilment of the

requirements for the degree of

MASTER OF COMMERCE
of
RHODES UNIVERSITY

By

JAVAN JOSHUA MNJAMA

December 2017

DECLARATION

I, Javan Joshua Mnjama, declare that the dissertation entitled, "*Towards a Threat Assessment Framework for Consumer Health Wearables*", which I hereby submit for the degree, Master of Commerce at Rhodes University, is my own work. I also declare that this dissertation has not previously been submitted by me for a degree at this or any other tertiary institution and that all the sources that I have used or quoted have been indicated and acknowledged by means of complete references.

Javan Joshua Mnjama

ABSTRACT

The collection of health data such as physical activity, consumption and physiological data through the use of consumer health wearables via fitness trackers are very beneficial for the promotion of physical wellness. However, consumer health wearables and their associated applications are known to have privacy and security concerns that can potentially make the collected personal health data vulnerable to hackers. These concerns are attributed to security theoretical frameworks not sufficiently addressing the entirety of privacy and security concerns relating to the diverse technological ecosystem of consumer health wearables. The objective of this research was therefore to develop a threat assessment framework that can be used to guide the detection of vulnerabilities which affect consumer health wearables and their associated applications.

To meet this objective, the Design Science Research methodology was used to develop the desired artefact (Consumer Health Wearable Threat Assessment Framework). The framework is comprised of fourteen vulnerabilities classified according to Authentication, Authorization, Availability, Confidentiality, Non-Repudiation and Integrity. Through developing the artefact, the threat assessment framework was demonstrated on two fitness trackers and their associated applications. It was discovered, that the framework was able to identify how these vulnerabilities affected, these two test cases based on the classification categories of the framework. The framework was also evaluated by four security experts who assessed the quality, utility and efficacy of the framework. Experts, supported the use of the framework as a relevant and comprehensive framework to guide the detection of vulnerabilities towards consumer health wearables and their associated applications.

The implication of this research study is that the framework can be used by developers to better identify the vulnerabilities of consumer health wearables and their associated applications. This will assist in creating a more securer environment for the storage and use of health data by consumer health wearables.

ACKNOWLEDGEMENTS

The completion of this dissertation has been a long journey, and if wasn't for the guidance, support, and patience of those around me, I wouldn't have gotten this far.

First of all, I would like to thank my Lord and saviour Jesus Christ for seeing me through all of this and giving me the opportunity and skill set to pursue this degree. I wish to thank my supervisors, Professor Greg Foster and Professor Barry Irwin who believed in me and pushed me to strive for the best. I have learnt a lot from them, and I am entirely grateful. Special thanks go to the staff of the Information Systems department at Rhodes University who helped to shape my research. Especially Professor Kirsten Krauss, who motivated me to strive and endeavour into research. If it wasn't for him, this journey would not have begun.

To my family, thank you. Especially my parents, Professor Nathan Mnjama and Mrs. Joy Mnjama for empowering me to pursue education. In addition, for constantly reminding me to keep pressing on even when things got difficult. To my siblings, David Mnjama, Evans Mnjama and Gladys Mnjama thank you for seeing the greatness within me. To my extended family, thank you.

To all my friends who have supported me through all this, thank you. Special thanks to all my peers in the Information Systems department, Harry Moongela, Tumaini Kabudi, Oridota Oyebode, Clement Simuja, Odifetse Lehasa, Tinahse Jani, Mwazvita Machiri, Auther Munjeri, Callie Thomson, Valeria Motsimu and Vinia Mabika thank you all.

Thank you to the support I also received from River of Life Church, Grahamstown. Especially, Pastor Innocent and Mrs. Matepo for your constant prayers and encouragement.

Thank you all.

TABLE OF CONTENTS

Declaration .... **ii**

Abstract .... **iii**

Acknowledgements .... **iv**

Table of Contents .... **v**

List of Figures .... **x**

List of Tables .... **xii**

Chapter 1: Research Context **1**

1.1 Introduction 1

1.2 Background 1

1.3 Problem Description 5

1.3.1 Problem Statement 7

1.4 Goal of Research 7

1.5 Research Methodology 8

1.6 Scope and Constraints 10

1.7 Ethical Considerations 10

1.8 Outline of Chapters 11

Chapter 2: Research Methodology **13**

2.1 Introduction 13

2.2 Research Design 13

2.3 Overview of Design Science Research 14

2.4 Design Science Research Framework 16

2.5 Design Science Process 20

2.5.1 Design Science Process for Research Study 21

2.6 Conclusion 23

Chapter 3: Consumer Health Data 24

3.1 Introduction 25

3.2 Physical Wellness 25

3.2.1 Consumer Health 26

3.3 Consumer Health Wearables 28

3.4 Consumer Health Data 30

3.4.1 Data types of Consumer Health Data 32

3.4.2 Aim and Significance of Consumer Health Data 33

3.4.3 Health Application Regulation 34

3.5 Conclusion 37

Chapter 4: Vulnerabilities In Consumer Health Wearables 38

4.1 Introduction 39

4.2 Consumer Health Wearable Ecosystem 39

4.2.1 Consumer Health Wearable Structure 41

4.2.2 Smartphone Application Architecture 42

4.2.3 Cloud Server Structure 46

4.3 Consumer Health Data Vulnerabilities 46

4.3.1 Vulnerabilities towards Consumer Health Wearables 46

4.3.2 Vulnerabilities towards Health Applications and Cloud Storage 48

4.4 Conclusion 51

Chapter 5: Theoretical Threat Assessment Frameworks 53

5.1 Introduction 54

5.2 Threat Assessment Frameworks 55

5.3 Attack Threat Models 56

5.3.1 The Three Orthogonal Dimensional Model 56

5.3.2 Information System Security Threat Cube Classification 58

5.4 Threat Impact Models 60

5.4.1 Microsoft STRIDE Threat Assessment Framework 60

5.4.2 CIA Triad 61

5.5 Key components for a Conceptual Framework 63

5.6 Conclusion 68

Chapter 6: Consumer Health Wearable Threat Assessment Framework 69

6.1 Introduction 70

6.2 Formation of Framework 71

6.2.1 Consumer Factors 71

6.2.2 Vulnerabilities towards Consumer Health Wearables 74

6.3 Consumer Health Wearable Threat Assessment Framework 77

6.3.1 Description of Framework 79

6.3.2 Vulnerability Criteria for Framework 80

6.4 Conclusion 83

Chapter 7: Framework Demonstration 84

7.1 Introduction 85

7.2 Demonstration Set-up 85

7.2.1 Description of Test Cases 85

7.2.2 Description of Mobile Device and Application Testing Software 86

7.2.3 Demonstration Procedure 87

7.3 Vulnerability Exposure of Test Case A 92

7.3.1 Third Party Analytics 92

7.3.2 Lack of Access Codes 92

7.3.3 Location Tracking 93

7.3.4 Insufficient transport-layer protection ... 94

7.3.5 Privacy Policy ... 94

7.3.6 Poor Authorization & Authentication ... 95

7.3.7 Threat Impact Review of Test Case A ... 96

7.4 Vulnerability Exposure of Test Case B ... 97

7.4.1 Third Party Analytics ... 97

7.4.2 Insufficient Transport Layer Protection ... 98

7.4.3 Poor Authorization and Authentication ... 98

7.4.4 Threat Impact Review of Test Case B ... 98

7.5 Utility and Efficacy of Framework ... 100

7.6 Conclusion ... 102

Chapter 8: Evaluation of Framework ... 103

8.1 Introduction ... 104

8.2 Method of Evaluation ... 105

8.2.1 Evaluation Process ... 106

8.2.2 Quality Assessment Strategy ... 108

8.2.3 Participants ... 112

8.2.4 Procedure of evaluation ... 113

8.3 Results ... 113

8.3.1 Vulnerability Assessment Results ... 113

8.3.2 Classification Assessment Results ... 118

8.3.3 Category Grouping Assessment Results ... 119

8.3.4 Overall Framework Assessment Results ... 124

8.4 Refinement of framework ... 125

8.5 Conclusion ... 127

Chapter 9: Conclusion 128

9.1 Introduction 129

9.2 Achievement of Research Objectives 129

9.3 Theoretical Contribution 131

9.4 Practical Contribution 134

9.5 Limitations 136

9.6 Future Research 136

9.7 Concluding Remarks 136

List of References 137

Appendices

Appendix A – Participant Letter 147

Appendix B – Expert Evaluation Form 149

Appendix C – Criteria for evaluation 157

LIST OF FIGURES

Figure 1.1: Consumer Health Wearable Ecosystem (Barcena, Wueest and Lau, 2014) 3

Figure 1.2: Security Practices (Sanzgiri, 2013) 6

Figure 1.3: Design Science Research Process (DSRP) Model (Peffers, et al., 2007) 9

Figure 2.1: Design Science Research Cycles (Hevner, 2007) 16

Figure 2.2: DSR Knowledge Contribution Framework (Gregor and Hevner, 2013) 17

Figure 2.3: Design Science Research Process (DSRP) Model (Peffers, et al., 2007) 20

Figure 2.4: Design Science Process Model for Research Study 21

Figure 3.1: Types of Consumer Health Wearables (Piwek et al., 2016) 28

Figure 4.1: Consumer Health Wearable Ecosystem (Funk, 2015) 40

Figure 4.2: Fitbit Flex (Fitbit, 2016) 41

Figure 4.3: Android Application Stack (Rai, 2013) 43

Figure 4.4: Application Structure 44

Figure 5.1: The Three Orthogonal Dimensional Model (Ruf et al., 2008) 57

Figure 5.2: Information System Security Threat Cube Classification (Geric and Zejko, 2007) .. 59

Figure 6.1: Consumer Factors 74

Figure 6.2:Consumer Health Wearable Threat Assessment Framework 78

Figure 6.3:Components of Framework 79

Figure 6.4: Summary of Framework Formation 83

Figure 7.1: Demonstration Procedure 87

Figure 7.2: Bluetooth Log File Setup 88

Figure 7.3: Testing WiFi IP Address 89

Figure 7.4: Proxy Setting of Mobile Device 90

Figure 7.5: Test Case A, Location Tracking 93

Figure 7.6: Test Case A, Insufficient Transport Layer Protection 94

Figure 7.7: Test Case A, Privacy Policy 94

Figure 7.8: Test Case A, Poor Authorization and Authentication 95

Figure 7.9: Summary of Results for Test Case A 96

Figure 7.10: Test Case B, Insufficient Transport Layer Protection 98

Figure 7.11: Summary of Result for Test Case B 99

Figure 8.1: Evaluation Framework (Venable et al., 2012) 105

Figure 8.2: Components of Threat Assessment Framework 109
Figure 8.3: Average results of relevance of vulnerabilities 114
Figure 8.4: Average results of appropriate terminology used for vulnerabilities 117
Figure 8.5: Average results of appropriate categorisation towards authorization 120
Figure 8.6: Average results of appropriate categorisation towards availability 121
Figure 8.7: Average results of appropriate categorisation towards non-repudiation 122
Figure 8.8: Average results of appropriate categorisation towards integrity 123
Figure 8.9: Refined Threat Assessment Framework 126
Figure 9.1: DSR Knowledge Contribution Framework (Gregor and Hevner, 2013) 131
Figure 9.2: Complete Consumer Health Wearable Threat Assessment Framework 133

LIST OF TABLES

Table 2.1: Philosophical Paradigms (Vaishnavi and Kuechler, 2004) 14

Table 2.2: Design Science Research Guidelines Adapted from Hevner (2007)........................... 19

Table 3.1:Mobile Device Functions for Health Intervention.. 30

Table 3.2: Data Type Examples of Consumer Health Data... 33

Table 4.1: Summary of Vulnerabilities... 52

Table 5.1: Assessment of Theoretical Threat Assessment Frameworks...................................... 66

Table 6.1: Example criteria of vulnerabilities.. 81

Table 7.1: Vulnerability List for Assessment 91

Table 7.2: Summary of Affect Areas for Test Case A.. 97

Table 7.3: Summary of Affect Areas for Test Case B 100

Table 7.4: Comparison of Test Cases 101

Table 8.1:Design Evaluation Framework (Helfert et al., 2012) 108

Table 8.2: Application of Design Evaluation Framework 110

Table 8.3: Biography of Security Experts... 112

Table 9.1: Example Criteria of Vulnerabilities... 134

Chapter 1: RESEARCH CONTEXT

1.1 INTRODUCTION

The purpose of this chapter is to introduce the research area and outline how the research study will be conducted. This chapter begins with Section 1.2 by firstly introducing the background and context of consumer health wearables and the privacy and security concerns relating to this environment. Section 1.3 will further expand on this by describing the problem of the consumer health wearable ecosystem. Through identifying the problem, Section 1.4 will highlight the goal of conducting this research study. Section 1.5 will outline the research methodology used, the scope and constraints of the research study (Section 1.6) as well as the ethical considerations made for this research (Section 1.7). A final Section 1.8, presents on the structure of the research dissertation through an outline of the chapters.

1.2 BACKGROUND

Physical wellness is important for the optimal wellbeing of an individual as it focuses on ensuring consistent physical activity, and appropriate nutrition and mental wellness (Adams, Bezner, Drabbs, Zambarano and Steinhardt, 2000). These are viewed as key components to ensure a person is healthy both physically and mentally (WHO, 1948). Given this, individuals have sort different ways in which they may attain knowledge to improve their physical wellbeing and wellness. Medical practitioners and health experts have guided individuals extensively in the best manner to look after their physical and mental wellness (Lewis, Chang and Friedman, 2010). Some of the advice given by health experts include performing certain types of exercises like running or cycling to improve cardio vascularity or eating certain food types rich in Omega 3 to improve mental wellness (Tähepold, van den Brink-Muinen and Maaroos, 2006).

The rise of internet usage has opened new ways for individuals to discover health related information about physical wellness. Search engines such as Google allow individuals to inquire about such information with ease (Tomlinson, Rotheram-Borus, Swartz and Tsai, 2013). This desire of individuals to participate and inquire about their physical wellbeing through technological resources can be described as Consumer Health (Piwek, Ellis, Andrews and Joinson, 2016).

Consumer health specifically focuses on how individuals of the general public, who do not have a medical background, improve their wellbeing through knowledge resources outside the confines of a medical setting (Lewis et al., 2010) and are referred to as Consumers (Flaherty, Hoffman-Goetz and Arocha, 2015). Currently, the major driving force of consumer health is consumer health wearables and their associated software that is installed on mobile devices (smartphones and tablets). Consumer health wearables are small devices that are typically worn or woven into clothing (Morera, de la Torre Díez, Garcia-Zapirain, López-Coronado and Arambarri, 2016). These devices allow consumers to learn more about themselves and their environment by tracking physical wellness health data like walking or sleeping (Marceglia, Fontelo and Ackerman, 2015). The market for these devices is growing tremendously, especially that of fitness trackers where it is estimated that in 2016 over 61 million units of fitness trackers and their associated applications were sold bringing in a revenue of $3.8 billion. This figure is expected to grow to over $6 billion by 2020 (Lamkin, 2016). As the market for consumer health wearables continues to grow it broadens the horizon of the health data that is collected through these devices.

As consumer health wearables are small devices they have a limited screen ratio for a consumer to extensively view the health data collected. As a result, consumer health wearables have their associated software which is typically installed on mobile devices (smartphones and tablets), and analyses the data from a consumer health wearable device when installed on a mobile device to provide health related information to individuals (Liu, Zhu, Holroyd and Seng, 2011). This health related information includes progress reports and recommendations on how a consumer may improve their physical wellbeing from the health data collected (Franklin and Pratt, 2016).

The type of health data that can be discovered from consumer health wearables may vary a great deal. However, typically there are three main categories; consumption data, physical activity data and physiological data (Dehling, Gao, Schneider and Sunyaev, 2015). In most cases consumption data includes the number of calories or water consumed in the day (Nazi, Hogan, Woods, Simon and Ralston, 2016). Physical activity data includes any data related to any physical activity an individual had participated in, this may be the number of steps taken (Jakicic et al., 2016). Finally, physiological data may include the heart rate of a user (Valdez, Holden, Novak and Veinot, 2014). Through the use of consumer wearables and their associated applications, a person may attain knowledge on a specific health or fitness aspect and furthermore identify how one's daily activities affect their physical wellbeing (Handel, 2011; Conroy, Yang and Maher, 2014). The typical flow of health data with the use of consumer health wearables and their associated applications is depicted in the consumer health wearable ecosystem model (Figure 1.1).

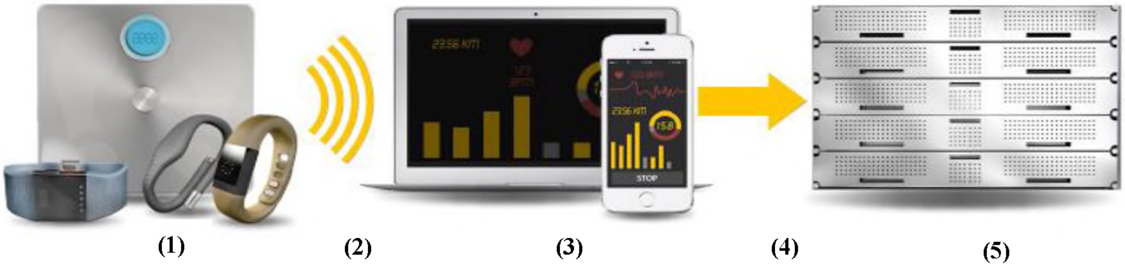


Figure 1.1: Consumer Health Wearable Ecosystem (Barcena, Wueest and Lau, 2014)

As health data is collected from a consumer health wearable device ***(1)***, it is sent to its associate application installed on a mobile device via Bluetooth or Near Field Communication (NFC) ***(2)***. This data is stored in the health application and transformed to information such as progress history or areas of improvement for a user to view on the mobile device ***(3)***. This information can either be stored locally in the health application and/or a copy is sent via Wi-Fi or cellular communications ***(4)*** to cloud servers ***(5)***. The information collected by consumer health wearables and their associated applications play an important role in an individual's healthcare management for physical wellness. However, despite the benefits consumer health wearables and their associated applications offer, they have security and privacy concerns. These concerns pose a risk to the personal health data of consumers collected via these mechanisms (Ralf, 2014; Safavi and Shukur, 2014; Valdez et al., 2014; Marceglia et al., 2015).

There is a good reason for this concern, as the protection and privacy of health data are of critical importance as it contains sensitive information that should not be disclosed to unwanted parties. Privacy is the right individuals have to control the use, disclose or acquisition of their data (Tavani and Moor, 2001). Security, on the other hand, is the physical, technological or administrative structures that are put in place to protect identifiable data (Cohn, 2006b). Due to the diverse components described from the consumer health wearable ecosystem, ensuring privacy and security for each of the technologies is of utmost importance as health data is in high demand from cyber criminals. Health data is sold for ten times more than any other type of data on the black market (Bryan, 2015). In addition, health data is worth more than credit card information. Once a criminal obtains health data, this information can be used to create new false IDs and passports (Humer and Finkle, 2014; Grimes, 2015). Furthermore, in the wrong hands, health related data can be utilised for false medical claims to purchase drugs or health equipment to resell on the black market (Humer et al., 2014).

Government institutions and health institutions have therefore created policies and structures to ensure the protection of health data due to this high demand from cyber criminals. However, research describes that many of these policies do not address consumer health wearables and their associated applications issues sufficiently and are mostly focused on applications used within a clinical setting (Appari and Johnson, 2010; Avancha, Baxi and Kotz, 2012; Caldwell, 2014). This excludes many consumer wearable devices and their associated applications as these tools are used outside the confines of medical institutions (Charani, Castro-Sánchez, Moore and Holmes, 2014; Franklin et al., 2016). Furthermore, the primary focus of these policies is on consumer rights and confidentiality of data; limited consideration is made on the security issues of consumer health wearables and their associated applications (Lupton, 2016; Morera et al., 2016).

Due to limited regulations and policies applicable to consumer health wearables, it has been identified that the use of these devices have security drawbacks that make an individual’s health data susceptible to intrusion by hackers (Free et al., 2010; Avancha et al., 2012). These security concerns can occur as data is transmitted and stored from the consumer health wearable device to the mobile device and also to cloud servers (Barcena, Wueest and Lau, 2014; Seals, 2016). It has been reported that 50% of consumer health wearable devices do not have a pin or pattern code to protect them (HP Fortify, 2015). As such, if the device is stolen, it can be accessed easily by unwanted users. Firmware is used to update the software of devices and these updates are often sent to wearable devices without encryption (Cyr, Horn, Miao and Specter, 2014; HP Fortify, 2015). Thus, any manipulation of the update can result in changing the functionality of the wearable device (Selinger, 2015). Furthermore, most health applications on mobile devices are cloud based and lack encryption structures of the data collected (Löhr, Sadeghi and Winandy, 2010; Barcena et al., 2014). In addition, poor session management has been identified, thus making a user vulnerable to hacking (Barcena et al., 2014). It is also apparent that developers of health applications have little consideration of the security factors and tend to focus on the features and functionality of the health application to increase sales or downloads (Symantec, 2014; Martínez-Pérez, de la Torre-Díez and López-Coronado, 2015).

1.3 Problem Description

Consumer health wearables and their associated applications are growing tremendously and are capable of collecting health related data continuously for an individual to assist improve their physical wellbeing. Medical practitioners and health experts have also identified the benefits of consumer health wearables towards individuals in the general public for physical wellness. However, health experts are unsure of the safest consumer health wearable to recommend to consumers due to privacy and security concerns (Adhikari, Richards and Scott, 2014; Ponemon Institute LLC, 2015).

It is considered that in to address the privacy and security concerns of consumer health wearables and their associated applications, the use of policies and regulations will aid to eradicate this problem (Wicks and Chiauzzi, 2015). However, many health regulations currently provide a barrier for mobile health applications in a clinical setting as they exclude many consumer health wearable devices (Zhou and Piramuthu, 2014; Huckvale, Prieto, Tilney, Benghozi and Car, 2015). A plausible solution is to extend the existing regulations of mobile applications in a clinical setting to that of consumer health wearables. However, to the large diversity of consumer health wearables and their associated applications, it is challenging to provide a '*one size, fits all*' approach (Dehling et al., 2015). Also, medical practitioners are reluctant with increasing the use of policies and regulations for consumer health wearables. They view this will hinder the innovation process and throughput of consumer health wearables if they are placed under strict policies and regulations (Digiulio, 2014).

It has further been suggested that existing security theoretical assessment models and frameworks can be used to assist application developers of consumer health wearables to understand the security vulnerabilities of consumer health wearables and their associated applications (Kumar and Lee, 2011). This method will subsequently assist developers to create more secure consumer health wearables for consumers. However, existing security theoretical threat assessment models are limited in addressing the entirety of concerns relating to consumer health wearables (Zhou et al., 2014; Gruessner, 2015; Williams and Maeder, 2015). This is due to the diverse technological ecosystem of consumer health wearables, where there are different architectures, applications and implementations; the wearable device, the associated application installed on a mobile device and furthermore cloud storage (Sanzgiri, 2013).

To create a secure environment in relation to privacy and security with the use of consumer health wearables and their associated applications, there are different security practices that can be used to incrementally mitigate the vulnerabilities. These security practices include, threat assessment, prevention, detection, mitigation and finally forensics, where threat assessment is the first and cheapest approach and forensics as the final most expensive mitigation approach (Figure 1.2) (Hunker and Probst, 2008; Sanzgiri, 2013).

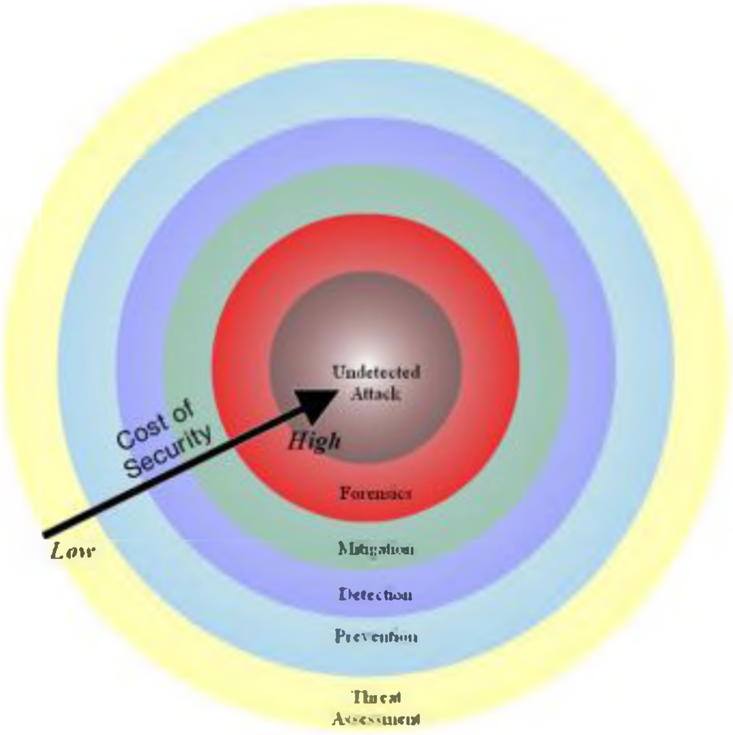


Figure 1.2: Security Practices (Sanzgiri, 2013)

In the process of developing a secure environment of consumer health wearables and their associated applications there is a need of a threat assessment framework specifically for consumer health wearables as this the first process of good security practice of threat mitigation (Kumar et al., 2011; Zhou et al., 2014; Sanzgiri, 2013). This threat assessment framework will help guide the detection of security vulnerabilities that are faced by consumer health wearables and their associated applications. In addition, such an assessment tool will assist stakeholders (Application Stores, Application Developers and Reviewers) to understand where security measures need to be implemented or improved (Li, Lou and Ren, 2010; Wicks et al., 2015).

1.3.1 Problem Statement

Due to limited regulations and policies applicable to consumer health wearables, it has been identified that the use of these devices have security drawbacks that make an individual's health data susceptible to intrusion by hackers.

1.4 GOAL OF RESEARCH

The objective of this research project is to develop a threat assessment framework that can be used to assess consumer health wearables and their associated applications as this is the first approach for good security practice for threat eradication. Through developing a threat assessment for consumer health wearables, a basis of coverage can be provided to understand which vulnerabilities affect consumer health wearables. In order to fulfil this objective, the following main research question is:

What are the components of a threat assessment framework for determining privacy and security vulnerabilities in consumer health wearables?

In order to address the main research question four sub-questions are required:

RQ1: What health data do consumer health wearables collect and store?

This question helps to gain an understanding of the type of health data that needs to be protected and how it is collected and stored by consumer health wearables.

RQ2: What vulnerabilities are associated with the consumer health wearables ecosystem?

From understanding the health data that is collected from consumer health wearables in RQ1. The vulnerabilities that contribute to the privacy and security of the health data collected from consumer health wearables can be identified. The vulnerabilities associated include from data transfer and data storage.

RQ.3: What threat assessment components should be incorporated into a threat assessment framework for consumer health wearables?

To formulate the desired threat assessment framework, an overview of current theoretical frameworks need to be reviewed. This will assist to identify the knowledge gaps and the elements required to be incorporated for the threat assessment for consumer health wearables.

RQ.4: How viable is the proposed threat assessment framework for determining the vulnerabilities for the consumer health wearable ecosystem?

This question helps to assess the developed framework by evaluating the utility, efficacy, and quality of the framework for its intended purpose.

1.5 RESEARCH METHODOLOGY

To effectively attain the objective of this research project, the Design Science Research methodology was utilised. Design Science Research aims to produce design artefacts that can be utilised to provide research contributions and provide solutions to real world problems and is well established within Information Systems (Hevner, March, Park and Ram, 2004; Gregor and Hevner, 2013). The design artefact produced may be a model, construct, method, instantiations or better design theories (Hevner et al., 2004; Hevner and Chatterjee, 2010). For this research project, the referred artefact will be a framework (construct) (Gregor et al., 2013). Furthermore, the research seeks to solve a problem and provide knowledge contributions by providing a basis for coverage of the vulnerabilities affecting consumer health wearables and their associated applications. For this research, Design Science Research Process Model of Peffers, Tuunanen, Rothenberger and Chatterjee (2007) will be utilised (Figure 1.3).

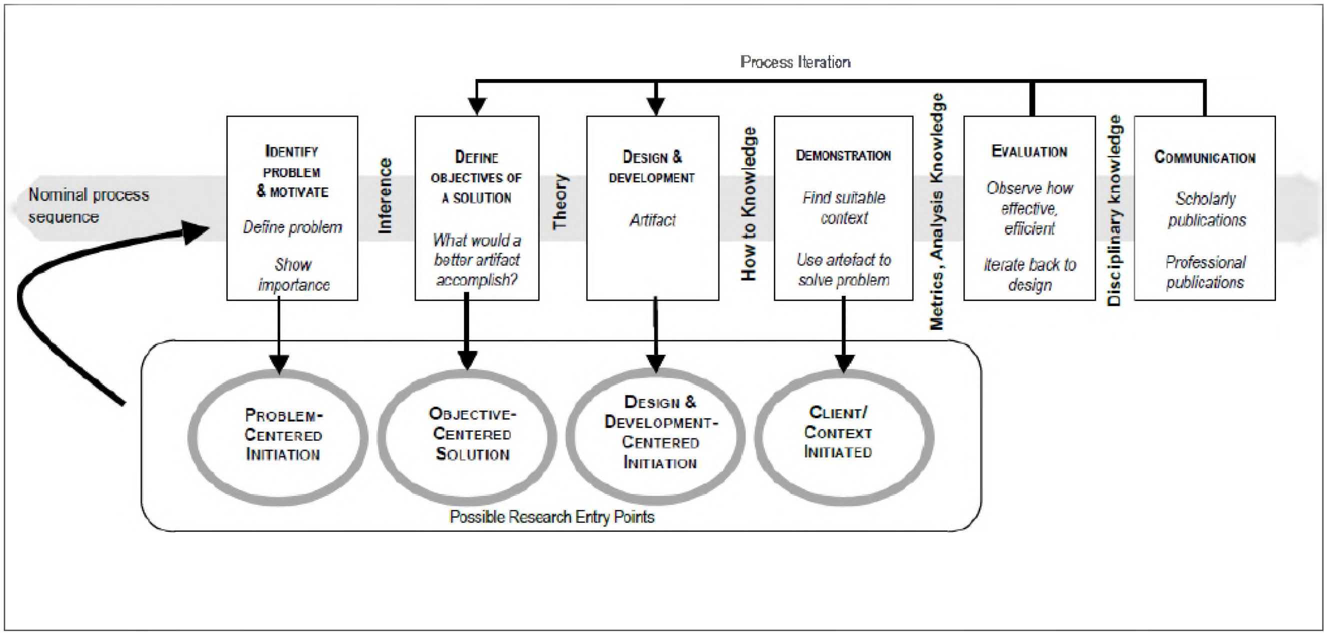

Process Iteration
Nominal process sequence
IDENTIFY PROBLEM & MOTIVATE
Define problem
Show importance
Inference
DEFINE OBJECTIVES OF A SOLUTION
What would a better artifact accomplish?
Theory
DESIGN & DEVELOPMENT
Artifact
How to Knowledge
DEMONSTRATION
Find suitable context
Use artefact to solve problem
Metrics, Analysis Knowledge
EVALUATION
Observe how effective, efficient
Iterate back to design
Disciplinary knowledge
COMMUNICATION
Scholarly publications
Professional publications
PROBLEM-CENTERED INITIATION
OBJECTIVE-CENTERED SOLUTION
DESIGN & DEVELOPMENT-CENTERED INITIATION
CLIENT/ CONTEXT INITIATED
Possible Research Entry Points

Figure 1.3: Design Science Research Process (DSRP) Model (Peffers, et al., 2007)

The model outlines six critical activities that are needed to be conducted; Identify the problem, Define the objectives of the solution, Design and Development, Demonstration, Evaluation and Communication of the solution. These six activities prescribed by Peffers et al. (2007) span over multiple chapters in order to answer the research question and sub questions. Activity 1: - **Identify problem and motivate** is conducted in Chapter 3 and 4 where the data collected by consumer health wearables are understood and the reason to better protect them. In addition, the vulnerabilities affecting consumer health wearables are also discussed. Activity 2: - **Define the objectives of the solution** is achieved in Chapter 5 where a literature review of the existing theoretical threat assessment frameworks is identified and their applicability towards consumer health wearables. Their shortcomings are also identified to which criteria will be outlined for developing a threat assessment framework specifically for consumer health wearables. Activity 3: - **Design and development** will be conducted in Chapter 6 where the gaps and criteria discovered from Activity 2 will be applied to develop the threat assessment for consumer health wearables and their associated applications. Activity 4: - **Demonstration** is achieved in Chapter 7 where the threat assessment framework is illustrated on two test cases to identify the utility and efficacy of the threat assessment framework. Activity 5: - **Evaluation** is conducted in Chapter 8 where the developed threat assessment framework is evaluated by experts to assess if it measures to industry standards and/specifications. Finally, Activity 6: - **Communication**, will be achieved through the written dissertation and the following article:

1. Mnjama, J., Foster, G. and Irwin, B., 2017. A Privacy and Security Threat Assessment Framework for Consumer Health Wearables. In: *Proceedings of the 2017 ISSA Conference. pp.66-73.*

In addition, Chapter 9 also provides a summary of the overall outcome achieved as presents the theoretical and practical outcome of the research.

1.6 Scope and Constraints

This research study focused on developing a threat assessment framework that can be used to provide a basis of coverage of the vulnerabilities affecting consumer health wearables. The scope is limited to fitness trackers only. Other forms of consumer health wearables are not considered.

1.7 Ethical Considerations

Human participants in the domain of security were used to evaluate the effectiveness of the developed Consumer Health Wearable Threat Assessment framework based on utility, quality and efficacy. Before the assessment was conducted, ethical approval was needed to be obtained from Rhodes University Ethical Standards Committee. The ethics number for this research is CIS17-11.

Informed Consent: All participants were provided with information to allow them and determine whether they desired to be part of the research study. Each participant was provided with an invitation letter (Appendix A) before the evaluation was conducted to inform them of the purpose of the research study, the reason of their involvement to partake in the evaluation process and the expected use of their responses. All participation was voluntary and each participant was required to sign a consent form.

Confidentiality and Anonymity: The privacy and confidentiality of each participant was maintained through the evaluation process to protect the anonymity of the participants. All participants were ensured that their confidentiality and anonymity relating to their personal details were maintained during the course and after the evaluation process. To ensure this a coding process was used to ensure the participants information was kept anonymous. This was done by identifying each security expert as XP.

1.8 Outline of Chapters

The dissertation chapters in sequential order are organised as follows:

Chapter 1: Research Context

This chapter introduces a background study to the research context. In addition to this it offers a problem description to this research context and the goal of conducting this research project. An outline of the research methodology is also described by outlining the scope and constraints and the ethical considerations made for conducting the research study.

Chapter 2: Research Methodology

This chapter focuses to discuss the research methodology used to guide the development of the Consumer Health Wearable Threat Assessment framework. The applied Design Science Research methodology is discussed within this chapter.

Chapter 3: Consumer Health Data

This chapter outlines and discusses the health data collected and stored from consumer health wearables. An outline will be provided on the categories of data collected and relationships made from this chapter. This chapter concludes by exploring the reasons and need to provide mechanisms to protect the health data collected from consumer health wearables.

Chapter 4: Vulnerabilities In Consumer Health Wearables

The aim of this chapter is to understand the vulnerabilities affecting consumer health wearables. This achieved by understanding the ecosystem of consumer health wearables. From understanding this ecosystem, the vulnerabilities affecting each component outlined from the ecosystem are described.

Chapter 5: Theoretical Threat Assessment Frameworks

This chapter sought to discover and understand existing theoretical threat assessment frameworks. From identifying these frameworks, their applicability towards consumer health wearables was discussed. This assisted to identify the gaps of the frameworks. The highlight of this chapter is an outline of the components needed for a threat assessment framework for consumer health wearables.

Chapter 6: Consumer Health Wearable Threat Assessment Framework

This chapter is aimed to describe the design and development of the Consumer Health Wearable Threat Assessment Framework. This is achieved by discussing the different components needed for the framework and how they were incorporated within the framework.

Chapter 7: Framework Demonstration

Chapter 7 focuses on illustrating the use of the framework. This was achieved by using the framework in two test cases, specifically two different types of fitness trackers and their associated applications. The chapter helped to understand the utility and efficacy of the Consumer Health Wearable Threat Assessment Framework.

Chapter 8: Evaluation of Framework

This chapter is aimed at evaluating the developed framework. This chapter outlines the procedure of the evaluation, the participants used and the results obtained through conducting the evaluation of the framework. This helped to substantiate the quality, utility and efficacy of the framework.

Chapter 9: Conclusion

This chapter is focused to provide a summation of the outcomes of conducting the research study. This is attained by detailing the achievements of the research objectives, the theoretical and practical contributions made. In addition, future research to be conducted to be improve the research study.

Chapter 2: RESEARCH METHODOLOGY

2.1 INTRODUCTION

The purpose of this chapter is to outline the research methodology used to structure this research dissertation and address the research problem. The chosen research methodology is Design Science Research and the chapter is structured as follows. Section 2.2 provides an overview of different research designs that can be used to guide the research within Information Systems. Section 2.3 explains the overview of Design Science Research and the reasons for its use within Information Systems. Section 2.4 explained the Design Science Research Framework and the manner in which it is utilised in Information Systems. Section 2.5 described the Design Science Research process and the manner in which it was approached for the research dissertation.

2.2 RESEARCH DESIGN

The core purpose of academic research is to produce new knowledge or contribute to the existing knowledge base (Hofstee, 2006). The chosen research design by a researcher is of critical importance for it guides the process in which the research project will be conducted and the production of knowledge. It is therefore vital for the researcher to carefully analyse the appropriate research strategy that will complement the goal for the research project in production and/or contribution of knowledge. Within the field of Information Systems, different research philosophies have been utilized to guide research. These philosophical paradigms aid the researcher to gain an understanding of the world. Prominent research paradigms within the field of Information Systems include; Positivism, Interpretivism, and Design Science Research. Each of these research philosophical paradigms have their advantages depending on the realities a researcher seeks to discover. Vaishnavi and Kuechler (2004) outline the key differences of these philosophical paradigms and the research perspective they offer. This comparison of the different paradigms is outlined in Table 2.1 by identifying the basic belief of each research perspective.

Table 2.1: Philosophical Paradigms (Vaishnavi and Kuechler, 2004)

	Research Perspective		
Basic Belief	**Positivist**	**Interpretive**	**Design Science Research**
Ontology: The nature of reality, seeks to identify that which is real	A single reality. Knowable, probabilistic	Multiple realities, socially constructed	Multiple, contextually situated alternative world-states. Socio-technologically enabled
Epistemology: the study of the nature of knowledge	Objective; dispassionate. Detached observer of truth	Subjective, i.e values and knowledge emerge from the researcher-participant interaction	*Knowing through making:* objectively constrained construction within a context. Iterative circumscription reveals meaning
Methodology: the process to which the research study is conducted	Observation; quantitative, statistical	Participation; qualitative. Hermeneutical, dialectical.	Developmental. Measure artefactual impacts on the composite system.
Axiology: the study of values, the values an individual or group adhere to	Truth: universal and beautiful; prediction	Understanding: situated and description	Control; creation; progress (i.e. improvement); understanding

For this research study Design Science Research approach was utilised. This approach is viewed to have its underpinnings within the pragmatic philosophical paradigm. This is so as it is centred on the development and performance of designed artefact with the intention of improving the socio-technical contextualised environment. This is beneficial for the dissertation as the objective was to develop a threat assessment framework that can be used to assess consumer health wearables and their associated applications. This threat assessment is to be used to provide a coverage to understand the vulnerabilities affecting consumer health wearables.

2.3 Overview of Design Science Research

For this research dissertation, the Design Science Research approach was utilized to meet the objective of the project. Design Science Research can be described as the way of utilising design as a technique for a research method. Where the aim of this research method is the creation of new knowledge through *design* and the evaluation of use and performance of the *designed artefact*

(Vaishnavi and Kuechler, 2004). Design Science Research draws its roots from the book 'The Sciences of the Artificial' by Simon (1996). The work of Simon (1996) describes the importance and role of design where he defines the science of the artificial (Design Science) as the study and design of artificial (man-made) objects. Within this study it is implored to researchers to incorporate design in the production of research. The art of design has been identified in several fields such as engineering and computer science, where not much so in more social disciplines. For a period of time the field of Information Systems has been considered as a technical discipline (Vaishnavi et al., 2004). However, Information Systems deals with various complexities such people, technology and organization structures. Much of which is described as 'wicked problems' (Hevner et al., 2004). The concept of incorporating design has been examined within Information Systems as a research method in addition for conducting research (Hevner et al., 2004; Peffers et al., 2007; Hevner et al., 2010). The concept of incorporating design helps to tackle these 'wicked problems' within the field of Information Systems (Hevner et al., 2004). The Information Systems viewpoint of Design Science is deemed as an approach that focuses on creating design activities that are framed for scientific activities (March and Smith, 1995). These design activities focus on the creation of an artefact to reach a solution. Where the referred to artefact is a construct, model, methods and instantiations. From the perspective of Information Systems, Design Science Research does not only focus on the process of instantiating a system, but it also includes the process of evaluating the product to review the performance of the core intention (Vaishnavi and Kuechler, 2015). This perspective is in conjunction with the work of Hevner et al. (2004). It is described here the importance of relevance within the problem area environment and the relevant knowledge base required to solve the desired environment (Hevner et al., 2004). Design Science Research artefacts are viewed as vital academic outputs due to the fact that they determine the utility, quality and efficacy of a particular artefact's appropriate use within its desired environment for intended use (Hevner et al., 2004). Apart from designing an artefact for appropriate use, Design Science Research also empowers researchers to understand and learn about the real world and the issues that pertain it (Pirkkalainen, 2015).

2.4 DESIGN SCIENCE RESEARCH FRAMEWORK

Design Science Research focuses on mainly two constructs. Firstly, design as an artefact (constructs, models, methods and instantiations), secondly, design as a process (building and evaluating). Hevner (2007) proposed a design science research framework to assist in the production and evaluation of IT artefacts (Figure 2.1). The Information Systems Research Framework (ISRF) aims to aid the development of Information Systems solutions within a socio-technical environment. The framework is comprised of three cycles; relevance cycle, design cycle and the rigor cycle (Figure 2.1).

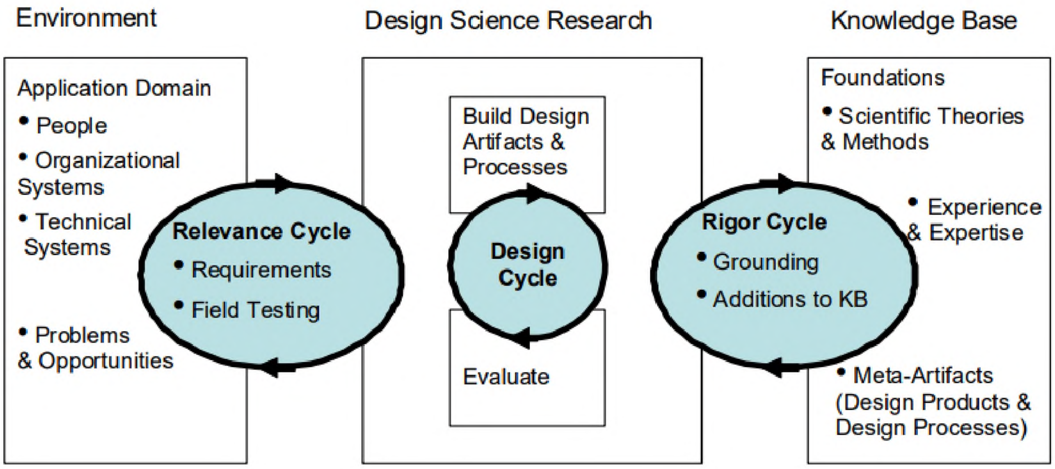
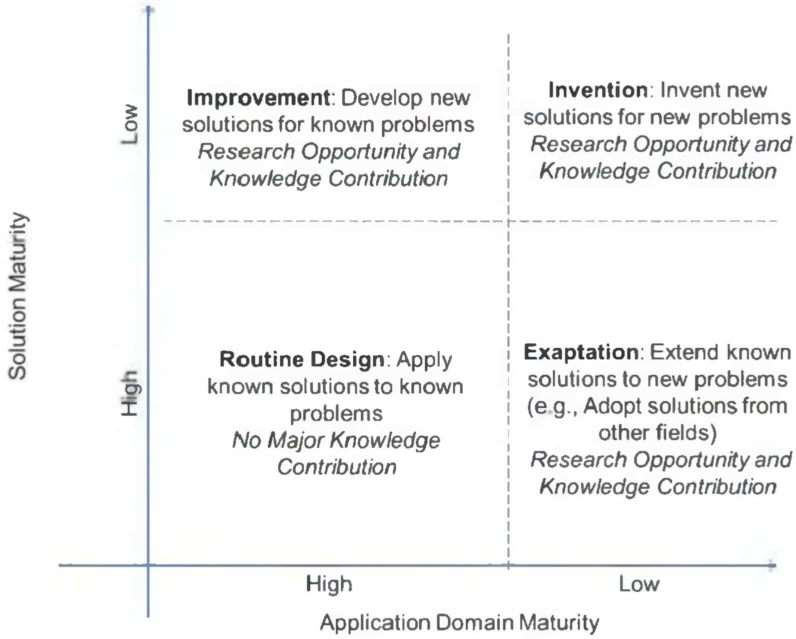


Figure 2.1: Design Science Research Cycles (Hevner, 2007)

Relevance focuses on assessing the environment which the artefact will be developed in. This aims to align the developed and designed artefact to the intended environment. This intended environment requires the researcher to assess the people, organization, technological systems and the opportunities and problems of the environment. The rigor cycle focuses on designing the artefact on sound existing theoretical foundations and frameworks that are applicable to the environment. These theoretical foundations are; knowledge of scientific theories and methods; experience and expertise; knowledge of existing and current developed artefacts and process pertaining to the application domain. This cycle aims to draw from and provide past knowledge so as to ensure the developed artefact is innovative. The relevance cycle and rigor cycle both contribute to the design cycle. The design cycle pertains to building and evaluating the designed artefact. It is also important to note that within the design cycle the developed artefact is iteratively assessed and refined by conducting case studies, experiments, field studies or simulation.

Hevner (2007) also describes within his framework the importance of creating additions to the knowledge of existing theoretical foundations and frameworks based from the designed artefact. Gregor and Hevner (2013) describe four possible types of contributions that may be produced by conducting Design Science Research (Figure 2.2).



Improvement: Develop new solutions for known problems Research Opportunity and Knowledge Contribution
Invention: Invent new solutions for new problems Research Opportunity and Knowledge Contribution
Routine Design: Apply known solutions to known problems No Major Knowledge Contribution
Exaptation: Extend known solutions to new problems (e.g., Adopt solutions from other fields) Research Opportunity and Knowledge Contribution
Low
High
Solution Maturity
High
Low
Application Domain Maturity

Figure 2.2: DSR Knowledge Contribution Framework (Gregor and Hevner, 2013)

Figure 2.2 identifies a 2 x 2 matrix with two important units; Solution Maturity and Application Domain Maturity. The y-axis (Solution Maturity) is a measure of the solutions available within the field of study. The x-axis (Application Domain Maturity) measures the degree to which the problem area has been addressed by individuals. Depending on Solution Maturity and Application Domain Maturity, four possible knowledge contribution can be produced; Invention, Improvement, Exaptation and Routine Design. The identified matrix is useful for it assists the researcher to understand and critique the research contribution. Furthermore, to communicate new ideas to stakeholder communities (Gregor et al., 2013). The identified matrix was used to assess the type of contribution formulated by the research framework. This assessment was done in conjunction, with Research Question 4; '*How viable is the proposed threat assessment framework for determining the vulnerabilities for the consumer health wearable ecosystem?*' Through this, the contribution fell into the **Exaptation** quadrant. A detailed discussion on the knowledge contribution is articulated in Chapter 9.

Hevner (2007) provides seven guidelines to explain the stages for conducting Design Science Research in Information Systems as it pertains to this research study (Table 2.2).

Table 2.2: Design Science Research Guidelines Adapted from Hevner (2007)

Guideline	Description	Application
Design as an artefact	Design- science research must produce a viable artefact in the form of a construct, a model a method or an instantiation	The developed artefact is a threat assessment framework that aids to identify the potential vulnerabilities towards consumer health wearables and their associated applications
Problem relevance	The objective of design-science research is to develop technology-based solutions to important and relevant business problems.	The problem recognized is there is a lack of guidance towards the vulnerabilities specifically towards consumer health wearables and their associated applications
Design Evaluation	The utility, quality, and efficacy of a design artefact must be rigorously demonstrated via well-executed evaluation methods.	The evaluation of the artefact is conducted through two phases demonstration and expert review to outline the utility, quality and efficacy (Peffers et al., 2007). The demonstration of the artefact demonstrates the utility and efficacy of the artefact. This was illustrated by utilising the threat assessment on two test cases. The artefact was also evaluated through expert review, by assessing the pragmatism, semantics and syntax. This assisted to evaluate the quality of the framework
Research Contributions	Effective design-science research must provide clear and verifiable contributions in the areas of the design artefact, design foundations, and/or design methodologies.	The developed artefact provides a research contribution exaptation by contributing to existing frameworks and extending them to new problems of consumer health wearables. This was done by classifying threats pertaining to consumer wearables in six categories (authentication, authorization, availability, confidentiality, non-repudiation and integrity)
Research Rigor	Design-science research relies upon the application of rigorous methods in both the construction and evaluation of the design artefact.	The construction of framework was guided by existing threat assessment frameworks and sound discovered vulnerabilities by security experts. The evaluation of the design artefact was also guided through a framework by Helfert, Donnellan and Ostrowski (2012)
Design as a Search Process	The search for an effective artefact requires utilizing available means to reach desired ends while satisfying laws in the problem environment.	The research questions were answered by using an analysis of literature, existing theories and previous studies. This method ensured a variety of different sound viewpoints to retrieve concrete, legitimate and relevant results.
Communication of Research	Design-science research must be presented effectively both to technology-oriented as well as management-oriented audiences.	The developed artefact provided a threat assessment framework to aid the assessment of vulnerabilities towards consumer health wearables and their associated applications. The framework has been communicated in a conference proceedings paper and the results made available through a written dissertation.

2.5 DESIGN SCIENCE PROCESS

Peffers et al. (2007) proposed a design science research process model to assist researchers with conducting design science research (Figure 2.3), which is based on the work of Hevner (2007). This model aids to enforce rigor, by both focusing on research and design. The proposed model is described as The Design Science Research Methodology (DSRM) Process Model (Peffers et al. 2007) (Figure 2.3).

