

# **DEVELOPMENT OF AN M-COMMERCE SECURITY FRAMEWORK**

**By: Mufudzi Anesu Chapman Marufu**

BSc, SHCT

Submitted in fulfilment of the requirements for the degree of  
Master of Computer Science



**University of Fort Hare**  
*Together in Excellence*

**Faculty of Science and Agriculture**

**Department of Computer science**

**Supervisor: Dr K Sibanda**

**January 2014**

---

## **Keywords**

M-Commerce Security Framework, ICT4D, Threat Mitigation, Siyakhula Living Lab, Marginalised Rural Users

---

## Abstract

Research shows how M-Commerce has managed to find its way to previously inaccessible parts of the world as a major Information and Communication Technologies (ICT) tool for development due to widespread introduction of mobile phones in remote areas. M-Commerce has offered valuable advantages: anytime, anywhere, more personal, more location-aware, more context-aware, more age aware, always online and instant connectivity. But this is not without its problems, of which security is high on the list. The security issues span the whole M-Commerce spectrum, from the top to the bottom layer of the OSI network protocol stack, from machines to humans. This research proposes a threat-mitigation modular framework to help address the security issues lurking in M-Commerce systems being used by marginalised rural community members. The research commences with a literature survey carried out to establish security aspects related to M-Commerce and to determine requirements for a security framework. The framework classifies M-Commerce security threat-vulnerability-risks into four levels: human behaviour and mobile device interaction security, mobile device security, M-Commerce access channel security, wireless network access security. This is followed by a review of the supporting structures or related frameworks that the proposed framework could leverage to address security issues on M-Commerce systems as ICT4D initiatives. The proposed security framework based on the requirements discovered is then presented. As a proof-of-concept, a case study was undertaken at the Siyakhula Living Lab at Dwesa in the Eastern Cape province of South Africa in order to validate the components of the proposed framework. Following the application of the framework in a case study, it can be argued that the proposed security framework allows for secure transacting by marginalised users using M-Commerce initiatives. The security framework is therefore useful in addressing the identified security requirements of M-Commerce in ICT4D contexts.

---

## Table of Contents

Keywords .....	i
Abstract .....	ii
Table of Contents .....	iii
List of Figures .....	vi
List of Tables .....	vii
List of Abbreviations .....	viii
List of Publications .....	xi
Statement of Original Authorship .....	xii
Acknowledgements .....	xiii
<b>Chapter 1: Introduction .....</b>	<b>1</b>
1.1 Background .....	1
1.2 Research Problem .....	2
1.3 Research Questions .....	3
1.4 Research Objectives .....	4
1.5 Scope and Significance of the Study .....	4
1.6 Thesis Outline .....	5
<b>Chapter 2. M-Commerce Security in ICT4D .....</b>	<b>7</b>
2.1 ICT for M-Commerce .....	7
2.1 Security issues in M-commerce (research scope) .....	10
2.1.1 Human Aspect of Security .....	11
2.1.2 Mobile device security .....	12
2.1.3 M-Commerce Access Channels Security .....	13
2.1.4 Wireless Network Access Security .....	19
2.2 Related Work .....	24
2.3 Chapter Summary .....	29
<b>Chapter 3. Research Design &amp; Methodology .....</b>	<b>30</b>
3.1 Research Design .....	30
3.1.1 Classification of Research Design .....	31
3.1.2 Qualitative Studies .....	33
3.1.3 Execution of Tasks .....	34
3.2 Research methods .....	34
3.2.1 Literature Review .....	34
3.2.2 Model-building Study .....	35
3.2.3 Case Study Scenario .....	37
3.3 Research Methodology .....	38
3.3.1 Identification and selection of data sources .....	38
3.3.2 Data collection .....	39
3.3.3 Data documentation .....	39
3.3.4 Data capturing and editing .....	39
3.3.5 Data analysis and interpretation (synthesis) .....	40

3.4	Chapter Summary .....	40
<b>Chapter 4. Existing M-Commerce security structures.....</b>		<b>42</b>
4.1	Regulations Linked to Information Security in South Africa .....	42
4.2	Information Technology Governance Frameworks and Models .....	44
4.2.1	COBIT.....	44
4.2.2	Business Model for Information Security (BMIS) .....	46
4.3	M-Commerce regulatory requirements and Acceptable Information security standards.....	49
4.3.1	ISO Standards .....	49
4.3.2	National Institute for Standards and Technology (NIST) Special Publication (SP).....	51
4.3.3	Adoption of Security Models into Proposed Framework .....	51
4.4	Concepts, Assumptions, Beliefs and Information Security Theories .....	52
4.4.1	System theory.....	53
4.4.2	Defence in Depth .....	53
4.4.3	Intentional Culture of Security .....	54
4.5	Chapter Summary .....	55
<b>Chapter 5. ICT M-Commerce Security Framework (ICTMS Framework) .....</b>		<b>56</b>
5.1	Background.....	56
5.2	Valuable Security Framework Aspects Summarised.....	56
5.2.1	Security is as strong as its weakest link. ....	57
5.2.2	No one size fits all.....	57
5.2.3	Security as an afterthought.....	58
5.2.4	Security and Human Considerations .....	60
5.3	Properties of the ICTMS Framework .....	60
5.3.1	Framework integration facets.....	60
5.3.2	Multi-layered modular approach.....	61
5.3.3	Threat mitigation approach .....	62
5.3.4	Principles-based and open to continuous improvement .....	62
5.4	ICTMS Framework Architecture.....	62
5.4.1	Framework input .....	65
5.4.2	Threat mitigation levels.....	65
5.4.3	Deliverables .....	66
5.5	ICTMS Framework Functionality .....	67
5.5.1	M-Commerce security environment.....	68
5.5.2	Framework inputs .....	69
5.5.3	Deliverables .....	69
5.6	Application of the ICTMS Framework.....	70
5.6.1	Rural M-Commerce Ecosystem .....	70
5.6.2	Threat and Vulnerability Framework Levels in a Rural Context .....	71
5.6.3	Threat and Vulnerability Mitigation (Provision for Framework Deliverables) .....	71
5.7	Validation of the ICTMS Framework.....	72
5.8	Beneficiaries of the ICTMS framework .....	73
5.8.1	Communicating Security Requirements with Stakeholders .....	73
5.8.2	Identifying Gaps for Future Research .....	74
5.8.3	M-Commerce User Considerations .....	75
5.9	Significance of the ICTMS Framework.....	75
5.10	Limitations of ICTMS Framework .....	76
5.11	Chapter Summary .....	77
<b>Chapter 6. Conclusion and Contribution .....</b>		<b>79</b>

---

6.1	Chapter Summary and Findings .....	79
6.2	Summary of Conclusions.....	80
6.3	Recommendations for Further Research.....	82
6.3.1	Improving the framework .....	82
6.3.2	Further validation of the framework .....	82
6.3.3	Investigating new security frameworks.....	83
6.3.4	Investigating more requirements .....	83
6.4	Closing remarks .....	83
<b>References</b>		<b>84</b>
Appendices.....		92
Appendix A: Case Study Setup.....		93
	Participants	93
	Instruments/ Methods .....	95
Appendix B: M-Commerce Ecosystem within a Rural Setup .....		100
	Mobile Phone Ownership .....	100
	Obtaining a Mobile device .....	102
	Mobile device as storage device.....	104
	Services accessed with mobile phones .....	104
	Trust of M-Commerce Systems.....	107
	Siyakhula Living Lab Network Setup .....	108
	Telecommunications Networks .....	110
Appendix C: Threat and Vulnerability Assessment.....		112
	Threats and vulnerabilities associated with the human aspect.....	112
	Threats and vulnerabilities associated with the handheld devices .....	114
	Threats and vulnerabilities on M-Commerce access channel.....	116
	Threats and Vulnerabilities in the network access technologies enabling M-Commerce .....	117
Appendix D: Threat and Vulnerability Mitigation .....		121
	Human Aspect Level Security .....	121
	Device Level Security .....	122
	M-Commerce Access Channel Security.....	124
	Wireless Network Access Security.....	126
Appendix E: Questionnaire on Mobile Phone Usage .....		130
Appendix F: Focus Group Interviewing .....		136
Appendix G: Mobile phones Prevalence Observations .....		138
Appendix H: Focus Group Picture Display .....		139
Appendix I: Safe Mobile Phone Use Guidelines .....		140
Appendix J: Safe Practices Transacting Online .....		141

---

## List of Figures

Figure 2.1: A flowchart of a user request processed in an M-Commerce system ....	9
Figure 2.2: Threat/Vulnerability levels identified in M-Commerce Transacting ....	10
Figure 4.1: The business Model for Information Security .....	47
Figure 5.1: Components in the ICTMS Framework .....	63
Figure 5.2: ICTMS Framework functioning components .....	68
Figure 0.1: Study participants' age range demographics .....	93
Figure 0.2: Distribution of monthly income of employed participants .....	94
Figure 0.3: Siyakhula Living Lab Network Setup -Dwesa Area .....	95
Figure 0.4: Mobile phone presence among the participants .....	100
Figure 0.5: Mobile phone prevalence .....	101
Figure 0.6: Sources of devices the participants are using .....	103
Figure 6.7: The state of phone on first use by participants .....	103
Figure 0.8: Where users store most of their data .....	104
Figure 0.9: Mobile phone usage by participants .....	105
Figure 0.10: User trust levels towards use of mobile services .....	107
Figure 0.11: Factors influencing network choice .....	111
Figure 0.12: Frequency participants received spam calls or SMS .....	116
Figure 0.13: Frequency participants responded to the spam calls or SMSs .....	117

---

## List of Tables

Table 2.1: Security Concerns of Network User and Operator .....	23
Table 2.2: Security at Various Layers of WiMAX .....	23
Table 3.1: Classification of the Research Design .....	32
Table 3.2: Organisation of studies on the dissertation .....	41
Table 5.1: Comparison of framework layers with the five resource components in information systems .....	73
Table 0.1: Mobile phone brand prevalence.....	102
Table 0.2: Focus group themes mapping to elements of security.....	113
Table 0.3: Presence of open ports within the Ngwane base station.....	120
Table 0.4: Picture display of focus groups carried out at two training centres in SLL .....	139



---

## List of Abbreviations

AES	Advanced Encryption Standard
BMIS	Business Model for Information Security
CIA	Confidentiality-Integrity-Availability
COBiT	Control Objectives for Information and Related Technology
CoE	Centre of Excellence
CPE	Customer-premises equipment
DAN	Distributed Access Networks
DES	Data Encryption Standard
DOCRSA	Department of Communication, Republic of South Africa
ECA	Electronic Communications Act
EDGE	Enhanced Data rates for GSM Evolution
GEIT	Governance of Enterprise IT
GPRS	General Packet Radio Service
GSM	Global Systems for Mobile Communications
HTTP	Hypertext Transfer Protocol
ICASA	Information Systems Audit and Control Association
ICASA	Independent Communications Authority of South Africa
ICT	Information Communication Technologies
ICT4D	Information Communication Technology for Development
ICTMS	ICT Mobile Commerce Security Framework
IEC	International Electrotechnical Commission
IP	Internet Protocol
ISMS	Information Security Management System
ISO	International Organisation for Standardisation

---

ITGI	IT Governance Institute
IT	Information technology
IVR	Interactive voice response
J2ME	Java 2 Micro Edition
JSS	Junior Secondary School
LAN	Local Area Network
LOS	Line of sight
MAC	media access control
MSISDN	Mobile Station International Subscriber Directory Number
NFC	Near-Field Communication
NIST	National Institute of Standards and Technology
OSI	Open Systems Interconnection
PIN	Personal Identification Number
RFID	Radio-frequency identification
SLL	Siyakhula Living Lab
SMS	Short Message Service
SP	Special Publications
SRM	Standard reference materials
TLS	Transport Layer Security
UMTS	Universal Mobile Telecommunications System
USB	Universal Serial Bus
USSD	Unstructured Supplementary Service Data
VoIP	Voice over Internet Protocol
VSAT	Very Small Aperture Terminal
WAP	Wireless Application Protocol
WEP	Wired Equivalence Privacy

---

Wi-Fi	Wireless Fidelity
WiMAX	Worldwide Interoperability for Microwave Access

---

## List of Publications

- 1) Marufu, A.M.C. & Sibanda, K., 2013a. An M-Commerce Security Framework for ICT4D Contexts. In R. Volkwyn, ed. *Southern Africa Telecommunication Networks and Applications Conference (SATNAC)*. Spier Wine Estate, Stellenbosch, Western Cape, South Africa, pp. 271–276.
- 2) Marufu, A.M.C. & Sibanda, K., 2013b. Mobile Device Threats and Vulnerabilities as M-Commerce Enablers for Marginalised Communities : Siyakhula Living Lab. In *15th Annual Conference on World Wide Web Applications*. Cape Peninsula University of Technology: OpenJournals Publishing., pp. 1–14.
- 3) Marufu, A.M.C., Sibanda, K. & Scott, M. S, 2013c. Human Aspect in security of M-Commerce services in ICTD : A Siyakhula Living Lab Case Study. *International Journal of Computer Science Issues*, 10(5), pp.25–33. Available at: <http://goo.gl/8SwO7C>.