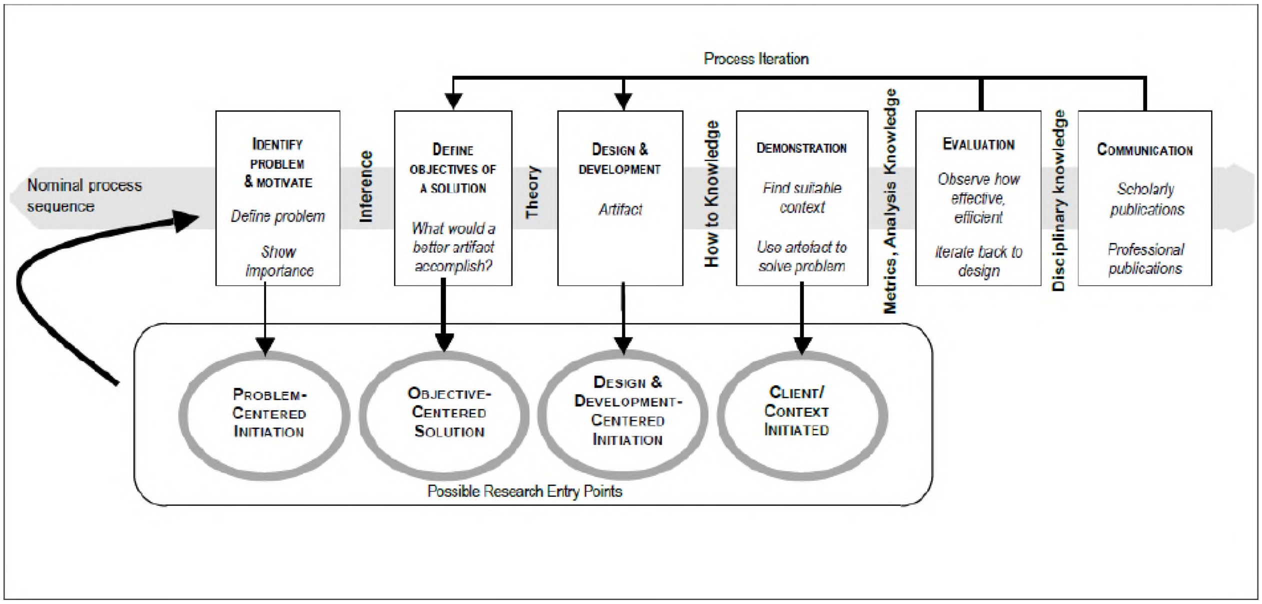

Process Iteration
Nominal process sequence
IDENTIFY PROBLEM & MOTIVATE
Define problem
Show importance
Inference
DEFINE OBJECTIVES OF A SOLUTION
What would a better artifact accomplish?
Theory
DESIGN & DEVELOPMENT
Artifact
How to Knowledge
DEMONSTRATION
Find suitable context
Use artifact to solve problem
Metrics, Analysis Knowledge
EVALUATION
Observe how effective, efficient
Iterate back to design
Disciplinary knowledge
COMMUNICATION
Scholarly publications
Professional publications
PROBLEM-CENTERED INITIATION
OBJECTIVE-CENTERED SOLUTION
DESIGN & DEVELOPMENT-CENTERED INITIATION
CLIENT/ CONTEXT INITIATED
Possible Research Entry Points

Figure 2.3: Design Science Research Process (DSRP) Model (Peffers, et al., 2007)

Figure 2.3 outlines six critical activities that need to be conducted with the DSRM Process Model; Identify the problem, Define the objectives of the solution, Design and Development, Demonstration, Evaluation and Communication of the solution.

2.5.1 Design Science Process for Research Study

For this research study the design science process model by Peffers et al. (2007) was used to attain an effective development of the artefact. This was conducted by processing through the six activities (Figure 2.4).

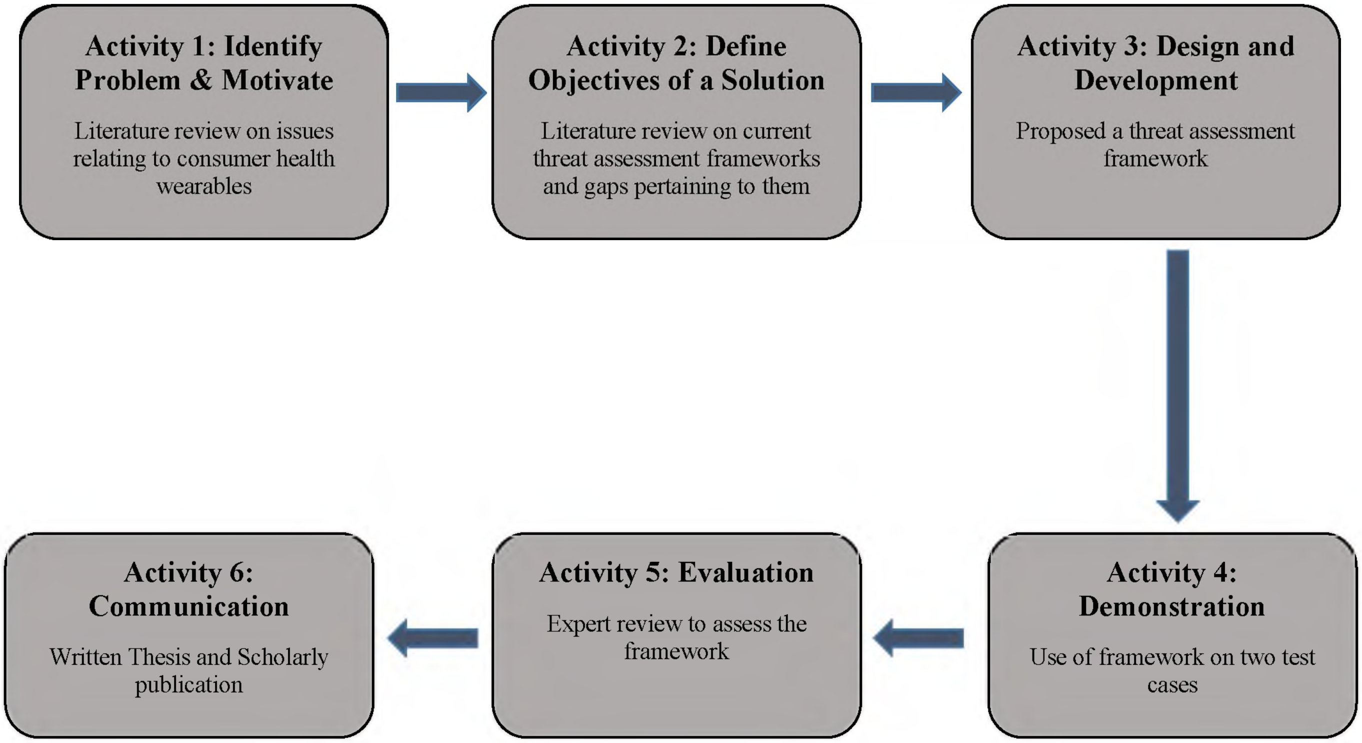

Activity 1: Identify Problem & Motivate
Literature review on issues relating to consumer health wearables
Activity 2: Define Objectives of a Solution
Literature review on current threat assessment frameworks and gaps pertaining to them
Activity 3: Design and Development
Proposed a threat assessment framework
Activity 4: Demonstration
Use of framework on two test cases
Activity 5: Evaluation
Expert review to assess the framework
Activity 6: Communication
Written Thesis and Scholarly publication

Figure 2.4: Design Science Process Model for Research Study

Step 1 Identify the Problem and Motivate: This activity involved understanding the problems related to the research project. To understand this, a literature review was conducted, focusing on the consumer health environment and the issues that pertain to it. This first step by Peffers et al. (2007) helped to answer **RQ1** and **RQ2**. This step was conducted in Chapter 3, and 4. Chapter 3 focused on understanding the consumer health environment which concentrated on the meaning of consumers, consumer health data and the technology used to collect consumer health data. This chapter concluded by identifying there is a great need for consumer health wearables and their associated devices specifically towards growing the patient-physician experience. Nonetheless, one of the greatest challenges facing this environment are the issues of privacy and security. Chapter 4 continued to identify the problem by highlighting the consumer health wearable architecture and the security concerns relating to this architecture. Fourteen collated potential security issues were identified that affect consumer health wearables and their associated applications.

Step 2 Define Objectives of a Solution: From understanding the problems, step 2 involves setting the objectives of how the solution can be accomplished. Within Design Science Research, this is attained by either conducting quantitative or qualitative research. For this research project a qualitative approach was conducted to attain a thorough understanding of how the problems identified in the previous step will need to be solved. This step will help answer **RQ3** where it was conducted in chapter 5. Chapter 5 focused on the process of defining the objectives of a solution by identifying the components needed to be incorporated for assessing the security of consumer health wearables. Through this, the manner in which threats pertaining to consumer health wearables can be better identified and assessed. This was attained by firstly understanding existing theoretical threat assessment frameworks by identifying their advantages, disadvantages and their applicability towards consumer health data. Within this process, there were gaps established within these frameworks that did not assist to fully help to assess consumer health wearables. Chapter 5 concluded by identifying a set of factors needed to be established to produce a threat assessment framework for consumer health wearables and their associated application

Step 3 Design and Development: This activity involves designing and developing the artefact. For this research project a security threat assessment framework was created from the exiting literature identified from the previous steps conducted. This step was conducted in chapter 6 where the gaps that were identified in chapter 5 from existing frameworks was assessed and created to formulate a framework to tackle the problem at hand.

Step 4 Demonstration: This activity involved demonstrating how the artefact can be utilised to address the problem. As the problem at hand, is the lack and need of a security threat assessment framework for consumer health wearables. Two test cases of fitness trackers and their associated applications were acquired. This demonstration was conducted in chapter 7 which identified the security vulnerabilities of these test cases. This demonstration phase helped to substantiate that through understanding the vulnerabilities then better processes to protect fitness trackers can be tackled. This activity will help to answer **RQ4**.

Step 5 Evaluation: Hevner (2007) describes that one of the important components of design science research is evaluation for the designed artefact. This step of evaluation focused on evaluating the developed artefact and assessing if the artefact fully addresses the problem. The evaluation of the artefact needs to be conducted by assessing the utility, efficacy and quality of the designed artefact (Hevner et al., 2004). The chosen instrument used to guide this process was the Information Quality Framework for Design Evaluation by Helfert, Donnellan and Ostrowski (2012). This assessment was conducted by four security experts who gauged the effectiveness of the threat assessment framework. The assessment was conducted through interviews with the use of questionnaire using semantic differentials. The questionnaire focused on three elements pragmatism, syntax and semantics of the threat assessment framework (Helfert et al., 2012). Feedback obtained from the expert review was used to identify which aspects of the framework are needed to be improved. The feedback obtained was used to iterate back to the design and development activity to reinforce the proposed security evaluation framework. This activity will help to answer **RQ4**. The full evaluation process and the results obtained through the process is outlined in chapter 8 of the research dissertation.

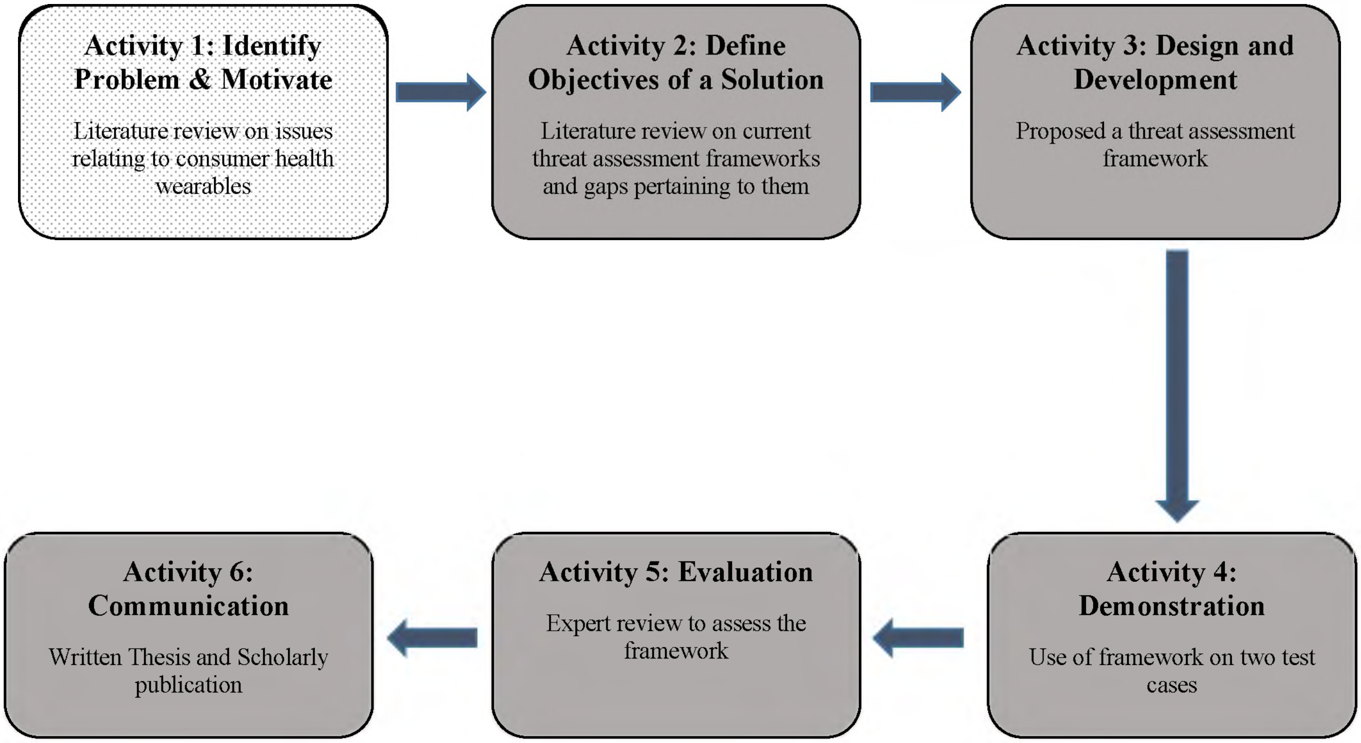
Step 6 Communication: Communication of the solution was achieved by a written thesis, and the following article:

1. Mnjama, J., Foster, G. and Irwin, B., 2017. A Privacy and Security Threat Assessment Framework for Consumer Health Wearables. In: *Proceedings of the 2017 ISSA Conference. pp.66-73.*

2.6 CONCLUSION

This chapter focused on describing the chosen research methodology for this research project. The Design Science Research approach is the overarching research approach. This approach focuses on creating artefacts that can be used for real world situations. For the development of the artefact the Peffers et al. (2007) design science research process model is model used to guide the process of the formulation of the framework.

Chapter 3: CONSUMER HEALTH DATA


Activity 1: Identify Problem & Motivate
Literature review on issues relating to consumer health wearables
Activity 2: Define Objectives of a Solution
Literature review on current threat assessment frameworks and gaps pertaining to them
Activity 3: Design and Development
Proposed a threat assessment framework
Activity 4: Demonstration
Use of framework on two test cases
Activity 5: Evaluation
Expert review to assess the framework
Activity 6: Communication
Written Thesis and Scholarly publication

3.1 Introduction

The main objective of this research is to develop a threat assessment framework that can be used to assess consumer health wearables and their associated applications. This threat assessment framework will assist to provide a basis of coverage of the vulnerabilities affecting this environment. In accordance with the Design Science Research Methodology by Peffers et al., (2007), this Chapter addresses **Activity 1** of: Identify The Problem And Motivate. To attain this, Chapter 3 focuses on answering research question 1, '*What health data do consumer health wearables collect and store?*'. Through, understanding this, can the requirements needed for a threat assessment for consumer health wearable be understood. This chapter begins by firstly introducing physical wellness and the manner in which it is being transformed through consumer health (Section 3.2). Section 3.3 will expand on this by describing consumer health wearables and their associated applications and how they empower consumers to improve their physical wellness. Through describing consumer health wearables, may a discussion be presented on the type of health data collected through these devices (Section 3.4) as well as the aim and significance of this health information. A final discussion (Section 3.5) is presented on the issues relating to health regulatory bodies towards health data collected by consumer health wearables.

3.2 Physical Wellness

Physical wellness can be described as the act of promoting and maintaining proper care of one's body for optimal health and conditioning (Adams et al., 2000). Physical wellness focuses on the balance of three areas to keep a person in the appropriate condition; physical activity, nutrition and mental wellbeing (Adams et al., 2000). To attain a healthy, fit lifestyle, we need to constantly attempt to improve our wellbeing (Callahan, 1973). This journey of continuously improving one's wellbeing is not an easy task. A person is required to exercise regularly, consume the appropriate foods and supplementation and furthermore make check-ups with a local physician to ensure that they are meeting their physical wellness goals (Lewis et al., 2010). As such, health experts have played a vital role in assisting and providing consultation to individuals to attain a healthy lifestyle.

A typical consultation with a health expert will include identifying a specific health related problem, investigating the causes of the problem, giving advice with the necessary remedies to combat the problem and finally making a course of action to rectify the health related issue (Tähepold et al., 2006). Through this, it assists and guides individuals to improve their physical wellbeing. Healthcare services have been physician-centric, the sole responsibility of the wellbeing of a patient is the physician (Archer, Fevrier-Thomas, Lokker, McKibbon and Straus, 2011). However, the rise of internet usage has formulated new avenues to attain health related information (Tomlinson et al., 2013). While online search engines such as Google Search, allow people to search for health related information such as nutrition and physical activity content with ease. All that is required is for an individual to have a device with a stable internet connection and they may search for any information to improve their wellbeing. The information discovered may then be shared to a local physician or family members with the manner in which they improved their wellbeing (Demiris et al., 2008). Information Technology as a result is providing avenues and shifting health services from physician-centric to patient-centric (Rozenblum and Bates, 2013). This is attained by individuals to not solely be reliant to obtain physical wellness recommendations from health experts, but also through online resources.

Modern-day ‘pop culture’ has also tremendously influenced a persons perceived ideal physique and healthy lifestyle that is displayed on advertisements, television and the internet (Barcena et al., 2014). People seek and have a need to identify ways that may improve their wellbeing physically, mentally and spiritually, outside the confines of a medical setting. An example is people desiring to know their total calorie intake of the day based on the foods or supplementation taken. This is supported by popular websites like My fitness Pal that offers the general public such services (Rooksby, Rost, Morrison and Chalmers, 2014). This desire and move of individuals in healthcare to participate and inquire about their physical wellbeing can be described as Consumer Health (Piwek et al., 2016).

3.2.1 Consumer Health

Consumer Health is a subject area that focuses on the need and desire of the public to improve their well-being through technological knowledge resources (Eysenbach, 2000; Flaherty et al., 2015). The American Medical Informatics Association (2016) elaborates on this as a field that is both consumer and patient-centric. It empowers consumers to learn and educate themselves on health and manage their own health through personal health records. A consumer within the consumer health ecosystem can be described with the following characteristics (Ferguson, 2000; Lewis et al., 2010);

1. A person within the general public, who is not a professional within healthcare.

2. Someone who is knowledge seeking of the embetterment of one self's healthcare.
3. Active decision makers of their own wellbeing.

Consumers do not use technology to substitute the role of medical practitioners. The technology utilised is an enabler to guide consumers to further enhance and educate themselves to gain a better health condition. Consumer health plays a critical role within healthcare services as it transforms consumers to be active participants with their health, and enhancing engagement with medical practitioners (Lobelo et al., 2016).

As described, the core of consumer health is the desire of individuals to make informed health related decisions based on the information they have received through technological resources (Alpay, Verhoef, Xie, Te'eni and Zwetsloot-Schonk, 2009). To make informed decisions, a person needs to understand what needs to be changed. Understanding is attained from knowledge, and knowledge is gained by learning; acquiring data (Ackoff, 1989). A growing market in which consumers make informed health decisions, is by quantifying behavioural activities with the use of consumer health wearables to understand how to improve their physical wellness through goal driven techniques. This quantified data is currently mostly utilised by individuals who desire to manage their weight and also for diabetic individuals (Dehling et al., 2015). Behavioural activities like calorie intake, alcohol consumption, sleeping patterns or physical activities (walking, running) are quantified for assessment. Through the quantified data collected, a consumer is able to self-manage, and track the areas to improve based on oneself and ultimately improve their physical wellbeing (Kotz, 2011; Avancha, Baxi and Kotz, 2012).

The 'Quantified Self' is a growing field within Consumer Health and it is viewed to make tremendous benefits for consumers to make better health decisions (Caldwell, 2014; Wicks et al., 2015). This is for the fact that consumer health wearables and their associated applications allow for a consumer to collect health data continuously; twenty-four hours in a day, seven days in a week (Barcena et al., 2014).

3.3 CONSUMER HEALTH WEARABLES

There is an array of tools to which a consumer may use to quantify and monitor their health data the most proliferate tool currently used are consumer health wearables. Consumer health wearables are technological devices used by consumers to track and learn more about their physical wellbeing. These devices in most cases are typically worn or woven into the clothing of individuals. There are numerous types of consumer health wearables available on the market for a consumer of which some include; smartwatches, smart jewellery, fitness trackers, smart clothing, head-mounted displays and implantable devices (Dehling et al., 2015). Figure 3.1 shows examples of the types of consumer health wearables that can be used by a consumer to track their health information (Piwek et al., 2016).

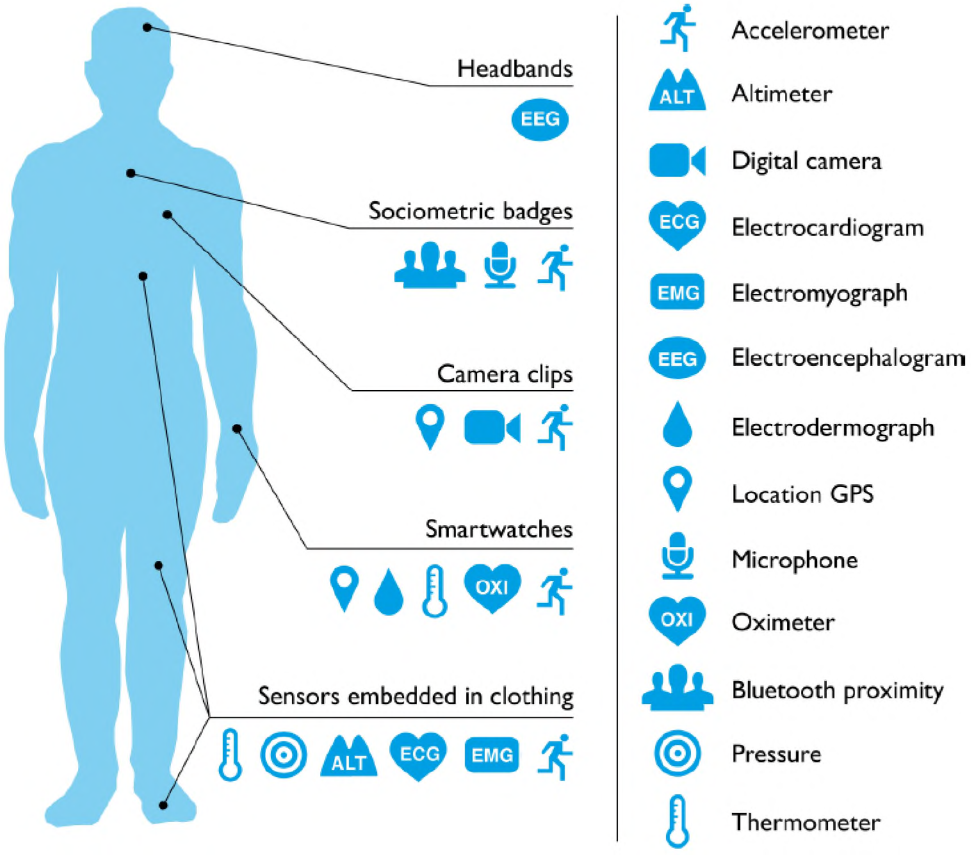


Figure 3.1: Types of Consumer Health Wearables (Piwek et al., 2016)

Each of the different types of consumer health wearable devices have their advantages for their target market, however one of the leading devices driving the consumer health wearable market are fitness trackers. Fitness trackers are growing at an exponential rate and it was estimated over 61 million units were sold in 2016 with a revenue of $3.8 billion. This figure is expected to rise to over $6 billion with over 187 million units being sold by the year 2020 (Lamkin, 2016). Consumer health wearables assist to promote physical wellness as they provide a consumer with the functionality to track their physical activity data through, accelerometers and GPS meters to monitor the distance travelled such as cycling. In addition, they assist to track physiological data like the heart rate of a consumer through oximeters. Common features imbedded in consumer health wearables include a battery, power button, motion sensor (accelerometer, gyroscopes), heart rate monitors, Bluetooth chip and a form of a LED display (Barcena et al., 2014).

As consumer health wearables have limited display screens they hinder the degree to which consumers may review their health data. This has led to consumer health wearables having associated software to be installed on mobile devices (smartphones and tablets). This associated software aids consumers to review health targets and how they improve their physical wellness. Mobile devices are growing as a suitable platform for the associated software of consumer health wearables due to their portability and internal features that allow for user health related engagement (Ahmed and Ahamad, 2012; La Polla, Martinelli and Sgandurra, 2013). This is a result of the variety of sensors that are contained within them; accelerometers, gyroscopes, GPS, and fingerprint sensors are just some of the few sensors (Mantovani, Quinn, Guihen, Habbig and Hert, 2013). Table 3.1 outlines some of the components embedded within a mobile device and how they can be applied to health inventions in conjunction with consumer health wearables.

Table 3.1:Mobile Device Functions for Health Intervention

Component	Application
Screen	Viewing rich detailed information. In addition with providing a multi-touch display for user engagement (Liu et al., 2011)
Network Coverage (WiFi, Broadband 3G/4G)	Capability to make internet connectivity to search for health related information.(Morera et al., 2016)
Keypad	For documentation of health information (Klasnja and Pratt, 2012).
Camera	Documentation of progress through visual representation. Used as a point of reflection of previous well-being (Klasnja et al., 2012)
Phone Storage	Storage of health data.
GPS	Location tracking and monitoring. GPS monitoring offers fitness individuals the capability to view the distance, speed and time of their fitness activity. (Michael and Njie, 2013)
Accelerometer, Gyroscope	Used to track movement conducted by an individual. A common application is tracking the number of steps taken by a person to improve the activity performance of inactive individuals (Barcena et al., 2014).
Speakers and Microphone	Sleep monitoring: to the assess the quality of sleep attained by an individual (Chen et al., 2013)

3.4 Consumer Health Data

The collection of health data from consumer health wearables is used to help guide an individual to reach a specific health target. This information may include their behaviour patterns like eating, drinking or sleeping (Flaherty et al., 2015). Consumer health wearables and their associated applications store health data of a consumer to provide user specific health information. Researchers have described health data for a consumer that is stored on consumer health wearables and their associated applications as a *Personal Health Record* or *Patient Generated Health Data* (Huba and Zhang, 2012; Shapiro, Johnston, Wald and Mon, 2012). However, there are two types of personal health records which are described by literature to which assist to collect medical related health data. These two types of personal health records are **stand alone personal health records** and **tethered/connected personal health records** (Office of the National Coordinator for

Health Information Technology (ONC), 2016). Tethered personal health records allow individuals to connect to an electronic health record system of a medical institution or a health plan's information system. Through this, individuals are able to access their information through a secure portal. In addition, the information that individuals may include in their personal health record are lab results, immunization history, and medical history. This information may be viewed by tethering to a medical institution medical systems.

Stand alone personal health records on the other hand include information that is filled by individuals from their own records or memories. This information is managed and stored on an individual's selected device that is used to record such information (Office of the National Coordinator for Health Information Technology (ONC), 2016).

However, the definitions of both tethered personal health records and stand alone personal health records does not fully describe the nature of health data collected by consumer health wearables and their associated applications. As compared to tethered personal health records, data collected from consumer health wearables are used outside the environment of medical institutions and are not primarily designed to connect medical portals. It also presented through the literature, that stand-alone personal health records are used in the act of journaling health data outside the confines of a medical setting. Consumer health wearables and their associated applications are not tools for journaling medical data. These devices are used to manage the health data of consumers where through this information, user based feedback from analytical servers are provided to consumers on the information collected on how to improve physical wellness. To fully describe the data collected by consumer wearables and their associated applications, the term 'Consumer Health Data' is used to annotate this (Mnjama, Foster and Irwin, 2017). The term consumer health data assists to align the manner in which consumers desire to improve their wellbeing outside the confines of a medical setting or system through the use of technological devices (Mnjama et al., 2017).

Through the use of literature different characteristics have been found to describe personal health records. These definitions can be used to outline the characteristics of consumer health data, based from the use of consumer health wearables. Löhr, Sadeghi and Winandy (2010) describe personal health records as a tool that individuals use to access, manage or share their own health information through technological devices. Tang et al. (2006) description of personal health records was in line with this viewpoint. However, it is described within the definition the representation of ‘patients’ who use personal health records. Where patients can be different stakeholders like family members, doctors, and individuals who provide access to the personal health record of a patient. The Office of the National Coordinator for Health Information Technology (ONC) (2016) further describes personal health records as the core responsibility of individuals to document and assess their wellbeing and they do not replace the medical records created by medical institutions. From these definitions consumer health data can be described with the following characteristics;

1. They are managed by individuals, through technological devices
2. May include self-documented information collected by an individual
3. Helps individuals to securely and confidentially store and monitor their health information, outside the confines of a medical setting.
4. They do not replace or separate the medical or legal records created by health care providers.

3.4.1 Data types of Consumer Health Data

Consumer health data collected from consumer health wearables is used to guide consumers through progress reports and goal driven mechanisms to achieve optimal physical wellness goals. Consumer health wearables may contain different data fields of consumer health data that allow a consumer to manage specific information about themselves. Table 3.2 outlines examples of some of the data fields of which consumers may record within health applications. Depending on the tool used to record the health data, there can be relationships across data to foster an environment for rich, detailed information (Dehling et al., 2015). For example, a consumer may solely be interested with improving their diet. This will require the user to record the types of food eaten and their composition of fats, carbohydrates and protein. Whereas, a different individual may desire to assess how their habit of smoking affects their sporting activities. This can be done by recording the number of cigarettes smoked in day, and the sporting activities accomplished.

Table 3.2: Data Type Examples of Consumer Health Data

Data Type	Description
Consumption: - Calories/Food - Alcohol - Water - Caffeine - Nicotine/Cigarettes	This data relates to consumption values. The data normally obtained from this is the nutrition composition of foods or amount of water consumed in litres during the course of the day. In most cases consumer health wearables are unable to automate the collection of consumption data. This information is manually documented on the associated application of the consumer health wearable device. Based on the data captured, the application will give recommended feedback.
Physical Activity: - Sport Activity - Sleep	This data relates to any physical activity that a consumer may have participated in. This can relate to swimming, running, the number of stairs climbed, the number of hours spent sitting down, the quality and quantity of sleep.
Physiological Statistics - Heart Rate - Temperature - Blood pressure	This data relates to the physiological data of a consumer. Currently, a majority of consumer health wearables collect heart rate data, body temperature and blood pressure

The protection and privacy of health data is of critical importance as it contains sensitive information that should not be disclosed to unwanted parties. Personal health data refers to any health related information that an individual may use to manage and share with others in a private, secure environment (Tang et al., 2006). Within the medical field, it very important to keep health related information confidential and private. Even a person’s age or gender is deemed personal (Nass, Levit and Gostin, 2009). Privacy of health information is important because it aims to protect an individual’s autonomy, and dignity. Furthermore, it helps to protect people from embarrassment, stigma and discrimination (Nass et al., 2009).

3.4.2 Aim and Significance of Consumer Health Data

Consumer health data is used as a reference to help guide consumers in the manner in which they may improve their physical wellbeing. Consumer health wearables are viewed by medical practitioners as not just step counters, but as devices to provide medical intervention towards consumers. Some of the uses identified by consumer health wearables to assist to identify health symptoms. The duration of sleep can assist to identify severity of depressive symptoms in consumer health wearables (Azar et al., 2013). Furthermore, consumer health wearables have been identified to assist consumers to tackle illnesses like obesity and hypertension they promoting physical activity (Nazi et al., 2016).

Consumer health wearables are viewed to enhance the patient-physician experience within the medical community. This patient-physician experience can be described as consumer using consumer health data to be activity engaged to improve their physical wellbeing (Franklin et al., 2016). Through the consumer health data collect consumers may discuss with physicians how their daily activities like exercising and sleeping affected their wellbeing (Franklin et al., 2016). Consumer health data can therefore be seen as a way of providing a holistic viewpoint of the patient to the medical expert. However, one of the major barriers hindering the adoption and growth of consumer health wearables within the medical are the issues of privacy and security.

3.4.3 Health Application Regulation

As consumer health data contain sensitive data, regulation is enforced to ensure that security and privacy is adhered to (Thompson and Brodsky, 2013; Charani et al., 2014; Wicks et al., 2015). Consumer health wearables and their associated applications can be regulated in two different ways; by application stores where the associate application is download from and by regulatory bodies. Currently, the two leading application stores are Google Play and Apple App Store (Mantovani et al., 2013). However, these stores have two different ways in which applications will be accredited and released for download. The Apple App Store is driven by quality, and standards. Whether an application is developed by a single person or a big corporation each application goes through peer review before it released on the application store (Cuadrado and Dueñas, 2012; Apple, 2016). However, this review is centred on aesthetics and functionality. Little consideration is made on the privacy and security concerns of the health application. Google Play on the other hand has a different approach in which applications are released. Focus is placed on innovation, and unlike Apple's App Store there is not a team to accredit the applications (Cuadrado et al., 2012; Google, 2016). Rather, there is an automated protocol that checks the security of application. If an application passes the security check, then it is available for download (Speed, Nykamp, Heiser, Anderson and Nampalli, 2013; Google, 2016). As a consumer acquiring applications on online stores, there needs to be assurance of that on purchase, the associated application of the consumer health wearable device is accredited for proper use by the general public. Nonetheless many of health applications available on application stores have security and privacy concerns.

There is good reason for this concern and it is for that intention that regulatory bodies like the NHS (National Health Services) and FDA (Food and Drug Administration) have attempted to formulate standards and guidelines to accredit health applications. These regulations are aimed to assist consumers as they search for health applications to choose only applications that are accredited. Furthermore, they aim to provide enforcement and oversight over health applications that are produced (Kamerow, 2013).

The FDA describes a medical health application as an application that connects to a medical device or a medical device that transforms a mobile platform for medical use (FDA, 2015). For example, health applications that connect to pace makers or health applications that are used to view PACS (digital images from radiological reports) (FDA, 2016). Although, the FDA is centred to enforce regulation, many consumer health wearables fall out the bounds of the set regulations. This due to the fact that the FDA mostly focus on applications that are utilised in the sphere of Mobile Health; connecting personal health records with electronic health records in hospitals (Charani et al., 2014; FDA, 2015). Some of these regulations for example are centred on applications that;

- Use GPS (Global Positioning System) locations to alert medical practitioners when an individual is in environmental area that could lead to an asthma attack
- Mobile applications that make the user enter behavioural or environmental information that are *pre-defined by a health practitioner*.
- Mobile applications that collect information such as sex, age and behavioural factors that are *used to help for counselling and preventative authorities* (medical experts)

Consumer health wearables that are outside the bounds of these regulations nonetheless, handle as much sensitive information as to those within the bounds (He, Naveed, Gunter and Nahrstedt, 2014). Consumer health wearables and their associated applications may utilise GPS service to determine the distance and area that was ran by an individual. Consumer health wearables and their associated applications furthermore gather behavioural activities of consumers to provide assistance to a better lifestyle (Barcena et al., 2014).

The United Kingdom also has a governing body known as the NHS (National Health Service). This governing body helps health professionals to recommend health applications to consumers. The accredited applications are aimed to give assurance of secure applications for both health professional and consumers (NHS, 2016). A research study was conducted by Huckvale et al., (2015b) and it was discovered that even accredited consumer health wearables in some cases are also as insecure as to those which are not accredited. 66% of the accredited applications did not encrypt health data and furthermore 67% of the accredited applications did not have any form of a privacy policy (Huckvale et al., 2015).

Within South Africa the Protection of Personal Information (POPI) Act has been signed by law, but it still yet to be commenced (Protection of Personal Information Act, 2013). This Act focuses to regulate the processing of personal information. Any entity that processes information for clients, suppliers, or individuals need to abide by this regulation. Although this act provides oversight of the principles to which personal information is handled. Limited guidance is provided to mobile developers in the manner in which it should be carried forth.

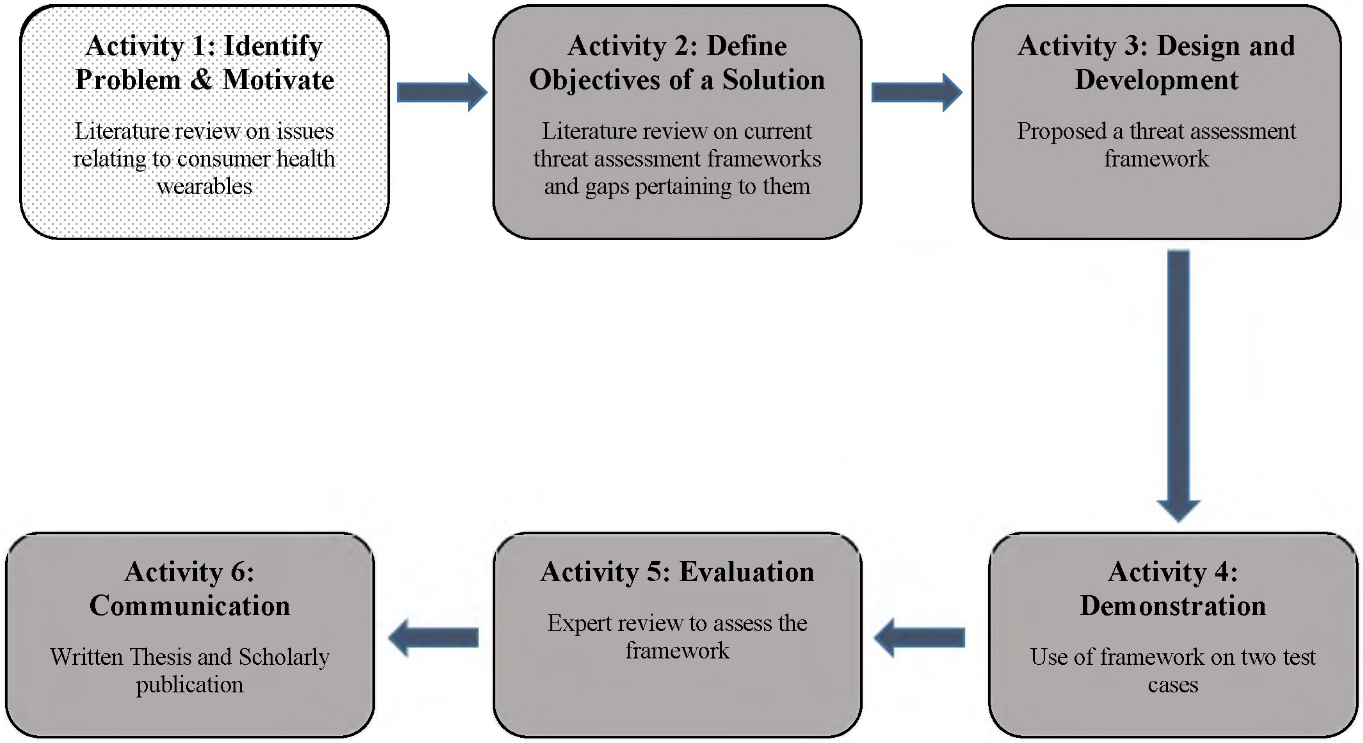
There is challenge facing the protection of consumer health data (Wicks et al., 2015). As consumers do not fully understand the inner workings of the health applications, the confidence that their health data is managed appropriately is based on trust of the device (Huckvale et al., 2015). It is vital therefore to ensure, that the inner workings of such devices are protected and unauthorized individuals will not be able to view such information.

The use of consumer health wearables by consumers is a growing phenomenon and people are still grappling to understand which is the safest way to protect personal health information (Liu et al., 2011; Caldwell, 2014). Developers and organizations face a challenge with the development of consumer health wearables and their associated applications (Adhikari et al., 2014). For those attempting to abide by regulations face a challenge as regulations set by corporations lag behind the change of technology (McCarney, 2016). A study was conducted, by IBM (Ponemon Institute LLC, 2015), to identify the causes and reasons behind the lack of mobile application security. The factors identified was firstly, that organizations and developers rush to release consumer health wearables and their associated application. In addition, there is a lack of security professionals to guide the process to instil security measures of the associated application of consumer health wearables. Very little funding is spent to research and address security concerns. Infrequent testing is made of mobile applications and finally organizations do not address the growing concerns of malicious software (malware) on mobile devices. Security of health applications is a major concern, and as consumer health informatics grows it imperative to identify and understand the risks of health applications so that they may be negated.

3.5 CONCLUSION

A consumer can be described as anyone seeking knowledge to improve their current health condition. Currently, consumers use consumer health wearables and their associated application to attain this knowledge. These applications collect consumer health data, such as physical activity data, consumption data and physiological data. These consumer health wearables nonetheless have privacy and security concerns that make the consumer health data of consumers insecure. As a result it is important to identify the vulnerabilities towards consumer health wearables and their associated applications.

Chapter 4: VULNERABILITIES IN CONSUMER HEALTH WEARABLES


Activity 1: Identify Problem & Motivate
Literature review on issues relating to consumer health wearables
Activity 2: Define Objectives of a Solution
Literature review on current threat assessment frameworks and gaps pertaining to them
Activity 3: Design and Development
Proposed a threat assessment framework
Activity 4: Demonstration
Use of framework on two test cases
Activity 5: Evaluation
Expert review to assess the framework
Activity 6: Communication
Written Thesis and Scholarly publication

4.1 INTRODUCTION

This chapter will focus on **Activity 1** of Identify Problem and Motivate as part of conducting the Design Science Research Process Model by Peffers et al. (2007). Through identifying and motivating the problem, a deeper understanding may be obtained in the development of the desired threat assessment framework. Chapter 3 focused on answering RQ1 "*What health data do consumer health wearables collect and store?*" Through understanding the type of health data collected through consumer health wearables and their associate applications may the vulnerabilities that affect consumer health data be identified. Chapter 4 focuses on answering research question 2, "*What vulnerabilities are associated with the consumer health wearables ecosystem?*" This Chapter is therefore constructed by firstly describing the consumer health wearable ecosystem (Section 4.2). Based from this ecosystem the vulnerabilities that pertain to each of the different technologies of the ecosystem are outlined (Section 4.3). This chapter finally concludes by providing a summary of the vulnerabilities discovered towards consumer health wearables (Section 4.4).

4.2 CONSUMER HEALTH WEARABLE ECOSYSTEM

The consumer health wearable ecosystem is comprised of different components that are used to track and assess the health condition of an individual. To understand the factors that contribute to the risk of consumer health wearables, it is important to first gain knowledge of the consumer health wearable ecosystem. This will aid to identify the components that hinder a secure platform for consumer health data.

An array of technologies may be used to relay information from one tier to another. Nonetheless, it has been discovered through literature that a typical model employed comprises three components that can be utilized to assist a consumer to record their health data (Li et al., 2010; Barcena et al., 2014; Cyr et al., 2014). These components include a wearable device, a health application which is installed on a mobile device and cloud storage to store the health data of the consumer. Each of these components communicate with one another to create a seamless environment for which a consumer may identify the areas to improve on one self (Figure 4.1). Each of the components identified in addition have their own structure to process information. Consumer health data is also contained in different forms throughout the lifetime of the ecosystem.

The consumer health data referred to in this figure can be any data type such as consumption data, physical activity data and physiological data.

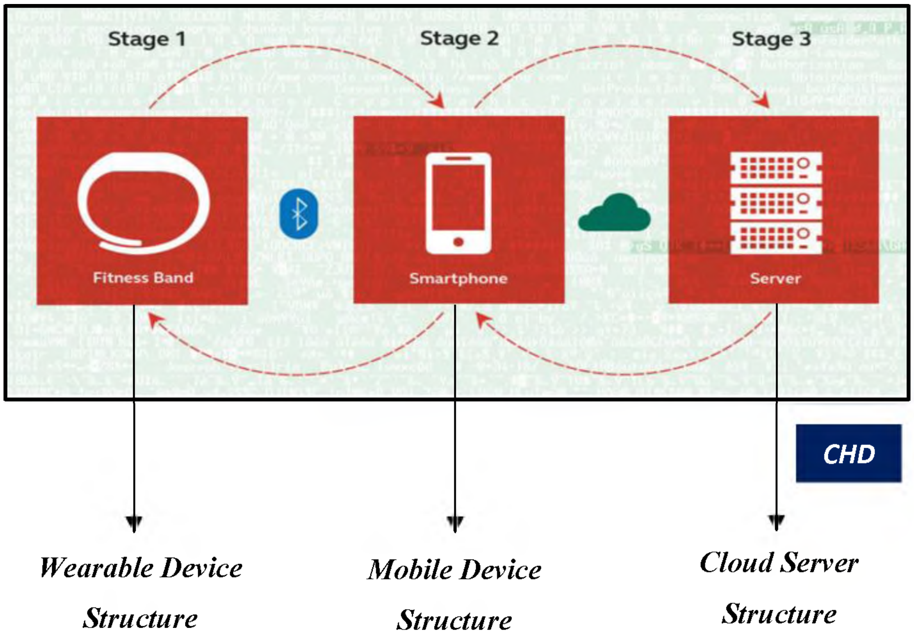


Figure 4.1: Consumer Health Wearable Ecosystem (Funk, 2015)

Three components primarily comprise the ecosystem of consumer health wearables; wearable device, mobile device (smartphone) containing the associated application and cloud storage (Figure 4.1). Each component within the ecosystem has a key function to play as information is sent from one stage to another. Wearables devices (***Stage 1***) generally do not have a rich user interface for a consumer to examine the information that is being collected. At this stage, raw data is collected by the wearable device (Barcena et al., 2014). Once the health data has been collected, it is sent to the mobile device (***Stage 2***). The communication between a wearable device and mobile device is achieved with Bluetooth Low Energy (BTLE) in most cases, but Near Field Communication (NFC) or cable synchronization are also mechanisms used by other devices to attain communication between the two devices. Upon successful transmission, the data is transformed to useful information such as progress history or areas of improvement within the health application. Mobile phones then communicate with cloud servers to back up the health information produced by the health application (***Stage 3***) (Cyr et al., 2014).

The flow of information between a wearable device, mobile devices and cloud storage is not lateral within stages, but cyclical (Cyr et al., 2014). For firmware updates to be made on wearable devices, this information is sent from cloud servers to a mobile device then finally back to the fitness tracker. Furthermore, in certain cases the service of transforming data to information is provided from the cloud. This requires the user have network capabilities such as WiFi or broadband coverage to assess health progress.

Each of the components used within the ecosystem contains its own structure. To formulate a threat assessment framework that may be utilized for developers, a further understanding of each individual structure of the apparatus within the ecosystems needs to be attained.

4.2.1 Consumer Health Wearable Structure

There is an array of different types of wearables that a consumer may purchase to collect their health data. These devices come in different shapes and forms and they can be worn or woven into clothing. Despite their physical structure their core functionality is to collect health data and to send the information to a dedicated receiver such as a mobile device to which they are paired to.

Figure 4.2: Fitbit Flex (Fitbit, 2016)

Common types of wearable devices used by consumers are fitness trackers (Figure 4.2). This device is able to track the number of steps taken by a consumer and their sleeping patterns. Different wearable devices will include different functionality depending on their capability. Common features that are available within fitness trackers include a battery, power button, motion sensor (accelerometers, gyroscopes), Bluetooth chip, form of LED display and syncing capability (jack, USB dongle) (Barcena et al., 2014).

Consumer health wearables contain firmware that is core control the functionality of the device. Firmware is permanent software stored and programmed into the ROM (Read Only Memory) of a device. Firmware assists to dictate how hardware will function. For example, key instructions to turn on or off a device (Cyr et al., 2014). Device manufacturers instil firmware into their devices to ensure they function effectively. Firmware is not usually updated. However, in certain cases firmware may be updated to ensure that the hardware will interact properly with current software.

Consumer health wearables do not have high computing power, but their core function is to collect raw health data and send them to a dedicated receiver (Cyr et al., 2014). They are also used to provide feedback depending on the goal of the user. These devices are created by different manufacturers. Developers may then exploit the functionality of the device depending on the hardware provided from the manufacturers (Funk, 2015). The functionality of the device depends on the firmware that is installed on the device. This firmware dictates how the data is collected and to whom and how the data will be sent.

4.2.2 Smartphone Application Architecture

Mobile devices, specifically smartphone devices, contain operating systems (OS) that allow to perform high performance tasks. The three major operating systems available to consumers include Apple OS, Google Android OS and Microsoft Windows OS (Mantovani et al., 2013). The consumer health wearable ecosystem is similar between all these operating systems. The internal mechanisms in which the health application is managed within the mobile device is different (Mantovani et al., 2013). Each of these operating systems have a specific structure that allows individuals to perform tasks and download applications on to the mobile device. Although each of these operating systems are capable of managing health applications, they all have different structures. Apple OS is programed in Objective C and Google Android is developed using Java. Each operating system uses a different platform and ecosystem in which mobile applications operate in (Dehling et al., 2015). The Android OS is a popular platform used by consumers. The associated application of consumer health wearables are mostly published by Apple or Google Android (Lupton, 2016; McCarney, 2016)

The Android Operating System is open source (Google Android, 2016). This means, that developers may continuously improve the software. This allows, incremental improvement with the software, from a wide array of individuals (Google Android, 2016). Google's Android can be installed on a mobile device depending on it compatibility. The latest Android software is version 8 which is known as Oreo. The Android OS Stack is grouped in layers of which each layer has specific function (Figure 4.3)

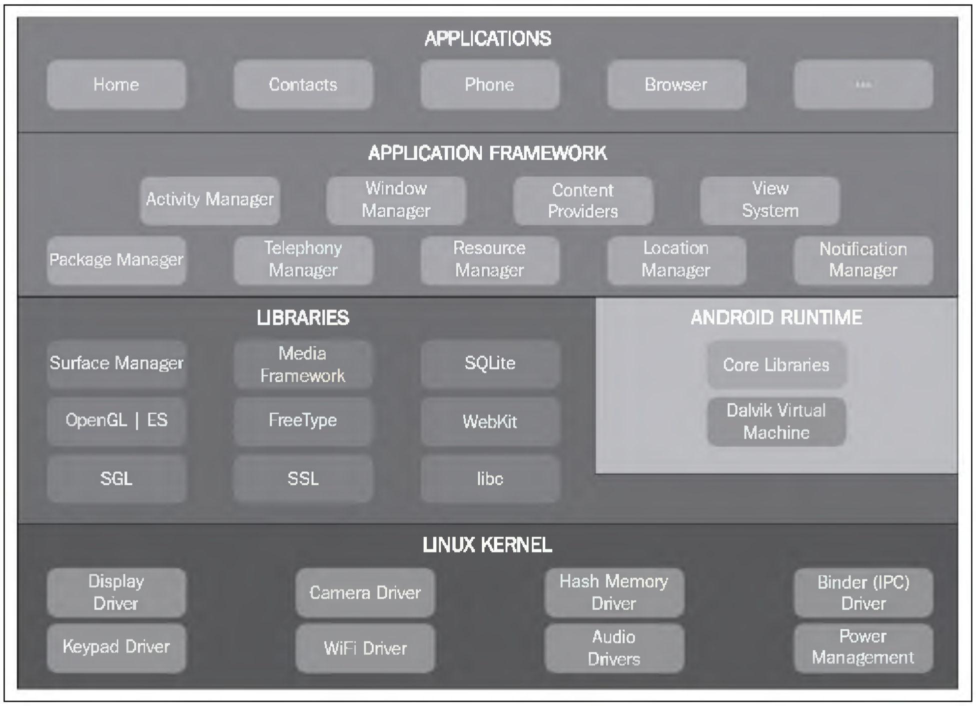


Figure 4.3: Android Application Stack (Rai, 2013)

Linux Kernel: This layer sits above the hardware components of the mobile device. It includes the driver mechanisms for the hardware to perform a specific function. Examples of the components within this layer, include the camera driver, the display driver and the audio drivers.

Libraries and Android Runtime: This layer contributes to the libraries needed for code execution. Examples of the components within this layer include SQLite and SSL.

Application Stack: This stack is split into two components; Application Layer and Application Framework.

Application Layer: Mobile applications that are available for the user to use, operate on this tier. Such applications may be the web browser, or phone contacts.

Application Framework: This layer handles the classes needed for application to use. Such classes include the Package Manager. The package manager is utilized for installing and uninstalling application on the mobile device.

Android Application Structure

Android mobile applications are developed using the java programming language (Google Android, 2016). Android Software Development Kit (SDK) tools are used to compile the solution into a complete package (Rai, 2013). The complete android package is known as an android application package (apk), which will include the data and resource files of the application (Rai, 2013). APK files are saved as Java Archive Files (JAR). An apk file has four key components; Activity, Service, Broadcast and Content Provider (Rai, 2013) (Figure 4.4)

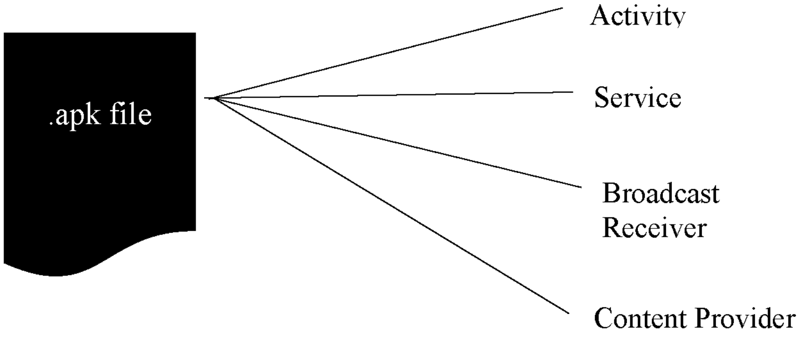


Figure 4.4: Application Structure

Activity: This is the User Interface of the application. The activity component handles the functions that a user will perform. An example of an activity is logging into the application.

Service: These are the services provided by the application. Services are not viewed from the frontend, but occur in the background. A typical service an application will perform is backing up information to cloud servers.

Broadcast Receiver: The broadcast receiver acts to receive information from the android operating system or from other applications. An example of message received is when the mobile device has completed booting (BOOT_completed)

Content Provider: This is the data storage components of the application which handles the manner in which data will be stored in the application.

Android Applications may also include other components which a developer may incorporate within the applications. These components are declared in the manifest file of the application (AndroidManifest.xml) (Google Android, 2016). When an apk file is downloaded to a mobile device, the Android OS assigns the application a unique ID on successful installation (Google Android, 2016). This unique ID is used to assign permissions to the mobile application. Android Security enforces permissions to authorize a mobile application the resources it desires to utilize. For example, if an application requires to use the spatial location of a user, this request needs to be outlined. These requests are placed in the manifest file of an application (Manifest.permission class). The manifest file will outline the permissions required for the application to work and the API level required for the Android Operating System. Android permissions have four protection levels (Rai, 2013). Permissions needs to be declared in the manifest file regardless of their level. Permissions assist with the security and privacy of mobile applications. By a user granting certain permissions to an application gives access to mobile features and/or data for the application to utilize.

Level 0 (Normal Permissions): Permissions on this level do not harm the users and are automatically granted. Nonetheless, the user may still view the resources used by the application and deactivate them. A type of permission within this level for example is using the functionality of vibration (android.permission.VIBRATE).

Level 1 (Dangerous Permissions): This level grants access to device features and data. Granting permissions at this level may cause harm to the user privacy. For example an application may request to use the location of the user (android.permission.ACCESS_FINE_LOCATION).

Level 2 (Signature Permissions): This grants access to two applications to communicate and share components with each other.

Level 3 (Signature/System Permissions): This grants access to the Android System. This level of permission is designed for manufacturers, carriers and system applications. This is a very powerful level, for it authorizes to manipulate system functionality. For example the permission request android.Permission.REBOOT will grant access to reboot the device.

4.2.3 Cloud Server Structure

Cloud Computing can be described as the manner of using remote servers hosted on the internet to store, manage, and process data (Mell and Grance, 2011). Mobile Cloud Computing is a form of cloud computing in which data storage and data processing are performed outside the confines of a mobile device (Dinh, Lee, Niyato and Wang, 2013). As mobile devices have limited resources; battery life, storage and computing power. Mobile Cloud Computing aids to improve the performance of mobile devices. This is attained by harnessing powerful, centralized computing located from the cloud (Huang, 2011; Dinh et al., 2013). Developers are aware of the limited resources of mobile devices. To counter this, a mobile application can be hosted on a remote server. Through which a user may then access the application features through network coverages; WiFi, or broadband coverage. This type of model is known as Software as a Service (SaaS). SaaS can be described as manner in which the applications information and data is accessed remotely from the cloud (Dillon, Wu and Chang, 2010).

4.3 CONSUMER HEALTH DATA VULNERABILITIES

From outlining the consumer health ecosystem, it is noticeable that there are various components needed to ensure processing and storage of health data. It is still vital to ensure that consumer health data is protected. Cohn (2006) describes security as the 'physical, technological, or administrative safeguards or tools used to protect identifiable health data from unwarranted access or disclosure.' It is important for developers to be aware of the security concerns of health applications and the use of fitness trackers. This will aid to understand and further create successful measures to protect personal health information of consumers.

4.3.1 Vulnerabilities towards Consumer Health Wearables

Consumer health wearables, can come in different shapes or forms, but their core function is to collect health related data and transport it to a dedicated receiver such as a smartphone or tablet. As previously mentioned, consumer health wearables currently lack a rich user interface making them dependent on the health application they are synchronized to. This unfortunately limits the authentication processes that can be employed to safeguard them from intruders. Google Glass for example although not commercially available at the moment, aids to identify the limitations and risk of consumer health wearables. These smart glasses can be used to check vital signs of a patient during surgery from the apparatus (Martinez, 2014; Allsopp, 2016). Individuals may also view health related information from the internet either through pairing to their mobile device of which will share the data connection or by prior Wi-Fi configuration. The Wi-Fi configuration is achieved through automatically generated QR (Quick Response) codes containing the connection setting when looked at when using the glasses (Martinez, 2014). However, by using QR codes this may mislead a user to connect to fake access points. Furthermore, it limits any input that can be made by the user during authentication. A further challenge with Fitness Trackers is a limitation with the use of access codes due to interface challenges. It has been discovered that 50% of wearable devices do not have a pin or pattern to protect it from unwanted users (HP Fortify, 2015). If the device is stolen, it can be accessed easily by unwanted users.

Consumer health wearable devices are designed and are capable to be worn by a user throughout the whole day. These sensors have a small storage capacity and need to be synchronized periodically to provide sufficient space to continuously collect data. The communication between consumer health wearable and its associated application in certain cases nonetheless has resulted in security risks with the use of Bluetooth (Cyr et al., 2014). As a wearable needs to communicate to a dedicated receiver, in certain cases these devices are not made invisible once a successful connection has been made (Barcena et al., 2014). Bluetooth signals contain important information such as serial numbers and internal IDs from a device. By this signal being constantly visible, this information may be used for location tracking (Cyr et al., 2014; Funk, 2015). As with some devices, the Bluetooth signal cannot be deactivated from the consumer health wearable device, but only from the health application. Furthermore, in some cases, a consumer health wearables can be paired to more than one device (Selinger, 2015). This is a major security concern, as if a wrong pairing is made to a mobile device, an individual’s health data will be sent to the mobile application as long as the device is in range and paired.

4.3.2 Vulnerabilities towards Health Applications and Cloud Storage

The associate application of consumer wearable devices is download from application stores. Currently, Google Android and Apple are the leading platforms of which consumers download the applications from (Lamkin, 2016). Through this, consumers may attain consumer health data seamlessly on their device. Nonetheless, there are security risks of these applications.

The consumer health wearable ecosystem identified mobile applications at the core of the model; to provide and analyse the information collected. The analytics conducted within health applications are achieved by third-party analytic tools. This allows developers to harness algorithms and methods that have been tested, to analyse health related information. However, few health applications encrypt health data as it is sent over to analytic systems. Data is sent unencrypted by using HTTP (Hyper Text Transfer Protocol) instead of HTTPS (Hyper Text Transfer Protocol Secure) (Michael et al., 2013). Furthermore, in addition to communicate with third-party analytical tools, mobile health applications contact multiple domains in support of the use of the application. This may include application frameworks (connecting to Amazon Web Servers), API's (connecting to social media applications) and Advertising Networks (for revenue generation) (Barcena et al., 2014). These are but a few of the domains that a health application may connect to. Nonetheless, by contacting different domains, metadata of a user's behaviour and activities are being collected.

The lack of encryption structures employed within health applications is of critical concern. This poses a security threat for consumers of which include data modification and eavesdropping. Data modification can be described as changing or replacing of information and sending back the modified data to the original receiver (Al Ameen, Liu and Kwak, 2012). Data modification can occur for example, as communication is established between a consumer wearable device and a health application. When wearable devices require updates such as firmware, the information is sent via the health application to the wireless body area sensor. Firmware is used to update software of devices. Any manipulation of the firmware update can result in changing functionality of the consumer health wearable device (Selinger, 2015). It is discovered that as firmware updates were sent to wearable devices from cloud servers, it is done without encryption (Cyr et al., 2014; HP Fortify, 2015).

Eavesdropping can be described as the unauthorized process of monitoring of communications or interception of data as it is being transmitted over a network (La Polla et al., 2013). Zubaydi, Saleh, Aloul and Sagahyroon, (2015) identify three types of eavesdropping security attacks that can occur with the use of mobile health applications; eavesdropping on unencrypted internet, eavesdropping on logged sensitive health information and eavesdropping on unencrypted SD card storage. Eavesdropping on an unencrypted internet can occur as data is transmitted on a network without any encryption mechanisms. Such attacks result as information is sent in clear text. Through this an intruder can discover health related information of consumers such as specific health conditions. Mobile health applications store user information in logs. Log information can be login credentials or a prescription history. If this information is not encrypted, an unwarranted individual may view a user's profile and use such information for identify theft (He et al., 2014). As health data is collected for a user, this information is stored within the application's storage directory (application's document sandbox) (Michael et al., 2013). This data could be audio files from a sleep monitoring application or pictures tracking health progress. Depending on the storage capacity of the mobile device this data can be stored on board the device or an external SD card. This data can be easily accessed, if it is not protected resulting in eavesdropping on unencrypted SD card storage (Zubaydi et al., 2015).

With the rise of consumer health wearables, developers make the applications of wearables free to gain awareness by consumers. To gain revenue from the application developed, mobile developers use advertising supporting software (adware) within the health application (Symantec, 2014). Adware automatically generates random adverts from organizations as a user utilizes the mobile application. Adware is growing at a rapid rate from 65 Ad libraries in 2013 to 88 Ad libraries in 2014 (Symantec, 2014). Unfortunately, adware is capable of collecting device information and location coordinates of an individual. This makes a user vulnerable to consumer generated marketing and furthermore their information becomes susceptible to hackers (Adhikari et al., 2014). For example, an advert for specific a drug could be advertised on a health application. If the user decides to read more about the product information, the drug researched by the consumer is sent to third-party advertisers (Michael et al., 2013; Pittman, 2014).

Mobile devices have grown tremendously with the hardware capabilities they contain. Today, it is norm for a mobile device to contain accelerometers, gyroscopes and GPS sensors. Through, health applications are able to harness computing technologies at their disposal. One of the common, technologies utilized by health applications is the GPS sensor. This sensor is used especially by fitness athletes to identify and track the route utilized exercise. When health applications are paired to the consumer health wearable with Bluetooth, the GPS sensor is used to track the distance and route that an individual travel with. Bluetooth signals contain unique IDs to identify the device is coming from. Through this it makes an individual susceptible to location tracking (Barcena et al., 2014). In the wrong hands this information can be utilized to understand behaviour habits of an individual.

As the associated application of consumer health wearables exist in the sphere of mobile devices, there are common security factors and issues that occur to all mobile applications and cloud servers. The Open Web Application Security Project (OWASP) identified ten top risks that developers should be aware of with the development of mobile applications. OWASP is a non-project organization that is centred on improving the security of software. This organization is centred on researching and documenting, tools and technologies that will assist to protect software (OWASP, 2014). These top mobile risks include the following:

Insecure Data Storage: This is a result of poorly encrypted information, caching information and allowing global permissions. This insecure data storage occurs either internal (on board) or external (to cloud services)

Weak Server-side controls: This occurs on the server side by not implementing proper security controls or configurations. Also disabling unnecessary back-end services.

Insufficient transport-layer protection: This applies to applications that use the HTTP protocol for communication (client-server). HTTPS provides transport layer protection, but if digital certificates are ignored or the use of plain-text communication is enforced. This places the information at risk.

Client-side injection: This for mobile web and hybrid applications. They are susceptible to SQL injections.

Poor authorization and authentication: As compared to web applications, users of mobile applications are not online at all times for authentication. Authentication occurs offline. Poor authorization and applying authentication poorly allows passwords, keys, or session tokens to be exploited.

Improper session handling: Sessions are used as a form of security, to allow a user to perform a specific action for a time period, until they are required to re-authenticate their credentials. This security is enforced by a server issuing a session cookie to a mobile application once a user has successfully authenticated and authorized service requests. Improper session handling occurs when appropriate procedures are not enforced, resulting in session cookies being intercepted by cybercriminals.

Unintended Data Leakage: Operating Systems, digital infrastructure and hardware, are just but the few components within mobile devices that can change with time. Developers are unable to handle these changes outside the bounds of the application. Due to these changes, it is possible for data to be lost. This data loss may occur if a full understanding in not acquired to readjust the application to interact with the changes.

Security Decisions Via Untrusted Inputs: An application may receive data from various sources. This can be achieved in most cases by the Inter Process Communication (IPC) within a mobile application. To reduce any risk, the mobile application should communicate with other trusted applications it interacts with. Furthermore, sensitive tasks should require the application user input.

Lack of Binary Protections: Applications can be reversed engineered at a binary level. This reverse engineering can occur when a programmer was not involved in the development of the application at a binary level. If the application is not protected at this level, and attacker may find flaws and reconfigure the application and re-sell the application as its own.

Broken Cryptography: Encryption is used to protect user data. However, by utilizing outdated algorithms and encryption techniques results in application insecurity.

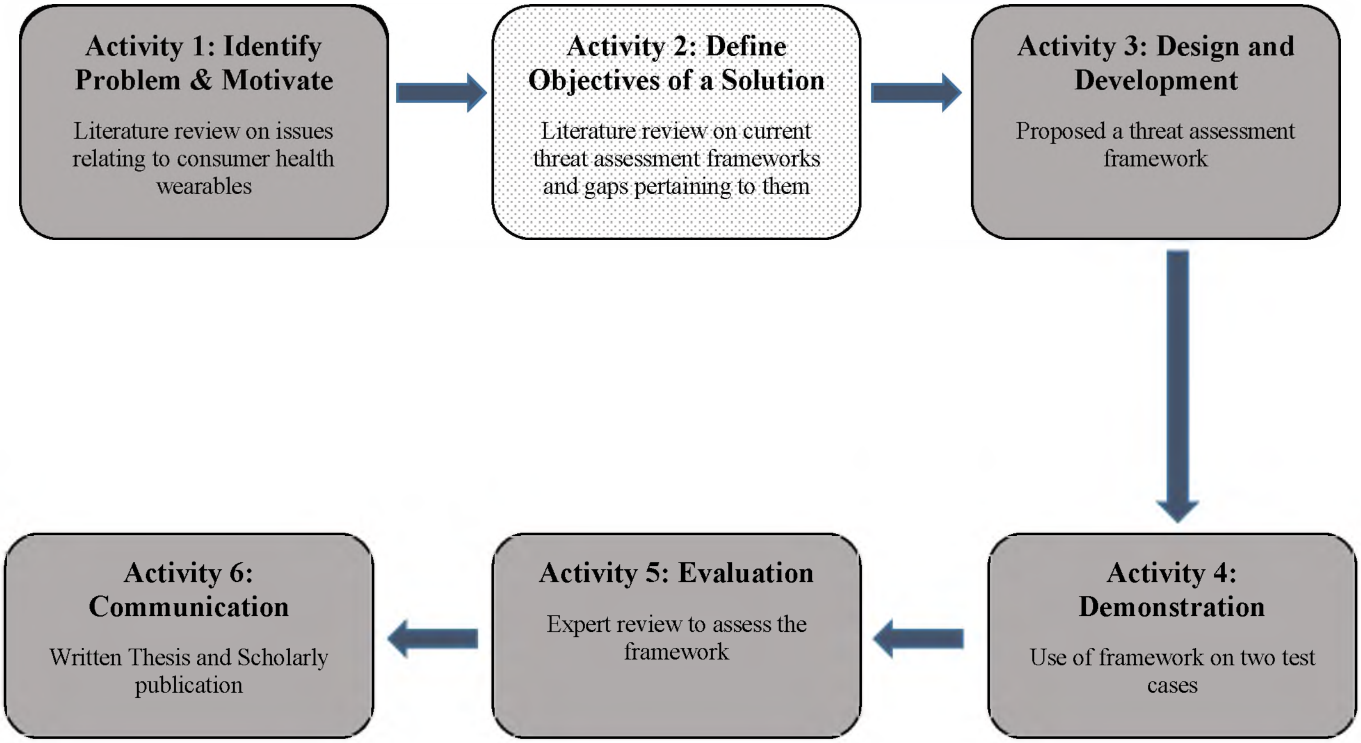
4.4 CONCLUSION

Consumer health wearables are growing and there are tremendous benefits of using such technologies, however there are vulnerabilities in the consumer health wearable ecosystem. Table 4.1 identifies a summary of the key vulnerabilities discovered from the use of consumer health wearables and their associated applications.

Table 4.1: Summary of Vulnerabilities

Vulnerabilities	
Threat Name	***Description***
1. Third Party Analytics	Mobile health applications use analytic tools to assess health data. In the process of communicating to these third party analytical servers, metadata of a user's behaviour and activity is collected (Adhikari et al., 2014; Goyal, Dragoni and Spognardi, 2016).
2. Lack of Access Codes	Many health applications and fitness trackers lack access codes to protect them from being viewed by outside parties. (HP Fortify, 2015; Goyal et al., 2016)
3. Location Tracking	GPS sensors are vulnerable to location tracking due to the unique ID displayed from Bluetooth signals (Barcena et al., 2014; Goyal et al., 2016).
4. Lack of Privacy Policy	Mobile Health applications utilize permissions that require a user's authorization to use the device features. In many cases, health applications lack privacy policies to state how a consumer's data will be utilized and the manner in which it will be collected. (Dinh et al., 2013; Goyal et al., 2016)
5. Insecure Data Storage	This is a result of poorly encrypted information, caching information and allowing global permissions. This insecure data storage occurs either internal (on board) or external (to cloud services) (Al Ameen et al., 2012; Michael et al., 2013; Huckvale et al., 2015; Goyal et al., 2016)
6. Weak Server-side Controls	This occurs on the server side by not implementing proper security controls or configurations. Also disabling unnecessary back-end services. (Symantec, 2014; Adhikari et al., 2014; OWASP, 2014; Huckvale et al., 2015)
7. Insufficient transport-layer protection	This applies to applications that use the HTTP protocol for communication (client-server). HTTPS provides transport layer protection, but if digital certificates are ignored or the use of plain-text communication is enforced. This places the information at risk. (Huckvale et al., 2015)
8. Client-side injection	This threat applies for mobile web and hybrid applications. These types are susceptible to SQL injection (OWASP, 2015; Goyal et al., 2016). SQL injection is a type of attack that uses SQL queries to manipulate a server in the favour of an attacker.
9. Poor authorization and authentication	As compared to websites, users of mobile applications are not online at all times for authentication. Authentication may also occur offline. Poor authorization and applying authentication poorly allows passwords, keys, or session tokens to be exploited (Martínez-Pérez et al., 2015; Goyal et al., 2016).
10. Improper session handling	Sessions are used as a form of security, to allow a user to perform a specific action for a time period, until they are required to re-authenticate their credentials. This security is enforced by a server issuing a session cookie to a mobile application once a user has successfully authenticated and authorized service requests. Improper session handling occurs when inappropriate procedures are not enforced, resulting in a session cookie being intercepted by cybercriminals. (Michael et al., 2013; Barcena et al., 2014; OWASP, 2014; Selinger, 2015)
11. Unintended Data Leakage	Operating Systems, digital infrastructure and hardware are just but the few components within mobile devices that can change with time. Developers are unable to handle these changes outside the bounds of the application. Due to these changes, it is possible for data to be lost. This data loss may occur if a full understanding in not acquired to readjust the application to interact with the changes (Huckvale et al., 2015; Martínez-Pérez et al., 2015).
12. Security Decisions Via Untrusted Inputs	An application may receive data from various sources. This can be achieved in most cases by the Inter Process Communication (IPC) within a mobile application. To reduce any risk, the mobile application should communicate with other trusted applications it interacts with. Furthermore, sensitive tasks should require the application user input (OWASP, 2014).
13. Lack of Binary Protections	Applications can be reversed engineered at a binary level. This reverse engineering can occur when a programmer was not involved in the development of the application at a binary level. If the application is not protected at this level, and attacker may find flaws and reconfigure the application and re-sell the application as its own (OWASP, 2014).
14. Broken Cryptography	Encryption is used to protect user data. However, by utilizing outdated algorithms and encryption techniques results in application insecurity (OWASP, 2014; Martínez-Pérez et al., 2015).

Chapter 5: THEORETICAL THREAT ASSESSMENT FRAMEWORKS



Activity 1: Identify Problem & Motivate

Literature review on issues relating to consumer health wearables

Activity 2: Define Objectives of a Solution

Literature review on current threat assessment frameworks and gaps pertaining to them

Activity 3: Design and Development

Proposed a threat assessment framework

Activity 4: Demonstration

Use of framework on two test cases

Activity 5: Evaluation

Expert review to assess the framework

Activity 6: Communication

Written Thesis and Scholarly publication

5.1 INTRODUCTION

The purpose of this research study is to develop a threat assessment framework that can be used to assess vulnerabilities that relate to consumer health wearables and their associated applications. This chapter will focus on **Activity 2** of Define The Objective Of A Solution through the Design Science Research Process Model by Peffers et al. (2007). Thus far, Chapter 3 and 4 have explored the literature addressesing sub-questions relating to the main research question: '*What are the components of a threat assessment framework for determining privacy and security vulnerabilities in consumer health wearables?*' Chapter 3 answered RQ1 by gaining an understanding of the type health data collected by consumer health wearables and their associated applications. Focusing on how they are used, for what purpose and by whom. It was identified that consumer health wearables pose a great benefit for individuals, specifically by providing user based consumer health data. In addition, the benefit for medical care institutions as it promotes the growth for the patient-physician experience. Nevertheless, one of the greatest challenges facing the growth of this field are the issues of privacy and security. Chapter 4, focused on RQ2 by identifying the vulnerabilities that contribute to consumer health wearables. It began by highlighting the privacy concerns of consumer health wearables. A further discussion was made on the consumer health wearable ecosystem and the privacy and security issues pertaining to this ecosystem. Chapter 4 concluded by identifying fourteen collated vulnerabilities that affect the consumer health wearable ecosystem.

Chapter 5 finalizes on the literature review by answering RQ3: '*What threat assessment components should be incorporated into a threat assessment framework for consumer health wearables?*' This chapter is organized by firstly describing the definition of information security threat assessment models and their use (Section 5.2). Theoretical information security threat assessment frameworks are then identified specifically focusing on four information security threat assessment frameworks. These frameworks are described by discussing their advantages, disadvantages and their applicability for consumer health wearables and their associated applications. Chapter 5 concludes by summarizing the key components extrapolated from these existing theoretical frameworks of which will be applicable to consumer health wearables.

5.2 THREAT ASSESSMENT FRAMEWORKS

Security professionals need to be able to protect systems and software from intruders to ensure that the program does not encounter plausible damages that may affect the confidentiality, availability and integrity of the application. Vulnerabilities may exist in different parts of a system and it is imperative to be conscious of these vulnerabilities so they not are exploited by attackers. Without understanding the sources of potential vulnerabilities, security professional may result in protecting system resources poorly (Jouini, Rabai and Aissa, 2014). Within the domain of information security there are a variety of dimensions it encompasses. To mention a few: policy dimension, best practice dimension, the insurance dimension, technical dimension, strategic/corporate governance dimension and the audit dimension (von Solms, 2001). All of these measures have been developed to help create a secure environment within information technology.

The international standards for information security include COBIT (Control Objectives for Information and Related Technology), NIST (The National Institute of Standards and Standards) and ISO. All of these organizations provide standards and guidelines for the proper adherence to information security. However, these organizations provide policies, guidelines and guidance to organizations at a high-level. The latest version of CORBIT (CORBIT 5) specifically focuses on audit and assurance, audit and assurance, risk management, information security, regulatory and compliance and governance of enterprise IT (ISACA, 2015). Nonetheless, these measures do not address the concerns of the of consumer health wearables to understand the vulnerabilities that affect them. CORBIT 5 aids large corporations for the adherence to best practices. NIST SP 1800 (Cyber security practice guides) provides a framework to guide organizations on the manner to which the internal systems are secure. This framework however, is suited for CIO's (chief security officers) and board of directors and not for low level for the software developers to assess applications (Mell et al., 2011; Jackson, 2014). ISO 27799 is an information security framework specifically for healthcare organisations. This framework assists to guide the proper adherence of medical information. Nonetheless, the components of this framework are applicable for mobile health devices in a clinical settings and negates much of mobile devices pertaining to consumer health wearables (ISO/IEC 27002, 2005; Siponen and Willison, 2009)

It is for this reason, theoretical threat assessments frameworks were created to assist security professionals in having a guiding tool to understand the source of threats and create a starting point to formulate a solution to counter the threat. Threat assessment models are also not only used to assist to identity and categorize threats. They can also be used to showcase the ideal state for a secure system.

There is an array of different theoretical threat assessment frameworks available for use by information security personnel of which are applicable for different contexts. Jouini, Rabai and Aissa (2014) classify threat assessment framework into two groups; classification methods which are based on attack techniques and classification methods which are based on threat impacts. Classification frameworks that focus on attack based techniques assist security professionals to classify threats based on the attack category. Threat impact classification frameworks assist by classifying threats and understanding the impact that the threat may pose to an application. Four threat assessment frameworks will be discussed that fall within these two categories. *The Three Orthogonal Dimensional Model* and the *Information System Security Threat Cube Classification model* both focus on attack based threats. *Microsoft STRIDE* and the *CIA Triad* are based on threat impacts. These frameworks were chosen as they provide an understanding of the manner to which vulnerabilities can be assessed towards consumer health wearables and their associated applications. This will further provide a perspective from both the attack perspective and threat based perspective. Each of these frameworks are discussed by highlighting their advantages, disadvantages and their applicability towards the consumer health wearable ecosystem.

5.3 ATTACK THREAT MODELS

5.3.1 The Three Orthogonal Dimensional Model

The Three Orthogonal Dimensional Model is a threat assessment model proposed by Ruf et al., (2008) that focuses on attack based threats. This model describes that threats occur through different dimensions. It is for this that it is important to identify threats through multilateral aspects from which a threat may occur. The Three Orthogonal Dimensional Model is used to view top level threats from three perspectives, threat agent, threat motivation and threat localization (Figure 5.1). The first dimension is the Threat Agent which is an actor that imposes the threat to an asset, which can be any valuable artifact to the application (Ruf et al., 2008). There are three different actors described that may pose as threat agents; human, technological and force majeure. Human agents are persons that pose a threat. These could be users, attackers, communities or governments. Technological agents are threats caused by physical or chemical processes with the material. Finally, Force Majeure agents are environmental threats such as earthquakes.

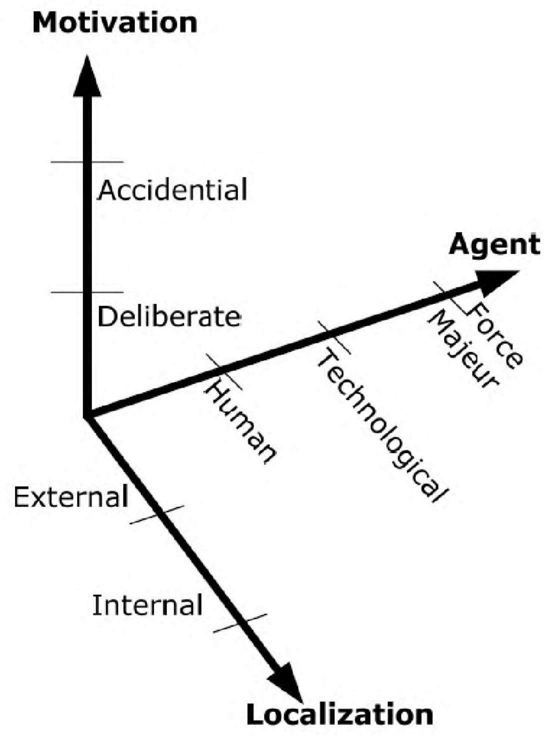


Figure 5.1: The Three Orthogonal Dimensional Model (Ruf et al., 2008)

The second dimension of the model focuses on Threat Motivation. This dimension categorizes threats on the motivation of the threat, whether the cause of the threat was *accidental* or *deliberate*. This dimension focuses on categorizing threats by understanding why the threat agent is motivated to produce a threat (Ruf et al., 2008). The third dimension focuses on Threat Localization. Threats are categorized in this dimension by understanding their origin. The origin of the threat may occur *internally* or *externally.* Threat localization focuses on understanding where the threat agent may threaten an asset (Ruf et al., 2008).

The three orthogonal dimensional model allows security professionals to have a high level broad understanding of the threats that may affect a system and categorizing threats within these dimensions. The core purpose is to fully understand the nature of threats. The work of Ruf et al.,

(2008) sets to understand the nature of threats by the three viewpoints mentioned; the who, the why and the where. This outlook is one of the key advantages of the framework as it provides a high-level understanding of the motivation of an attack on a system (Kamatchi and Ambekar, 2016).

In relation to the consumer health wearable ecosystem, a security professional may identify one of the threats as client-side injection. Client-side injection is executing malicious code on the client side which is in this case the mobile device through the mobile health application. Using the three orthogonal dimensional model, the principle threat agent that may desire to use client side injection towards the mobile health application is a *human*. The threat attack motivation is *deliberate* as client-side injection is used as form to manipulate data on a device or obtain the data. The threat can be located both *internally* and *externally*. Through this information a security professional may understand the actors involved who may affect a system based on a particular threat. Whether it is a deliberate action and the area the threat may occur. This information provides a starting point to create counter measures for the attack. This is the power of the three orthogonal model, it provides the who, the why and where of a particular threat. However, a criticism of this model is that it is high level and is suitable for more experienced professionals who have a broad understanding of the threats that may affect a system. For novice security professionals, they may not fully understand the starting point to protect a system based on this model. Particularly for the consumer health wearable ecosystem which is a growing field that requires a greater understanding of the threats that pertain to this environment (Huckvale et al., 2015).

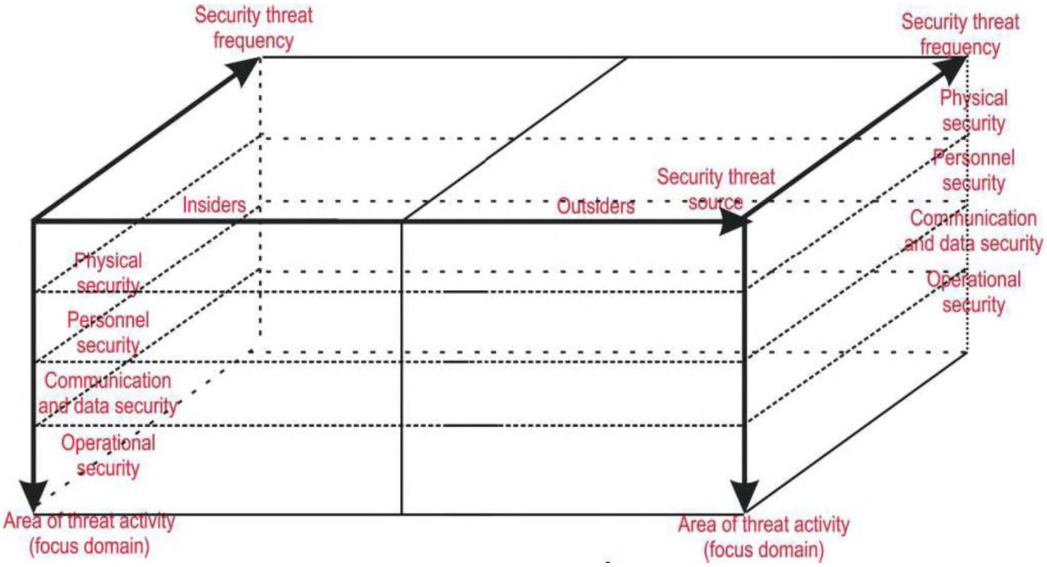
5.3.2 Information System Security Threat Cube Classification

The Information System Security Threat Cube Classification also known as the C^3 Model was developed by Geric and Zejko (2007). This security threat assessment focuses on three factors; security threat frequency, area or focus domain of the security threat activity and finally the security threat source (Figure 5.2)

1. Security Threat Frequency: This branch focuses on the frequency of the security threat occurrence on a continuum.
2. Area (or focus domain) of security threat activity: This category identifies the domain of the security threat on which part of the system it may occur. The C^3 Model provides a pre-

defined category of threats that may fall within this classification. These include, *physical security, personnel security, communication and data security and operational security.*

3. Security threat source: This category describes that security threats may occur from two pre-defined categories, *insiders* and *outsiders.* Insiders are persons authorized to use the system such as employees. Outsiders are unauthorized individuals such as an attacker of the system.



Security threat frequency
Security threat frequency
Physical security
Personnel security
Communication and data security
Operational security
Security threat source
Insiders
Outsiders
Physical security
Personnel security
Communication and data security
Operational security
Area of threat activity (focus domain)
Area of threat activity (focus domain)

Figure 5.2: Information System Security Threat Cube Classification (Geric and Zejko, 2007)

The core purpose of the C³ Model is to understand the frequency of a threat. As compared to Three Orthogonal Dimensional which focuses on motivation, the C³ Model focuses on how frequent a threat may occur within a specific domain of a system and the threat source in that domain. By understanding how frequent an attack may occur on a particular domain of the system assists to identity the weak areas of an application for an intruder to exploit it.

One of the key areas of which threats may occur with consumer health wearables is on the *communication and data security domain* as described in the C³ Model. This is so as wearables devices are heavily reliant on communication protocols for processing and analyzing data. The C³ Model can be utilized as a tool to categorize threats and identify how frequent threats can occur on a particular domain. Similar to the Three Orthogonal Model, the C³ Model is also high level.

Security professionals or developers will need to have an in depth understanding of a threat and the frequency in which the attack may occur based on the architecture of the application. This a specialized knowledge base which will require persons to have experience with the domain.

5.4 Threat Impact Models

5.4.1 Microsoft STRIDE Threat Assessment Framework

STRIDE is a classification technique used to understand the kind of exploit that can occur to a system (Microsoft, 2005). Microsoft STRIDE Threat Assessment Framework is described as a classification framework that focuses on threat impact. STRIDE is an acronym for *Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege*. Threats are first classified with these six categories of the framework and further weighted to identify their impact based on their categories. In addition, the Microsoft STRIDE Threat Assessment Framework helps to understand threats from the attacker perspective. The goal of STRIDE is to help identify attacks and classify them under each of the different exploits that may occur (Shostack, 2014).

1. Spoofing: Spoofing can be described as a manner in which an attacker pretends or poses to be something or someone else. The main objective of spoofing is to gain access to the system by creating a false identify (for example, falsely creating a user profile). Countermeasures against spoofing include using strong authentication, not passing credentials in plain text and protecting authentication cookies.
2. Tampering: This is unauthorized modification of data as it is being sent within the communication channel. Countermeasures against tampering include; using data hashing, digital signatures, strong authentication and secure communication links.
3. Repudiation: This focuses on audit trails and access logs. Ensuring that there is a track record of transactions that a user perform. This provides accountability that user performed legitimate actions or transactions. Countermeasures against repudiation include using secure audit trails and digital signatures.
4. Information Disclosure: This is unwanted disclosure of private data. This can occur if few encryption structures are in place. This can occur if information is sent in plain text over a network. Countermeasures against information disclosure include, using strong encryption

and authorization, not storing private information in plain text and using secure communication channels.

5. Denial of Service: This a way in which an attacker makes an application or system unavailable for service. Countermeasures against denial of service include validating and filter input.
6. Elevation of Privilege: Different users have different privileges and access to an application. One user may have greater access to an application as to that of another one. Elevation of privilege occurs when an attacker with limited access, elevates him/herself to gain greater access to comprise the system. Countermeasures against elevation of privilege include; “following the principle of least privilege and use least privileged service accounts to run processes and access resources

The main goal of Microsoft’s STRIDE Threat Assessment Framework is to understand the threats pertaining to a specific application and then further classifying threats under each of the six categories based on how they can occur in an application (Microsoft, 2005). For example, with regards to the consumer health wearable ecosystem which are threats that pertain to spoofing the health application. This process will be conducted for each of the categories of STRIDE until a full list detailing all the threats pertaining to the application a collated. Once this documentation is complete, threats are ranked based on their impact, degree of mitigation and ease of exploitation.

Microsoft’s STRIDE framework is a structured framework as it provides users the key factors that may affect an application; spoofing, tampering, repudiation, denial of service and elevation of privilege. This gives developers and security professional a guiding instrument of the core factors that are needed to be cautious of with the set application. When compared to the Three Orthogonal Dimensional Model which focuses on the nature of threats and the C^3 Model which focuses on the frequency of threats based on a particular domain, STRIDE aims to identify the potential attackers within six categories. Although, this is beneficial this approach limits the perspective of security professional to focus on threats on six main categories. With the constant change of technology, it may limit individuals to identify threats from other potential avenues.

5.4.2 CIA Triad

The CIA triad is at times referred to by researchers as the heart of information security (Feruza and Kim, 2007). The CIA is an acronym that stands for confidentiality, integrity and availability.

This triad has been used for different context within information security such as setting security goals, or the building blocks for information security. The CIA triad can also be used as a threat assessment tool to classify threats within each of the components of the three components. These three components can be described as follows.

1. Confidentiality: can be described as the form of keeping information secure so that it is not disclosed to unwanted individuals. Confidentiality also focuses on the obligation on individuals that once the information has been received, the intended party has an obligation to ensure that it not disclosed to unwarranted individuals.
2. Integrity: ensures to enforce the authenticity of information. When information is being stored, transformed or in transit it is important to ensure that the data is complete and accurate. The key focus of integrity is guaranteeing that information is not modified unless specified by intended parties.
3. Availability: focuses on warranting that information is accessible to intended parties when required. Availability is very important as any disruptions can result in denial of service attacks that can hinder key functionality of a system.

The CIA triad is viewed as the heart of information security as it enforces the relationship between security and privacy (Feruza et al., 2007). Data privacy is the relationship between technology and the legal practices enforced to ensure that data is properly collected, stored and shared within the technological sphere. The CIA triad extends the classification mechanism by not only identifying the threats that may affect confidentiality, integrity and availability, but also seeks to understand how confidentiality, integrity and availability can be hampered towards the users of the application in terms of privacy. With regards to the consumer health ecosystem, one of the threats that may affect this ecosystem is improper session handling. Improper session handling can occur, by not generating new session tokens for users. If a session token is obtained by an intruder, it can be used to impersonate a user and view confidential information. Furthermore, user details can be changed or deleted affecting the availability and integrity of consumer health data. This threat therefore affects confidentiality, integrity and availability and by using the CIA Triad framework gains a further insight of how a user's privacy is hampered based on threat.

This is one of the key advantages of the CIA Triad as compared to the other outlined frameworks. It provides insight of the relationship between data privacy and security. However, researchers have also described that some of the challenges of the CIA triad is its limitation of scope to information security. This framework neglects to focus on elements such as authentication, authorization, and elevation of privilege. Like Microsoft's STRIDE framework it only allows security experts to focus on three domains of security.

5.5 KEY COMPONENTS FOR A CONCEPTUAL FRAMEWORK

The key focus of this chapter is answering RQ3: *Which threat assessment components should be incorporated for assessing the security risk of consumer health wearables?* Up till now, existing theoretical frameworks have been outlined, each having a purpose that can be utilised for threat assessment. Each of these frameworks have advantages and disadvantages for their applicability towards consumer health wearables. However, they do not fully meet the main purpose of this research of a threat assessment framework to be used to assess the vulnerabilities towards consumer health wearables. Nonetheless, each of the frameworks contain components that can be incorporated for a threat assessment framework for consumer health wearables. The work of Abomhara and Koien (2015) identifies eight unique questions that are tailored for identifying threats and system vulnerabilities. These questions are geared to help determine if a security solution is secure against threats (Abomhara et al., 2015). These questions are the following;

1. What are the assets
   - ➢ This question focuses on identifying the assets of the system. In terms of privacy and security it is critical to identify the valuable components of the application that an attacker may desire to exploit.
2. Who are the principal entities?
   - ➢ This question focuses on the actors who are involved with interacting with the system. These could be persons or other systems interacting with the application.
3. What are the threats?
   - ➢ This questions focuses on identify the possible threats that may affect the application.
4. Who are the threat actors?
   - ➢ These are actors that pose as threats towards the application. Different types of threat actors may include people, other systems, governments or technological factors.

5. What capability and resource levels do threat actors have?
   - ➢ Based on the threat actors, a review is made on the resources and restrictions the actors have towards the system for exploitation.
6. Which threats can affect what assets?
   - ➢ Threat are classified to see the manner which they affect assets.
7. Is the current design protected against threats?
   - ➢ Once question 1- 6 have been answered, this question focuses on identifying and reviewing how the current design is protected or vulnerable to threats identified.
8. What security mechanisms should be used against threats?
   - ➢ This focuses on creating counter measures and steps to counter the threats.

As described these questions provide a guiding tool to understand threats and their attributes pertaining to a particular application environment. This achieved by understanding the assets, the users of the application, the threats affecting the assets, the agents creating the threats, and counter measures to be used to counter the threats. This guideline can be applied for consumer health wearables. As the main goal of this research is to understand how consumer health wearables and their associated application can be better protected with the use of a threat assessment framework. Researchers describe, that threat assessment frameworks can be used to understand potential threats of an application and provide measure for security (Jouini et al., 2014). Therefore, in the process of identifying the components that are needed for assessing the security consumer health wearables. These eight questions provide guidance for this process and have been adapted to identify the necessary components for a threat assessment framework for consumer health wearables.

1. Does the framework assist to identify the assets for Consumer Health Wearables?
2. Does the framework assist to identify the principle entities for Consumer Health Wearables?
3. Does the framework assist to identify threats for Consumer Health Wearables?
4. Does the framework assist to identify the threat actors affecting Consumer Health Wearables?
5. Does the framework identify the capability and resource levels the threat actors have towards Consumer Health wearables?

6. Does the framework classify the threats based on assets they affect towards Consumer Health Wearables?
7. Does the threat assessment framework design provide sufficient protection against threats towards Consumer Health wearables?
8. Does the framework provide security mechanisms or guidelines to be used against the threats affecting Consumer Health wearables?

These eight adapted questions are used to evaluate the existing theoretical frameworks described within this chapter. Through this evaluation, an understanding can firstly be obtained to view the manner in which existing theoretical frameworks address in assisting to better protect consumer health framework. In addition, this evaluation will help to identify gaps in which the desired framework can be produced to better protect consumer health wearables (Table 5.1).

Table 5.1: Assessment of Theoretical Threat Assessment Frameworks

Framework	Questions							
	1	*2*	*3*	*4*	*5*	*6*	*7*	*8*
The Three Orthogonal Dimensional Model	No	No	Focuses on Localization: Internal and External	Yes: Human, Technological, Force Majeure	Focuses on motivation: Accidental and Deliberate	No	Insufficient	No
C³ Model	No	No	Focuses on Localization: Physical security, personnel security, communication and data security and operational security	Yes: Insiders and Outsiders	Focuses on the threat frequency	No	Insufficient	No
Microsoft STRIDE	No	No	Yes: Six types of threats described; spoofing, tampering, repudiation, information disclosure, elevation of privilege	No	No	No	Moderate	No
CIA TRIAD	No	No	Yes: Three types of threats described; confidentiality, integrity, availability	No	No	No	Moderate	No

Question 1: It was identified that none of the existing frameworks help to identify the assets towards consumer health wearables. However, from the literature review outlined in chapter 3 it can be described that main asset to be protected within consumer health wearables is the consumer health data stored or processed within these devices.

Question 2: None of the frameworks helps to explicitly identify the key users of consumer health wearables and their associated devices. Key users identified from literature are described as consumers (Chapter 3). Of which a consumer is described as a person who is not medical professional but is knowledge seeking for the embetterment of their physical wellbeing.

Question 3: Each of the theoretical frameworks helps to assist to identify threats pertaining to consumer heath wearables in their unique way. The Three Orthogonal Dimensional Model focuses on identifying threats on their localization either internally or externally. The C^3 Model helps to identify threats on their threat source from either physical security, personnel security, communication and data security and operational security. Microsoft STRIDE helps to identify threats by using six categories of attacks; spoofing, tampering, repudiation, information disclosure, elevation of privilege. Finally, CIA triad helps to identify threats by using three categories; confidentiality, integrity and availability.

Question 4: Only the Three Orthogonal Dimensional Model and the C^3 Model assist to identify threat actors. The Three Orthogonal Dimensional Model identifies three actors; human, technological and force majeur. Whereas the C^3 Model identifies two actors; insiders and outsiders.

Question 5: Only the Three Orthogonal Dimensional Model and the C^3 Model assist to identify the capability and resource levels of the actors. Both of the frameworks however, take a high level approach towards this. The Three Orthogonal Dimensional Model focus on the capability as either accidental or deliberate. Whereas, the C^3 Model focuses the frequency of the capability.

Question 6: Although each of the frameworks classify threats in their unique way. None of the frameworks classify threats that affect the assets towards consumer health wearables.

Question 7: The Three Orthogonal Dimensional Model and the C^3 Model were deemed to have insufficient protection against threats towards consumer health wearables as they are viewed to be high level threat assessment frameworks. This is so, as literature describes that consumer health is still a growing field and greater guidance is needed within this arena. These two specific framework therefore provide limited guidance towards. On the other hand, Microsoft STRIDE and the CIA triad were viewed to have moderate protection as they provide a starting to point to identify threats based on their criteria. However, limited knowledge in security may result in novice individuals to not understand the threats that may pertain to the criteria outlined within these frameworks.

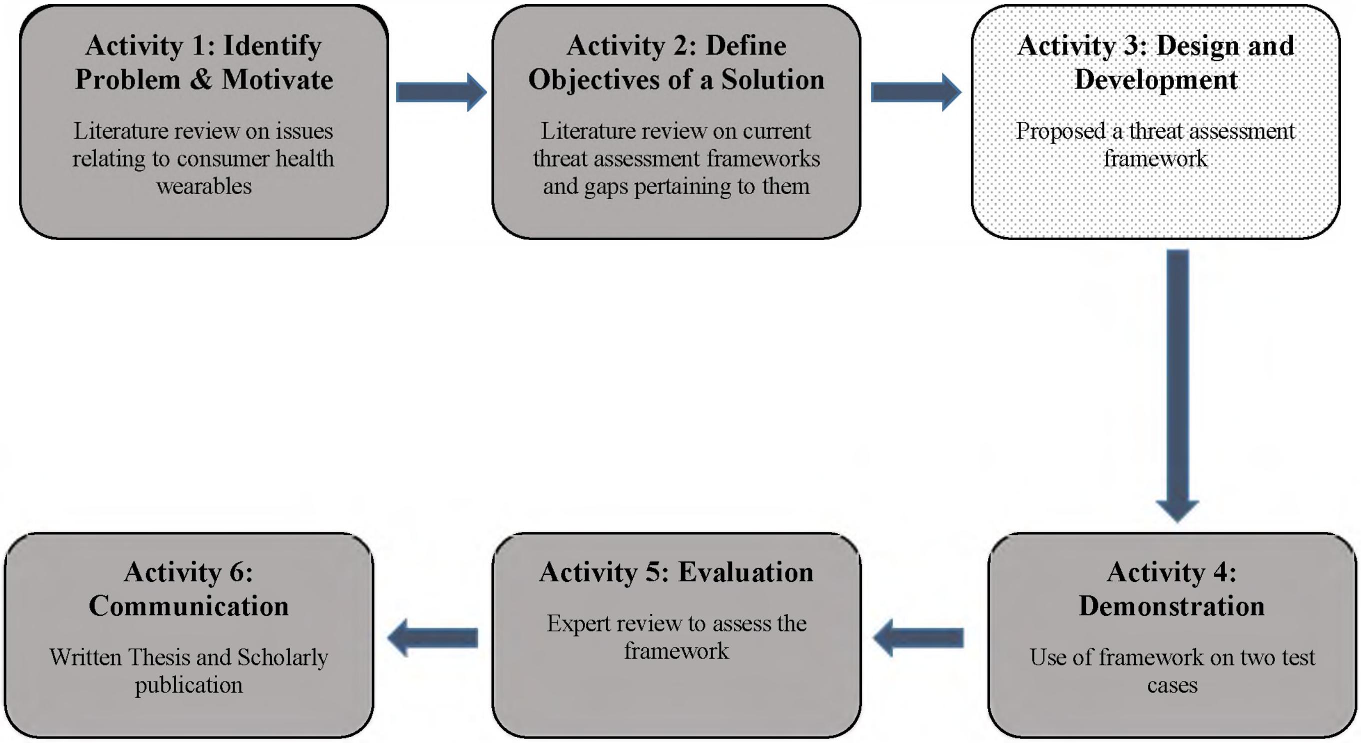
Question 8: None of the frameworks provide guidelines or security mechanism to help assist to counter the threats affecting consumer health wearables.