---

## **Statement of Original Authorship**

The work contained in this thesis has not been previously submitted to meet requirements for an award at this or any other higher education institution. To the best of my knowledge and belief, the thesis contains no material previously published or written by another person except where due reference is made.

Signature: \_\_\_\_\_

Date: \_\_\_\_\_

---

## Acknowledgements

I would like to thank the almighty God, the creator of the universe, for making this project possible under difficult and challenging conditions.

I would also like to thank my supervisor Dr Khulumani Sibanda, for his guidance, support, unbiased criticism and patience in the whole process of this research.

Special thanks go to my strong mother and siblings, for their encouragement and advice that kept me going at the hardest time of my life. Your financial, moral, and emotional support made this research possible.

Lastly but not least, I would like to thank the Department of Computer of Science and Telkom Centre of excellences for allowing me to pursue this research. Special mention goes to Ms Hafeni Mthoko, Mr Nobert Jere, Professor Mamello Thinyane, Ms Sibukele Gumbo, Mr MS Scott and my peers in the Computer Science Department.

---

## Chapter 1: Introduction

This chapter presents the background that inspired this study by briefly discussing how M-Commerce is finding its way to previously inaccessible parts of the world as major ICT tools for development. Security within the M-Commerce ecosystem is also emphasised. The chapter then outlines the statement of the problem in Section 1.2. Defining the statement of the problem leads to the aims and the objectives in Section 1.3. This is followed by a discussion of the research methodology and the significance of the study. An outline of the remaining chapters of the thesis concludes the chapter.

### 1.1 Background

Evidently, mobile transacting or mobile commerce (M-Commerce) has managed to find its way to previously inaccessible parts of the world as a major Information and Communication Technologies (ICT) tool for development due to widespread introduction of mobile phones in remote areas. Information and communication technology for development (ICT4D) can be described as the application of ICTs within the fields of socioeconomic development, international development and human rights (Heeks, 2009). These services are proving to be great ICT4D initiatives (West, 2013; Adesola, 2012; Duga & Getachew 2009)

Compared with the traditional desktop- based E-Commerce, M-Commerce has offered incomparable advantages: anytime, anywhere, more personal, more location- aware, more context-aware, more age aware, always online and instant connectivity (Zhang & Hilton, 2012). Despite these advantages, M-Commerce also faces some challenges, where security ranks high on the list of the cons. In a study by Yazdanifard et al. (2011) security was noted to be critical to the success of M-Commerce, and further research deemed a necessity in making mobile transactions more secure. Further study by Joubert & Belle, (2009); Zhang & Hilton, (2012); Networks, (2012), also supports the idea that security is a worthwhile endeavour to pursue in the M-Commerce field.

Security issues span the whole M-Commerce spectrum; from the top to the bottom layer of the OSI network protocol stack, and from machines to humans (Gururajan, 2006). Given such a setup, it is evident that security can only be as strong as its weakest link. All security considerations (including such models of security as CIA Triad) have to be thought through

---

and integrated in every single domain (people, process, and technology) of a business, community or institution (Andress, 2011). The technology factor of the equation is rarely contested, and most researchers agree that “people” and “process” are equally important (Mark, 2007).

From the technology end, M-Commerce security is tightly coupled with mobile device security, network security and end- to- end protocols. Without security of such underlying technologies and protocols, M-Commerce may not live up to its expectations. Technology-wise there is lack of unified security standards, different wireless networking technologies and mobile computing platforms support different aspects and levels of security features. More than this, the lack of security as a core element in the initial design of the infrastructure has made networks, mobile platforms and information systems increasingly vulnerable to continuous and innovative intrusions and attacks (Slyke & Belanger, 2002; Grami & Schell, 2004).

From the “people” and “process” end, security of M-Commerce systems cannot be addressed by technical means alone; a significant aspect of protection boils down to the attitudes, awareness, behaviour and capabilities of the people involved. At present, factors such as lack of awareness and understanding, combined with unreasonable demands from security technologies, can dramatically impede their ability to achieve this security. A large portion of the South African rural communities only have intermittent access to computers (now recently mobile phones) and are not familiar, nor entirely comfortable, with the use of internet communication or electronic devices (Grobler et al., 2011).

With privacy and security issues such as identity theft, fraud and money laundering on the rise and even affecting the literate users of mobile devices and M-Commerce systems, rural users may be left greatly exposed if the already existing security measures and mechanisms are not carefully scrutinised to create secure M-transacting solutions. Further, M-Commerce, which has been stated as an important tool in ICT4D, might fail to live up to its fullest potential. Evidently there is need to address the numerous issues plaguing the M-Commerce ecosystem.

## **1.2 Research Problem**

Vast arrays of security patches, models and frameworks have been suggested within research in an effort to alleviate M-Commerce security issues. A point of departure is that the different



---

frameworks generalise and look at security from a broader and more abstract level. Minor consideration of grass- root end-user security is looked at. In addition, to the best of our knowledge the existing security patches and models do not take a holistic approach or look at security systemically. Thus there is a need to provide a security framework that integrates these disparate security tools to provide a holistic, secure environment for M-Commerce systems within an ICT4D context.

### 1.3 Research Questions

The research questions are formulated in such a way as to guide the research process to reach the research objectives. Chapters 2, 4 and 5 of the dissertation provide specific answers that contribute to the overall answer to the main research question.

The main research question for this study is: ***How can an M-Commerce security framework be developed to solve security issues within an ICT4D context?***

To answer this question one needs to answer the following sub-questions:

Sub-question 1: ***What security aspects are related to M-Commerce as an ICT4D initiative?***

The aim of this question is to identify security aspects related to M-Commerce and to provide a theoretical context for the research. This question also seeks to determine characteristics that will be used as requirements for a security framework

Sub-question 2: ***What are the requirements of an M-Commerce security framework?*** This question seeks to establish characteristics that will be used as requirements for an M-Commerce security framework. This involves reference to currently established frameworks.

Sub-question 3: ***What existing security structures are related to the M-Commerce security?***

The aim of this question is to identify the existing security structures: frameworks, models and theories, which are currently in place and inspiring the development of the proposed framework context. This question is intended to evaluate these existing security structures and to determine components applicable to the proposed M-Commerce framework.

---

Sub-question 4: *What are the components of a security framework for the M-Commerce security framework?* The aim of this question is to identify elements or components that are needed to compile a security framework from the existing security structures and M-Commerce security environment.

#### **1.4 Research Objectives**

The main aim of this study is to develop a security framework which seeks to ensure secure transacting by users using an array of M-Commerce initiatives at their disposal.

The objectives of the study are formulated in such a way that they provide the means for answering the proposed research questions. The objectives of the study are:

Objectives

- To describe the security aspects related to M-Commerce
- To establish the requirements of an M-Commerce security framework
- To determine components from existing security frameworks that can be used for M-Commerce security
- To establish the components of the proposed M-Commerce security framework
- To demonstrate the applicability of the M-Commerce security framework.

#### **1.5 Scope and Significance of the Study**

The choice of developing a security framework rather than focus on a single protocol, was inspired by the idea that a framework is generally more comprehensive than a protocol and more prescriptive than a structure. In this research it is argued that developing mitigation measures as standalone solutions to address the aforementioned security issues would not be comprehensive enough. There is need to integrate these measures in a way that would blend in well with existing frameworks or security structures in M-Commerce systems being used by marginalised rural users. The proposed framework should integrate the different

---

mitigation measures, solutions and suggestions, as well as complementing already- existing security structures in the M-Commerce sphere. Importantly, a framework of such a nature should be extensible enough to correlate or fall in place with already- existing security standards, frameworks and models. It is envisaged that implementation of such a framework will fill in the security vacuum between the upper-level security structures from M-Commerce platform developers and the lower- level user-end.

The framework proposed in this research permits a detailed evaluation of security issues plaguing M-Commerce environment by implementing a security analysis on a module- by- module basis, thereby ensuring that M-Commerce service providers who understand discovered threats can better decide where and how to deploy mitigation technologies.

Thus, the current research is important as it seeks to provide solutions to enhance current security in M-Commerce systems as ICT4D initiatives. Findings that are unearthed will provide a valuable background for future authors seeking to tackle the issue of security within an ICT4D research space.

## **1.6 Thesis Outline**

The following table outlines the chapters of the dissertation and provides a brief description of the contents of each.

<b>INTRODUCTION</b>	<p><b>Chapter 1: Introduction</b></p> <p>Provides a background to the study, research problem, research objectives, Research questions, delimitation of the study, and the structure of the dissertation.</p>
<b>THEORETICAL FRAMEWORK</b>	<p><b>Chapter 2: Overview of M-Commerce</b></p> <p>Provides an overview of M-Commerce as an ICT4D initiative, then details the security threats that plague the whole M-Commerce ecosystem. The chapter also describes the security aspects and the requirements of an M-Commerce security framework from literature</p>
<b>DESIGN AND METHODS</b>	<p><b>Chapter 3: Research design and methodology</b></p> <p>Provides a discussion of the research design followed to develop a security framework M-Commerce applicable to a rural context. Motivation for the selected research design is presented together with its limitations</p>
<b>RESEARCH FINDINGS AND ANALYSIS</b>	<p><b>Chapter 4: Analysis of existing M-Commerce security structures- frameworks, models</b></p> <p>The chapter extracts requirements of a security framework and establishes supporting frameworks to which the suggested framework may integrate.</p>
	<p><b>Chapter 5: A security framework for M-Commerce system</b></p> <p>The chapter presents the proposed security framework. Components and functionalities of the framework are explained. The framework is validated and evaluated by use of a case study.</p>
<b>CONCLUSION</b>	<p><b>Chapter 6: Conclusion and Contribution</b></p> <p>The chapter discusses the contribution made by the study. It presents a summary of the study and its findings, and provides recommendations for future research.</p>
<b>REFERENCES</b>	List of literature referred to in the dissertation.
<b>APPENDICES</b>	List of appendix pages

---

## Chapter 2. M-Commerce Security in ICT4D

This chapter comprises the literature review which summarises, interprets, and critically evaluates existing "literature" (or published material) in order to establish current knowledge of our research subject. The purpose for doing so was to establish the need for additional research, and define the topic of our inquiry. Thus, a background on ICTs as tools of poverty alleviation, the influence ICTs have been having in Africa on marginalised rural communities and how M-Commerce is a valuable ICT4D initiative are presented first. This is followed by a tour on security issues: the current security trends affecting M-Commerce; models/fundamentals of security and security issues this research seeks to address. Related work then concludes the proceedings of the chapter.

### 2.1 ICT for M-Commerce

Information and Communication Technology for Development (ICT4D) is a general term referring to the application of Information and Communication Technologies (ICTs) within the fields of socioeconomic development, international development and human rights (Heeks, 2009). Simply put, ICT4D is the use of ICT to enhance development processes/initiatives in both developed and underdeveloped societies. This research stands firmly with the ideology that ICT can be harnessed more effectively for development. This is acknowledged by the United Nations Millennium Development Declaration, which calls to ensure that the benefits of new technologies, especially information and communication technologies are available to all. ICT can play a role in reaching Millennium Development Goals such as the elimination of extreme poverty, combating serious disease, and achieving universal primary education and gender equality by improving access to information and by enabling communication (Braund, 2006; Zefa, 2010). ICTs permit information and knowledge to expand in quantity and accessibility (Duga & Getachew, 2009).

However, marginalised residents in developing countries often lack information vital for the work they do: current market prices, weather reports, and new opportunities for earning income among others. Hence, if improved access to information and channels of communication are made available to poor communities, ICTs can be leveraged to raise income significantly. Information Economy report 2010: Enterprises and Poverty Alleviation,

---

shows that in low income countries, farmers, fishermen and entrepreneurs have used mobile phones and other forms of technologies to improve their livelihoods.

Furthermore, due to the rapid diffusion of mobile telephony it is becoming possible for marginalised communities to have immediate access to interactive communications. Penetration rate of mobile phones is much higher than other ICTs such as fixed telephone subscriptions, internet use and broadband subscriptions (Languepin, 2010). In addition, a considerable number of research studies also indicate that the use of mobile phones as ICT4D enablers has proven to be a success (Diga, 2007; Languepin, 2010; World Wide Worx, 2011). It is also due to this proliferation of mobile phones that M-Commerce has been recognised as a valuable ICT4D initiative in alleviating poverty in developing countries (Yusoff & Lim, 2003; Diga, 2007; Summary, 2008.; Mathias, 2009; Adesola, 2012; West, 2013).

M-Commerce is a subset of e-Commerce (Hsieh, 2007; Sharma et al., 2011), and any transaction involving the transfer of ownership or rights to use goods and services, which is initiated and/or completed by using mobile access to computer-mediated networks with the help of an electronic device (Tiwari & Buse, 2007). M-Commerce offers valuable advantages as ICT4D initiatives: anytime, anywhere, more personal, more location- aware, more context-aware, more age aware, always online, instant connectivity (Zhang & Hilton, 2012) and employment creation. The products and services M-commerce provides include 1) mobile ticketing, 2) mobile vouchers, coupons and loyalty cards, 3) content purchase and delivery 4) location- based services e.g. weather, local discounts, 5) information services e.g. news, stock quotes, traffic reports 6) mobile banking, 7) mobile Storefront, 8) Mobile marketing and advertising among others. The major focus of this study, however, lies on mobile payment and banking services.

In order to deliver the above mentioned M-Commerce services, the M-Commerce value chain participants are the major driving force behind the M-Commerce supply chain (Mennecke & Strader, 2003). According to Hsieh (2007), these can be grouped into three major categories: 1) Technology developers, 2) Technology applications developers 3) Service Providers. M-Commerce participants fundamentally include mobile consumers, wireless network providers, content providers, service providers, application developers and technology providers. Varshney and Vetter (2002) suggested an M-Commerce life cycle that includes application developers, content providers, and service providers.

An M-Commerce system is inherently interdisciplinary and could be implemented in various ways. Lee et al. (2005) suggested the structure of an M-Commerce system and a typical example of such a system. The system structure includes six components: i) M-Commerce applications, ii) mobile handheld devices, iii) mobile middleware, iv) Wireless Networks, v) wired networks, and vi) Host Computers.

To explain how the mobile commerce components work together Figure 2.1 shows a flowchart of how a user request is processed by the components in a mobile commerce system, along with brief descriptions of how each component processes the request.

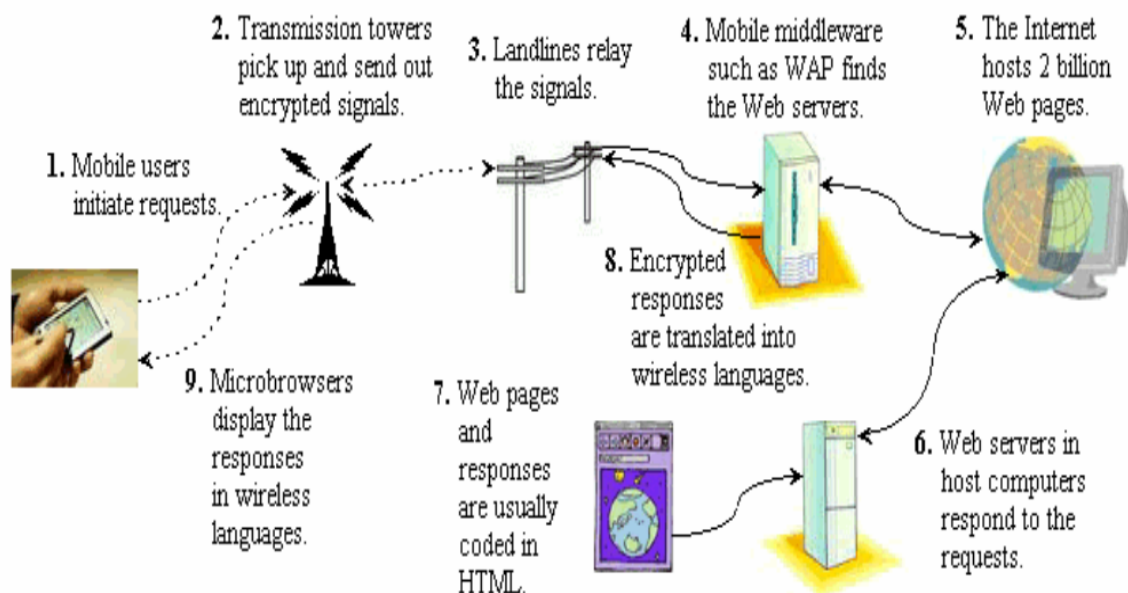


Figure 2.1: A flowchart of a user request processed in an M-Commerce system (Lee et al., 2005)

Driven by the ubiquitous deployment of mobile systems, widespread use of the Internet, rapid advances in wireless technologies, the insatiable demand for high-speed interactive multimedia services, and the growing need for secure wireless machine-to-machine communications, M-Commerce is rapidly approaching the business forefront. According to the latest predictions and occurrences (Dhir et al., 2012) the future of M-Commerce is bright. Regardless of these positive predictions for M-Commerce, its prosperity and popularity will be brought to a higher level (in ICT4D contexts) only if information can be securely and safely exchanged among end systems.

From the realisation of the security vulnerability categories discussed, a framework was suggested as a solution to tackle the security issues related to M-Commerce transactions. The next section presents the related works from academia done to alleviate some of these security dilemmas in ICT4D tools like M-Commerce through solutions, frameworks and/or models

## 2.1 Security issues in M-commerce (research scope)

The security and privacy issues span the whole M-Commerce spectrum, from the top layer to the bottom of the OSI network protocol stack, from machines to humans. However, if a typical end-to-end M-Commerce transaction is considered, the major security threats and weaknesses when carrying out the transaction may be categorised as: lack of user awareness, limited computing power, possible loss or theft of device, incomplete authentication schemes, the use of wireless transmissions, vulnerable operating systems, and the use of unsecured technologies (Fuller, 2005). In this research the aforementioned threats and vulnerabilities can be classified into four main levels of security threats and vulnerability: human behaviour and device interaction (human aspect; [1a], [1b]), mobile device security [2], M-Commerce access channel [3], and the underlying network infrastructure/technologies (wireless network access channels [4]) sever side and back end systems security (5,6). Figure 2.2 shows a visualisation of the different categories.

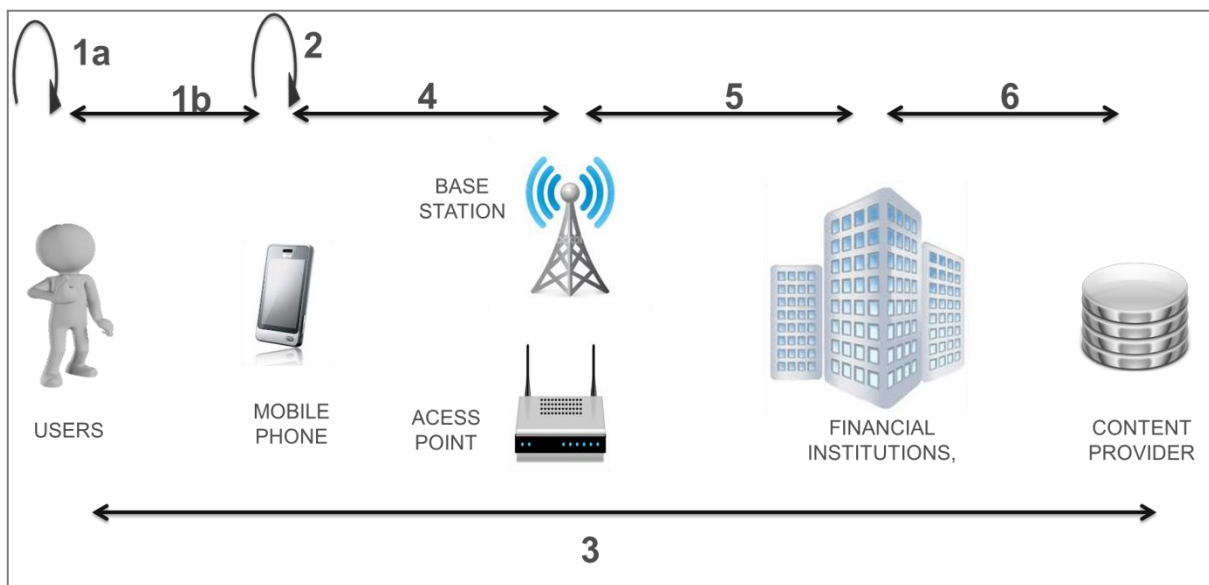


Figure 2.2: Threat/Vulnerability levels identified in M-Commerce Transacting (Marufu & Sibanda, 2013a)



---

Likewise this section provides a brief background to the various security issues at the four levels that need to be addressed in the immediate future for the better security of M-Commerce systems. The separation of these vulnerabilities and threat levels allows for a more understandable approach to address these security issues. The following subsections therefore explore each level of threats/vulnerabilities in depth, providing a brief background to the various security issues needing to be addressed, putting in perspective the levels to a marginalised rural area context.

### **2.1.1 Human Aspect of Security**

Focus in Information Technology (IT) and computer security has been drawn towards the technical aspects of the discipline such as firewalls, antivirus and intrusion detection systems among others. However, it is increasingly being recognised that technology alone cannot deliver a complete solution to security. People represent a key facet in achieving security. Literature suggests that this is often the point of failure (Dlamini et al., 2009; Furnell & Clarke, 2012). Hence there is a need to address human aspects of security (Humaidi & Balakrishnan, 2012). At the core of every IT security environment, people must understand the threats they face and be able to use the protection available to them, and although this has not been entirely ignored, it has not received the level of attention that it merits (Furnell & Clarke, 2012). Indeed, security surveys commonly reveal that the more directly user-facing aspects such as policy, training and education are prone to receiving significantly less attention than technical controls such as firewalls, antivirus and intrusion detection. The underlying reason for such disparity, as stated by (Furnell & Clarke, 2012), is that the human aspects are in many ways a more challenging problem to approach, not least because they cannot be easily targeted with a product-based solution. There is also a direct overlap of the human aspect into the technical area, with issues such as the usability and acceptability of technology solutions having a direct impact upon the actual protection that they are able to deliver. Another problem that most authors seem to agree on is that mobile device security and M-Commerce system security is a human versus human conflict (Mathias, 2009). In other words, in information security the adversaries are not the computers and programs that are used as tools, but the persons behind the tools.

Hence in the present research, it is acknowledged that M-Commerce security cannot be addressed by technical means alone, and that a significant aspect of protection comes down to the attitudes, awareness, behaviour and capabilities of the people involved. Indeed, people

---

can potentially represent a key asset in achieving a secure M-Commerce system, but at present, factors such as lack of awareness and understanding, combined with unreasonable demands from security technologies, can dramatically impede their ability to do so. Ensuring appropriate attention and support for the needs of users should therefore be seen as a vital element of a successful security strategy.

While the human aspect refers to all the different levels where human interaction with the processing of a transaction is evident across the M-Commerce system, the human aspect phase of this research specifically addresses information security issues that relate to end-users behaviour and their use of M-Commerce systems- enabling tools, i.e. mobile phones. It concerns the methods that inform and guide users' understanding of security, and the technologies that can benefit and support them in achieving protection. The reason for focussing on end users is because other human interactions security issues are catered for by enterprise policy, security frameworks and models (COBIT, IBMS, etc.). The end-user side of M-Commerce transacting is the more exposed area which the suggested framework in this research dwells much on (Marufu et al., 2013).

### **2.1.2 Mobile device security**

From the information security view, information in mobile devices is an asset like other important business assets, which is therefore essential to an organization's business and consequently needs to be suitably protected. The use of a mobile device involves the sharing of its functions between the official and personal use of the data in the same device.

As Couture (2010) states, a holistic analysis of the mobile threat environment, giving appropriate attention to threats generated by the unique portability of the devices themselves and by their highly connected natures, is necessary in any environment considering placing sensitive data on mobile networks. This is supported by our work in (Marufu & Sibanda, 2013b).

Previously, hackers were inspired by curiosity and personal notoriety; the motivations have shifted almost completely to financial gain. So far, there has not been a strong need to exploit mobile devices for use in botnets or for the personal or corporate information stored within (Couture, 2010). With the significant increase of data speeds and always-on connectivity, exploiting mobile devices is becoming more palatable as a means to leverage mobile devices

---

to send spam or launch denial of service attacks. Hence, as more users push valuable data to their phones, they can only become a desirable target to cyber criminals.

Further, the diversity of handsets, operating systems and their configurations, installed software and service providers makes establishing a security baseline drastically more challenging than even a heterogeneous Windows/Unix desktop environment, where mature security best practices and thorough expert knowledge exists (Couture, 2010).