Based on these findings it can be deemed that existing theoretical threat assessments provide moderate protection that be used to better protect consumer health wearables. However, there are gaps within these frameworks. It is therefore vital to propose a elements that can be used to better protect consumer health wearables. Chapter 6 will focus and highlight a proposed threat assessment framework for consumer health wearables based on the gaps identified from Table 5.1.

5.6 CONCLUSION

This chapter sought to discover threat assessment components that would be needed to be incorporated for assessing the security risk of consumer health wearables. To achieve this, existing theoretical frameworks were discussed, by outlining their advantages, disadvantages and their applicability for consumer health wearables. It was further discovered that each these framework has drawback limiting the protecting of consumer health wearables. Eight questions were finally utilized to discover the elements need to better protect consumer health wearables.

Chapter 6: CONSUMER HEALTH WEARABLE THREAT ASSESSMENT FRAMEWORK



Activity 1: Identify Problem & Motivate

Literature review on issues relating to consumer health wearables

Activity 2: Define Objectives of a Solution

Literature review on current threat assessment frameworks and gaps pertaining to them

Activity 3: Design and Development

Proposed a threat assessment framework

Activity 4: Demonstration

Use of framework on two test cases

Activity 5: Evaluation

Expert review to assess the framework

Activity 6: Communication

Written Thesis and Scholarly publication

6.1 INTRODUCTION

This research aims to create a threat assessment framework that can be used to assess potential vulnerabilities that affect consumer health wearables and their associated applications. The Design Science Research Process Model by Peffers et al. (2007) has been the overarching methodology used to reach towards this goal. This chapter will focus on **Activity 3** of Design and Development of the research artefact.

Up until this point, an understanding of the research environment has been assessed by existing literature to understand the problem and define the objectives of a solution. Chapter 3 focused on understanding the health data collected by consumer health wearables and how it is stored. This chapter concluded by identifying there is a great need for consumer health wearables and their associated devices specifically towards growing the patient-physician experience. Nonetheless, one of the greatest challenges facing this environment are the issues of privacy and security towards consumer health data. Chapter 4 continued to identify the problem by highlighting the consumer health wearable ecosystem and the security vulnerabilities relating to this ecosystem. Fourteen collated potential security issues were identified that affect consumer health wearables and their associated applications. Chapter 5 then focused on the process of defining the objectives of a solution by identifying the components needed to be incorporated for assessing the security threats of consumer health wearables. Through this, the manner in which vulnerabilities pertaining to consumer health wearables can be better identified and assessed. This was attained by firstly understanding existing theoretical threat assessment frameworks by identifying their advantages, disadvantages and their applicability towards consumer health data. Within this process, there were gaps established within these frameworks that did not assist to fully help to assess consumer health wearables. Chapter 5 concluded by identifying a set of components needed to be established to produce a threat assessment framework for consumer health wearables and their associated applications. This chapter, continues from Chapter 5 and aims to Design and Develop a threat assessment framework based on the gaps identified in Chapter 5 and the knowledge attained from Chapter 3 and 4.

This Chapter will therefore be organised by describing the formation for a threat assessment framework (Section 6.2). This will include the components required for the framework, and how they were formed within the Consumer Health Wearable Threat Assessment Framework. The developed framework will further be described (Section 6.3) with an outline of vulnerability criteria. A final conclusion will be presented (Section 6.4) on how the theorized threat assessment framework meets the objective of the research.

6.2 FORMATION OF FRAMEWORK

The main aim of this research project is to formulate a threat assessment framework that can be used to assesses and understand which vulnerabilities pertain to consumer health wearables and their associated applications. Chapter 5 identified a set of questions by Abomhara and Koien (2015) that are tailored for identifying threats and system vulnerabilities. Within chapter 5 these eight questions were adapted and utilized to evaluate existing theoretical frameworks and identify the gaps in which they lacked applicability towards consumer health wearables. The gaps that were identified included:

a) Being unable to identify the assets for consumer health wearables
b) Being unable to identify the principal entities for consumer health wearables
c) Being unable to identify threat actors affecting consumer health wearables
d) Being unable to identify the capability and resource levels the threat actors have towards consumer health wearables
e) Not classifying the threats based on the assets that affect consumer health wearables.

From these gaps, the formation of the Consumer Health Wearable Threat Assessment Framework was developed through this.

6.2.1 Consumer Factors

Chapter 5 described different theoretical threat assessment frameworks of which are generic and cater for different assets within a specifc context. This research on the other hand narrows on consumer health wearables specifically on creating a threat assessment for this environment. ISO/IEC 27002 (2005) defines an asset as any valuable object to an organization. This object can be tangible like hardware or intangible like information, software or the reputation of an organization. In light of consumer health wearables, the term asset can differ depending on the whether the asset is viewed from the perspective of the organization or the perspective of the user of the product. An asset within an organizational context can be the actual physical device of a consumer health wearable. Whereas for a user of the product the asset can be the consumer health data stored within a health application. There is an array of different assets for computer health wearables such as computing devices, infrastructure, services, or telecommunication systems. However, the literature has outlined (Chapter 3 and 4) that one of the major assets affected with consumer health wearables and their associated applications is consumer health data (Ahmed and Ahamad, 2012; La Polla, Martinelli and Sgandurra, 2013). This is so, as consumer health data is the principal agent consumers used to improve their physical wellness (Lewis et al., 2010). In addition, it is the main objective for which organizations produce consumer health wearables. So as, consumer health data can be used for storage, accessibility, management and analysis of their target market.

In light of a threat assessment framework, it is vital to define the factors within the asset of consumer health data that makes its important. Through this may an understanding of the vulnerabilities that affect this asset can be reviewed. It is described that for the protection of an asset, there needs to be protection against illicit access, use, disclosure, alteration, destruction or theft of information (von Solms, 2001). These factors of protection speak of different facets within the asset of consumer health data that can prone to threats. Based from the CIA Triad and Microsoft STRIDE Threat Assessment Framework, the key elements used to protect assets are Authentication, Authorization, Availability, Confidentiality, Non-Repudiation and Integrity (Microsoft, 2005; Feruza et al., 2007). These elements all aid in the protection of consumer health data.

1. **Authentication:** As consumer health data is accessed, managed or viewed there needs to be authentication procedures of identifying a user. This is to ensure that the correct user is viewing the correct data.
2. **Authorization:** As consumer health data is accessed, managed or viewed there needs to be authorization methods. Authorization differs to authentication as it identifies whether a user has appropriate rights to access a resource. This ensures that a low level user does not have admin rights.
3. **Availability:** Consumer health data needs to be available to authorized users when requested. An authorized user should have the freedom to view their data when they desire.

4. **Confidentiality:** As consumer health data is central to consumer health wearables. It is vital to keep this data secure and only revealing it to intended parties.
5. **Non-repudiation:** The assurance that someone cannot deny something (digital signature, time stamps, certificates). This is vital when updates are made. There needs to be assurance that any changes to software or hardware firmware is from the manufacturer.
6. **Integrity:** When consumer health data is accessed or managed there is need to be assurance that it is not modified in transit or at rest. In case data is tampered, it can be identified.

These six elements are described as Consumer Factors as they each form as part of a segment of the asset of consumer health data. It can also be identified that these factors are similar and parallel to that of the CIA Triad and Microsoft STRIDE Threat Assessment Framework. As compared to the CIA Triad and Microsoft STRIDE Threat Assessment Framework, are user needed to infer how the vulnerabilities described in the frameworks affected the assets. These six elements on the other hand speak and are the core factors to the asset of consumer health data. This is so, due to the high level ecosystem of consumer health wearables described in Chapter 4. Within Chapter 4 it was described that consumer health data exists in different forms as the data is accessed, managed or viewed by consumers with the use of consumer health wearables and their associated applications. When consumer health data is collected by the wearable device, there needs to be **authentication** and **authorization** mechanisms to determine that the consumer health data is being sent to a correct paired device and synced to the correct user. When a user desires to view their consumer health data, it needs to be **available**. In addition, the information needs to be **confidential** and only viewed to intended parties. When periodic updates are made to a wearable device there needs to be assurance (**non-repudiation**) that it was sent by the manufacture and not by a malicious attacker. Finally, there needs to be **integrity** of the consumer health data that it cannot be modified in transit or at rest. The representation of these consumer factors can be viewed in Figure 6.1. These elements are deemed as assets towards consumer health wearables and their associated applications as they need to exist when the principle agent who is the consumer interacts with the device.

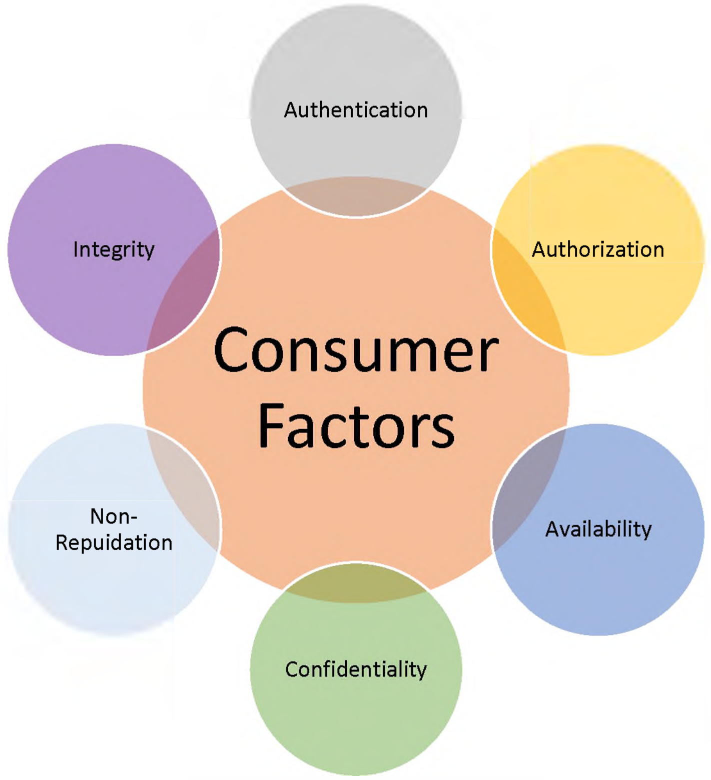


Figure 6.1: Consumer Factors

6.2.2 Vulnerabilities towards Consumer Health Wearables

Systems are prone to attackers attempting to intrude the particular environment and attain the valuables of the organization (von Solms and van Niekerk, 2013). It is for this nature that security mechanisms are created to protect systems against intruders. From identifying the assets of consumer health wearables the next phase of the process of developing the framework includes identifying the vulnerabilities that may affect consumer health wearables and theirs associated applications. Chapter 4 conducted a literature study on the threats that have been identified by literature. In addition, threats that were identified by OWASP Top 10 mobile threats were also listed in chapter 4. Fourteen vulnerabilities were outlined that pertain to consumer health wearables and their associated applications. Vulnerabilities which were similar to OWASP Top were grouped within the similar heading to ensure consistency.

1. **Third Party Analytics:** Mobile health applications use analytic tools to assess health data. In the process of communicating to these third party analytical servers, metadata of a user's behavior and activity is collected (Adhikari et al., 2014; Goyal et al., 2016).

2. **Lack of Access Codes:** Many health applications and fitness trackers lack access codes to protect them from being viewed by outside parties. (HP Fortify, 2015; Goyal et al., 2016)

3. **Location Tracking:** GPS sensors are vulnerable to location tracking due to the unique ID displayed from Bluetooth signals (Barcena et al., 2014; Goyal et al., 2016).

4. **Lack of privacy policy:** Mobile Health applications utilize permissions that require a user's authorization to use the device features. In many cases, health applications lack privacy policies to state how a consumer's data will be utilized and the manner in which it will be collected. (Dinh et al., 2013; Goyal et al., 2016)

5. **Insecure Data Storage:** This is a result of poorly encrypted information, caching information and allowing global permissions. This insecure data storage occurs either internal (on board) or external (to cloud services) (Al Ameen et al., 2012; Michael et al., 2013; Huckvale et al., 2015; Goyal et al., 2016)

6. **Weak Server Side Controls:** This occurs on the server side by not implementing proper security controls or configurations. Also disabling unnecessary back-end services. (Symantec, 2014; Adhikari et al., 2014; OWASP, 2014; Huckvale et al., 2015)

7. **Insufficient transport-layer protection:** This applies to applications that use the HTTP protocol for communication (client-server). HTTPS provides transport layer protection, but if digital certificates are ignored or the use of plain-text communication is enforced. This places the information at risk. (Huckvale et al., 2015)

8. **Client-side injection:** This threat applies for mobile web and hybrid applications. These types are susceptible to SQL injection (OWASP, 2015; Goyal et al., 2016). SQL injection is a type of attack that uses SQL queries to manipulate a server in the favor of an attacker.

9. **Poor authorization and authentication:** As compared to websites, users of mobile applications are not online at all times for authentication. Authentication may also occur

offline. Poor authorization and applying authentication poorly allows passwords, keys, or session tokens to be exploited (Martínez-Pérez et al., 2015; Goyal et al., 2016).

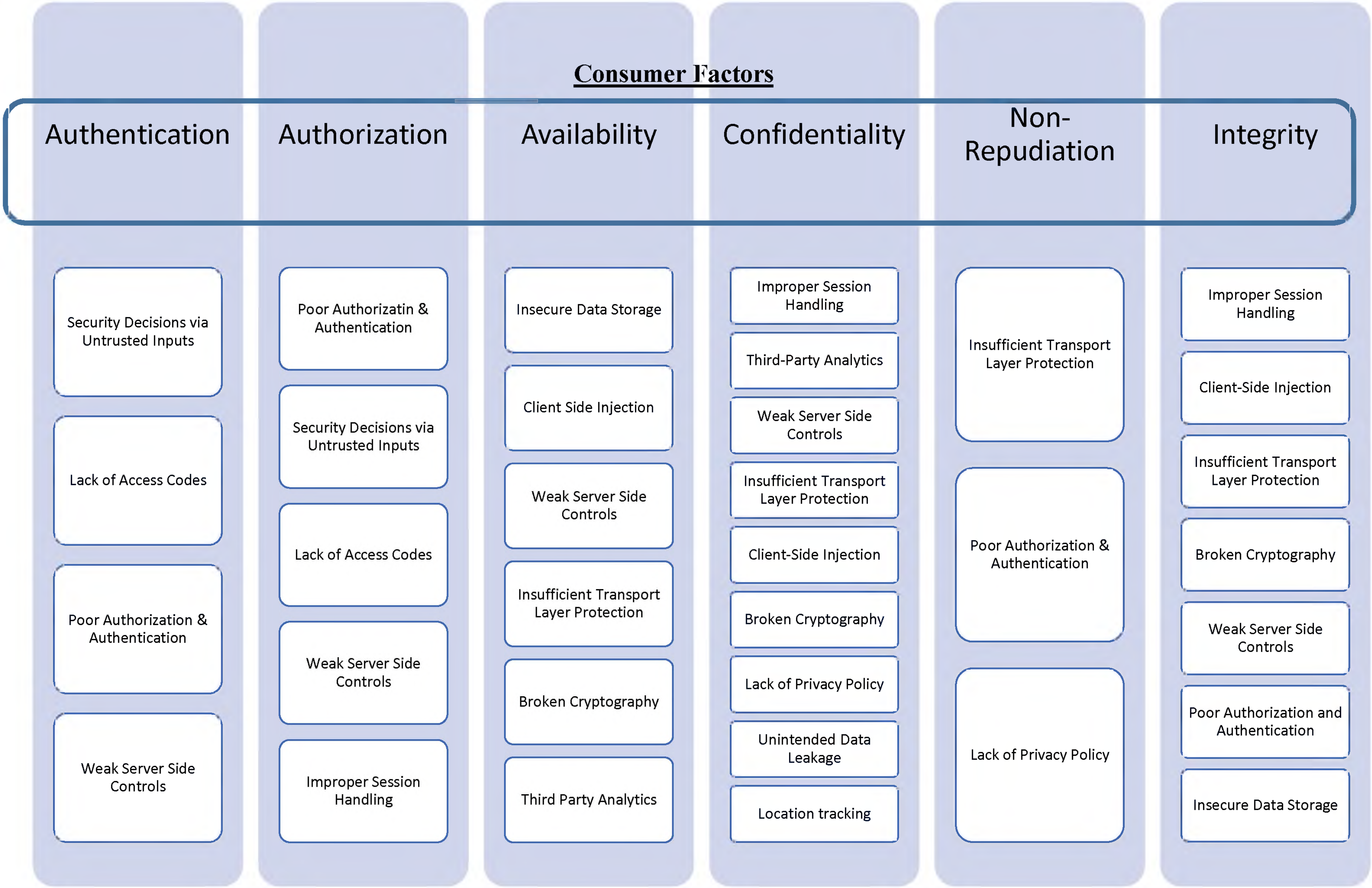
10. **Improper session handling:** Sessions are used as a form of security, to allow a user to perform a specific action for a time period, until they are required to re-authenticate their credentials. This security is enforced by a server issuing a session cookie to a mobile application once a user has successfully authenticated and authorized service requests. Improper session handling occurs when inappropriate procedures are not enforced, resulting in a session cookie being intercepted by cybercriminals. (Michael et al., 2013; Barcena et al., 2014; OWASP, 2014; Selinger, 2015)
11. **Unintended data leakage:** Operating Systems, digital infrastructure and hardware are just but the few components within mobile devices that can change with time. Developers are unable to handle these changes outside the bounds of the application. Due to these changes, it is possible for data to be lost. This data loss may occur if a full understanding in not acquired to readjust the application to interact with the changes (Huckvale et al., 2015; Martínez-Pérez et al., 2015).

12. **Security Decisions via untrusted inputs:** An application may receive data from various sources. This can be achieved in most cases by the Inter Process Communication (IPC) within a mobile application. To reduce any risk, the mobile application should communicate with other trusted applications it interacts with. Furthermore, sensitive tasks should require the application user input (OWASP, 2014).
13. **Lack of Binary Protections:** Applications can be reversed engineered at a binary level. This reverse engineering can occur when a programmer was not involved in the development of the application at a binary level. If the application is not protected at this level, and attacker may find flaws and reconfigure the application and re-sell the application as its own (OWASP, 2014).

14. **Broken Cryptography:** Encryption is used to protect user data. However, by utilizing outdated algorithms and encryption techniques results in application insecurity (OWASP, 2014; Martínez-Pérez et al., 2015)

6.3 Consumer Health Wearable Threat Assessment Framework

From identifying the vulnerabilities that may affect the asset of consumer health data. The next phase includes the classification phase where the threats are classified based on the consumer factor they affect. This classification was conducted by firstly identifying a vulnerability from the collated list then reviewing the manner in which it affects a consumer factor. Take for example the threat of Improper Session Handling, this vulnerability focuses on sessions not being handled correctly. This results in poor *Authentication* by not auto generating session tokens. If a session token is intercepted, a malicious attacker can falsely authenticate themselves into a user's account. This threat will also affect the *Confidentiality* of a user. In addition, the *Integrity* of consumer health data may be affected if an attacker desires to alter consumer health data. This process was conducted for each of the vulnerabilities identified (Section 6.2.2). The final product through the classification process is a threat assessment framework coined as the 'Consumer Health Wearable Threat Assessment Framework' (Figure 6.2).



Consumer Factors

Authentication

Security Decisions via Untrusted Inputs

Lack of Access Codes

Poor Authorization & Authentication

Weak Server Side Controls

Authorization

Poor Authorizatin & Authentication

Security Decisions via Untrusted Inputs

Lack of Access Codes

Weak Server Side Controls

Improper Session Handling

Availability

Insecure Data Storage

Client Side Injection

Weak Server Side Controls

Insufficient Transport Layer Protection

Broken Cryptography

Third Party Analytics

Confidentiality

Improper Session Handling

Third-Party Analytics

Weak Server Side Controls

Insufficient Transport Layer Protection

Client-Side Injection

Broken Cryptography

Lack of Privacy Policy

Unintended Data Leakage

Location tracking

Non-Repudiation

Insufficient Transport Layer Protection

Poor Authorization & Authentication

Lack of Privacy Policy

Integrity

Improper Session Handling

Client-Side Injection

Insufficient Transport Layer Protection

Broken Cryptography

Weak Server Side Controls

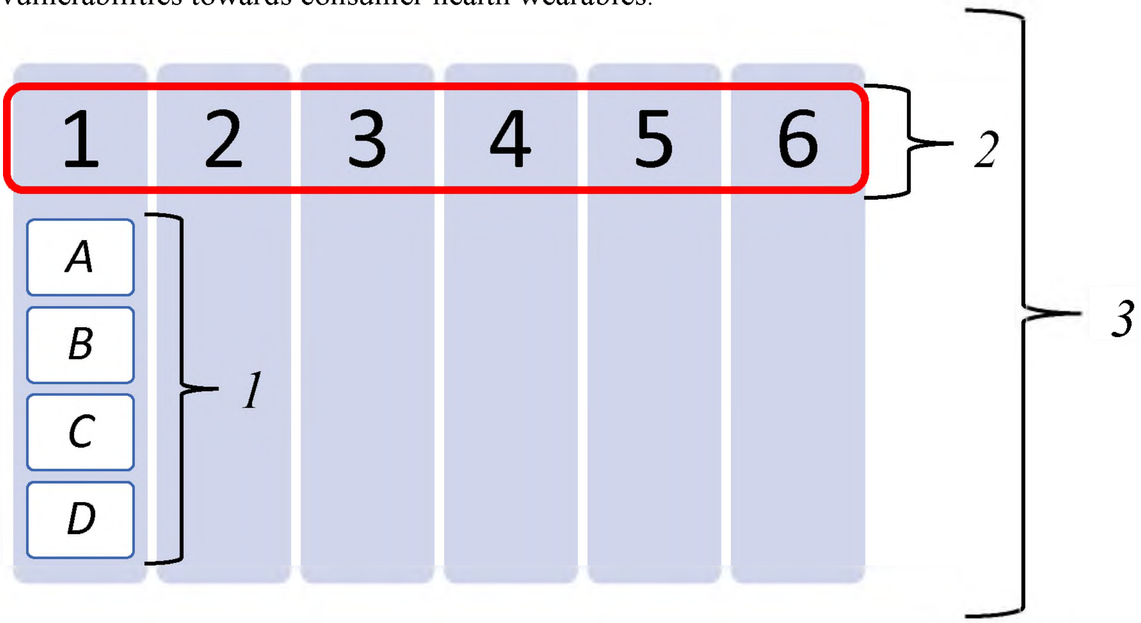
Poor Authorization and Authentication

Insecure Data Storage

Figure 6.2:Consumer Health Wearable Threat Assessment Framework

6.3.1 Description of Framework

The Consumer Health Wearable Threat Assessment Framework provides a classification of the threats that may affect consumer factors. This framework focuses solely on consumer health wearables and their associated applications. As compared to the other theoretical frameworks described in Chapter 5, the Consumer Health Wearable Threat Assessment Framework identifies the assets, and the vulnerabilities affect them. This is deemed beneficial for novice developers and security professionals are it provides a guiding and review process of the vulnerabilities pertaining to this environment. The Consumer Health Wearable Threat Assessment Framework is comprised of three components (Figure 6.3). The first component includes the vulnerability list which affect consumer health wearables. The second component includes the key classification tiers for consumer health wearables and their associated applications. In addition to this, the vulnerabilities classified within these tiers. The third component is the overall threat assessment framework which provides a basis of coverage of the vulnerabilities towards consumer health wearables.



Component:

1: - Vulnerability affecting consumer health wearables

2: - Classification tiers and categorization

3: - Overall overview of the framework

Figure 6.3: Components of Framework

The Consumer Health Wearable Threat Assessment Framework is viewed to meet the objective of the research. As it takes into consideration the diverse components of the consumer health wearable ecosystem. This achieved, by identify the consumer factors which are key components towards consumer health wearables. In addition, the framework helps to guide the detection of security vulnerabilities that are faced towards consumer health wearables by identifying and classifying vulnerabilities within this contextualised environment. Through this it supports developers to understand where security measure are needed to be implemented or improved.

6.3.2 Vulnerability Criteria for Framework

As described this research seeks to formulate a threat assessment framework that can be used to identify vulnerabilities that affect consumer health wearables and their associated applications. Thus far, this process has been conducted by identifying the assets and the threats that affect these assets. From this a classification framework has been produced as a guiding light to help identify which vulnerabilities affect and pertain to an asset. However, this classification is incomplete without a set of check list criteria to help detect the vulnerabilities pertaining to consumer health wearables. Table 6.1 outlines a check list criteria to help assist to detect the threats. Table 6.1 outlines example criteria, this criteria can adapt with the change in technology and software of devices (Rai, 2013; OWASP, 2014; Morera et al., 2016)

Table 6.1: Example criteria of vulnerabilities

Vulnerabilities
Third Party Analytics ➢ Lack of encryption or weak encryption algorithms as data is sent to third party analytics. Weak encryption algorithms RC2, MD4, MD5, SHA1 ➢ Sending data in clear text ➢ Lack of SSL or TLS standards during transmission ➢ Certificates not up to data
Lack of Access Codes ➢ Wearable device has no authentication during pairing ➢ Lack of authentication during re-paring of devices ➢ Wearable devices and application has no passwords or pins to protect user data
Location Tracking ➢ Bluetooth signal not masked or hidden from nearby devices
Lack of Privacy Policy ➢ No documentation of the manner in which data will be handled or processed. ➢ Not detailing the permissions that will be used by the device
Insecure Data Storage ➢ Storing sensitive data on the file system: usernames, authentication tokens, passwords, cookies, device name, network, connection name, personal information (address, credit card data), application data, GPS/tracking information. ➢ Not using an API login scheme (over HTTPS). Furthermore, sensitive data should be stored on the server side. Assuming that there is a secure network connectivity. ➢ Not using SQLite for database encryption
Weak Server Side Controls ➢ Unencrypted access to server-side API ➢ Access to user data without authorization
Insufficient Transport-Layer Protection ➢ Are all connections being not secure and properly encrypted ➢ SSL certificates should be up to date ➢ SSL certificate should be not self-signed ➢ SSL should use high ciphers ➢ Application should not accept user accepted certificates
Client-Side Injection ➢ Overly detailing error reporting can help identify the type of server utilised. This will assist to determine the type of query language used. ➢ Not parametrizing queries. This can be checked by inserting a“ %,@, ’, OR ” ➢ Whitelisting instead of blacklisting ➢ Disable JavaScript and plugin support ➢ Do not let outside sources control user data and messages or any part of the format string
Poor Authorization and Authentication ➢ Where possible the authentication should occur on the server side. Successful authentication will load application data on the mobile device. This ensures application data is only available when the user has successfully authenticated.

➢ User passwords should not be stored on the device if persistent authentication (remember me) is utilised ➢ 4 digit passwords should not be utilised ➢ Persistent authentication should be available by default, but by opt-in.
Improper Session Handling ➢ Lack of adequate timeout sessions. Mobile application allows for long periods of timeout sessions. ➢ Failure to validate session tokens on the server side. ➢ Failure to properly rotate cookies by using auto generate mechanisms.
Unintended Data Leakage ➢ Analytical data sent to 3rd parties is unencrypted ➢ URL caching ➢ HTML 5 data storage ➢ Browser cookie objects ➢ Keyboard press caching ➢ Copy/paste buffer caching
Security Decisions via Untrusted Inputs This vulnerability can be checked via tools like Drozer. This will interact with the Inter process communication (IPC) to assess endpoints ➢ Sensitive data should not be sent through Inter Process Communication mechanism ➢ Any sensitive actions should have user interaction before an action is performed. ➢ Allow permissions of the application to access all components.
Lack of Binary Protections ➢ Can the application be modified to change the presentation layer within the application? ➢ Can automated tool be used like Hopper for visualisation of control-flow? ➢ Can the application be reversed engineered using automated tools (dex2jar for example)? ➢ Can the application be modified at the application's binary level using a hex editor?
Broken Cryptography ➢ Reliance on built-in code encryption processes ➢ Poor key management processes (Do not create own protocol for key management) ➢ Creation and use of custom encryption protocols ➢ Use of insecure and/or deprecated algorithms: RC2, MD4, MD5, SHA1

6.4 CONCLUSION

This chapter focused on the Consumer Health Wearable Threat Assessment Framework developed for assessing consumer health wearables and their associated applications. The development of this framework was conducted through three phases focusing on consumer factors, vulnerabilities and vulnerability criteria (Figure 6.4). Consumer Factors focused on identifying the assets of consumer health wearables which are prone to vulnerabilities. The vulnerability phase focused on listing the vulnerabilities pertaining to consumer health wearables. This phase also focused on developing the Consumer Health Wearable Threat Assessment Framework by classifying the threats based on the consumer factor they affect. The final phase focused on producing a set of vulnerability criteria to identify the vulnerabilities that affect consumer health wearables. These criteria help to identify the tiers in which a certain section is weak within the Consumer Health Wearable Threat Assessment Framework.

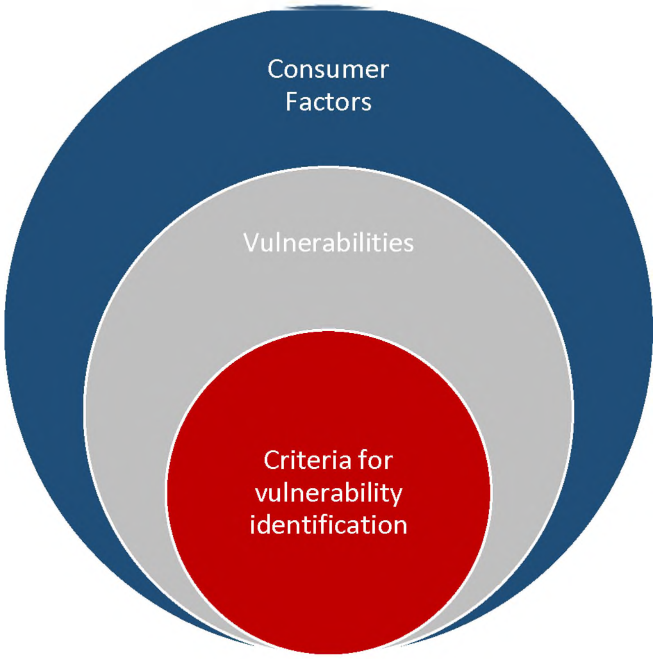
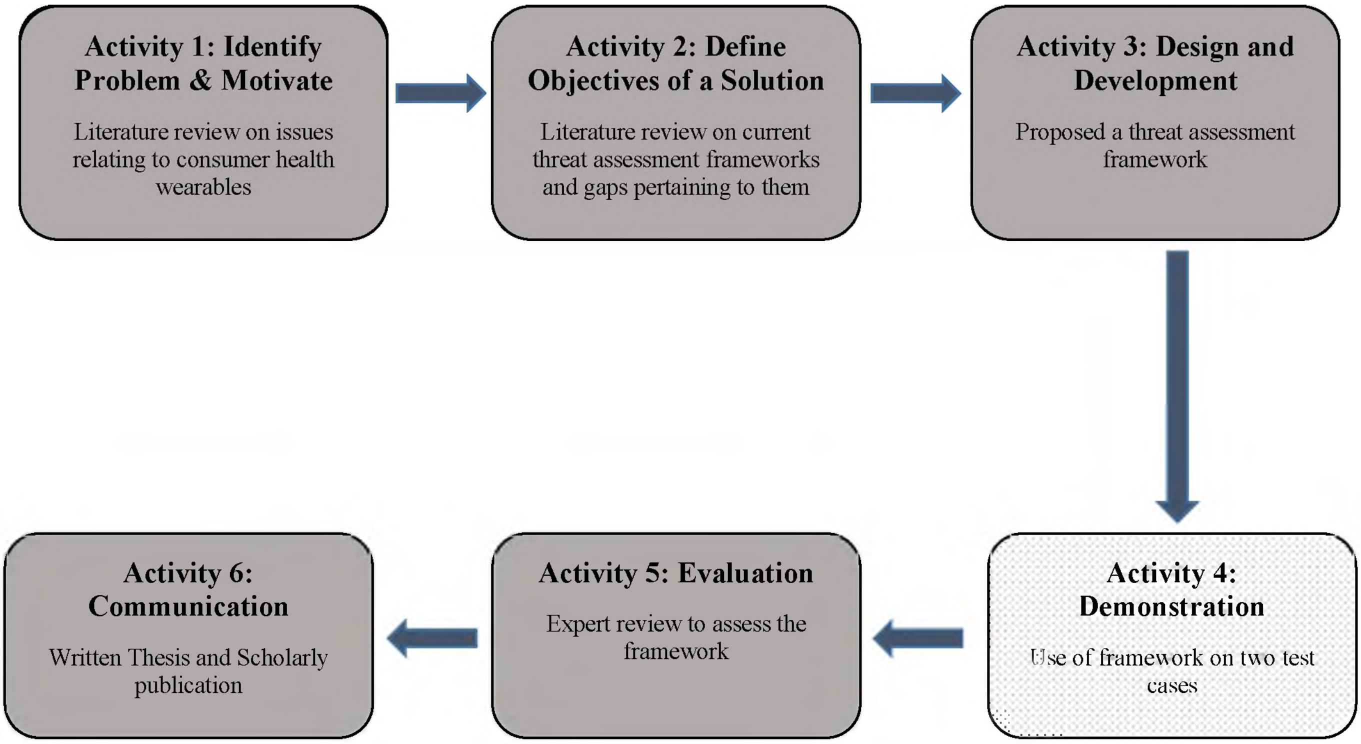


Figure 6.4: Summary of Framework Formation

Chapter 7: FRAMEWORK DEMONSTRATION


Activity 1: Identify Problem & Motivate
Literature review on issues relating to consumer health wearables
Activity 2: Define Objectives of a Solution
Literature review on current threat assessment frameworks and gaps pertaining to them
Activity 3: Design and Development
Proposed a threat assessment framework
Activity 4: Demonstration
Use of framework on two test cases
Activity 5: Evaluation
Expert review to assess the framework
Activity 6: Communication
Written Thesis and Scholarly publication

7.1 INTRODUCTION

This chapter will focus on **Activity 4** of Demonstration as part of conducting the Design Science Research Process Model by Peffers et al. (2007). Demonstration of a developed artefact is a key activity of Design Science Research. As it illustrates the utility and efficacy of the artefact. In addition, assists to demonstrate how well the produced artefact actually performs within the contextualised environment. The demonstration will illustrate the use of the Consumer Health Wearable Threat Assessment Framework on two test cases. To guide and assist in the identification of potential security vulnerabilities in consumer health wearables. This chapter is organized by firstly, explaining the demonstration set up (Section 7.2), and the procedure conducted for each test case. From describing the demonstration set up, the vulnerabilities discovered from the test cases, and a review how these vulnerabilities impact the consumer health wearables will be outlined (Section 7.3 and 7.4). A discussion will also be presented (Section 7.5) on the utility and efficacy of the framework towards consumer wearables.

7.2 DEMONSTRATION SET-UP

To demonstrate the Consumer Health Wearable Threat Assessment Framework requires setting up an environment to assess the degree to which the fitness trackers and their associated mobile health applications contain the potential vulnerabilities as per described in the framework. Setting up the demonstration environment requires a characteristic of the consumer health wearable ecosystem (Section 4.3). This requires a fitness tracker, a mobile device, the corresponding health application installed on the mobile device, a laptop to perform the testing and a WiFi connection. For this demonstration, a WiFi connection was used rather than cellular connection on the mobile device. This was done to perform penetration testing attacks and to view and assess the network traffic from the mobile device as information was sent to cloud servers.

7.2.1 Description of Test Cases

Test Case A

Test case A, is a popular fitness tracker used for the casual enthusiast. The fitness tracker used utilises Bluetooth Low Energy (BLE), and contains a heart rate monitor, a minimal display screen (OLED), 3-axis accelerometer (to record movement), altimeter, and vibration motor. In addition to this the fitness tracker contains a Bluetooth dongle which can be used to connect to a laptop and perform syncing to cloud servers. No pre-setup, was required for this test case to perform the testing.

Test Case B

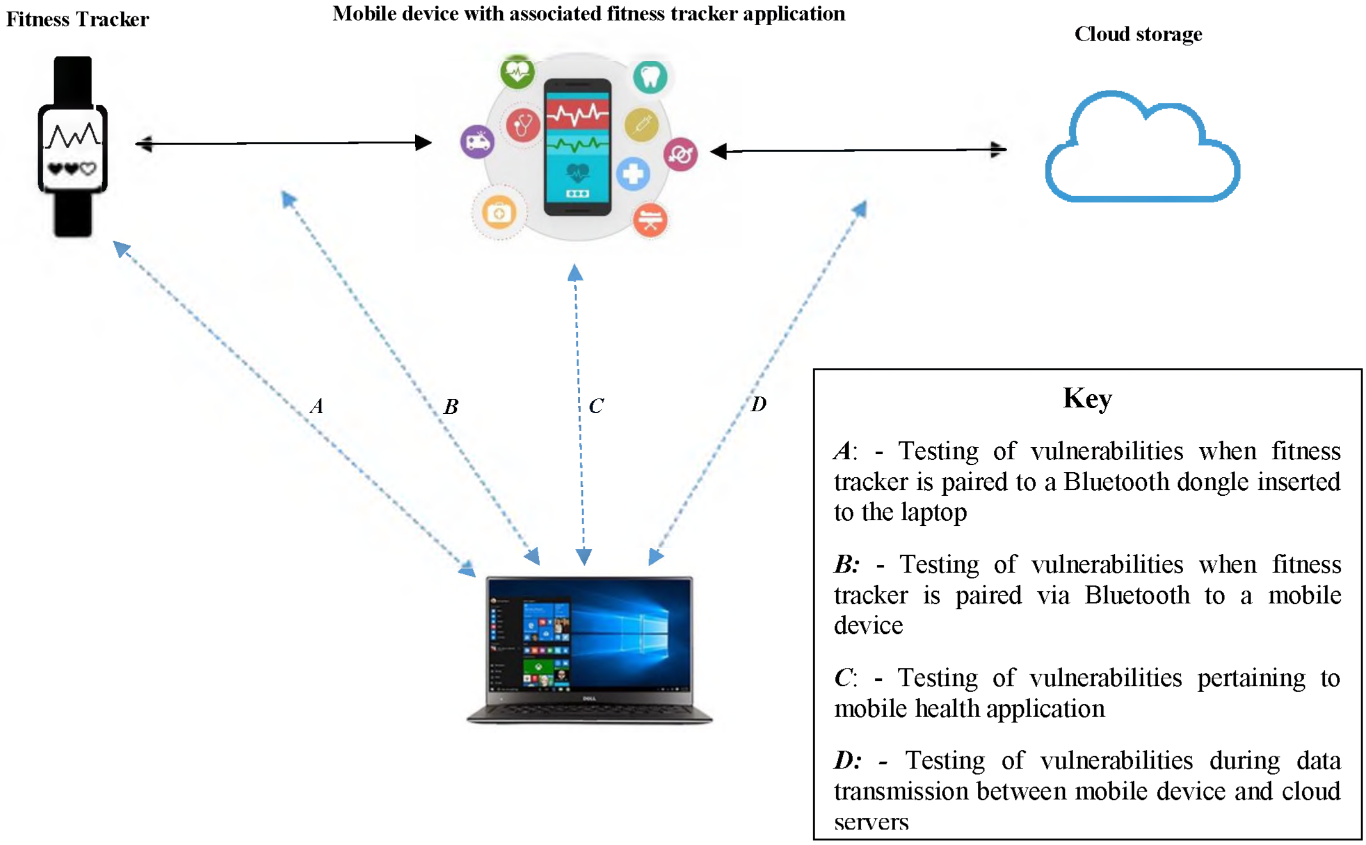
Test Case B is a popular fitness tracker for more professional users. This fitness tracker can also be used as a smartwatch with a detailed display screen for a user to receive notification feedback. The device contains, Bluetooth Low Energy (BLE), a heart rate monitor, 3-axis accelerometer, altimeter, vibration motor, and is also water proof. The fitness tracker also supports wireless chest based monitors to track additional health related data. This device requires an initial pre-setup before it may be used. As compared to Test Case A where all that was required was for the user to install the application on the mobile device and pair it to the fitness tracker. Test Case B required the user to register the device before any pairing could be performed. Test Case B has an in-built USB standard-A plug which can be inserted to a computer. Before a user may start to record and view their consumer health data on a mobile device, the device needs to be registered on the on cloud servers of the device. This registration is conducted by first installing the web service application on a laptop. This web service will also require the user to create a user profile and password. On successful installation of the web service application and creation of a user account, the fitness tracker will need to be plugged into the laptop via the USB connection to perform the registration of the device. This registration records the MAC address of the fitness tracker and gives it a unique identifier. Once registered, the fitness tracker is linked to the user profile to whom the tracker belongs. When this initial setup is complete, may the user download the application on the mobile device and pair it to the fitness tracker. Only, when the device is successfully registered, may the user perform syncing and view their consumer health data on a mobile device.

7.2.2 Description of Mobile Device and Application Testing Software

The mobile device used for testing both test cases was an Android based device running Android Version 6.0 (Marshmallow). The application testing conducted on the laptop used Windows 10 and Kali Linux installed on Virtual Box. The software tools used to analyse the vulnerabilities included Wireshark and Burp Suite Free Edition.

7.2.3 Demonstration Procedure

The procedure in which the testing was conducted for the two test cases can be described with Figure 7.1.



Key

A: - Testing of vulnerabilities when fitness tracker is paired to a Bluetooth dongle inserted to the laptop

B: - Testing of vulnerabilities when fitness tracker is paired via Bluetooth to a mobile device

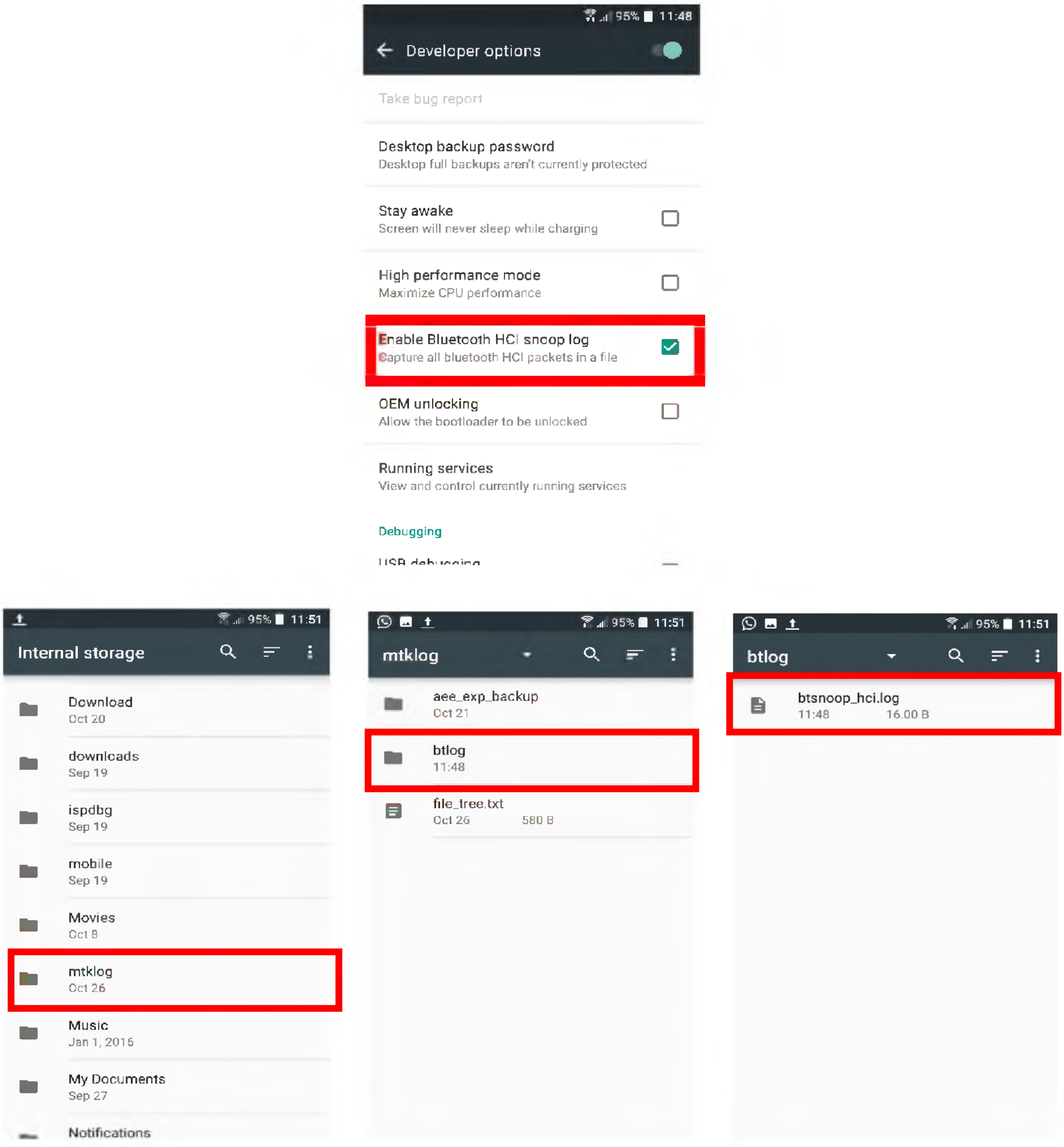
C: - Testing of vulnerabilities pertaining to mobile health application

D: - Testing of vulnerabilities during data transmission between mobile device and cloud servers

Figure 7.1: Demonstration Procedure

Connection A and B

The test case fitness trackers were paired to a mobile device with their associated mobile health applications of the fitness tracker. To test if there are possible vulnerabilities during the pairing phase, two methods were conducted; through connection ***A*** and ***B*** (Figure 7.1). When point ***A*** was utilised, a Bluetooth dongle of the fitness tracker was inserted into the laptop and paired to the fitness tracker. Once paired, Wireshark was used to assess the packets during the data transfer. Connection ***B*** was also a method used to assess the vulnerabilities during the pairing phase between the fitness tracker and mobile device. This method was done by turning on the developer options on the android based mobile device. By default, on android devices, the developer options are not displayed on the settings menu. This required, tapping multiple times on the software number to activate the developer options. Once the developer options were activated the Bluetooth HCI (Host Controller Interface) snoop log was selected (Figure 7.2). This functionality keeps a log file of Bluetooth capture within a file directory on the mobile device. The log file will contain the time stamp of transfer, source of device, destination point, protocol used, length of packets, information of the data that was sent. The log data was captured when the mobile device was paired to the fitness tracker and a synchronization processes was conducted. The log data captured was then downloaded from the mobile device and reviewed on Wireshark to assess any vulnerabilities (Figure 7.2).



Take bug report

Desktop backup password
Desktop full backups aren't currently protected

Stay awake □
Screen will never sleep while charging

High performance mode □
Maximize CPU performance

Enable Bluetooth HCI snoop log ☑
Capture all bluetooth HCI packets in a file

OEM unlocking □
Allow the bootloader to be unlocked

Running services
View and control currently running services

Debugging

USB debugging

Download
Oct 20

downloads
Sep 19

ispdbg
Sep 19

mobile
Sep 19

Movies
Oct 8

mtklog
Oct 26

Music
Jan 1, 2015

My Documents
Sep 27

Notifications

aee_exp_backup
Oct 21

btlog
11:48

file_tree.txt
Oct 26 580 B

btsnoop_hci.log
11:48 16.00 B

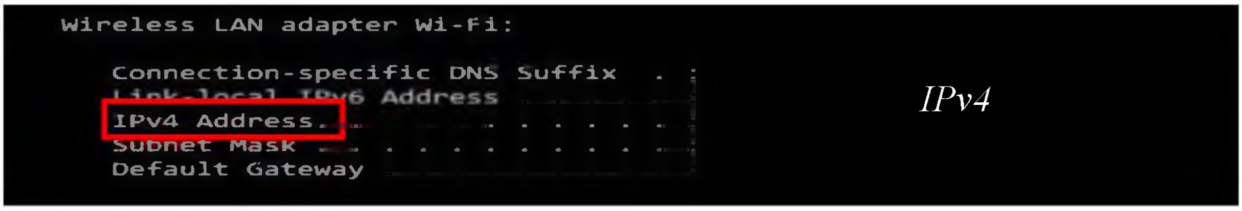
Figure 7.2: Bluetooth Log File Setup

Connection C

At connection ***C*** the associated application of the fitness trackers stored on the mobile device was manually reviewed on a laptop to assess if there any pertaining vulnerabilities. This review was done by installing the fitness tracker associated application APK (android package kit) on the Android Studio IDE (Google Android, 2016). An android emulator on the IDE was used for this point running Android 6.0. This version was used to maintain consistency as the testing mobile device. The testing focused on reviewing application file system, application database, caches, configuration files and key stores.

Connection D

Connection ***D*** focuses on identifying vulnerabilities that may occur as consumer health data is transferred from the mobile device to cloud servers. To perform this, traffic was bypassed from the mobile device through a laptop before it was sent to cloud servers. This was done to perform penetration testing attacks and to view and assess the network traffic from the mobile device as information was sent to cloud servers. To perform this, the proxy settings of the mobile device was changed, making the testing laptop the 'man-in-the-middle' to eavesdrop the communication. As both the testing laptop and mobile device are connected to same WiFi connection, the proxy hostname name on the mobile device was set to the WiFi IP address of the laptop and the proxy port of the mobile device was set to 8888. To conduct this, firstly the WiFi IP address from the laptop needs to be obtained via *ipconfig* command typed within command prompt (Figure 7.3).