Mobile phones share many of the vulnerabilities of personal computers, but the attributes that make mobile phones easy to carry, use, and modify open them to a range of attacks (Jansen & Ayers, 2007). This could be attributed to the idea that mobile handheld devices are being developed with specialized built-in hardware to provide productivity benefits (Ben-asher et al., 2011); they are also posing new risks to users on M-Commerce transacting platforms, discussed later in this section. A vast array of research has been conducted pointing out the various threats that affect mobile devices/phones in the works of (Fuller, 2005; Espiner, 2006; Jansen & Scarfone, 2008; Jansen & Ayers, 2007; Al-zarouni, 2007; Team, 2010; Ruggiero & Foote, 2011; Schlegel et al., 2011; ViaForensics, 2012; Marufu & Sibanda, 2013b). The different channels that make mobile phones susceptible to threat as M-Commerce enablers include: possible theft or loss, vulnerable operating systems, infected mobile applications, use of unsecure technologies, lack of complete authentication, mobile spam, and location tracking services. Various researchers accept that a multitude of threats exist for mobile phones, and that the list will continue to grow as new vulnerabilities draw the attention of malicious factors (Jansen et al. 2007; Ruggiero & Foote, 2011). In addition, Verma (2011) and Sawyer et al., (2012) made valuable contributions on mobile vulnerability and exploitation assessment on mobile apps.

The device security level in this current research is intended to provide solutions on how mobile devices as M-Commerce enablers can protect user data. Since mobile phones are enablers of M-Commerce systems, failure to realise and address the various threats on these tools may have long-term repercussions on the security of M-Commerce systems, and hence the adoption of these systems.

### **2.1.3 M-Commerce Access Channels Security**

Transacting on an M-Commerce platform can either be through Short text message (SMS), Unstructured Supplementary Service Data (USSD), Near Field Communication (NFC),

---

(Interactive Voice Recognition) IVR or Applications (Web, Hybrid or Native based Applications).

Using SMS, the customer sends a simple text message, which identifies the service and the amount to be paid, to a short code, and is given the goods/services, usually with an SMS-based confirmation. USSD is a mobile phone interface which has a web ‘look and feel’, based on browsing menu options. This gives customers a great deal of flexibility and allows operators to expand the number of interactive services they offer their customers. IVR is the most well-known way to interact with the system to top up a prepaid credit account. It identifies the subscriber who can perform an m-payment by entering the product or service id and the amount to be paid. Web will be the natural interface for on-portal payments. The customers will be authenticated by entering their Mobile Station International Subscriber Directory Number (MSISDN) and Personal Identity Number (PIN) code. They could also potentially receive a confirmation SMS on their mobile phone to increase the overall security of the transaction.

The current research study takes a look at only those M-Commerce- enabling channels for transacting available to the marginalised users thus far, SMS, USSD, Web-based applications and Mobile based applications. Other channels such as NFC, IVR, and RFID were not included in the channels under analysis in this study as these technologies/channels are less common among rural users thus far, but as an area for future work the proposed framework in the current research is open to their inclusion. The following sub-sections present an in-depth discussion of the five chosen channels, pointing out security issues affecting the channel(s) and related work addressing the security issues.

### ***2.1.3.1 Security issues with SMS***

SMS is a popular service protocol within the GSM standard, which has long been considered generally harmless. Misuse of SMS often amounted to nothing but unsolicited SMS spam directed at user handsets. The initial idea for SMS usage was intended for subscribers to send non-sensitive messages across the open GSM network. Mutual authentication, text encryption, end-to-end security, non-repudiation were omitted during the design of GSM architecture. While the most common use of SMS is messaging, the underlying protocol, Wireless Application Protocol (WAP) provides the ability to send network and phone configuration details over the mobile phone network. In their paper Miller & Mulliner (2009)

---

showed the techniques they developed to fake or ‘inject’ the transmission of SMS within a phone’s protocol stack which allowed them to send massive amounts of ‘text messages’ and permitted them to bombard the phone with thousands of permutations of non-standard message formats. This technique, known as fuzzing, revealed certain cases where a particular message would result in a crash or some other unexpected outcome that can be leveraged to deny service to the phone user, or possibly inject malware onto the phone. The recipient’s phone can even be hacked while in ‘sleep’ mode, and the exploit can be leveraged to retrieve the phone’s unique identification numbers, personal information or other data stored on the device. Variations of the hack are effective against Windows Mobile, Apple iPhone and Google Android. At the Blackhat conference, 2009, Miller showed how he could send a malformed SMS message and crashes the recipient iPhone, generating a denial of service on the recipient handset, or executes arbitrary code. A potential weakness is that SMS messages are generally not blocked, firewalled or examined by network intrusion detection systems, and thus could constitute a simple circumvention of the best-laid network security plans, providing a means through which to infect a device with malware while completely circumventing IP network connectivity and any protective measures in place. “SMS is an incredible attack vector for mobile phones”, said Miller. All that is needed is one’s phone number. There is no need for clicking a link or anything. SMS remains largely unexplored and may, under scrutiny, reveal further security vulnerabilities.

SMS spoofing is another attack that involves a third party sending out SMS messages that appear to be from a legitimate sender. It is possible to alter the originator’s address field in the SMS header to another alpha-numerical string. It hides the original sender’s address, allowing the sender to transmit hoax messages and perform masquerading attacks. Further, by default, data format for SMS messages is sent out in plaintext. The only encryption involved during transmission is the encryption between the base transceiver station and the mobile station. End-to-end encryption is currently not available. The encryption algorithm used is A5, which has been shown to be vulnerable. A more secure algorithm is therefore needed. The SMS security mechanism relies on GSM/UMTS signalling plane security mechanism. Likewise an SMS may be eavesdropped by the man-in-the-middle attack, as no encryption is applied to SMS message transmission. Chikomo et al. (2006) presented some solutions to some of the challenges in transacting using SMS for banking.

In South Africa a recent trend that is being observed with much concern is the idea of scams being propagated through the different network providers. On the same note network

---

providers such as MTN and Vodacom have dedicated pages on their official websites on “Current Scams and Hoaxes” which the general public should be aware of. These include:

MTN	Vodacom
SMS scam	Nokia Promotion Scam
MTN Play Scam	Recharge Voucher Scam
Please Call Me hoax	Airtime transfer Scam
FIFA Competition Scam	FIFA Mobile Draw Scam
Phishing Sites	International call/call forwarding fraud

What is even more interesting is that network providers are aware of these scams and hoaxes and advise subscribers to exercise extreme caution as these communications are fraudulent. They advise customers that should they suspect that an electronic communication sent to them is false, they are not to respond or engage.

### ***2.1.3.2 Security Issues with USSD***

USSD applications can be implemented using a wide variety of mobile application platforms such as J2ME, WAP, SIM Toolkit, CAMAL, or simply using USSD commands. The strategy for USSD channel determines how, where, and when the USSD-based M-Commerce solution can be adopted to realize the underlying mobile commerce business models (Goudar, 2010). Overall, USSD possesses no separate security properties; instead it relies on GSM/UMTS signalling plane security mechanism (Chikomo et al., 2006). Likewise the biggest debate likely to be exchanged by most operators and financial regulators today in using USSD channels is that they offer no encryption. As such, they have been deemed “insecure” because of the “apparent” potential high risk in having a subscriber’s MPIN exposed to a fraudster.

### ***2.1.3.3 Mobile Applications***

The numbers of M-Commerce applications (apps) and application types have grown at rates matching the rate at which Web sites were launched during the early days of the Internet commerce boom. A wide array of financial apps can provide value to the mobile phone owner, regardless of whether the owner is a business or a consumer.

---

One of the most significant developments in mobile device technology has been the community-driven application market. Although these lightweight programs provide minimal functionality, they often are innovative and inexpensive, which increases their appeal. Applications are either web-based (mobile web apps) or thick clients that need to be installed on the mobile device (native apps). These two application architectures pose different risks to both the local device and the user data, and they require different front-end, or black box, testing strategies (EYGM, 2012)

Mobile Web apps can be further separated into two groups; WAP-based and HTML5-based web apps. Mobile websites are often referred to as WAP sites. WAP stands for Wireless Application Protocol, which is a standard used to guide how the mobile version of a website is designed, created, and displayed (Singel & Preneel, 2003). Some mobile websites have unique device detection capabilities; able to identify that a visitor is using a mobile device, and the kind of device being used (Meng & Ye, 2008). The mobile website is then modified so that it displays in the best format possible for the specific device. One advantage of this is that the mobile website is accessible from a wide variety of mobile devices and the user does not have to download a program to their mobile device in order to view the website. The only requirement would be data connection and a mobile browser, which is a standard feature pre-installed on many phones sold today.

#### *2.1.3.3.1 Web-based Mobile Applications Vulnerability*

The mobile device resident mobile browser is used to access the mobile customized WAP or web applications, with which customers can engage in various types of mobile business transactions. This channel can be widely used by educated users (technically savvy) and at the same time many uneducated or under-educated customers may find this channel difficult to use. This channel is relatively easier to adopt, since the existing web channels and web applications can be quickly customized for mobile devices (Goudar, 2010).

Although web applications can provide convenience and efficiency, there are also a number of new security threats, which could potentially pose significant risks to an organisation's information technology infrastructure if not handled properly. The rapid growth in web application deployment has created more complex, distributed IT infrastructures that are harder to secure (HKSAR, 2008b). However, now that more and more attacks are targeting security flaws in the design of web applications, such as injection flaws, traditional network

---

security protection may not be sufficient to safeguard applications from such threats (Goudar, 2010). These threats originate from non-trusted client access points, session-less protocols, the general complexity of web technologies, and network-layer insecurity. With web applications, client software usually cannot be controlled by the application owner. Input from a client running the software cannot therefore be completely trusted and processed directly. An attacker can forge an identity to look like a legitimate client, duplicate a user's identity, or create fraudulent messages and cookies. In addition, Hypertext Transport Protocol (HTTP) is a session-less protocol, and is therefore susceptible to replay and injection attacks (HKSAR, 2008a). Hypertext Transport Protocol messages can easily be modified, spoofed and sniffed. As such, organisations must understand and be fully aware of the threats to properly implement appropriate defensive strategies

Consumers use web pages displayed or additional applications downloaded and installed on the mobile phone to make a payment. It uses WAP (Wireless Application Protocol) as underlying technology and thus inherits all the advantages and disadvantages of WAP.

The Wireless Application Protocol (WAP) was initially proposed as a way to get Internet (or a sort of Internet) to small wireless and mobile devices, e.g. mobile phones, while accommodating the special characteristics of such devices (Clarke, 2008). WAP became an application environment and a set of communication protocols for wireless devices. It enables the wireless devices, independent access to the Internet. WAP bridges the mobile world and the Internet. It also connects the corporate intranets. Because of this, users can access the same amount of information by using a pocket-sized device as they can from a desktop PC.

WAP, an industry-initiated world standard, has emerged as a common communications technology and uniform interface standard for presenting and delivering wireless services on wireless devices. WAP specifications include a micro-browser, access functions, and layered communication specifications for sessions, transport, and security. The WAP gateway is used to translate the WAP protocols (protocols that have been optimized for low bandwidth, low power consumption, limited screen size, and low storage) into the traditional Internet protocols (TCP/IP). These specifications enable bearer-independent and interoperable applications. In short, future trends clearly indicate that the device manufacturers, as well as service and infrastructure providers, will keep adopting the WAP standard (Grami & Schell, 2004).



---

#### *2.1.3.3.2 Native Mobile Application Vulnerability*

In this channel, the mobile device specific (APIs, OS) mobile applications are used to conduct the mobile transactions. The mobile applications are device-specific and are OS-specific, and usually provide rich user interfaces for the mobile devices. The cost associated with mobile application channel is relatively high, as the applications need to be developed to a specific set of devices and also the customer coverage is somewhat restricted to those specific devices upon which the specific mobile applications can run. The rich user interfaces and secured transaction processing capabilities offered by these application APIs, can be very useful to bring tailored mobile solutions to target customers (Goudar, 2010).

J2ME (Java 2 Micro Edition) is a feature that allows the device to run small, user-installable software applications written especially for mobile devices (Kmal and Abdullah 2009). J2ME requires a phone that can support the GPRS download of the initial application, or the phone should be pre-provisioned with the application. The phone would have to also have enough memory capability to support or house the application, and sufficient graphic ability to display the application. Once installed on the phone, the application would use GPRS, USSD or SMS to carry the consumer data or instruction from the device to the service provider. This can be in an encrypted format. The user experience is similar to that of a web site and brings the same content and graphic rich benefits of the internet to the mobile phone. A consumer would browse through his phone menu until he finds the J2ME application, select and launch the application, and follow the JAVA browser menus to complete a transaction. The data are typically encrypted prior to leaving the handset and being sent to the service provider or bank. Once received, the service provider or bank would decrypt the message and process the consumer's instruction. J2ME applications can be pushed to the mobile phone by a service provider or downloaded by a consumer by accessing the service provider's mobile internet site (Kmal and Abdullah 2009).

Depending on an application's functionality, testing can be done either in a simulator or on a physical device, or both. During the assessment, the application's functionality, any internal logic controls and external connections are ascertained.

#### **2.1.4 Wireless Network Access Security**

Mobile Commerce security is tightly coupled with network security. Hence, without addressing security issues of the underlying network technologies, M-Commerce security

---

may be inadequate. Wireless technology, by its nature, violates fundamental security principles (Grami & Schell, 2004). Importantly, with the growing accessibility of information, computing and service resources and the lack of security as a core element in the initial design of the infrastructure, networks and information systems are becoming increasingly vulnerable to continuous and innovative intrusions and attacks (Jiang, 2012). Interests in this section focus on the unique aspects of M-Commerce network infrastructure-wireless network; thereby narrowing the research scope and omitting any security issues on the wired networks.

M-Commerce can be conducted over *ad hoc* or infrastructure-based wireless networks. The network is *ad hoc* because it does not rely on a pre-existing infrastructure, such as routers in wired networks or access points in managed (infrastructure) wireless networks. According to (Osman & Taylor, 2008) an *ad hoc* network typically refers to any set of networks where all devices have equal status on a network and are free to associate with any other *ad hoc* network device in link range. Background survey (Marufu & Sibanda, 2013a; Pade et al., 2009) revealed that this type of transacting is yet to be realised in MRAs of South Africa. Likewise, to narrow the scope and increase relevancy (as this is an applied research) the current research study focuses on infrastructure-based wireless networks. It is worth pointing out though that the area of *ad hoc* wireless networking is a serious area for future work on ICT initiatives for development. Infrastructure-based wireless networks have base stations (access points). Examples include Wireless Local Area Networks (LANs), paging systems and cellular phone systems.

So which wireless network technologies are in existence to the marginalised communities? To help answer this question a typical marginalised rural community in the Eastern Cape was chosen. This study considers network infrastructures available to users in the Dwesa-Cwebe communities: Siyakhula Living Lab Network (broadband islands) and Telecommunications Networks.

#### **2.1.4.1 Wireless Access Security**

There are wireless threats that are significantly more likely to occur in WLANs than in cellular networks, such as interception (passive eavesdropping), man-in-the-middle attack (active eavesdropping), and denial-of-service (jamming). Interception occurs when the signal is transmitted over a radio path (which is an open, uncontrolled medium) and compatible

---

receivers, equipped with mobile scanners, can listen to the message. The sender and the intended receiver of the message may not even be aware of the intrusion.

Interception is used to gather information on the network under attack, such as who uses the network, what is accessible, and what the coverage area is. A man-in-the-middle attack aims to subvert the confidentiality and integrity of the session. Here, the attacker impersonates a network resource to sniff the traffic of another wireless client by sending unsolicited signals to target stations. The target stations will send all traffic to the attacker instead of the intended destination, and the attacker is now in a position to modify communications. In the default mode, WLANs do not provide any security (Grami & Schell, 2004). To provide a certain level of security, the IEEE-defined Wired Equivalent Privacy (WEP) was designed. However, it is now clear that WEP authentication is completely insecure (Schwidorski-Grosche & Knospe, 2002); an attacker can intercept an authentication exchange without knowing the secret keys. In fact, if many frames are intercepted, the WEP keys can be recovered using statistical analysis. There is another limitation. Due to the fact that all participants must have the same key, public portals (e.g., hotels, airports) provide no security. In response to the deficiencies in WEP standards, the emerging IEEE 802.11i standards have been introduced to improve the WLAN security problems and to turn wireless networking into a trusted medium for all wireless users (Maxim & Pollino, 2002). Denial-of-services is caused when the entire network is jammed. The jamming attack could be against the client's wireless device or against the network's access point. The jamming may be difficult to prevent or stop. Most wireless local area networking technologies use unlicensed frequencies and are subject to interference from a variety of sources. To prevent unintentional jamming, site surveys are recommended, and to stop intentional denial-of-service, jamming equipment must be identified and removed (Maxim & Pollino, 2002).

Various wireless network technologies exist today. World Interoperability Microwave Access (WiMAX) broadband wireless network promises to solve the bandwidth bottleneck, as Wireless Fidelity (Wi-Fi) failed to provide high data rate in the wireless transmission. WiMAX capabilities extend to wider range coverage without line of sight (LOS) and ability to be used as a backhaul technology for several network services. The other main consideration for WiMAX was better security compared to the Wi-Fi, which failed due to its compromised security mechanism and protocols, for example Wired Equivalent Privacy (WEP). As much as Wi-Fi faced many security challenges, it can be used as an access technology since there are no end-user devices which can select and utilize the WiMAX

---

signal during communication (Jha & Dalal, 2011a). The existence of these wireless technologies is important as they complement each other in service provision. The Alvarion BreezeMAX equipment in the SLL is 802.16d and 802.16e compliant. IEEE 802.16 standards integrate seamlessly into most wired networks, much like 802.11 (WiFi) standards.

VSAT, WIMAX and Wi-Fi featured relevant factors for convergence and therefore were considered to provide the rural Internet connectivity and telecommunication services to the community. Via the broadband islands deployed in the SLL, communities have access to various services such as M-Commerce payments, email, VoIP, the Internet and the TeleWeaver multi-service platform (providing for E-Commerce). Without the deployment of a local access network the communities would not be able to share these vital resources and would instead each require access to their own installations of the resources, which becomes expensive. Security of the wireless access network is deemed a necessity.

#### **2.1.4.2 WiMAX security**

WiMAX is open to more security threats than other wireless systems (Jha & Dalal, 2011a). Hence for a broadband wireless standard such as WiMax to be realised for its complete benefits, security is important and must be addressed (Ahuja & Collier, 2010; Deepti et al., 2012). To compete with existing broadband cable or DSL services, the WiMax network must offer comparable security. The issue of security is an important concern for network operators and the network users as shown in Table 2.1 (Deepti et al., 2012). The network operator needs to know that the users and the devices connected to their network can be trusted (to prevent malicious attacks, user spoofing), accessing services that they are authorized to access and usually that the network users pay for the services they have used. The network users want to ensure that their privacy is protected, that the integrity of the data they send and receive is not compromised, that they can access the services they have subscribed to and that they are not over-charged for those services. Security Concerns of Network User and Operator are shown in Table 2.1

Table 2.1: Security Concerns of Network User and Operator (Jha & Dalal, 2011a)

Stakeholder	Security Concern	Comment
Network user	Privacy	Protect from eavesdropping
	Data integrity	Protect user data from being tampered with in transit
	Access to services	User has the correct credentials
	Correct accounting	Accuracy and efficiency of accounting
Network Operator	User authentication	Is the user who he says he is?
	Device authentication	Is the device the correct device?
	Authorization	Is the user authorized to receive a particular Service?
	Access control	Only authorized users have access to services

WiMAX security has two goals: one is to provide privacy across the wireless network and the other is to provide access control to the network. Privacy is accomplished by encrypting connections between the subscriber station and the base station. Broadband wireless access security becomes more complicated when wireless devices are added to the network (Jha et al., 2012). Threats are ranked according to the level of risk they present. Comment also presented the Threats and solutions at different layers of WiMAX are given in Table 2.2

Table 2.2: Security at Various Layers of WiMAX (Jha & Dalal, 2011b)

Layers	Threats	Solutions
Application	Worms, Trojans, Viruses	Antivirus, IDP, FW
Transport	Transport layer-based attacks	TLS algorithm
Network	IP-related security , Misbehaving node	IP security algorithms
MAC	Eavesdropping, Man in the middle attack, Denial of service	AES, DES algorithms
Physical	Jamming and Scrambling	Using spread spectrum, Jamming-resistant network

Thus far, the different levels of threat and vulnerability have been mapped out, pointing out the vulnerabilities and threats present within the M-Commerce landscape. The discussion

---

presented some of the key areas to consider if one plans to address security issues plaguing M-Commerce Systems in use by marginalised communities. It is therefore appropriate at this stage to ask of what value the previous discussion in this chapter is to this research, and how the research positions itself within the literature. The next section discusses work that has been happening in order to address the security issues plaguing M-Commerce systems as ICT4D initiatives. The strengths and shortfalls of these frameworks are discussed, supporting the development of the framework proposed in our research work. Components that maybe leveraged by the proposed framework are also noted.

## **2.2 Related Work**

In a recent study, Charles et al. (2000) determined those aspects that, if fulfilled, would ensure that M-Commerce is lucrative and profitable. The results of their survey show that M-Commerce can be seen as a means of allowing organisations to be introduced to new markets and new channels within that industry. Most respondents in their survey found security to be critical to the success of M-Commerce to which the researchers rightly concluded that further research should be conducted in this area, in order to determine methods of making mobile transactions more secure. Further work from Tsalgaidou and Veijalainen, (2000), Gururajan (2006), Bailes et al. (2006), Meng and Ye, (2008), Yeh et al. (2009), Dai and Tang (2010) and Hui (2011), agree that security is a worthwhile endeavour to pursue. It is from such works and understanding that our study gets its foundation.

Some work is evident in ensuring that users of technologies in marginalized communities are protected from various risks and threats against privacy and security issues when using ICTs. A large portion of the South African rural communities have only intermittent access to computers (now recently mobile phones) and are not familiar, nor entirely comfortable, with the use of internet communication or electronic devices (Grobler et al., 2011). The same research by Grobler *et al*, confirms that this lack of awareness, combined with the inherent dangers posed by the internet, expose especially local marginalized communities to cyber threats. Although their work can be viewed as a base to our research it mostly focused on promoting cyber security awareness towards the newly released broadband capability and knowledge transfer within rural communities by means of a voluntary community-based training program. The cyber security awareness program modules are divided into four main themes: physical security, malware and malware countermeasures, safe surfing and social

---

aspects of cyber security to which mobile device use and safe/secure mobile transacting was barely addressed. Our work seeks not only to push forward a training program to complement the work by Grobler *et al.*, as stated, but also envisages delivering a security framework that guides marginalized communities towards a safer and secure M-Commerce transacting environment.

When it comes to suggesting security solutions, some work is evident, where different authors have come up with a security framework, model and/or solutions to improve privacy and security of M-Commerce and related systems. This section will take into account such works, and proceed to point out some aspects that can be integrated with the suggested framework. Such work includes the work of the following authors:

Howie et al. (2001) presented a framework model for guiding the systematic investigation of mobile security. Based on the introduction of some background viewpoints of security targets from a novel perspective, the framework was described as a hierarchical model in which mobile security research is partitioned into three different layers, including Property Theory, Limited Targets, and Classified Applications. Their work provides a platform to position the present work as an M-Commerce security research across all the layers: Property Theory, Limited Targets and Classified Applications.

Van de Merwe (2003) focused on the risk involved in M-Commerce for the banking industry. The dissertation provides a detailed overview of basic services that any M-Commerce application should provide to the banking industry. It was from these principles that the author presented the foundation for securing any financial transaction over intrusted networks. In the work an evaluation of the security offered by GSM and the assessment of potential attacks was carried out. This was with a view to understanding the risks associated with M-Commerce applications over GSM networks. Van der Merwe's work is different from the suggested work in this research in a number of aspects. The main focus was on the GSM network, and the only enabling technologies discussed are the SIM Application Toolkit and WAP, which is different from our work which seeks to address security issues of the network technologies currently available in Dwesa area (study area) and rural areas alike. Under this tier of the framework three types of wireless access networks are considered: VSAT, WiMAX and mobile networks. Further, since this is applied research, it focuses beyond just analysing and suggesting solutions, but envisages some deliverables for the users of M-Commerce, IT specialists even service providers. Some variables in Van der Merwe's work, though important at the time, are now out-dated. At the time of the work in question,

---

network operators in South Africa where yet to establish a commercially sustainable GPRS network infrastructure. A lot of change has taken place since then. Likewise our work aims to include analysis of threats and vulnerabilities in these new technologies in providing a secure and safe M-Commerce environment. Importantly van der Merwe's work intentionally sidelines rural area users, giving as reasons that they were not easily accessible to the traditional banking fraternity despite the mobile transacting potential we present in our research.