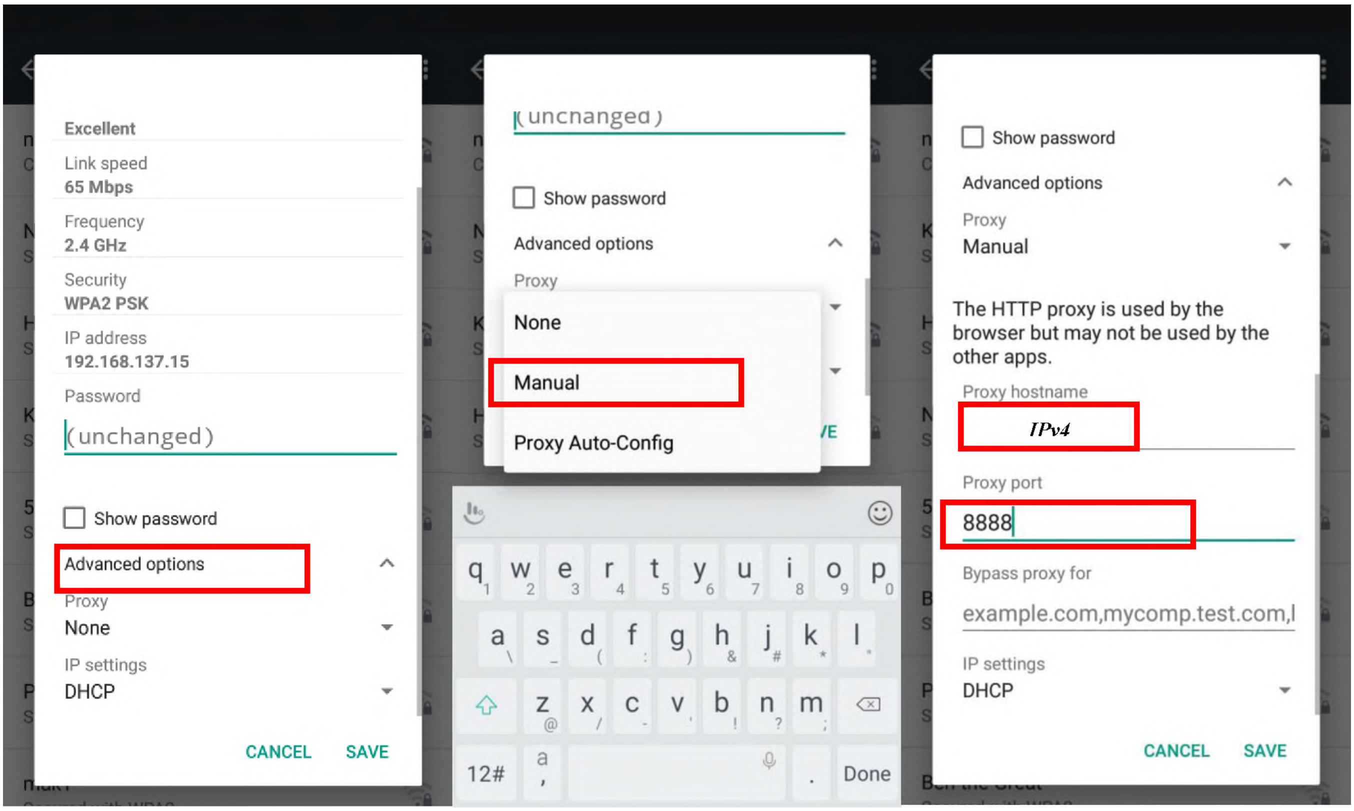


```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address
   IPv4 Address. . . . . . . . . . . :
   Subnet Mask . . . . . . . . . . . :
   Default Gateway
```

Figure 7.3: Testing WiFi IP Address

The WiFi IP address was then used as the proxy hostname within the mobile device so the network traffic can be reviewed from a computer. The proxy name was set in the mobile device by selecting the WiFi network name connected. When this was done, a list of options was given. *Advanced options* was chosen where a further drop down list was shown and *manual* was chosen. Within the manual settings, the proxy hostname was set as the *IPv4* from the WiFi IP address and the proxy port was set as 8888 (Figure 7.4).



Excellent

Link speed: 65 Mbps

Frequency: 2.4 GHz

Security: WPA2 PSK

IP address: 192.168.137.15

Password: (unchanged)

□ Show password

Advanced options

Proxy: None

IP settings: DHCP

The HTTP proxy is used by the browser but may not be used by the other apps.

Proxy: Manual

Proxy hostname: *IPv4*

Proxy port: 8888

Bypass proxy for: example.com,mycomp.test.com,l

IP settings: DHCP

Figure 7.4: Proxy Setting of Mobile Device

It is also important to note, that for these particular test cases, the researcher did not have authorization to review and assess the vulnerabilities that could pertain to the cloud storage of the fitness tracker. For each connection (***A, B, C, D***), the testing was conducted by iterating through all the vulnerabilities listed (Table 7.1) by reviewing if they affect the test case. Once a vulnerability was discovered it was marked under the tier it affected from the Consumer Health Wearable Threat Assessment Framework. Once this was completed, the weak areas whether be it authentication, authorization, availability, confidentiality, non-repudiation and integrity from the threat assessment framework can be assessed. This assessment involved identifying which tier was most affected.

Table 7.1: Vulnerability List for Assessment

Vulnerabilities	
Threat Name	*Description*
1. Third Party Analytics	Mobile health applications use analytic tools to assess health data. In the process of communicating to these third party analytical servers, metadata of a user's behaviour and activity is collected (Adhikari et al., 2014; Goyal et al., 2016).
2. Lack of Access Codes	Many health applications and fitness trackers lack access codes to protect them from being viewed by outside parties. (HP Fortify, 2015; Goyal et al., 2016)
3. Location Tracking	GPS sensors are vulnerable to location tracking due to the unique ID displayed from Bluetooth signals (Barcena et al., 2014; Goyal et al., 2016).
4. Lack of Privacy Policy	Mobile Health applications utilize permissions that require a user's authorization to use the device features. In many cases, health applications lack privacy policies to state how a consumer's data will be utilized and the manner in which it will be collected. (Dinh et al., 2013; Goyal et al., 2016)
5. Insecure Data Storage	This is a result of poorly encrypted information, caching information and allowing global permissions. This insecure data storage occurs either internal (on board) or external (to cloud services) (Al Ameen et al., 2012; Michael et al., 2013; Huckvale et al., 2015; Goyal et al., 2016)
6. Weak Server-side Controls	This occurs on the server side by not implementing proper security controls or configurations. Also disabling unnecessary back-end services. (Symantec, 2014; Adhikari et al., 2014; OWASP, 2014; Huckvale et al., 2015)
7. Insufficient transport-layer protection	This applies to applications that use the HTTP protocol for communication (client-server). HTTPS provides transport layer protection, but if digital certificates are ignored or the use of plain-text communication is enforced. This places the information at risk. (Huckvale et al., 2015)
8. Client-side injection	This threat applies for mobile web and hybrid applications. These types are susceptible to SQL injection (OWASP, 2015; Goyal et al., 2016). SQL injection is a type of attack that uses SQL queries to manipulate a server in the favour of an attacker.
9. Poor authorization and authentication	As compared to websites, users of mobile applications are not online at all times for authentication. Authentication may also occur offline. Poor authorization and applying authentication poorly allows passwords, keys, or session tokens to be exploited (Martínez-Pérez et al., 2015; Goyal et al., 2016).
10. Improper session handling	Sessions are used as a form of security, to allow a user to perform a specific action for a time period, until they are required to re-authenticate their credentials. This security is enforced by a server issuing a session cookie to a mobile application once a user has successfully authenticated and authorized service requests. Improper session handling occurs when inappropriate procedures are not enforced, resulting in a session cookie being intercepted by cybercriminals. (Michael et al., 2013; Barcena et al., 2014; OWASP, 2014; Selinger, 2015)
11. Unintedend Data Leakage	Operating Systems, digital infrastructure and hardware are just but the few components within mobile devices that can change with time. Developers are unable to handle these changes outside the bounds of the application. Due to these changes, it is possible for data to be lost. This data loss may occur if a full understanding in not acquired to readjust the application to interact with the changes (Huckvale et al., 2015; Martínez-Pérez et al., 2015).
12. Security Decisions Via Untrusted Inputs	An application may receive data from various sources. This can be achieved in most cases by the Inter Process Communication (IPC) within a mobile application. To reduce any risk, the mobile application should communicate with other trusted applications it interacts with. Furthermore, sensitive tasks should require the application user input (OWASP, 2014).
13. Lack of Binary Protections	Applications can be reversed engineered at a binary level. This reverse engineering can occur when a programmer was not involved in the development of the application at a binary level. If the application is not protected at this level, and attacker may find flaws and reconfigure the application and re-sell the application as its own (OWASP, 2014).
14. Broken Cryptography	Encryption is used to protect user data. However, by utilizing outdated algorithms and encryption techniques results in application insecurity (OWASP, 2014; Martínez-Pérez et al., 2015).

7.3 VULNERABILITY EXPOSURE OF TEST CASE A

7.3.1 Third Party Analytics

It was discovered that five third party analytics are used to analyse consumer health data. In addition, in communication with these third-party analytics data is sent over HTTP rather than HTTPS. These third-party analytics included *googleapis*, *crashlytics*, *mixpanel*, *flurry* and *cmcm*. In relation to the threat assessment framework, this vulnerability can affect the *availability* and *confidentiality* towards consumer health data.

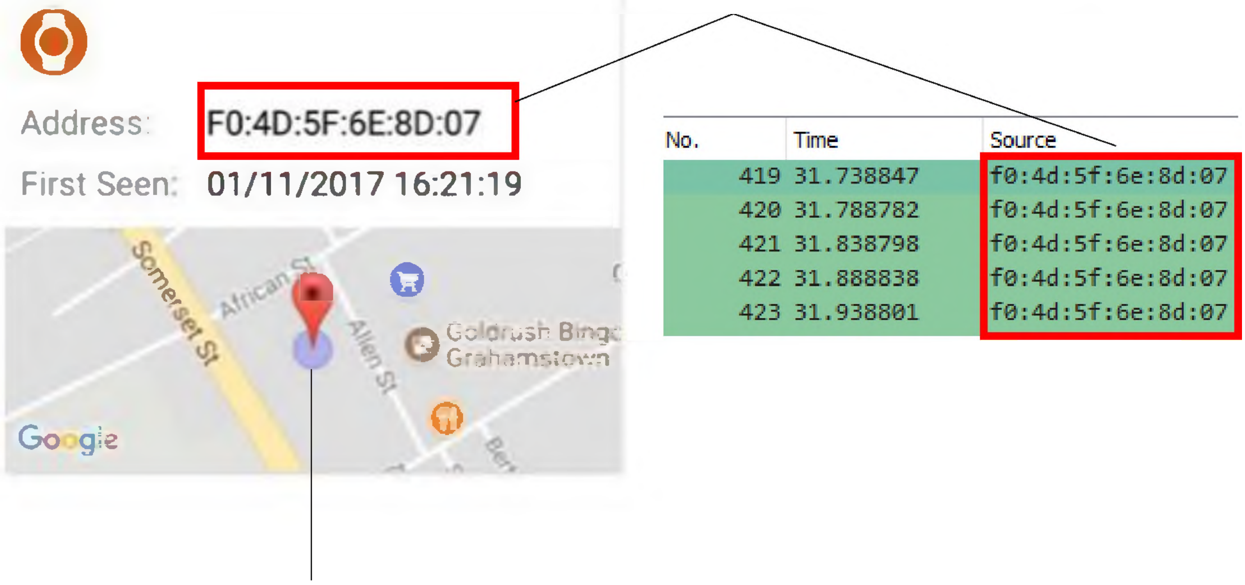
7.3.2 Lack of Access Codes

The fitness tracker had no access codes for protecting the consumer health data in case it was lost or stolen. In addition, a unique identifier was not used to register the tracker on cloud servers. By not enforcing any form of registration of the fitness tracker any individual is able to pair the fitness tracker to a different mobile device at any given chance and obtain, the consumer health data that was stored on the fitness tracker. In relation to the threat assessment framework, this vulnerability can affect the *authentication* and *authorization* towards consumer health data.

7.3.3 Location Tracking

The Bluetooth signal is always discoverable to nearby individuals. Furthermore, the Bluetooth MAC address is fixed and a virtual MAC address created when rebooted. The RamBLE Android application was used to discover the geolocation of the fitness tracker. By not creating a vitual MAC address the fitness tracker can be located by attackers. Figure 7.5 shows an image of the geolocation of the fitness tracker obtained from testing. Figure 7.5 also shows the fixed MAC address discovered from both Wireshark and RamBLE. In relation to the threat assessment framework, this vulnerability can affect the *confidentiality* towards consumer health data between the fitness tracker the mobile device as eavesdropping and man-in-the-middle-attacks may occur through this.

MAC Address



Address: F0:4D:5F:6E:8D:07

First Seen: 01/11/2017 16:21:19

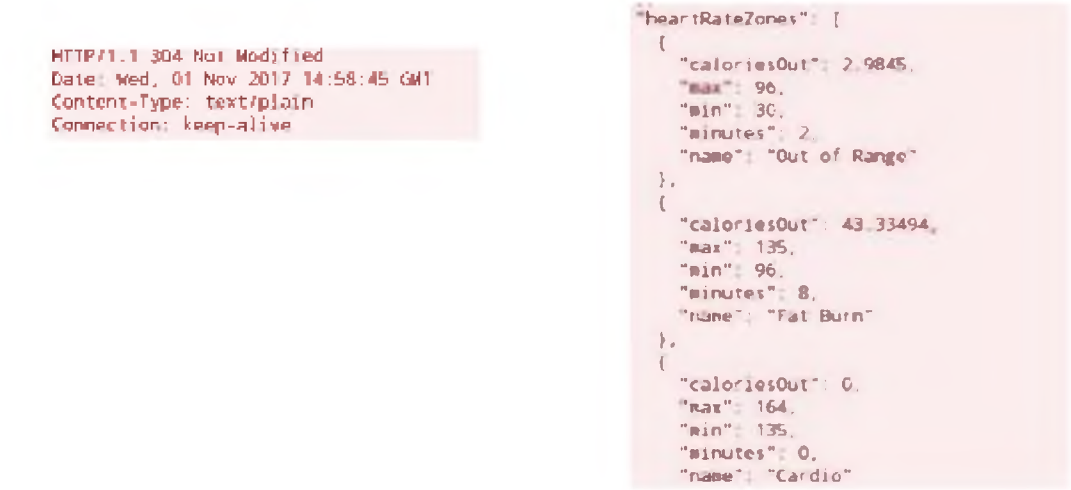
No.	Time	Source
419	31.738847	f0:4d:5f:6e:8d:07
420	31.788782	f0:4d:5f:6e:8d:07
421	31.838798	f0:4d:5f:6e:8d:07
422	31.888838	f0:4d:5f:6e:8d:07
423	31.938801	f0:4d:5f:6e:8d:07

Geo-Location

Figure 7.5: Test Case A, Location Tracking

7.3.4 Insufficient transport-layer protection

The fitness tracker sends consumer health to cloud servers for analytical purposes. It was discovered data transmissions were sent over HTTP including critical transmissions such as usernames, passwords and consumer health data. In relation to the threat assessment framework, this vulnerability can affect the *availability*, *confidentiality*, *non-repudiation* and *integrity* towards consumer health data. Figure 7.6 shows a post request sent through HTTP in plain text. On inspection the consumer health data sent were the heartrate zones when the user performed an exercise.



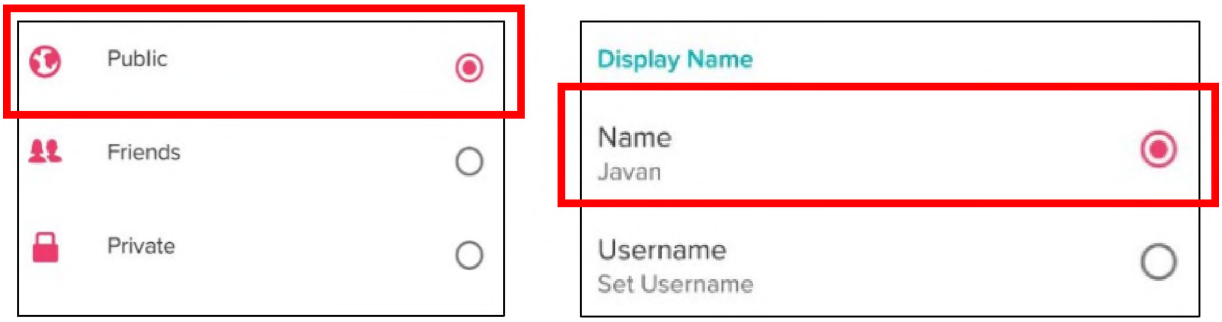
```
HTTP/1.1 304 Not Modified
Date: Wed, 01 Nov 2017 14:58:45 GMT
Content-Type: text/plain
Connection: keep-alive
```

```
"heartRateZones": [
  {
    "caloriesOut": 2.9845,
    "max": 96,
    "min": 30,
    "minutes": 2,
    "name": "Out of Range"
  },
  {
    "caloriesOut": 43.33494,
    "max": 135,
    "min": 96,
    "minutes": 8,
    "name": "Fat Burn"
  },
  {
    "caloriesOut": 0,
    "max": 164,
    "min": 135,
    "minutes": 0,
    "name": "Cardio"
```

Figure 7.6: Test Case A, Insufficient Transport Layer Protection

7.3.5 Privacy Policy

By default, on sign up, real names and a user's consumer health data is available to the public (Figure 7.7) can lead to username enumeration. However, this privacy setting can be changed by a user if they desire to do so. By this being set by default, this affects the *confidentiality* of consumer health data in relation to the framework.



Public ●
Friends ○
Private ○

Display Name
Name
Javan ●
Username
Set Username ○

Figure 7.7: Test Case A, Privacy Policy

On further inspection of the vulnerability, it was discovered that this exposure can lead to user transversal. When testing the researcher was able to view another's consumer's health data who were not on my friend list. The was achieved as these consumer's health data was set to public by default.

7.3.6 Poor Authorization & Authentication

No account lockout policy is instilled. Meaning, a potential attacker can attempt brute force attacks to obtain a user's profile. This was tested by attempting an incorrect password six times. Furthermore, on sign up for a user profile, a minimum of eight characters is required (Figure 7.8). However, there is no use of special characters such as a mixture of uppercase, lowercase, and alphanumeric characters for password management. This was tested, by setting up a password with no special characters; password was *11111111*. This vulnerability affects the tier of *authentication* as brute force attacks can be automated to gain access for a user's profile. In addition, this vulnerability affects the tier of *authorization*.

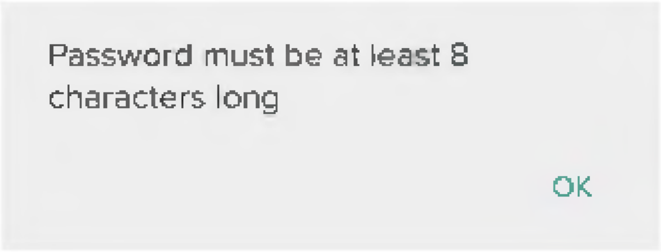

Password must be at least 8 characters long

Figure 7.8: Test Case A, Poor Authorization and Authentication

7.3.7 Threat Impact Review of Test Case A

By identifying the vulnerabilities that affect this test case based from the vulnerability list. A holistic viewpoint of the weak points of the fitness tracker and its associated application can be reviewed from the Consumer Health Wearable Threat Assessment Framework. Figure 7.9 describes a summary of the weak areas that are affected by fitness tracker and its associated application. In isolation a developer may review that only six vulnerabilities were discovered. However, by utilising the Consumer Health Wearable Threat Assessment Framework, the developer is guided with the knowledge that in actual realisation the six core areas pertaining to consumer health are in fact affected. These six areas affected from the vulnerabilities (Figure 7.9) include *authentication, authorization, availability, confidentiality, non-repudiation and integrity*

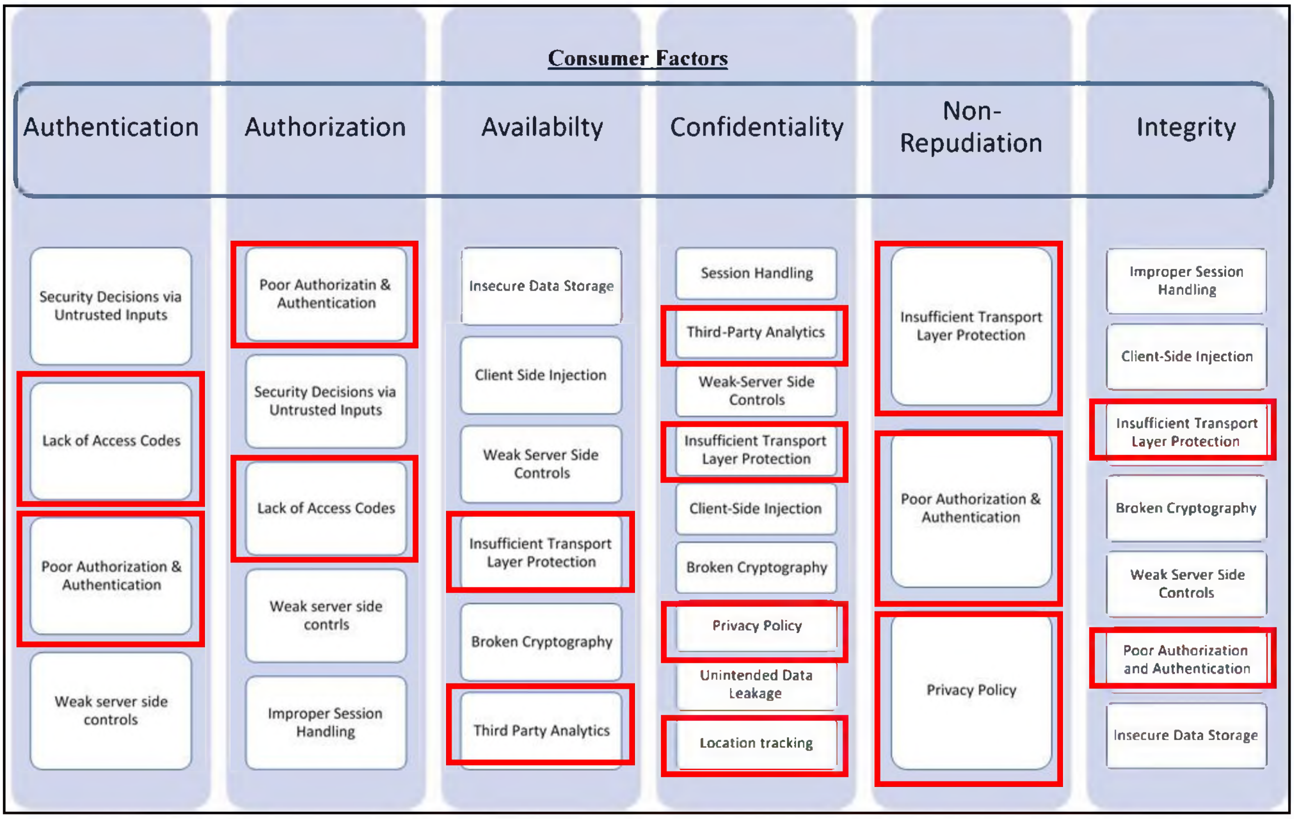

Consumer Factors
Authentication
Security Decisions via Untrusted Inputs
Lack of Access Codes
Poor Authorization & Authentication
Weak server side controls
Authorization
Poor Authorizatin & Authentication
Security Decisions via Untrusted Inputs
Lack of Access Codes
Weak server side contrls
Improper Session Handling
Availabilty
Insecure Data Storage
Client Side Injection
Weak Server Side Controls
Insufficient Transport Layer Protection
Broken Cryptography
Third Party Analytics
Confidentiality
Session Handling
Third-Party Analytics
Weak-Server Side Controls
Insufficient Transport Layer Protection
Client-Side Injection
Broken Cryptography
Privacy Policy
Unintended Data Leakage
Location tracking
Non-Repudiation
Insufficient Transport Layer Protection
Poor Authorization & Authentication
Privacy Policy
Integrity
Improper Session Handling
Client-Side Injection
Insufficient Transport Layer Protection
Broken Cryptography
Weak Server Side Controls
Poor Authorization and Authentication
Insecure Data Storage

Figure 7.9: Summary of Results for Test Case A

Table 7.2 describes a summary of the affected areas based on the consumer factors they affect. This summary aids to identify the major and weak areas affected within the Test Case A. Through this may rectification process begin to improve the security of the fitness tracker and it associated application.

Table 7.2: Summary of Affect Areas for Test Case A

Consumer Factor	Description	Vulnerabilities Discovered
Authentication	As consumer health data is accessed, managed or viewed there needs to be authentication procedures of identifying a user. This is to ensure that the correct user is viewing the correct data.	Two areas out of four areas are affected
Authorization	As consumer health data is accessed, managed or viewed there needs to be authorization methods. Authorization differs to authentication as it identifies whether a user has appropriate rights to access a resource. This ensures that a low level user does not have admin rights.	Two areas out of five areas are affected
Availability	Consumer health data needs to be available to authorized users when requested. An authorized user should have the freedom to view their data when they desire.	Two areas out of six areas are affected
Confidentiality	As consumer health data is central to consumer health wearables. It is vital to keep this data secure and only revealing it to intended parties.	Four areas out of nine areas are affected.
Non-Repudiation	The assurance that someone cannot deny something (digital signature, time stamps, certificates). This is vital when updates are made. There needs to be assurance that any changes to software or hardware firmware is from the manufacturer.	Three area out of three areas are affected.
Integrity	When consumer health data is accessed or managed there is need to be assurance that it is not modified in transit or at rest. In case data is tampered, it can be identified.	Two areas out seven areas are affected.

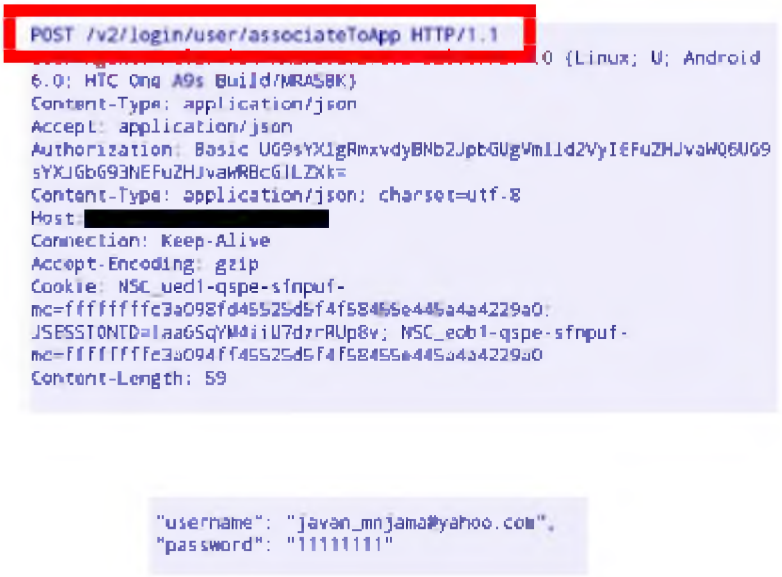
7.4 VULNERABILITY EXPOSURE OF TEST CASE B

7.4.1 Third Party Analytics

By default, this fitness tracker and its associated application do not use any third-party analytics. However, a user my chose to connect the application to other services and health related application. It was discovered, that when connected to other services the consumer health data was sent over HTTP rather than HTTPS. These third-party analytics included *googleapis*, *strava*, *myfitnesspal*, *trainingpeaks* and *nikeplus*. In relation to the threat assessment framework, this vulnerability can affect the *availability* and *confidentiality* towards consumer health data.

7.4.2 Insufficient Transport Layer Protection

Data transmissions of consumer health data were sent over HTTP. From testing, due to this vulnerability the research was able to attain the username and password (Figure 7.10). In relation to the threat assessment framework, this vulnerability can affect the *availability*, *confidentiality*, and *integrity* towards consumer health data.



```
POST /v2/login/user/associateToApp HTTP/1.1
0 (Linux; U; Android
6.0; HTC One A9s Build/MRA58K)
Content-Type: application/json
Accept: application/json
Authorization: Basic UG9sYXlgRmxvdyBNb2JpbGUgVmlld2VyIEFuZHJvaWQ6UG9
sYXJGbG93NEFuZHJvaWRBcGlLZXk=
Content-Type: application/json; charset=utf-8
Host: [redacted]
Connection: Keep-Alive
Accept-Encoding: gzip
Cookie: NSC_ued1-qspe-sfnpuf-
mc=ffffffffc3a098fd45525d5f4f58455e445a4a4229a0;
JSESSIONID=laaGSqYM4iiU7dzrRUp8v; NSC_eob1-qspe-sfnpuf-
mc=ffffffffc3a094ff45525d5f4f58455e445a4a4229a0
Content-Length: 59
```

```
"username": "javan_mnjama@yahoo.com",
"password": "11111111"
```

Figure 7.10: Test Case B, Insufficient Transport Layer Protection

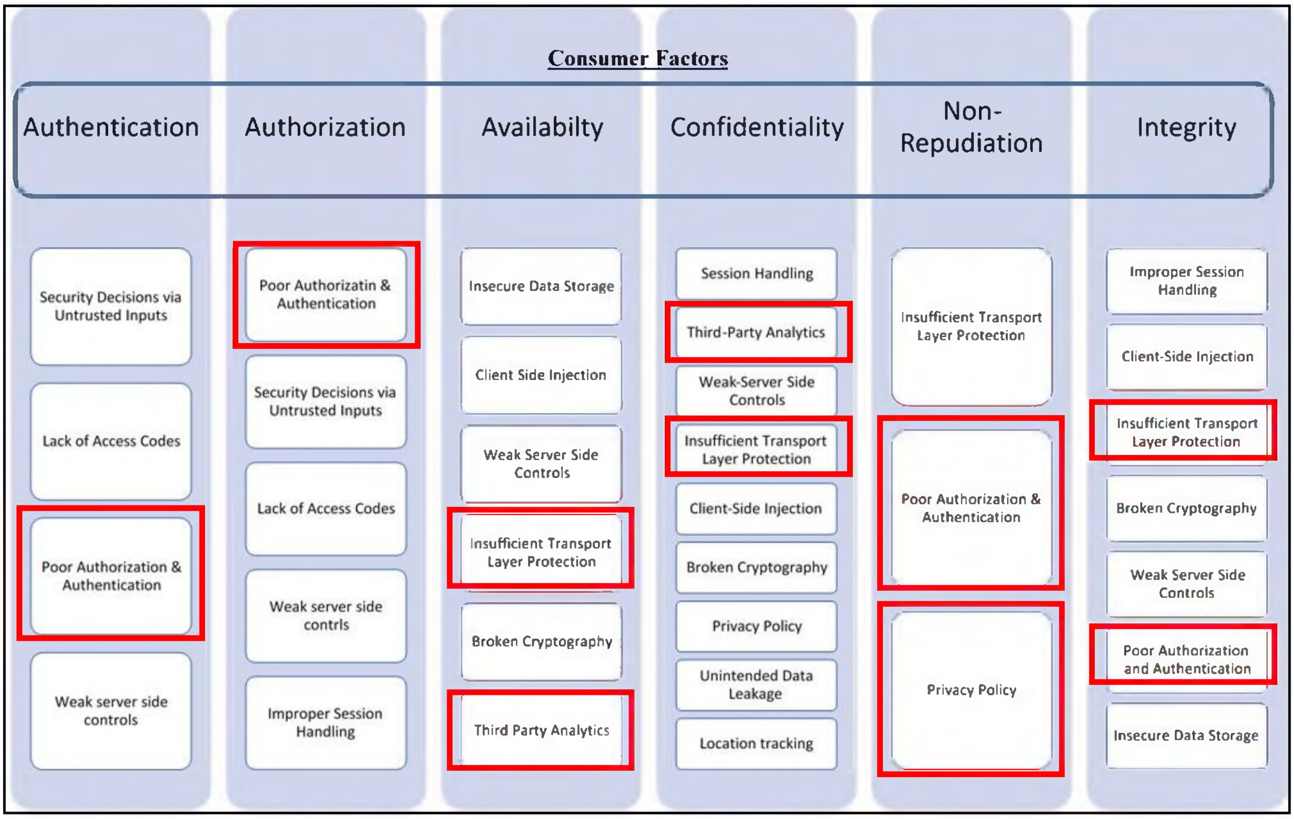
7.4.3 Poor Authorization and Authentication

No account lockout policy is instilled. Meaning, a potential attacker can attempt brute force attacks to obtain a user's profile. This was tested by attempting an incorrect password six times. Furthermore, on sign up for a user profile a minimum of eight characters is required. However, there is no use of special characters such as a mixture of uppercase, lowercase, and alphanumeric characters for password management. This was tested, by setting up a password with no special characters; password was *11111111*. This vulnerability affects the tier of *authentication* as brute force attacks can be automated to gain access for a user's profile. In addition, this vulnerability affects the tier of *authorization*.

7.4.4 Threat Impact Review of Test Case B

As compared to Test Case A it is noticeable that there are fewer vulnerabilities that are affected on the test subject. However, as previously described the aim of the threat assessment is to provide a holistic understanding of the areas affected by a fitness tracker and its associated application. In isolation a developer may not fully understand how the vulnerability of

Insufficient Transport Layer Protection affects Test Case B. However, it is identified (Figure 7.11) that this particular vulnerability affects the availability, confidentiality, non-repudiation and integrity of consumer the health data. Through the visual representation, guidance is provided for the weak areas of the fitness tracker and its associated application.



Consumer Factors
Authentication
Authorization
Availabilty
Confidentiality
Non-Repudiation
Integrity
Security Decisions via Untrusted Inputs
Lack of Access Codes
Poor Authorization & Authentication
Weak server side controls
Poor Authorizatin & Authentication
Security Decisions via Untrusted Inputs
Lack of Access Codes
Weak server side contrls
Improper Session Handling
Insecure Data Storage
Client Side Injection
Weak Server Side Controls
Insufficient Transport Layer Protection
Broken Cryptography
Third Party Analytics
Session Handling
Third-Party Analytics
Weak-Server Side Controls
Insufficient Transport Layer Protection
Client-Side Injection
Broken Cryptography
Privacy Policy
Unintended Data Leakage
Location tracking
Insufficient Transport Layer Protection
Poor Authorization & Authentication
Privacy Policy
Improper Session Handling
Client-Side Injection
Insufficient Transport Layer Protection
Broken Cryptography
Weak Server Side Controls
Poor Authorization and Authentication
Insecure Data Storage

Figure 7.11: Summary of Result for Test Case B

Table 7.3 describes a summary of the affected areas based on the consumer factors they affect. This summary aids to identify the major and weak areas affected within the Test Case B. Through this may rectification process begin to improve the security of the fitness tracker and it associated application.

Table 7.3: Summary of Affect Areas for Test Case B

Consumer Factor	Description	Vulnerabilities Discovered
Authentication	As consumer health data is accessed, managed or viewed there needs to be authentication procedures of identifying a user. This is to ensure that the correct user is viewing the correct data.	One area out of four areas are affected
Authorization	As consumer health data is accessed, managed or viewed there needs to be authorization methods. Authorization differs to authentication as it identifies whether a user has appropriate rights to access a resource. This ensures that a low level user does not have admin rights.	One area out of five areas are affected
Availability	Consumer health data needs to be available to authorized users when requested. An authorized user should have the freedom to view their data when they desire.	Two areas out of six areas are affected
Confidentiality	As consumer health data is central to consumer health wearables. It is vital to keep this data secure and only revealing it to intended parties.	Two areas out of nine areas are affected.
Non-Repudiation	The assurance that someone cannot deny something (digital signature, time stamps, certificates). This is vital when updates are made. There needs to be assurance that any changes to software or hardware firmware is from the manufacturer.	Two area out of three areas are affected.
Integrity	When consumer health data is accessed or managed there is need to be assurance that it is not modified in transit or at rest. In case data is tampered, it can be identified.	Two areas out seven areas are affected.

7.5 UTILITY AND EFFICACY OF FRAMEWORK

The main of objective of this research is to develop a threat assessment framework to assess consumer health wearables and their associated applications. This was conducted to provide a basis of coverage to understand which vulnerabilities affect consumer health wearables. Through developing the Consumer Health Wearable Threat Assessment Framework, it is important to demonstrate the framework (*utility*) to assess the manner how the framework performs towards the intended environment (*efficacy*) (Hevner et al., 2004). Without this, the framework will only be a theorized assertion of utility that the artefact actually performs as intended without proof of this (Venable, Pries-Heje and Baskerville, 2016).

Through conducting the demonstration, it was discovered the Consumer Health Wearable Threat Assessment Framework was able to assess the test cases on how vulnerabilities affected the Authentication, Authorization, Availability, Confidentiality, Non-Repudiation and Integrity. Through demonstrating the framework, a comparison can be drawn from two fitness trackers and their associated applications (Table 7.4).

Table 7.4: Comparison of Test Cases

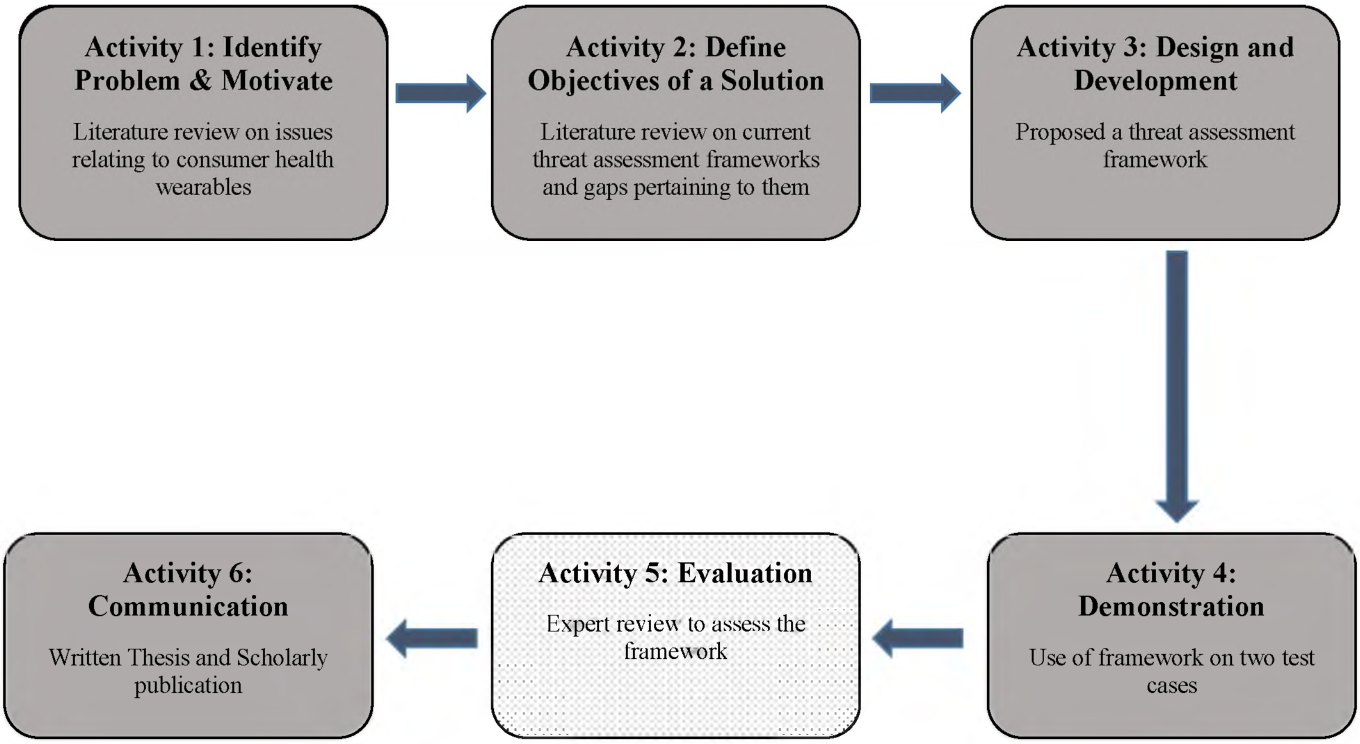
Consumer Factor	Description	Test Case A	Test Case B
Authentication	As consumer health data is accessed, managed or viewed there needs to be authentication procedures of identifying a user. This is to ensure that the correct user is viewing the correct data.	**Two** areas out of four areas are affected	**One** area out of four areas are affected
Authorization	As consumer health data is accessed, managed or viewed there needs to be authorization methods. Authorization differs to authentication as it identifies whether a user has appropriate rights to access a resource. This ensures that a low level user does not have admin rights.	**Two** areas out of five areas are affected	**One** area out of five areas are affected
Availability	Consumer health data needs to be available to authorized users when requested. An authorized user should have the freedom to view their data when they desire.	**Two** areas out of six areas are affected	**Two** areas out of six areas are affected
Confidentiality	As consumer health data is central to consumer health wearables. It is vital to keep this data secure and only revealing it to intended parties.	**Four** areas out of nine areas are affected.	**Two** areas out of nine areas are affected.
Non-Repudiation	The assurance that someone cannot deny something (digital signature, time stamps, certificates). This is vital when updates are made. There needs to be assurance that any changes to software or hardware firmware is from the manufacturer.	**Three** area out of three areas are affected.	**Two** area out of three areas are affected.
Integrity	When consumer health data is accessed or managed there is need to be assurance that it is not modified in transit or at rest. In case data is tampered, it can be identified.	**Two** areas out seven areas are affected.	**Two** areas out seven areas are affected.

Through this comparison of the test cases (Table 7.4) it supports the utility of the framework to assess consumer health wearables. Where more vulnerabilities pertaining to consumer health wearables were discovered in Test Cases A than in Test Case B. Through the assessment, the mitigation of these vulnerabilities can be directed based on the areas to which the vulnerabilities affect (Authentication, Authorization, Availability, Confidentiality, Non-Repudiation and Integrity). The demonstration of the framework, also supports the efficacy of the framework as the intended use was to assess consumer health wearable devices. From reviewing the summary of results from the test cases it is also noticeable that it correlates to the security concerns also described from literature. The vulnerabilities discovered such as Insufficient Transport Layer Protection, Location Tracking, Third-Party Analytics and Privacy Policies are factors that have been documented by various researchers (Barcena et al., 2014; Huckvale et al., 2015; Morera et al., 2016).

7.6 CONCLUSION

The main aim of this chapter was to demonstrate the Consumer Health Wearable Threat Assessment Framework. Through the demonstration vulnerabilities were discovered for both Test Case A and B. These vulnerabilities were mapped onto the Consumer Health Wearable Threat Assessment Framework to understand how the vulnerabilities affected the consumer wearables devices. It was finally reviewed the framework provides meets the objective of the research of utility and efficacy.

Chapter 8: EVALUATION OF FRAMEWORK


Activity 1: Identify Problem & Motivate
Literature review on issues relating to consumer health wearables
Activity 2: Define Objectives of a Solution
Literature review on current threat assessment frameworks and gaps pertaining to them
Activity 3: Design and Development
Proposed a threat assessment framework
Activity 4: Demonstration
Use of framework on two test cases
Activity 5: Evaluation
Expert review to assess the framework
Activity 6: Communication
Written Thesis and Scholarly publication

8.1 INTRODUCTION

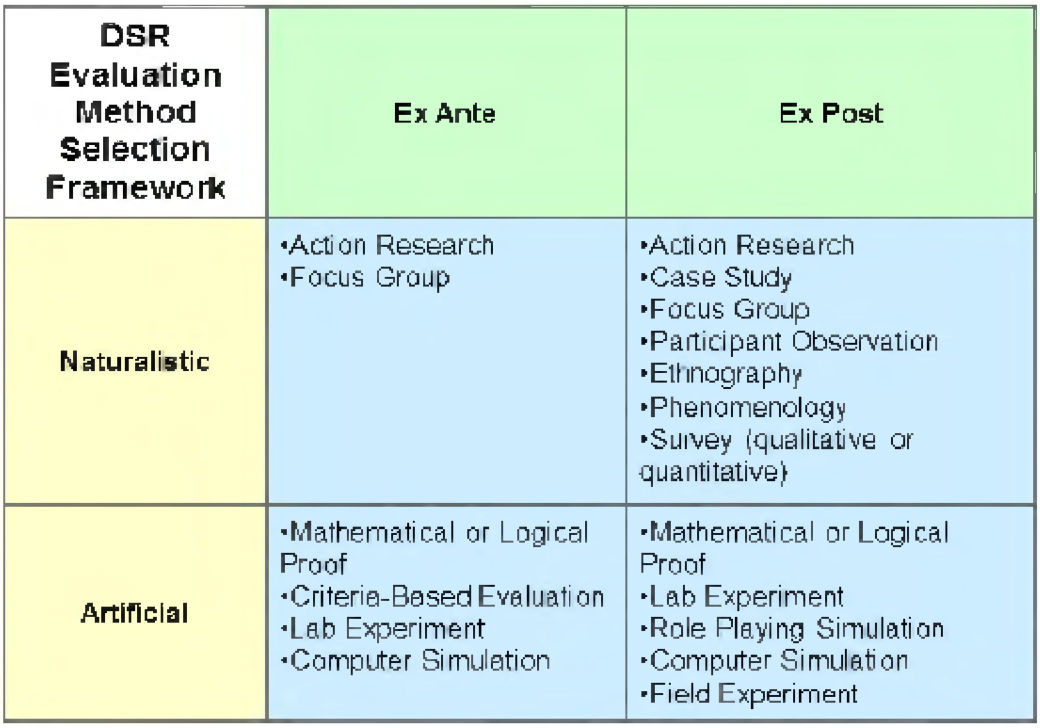
One of the important activities of the Design Science Research Process Model is evaluation of the designed artefact (Peffers et al., 2007). This is so, as without this element of evaluation, the designed artefact is only a theorized assertion of utility that the artefact actually performs as intended without proof of this (Venable et al., 2016)

One of the guidelines prescribed through evaluation of the designed artefact requires assessing the *utility, efficacy and quality* of the artefact (Hevner et al., 2004). Through applying the activities prescribed by Peffers et al. (2007) the evaluation was conducted in two phases. Phase one focused on the activity of demonstration of the framework in Chapter 7. This demonstration assisted to illustrate the *utility* of the framework by using the threat assessment on two tests cases. In addition, Chapter 7 also demonstrated the *efficacy* of the framework by illustrating the intended use of the framework by assisting to assess and guide the detection of security vulnerabilities with the two fitness trackers and their associated applications. Chapter 8 is centred on the second phase of the evaluation process by mainly assessing the *quality* of the framework, for providing a basis of coverage of the vulnerabilities affecting the consumer health wearable ecosystem. In addition, further evaluation components of *utility* and *efficacy* were also addressed in this chapter. This assisted to not only review the *quality* of the framework, but also to assess the usability and relevance of the framework based on expert opinion.

This chapter is therefore structured by firstly outlining the method (Section 8.2) used to evaluate the quality of the Consumer Health Wearable Threat Assessment Framework. This section will also describe the participants used to evaluate the framework and the procedure used. The following section of this chapter is centred on describing the results (Section 8.3) the participants gave with regard to the framework. Based from these results a discussion of the refinement (Section 8.4) of the framework is described. This refinement of the framework is important as it aids to enforce relevance and rigor of the intended use of contextualised environment of the Consumer Health Wearable Threat Assessment Framework. Chapter 8 will finally conclude (Section 8.5) by describing the final quality review of the framework and measure to which it is applicable.

8.2 METHOD OF EVALUATION

Different researchers have described the importance of evaluating artefacts and the manner in which it should be conducted (Hevner et al., 2004; Peffers et al., 2007; Helfert et al., 2012; Venable, Pries-Heje and Baskerville, 2012). The evaluation of an artefact can be described by a two-by-two framework (Figure 8.1) of the strategies for evaluation in Design Science Research (DSR).



DSR Evaluation Method Selection Framework	Ex Ante	Ex Post
Naturalistic	•Action Research •Focus Group	•Action Research •Case Study •Focus Group •Participant Observation •Ethnography •Phenomenology •Survey (qualitative or quantitative)
Artificial	•Mathematical or Logical Proof •Criteria-Based Evaluation •Lab Experiment •Computer Simulation	•Mathematical or Logical Proof •Lab Experiment •Role Playing Simulation •Computer Simulation •Field Experiment

Figure 8.1: Evaluation Framework (Venable et al., 2012)

The first two quadrants of the framework focus on the different time intervals to conduct the evaluation process; this can either be ex ante or ex post evaluation (Venable et al., 2012). Ex ante evaluation is conducted before the design and development phase of the artefact (Stefanou, 2001; Venable et al., 2012). This done as a predictive measure to assess the future impact the artefact will make on the intended environment. Ex post evaluation on the other hand is conducted after the artefact has been designed and developed (Klecun and Cornford, 2005). The aim of this evaluation process is to review the value of the developed artefact. Ex post evaluations can be regarded as summative evaluation episodes because they aid to measure the results of artefact (Venable et al., 2012).

The two other quadrants focus on the difference in which the evaluation process will be conducted; this can be naturalistic or artificial (Venable et al., 2012). Artificial evaluations are geared at creating imaginary or simulated settings to conduct the evaluation process. Artificial evaluations are beneficial for low cost scenarios and purely technical artefacts. Naturalistic evaluations on the other hand are beneficial to assess to the artefact effectiveness through diverse stakeholders (Venable et al., 2012).

For this research dissertation, the evaluation process is positioned as **ex post** as the goal is to mainly evaluate the quality of the developed artefact. This will help to review the value and relevance of the Consumer Health Wearable Threat Assessment Framework for providing a basis of coverage of vulnerabilities affecting consumer health wearables. In addition to this, the evaluation process is also positioned as a **naturalist** evaluation as security experts will assess the value and effectiveness of the framework. There are different methods provided by Venable et al. (2012) for conducting **naturalistic ex post** evaluation episodes; one method includes the use of surveys. A questionnaire using semantic differentials was used to perform the survey. Semantic differentials were the chosen instrument to conduct the survey as they aid to measure the meaning of concepts and also to derive the attitude towards the concept (Osgood, May and Miron, 1975). This aligns with goal of the evaluation method (Venable et al., 2012) as it will assist to assess the measure to which the Consumer Health Wearable Threat Assessment Framework conforms to the quality of industry standards and/or specifications based from expert opinion.