Wei et al. (2006a) presented a five-layer 'onion ring' framework for analysing M-Commerce security requirements and for improving system security performance. Two quantifiable approaches, based on weighted scores applied to either a spider diagram or a decision solution matrix, are used to demonstrate how the security level can actually be objectively measured and evaluated in addition to the technical discussions on the framework's architecture. It is from this framework that our work adopts a layered approach in dealing with threats that affect the marginalised communities in transacting on M-Commerce platforms. The 'onion ring' framework introduced in this paper classifies M-Commerce security into five levels, and the key to understanding the success of the framework was inherent in the notion that protection needs to be in place in several layers. Each succeeding layer should also act as a kind of enclosure for the next layer, thereby increasing effectiveness, a feature emphasised by the Defence in Depth approach. Though the structure for the ICTMS framework in the research seeks to adopt a multi-layered approach the emphasis will be on the main levels threat from the time a user initiates a transaction up to the access network.

Kark et al. (2007) demonstrated that a comprehensive security framework boils down to three familiar basic components: people, technology, and process. When correctly assembled, the people, technology, and process elements of your information security program work together to secure the environment and remain consistent with business objectives. A comprehensive framework according to them must be based on these three components and must also ensure policy definition, enforcement, measurement, monitoring, and reporting for each of the components. In their document they established a high-level framework that can be used either as a starting point for a new security program or as a blueprint for assessing your current security program. This research provides input to the M-Commerce framework, on how best to integrate the important aspect of the three domains of security that have to be addressed in an information security plan or framework.



---

Thomas (2007) proposed a framework that would aid IT administrators in healthcare to ensure that privacy and security of health information is extended to mobile devices. The research uses a comparison between best practices in ISO 17799:2005 and regulatory requirements stipulated in HIPAA to provide a baseline of the mobile computing security model. The comparison ensured that the model meets both the healthcare specific requirement and the international information security standard. This approach seems logical to incorporate in a framework of such nature as it is built on top of well accredited pillars of information security. Likewise, we envisage a similar approach in our research by comparing some international information standards and M-Commerce-specific regulatory requirements. However, although this approach of creating a security framework has its positives, it is worthwhile noting that though the internationally accepted standards and frameworks help to fill the gap in the knowledge base, they have traditionally overlooked the enterprise as a system (Ena et al, 2010), considering things such as culture and emergence. Basically the framework was developed using a security management approach, which means it takes an abstract view of the problem our work is trying to address. These shortfalls will be addressed in the M-Commerce framework in our study. Further, our framework goes beyond the higher level of assessing risk into an in-depth layer-by-layer modular approach.

Patil (2008) looked at implementation of proper policies, procedures, and standards in the organisation in compliance with the laws and regulations. In this work Patil chose one comprehensive information security framework from different frameworks in the literature. The Information security framework of the manufacturing organisation was also studied and mapped to the framework chosen from the literature survey. Mapping allowed identification of some few flaws in the organisation's information security framework which led to some recommendations. Despite a difference in the area of research (manufacturing to M-Commerce) Patil's project only addressed non-technical issues, a deviation from the M-Commerce framework in this research, as it seeks to address both areas, technical and non-technical security issues. As a result the scope of Patil's work is limited to 1) IT Governance and Compliance, 2) Policies and Procedures, 3) Impact of Laws and Regulations on the Organisation, and 4) Risk Analysis and Assessment. However a valuable output gained from Patil's research, as in other works under review in this section, is that a framework of a similar nature should consider higher levels of security (IT Governance and Compliance). Likewise different frameworks, policies, laws and regulations shall form a backbone in the M-Commerce framework. Another take-away point is support of the idea that security should

---

not only focus on technology issues but other elements of the organisation: people, process, business strategies, etc.

Kmal & Abdullah (2009) presented suggestions for improving M-Commerce security and limiting the M-Commerce drawbacks. These suggestions related to End-to-End Transport Layer Security by Java 2 micro edition/ mobile information device profile (J2ME/MIDP). Using J2ME/MIDP to mobile communication overcomes the security challenges faced with WAP technology, but securing the XML messages transferred between the mobile phone and the server would give a high level of integrity for the data itself, but not for the physical connection. This result of Kmal and Abdullah's work is valuable to our work as it relates to a section of our research. WAP technology security is discussed as part of level 3 on the threat mitigation layer. This layer looks at security issues on the channels through which M-Commerce transactions can be conducted: USSD, SMS, WAP, and Mobile Applications. Hence our work has a broader focus than that of Kmal and Abdullah.

While it can be agreed that the many noteworthy applications, models, and analyses identified in the research efforts indicated above have indeed been useful, studies that can address M-Commerce security technical components, as well as application processes and people together, are still lacking. In addition, there is a need for proven comprehensive approaches that M-Commerce experts can actually use to assess vulnerabilities in M-Commerce systems incorporating users, especially those in marginalised communities. This study is a pioneer effort aimed at addressing both those areas of need in the M-Commerce security literature.

It can thus far be assumed that there is nothing like a complete security solution for M-Commerce systems, but various patches at different levels. It can also be assumed that lack of adequate security on these M-Commerce systems is the reason behind the lack of full adoption of the on-going technologies being introduced. Further, no work known to us has suggested a framework that can be used to alleviate the various security issues identified in this research to inhibit use of M-Commerce ICT4D initiatives.

Although some frameworks help to fill the gap in the knowledge base, they traditionally have not looked at the enterprise as a system, considering things such as culture and emergence. The different frameworks generalise and look at security from a broader, more abstract level. Minor consideration of grass-root end-user security is considered: an important consideration in the proposed security framework in this research. Further, while there are existing models

---

for security from academia as well, they have not taken a holistic approach or look at security systemically. The ICTMS framework proposed in this research presents a holistic and modular threat mitigation approach to managing M-Commerce security that can be applied and is relevant to even marginalised communities, and fills the gap that other standards and frameworks have not.

### **2.3 Chapter Summary**

This chapter helps to map out the scope and direction of the research study. A background discussion of the current research work is laid out in the initial section. This sets up an understanding of where the work lies within the body of knowledge through a dissection of related works. The present work lies within M-Commerce and ICT4D bodies of knowledge. Furthermore, a dissection of the threats/vulnerabilities plaguing M-Commerce into 4 levels: Human aspect, Mobile device, Wireless network access channels, M-Commerce enabling channel was done. This is followed by a detailed discussion of each of these threat/vulnerability levels which form the fulcrum of the proposed framework in this research. Related work was then discussed, indicating some interesting components that can be integrated into the proposed framework. This chapter lays the foundation for the research design that follows in the next chapter.

---

## Chapter 3. Research Design & Methodology

The purpose of the study is to compile a security framework that can be used to address security issues faced by M-Commerce systems in ICT4D. This chapter provides an outline of the research design, methodology and methods followed in reaching the objectives of the study. The chapter is structured as follows: the first section discusses the research design, which includes classification of the research design, execution order of the studies and the validation process to be adopted. The second section details the research methods to be employed in the study. The third section contains a detailed presentation of the research process adopted in our research. Finally, we present a summary that concludes the chapter.

### 3.1 Research Design

A research design is defined as a plan or blueprint of how one intends to conduct research (Mouton, 2001). A research design focuses on the end product of the research process, that is, the type of study being planned and the type of results aimed at. Its point of departure is the research problem, and hence it focuses on the type of evidence required to address the problem adequately.

According to Mouton (2001), research designs are tailored to address different kinds of research questions. Therefore, when attempts are made to classify different kinds of research studies to different design types, they are classified by the kind of research questions they are able to answer. Research designs can be mapped out to the types of research questions (research problem) using four dimensions: 1) empirical versus non-empirical dimension, 2) using primary versus secondary data, 3) the nature of the data (numerical versus textual data) and 4) the degree of control (structured (laboratory) conditions versus natural field settings).

The first dimension, which is relevant to our study, is that of empirical versus non-empirical studies. Empirical studies involve observing and measuring reality, thereby confirming knowledge through direct experience. Non-empirical (theoretical) studies involve developing and exploring theories that account for given data.

The second dimension is that of the nature of data used in the study. Data used in empirical studies can be numeric, textual or a combination of both. When the basic data used in an empirical study consist of words, the research is classified as qualitative; whereas if the data

---

used are numeric, the research is classified as quantitative. A research design may also combine quantitative and qualitative methods to achieve more rounded and reliable results than either method can give in isolation. The following section comments on the classification of our study based on the two dimensions noted above as they define parameters relevant to our study

### **3.1.1 Classification of Research Design**

This section discusses two ways in which our research design was classified.

#### *Classification 1:*

Kothari and Garg (2014) discuss different basic types of research, where the type of research effectively determines the research design and the research process a particular study would follow. These research types are classified into: 1) Descriptive versus Analytical, 2) Applied versus Fundamental, 3) Quantitative versus Qualitative, 4) Conceptual versus Empirical 5) other types (essentially variations of the previously stated). By mapping this study to the first two classes/dimensions, this research can be described as a descriptive-applied research. Descriptive research includes surveys and fact-finding enquiries of various forms (Kothari & Garg, 2014). The major purpose of descriptive research is description of the state of affairs (security issues in M-Commerce systems in this case) as it exists at present. Furthermore, research can either be applied (or action) research or fundamental (basic or pure) research. Applied research is aimed at finding a solution for an immediate problem facing a society, industrial or business organisation, while fundamental research is mainly concerned with generalisations and with the formulation of a theory (Kothari & Garg, 2014). Using the second dimension, our research can be classified as applied research, as it is intended to solve specific, practical questions; understanding of M-Commerce security issues and framework development.

#### *Classification 2:*

By considering how a research problem is formulated as research questions (Mouton, 2001), a distinction should be made between empirical and non-empirical questions. From the research questions identified in Section 1.3, we categorise those questions that address real-life problems (world 1) as empirical questions and questions of theoretical linkage (world 2)

---

or conceptual models as non-empirical questions. According to Mouton (2001), world 1 context involves the world of everyday life and lay knowledge (non-scientific knowledge). Stated differently, world 1 involves the ordinary social and physical reality that we exist in while world 2 - the world of science and scientific research, involves the search for ‘truthful knowledge’, for example, to generate valid and reliable descriptions, models and theories of the world (Mouton, 2001).

The research questions classified as non-empirical research questions in this study include:

- 1. What security aspects are related to M-Commerce as an ICT4D initiative?*
- 2. What are the requirements of an M-Commerce security framework?*
- 3. What existing security structures are related to the M-Commerce security framework?*
- 4. What are the components of a security framework for the M-Commerce security framework?*

Our study therefore employed different non-empirical methods in order to answer these questions. A literature review, which included document analysis, was used to answer sub-questions one, two and three. A model-building approach was suggested to answer sub-question four. In addition, this study employs a case study as a proof-of-concept. A case study is a qualitative empirical study to further strengthen the research applicability (and validation). Since the research methods directly responding to the research questions (Literature review and Model building) make use of textual data, we classified this study as a qualitative study. Table 3.1 below summarises the classification of this study in terms of the dimensions discussed above.

Table 3.1: Classification of the Research Design

Research Method	Dimension 1	Dimension 2
Literature review	Non-empirical	Qualitative
Model building	Non-empirical	Qualitative
Case study	Empirical	Mixed Method

---

### 3.1.2 Qualitative Studies

Qualitative studies are research approaches in which the basic data used in the research process consist of words or languages (Mouton, 2001). A qualitative study is useful where an in-depth understanding of a particular situation is required. Since the qualitative research does not involve numerical data, it is not amenable to direct measurement, and therefore the researcher must convince others that the research is reliable.

In qualitative research the reliability and validity of the research are assessed in terms of auditability, credibility and comprehensiveness. Auditability involves the repeatability of the research process. Credibility looks at whether the research results are internally valid, for example: Is the explanation given for the results the only valid explanation? The comprehensiveness aspect ensures an in-depth description of subjects and their relationship to their context.

The qualitative approach was considered for this research for the following reasons:

- 1) In order to generate new theories it is necessary to use qualitative methods, as quantitative methods can only be used to make measurements about existing theories and not to provide tools for discovering new theories.
- 2) In order to be able to concentrate on details in a specific context rather than to focus on generalisation of broad range of contexts, it is necessary to use qualitative methods.
- 3) Qualitative methods help in reaching a deep, detailed understanding of situations.

Another concept related to qualitative studies is that of the researcher's philosophy. (Mouton, 2001) includes positivism, interpretivism and critical theory as the epistemological research approaches. In positivism, a positivist believes that there is such a thing as absolute truth and therefore an answer exists that is the truth. In this philosophy, the researcher's role is to find the true answer and describe it. In interpretivism, an interpretivist feels that 'reality is too complex to control every variable'. The researcher's role, therefore, is to find a coherent way of understanding a situation within a particular context. In critical theory, a critical researcher assumes that social reality is built by people historically. The approach followed in this research is interpretivist in nature. We set out to understand and address security issues within the M-Commerce and ICT4D domains of research. Since M-Commerce security is a huge area for consideration, reviewing the application of the proposed security framework will aid in an understanding of this area in a simplified manner.

---

### **3.1.3 Execution of Tasks**

The research began with a literature review directed at tackling the first three research sub-questions (Section 1.3). The literature review is presented in Chapter 2 of this thesis. This is followed by Chapter 3, aimed to answer demands of sub-question 2. This was achieved through an analysis of literature. A model-building study follows to answer the research sub-question 4. The model-building study depends on the findings from the literature review. The model-building study result is presented in Chapter 5 as the first segment of the framework chapter. The framework is validated with respect to its construct and implementation (Section 5.6). A case study scenario which follows strengthens the applicability and reliability of the compiled framework. The case study depends on the results of both the literature review and the model-building study. The use of the case study will be presented in Section 5.6, showing application of the proposed framework. This order of execution of our study was inspired by Anand, (2007), Mbaya et al., (2007) and Patil, (2008).

## **3.2 Research methods**

Research methods may be understood as all those methods or techniques that are used for conducting research (Kothari & Garg, 2014). The following sections present a detailed discussion of the selected methods:

### **3.2.1 Literature Review**

Literature review is defined by Mouton (2001) as a study that provides an overview of scholarship in a certain field through an analysis of trends and debates. A literature review creates a coherent picture of how different concepts fit together. It helps to identify trends in research activity and to define areas of theoretical and empirical weakness (Mouton, 2001) A literature review is a non-empirical study, in which the unit of analysis is based on data from an existing academic body of knowledge (Mouton, 2001; Olivier, 2004). There is exclusive reliance of literature review on secondary literature, thus prompting the use of inductive reasoning from a sample of text read to derive a proper understanding of a specific domain of scholarship.

The purpose of conducting a literature review in this study is to provide a sound understanding of the issues and debates in the area of M-Commerce security within a rural



---

context. It also provides current thinking and definitions of the M-Commerce terminologies, as well as studying previous works on security frameworks. A survey of literature on related research on framework development was used to obtain the validation techniques that could best be used.

The literature review in this study involves document analysis in which information is extracted from existing literature. The document analysis provides a means of answering the first three research sub-questions, and therefore reaches the first three objectives of the study. Stated differently, the document analysis helps the study to describe security aspects related to M-Commerce in ICT4D contexts, to establish the requirements for the proposed security framework and to determine components from existing security frameworks that can be used for the proposed framework. Furthermore, the literature review aided in planning of the case study.

The selection of sources for a literature review is based on theoretical factors such as the objectives of the study, research questions, time-frames, etc. The findings from the literature review are presented in Chapters 2 and 4, and the extraction of information from the literature in these respective chapters is presented in Chapter 5.

### **3.2.2 Model-building Study**

Model-building studies aim at developing new models and theories to explain particular phenomena (Mouton, 2001). Model-building studies are used to answer questions of theoretical linkages and coherence between conceptual models. A model can be defined as a blueprint of a system or process that represents particular phenomena in a clear and concise manner (Mouton, 2001). According to Olivier (2004), ‘a model captures the essential aspects of a system or process, while it ignores the nonessential aspects’. A model may describe the system in terms of its components, roles and interfaces in the system. An essential model depicts only the essence of the system, neglecting how the system will be physically implemented (Mbaya et al., 2007). By using models, one can bring conceptual coherence to a particular phenomenon and simplify the understanding of our world (Mouton, 2001). Models provide simplicity, comprehensiveness, generality, exactness, and clarity in problem-solving researches (Olivier, 2004).

Model-building studies are non-empirical studies that utilise secondary data from an existing academic body of knowledge. Olivier (2004) identified three objectives of model-building

---

studies: clarification, differentiation and generalisation. Tentative models are used to clarify whether the problem does actually exist. Differentiated models make explicit assumptions to address specific forms of the problem in detail. General models cater for most of the different assumptions made in previous models.

Model-building studies are mainly done through either inductive or deductive reasoning. Deductive reasoning is more formal in that a set of axioms is formulated and used to deduce additional theoretical propositions. Inductive reasoning is commonly used in statistical model-building, where a model is built to explain particular empirical data. For non-empirical qualitative research, analogical reasoning, which is a variation of inductive reasoning, is used. In analogical reasoning a model of a phenomenon is constructed based on its similarities to another phenomenon (Mouton, 2001).

The purpose of using model-building in this research is to develop an M-Commerce security framework. The model-building study helps the researcher to answer the fourth research sub-question: What are the components of a security framework for the M-Commerce security framework? In doing so, the last two objectives of the research will be achieved, namely, establishing the components and compiling of the M-Commerce security framework.

Assumptions made in specifying a model are the main source of error in model-building studies. Models are limited in that they can make claims that are conceptually incoherent, inconsistent and confusing (Mouton, 2001).

The approach that will be followed in compiling the proposed M-Commerce security framework will be based on the construction and functionality of related frameworks. The construction of the proposed security framework will therefore involve identifying essential components of a security framework, adapting these essential components to the framework's requirements and lastly, integrating the adapted components to form the proposed security framework

The findings of the model-building study will be presented in Chapter 5. In the next section a discussion of framework case study application is presented as a proof-of-concept.

---

### 3.2.3 Case Study Scenario

The study aims to use a case study scenario to provide an in-depth mapping of the framework to a practical situation. The case study allowed the proposed framework components to be studied in more detail through implementation within a selected setup.

Case studies are empirical in nature and may use qualitative or quantitative information to provide an in-depth description of a small number of cases (Mouton, 2001). The study sets out precisely what is to be studied and how the study is to be performed. It spells out what is expected to be learned from the case scenario. It also lists the aspects of each case that should be observed. The strengths of case studies include high construct validity and valuable in-depth insights. Two techniques are usually used for case selection, namely literal replication and theoretical replication. In literal replication, cases are selected in such a way that they will test the theory in extreme cases. In theoretical replication, cases are selected in such a way that the theory applies in some cases, and does not apply to other cases (Olivier, 2004).

The weakness of using a case study is that it lacks the generalisation of results and non-standardisation of measurements (Mouton, 2001). To obtain more general results, multiple-case scenarios may be used. The potential bias of the researcher, especially in case selection, may lead to results of little value (Mouton, 2001). The advantage of a case study scenario is that it may combine both qualitative and quantitative data (Olivier, 2004).

The purpose of using case study in this research is to apply different components of the proposed security framework to a real-life setup within a chosen setup as a proof-of-concept. The intention is to ‘prove’ the concept. In this context the term ‘prove’ refers to demonstrating that the proposed security framework works. The proof-of-concept scenario is also used to strengthen the validity of the framework components. An ideal rural application scenario was selected from the literature and through the researcher’s personal consultations. The design and implementation of the case study will be presented in Section 5.6 and related appendix articles of this document.

#### 3.2.3.1 *Use of Cases as a Validation Technique*

Related works in academia that sought to develop a security framework were analysed with the aim of establishing an ideal validation and evaluation technique that could be employed in our study. A considerable number of authors validated their work by supporting the construct of the framework through referencing peer-reviewed work and models (Howie et al., 2001;

---

Thomas, 2007; Patil, 2008; Sreenivasan & Mara, 2010). Wei et al. (2006a) validated their framework through its construct by peer-reviewed works and evaluated the same framework through two proven assessment methods based on weighted scores applied: spider diagram (spider-weighted method) or decision solution matrix (relative-weighted method). Another cluster of researchers validated and evaluated the framework through implementation, i.e. made use of case study (Anand, 2007), application scenarios (Mbaya et al., 2007), schemes (Clarke, 2008), event modelling and behavioural analysis (Saraydaryan et al., 2009), and experiments (Jiang, 2012). In our research, the framework is validated and evaluated using two of the above-mentioned techniques: through construction and within a case study (Section 5.6).

### **3.3 Research Methodology**

This section presents the research methodology (research process) to be followed in the execution of the research project. A research methodology focuses on the research process and the kind of tools and procedures to be used in the research project (Mouton, 2001). Its point of departure is specific tasks at hand such as case selection, data documentation, etc.; hence the focus on individual steps of the research process.

The approach used in this research is adapted from the approach described by Mouton (2001) to fit the qualitative study followed. The approach is executed in an almost similar fashion to the work by Mbaya et al. (2007). The approach includes: 1) identification and selection of data sources, 2) collection of data, 3) data documentation, 4) data capturing and editing, and 5) data analysis and interpretation. Each of these stages of the research process is discussed in the following subsections.

#### **3.3.1 Identification and selection of data sources**

The research makes use of documentary sources, which involves existing textual documents available in electronic and printed media. Empirical sources of data were also obtained during the case study. This selection of the case study scenario was justified as having the best-suited setup to elicit data within a rural environment, as explained in Section 5.6.2

---

### **3.3.2 Data collection**

This research project makes use of textual analysis as a means of data collection. Textual analysis involves both content analysis and textual interpretations. Based on the research departure points, namely the Mobile Commerce in ICT4D and security frameworks, the contents of the referenced publications were analysed to find their applicability to the study. Furthermore, textual interpretation of a relevant publication led to the identification of additional publications relevant to the study. Preliminary data were also collected in conducting the case study. A mixed-method approach was employed to elicit different pieces of information surrounding the framework implementation within a rural setup. A broad array of methods/data collection tools (questionnaires, interviews, focus groups, observations) was employed

### **3.3.3 Data documentation**

Data documentation involves the presentation of data in a clear, complete and unbiased manner to enable conclusions to be drawn. In a qualitative study, textual data can be summarised in tables, figures, and matrices. For instance, the theoretical framework presented in Chapter 2 includes Figure 2.1 with a summary of M-Commerce flow when transacting, and the envisaged security issues. In a model-building study, textual data are compiled into a diagram that visualizes the proposed model in terms of its components and interactions between different components.

### **3.3.4 Data capturing and editing**

Textual data are rich in meaning and difficult to capture in a short and structured manner (Mouton 2001). In this research relevant publications were summarised to capture the information provided by the references. Similar information from different publications was categorised and grouped to simplify and obtain a coherent understanding of a particular domain. The theoretical framework was then developed and presented in Chapter 2 of this document. Within the case study data collected by each tool were processed and cleaned using recommended techniques by experts in the area of qualitative research.

---

### **3.3.5 Data analysis and interpretation (synthesis)**

Data analysis is defined by Mouton (2001) as breaking up the data into manageable themes, patterns, trends, and relationships. The aim of the data analysis stage is to turn the data into the evidence for the research findings. Hence, in order to understand the different constitutive elements of the data, an inspection is carried out on the relationships between concepts. For the purpose of this dissertation, data analysis will involve theoretical findings such as the presentation of the M-Commerce security framework, coupled with descriptive findings such as identification of interesting and significant patterns in existing security frameworks.

According to Mouton (2001), data interpretation involves the organisation of data into larger coherent wholes. For the purpose of this study, the interpretation of data involves relating the research results to the existing theoretical framework presented in Chapter 2. The aim of the data interpretation stage is to show whether the existing theoretical framework is supported or falsified by the research findings. In this dissertation, interpretation of data will include application of the proposed security framework to a rural case study scenario. The research findings and the synthesis will be presented in Chapters 4 and 5.

### **3.4 Chapter Summary**

This chapter presented the systematic approach; research design and methodology to be followed in the execution of the research process in developing the ICTMS framework. The research follows a qualitative approach based on secondary, textual data. The approach uses both non-empirical and empirical methods to reach the research objectives. Two non-empirical methods, namely literature review and model-building study, have been identified for answering the non-empirical research questions. One empirical method, namely case study, will be used to strengthen the validity and reliability of the research results. The literature review is presented in Chapters 2 and 4, while the model-building and the case study (as validation of the framework) is presented in Chapter 5. Table 3.2 below summarises the relationship between the research questions, research methods and the dissertation chapters.