8.2.1 Evaluation Process

To conduct the evaluation process, Venable et al. (2016) provides a process for evaluation in Design Science Research. This process consists of four steps; explicate the goals of the evaluation, choose the evaluation strategy or strategies, determine the properties to evaluate and design the individual evaluation episodes (Venable et al., 2016).

<u>Step 1: Explicate the goals</u>: The goal of this evaluation process is to mainly evaluate the quality of the developed artefact through expert review, but through the evaluation process also aids to approve the utility and efficacy of the artefact from experts. This goal enforces rigor (Hevner et al., 2004) as it assess the degree to which the artefact is applicable for the intended environment based on theoretical knowledge applied to the framework.

Step 2: Choose a strategy or strategies for evaluation: Venable et al. (2016) outlines four possible strategies that can be used.

1. Quick and Simple: This is intended for small and simple designed artefacts where there is low social, technical risk and uncertainty.
2. Human Risk and Effectiveness: This is for major and big design artefacts that are social and user oriented. In addition, if the design artefact benefits real situations in the long run.
3. Technical Risk and Efficacy: This is for artefacts that are technically oriented and it is expensive to evaluate with real users and real systems in a real setting.
4. Purely Technical Artefact: These are for purely technical artefacts that will be used in the future.

The strategy chosen to evaluate the framework was the **quick and simple technique**. The framework is viewed to have a low social risk, technical risk and uncertainty. It has limited ethical considerations for human participants using the framework; there is low technical risk and uncertainty as the framework is used an assessment guide. The work of Venable et al. (2016) describes the **quick and simple technique** follows to perform few evaluation episodes. Where one evaluation episode is suitable to reach project summative conclusions (Venable et al., 2016). This research project, used one evaluation episode with the **quick and simple technique** as there is a limited time period to perform the evaluation results and reach project conclusions.

Step 3: Determine the properties to evaluate: The next step of the process focus on the element to evaluate. Different properties of the artefact can be evaluated which may include comprehensibility of the framework or reusability of the framework. For this evaluation process the property chosen for evaluation is quality. Where quality is defined as the pragmatic, semantic and syntactical use of the artefact for the intended environment (Helfert et al., 2012). This is so, as it gauges how the framework can be instantiated within the security domain specifically for consumer health wearables.

Step 4: Design the individual evaluation episode: This process focuses on designing the actual evaluation process. A framework can be described as the interrelation of concepts, texts, and systems used for solving a problems (Stamer, Zimmermann and Sandkuhl, 2016). The Information Quality Framework for Design Evaluation was chosen as the strategy for assessing the threat assessment framework. As its aids to assess how the interrelated components of the framework (construct) confirm to the quality standards and terminology within security and privacy. In addition, the property chosen to evaluate the Consumer Health Wearable Threat Assessment is *quality*. The Information Quality Framework for Design Evaluation by Helfert et al. (2012) was chosen to guide the quality assessment strategy.

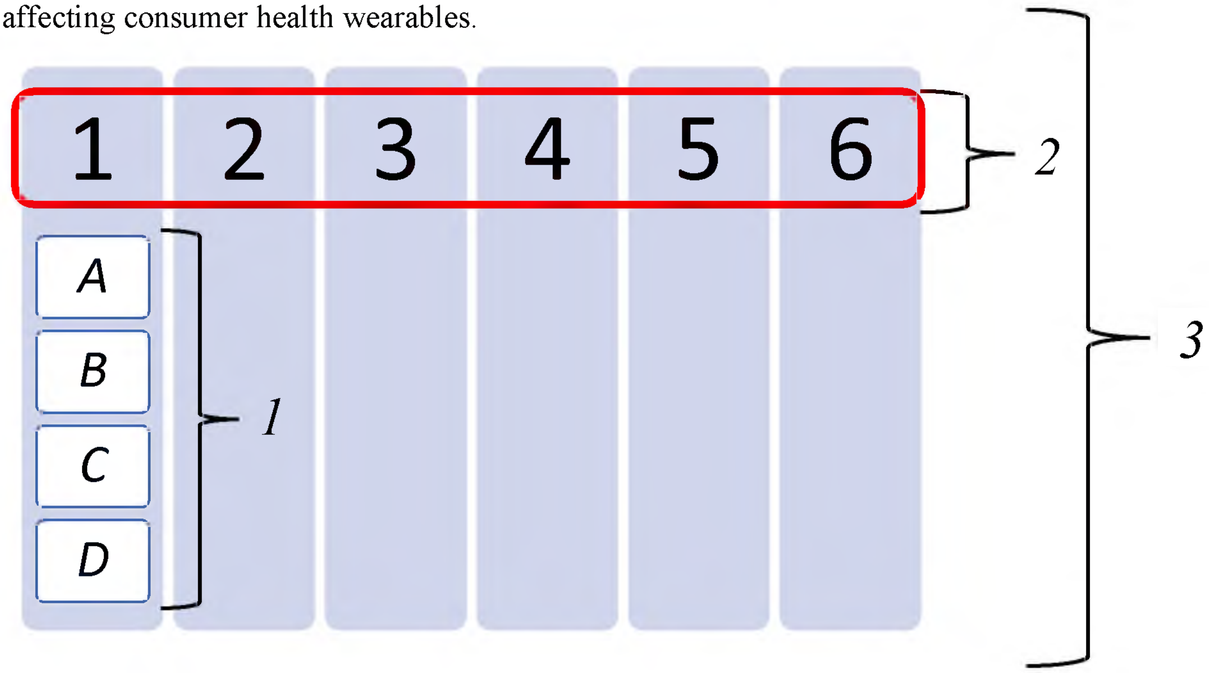
8.2.2 Quality Assessment Strategy

Helfert et al. (2012) provide an Information Quality Framework for Design Evaluation. This framework outlines three levels of semiotics (pragmatism, semantics and syntax) in the evaluation process of quality. These three levels assist to evaluate the design of artefacts to the degree to which they conform to quality standards and/or specifications to the contextualised environment (Helfert et al., 2012). The list of criteria of the three semiotic levels are identified in Table 8.1.

Table 8.1:Design Evaluation Framework (Helfert et al., 2012)

Semiotic Level	Example Criteria
Pragmatic	Relevance, usability, completeness, timeliness, actuality, efficiency
Semantic	Precise definitions and terminology, easy to understand, interpretability, accuracy (free-of error), consistent content
Syntax	Consistent and adequate syntax, syntactical correctness, consistent representation, accessibility

These semiotic levels (pragmatic, semantic and syntax) are deemed beneficial for the quality assessment for the Consumer Health Wearable Threat Assessment Framework as it aids to gauge the level to which the framework confirms to industry standards in the domain of security based on expert review. In addition, it measures the relevance and usability of the framework towards consumer health wearables and their associated mobile health applications. To apply the Information Quality Framework for Design Evaluation firstly requires to, understand the components of the Consumer Health Wearable Threat Assessment Framework. The Consumer Health Wearable Threat Assessment Framework is composed of three components which is outlined in Figure 8.2; the vulnerability list, the classification tiers in which the vulnerabilities are categorized to and the overall holistic framework. Component one, the vulnerability list consists of the fourteen vulnerabilities discovered (Section 6.1.2). Component two, the classification tiers include the six tiers of authentication, authorization, availability, confidentiality, non-repudiation and integrity (Section 6.1.1). In addition to these classification tiers, include the vulnerabilities classified within these categories. Finally, the third component is the overall framework which is a summation of the elements of coverage of the factors affecting consumer health wearables.



Component:

1: - Vulnerability assessment of factors affecting consumer health wearables

2: - Classification and category assessment

3: - Overall overview of the framework

Figure 8.2: Components of Threat Assessment Framework

To evaluate the threat assessment framework, each of these three components will need to undergo a quality assessment based from the Information Quality Framework for Design Evaluation. Each of these three components of the developed framework will be assessed on semiotic level of either pragmatism, semantic and syntax. Component one of the framework will focus on assessing the vulnerabilities affecting consumer health wearables. Component two of the framework will focus on assessing the classification tiers and the categorization of the vulnerabilities. Finally, Component three will focus to assess the entirety of the overall framework. Table 8.2 displays a summary of the quality factors assessed from each of the three components based on the semiotic levels.

Table 8.2: Application of Design Evaluation Framework

Component 1	Component 2	Component 3
Completeness (*Pragmatism*)	Completeness (*Pragmatism*)	Usability (*Pragmatism*)
Relevance (*Pragmatism*)	Relevance (*Pragmatism*)	Timely (Pragmatism)
Terminology (*Semantics*)	Terminology (*Semantics*)	Consistent Representation (*Syntax*)

Component 1: Vulnerability List Assessment

Component one focused on evaluating the vulnerabilities on completeness, relevance and terminology. Assessing the completeness of the vulnerability list is important, because it aids to understand the comprehensiveness of the factors affecting consumer health wearables. Secondly, the relevance of each of the vulnerabilities will be assessed to view the level to which they meet the contextualised environment of consumer health wearables. Thirdly, based on these vulnerabilities an assessment is required to gauge the terminology used based on industry standards. Therefore, the following three questions were formulated to perform a quality assessment of the vulnerability list:

1. To what extent is the vulnerability list comprehensive? This question focused to evaluate the completeness of the vulnerability list. This question is geared to the semiotic level of *Pragmatism.*
2. To what extent are the vulnerabilities relevant for consumer health wearables? This question focused to evaluate the relevance of the vulnerabilities. This question is geared to the semiotic level of *Pragmatism.*
3. To what extent is the naming convention correct? This question focused to evaluate the terminology used for the vulnerabilities. This question is geared to the semiotic level of *Semantics.*

Component 2: Classification and category evaluation

Component two is centred to evaluate the six classification tiers of Authentication, Authorization, Availability, Confidentiality, Non-Repudiation and Integrity. The criteria chosen to evaluate these classification tiers include; completeness, relevance and terminology. These criteria were chosen, as firstly, it gauges to identify the entirety of the tiers. Secondly, they gauge how relevant these classification tiers are towards consumer health wearables.

Thirdly, the precise terminology used for industry standards. Therefore, the following three questions were formulated to assess the quality for the classification tiers:

1. To what extent are the categories comprehensive? This question focused to evaluate the completeness of classification tiers. This question is geared to the semiotic level of *Pragmatism.*
2. To what extent are the categories relevant? This question focused to evaluate the relevance of the classification tiers. This question is geared to the semiotic level of *Pragmatism.*
3. To what extent were you able to understand the terms? This question focused to evaluate the terminology of the classification tiers. This question is geared to the semiotic level of *Semantics.*
4. To what extent were the correct terms used? This question focused to evaluate the terminology of the classification tiers. This question is geared to the semiotic level of *Semantics.*

The second evaluation process of this level focused on evaluating the category groupings of the vulnerabilities within the classification tiers. The criteria chosen to evaluate the categorization focused on terminology focusing on the accuracy of the classification. Therefore, the following question formulated to perform a quality assessment of the categorization of each of the tiers was:

1. To what extent are each of the vulnerabilities listed correctly categorised. This question is geared to the semiotic level of *Semantics.*

Component 3: Overall assessment of the framework

Component three is centred to evaluate the overall quality of the framework. As Component three is a summation of component one and two, this component was not measured on completeness, relevance and terminology. As the results from the previous components are assimilated to this component. It is inferred that if component one and two pass the quality assessment of completeness, relevance and terminology then it is expected the overall framework contains complete, relevant components with the correct terminology. Component three on the other hand focused to evaluate the usability, timeliness and consistent representation of the framework. Usability assesses the manner in which the framework is applicable in an organizational context. Secondly, timeliness gauges whether the framework is applicable in the current era of consumer health wearable. Thirdly, the consistent representation gauges the measure of the visual representation of the framework. Therefore, the following three questions were formulated to perform a quality assessment for the overall framework:

1. To what extent do you think this framework can be easily used in an organization context? This question focused to evaluate the usability of the framework. This question is geared to the semiotic level of *Pragmatism*. This question furthermore assists to evaluate the *utility* of the framework (Hevner et al., 2004) based on expert opinion.
2. To what extent is this a relevant framework for consumer health wearables? This question focused to evaluate the relevance of the Consumer Health Wearable Threat assessment framework. This question is geared to the semiotic level of *Pragmatism*. This question furthermore assists to evaluate the *efficacy* of the framework (Hevner et al., 2004) based on expert opinion.
3. To what extent were you able to understand the visual representation of the framework? This question focused to evaluate the consistent representation of the framework. This question is geared to the semiotic level of *Syntax*.

8.2.3 Participants

To perform the evaluation of the framework expert evaluation was used to assess the three components of the framework. Four experts (XP) within the domain of security were used to evaluate the quality of the framework. The security experts chosen came from different market sectors. This was beneficial as it provided different ideologies to review the framework. The biography of the experts is available from Table 8.3

Table 8.3: Biography of Security Experts

Expert	Occupation	Highest Qualification	Market Sector	Security Experience	Mobile Security Experience
XP 1	Cyber Security Analyst	Honours: Information Systems	Finance	3 years	3 years
XP 2	Information Security Consultant	Honours: Computer Engineering	Information Security	3 years	3 years
XP 3	Information Security Consultant	Honours: Computer Engineering	Information Security	1 year	1 year
XP 4	Researcher	Honours: Information Technology	Security Researcher	10 years	3 years

8.2.4 Procedure of evaluation

The assessment of the framework was conducted through interviews. The interview was conducted by using a questionnaire where each participant needed to respond based on semantic differentials. A seven-point semantic differential scale was used and experts were required to justify their rating for each question. Review of the questionnaire is available from Appendix B. The evaluation process was conducted by:

1. Experts detailing their biography information
2. Reviewing the additional information (Appendix C). This additional information included the name of each vulnerability and a description of the vulnerability. In addition, the Consumer Health Wearable Threat Assessment Framework
3. Evaluating each component of the Consumer Health Wearable Threat Assessment Framework from the semantic differential scale
4. Justifying the reason of their opinion from the semantic differential scale

8.3 RESULTS

8.3.1 Vulnerability Assessment Results

Question 1: To what extent is the vulnerability list comprehensive?

The bipolar ordinal scale used for this question was *not at all comprehensive* (with a score of 1) *to very comprehensive* (with a score of 7). The average score given towards the comprehensiveness of the vulnerability list by experts was 6.3. This result approves the vulnerability list as very comprehensive towards consumer health wearables. All four experts confirmed the fourteen vulnerabilities were very comprehensive and complete. XP 1 mentioned, "*this was a very comprehensive list especially for mobile health applications. With their experience with dealing with threats if all the controls are covered the application will be very secure.*"

Question 2: To what extent are the vulnerabilities relevant for consumer health wearables?

The bipolar ordinal scale used for this question was *not relevant* (with a score of 1) to *very relevant* (with a score of 7). On average from the results obtained of relevance it is deduced that all experts view the vulnerabilities as relevant towards consumer health wearables. Each vulnerability had an average relevance of 3.5 and higher (Figure 8.3). This implies that the experts view these vulnerabilities towards consumer health wearables as relevant.

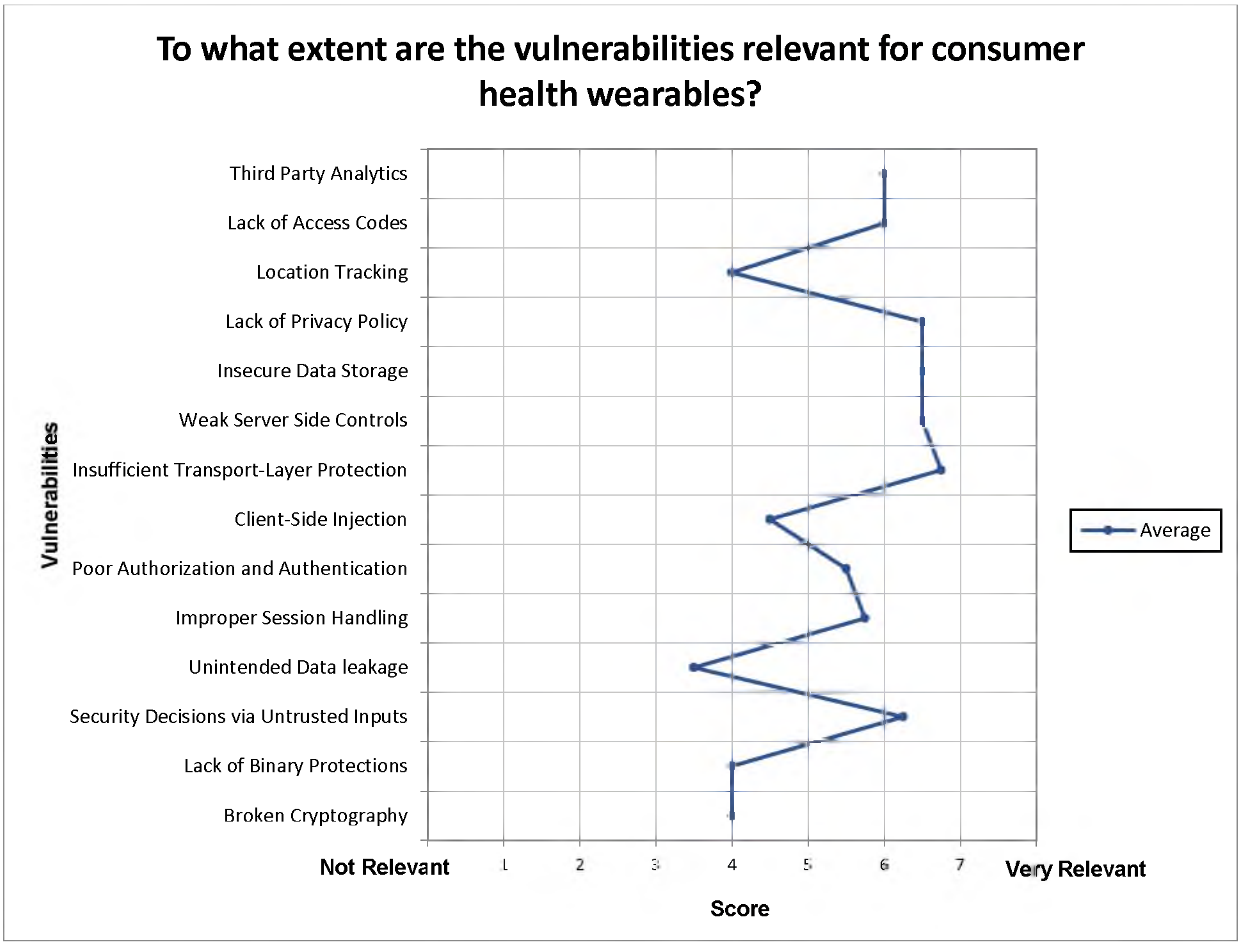


Figure 8.3: Average results of relevance of vulnerabilities

From the assessment given from the experts the vulnerability deemed least relevant was Unintended Data Leakage with an average score of 3.5 (Figure 8.3). XP 2 and XP 3 both considered this was not a relevant vulnerability specifically if the focus was on the mobile device. As the data leakage is very minimal on software or hardware changes, to cause any data loss. However, on the server side this vulnerability would pose as a threat, but it would not be likely. The most relevant vulnerability considered by experts was Insufficient Transport-Layer Protection (Figure 8.3). All experts confirmed this as a relevant vulnerability within the consumer health wearable environment. Especially, due the fact health data is transferred between a health wearable device to the mobile device and finally to cloud servers extensively it was therefore important to ensure the appropriate controls are in place. The average responses given to the other vulnerabilities are as follows:

1. Third Party Analytics: All experts considered this as relevant vulnerability affecting consumer health wearables. Especially due the numerous analytical cloud servers consumer health wearables and their associated applications connect to. This vulnerability had an average score of 6.
2. Lack of Access Codes: This vulnerability had an average score of 6. XP 4 mentioned that currently very few consumer wearables have few access codes to protect them and is still yet to find "*a fitness tracker with proper protection.*" The opinion of the experts was that this was the norm of these devices presently due to physical structure limiting them to have adequate access codes.
3. Location Tracking: All experts considered this is an issue and this vulnerability had an average score of 4. XP 2 mentioned, "*with all the array and growth of Bluetooth it is will be difficult to pinpoint the actual device, but it is a pertinent issue. Many portable devices currently emit Bluetooth signals such as headphones, cars and cell phones.*"
4. Lack of Privacy Policy: All experts believe this is a very relevant issue, this vulnerability had an average score of 6.5. XP 3 mentioned "*specifically in South Africa with the POPI Act. It is very important for health related devices to state how they will handle data.*"
5. Insecure Data Storage: All experts believed this was a very relevant vulnerability with an average score of 6.5. XP 4 mentioned "*well this should be the main objective. They are collecting health data; it needs to be stored properly.*"
6. Weak Server Side Controls: All experts believed this was a very relevant vulnerability with an average score of 6.5. XP 1 specifically mentioned, "*this was very important especially for updates on devices.*"
7. Client-Side Injection: Experts saw this vulnerability as relevant, but only to a certain degree. This vulnerability had an average score of 4.5. XP 1 believes this is a very relevant vulnerability for the mobile device. XP 2, XP 3 and XP 4 also believe this is a

relevant vulnerability, however, they believe an attacker getting to this level is difficult on a mobile device on the inbuilt database if the health data is store on board. XP 4 mentioned, "*attackers would be more interested to attack the server side than the client side to attain the health data of all users.*"

8. Poor Authorization and Authentication: All experts agreed that this was a relevant vulnerability with an average score of 5.5. However, XP 2 and XP 3 believed this was dependant on the security measures the phone had. XP 2 mentioned, "*the mobile health application should not only be reliant on the lock screen pattern or biometric scanner to lock the phone. Such measures possibly be in place for mobile health applications and left for third-party manufactures of the device.*"
9. Improper Session Handling: This vulnerability had an average score of 5.8. XP 1, XP 3 and XP 4 all considered this as a relevant vulnerability. However, XP 2 considered this was only relevant if the session token was poorly implemented such the session token could be predicted and stored on board the mobile device.
10. Security Decisions via Untrusted Inputs: This vulnerability had an average score of 6.3. All experts viewed this as a pertinent threat towards consumer health wearables, especially in the manner to which they communicate with other applications.
11. Lack of Binary Protections: This vulnerability had an average score of 4. All experts viewed that this vulnerability was relevant to a certain degree. Both XP 1 and XP 2 described this vulnerability is dependent on whether if the attacker is able to understand how the legitimate application communicates with it servers.
12. Broken Cryptography: This vulnerability had an average score of 4. All experts saw this vulnerability as somewhat relevant especially if any data was stored offline. "*An attacker will need the physical device to crack the hashes*" XP 1, XP 2 and XP 4 mentioned.

Question 3: To what extent is the naming convention correct?

The bipolar ordinal scale used for this question was *poor naming convention* (with a score of 1) to *excellent naming convention* (with a score of 7). On average from the results obtained of terminology it is deduced that all experts confirm and consider the correct terminology is used for the vulnerabilities based on industry standards. Each vulnerability had an average terminology score of 4.5 and higher (Figure 8.4).

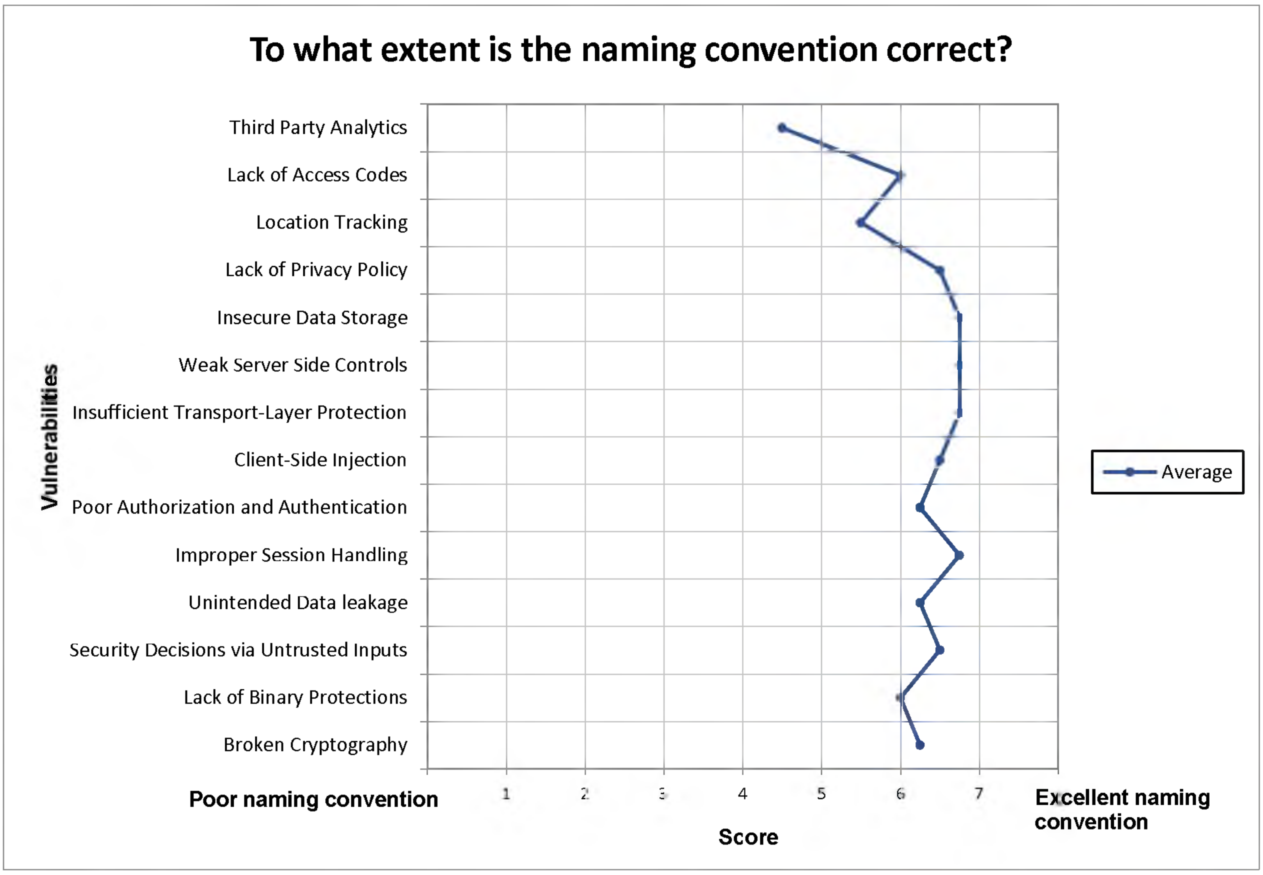


Figure 8.4: Average results of appropriate terminology used for vulnerabilities

From the assessment given from the experts the vulnerability deemed with the least correct naming convention used was Third Party Analytics. This had an average score of 4.5. XP 3 mentioned, "*to an outside individual the name doesn't state exactly what the vulnerability is.*" It was suggested to possibly change the vulnerability name to *poor use of third-party analytics*. On average all experts viewed the naming convention used for the vulnerabilities was correct, with XP 1 and XP 4 both mentioning that, "*they align with industry standards.*" However, they were a few exceptions where the security experts felt the naming conventions could be improved. These vulnerabilities include; Location Tracking, Poor Authorization and Authentication, Unintended Data Leakage.

1. Location tracking: XP 1 suggested to possibly change to *"poor location privacy"*
2. Poor Authorization and Authentication: XP 2 mentioned "*the use of the word poor was too strong*" he suggested changing the name to "*improper authorization and authentication"*
3. Unintended Data Leakage: XP 4 suggested a possible change to "*unintended data leakage and emissions."* This is so as the emissions of data has been identified for this vulnerability in certain cases.

8.3.2 Classification Assessment Results

Question 1: To what extent are the categories comprehensive?

The bipolar ordinal scale used for this question was *not at all comprehensive* (with a score of 1) to *very comprehensive* (with a score of 7). The average score given towards the completeness of the classification tiers was 7. This result supports the classification tiers as very complete towards consumer health wearables. XP 3 mentioned, "*the classification tiers are very comprehensive and important for consumer health wearables."*

Question 2: To what extent are the categories relevant?

The bipolar ordinal scale used for this question was *not relevant* (with a score of 1) *to very relevant* (with a score of 7). The average score given towards the relevance of the classification tiers was 6.5. This result supports the classification tiers as relevant towards consumer health wearables. All experts considered the classification tiers were very relevant. XP 1 mentioned, "*these categories are all important for consumer health wearables."*

Question 3: To what extent were you able to understand the terms?

The bipolar ordinal scale used for this question was *not understandable* (with a score of 1) to *completely understandable* (with a score of 7). The average score given towards the comprehensibility (*terminology*) of the classification tiers was 7. This result supports the classification tiers as comprehensible to users of the framework. All experts said they fully understood the term and did not have issues. XP 3 specifically mentioned, "*these are terms we occasionally use in the workplace so it was not difficult to understand.*"

Question 4: To what extent were the correct terms used?

The bipolar ordinal scale used for this question was *poor naming convention* (with a score of 1) to *excellent naming convention* (with a score of 7). The average score given towards the terminology of the classification tier was 7. It is deduced that all experts confirm and consider the correct terminology is used for the classification tiers based on industry standards. All experts believed the correct terms were used. XP 1 mentioned, "*these are terms we use in the security domain*"

8.3.3 Category Grouping Assessment Results

Question: To what extent are each of the vulnerabilities listed correctly categorized?

The bipolar ordinal scale used to assess the categorisation of the vulnerabilities for each classification tier was *incorrectly categorised* (with a score of 1) to *correctly categorised* (with a score of 7).

Tier 1: Authentication

The average score given towards the categorisation of the vulnerabilities towards authentication was 6.8. From the assessment all experts viewed the vulnerabilities affecting authentication were correctly categorized. XP 4 mentioned, "*these are all factors that can affect authorization.*"

Tier 2: Authorization

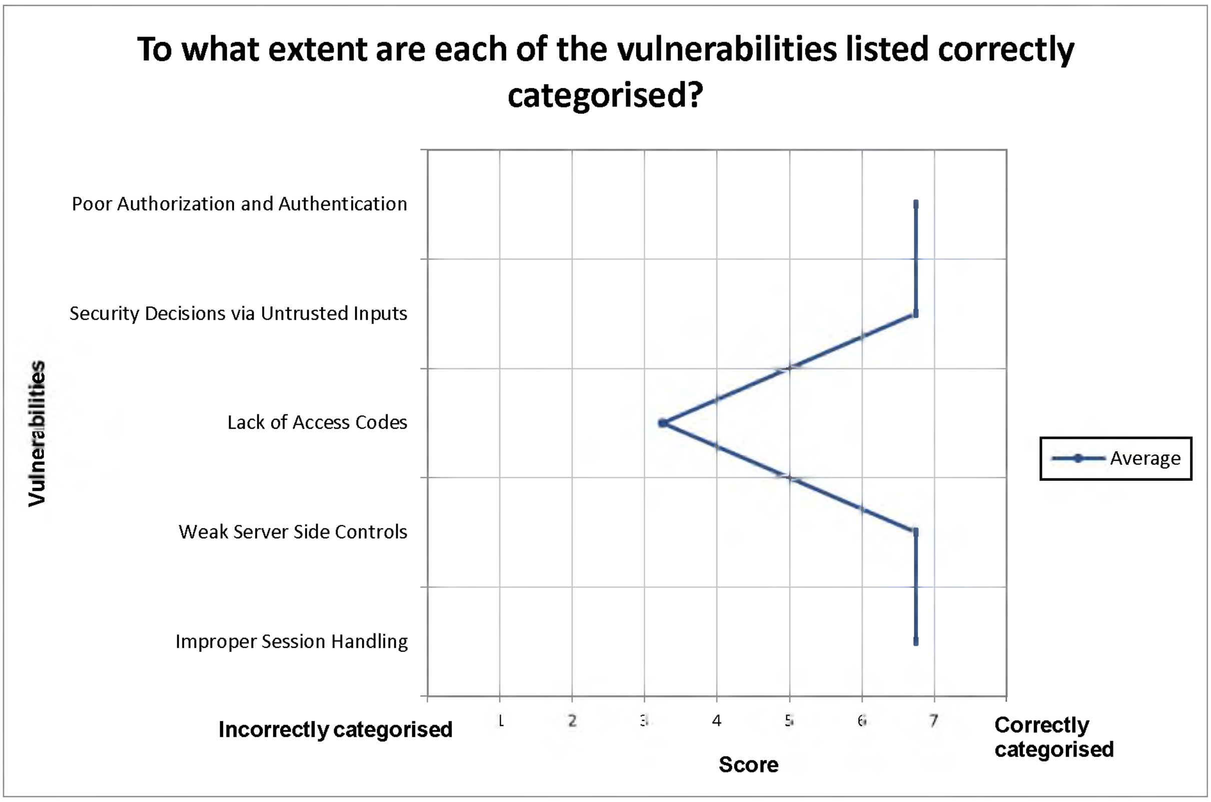


Figure 8.5: Average results of appropriate categorisation towards authorization

All experts viewed the vulnerabilities affecting authentication were correctly categorized each having an average score of 6.8 (Figure 8.5), apart from lack of access of codes. The vulnerability with the lowest score of 3.4 was lack of access codes for its categorization towards authorization. XP 2 and XP 3, viewed this vulnerability as not a pertinent issue for authorization. Authorization differs to authentication as it identifies whether the authenticated user has the appropriate rights to access a resource. XP 2 and XP 3 both described as currently they are not different levels of users who connect to a singular consumer health wearable device. The lack of access codes is not a pertinent issue currently for authorization.

Tier 3: Availability

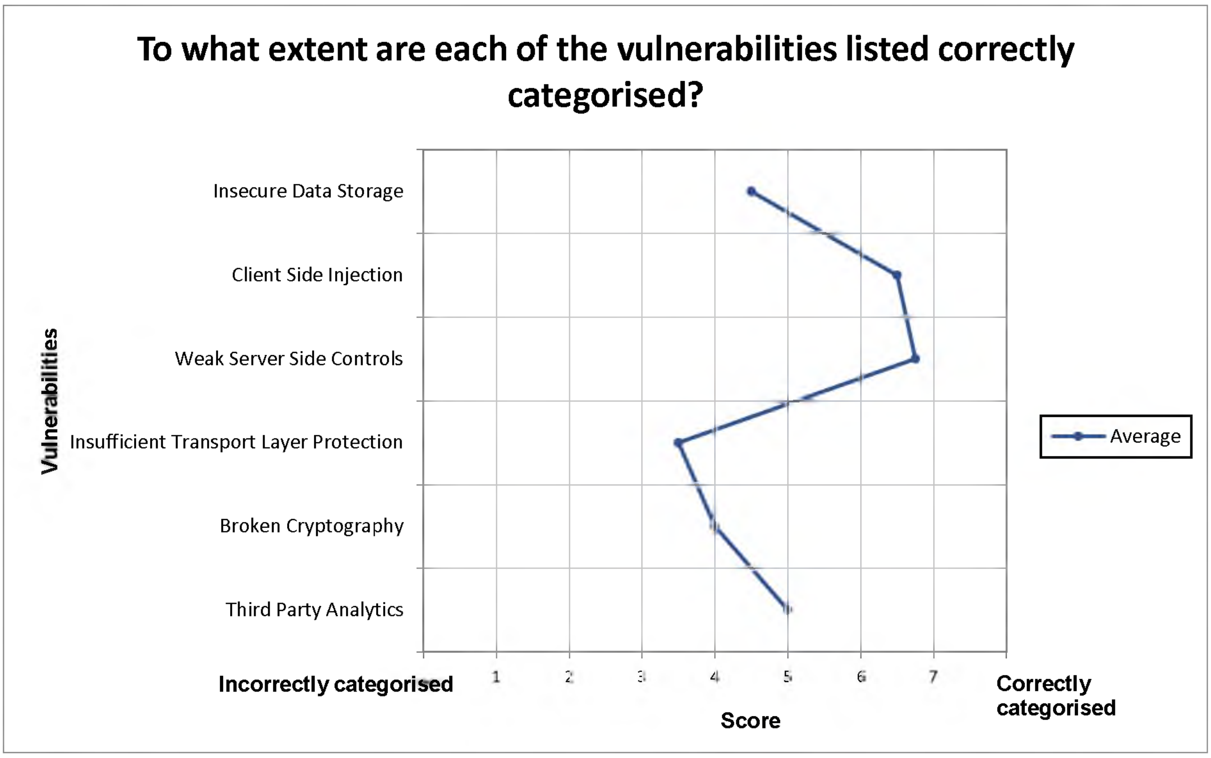


Figure 8.6: Average results of appropriate categorisation towards availability

The responses given for the vulnerabilities affecting the tier of availability varied. On average nonetheless, experts believe the vulnerabilities were correctly categorised. The highest vulnerability considered correctly categorised was weak server side controls with an average score of 6.5 (Figure 8.6). XP 1 and XP 3 both described that if this vulnerability is not handled correctly, it will tamper the availability of data. Especially for insurance companies. XP 4 added on this, "*the vulnerabilities affecting availability will depend on how you view the importance from either upstream or downstream. From a user's perspective, a few minutes of not being able to see how many steps I made may not be important. For an insurance company, this is major!*" The vulnerability with the lowest score of 3.5 was insufficient transport layer protection. XP 3 viewed this vulnerability as not directly affecting the availability of health data. XP 3 described not having the appropriate measures of transport layer protection may still allow a user to obtain their data. XP 3 described it will depend on the intent of the attacker.

Tier 4: Confidentiality

The average score given towards the categorisation of the vulnerabilities towards confidentiality was 6.8. From the assessment all experts viewed the vulnerabilities affecting confidentiality were correctly categorized. XP 1 iterated that of the important factors was privacy policies, *"In South Africa ensuring the privacy policy abides to standards will be very important with the POPI act coming in place"*

Tier 5: Non-Repudiation

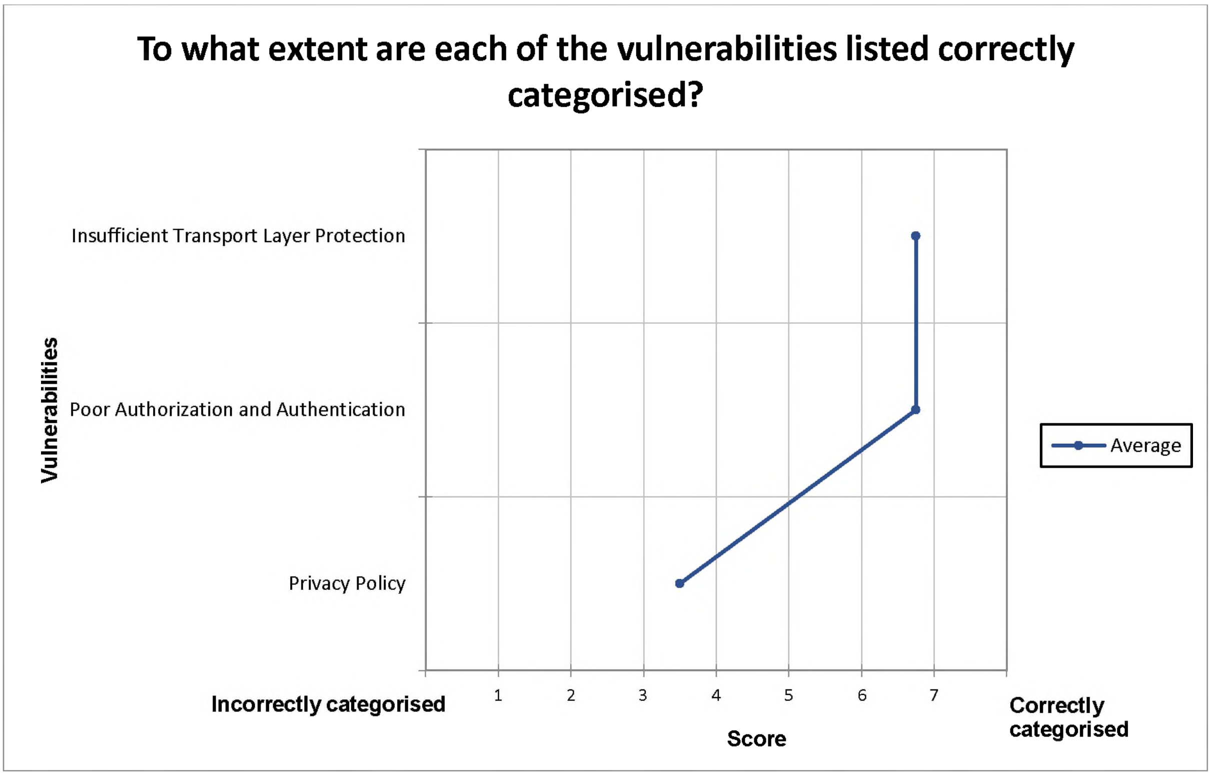


Figure 8.7: Average results of appropriate categorisation towards non-repudiation

All experts viewed the vulnerabilities affecting non-repudiation were correctly categorised and there was an average score of 6.8 apart from the vulnerability of privacy policy. This vulnerability had an average score of 3.5 (Figure 8.7). XP 2 and XP 3 viewed policies are not a vulnerability that affect non-repudiation directly. This is so as non-repudiation focuses on the assurance and authenticity of someone sending information. XP 2 and XP 3 both viewed that privacy policies assist to state the manner in which information will sent, but it does not give the assurance and authenticity explicitly. XP 1 and XP 4 on the other hand viewed that privacy policies were important for manufactures to state how information was to be sent to users as this gives assurance legally to the users in the manner in which it will sent.

Tier 6: Integrity

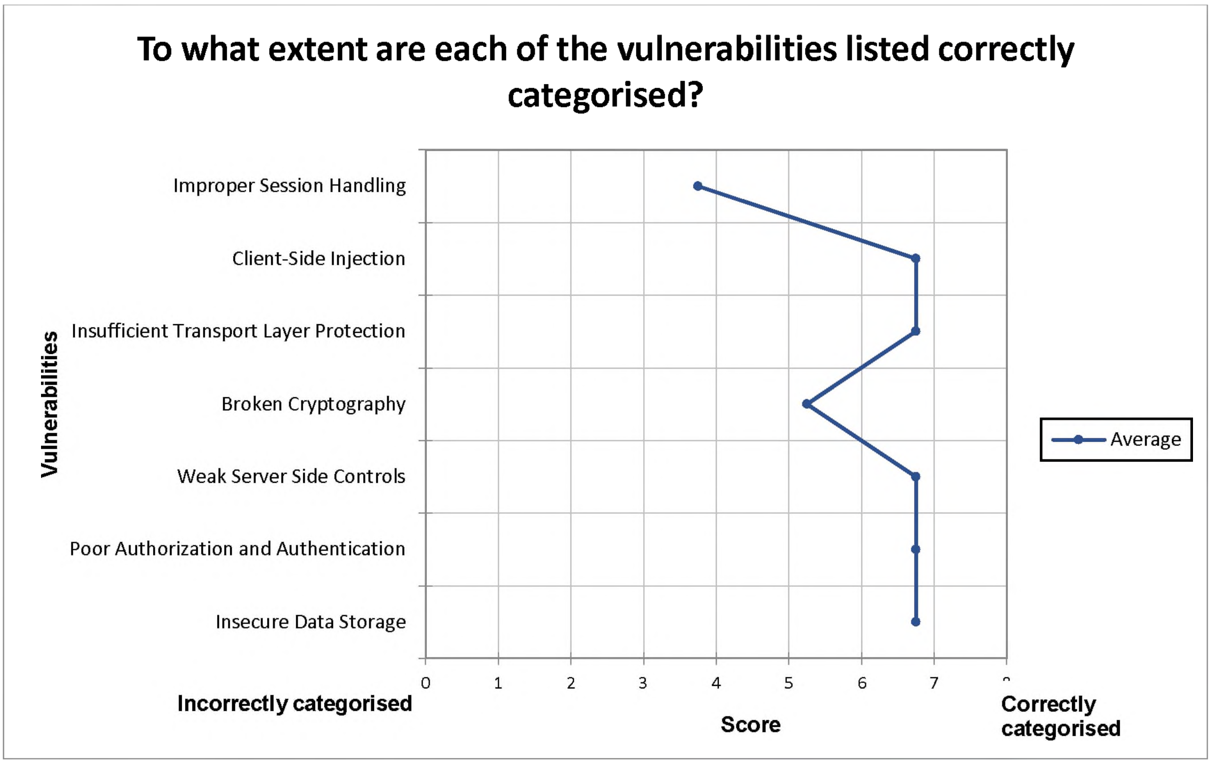


Figure 8.8: Average results of appropriate categorisation towards integrity

The responses given for the vulnerabilities affecting the tier of integrity varied. On average, experts believe the vulnerabilities were correctly categorised with each vulnerability having a score of 3.8 and higher (Figure 8.8). The highest vulnerabilities considered correctly categorised were client-side injection, insufficient transport layer protection, weak server side controls, poor authorization and authentication and insecure data storage each having an average score of 6.8. The vulnerability with the lease score of 3.8 was improper session handling. XP 2 and XP 3 both considered this vulnerability of improper session handling did not directly impact the integrity of the health data. Both XP 2 and XP 3 described whether or not session tokens were not appropriately correctly handled would not tamper the integrity of health data directly. This vulnerability was dependant on the intent of the attacker in the manner in which they wanted to tamper to the integrity if there was improper session handling.

8.3.4 Overall Framework Assessment Results

<u>Question 1:</u> To what extent do you think this framework can be easily used in an organizational context?

The bipolar ordinal scale used for this question was *not easy to use* (with a score of 1) to *very easy to use* (with a score of 7). The average score given by experts was 6.3. All experts believe the framework can be used in an organizational context. XP 2 mentioned, "*It is a nice framework to review applications and how they measure up.*" XP 3 mentioned, "*It is straightforward and conveys which factors affect which tier.*"

<u>Question 2:</u> To what extent is this a relevant framework for consumer health wearables?

The bipolar ordinal scale used for this question was *not relevant* (with a score of 1) to *very relevant* (with a score of 7). The average score given by experts was 6.3. All experts believed it was a relevant framework for consumer health wearables as it displayed vulnerabilities that directly impacted the environment. XP 1 mentioned, "*the vulnerabilities are relevant and the tiers showed in the framework are relevant. Fitness trackers are growing, and this framework shows what to look out for.*"

<u>Question 3</u>: To what extent were you able to understand the visual representation of the framework?

The bipolar ordinal scale used for this question was *unable to understand* (with a score of 1) to *completely understood* (with a score of 7). The average score given by experts was 6.8. All expert felt they understood the visual representation of the framework and did not have any issues. XP 4 mentioned "*I like the way how you have taken complex terms and vulnerabilities and displayed them with simplicity!*"

8.4 REFINEMENT OF FRAMEWORK

To ensure the Consumer Health Wearable Threat Assessment Framework is applicable for the intended environment, an alignment based from expert review needs to be met. From conducting the evaluation of the framework, XP1, XP2 and XP4 had a few refinements in which to improve the framework, these are outlined from Figure 8.9. This refinement of the framework is within three distinct categories: Terminology, Categorization Additions, Categorization Grouping.

Terminology

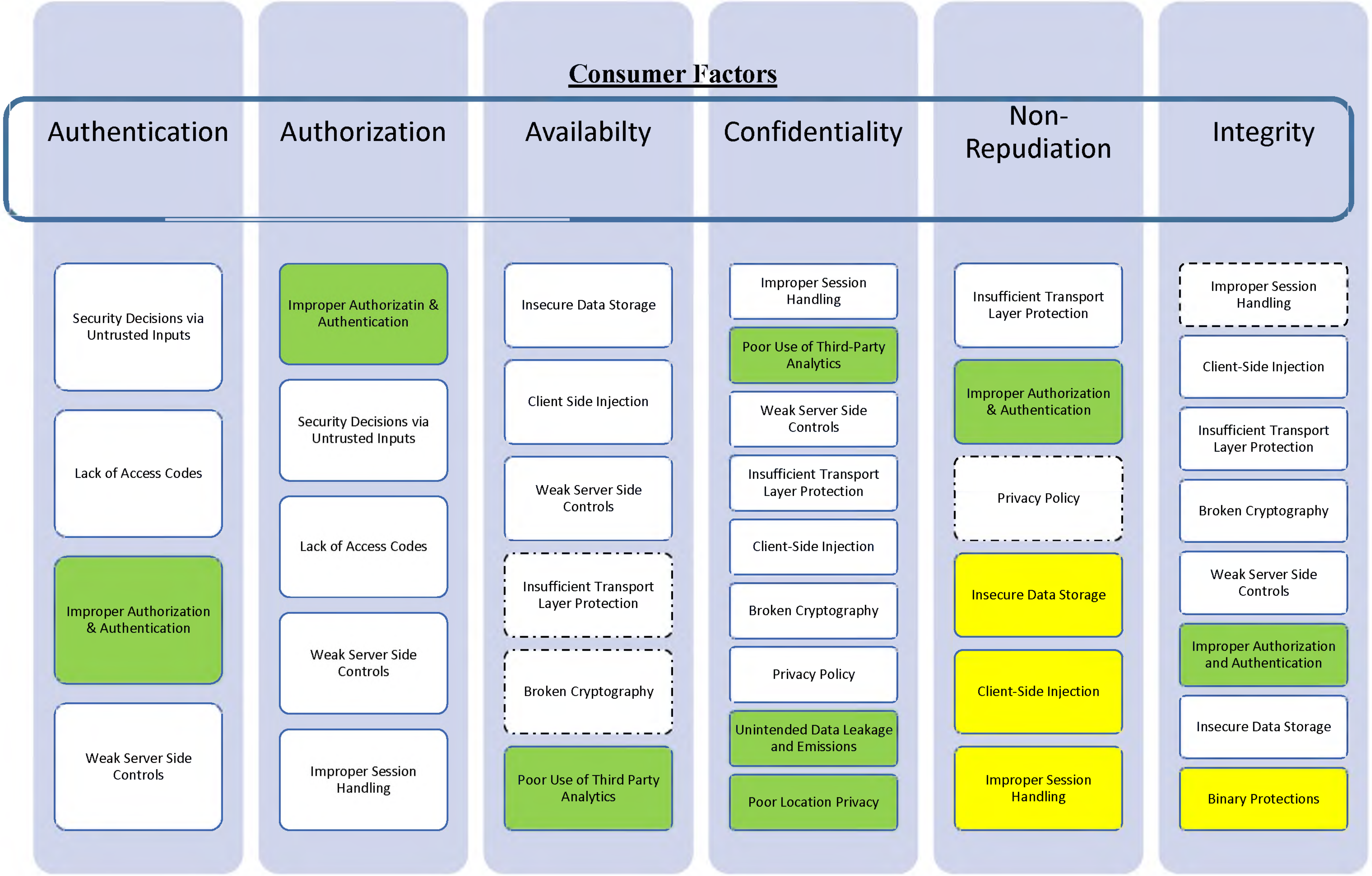
From the vulnerability list assessment experts mentioned and suggested name changes to better convey the vulnerabilities towards consumer health wearables. These name suggestions include; Poor Use of Third Party Analytics, Poor Location Privacy, Improper Authorization and Authentication and Unintended Data Leakage and Emissions. These changes are highlighted in green.

Categorization Additions

XP 1 and XP 2 believed it was important to include Improper Session Handling towards the classification tier of Non-Repudiation. This is so as updates are sent from the server side, it is important to protect the session so as man-in-the-middle attacks may not be utilised. XP 4 also believed it was important to include Insecure Data Storage and Client-Side Injection to Non-Repudiation. XP 4 also believed it was important to include Lack of Binary Protections to the classification tier of Integrity. This is so as any reverse engineering of the application can hinder the integrity of the application. These additions to the threat assessment are highlighted in yellow.

Categorization Groupings

From conducting the category grouping assessment, some vulnerabilities were viewed not to be correctly categorised. These vulnerabilities were viewed to have a lesser importance to the category they were grouped to. Therefore, these vulnerabilities have been outlined with a dotted line. These vulnerabilities, include Insufficient Transport Layer Protection and Broken Cryptography for Availability and Privacy Policies for Non-Repudiation.



Consumer Factors

Authentication

- Security Decisions via Untrusted Inputs
- Lack of Access Codes
- Improper Authorization & Authentication
- Weak Server Side Controls

Authorization

- Improper Authorizatin & Authentication
- Security Decisions via Untrusted Inputs
- Lack of Access Codes
- Weak Server Side Controls
- Improper Session Handling

Availabilty

- Insecure Data Storage
- Client Side Injection
- Weak Server Side Controls
- Insufficient Transport Layer Protection
- Broken Cryptography
- Poor Use of Third Party Analytics

Confidentiality

- Improper Session Handling
- Poor Use of Third-Party Analytics
- Weak Server Side Controls
- Insufficient Transport Layer Protection
- Client-Side Injection
- Broken Cryptography
- Privacy Policy
- Unintended Data Leakage and Emissions
- Poor Location Privacy

Non-Repudiation

- Insufficient Transport Layer Protection
- Improper Authorization & Authentication
- Privacy Policy
- Insecure Data Storage
- Client-Side Injection
- Improper Session Handling

Integrity

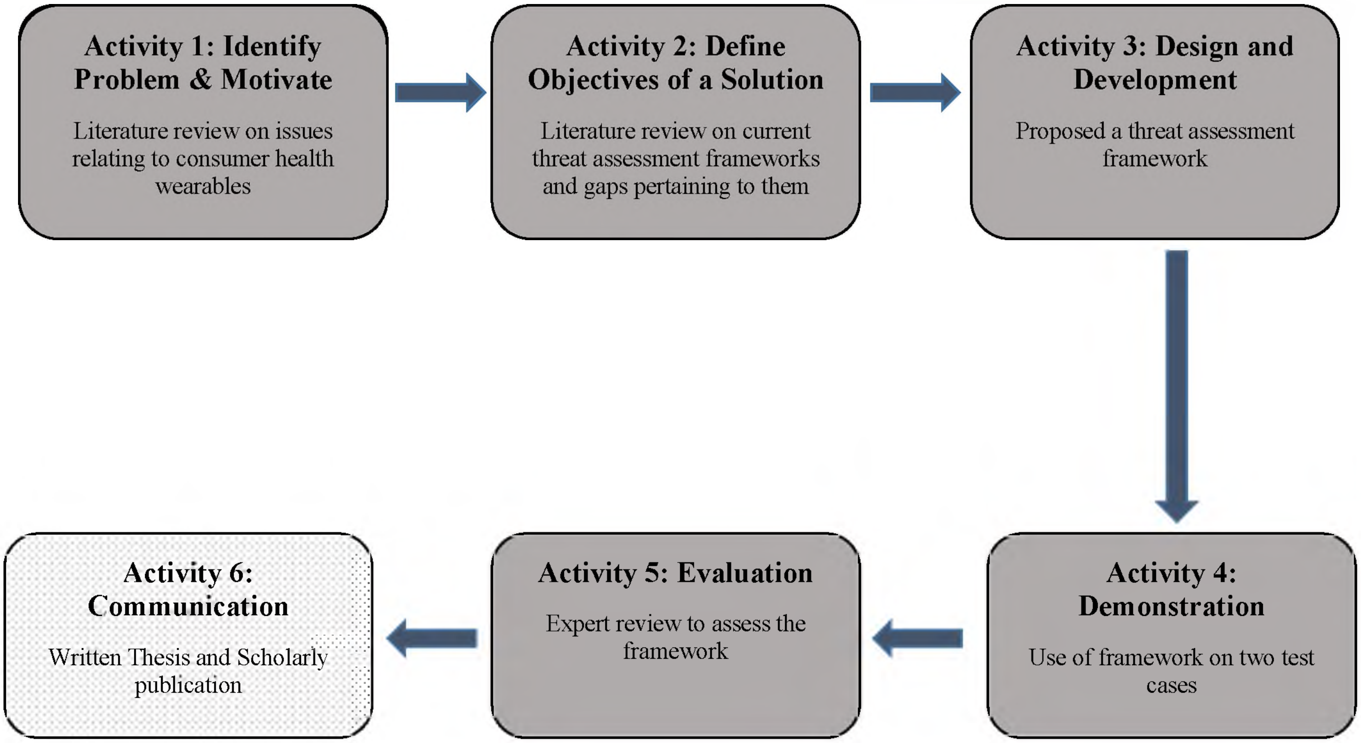
- Improper Session Handling
- Client-Side Injection
- Insufficient Transport Layer Protection
- Broken Cryptography
- Weak Server Side Controls
- Improper Authorization and Authentication
- Insecure Data Storage
- Binary Protections

Figure 8.9: Refined Threat Assessment Framework

8.5 CONCLUSION

This chapter focused on performing a quality assessment of the framework based on the Information Quality Framework for Design Evaluation by Information Quality Framework for Design Evaluation. Based on the results obtained from security professionals it was identified that security experts view the framework as a relevant, complete framework specifically for consumer health wearables. In addition to this, experts described the ease of use of the framework, especially by condensing pertinent vulnerabilities in a simplified format. Based on these results, it can be viewed the Consumer Health Wearable Threat Assessment Framework offers a basis of coverage for the vulnerabilities in this environment.

Chapter 9: CONCLUSION


Activity 1: Identify Problem & Motivate
Literature review on issues relating to consumer health wearables
Activity 2: Define Objectives of a Solution
Literature review on current threat assessment frameworks and gaps pertaining to them
Activity 3: Design and Development
Proposed a threat assessment framework
Activity 4: Demonstration
Use of framework on two test cases
Activity 5: Evaluation
Expert review to assess the framework
Activity 6: Communication
Written Thesis and Scholarly publication

9.1 INTRODUCTION

This final chapter focuses to summarise and communicate the results with reference to the research questions to meet the research objective. The chapter begins from outlining how the research objective was achieved (Section 9.2). This chapter will also discuss the theoretical contribution (Section 9.3) made through undertaking this research project. In addition, the practical contribution created (Section 9.4). The limitation of the research study will also be discussed in Section 9.5 with a further discussion on future research (Section 9.6) that can be conducted to improve the contextualised domain.

9.2 ACHIEVEMENT OF RESEARCH OBJECTIVES

The objective of this research was to develop a threat assessment framework that can be used to assess health applications as this first and low cost approach for good security practice (Sanzgiri, 2013). Through developing a threat assessment framework, a basis of coverage can be provided to understand the vulnerabilities towards the consumer health wearable ecosystem. This objective was met by answering the main research question:

What are the components of a threat assessment framework for determining privacy and security vulnerabilities in consumer health wearables?

To attain the objective the Design Science Research Process model by Peffers et al. (2007) was used. This process model assisted the researcher to achieve this objective through four research questions. RQ1 - '*What health data do consumer health wearables collect and store?*' This research question helped to firstly understanding the contextualised environment of consumer health data. This question was answered in Chapter 3 where it was discovered, that consumers are people who collect health data outside the confines of a medical setting to improve their physical wellness. The type of health data collected in this ecosystem are referred as consumer health data. During the research study the prominent technology driving consumer health was fitness trackers. These devices prominently collect three categories of consumer health data to guide an individual. These categories include physical activity data, consumption data and physiological data. These categories do not exist insolation, but are used to create relationships between data tables so as to assist a consumer to a healthier lifestyle.

Chapter 4 focused on answering, RQ2 - '*What vulnerabilities are associated with the consumer health wearable ecosystem?*' This chapter firstly discovered to understand the ecosystem of consumer health wearables used to assist to collect consumer health data. Based from this ecosystem, fourteen vulnerabilities were discovered that affect this environment. These vulnerabilities were discovered from literature and from the OWASP Top 10 mobile security threats which correlate to the consumer health wearable ecosystem. It was further discovered that these vulnerabilities affect the manner in which consumers can manage, access and share their data within a secure environment.

Chapter 5 was centred on answering RQ3 - '*What threat assessment components should be incorporated into a threat assessment framework for consumer health wearables?*' This question was answered by discovering existing theoretical security threat assessment frameworks and how they assist towards providing a basis of coverage for assessment towards consumer health wearables. Four frameworks were assessed, the Three Orthogonal Dimensional model, the Information System Security Threat Cube Classification, Microsoft STRIDE Threat Assessment Framework and the CIA Triad. Each of these frameworks and their advantages and disadvantages were outlined. It was discovered in this chapter that some of the challenges of these frameworks was not assisting to identifying the assets of consumer health wearables in addition not classifying and providing the threats that affect consumer health wearables.

Chapter 6 focused on developing the threat assessment based on the gaps identified from Chapter 5. Chapter 6 developed the Consumer Health Wearable Threat Assessment Framework which consisted of six core elements (Authentication, Authorization, Availability, Confidentiality, Non-Repudiation and Integrity) from the CIA Triad and Microsoft STRIDE Framework. In addition, the framework consists of fourteen vulnerabilities (discovered from chapter 4) classified within these six core elements. It was theorized through this framework that it assists to provide a holistic understanding of the vulnerabilities affecting the consumer health wearable ecosystem.

Through developing the framework, Chapter 7 and 8 aimed to answer RQ4 - '*How viable is the proposed threat assessment framework for determining the vulnerabilities for the consumer health wearable ecosystem?*' Chapter 7 was centred on illustrating the framework on two test cases.

Through this illustration it was discovered that the framework assisted to provide the weaknesses of the test cases based on how they affect Authentication, Authorization, Availability, Confidentiality, Non-Repudiation and Integrity. Chapter 8 focused on assessing the quality of the framework through expert evaluation. It was discovered through this evaluation that security professionals deemed the framework as a very comprehensive, relevant framework that assisted to provide a basis coverage of the vulnerabilities for this current time period.

9.3 THEORETICAL CONTRIBUTION

One of the key factors of conducting Design Science Research is to make knowledge contributions. Based on the Design Science Knowledge Contribution Framework the theoretical contribution formulated is **Exaptation** (Figure 9.1).

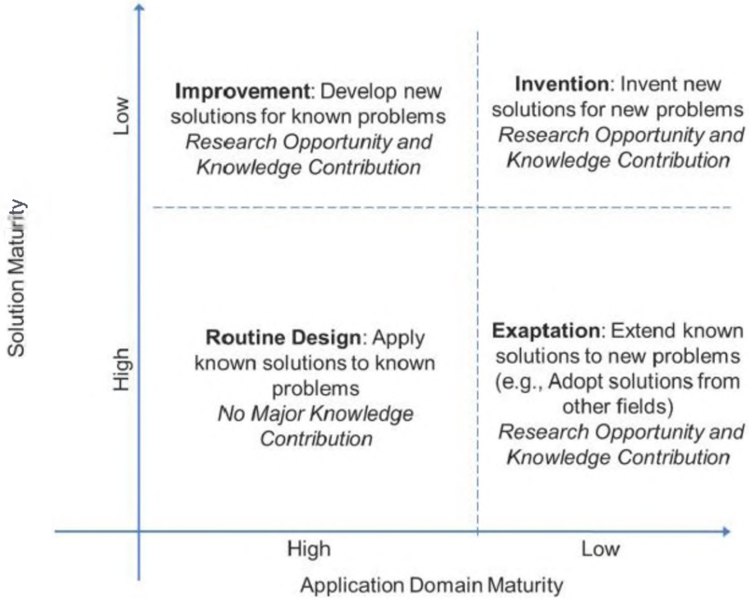
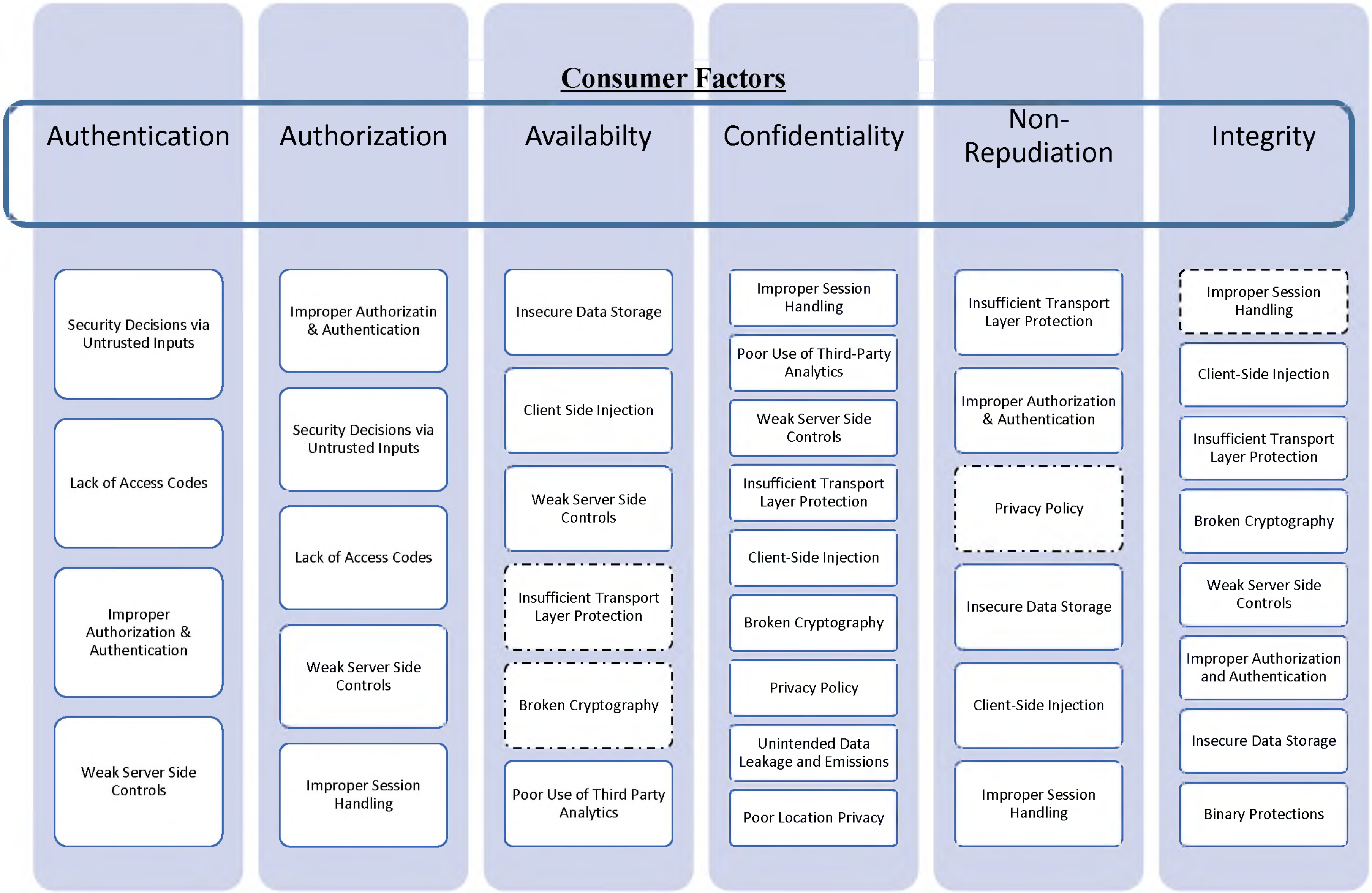

Solution Maturity
Low
High
Improvement: Develop new solutions for known problems *Research Opportunity and Knowledge Contribution*
Invention: Invent new solutions for new problems *Research Opportunity and Knowledge Contribution*
Routine Design: Apply known solutions to known problems *No Major Knowledge Contribution*
Exaptation: Extend known solutions to new problems (e.g., Adopt solutions from other fields) *Research Opportunity and Knowledge Contribution*
High
Low
Application Domain Maturity

Figure 9.1: DSR Knowledge Contribution Framework (Gregor and Hevner, 2013)

This research study assisted to extend known solutions of the CIA Triad and Microsoft STRIDE framework to new problems of consumer health wearables. The CIA Triad and Microsoft STRIDE framework are limited with addressing the concerns of consumer health wearables by identifying relevant vulnerabilities affecting consumer health wearables and classifying them. The Consumer

Health Wearable Threat Assessment considers the vulnerabilities pertaining to the consumer health wearable ecosystem. The extended solution (**Exaptation**) was conducted by firstly using the components of Authorization, Availability, Confidentiality, Non-Repudiation and Integrity from the CIA Triad and Microsoft STRIDE framework and classifying vulnerabilities from the consumer health wearable ecosystem to each of these components. This assists individuals to attain a holistic understanding of firstly the key components required for consumer health wearables. These key components include Authorization, Availability, Confidentiality, Non-Repudiation and Integrity. Secondly, through these key components, stakeholders (Application Stores, Developers and Reviewers) are able to review the vulnerabilities affecting the environment specifically pertaining to consumer health wearables. The Consumer Health Wearable Threat Assessment Framework therefore, as a theoretical knowledge contribution provides guidance and knowledge of the vulnerabilities affecting the consumer health wearable ecosystem (Figure 9.2).



Consumer Factors

Authentication	Authorization	Availabilty	Confidentiality	Non-Repudiation	Integrity
Security Decisions via Untrusted Inputs	Improper Authorizatin & Authentication	Insecure Data Storage	Improper Session Handling	Insufficient Transport Layer Protection	Improper Session Handling
Lack of Access Codes	Security Decisions via Untrusted Inputs	Client Side Injection	Poor Use of Third-Party Analytics	Improper Authorization & Authentication	Client-Side Injection
Improper Authorization & Authentication	Lack of Access Codes	Weak Server Side Controls	Weak Server Side Controls	Privacy Policy	Insufficient Transport Layer Protection
Weak Server Side Controls	Weak Server Side Controls	Insufficient Transport Layer Protection	Insufficient Transport Layer Protection	Insecure Data Storage	Broken Cryptography
	Improper Session Handling	Broken Cryptography	Client-Side Injection	Client-Side Injection	Weak Server Side Controls
		Poor Use of Third Party Analytics	Broken Cryptography	Improper Session Handling	Improper Authorization and Authentication
			Privacy Policy		Insecure Data Storage
			Unintended Data Leakage and Emissions		Binary Protections
			Poor Location Privacy		

Solid line vulnerabilities: mandatory *Dotted Line Vulnerabilities: non-mandatory*

Figure 9.2: Complete Consumer Health Wearable Threat Assessment Framework

9.4 Practical Contribution

The practical contribution created through conducting this research study is the Consumer Health Wearable Threat Assessment Framework. This framework assists users to understand the vulnerabilities affecting consumer health wearables. To assist to guide the detection of the vulnerabilities outlined from the Consumer Health Wearable Threat Assessment Framework (Figure 9.2), a list of elements for each of the vulnerabilities was provided (Table 9.1).

Table 9.1: Example Criteria of Vulnerabilities

Vulnerabilities
Poor Use of Third Party Analytics ➢ Lack of encryption or weak encryption algorithms as data is sent to third party analytics. Weak encryption algorithms RC2, MD4, MD5, SHA1 ➢ Sending data in clear text ➢ Lack of SSL or TLS standards during transmission ➢ Certificates not up to data
Lack of Access Codes ➢ Wearable device has no authentication during pairing ➢ Lack of authentication during re-paring of devices ➢ Wearable devices and application has no passwords or pins to protect user data
Poor Location Privacy ➢ Bluetooth signal not masked or hidden by nearby devices
Lack of Privacy Policy ➢ No documentation of the manner in which data will be handled or processed. ➢ Not detailing the permissions that will be used by the device
Insecure Data Storage ➢ Storing sensitive data on the file system: usernames, authentication tokens, passwords, cookies, device name, network, connection name, personal information (address, credit card data), application data, GPS/tracking information. ➢ Not using an API login scheme (over HTTPS). Furthermore, sensitive data should be stored on the server side. Assuming that there is a secure network connectivity. ➢ Not using SQLite for database encryption
Weak Server Side Controls ➢ Unencrypted access to server-side API ➢ Access to user data without authorization
Insufficient Transport-Layer Protection ➢ Are all connections being not secure and properly encrypted ➢ SSL certificates should be up to date ➢ SSL certificate should be not self-signed ➢ SSL should use high ciphers ➢ Application should not accept user accepted certificates

Client-Side Injection

- Overly detailing error reporting can help identify the type of server utilised. This will assist to determine the type of query language used.
- Not parametrizing queries. This can be checked by inserting a“ %,@, ’, OR ”
- Whitelisting instead of blacklisting
- Disable JavaScript and plugin support
- Do not let outside sources control user data and messages or any part of the format string

Improper Authorization and Authentication

- Where possible the authentication should occur on the server side. Successful authentication will load application data on the mobile device. This ensures application data is only available when the user has successfully authenticated.
- User passwords should not be stored on the device if persistent authentication (remember me) is utilised
- 4 digit passwords should not be utilised
- Persistent authentication should be available by default, but by opt-in.

Improper Session Handling

- Lack of adequate timeout sessions. Mobile application allows for long periods of timeout sessions.
- Failure to validate session tokens on the server side.
- Failure to properly rotate cookies by using auto generate mechanisms.

Unintended Data Leakage and Emissions

- Analytical data sent to 3rd parties is unencrypted
- URL caching
- HTML 5 data storage
- Browser cookie objects
- Keyboard press caching
- Copy/paste buffer caching

Security Decisions via Untrusted Inputs

This vulnerability can be checked via tools like Drozer. This will interact with the Inter process communication (IPC) to assess endpoints

- Sensitive data should not be sent through Inter Process Communication mechanism
- Any sensitive actions should have user interaction before an action is performed.
- Allow permissions of the application to access all components.

Lack of Binary Protections

- Can the application be modified to change the presentation layer within the application?
- Can automated tool be used like Hopper for visualisation of control-flow?
- Can the application be reversed engineered using automated tools (dex2jar for example)?
- Can the application be modified at the application’s binary level using a hex editor?

Broken Cryptography

- Reliance on built-in code encryption processes
- Poor key management processes (Do not create own protocol for key management)Creation and use of custom encryption protocols
- Use of insecure and/or deprecated algorithms: RC2, MD4, MD5, SHA1

9.5 LIMITATIONS

One of the major limitations for this research was the demonstration of the framework to assess the vulnerabilities on cloud servers of consumer health wearables. The limitation may result in not identifying additional vulnerabilities within the consumer health wearable ecosystem. Currently, based on this limitation the vulnerabilities identified are based and theorized from literature. There is also a limited selection of theoretical frameworks upon the research was developed. Four theoretical frameworks were selected. A further limitation was the demonstration of the framework was only conducted on android based mobile devices.

9.6 FUTURE RESEARCH

To refine and improve the research, a consideration is to include weighted statistical impact values of the vulnerabilities outlined from the Consumer Health Wearable Threat Assessment Framework. This will benefit the research as it will augment the framework for threat impact analysis to assess the magnitude of a threat based on which category it may impact (Authentication, Authorization, Availability, Confidentiality, Non-Repudiation and Integrity).

9.7 CONCLUDING REMARKS

This research study aimed to develop a threat assessment framework that can be used to assess health applications. The Design Science Research Process model by Peffers et al. (2007) was used to achieve this research objective. This assisted to understand the consumer health environment and the factors affecting it. In addition to this, theoretical threat assessment models were identified to which they can be adapted to provide a basis of coverage of the vulnerabilities affecting consumer health wearables. The study was able to answer the main research question of, 'What are the components of a threat assessment framework for determining privacy and security vulnerabilities in consumer health wearables? ' This research question was answered by developing a Consumer Health Wearable Threat Assessment Framework. To which the framework was evaluated to ensure it adhered to relevant and comprehensive vulnerabilities to which affect consumer health wearables.

LIST OF REFERENCES

Abomhara, M. and Koien, G.M., 2015. Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks. *Journal of Cyber Security and Mobility*, [online] 4(1), pp.65–88. Available at: <http://www.riverpublishers.com/journal_read_html_article.php?j=JCSM/4/1/4>.

Ackoff, R., 1989. From Data to Wisdom: Presidential Address to ISGSR. *Journal of Applied Systems Analysis*, 16, pp.3–9.

Adams, T.B., Bezner, J.R., Drabbs, M.E., Zambarano, R.J. and Steinhardt, M.A., 2000. Conceptualization and Measurement of the Spiritual and Psychological Dimensions of Wellness in a College Population. *Journal of American College Health*, [online] 48(4), pp.165–173. Available at: <http://www.tandfonline.com/doi/pdf/10.1080/07448480009595692> [Accessed 5 May 2017].

Adhikari, R., Richards, D. and Scott, K., 2014. Security and Privacy Issues Related to the Use of Mobile Health Apps. In: *25th Australasian Conference on Information Systems (ACIS 2014)*. pp.1–11.

Ahmed, M. and Ahamad, M., 2012. Protecting health information on mobile devices. In: *Proceedings of the second ACM conference on Data and Application Security and Privacy - CODASKY '12*. New York, New York, USA: ACM Press, pp.229–239.

Allsopp, A., 2016. *Google Glass vs Sony SmartEyeglass vs Toshiba Glass - Review - PC Advisor*. [online] TechAdvisor. Available at: <http://www.pcadvisor.co.uk/review/wearable-tech/google-glass-vs-sony-smarteyeglass-vs-toshiba-glass-3593995/> [Accessed 24 Feb. 2016].

Alpay, L., Verhoef, J., Xie, B., Te'eni, D. and Zwetsloot-Schonk, J.H.M., 2009. Current Challenge in Consumer Health Informatics: Bridging the Gap between Access to Information and Information Understanding. *Biomedical informatics insights*, 2(1), pp.1–10.

Al Ameen, M., Liu, J. and Kwak, K., 2012. Security and privacy issues in wireless sensor networks for healthcare applications. *Journal of Medical Systems*, 36(1), pp.93–101.

American Medical Informatics Association, 2016. *Consumer Health Informatics | AMIA*. [online] Available at: <https://www.amia.org/applications-informatics/consumer-health-informatics> [Accessed 5 Apr. 2016].

Appari, A. and Johnson, M.E., 2010. Information security and privacy in healthcare: current state of research. *International Journal of Internet and Enterprise Management*, 6(4), pp.279–314.

Apple, 2016. *App Store Review Guidelines - Apple Developer*. [online] Available at: <https://developer.apple.com/app-store/review/guidelines/> [Accessed 18 Apr. 2016].

Archer, N., Fevrier-Thomas, U., Lokker, C., McKibbon, K.A. and Straus, S.E., 2011. Personal health records: a scoping review. *Journal of the American Medical Informatics Association*, 18(4), pp.515–522.

Avancha, S., Baxi, A. and Kotz, D., 2012. Privacy in mobile technology for personal healthcare. *ACM Computing Surveys*, 45(1), pp.1–54.

Azar, K.M.J., Lesser, L.I., Laing, B.Y., Stephens, J., Aurora, M.S., Burke, L.E. and Palaniappan, L.P., 2013. Mobile applications for weight management: theory-based content analysis. *American journal of preventive medicine*, 45(5), pp.583–589.

Barcena, M., Wueest, C. and Lau, H., 2014. *How safe is your quantified self?* [online] Symantec. Available at: <https://www.symantec.com/content/dam/symantec/docs/white-papers/how-safe-is-your-quantified-self.pdf> [Accessed 12 Aug. 2015].

Bryan, G., 2015. *Healthcare sector 340% more prone to IT security threats*. [online] Available at: <http://www.computerweekly.com/news/4500254005/Healthcare-sector-340-more-prone-to-IT-security-threats> [Accessed 28 Oct. 2015].

Caldwell, T., 2014. The quantified self: a threat to enterprise security? *Computer Fraud & Security*, 1(11), pp.16–20.

Callahan, D., 1973. The WHO Definition of â€™ Health '. *The Concept of Health*, 1(3), pp.77–87.

Charani, E., Castro-Sánchez, E., Moore, L.S.P. and Holmes, A., 2014. Do smartphone applications in healthcare require a governance and legal framework? It depends on the application! *BMC medicine*, 12(29), pp.1–3.

Chen, Z., Lin, M., Chen, F., Lane, N., Cardone, G., Wang, R., Li, T., Chen, Y., Choudhury, T. and Cambell, A., 2013. Unobtrusive Sleep Monitoring using Smartphones. In: *Proceedings of the ICTs for improving Patients Rehabilitation Research Techniques*. [online] IEEE. Available at: <https://www.researchgate.net/profile/Tianxing_Li2/publication/261054378_Unobtrusive_Sleep_Monitoring_using_Smartphones/links/5755907708ae10c72b66a804.pdf> [Accessed 9 Mar. 2017].

Cohn, S.P., 2006a. *Privacy and confidentiality in the nationwide health information network*. [online] National Committe on Vital and Health Statistics. Available at: <http://www.ncvhs.hhs.gov/060622lt.html> [Accessed 27 Feb. 2016].

Cohn, S.P., 2006b. *Recommendations on Privacy and Confidentiality*. [online] National Commitee on Vital and Health Statistics(NCVHS). Available at: <http://www.cdc.gov/nchs/data/ncvhs/ncvhs06-08.pdf> [Accessed 4 Apr. 2016].

Conroy, D.E., Yang, C.-H. and Maher, J.P., 2014. Behavior change techniques in top-ranked mobile apps for physical activity. *American journal of preventive medicine*, 46(6), pp.649–652.

Cuadrado, F. and Dueñas, J., 2012. Mobile application stores: success factors, existing approaches, and future developments. *IEEE Communications Magazine*, 50(11), pp.160–167.

Cyr, B., Horn, W., Miao, D. and Specter, M., 2014. Security Analysis of Wearable Fitness Devices (Fitbit). *Massachusetts Institute of Technology*, pp.1–14.

Dehling, T., Gao, F., Schneider, S. and Sunyaev, A., 2015. Exploring the Far Side of Mobile Health: Information Security and Privacy of Mobile Health Apps on iOS and Android. *JMIR mHealth and uHealth*, [online] 3(1), pp.1–20. Available at: <http://www.ncbi.nlm.nih.gov/pubmed/25599627>.

Demiris, G., Afrin, L.B., Speedie, S., Courtney, K.L., Sondhi, M., Vimarlund, V., Lovis, C., Goossen, W. and Lynch, C., 2008. Patient-centered Applications: Use of Information Technology to Promote Disease Management and Wellness. A White Paper by the AMIA Knowledge in Motion Working Group. *Journal of the American Medical Informatics Association*, 15(1), pp.8–13.

Digiulio, S., 2014. Mobile Health Apps: Should They Be Regulated? *Oncology Times*, 36(10), p.60.

Dillon, T., Wu, C. and Chang, E., 2010. Cloud Computing: Issues and Challenges. In: *2010 24th IEEE International Conference on Advanced Information Networking and Applications*. IEEE, pp.27–33.

Dinh, H.T., Lee, C., Niyato, D. and Wang, P., 2013. A survey of mobile cloud computing: architecture, applications, and approaches. *Wireless Communications and Mobile Computing*, 13(18), pp.1587–1611.

Eysenbach, G., 2000. Recent advances: Consumer health informatics. *BMJ*, 320(7251), pp.1713–1716.

FDA, 2015. *Mobile Medical Applications*. [online] U.S. Deapartment of Health and Human Services Food and Drug Administration. Available at: <http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM263366.pdf> [Accessed 23 Apr. 2016].

FDA, 2016. *Digital Health*. [online] U.S. Deapartment of Health and Human Services Food and Drug Administration. Available at: <http://www.fda.gov/MedicalDevices/DigitalHealth/default.htm> [Accessed 23 Apr. 2016].

Ferguson, T., 2000. Online patient-helpers and physicians working together: a new partnership for high quality health care. *BMJ*, 321(7269), pp.1129–1132.

Feruza, S. and Kim, T.-H., 2007. IT Security Review: Privacy, Protection, Access Control, Assurance and System Security. *International Journal of Multimedia and Ubiquitous Engineering*, 2(2).

Flaherty, D., Hoffman-Goetz, L. and Arocha, J.F., 2015. What is consumer health informatics? A systematic review of published definitions. *Informatics for health & social care*, 40(2), pp.91–112.

Franklin, N.C. and Pratt, M., 2016. Let's Face It: Consumer-Focused Technology Is the Future of Cardiovascular Disease Prevention and Treatment. *Progress in Cardiovascular Diseases*, 58(6), pp.577–578.

Free, C., Phillips, G., Felix, L., Galli, L., Patel, V. and Edwards, P., 2010. The effectiveness of M-health technologies for improving health and health services: a systematic review protocol. *BMC research notes*, 3(1), pp.1–7.

Funk, C., 2015. *IoT Research – Smartbands*. [online] SecureList. Available at: <https://securelist.com/analysis/publications/69412/iot-research-smartbands/> [Accessed 21 Jan. 2016].

Geric, S. and Zejko, H., 2007. Information System Security Threats Classifications. *Journal of information and organizational sciences*, 31(1), pp.51–61.

Google, 2016. *Launch Checklist | Android Developers*. [online] Available at: <http://developer.android.com/distribute/tools/launch-checklist.html> [Accessed 22 Apr. 2016].

Google Android, 2016. *Android Developer*. [online] Available at: <https://developer.android.com/> [Accessed 10 Sep. 2016].

Goyal, R., Dragoni, N. and Spognardi, A., 2016. Mind the tracker you wear. In: *Proceedings of the 31st Annual ACM Symposium on Applied Computing - SAC '16*. New York, New York, USA: ACM Press, pp.131–136.

Gregor, S. and Hevner, A.R., 2013. Positioning and Presenting Design Science Research for maximum impact. *MIS Quarterly*, 37(2), pp.337–356.

Grimes, A., 2015. *Cyber Criminals Want Health Information*. [online] Available at: <http://www.thenashvilleglobe.com/cyber-criminals-health-information/> [Accessed 28 Oct. 2015].

Gruessner, V., 2015. *Too Many Apps Lack Strong Mobile Health Security Features*. [online] mHealth Intelligence. Available at: <http://mhealthintelligence.com/news/too-many-apps-lack-strong-mobile-health-security-features> [Accessed 5 May 2016].

Handel, M.J., 2011. mHealth (Mobile Health)—Using Apps for Health and Wellness. *EXPLORE: The Journal of Science and Healing*, 7(4), pp.256–261.

He, D., Naveed, M., Gunter, C.A. and Nahrstedt, K., 2014. Security Concerns in Android mHealth Apps. *AMIA Annual Symposium proceedings / AMIA Symposium*, 2014, pp.645–654.

Helfert, M., Donnellan, B. and Ostrowski, L., 2012. The case for design science utility and quality -Evaluation of design science artifact within the sustainable ICT capability maturity framework. *Systems, Signs & Actions An International Journal on Information Technology Action, Communication and Workpractices*, 6(1), pp.46–66.

Hevner, A., 2007. A Three Cycle View of Design Science Research. *Scandinavian Journal of Information Systems*, 19(2), pp.87–92.

Hevner, A. and Chatterjee, S., 2010. *Design Research in Information Systems: Theory and Practice*. New York: Springer Science & Business Media.

Hevner, A., March, S., Park, J. and Ram, S., 2004. Design Science in the Information Systems Research. *MIS Quarterly*, 28(1), pp.75–105.

Hofstee, E., 2006. *Constructing a Good Dissertation: A Practical Guide to Finishing a Master's, MBA or PhD on schedule*. Sandton: EPE.

HP Fortify, 2015. *Internet of Things Security Study : Smartwatches*. [online] HP. Available at: <https://www.ftc.gov/system/files/documents/public_comments/2015/10/00050-98093.pdf> [Accessed 14 Aug. 2015].

Huang, D., 2011. Mobile Cloud Computing. *IEEE COMSOC Multimedia Communications Technical Committee (MMTC) E-Letter*, 6(10), pp.27–31.

Huba, N. and Zhang, Y., 2012. Designing Patient-Centered Personal Health Records (PHRs): Health Care Professionals' Perspective on Patient-Generated Data. *Journal of Medical Systems*, [online] 36(6), pp.3893–3905. Available at: <http://link.springer.com/10.1007/s10916-012-9861-z> [Accessed 10 Mar. 2017].

Huckvale, K., Prieto, J.T., Tilney, M., Benghozi, P.-J. and Car, J., 2015. Unaddressed privacy risks in accredited health and wellness apps: a cross-sectional systematic assessment. *BMC medicine*, 13, p.214.

Humer, C. and Finkle, J., 2014. *Your medical record is worth more to hackers than your credit card.* [online] Available at: <http://www.reuters.com/article/2014/09/24/us-cybersecurity-hospitals-idUSKCN0HJ21I20140924> [Accessed 28 Oct. 2015].

Hunker, J. and Probst, C.W., 2008. Insiders and Insider Threats An Overview of Definitions and Mitigation Techniques. *Journal of Wireless Mobile Networks*, 2(1), pp.4–27.

ISACA, 2015. *COBIT 5: A Business Framework for the Governance and Management of Enterprise IT.* [online] Information systems Audit and Control Association (ISACA). Available at: <http://www.isaca.org/COBIT/Pages/default.aspx> [Accessed 11 May 2016].

ISO/IEC 27002, 2005. IS/ISO/IEC 13335-1 (2004): Information Technology - Security Techniques - Management of Information and Communications Technology Security, Part 1: Concepts and Models for Information and Communications Technology Security Management. [online] Available at: <https://law.resource.org/pub/in/bis/S04/is.iso.iec.13335.1.2004.pdf> [Accessed 15 Mar. 2017].

Jackson, J., 2014. *How the NIST cyber security framework can help secure the enterprise.* [online] InfoWorld. Available at: <http://www.infoworld.com/article/2610022/security-management/how-the-nist-cyber-security-framework-can-help-secure-the-enterprise.html> [Accessed 3 May 2016].

Jakicic, J.M., Davis, K.K., Rogers, R.J., King, W.C., Marcus, M.D., Helsel, D., Rickman, A.D., Wahed, A.S. and Belle, S.H., 2016. Effect of Wearable Technology Combined With a Lifestyle Intervention on Long-term Weight Loss. *JAMA*, [online] 316(11), p.1161. Available at: <http://jama.jamanetwork.com/article.aspx?doi=10.1001/jama.2016.12858> [Accessed 17 Nov. 2017].

Jouini, M., Rabai, L.B.A. and Aissa, A. Ben, 2014. Classification of Security Threats in Information Systems. *Procedia Computer Science*, [online] 32, pp.489–496. Available at: <http://linkinghub.elsevier.com/retrieve/pii/S1877050914006528> [Accessed 26 Apr. 2017].

Kamatchi, R. and Ambekar, K., 2016. Analyzing Impacts of Cloud Computing Threats in Attack based Classification Models. *Indian Journal of Science and Technology*, [online] 9(21). Available at: <http://www.indjst.org/index.php/indjst/article/viewFile/95282/70310> [Accessed 12 Jun. 2017].

Kamerow, D., 2013. Regulating medical apps: which ones and how much? *BMJ (Clinical research ed.)*, 3(47).

Klasnja, P. and Pratt, W., 2012. Healthcare in the pocket: Mapping the space of mobile-phone health interventions. *Journal of Biomedical Informatics*, [online] 45(1), pp.184–198. Available at: <http://dx.doi.org/10.1016/j.jbi.2011.08.017>.

Klecun, E. and Cornford, T., 2005. A critical approach to evaluation. *European Journal of Information Systems*, 14(3), pp.229–243.

Kumar, P. and Lee, H.-J., 2011. Security issues in healthcare applications using wireless medical sensor networks: a survey. *Sensors*, [online] 12(12), pp.55–91. Available at: <http://www.mdpi.com/1424-8220/12/1/55/>.

Lamkin, P., 2016. *Wearable Tech Market To Be Worth $34 Billion By 2020*. [online] Forbes. Available at: <https://www.forbes.com/sites/paullamkin/2016/02/17/wearable-tech-market-to-be-worth-34-billion-by-2020/#420a723d3cb5> [Accessed 30 Mar. 2017].

Lewis, D., Chang, B.L. and Friedman, C.P., 2010. Consumer health informatics. *Studies in health technology and informatics*, 151, pp.1–7.

Li, M., Lou, W. and Ren, K., 2010. Data security and privacy in wireless body area networks. *IEEE Wireless Communications*, 17(1), pp.51–58.

Liu, C., Zhu, Q., Holroyd, K. and Seng, E., 2011. Status and trends of mobile-health applications for iOS devices: A developer's perspective. *Journal of Systems and Software*, 84(11), pp.2022–2033.

Lobelo, F., Kelli, H.M., Tejedor, S.C., Pratt, M., McConnell, M. V., Martin, S.S. and Welk, G.J., 2016. The Wild Wild West: A Framework to Integrate mHealth Software Applications and Wearables to Support Physical Activity Assessment, Counseling and Interventions for Cardiovascular Disease Risk Reduction. *Progress in Cardiovascular Diseases*, 58(6), pp.584–594.

Löhr, H., Sadeghi, A. and Winandy, M., 2010. Securing the e-health cloud. In: *Proceedings of the ACM international conference on Health informatics - IHI '10*. New York, New York, USA: ACM Press, p.220.

Lupton, D., 2016. Digitised health, medicine and risk. *Health, Risk & Society*, [online] 17(7–8), pp.473–476. Available at: <http://www.tandfonline.com/action/journalInformation?journalCode=chrs20>.

Mantovani, E., Quinn, P., Guihen, B., Habbig, A.-K. and Hert, P., 2013. eHealth to mHealth – A Journey Precariously Dependent Upon Apps? *European Journal of ePractice*, (21), pp.48–66.

Marceglia, S., Fontelo, P. and Ackerman, M.J., 2015. Transforming consumer health informatics: connecting CHI applications to the health-IT ecosystem. *Journal of the American Medical Informatics Association*, pp.1–3.

March, S.T. and Smith, G.F., 1995. Design and natural science research on information technology. *Decision Support Systems*, 15(4), pp.251–266.

Martínez-Pérez, B., de la Torre-Díez, I. and López-Coronado, M., 2015. Privacy and Security in Mobile Health Apps: A Review and Recommendations. *Journal of Medical Systems*, 39(1), pp.1–8.

Martinez, R., 2014. *The world at your fingertips… and theirs too*. [online] SecureList. Available at: <https://securelist.com/blog/research/66435/the-world-at-your-fingertips-and-theirs-too/> [Accessed 25 Jan. 2016].

McCarney, S., 2016. *5th Annual State of Application Security Report January 2016*. [online] Arxan Technologies. Available at: <https://www.arxan.com/arxans-5th-annual-state-of-application-security-report-reveals-disparity-between-mobile-app-security-perception-and-

reality/> [Accessed 14 Jan. 2016].

Mell, P. and Grance, T., 2011. The NIST Definition of Cloud Computing Recommendations of the National Institute of Standards and Technology.

Michael, C. and Njie, L., 2013. Technical Analysis of the Data Practices and Privacy Risks of 43 Popular Mobile Health and Fitness Applications. pp.1–31.

Microsoft, 2005. *The STRIDE Threat Model*. [online] Available at: <https://msdn.microsoft.com/en-us/library/ee823878(v=cs.20).aspx> [Accessed 27 Jul. 2017].

Mnjama, J., Foster, G. and Irwin, B., 2017. A Privacy and Security Threat Assessment Framework for Consumer Health Wearables. In: *Proceedings of the 2017 ISSA Conference*. pp.66–73.

Morera, E.P., de la Torre Díez, I., Garcia-Zapirain, B., López-Coronado, M. and Arambarri, J., 2016. Security Recommendations for mHealth Apps: Elaboration of a Developer's Guide. *Journal of Medical Systems*, 40(6), p.152.

Nass, S.J., Levit, L.A. and Gostin, L.O., 2009. *The Value and Importance of Health Information Privacy*. 2nd ed. Washington: National Academies Press (US).

Nazi, K.M., Hogan, T.P., Woods, S.S., Simon, S.R. and Ralston, J.D., 2016. Consumer Health Informatics: Engaging and Empowering Patients and Families. In: *Clinical Informatics Study Guide*. Cham: Springer International Publishing, pp.459–500.

NHS, 2016. *Health Applications*. [online] National Health Services. Available at: <http://www.nhs.uk/pages/home.aspx> [Accessed 24 Apr. 2016].

Office of the National Coordinator for Health Information Technology (ONC), 2016. *Personal Health Records*. [online] Available at: <https://www.healthit.gov/> [Accessed 28 Jun. 2016].

Osgood, C.E., May, W.H. and Miron, M.S., 1975. *Cross-cultural universals of affective meaning. Cross-cultural universals of affective meaning.* Champaign, IL, US: University of Illinois Press.

OWASP, 2014. *OWASP Mobile Security Project - Top Ten Mobile Risks*. [online] OWASP. Available at: <https://www.owasp.org/index.php/OWASP_Mobile_Security_Project#Top_Ten_Mobile_Risks > [Accessed 14 Jan. 2015].

OWASP, 2015. *Application Threat Modeling - OWASP*. [online] Open Web Application Security Project (OWASP). Available at: <https://www.owasp.org/index.php/Application_Threat_Modeling> [Accessed 13 May 2016].

Peffers, K., Tuunanen, T., Rothenberger, M.A. and Chatterjee, S., 2007. A Design Science Research Methodology for Information Systems Research. *Journal of Management Information Systems*, 24(3), pp.45–77.

Pirkkalainen, H., 2015. Dealing with emergent design science research projects in IS. pp.20–29.

Pittman, D., 2014. 5 Problems With Mobile Health App Security. *MedPage Today*, [online] 2 May, pp.1–3. Available at: <http://www.medpagetoday.com/PracticeManagement/InformationTechnology/44161>.

Piwek, L., Ellis, D.A., Andrews, S. and Joinson, A., 2016. The Rise of Consumer Health Wearables: Promises and Barriers. *PLOS Medicine*, 13(2), pp.1–9.

La Polla, M., Martinelli, F. and Sgandurra, D., 2013. A Survey on Security for Mobile Devices. *IEEE Communications Surveys & Tutorials*, 15(1), pp.446–471.

Ponemon Institute LLC, 2015. *The State of Mobile Application Insecurity*. [online] IBM. Available at: <http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=WH&infotype=SA&htmlfid=WGL03074USEN&attachment=WGL03074USEN.PDF> [Accessed 14 Jan. 2016].

Protection of Personal Information Act, 2013.

Rai, P.O., 2013. *Android Application Security Essentials*. 1st ed. Birmingham: Packt Publishing Ltd.

Ralf, J., 2014. *mHealth App Developer Economics Report 2014*. [online] Research2Guidance. Available at: <www.mHealthEconomics.com> [Accessed 13 Sep. 2015].

Rooksby, J., Rost, M., Morrison, A. and Chalmers, M.C., 2014. Personal tracking as lived informatics. In: *Proceedings of the 32nd annual ACM conference on Human factors in computing systems - CHI '14*. [online] New York, New York, USA: ACM Press, pp.1163–1172. Available at: <https://courses.cs.washington.edu/courses/cse440/15au/readings/PersonalInformatics-Rooksby2014.pdf> [Accessed 7 Mar. 2017].

Rozenblum, R. and Bates, D.W., 2013. Patient-centred healthcare, social media and the internet: the perfect storm? *BMJ Quality & Safety*, 22(3), pp.183–186.

Ruf, L., Thorn, A., Christen, T., Gruber, B. and Portmann, R., 2008. Threat Modeling in Security Architecture – The Nature of Threats. *ISSS Working Group on Security Architectures*, [online] pp.1–4. Available at: <https://pdfs.semanticscholar.org/09fc/831b360dce8f9924a67aed274f15bebf3e9b.pdf> [Accessed 8 Jun. 2017].

Safavi, S. and Shukur, Z., 2014. Conceptual Privacy Framework for Health Information on Wearable Device. *PLoS ONE*, 9(12), pp.1–16.

Sanzgiri, A.M., 2013. *A Comprehensive Threat Assessment Framework for Securing Emerging Technologies*. University at Bufffalo, State University of New York.

Seals, T., 2016. *Most Health and Financial Mobile Apps Are Rife with Vulnerabilities - Infosecurity Magazine*. [online] Infosecurity Magazine. Available at: <http://www.infosecurity-magazine.com/news/health-financial-mobile-apps-rife/> [Accessed 14 Jan. 2016].

Selinger, M., 2015. *Test : Fitness Wristbands Reveal Data*. [online] AV-Test: The Independent IT- Security Institute. Available at: <https://www.av-test.org/en/news/news-single-view/test-fitness-wristbands-reveal-data/> [Accessed 23 Jun. 2015].

Shapiro, M., Johnston, D., Wald, J. and Mon, D., 2012. *Patient-Generated Health Data - White Paper*. [online] *Prepared for the Office of Policy and Planning, Office of the National Coordinator for Health Information Technology. Research Triangle Park, NC: RTI Internation*, Available at: <http://healthitgov.ahrqdev.org/sites/default/files/rti_pghd_whitepaper_april_2012.pdf>

[Accessed 10 Mar. 2017].

Shostack, A., 2014. *Threat Modeling: Designing for Security*. 1st ed. Indianapolis: John Wiley and Sons Inc.

Simon, H.A., 1996. *The Sciences of the Artificial*. 3rd ed. Massachusetts: The MIT Press.

Siponen, M. and Willison, R., 2009. Information security management standards: Problems and solutions. *Information & Management*, 46(5), pp.267–270.

von Solms, B., 2001. Information Security — A Multidimensional Discipline. *Computers & Security*, 20(6), pp.504–508.

von Solms, R. and van Niekerk, J., 2013. From Information Security to Cyber Security. *Computers & Security*, [online] 38, pp.97–102. Available at: <http://linkinghub.elsevier.com/retrieve/pii/S0167404813000801> [Accessed 15 Mar. 2017].

Speed, T., Nykamp, D., Heiser, M., Anderson, J. and Nampalli, J., 2013. *Mobile Security: How to Secure, Privatize, and Recover Your Devices*. 1st ed. Birmingham: Packt Publishing Ltd.

Stamer, D., Zimmermann, O. and Sandkuhl, K., 2016. What Is a Framework? - A Systematic Literature Review in the Field of Information Systems. Springer, Cham, pp.145–158.

Stefanou, C.J., 2001. A framework for the ex-ante evaluation of ERP software. *European Journal of Information Systems*, 10(4), pp.204–215.

Symantec, 2014. Internet Security Threat Report. *Symantec 2013Trends*, 19, pp.1–98.

Tähepold, H., van den Brink-Muinen, A. and Maaroos, H.-I., 2006. Patient expectations from consultation with family physician. *Croatian medical journal*, 47(1), pp.148–54.

Tang, P.C., Ash, J.S., Bates, D.W., Overhage, J.M. and Sands, D.Z., 2006. Personal health records: Definitions, benefits, and strategies for overcoming barriers to adoption. *Journal of the American Medical Informatics Association*, 13(2), pp.121–126.

Tavani, H.T. and Moor, J.H., 2001. Privacy protection, control of information, and privacy-enhancing technologies. *ACM SIGCAS Computers and Society*, 31(1), pp.6–11.

Thompson, B.M. and Brodsky, I., 2013. Should the FDA regulate mobile medical apps? *BMJ (Clinical research ed.)*, [online] 347. Available at: <http://0-www.bmj.com.wam.seals.ac.za/content/347/bmj.f5211.abstract> [Accessed 3 Nov. 2015].

Tomlinson, M., Rotheram-Borus, M.J., Swartz, L. and Tsai, A.C., 2013. Scaling Up mHealth: Where Is the Evidence? *PLoS Medicine*, 10(2), pp.1–5.

Vaishnavi, V. and Kuechler, B., 2004. Design Science Research in Information Systems. *Association for Information Systems*, p.54.

Vaishnavi, V. and Kuechler, W., 2015. *Design science research methods and patterns : innovating information and communication technology*. 2nd ed. CRC Press.

Valdez, R.S., Holden, R.J., Novak, L.L. and Veinot, T.C., 2014. Transforming consumer health informatics through a patient work framework: connecting patients to context. *Journal of the American Medical Informatics Association*, pp.1–7.

Venable, J., Pries-Heje, J. and Baskerville, R., 2012. A Comprehensive Framework for Evaluation in Design Science Research. In: *International Conference on Design Science Research in Information Systems*. [online] Berlin, Heidelberg: Springer, pp.423–438. Available at: <http://link.springer.com/10.1007/978-3-642-29863-9_31>.

Venable, J., Pries-Heje, J. and Baskerville, R., 2016. FEDS: a Framework for Evaluation in Design Science Research. *European Journal of Information Systems*, 25(1), pp.77–89.

WHO, 1948. *WHO definition of Health*. [online] Available at: <http://www.who.int/about/definition/en/print.html> [Accessed 22 Mar. 2016].

Wicks, P. and Chiauzzi, E., 2015. 'Trust but verify' – five approaches to ensure safe medical apps. *BMC Medicine*, 13(1), pp.1–5.

Williams, P.A.H. and Maeder, A.J., 2015. 'Security and Privacy Issues for Mobile Health'. In: *Mobile Health*, 1st ed. [online] Springer International Publishing, pp.1067–1088. Available at: <http://link.springer.com/10.1007/978-3-319-12817-7_44> [Accessed 20 Oct. 2016].

Zhou, W. and Piramuthu, S., 2014. Security/privacy of wearable fitness tracking IoT devices. In: *2014 9th Iberian Conference on Information Systems and Technologies (CISTI)*. [online] IEEE, pp.1–5. Available at: <http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6877073>.

Zubaydi, F., Saleh, A., Aloul, F. and Sagahyroon, A., 2015. Security of mobile health (mHealth) systems. In: *2015 IEEE 15th International Conference on Bioinformatics and Bioengineering (BIBE)*. IEEE, pp.1–5.

APPENDICES

APPENDIX A – PARTICIPANT LETTER

RHODES UNIVERSITY
Where leaders learn

Department of Information Systems
Hamilton building, Prince Alfred Street, Grahamstown, 6139, South Africa
PO Box 94, Grahamstown, 6140, South Africa
t: +27 (0) 46 603 8244
f: +27 (0) 46 603 7608
e: informationsystems@ru.ac.za
www.ru.ac.za

10 October 2017

Dear Sir/Madam,

Re: Invitation to participate in research study

You are invited to participate in a research study entitled ‘Towards a threat assessment framework for Consumer Health Wearables’ The aim of this research study is to determine how well the framework guides the detection of security vulnerabilities pertaining to consumer health wearables and their associated mobile health applications for physical wellness. Your participation and cooperation is important so that the results of the research are accurately portrayed.

The research will require you to partake in interviews and the data to be collected from this research will be used to refine the developed threat assessment framework. Your identity and that of your institution will be treated with complete confidentiality. The collection of this data will require about 60 minutes of your time to complete.

We will provide you with all the necessary information, both verbally and written documentation to assist you to understand the study and explain what would be expected of you (the participant). These guidelines would include the risks, benefits, and your rights as a study subject. Furthermore, it is important that you are aware that this study has been approved by a Research Ethics Committee of the university.

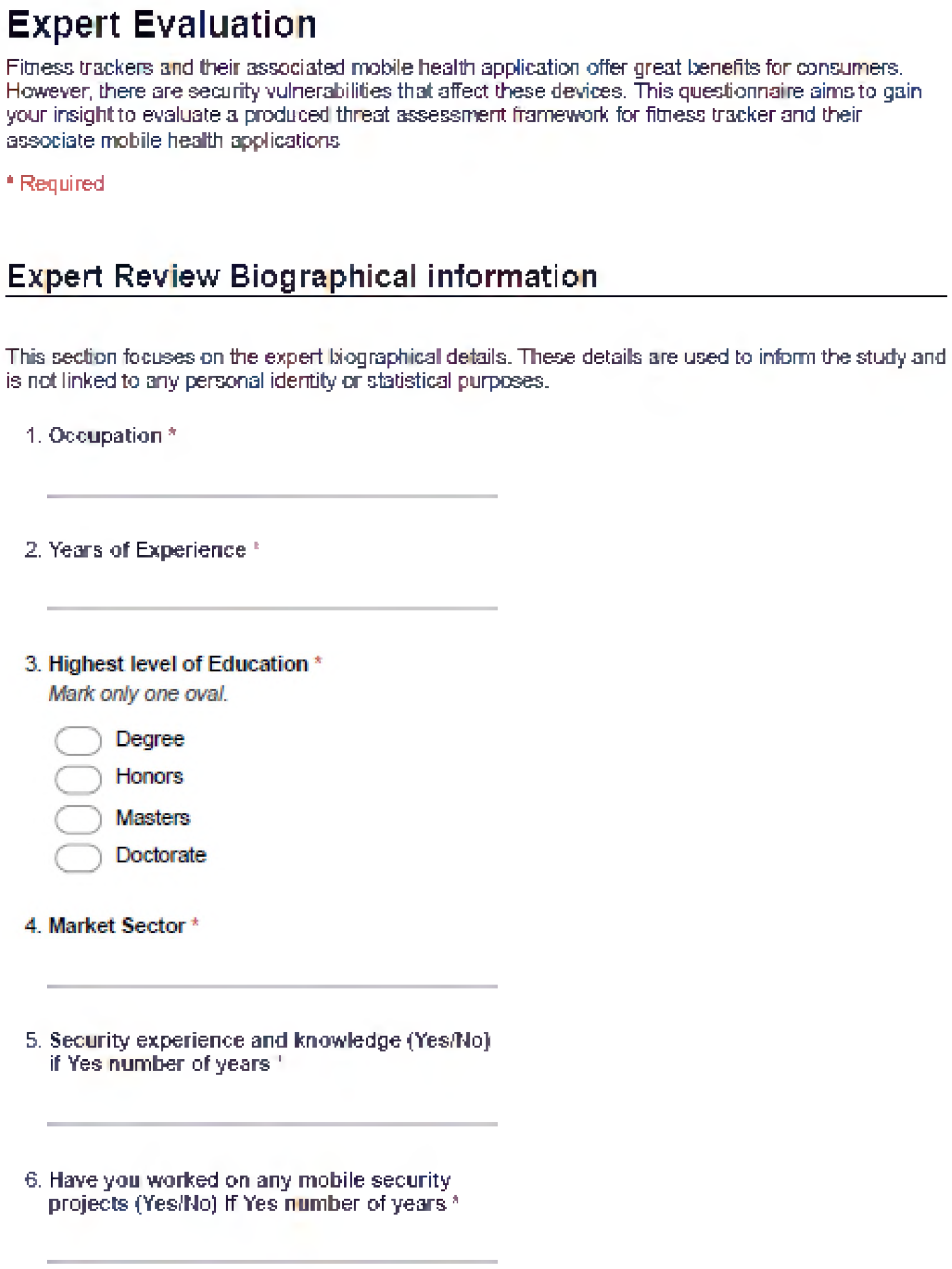
Participation in this research is completely voluntary and this letter of invitation does not obligate you to take part in this research study. To participate, you will be required to provide written consent that will include your signature, date and initials to verify that you understand and agree to the conditions. Please note that you have the right to withdraw at any given time during the study without penalty.

Thank you for your time and I hope that you will find our request favourable.

Yours sincerely,

Javan Joshua Mnjama	Professor Greg Foster	Professor Barry Irwin
Research Student	Supervisor	Co-Supervisor

APPENDIX B – EXPERT EVALUATION FORM



Expert Evaluation

Fitness trackers and their associated mobile health application offer great benefits for consumers. However, there are security vulnerabilities that affect these devices. This questionnaire aims to gain your insight to evaluate a produced threat assessment framework for fitness tracker and their associate mobile health applications

* Required

Expert Review Biographical information

This section focuses on the expert biographical details. These details are used to inform the study and is not linked to any personal identity or statistical purposes.

1. Occupation *

   ____

2. Years of Experience *

   ____

3. Highest level of Education *

   Mark only one oval.

   ○ Degree
   ○ Honors
   ○ Masters
   ○ Doctorate

4. Market Sector *

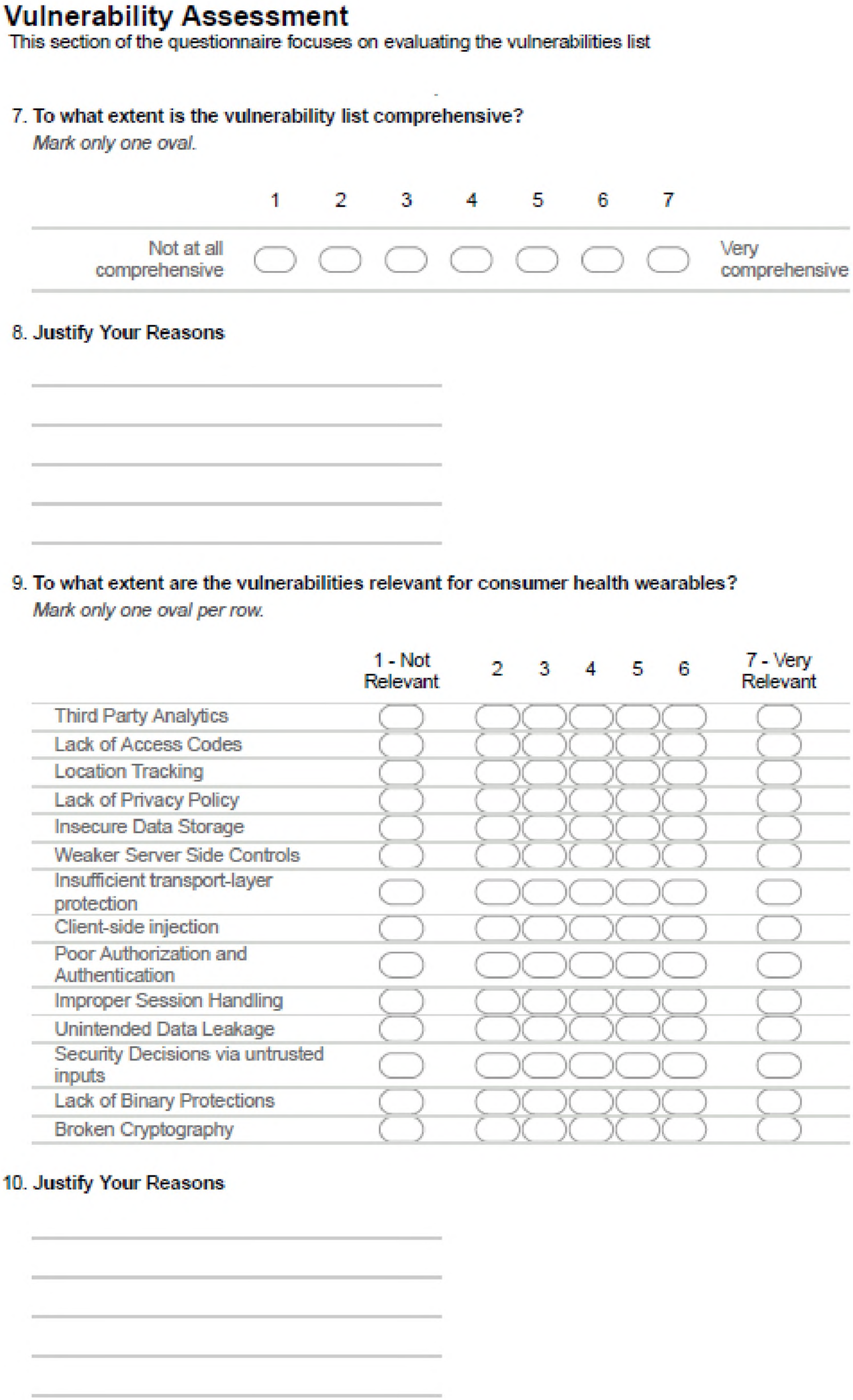
   ____

5. Security experience and knowledge (Yes/No) if Yes number of years *

   ____

6. Have you worked on any mobile security projects (Yes/No) If Yes number of years *

   ____



Vulnerability Assessment

This section of the questionnaire focuses on evaluating the vulnerabilities list

7. **To what extent is the vulnerability list comprehensive?**

Mark only one oval.

	1	2	3	4	5	6	7	
Not at all comprehensive	○	○	○	○	○	○	○	Very comprehensive

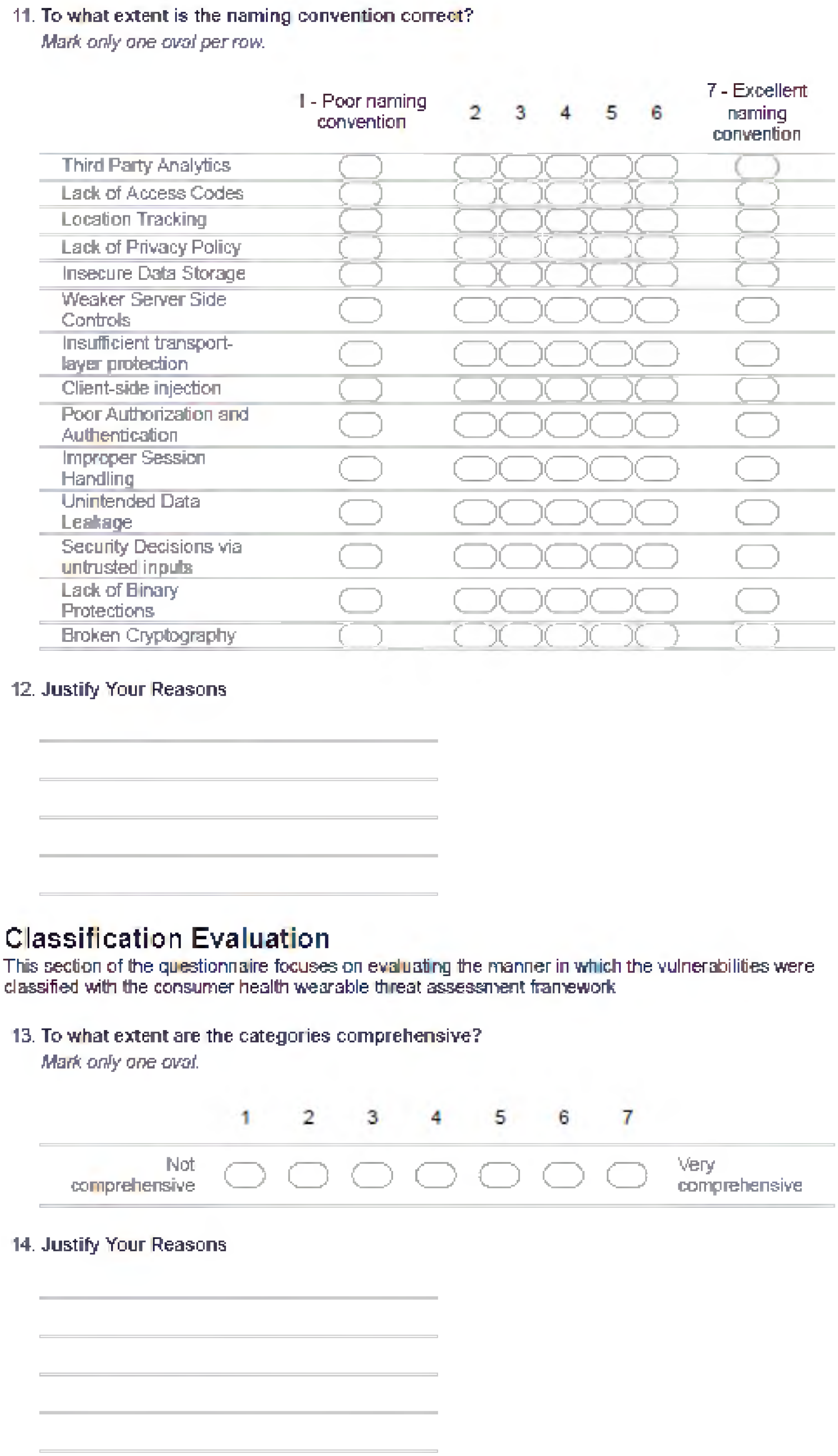
8. **Justify Your Reasons**

9. **To what extent are the vulnerabilities relevant for consumer health wearables?**

Mark only one oval per row.

	1 - Not Relevant	2	3	4	5	6	7 - Very Relevant
Third Party Analytics	○	○	○	○	○	○	○
Lack of Access Codes	○	○	○	○	○	○	○
Location Tracking	○	○	○	○	○	○	○
Lack of Privacy Policy	○	○	○	○	○	○	○
Insecure Data Storage	○	○	○	○	○	○	○
Weaker Server Side Controls	○	○	○	○	○	○	○
Insufficient transport-layer protection	○	○	○	○	○	○	○
Client-side injection	○	○	○	○	○	○	○
Poor Authorization and Authentication	○	○	○	○	○	○	○
Improper Session Handling	○	○	○	○	○	○	○
Unintended Data Leakage	○	○	○	○	○	○	○
Security Decisions via untrusted inputs	○	○	○	○	○	○	○
Lack of Binary Protections	○	○	○	○	○	○	○
Broken Cryptography	○	○	○	○	○	○	○

10. **Justify Your Reasons**



11. **To what extent is the naming convention correct?**

Mark only one oval per row.

	1 - Poor naming convention	2	3	4	5	6	7 - Excellent naming convention
Third Party Analytics	○	○	○	○	○	○	○
Lack of Access Codes	○	○	○	○	○	○	○
Location Tracking	○	○	○	○	○	○	○
Lack of Privacy Policy	○	○	○	○	○	○	○
Insecure Data Storage	○	○	○	○	○	○	○
Weaker Server Side Controls	○	○	○	○	○	○	○
Insufficient transport-layer protection	○	○	○	○	○	○	○
Client-side injection	○	○	○	○	○	○	○
Poor Authorization and Authentication	○	○	○	○	○	○	○
Improper Session Handling	○	○	○	○	○	○	○
Unintended Data Leakage	○	○	○	○	○	○	○
Security Decisions via untrusted inputs	○	○	○	○	○	○	○
Lack of Binary Protections	○	○	○	○	○	○	○
Broken Cryptography	○	○	○	○	○	○	○

12. **Justify Your Reasons**

Classification Evaluation

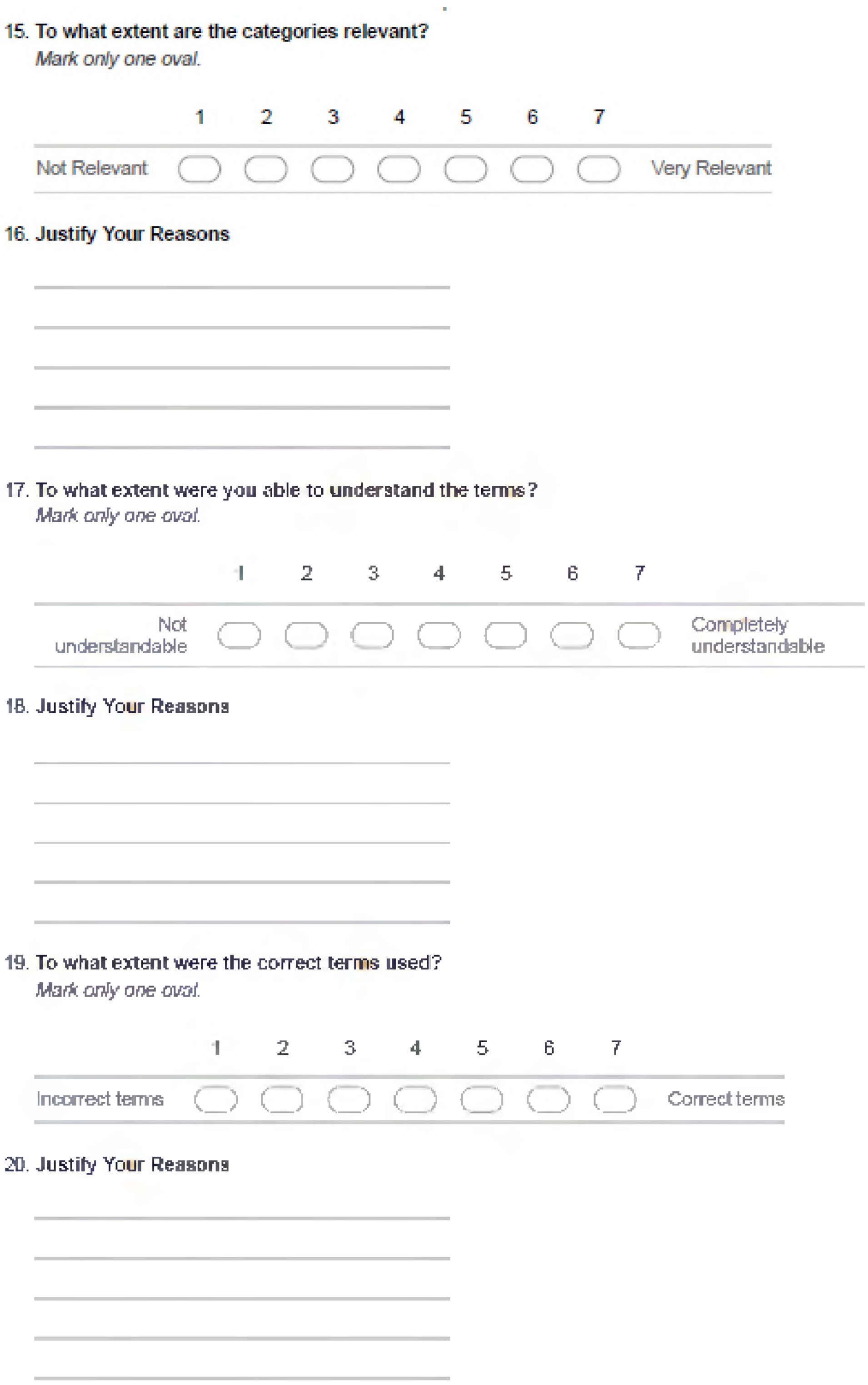
This section of the questionnaire focuses on evaluating the manner in which the vulnerabilities were classified with the consumer health wearable threat assessment framework

13. **To what extent are the categories comprehensive?**

Mark only one oval.

	1	2	3	4	5	6	7	
Not comprehensive	○	○	○	○	○	○	○	Very comprehensive

14. **Justify Your Reasons**



15. **To what extent are the categories relevant?**
Mark only one oval.

	1	2	3	4	5	6	7	
Not Relevant	○	○	○	○	○	○	○	Very Relevant

16. **Justify Your Reasons**

17. **To what extent were you able to understand the terms?**
Mark only one oval.

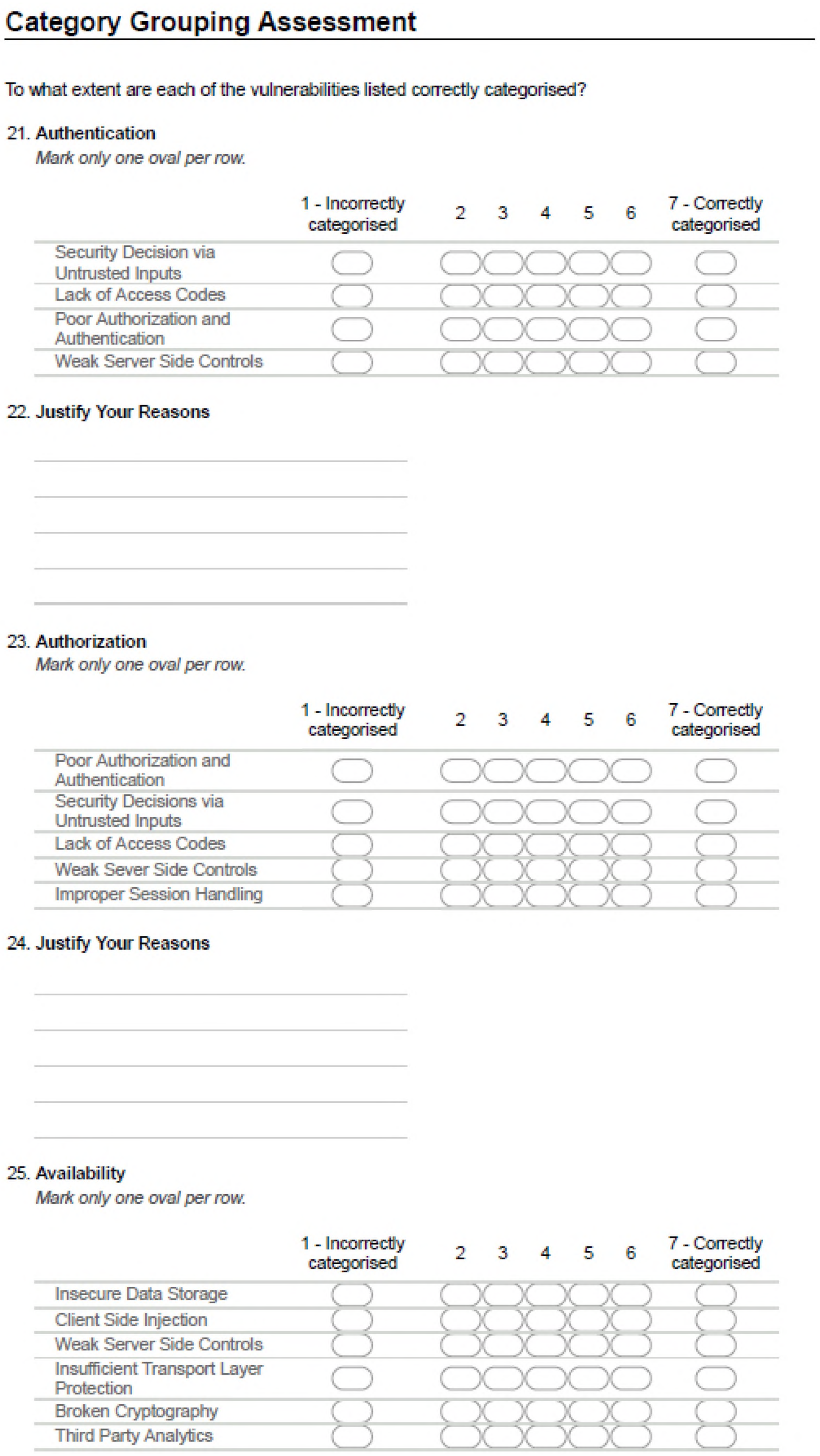
	1	2	3	4	5	6	7	
Not understandable	○	○	○	○	○	○	○	Completely understandable

18. **Justify Your Reasons**

19. **To what extent were the correct terms used?**
Mark only one oval.

	1	2	3	4	5	6	7	
Incorrect terms	○	○	○	○	○	○	○	Correct terms

20. **Justify Your Reasons**



Category Grouping Assessment

To what extent are each of the vulnerabilities listed correctly categorised?

21. **Authentication**

Mark only one oval per row.

	1 - Incorrectly categorised	2	3	4	5	6	7 - Correctly categorised
Security Decision via Untrusted Inputs	○	○	○	○	○	○	○
Lack of Access Codes	○	○	○	○	○	○	○
Poor Authorization and Authentication	○	○	○	○	○	○	○
Weak Server Side Controls	○	○	○	○	○	○	○

22. **Justify Your Reasons**

23. **Authorization**

Mark only one oval per row.

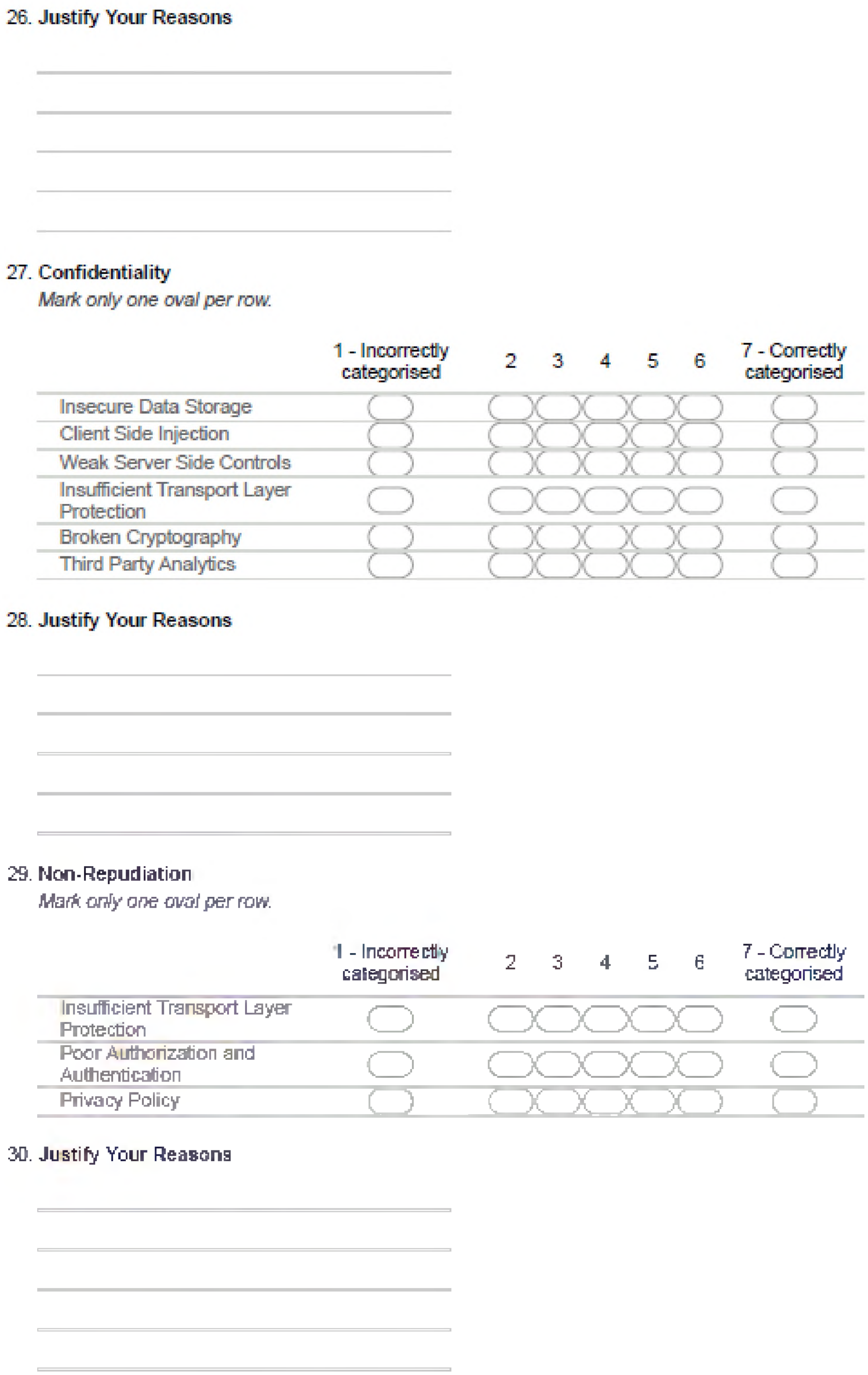
	1 - Incorrectly categorised	2	3	4	5	6	7 - Correctly categorised
Poor Authorization and Authentication	○	○	○	○	○	○	○
Security Decisions via Untrusted Inputs	○	○	○	○	○	○	○
Lack of Access Codes	○	○	○	○	○	○	○
Weak Sever Side Controls	○	○	○	○	○	○	○
Improper Session Handling	○	○	○	○	○	○	○

24. **Justify Your Reasons**

25. **Availability**

Mark only one oval per row.

	1 - Incorrectly categorised	2	3	4	5	6	7 - Correctly categorised
Insecure Data Storage	○	○	○	○	○	○	○
Client Side Injection	○	○	○	○	○	○	○
Weak Server Side Controls	○	○	○	○	○	○	○
Insufficient Transport Layer Protection	○	○	○	○	○	○	○
Broken Cryptography	○	○	○	○	○	○	○
Third Party Analytics	○	○	○	○	○	○	○



26. **Justify Your Reasons**

27. **Confidentiality**

Mark only one oval per row.

	1 - Incorrectly categorised	2	3	4	5	6	7 - Correctly categorised
Insecure Data Storage	○	○	○	○	○	○	○
Client Side Injection	○	○	○	○	○	○	○
Weak Server Side Controls	○	○	○	○	○	○	○
Insufficient Transport Layer Protection	○	○	○	○	○	○	○
Broken Cryptography	○	○	○	○	○	○	○
Third Party Analytics	○	○	○	○	○	○	○

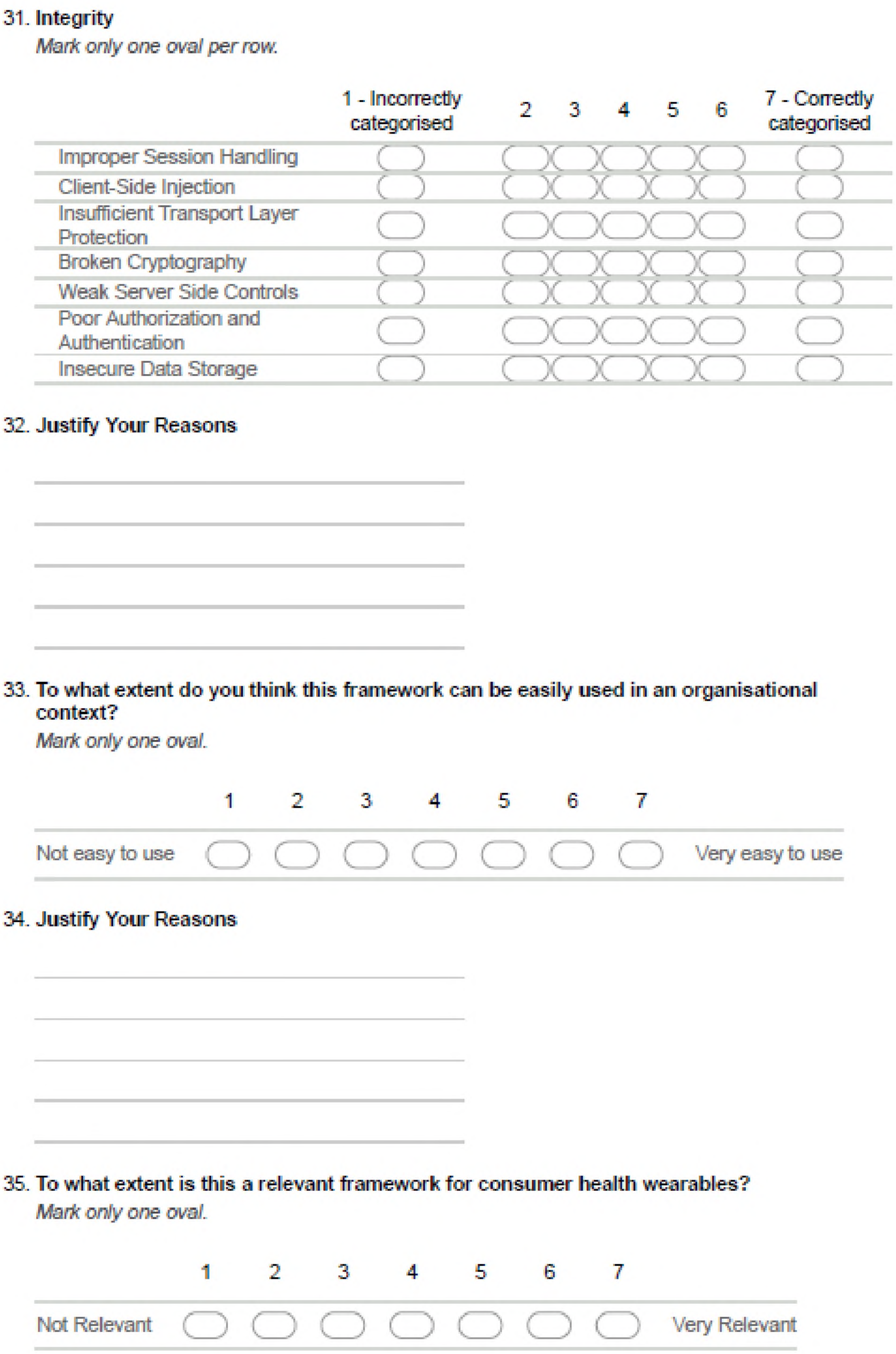
28. **Justify Your Reasons**

29. **Non-Repudiation**

Mark only one oval per row.

	1 - Incorrectly categorised	2	3	4	5	6	7 - Correctly categorised
Insufficient Transport Layer Protection	○	○	○	○	○	○	○
Poor Authorization and Authentication	○	○	○	○	○	○	○
Privacy Policy	○	○	○	○	○	○	○

30. **Justify Your Reasons**



31. **Integrity**

Mark only one oval per row.

	1 - Incorrectly categorised	2	3	4	5	6	7 - Correctly categorised
Improper Session Handling	○	○	○	○	○	○	○
Client-Side Injection	○	○	○	○	○	○	○
Insufficient Transport Layer Protection	○	○	○	○	○	○	○
Broken Cryptography	○	○	○	○	○	○	○
Weak Server Side Controls	○	○	○	○	○	○	○
Poor Authorization and Authentication	○	○	○	○	○	○	○
Insecure Data Storage	○	○	○	○	○	○	○

32. **Justify Your Reasons**

33. **To what extent do you think this framework can be easily used in an organisational context?**

Mark only one oval.

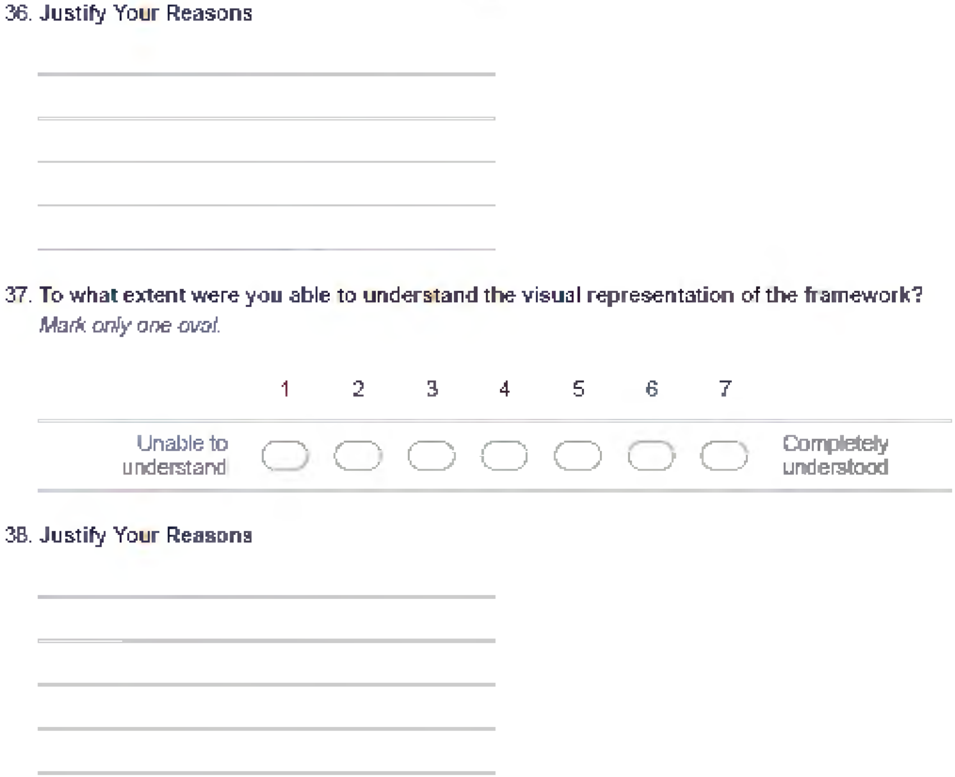
	1	2	3	4	5	6	7	
Not easy to use	○	○	○	○	○	○	○	Very easy to use

34. **Justify Your Reasons**

35. **To what extent is this a relevant framework for consumer health wearables?**

Mark only one oval.

	1	2	3	4	5	6	7	
Not Relevant	○	○	○	○	○	○	○	Very Relevant



36. **Justify Your Reasons**

____

____

____

____

____

37. **To what extent were you able to understand the visual representation of the framework?**
Mark only one oval.

	1	2	3	4	5	6	7	
Unable to understand	○	○	○	○	○	○	○	Completely understood

38. **Justify Your Reasons**

____

____

____

____

____

APPENDIX C – CRITERIA FOR EVALUATION

Vulnerability List

1. Third Party Analytics: Mobile health applications use analytic tools to assess health data. In the process of communicating to these third party analytical servers, metadata of a user's behavior and activity is collected

2. Lack of Access Codes: Many health applications and fitness trackers lack access codes or pins to protect them from being viewed by outside parties.

3. Location Tracking: GPS sensors are vulnerable to location tracking due to the unique ID displayed from Bluetooth signals

4. Lack of Privacy Policies: Mobile Health applications utilize permissions that require a user's authorization to use the device features. In many cases, health applications lack privacy policies to state how a consumer's data will be utilized and the manner in which it will be collected.

5. Insecure Data Storage: This is a result of poorly encrypted information, caching information and allowing global permissions. This insecure data storage occurs either internal (on board) or external (to cloud services)

6. Weak Server Side Controls: This occurs on the server side by not implementing proper security controls or configurations. Also disabling unnecessary back-end services.

7. Insufficient Transport Layer Protection: This applies to applications that use the HTTP protocol for communication (client-server). HTTPS provides transport layer protection, but if digital certificates are ignored or the use of plain-text communication is enforced. This places the information at risk.

8. Client Side Injection: SQL injection is a type of attack that uses SQL queries to manipulate a server in the favor of an attacker.This threat applies for mobile web and hybrid applications. These types are susceptible to SQL injection.

9. Poor Authorization and Authentication: As compared to websites, users of mobile applications are not online at all times for authentication. Authentication may also occur offline. Poor authorization and applying authentication poorly allows passwords, keys, or session tokens to be exploited.

10. Improper Session Handling: Sessions are used as a form of security, to allow a user to perform a specific action for a time period, until they are required to re-authenticate their credentials. This security is enforced by a server issuing a session cookie to a mobile application once a user has successfully authenticated and authorized service requests.

11. Unintended Data Leakage: Operating Systems, digital infrastructure and hardware are just but the few components within mobile devices that can change with time. Due to these changes, it is possible for data to be lost. This data loss may occur if a full understanding in not acquired to readjust the application to interact with the changes

12. Security Decisions via Untrusted Inputs: An application may receive data from various sources. This can be achieved in most cases by the Inter Process Communication (IPC) within a mobile application. To reduce any risk, the mobile application should communicate with other trusted applications it interacts with.

13. Lack of Binary Protections: Applications can be reversed engineered at a binary level. This reverse engineering can occur when a programmer was not involved in the development of the application at a binary level. If the application is not protected at this level, and attacker may find flaws and reconfigure the application and re-sell the application as its own

14. Broken Cryptography: Encryption is used to protect user data. However, by utilizing outdated algorithms and encryption techniques results in application insecurity

Consumer Health Wearable Threat Assessment Framework

Classification Categories

The framework contains six main categories. These include:

1. Authentication: As consumer health data is accessed, managed or viewed there needs to be authentication procedures of identifying a user.

2. Authorization: As consumer health data is accessed, managed or viewed there needs to be authorization methods. Authorization differs to authentication as it identifies whether a user has appropriate rights to access a resource.

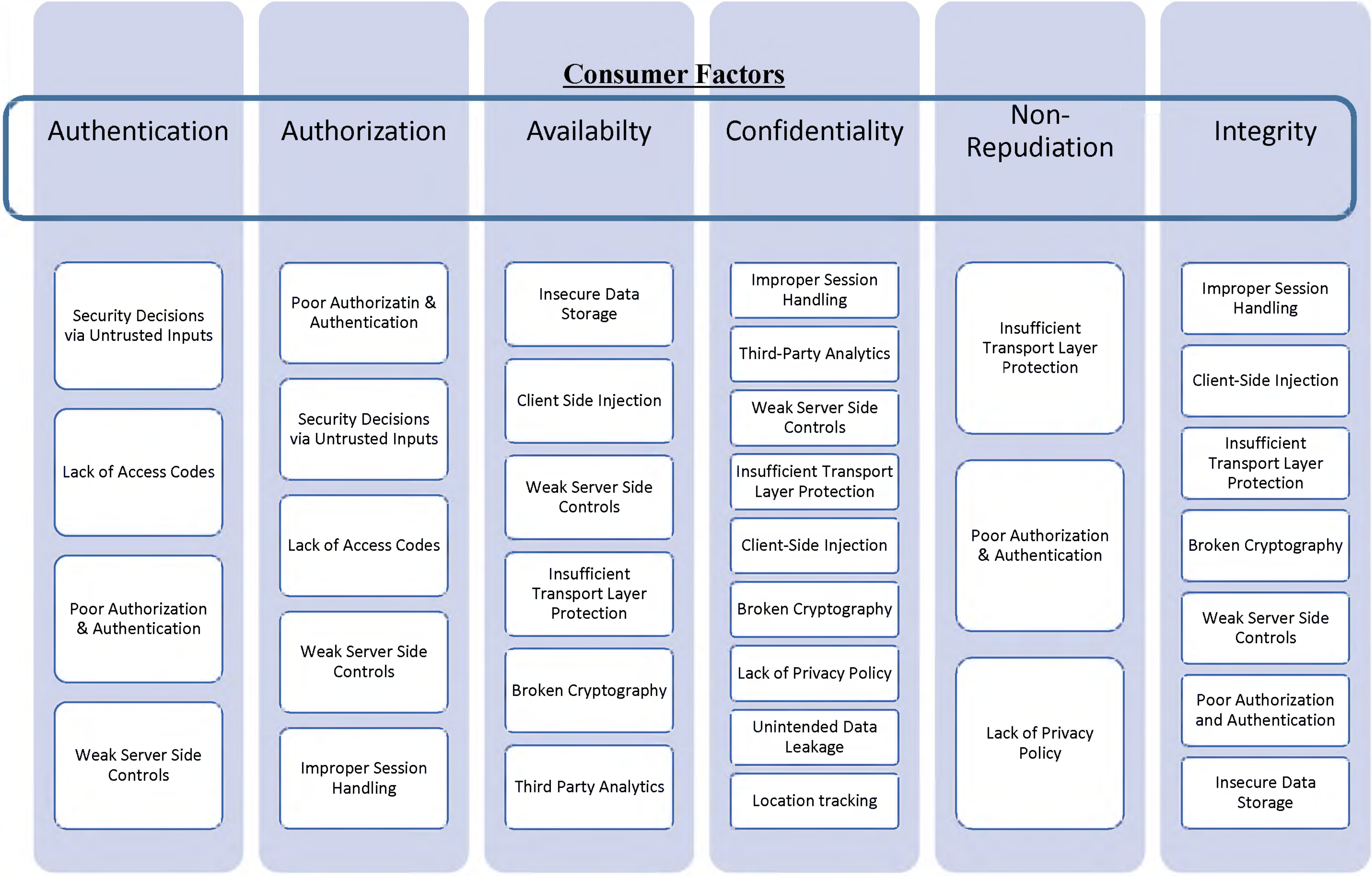
3. Availability: Consumer health data need to be available to authorized users when requested.

4. Confidentiality: As consumer health data is central to consumer health wearables. It is vital to keep this data secure and only revealing it to intended parties.

5. Non-Repudiation: The assurance that someone cannot deny something (digital signature, time stamps, certificates).

6. Integrity: When consumer health data is accessed or managed there is need to be assurance that it is not modified in transit or at rest. In case data is tampered, it can be identified.

Consumer Health Wearable Threat Assessment Framework



Consumer Factors

Authentication	Authorization	Availabilty	Confidentiality	Non-Repudiation	Integrity
Security Decisions via Untrusted Inputs	Poor Authorizatin & Authentication	Insecure Data Storage	Improper Session Handling	Insufficient Transport Layer Protection	Improper Session Handling
Lack of Access Codes	Security Decisions via Untrusted Inputs	Client Side Injection	Third-Party Analytics	Poor Authorization & Authentication	Client-Side Injection
Poor Authorization & Authentication	Lack of Access Codes	Weak Server Side Controls	Weak Server Side Controls	Lack of Privacy Policy	Insufficient Transport Layer Protection
Weak Server Side Controls	Weak Server Side Controls	Insufficient Transport Layer Protection	Insufficient Transport Layer Protection		Broken Cryptography
	Improper Session Handling	Broken Cryptography	Client-Side Injection		Weak Server Side Controls
		Third Party Analytics	Broken Cryptography		Poor Authorization and Authentication
			Lack of Privacy Policy		Insecure Data Storage
			Unintended Data Leakage		
			Location tracking		