---

Table 3.2: Organisation of studies on the dissertation

Research question	Research Method	Related Chapter
What security aspects are related to M-Commerce as an ICT4D initiative?	Literature Review (document analysis)	Chapter 2
What are the requirements of an M-Commerce security framework?	Literature Review (document analysis)	Chapter 2
What existing security structures are related to the M-Commerce security?	Literature Review (document analysis)	Chapter 4
What are the components of a security framework for the M-Commerce security framework?	Model-building study	Chapter 5
	Case study	Chapter 5

---

## **Chapter 4. Existing M-Commerce security structures**

This chapter discusses the related M-Commerce security structures that exist in order to ascertain the supporting structures or related frameworks that the proposed framework could leverage to address security issues on M-Commerce systems as ICT4D initiatives. Essentially, work in this section forms the framework input components in the ICTMS framework presented later in Chapter 5. An in-depth literature survey allowed for the discovery of a vast array of frameworks that align well with the development of the ICTMS framework. It should be noted that, while the proposed ICTMS framework complements some governance frameworks and models, its basic structure was also built on some of these frameworks' security principles. Discovery of these frameworks allowed for the realization and development of an integration platform of the proposed ICTMS framework to already existing frameworks. Most of the frameworks are focused on governance of information systems security. On the same wavelength, we noted a vast array of Laws, Policies and Acts the South African government put in place (and continues to put in place) which have a positive impact on improving the M-Commerce security environment directly and indirectly. Thus, the following subsections will be discussed in depth: 1) the Bills and Laws that have been put in place by the South African government towards M-Commerce security and valuable governance frameworks and models, 2) the current M-Commerce regulatory requirements and acceptable Information Security standards 3) the related IS and security theories that provided the fundamental foundation on which the ICTMS framework was developed.

### **4.1 Regulations Linked to Information Security in South Africa**

The South African government has had a number of disparate pieces of legislation that govern the ICT sector (DOCRSA), many of which have undergone subsequent amendments. These include: The Broadcasting Act 1999; the Independent Communications Authority of South Africa Act 2000 (ICASA Act); and the Interception and Monitoring Act 2002. These legislative reforms, amongst others, culminated in the enactment of the Electronic Communications and Transactions Act 2002 (ECTA), which provides a legal framework for electronic transactions, deals with cryptography, cyber-crime and the protection of privacy.



---

These legislative reforms resulted in the adoption of the Electronic Communications Act of 2006, which was to regulate the convergence of technologies in the ICT sector (Jobodwana, 2009). The Electronic Communications Act (ECA) seeks to promote convergence in the broadcasting, signal distribution and telecommunications sectors, and to provide the legal framework for convergence of these sectors. The act set the stage to make new provisions for the regulation of electronic communications services, electronic communications network services and broadcasting services. The passing of the Act enabled the ICT sector to reflect the integration of telecommunications with information technology, broadcasting and signal distribution. The Act has since been amended in 2012 so as to align it with broad-based black economic empowerment; to incorporate the authority's recommendation on ownership and control of commercial broadcasting services; to introduce a Spectrum Management Agency and clarify the responsibilities of the Agency and the Authority in respect of frequency spectrum management; to refine licensing issues; to improve the competition provisions; to improve turn-around times for consultative processes; to improve the governance provisions of the Universal Service and Access Agency of South Africa; to remove regulatory bottlenecks; and to provide for matters connected therewith.

In addition, government also enacted the ICASA Amendment Act which further incorporates postal regulation into the mandate of the Independent Communications Authority of South Africa (ICASA) (Jobodwana, 2009). All these pieces of legislation provide evidence that the government has been active in creating conditions to protect consumers transacting electronically in this digital age. However, is this high level type of activity from the government effective enough to ensure security of M-Commerce user's information and data, down to the grass roots level? In this research it is argued that reliance on this high level security legislation only is inadequate. The corporate sector, the government and academia should all participate in ensuring security of ICT4D initiatives (like M-Commerce, M-Health, etc.) This research contributes in this space by providing grass-root innovative ideas which can blend in well with existing information security structures to ensure a secure M-Commerce environment for marginalised users.

The Department of Public Service and Administration recently released a circular that now compels all government departments and entities to adopt an ICT governance framework. In this context, a Corporate Governance of ICT (CGICT) Policy Framework has been issued by the Department, which maps out how governance of ICT within government entities is to be applied, structured and implemented (<http://goo.gl/Qdnma>). The development of the CGICT

---

policy framework was primarily a result of the assessments conducted by the Auditor General over the last couple of years. In 2010/11, the Auditor General concluded that only 21% of departments had implemented adequate governance controls, and that 79% of institutions did not have an ICT governance policy framework (<http://goo.gl/Qdnma>). The CGICT policy framework depicts the COBIT Governance Framework as the core reference for the governance of ICT as COBIT is the internationally recognised business framework for the governance and management of enterprise IT. This initiative can be seen as a huge step towards ICT security, but is it enough for one to conclude that marginalised users using the various ICT tools (like M-Commerce, M-Health, E-Government services) are guaranteed safety of their personal data and funds? The emphasis in this research is on the need for addressing security at all levels, especially the grass-root levels, where human activity and most security issues are prominent.

## **4.2 Information Technology Governance Frameworks and Models**

The following subsections present the IT governance frameworks and models facilitating the development of the ICTMS framework proposed in this study.

### **4.2.1 COBIT**

When approaching IT Governance, there are a number of frameworks, maintained by various governing bodies. The focus of this section will be on the COBIT framework (COBIT 5 being the latest) as this framework concerns the governance and management of enterprise information.

COBIT is an IT governance framework and supporting toolset that allows managers to bridge the gap between control requirements, technical issues and business risks. COBIT enables clear policy development and good practice for IT control throughout organizations. COBIT emphasizes regulatory compliance, helps organizations to increase the value attained from IT, enables alignment and simplifies implementation of the COBIT framework (<http://goo.gl/j8GtT>).

COBIT has had the following major releases: In 1996, the first edition of COBIT was released. In 1998, the second edition added “Management Guidelines”. In 2000 the third edition was released. In 2003, an online version became available. In December 2001, the

---

fourth edition was initially released and in May 2007, the 4.1 revision was released. COBIT 5 was released in April 2012; it addresses governance and management of enterprise IT. COBIT 5 combines COBIT 4.1, Val IT 2.0 and Risk IT as well as concepts from the Business Model for Information for a detailed framework for the effective governance and management of IT enabled business (ICASA, 2011). While COBIT 4.1 ensures that IT is working as effectively as possible to maximize the benefits of technology investment, Val IT helps enterprises make better decisions about where to invest, ensuring that the investment is consistent with the business strategy. Similarly, COBIT 4.1 provides a set of controls to mitigate IT risk in IT processes whilst Risk IT provides a framework for enterprises to identify, govern and manage IT-related risks.

COBIT 5 also aligns itself at a high level with existing frameworks such as ITIL and TOGAF, PMBOK, PRINCE 2 and ISO, which makes it an umbrella for governance and management of IT (ICASA, 2011). This integration supports a holistic view of management and governance in the enterprise. Likewise the ICTMS framework in this research seeks to work in a complementary manner to COBIT 5 on a higher governance level.

COBIT 5 is a major strategic improvement for Information Systems Audit and Control Association (ISACA), providing the next generation of SACAs guidance on the enterprise governance of IT. Building on the more than 15 years of practical usage and application of COBIT by many enterprises and users from the business, IT, security and assurance communities, COBIT 5 is designed to meet the current needs of stakeholders and align with the most up-to-date thinking in enterprise governance and IT management techniques (Khanyile & Abdullah, 2012). Further, COBIT 5 is an end-to-end umbrella framework that pulls together many existing frameworks designed to meet the current needs of stakeholders and align with the most up-to-date thinking in enterprise governance and IT management techniques.

While COBIT sets good practices for the means of risk management by providing a set of controls to mitigate IT risk. Risk IT sets good practices for the ends by providing a framework for enterprises to identify, govern and manage IT risk (ICASA, 2011).

There are some benefits the M-Commerce field and the proposed ICTMS framework (from the governance stand point) can gain from a framework of COBIT's nature. According to the IT Governance Institute, when looking at business outcomes of the Governance of Enterprise IT (GEIT), companies who have implemented COBIT 5 are experiencing improved

---

management of IT- related risk, improved communication and relationships between business and IT, lower IT costs, improved IT delivery of business objectives and improved competitiveness (ISACA and ITGI, 2011).

Moreover, COBIT 5 provides a clear distinction between governance and management of IT, providing a holistic view of the enterprise which covers the business and IT from end-to-end and enables the effective governance and management of enterprise IT assets. It enables business user satisfaction with IT engagement to the business to achieve business objectives. COBIT 5 also provides an easy to access Process Reference Guide at the same level of detail because it consolidates all previous research of ISACA (ICASA, 2012).

COBIT 5 is built on 5 key principles for the governance and management of enterprise Information Technology: *Principle 1: Meeting Stakeholder Needs; Principle 2: Covering the Enterprise End-to-End; Principle 3: Applying a Single Integrated Framework; Principle 4: Enabling a Holistic Approach; Principle 5: Separating Governance from Management*

COBIT 5 has 5 domains which are divided into governance and management domains; each domain has processes which enable it to achieve its objective(s). One domain addresses the governance and the other four domains cover management. The governance section provides guidance on evaluation, direction and monitoring of IT processes and is aligned with the ISO38500 “standard for corporate governance of information technology.” The management domains are in line with the four equivalent domains of COBIT 4.1.

#### **4.2.2 Business Model for Information Security (BMIS)**

In 2008, ISACA entered into a formal agreement with the University Of Southern California Marshall School Of Business Institute for Critical Information Infrastructure Protection to continue the development of its Systemic Security Management Model. The BMIS takes a business oriented approach to managing information security, building on the foundational concepts developed by the Institute (Ena et al., 2010). It utilizes 1) a systems thinking (Systems Theory) approach to clarify complex relationships within the enterprise, and thus to more effectively manage security, and 2) intentional security culture focusing on the enterprise’s governance needs Figure 4.1.

Systems theory is not a new concept. According to systems theory, a system essentially consists of objects (physical or logical), attributes that describe the objects, relationships among the objects and the environment in which the system is contained (ICASA 2011). A

---

critical piece of the model that differentiates it from many others is the importance it places on organizational culture (Ena et al., 2010). Creating an intentional security culture is a primary objective for the model, as applied to information security.

The BMIS recognizes that it is a dynamic and complex world, and provides a way information security managers can take when managing information security while directly addressing business objectives. The model also provides a common language for information security and business management to discuss information protection.

The BMIS is made up of four elements and six dynamic interconnections, where the model looks at each of these areas in-depth and, more importantly, the relationships between the areas. The BMIS can be viewed as a three-dimensional model, best visualized as a pyramid. Essentially all aspects of the model interact with each other. If any one part of the model is changed, not addressed or managed inappropriately, it will distort the balance of the Model (Ena et al., 2010). The dynamic interconnections act as tensions, exerting a push/pull force in reaction to changes in the enterprise, allowing the model to adapt as needed.

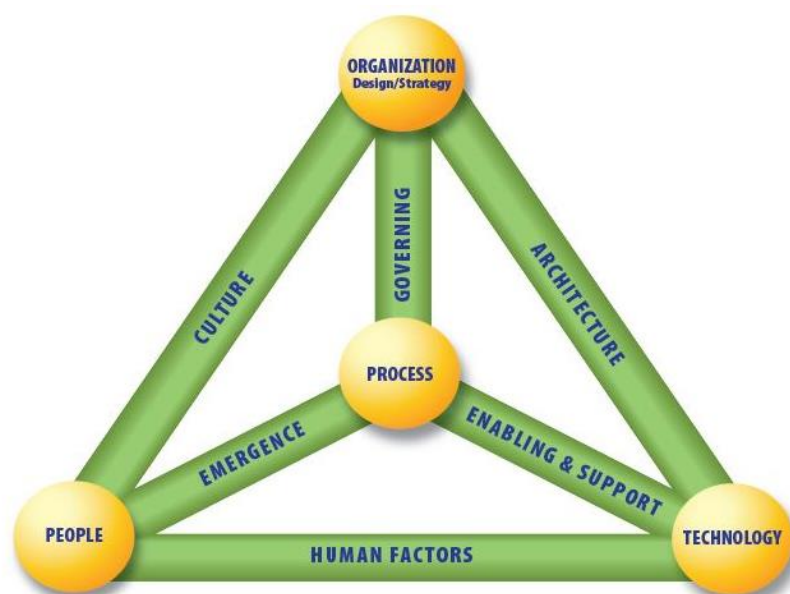


Figure 4.1: The business Model for Information Security (Ena et al., 2010)

**Organization Design and Strategy:** An organization is a network of people, assets and processes interacting with each other in defined roles and working toward a common goal. An enterprise's strategy specifies its business goals and the objectives to be achieved as well as the values and missions to be pursued. The strategy should adapt to external and internal

---

factors. Design defines how the organization implements its strategy. Processes, culture and architecture are important to determining the design (Ena et al., 2010).

- **People:** The people element represents the human resources and the security issues that surround them.
- **Process:** Process includes formal and informal mechanisms (large and small, simple and complex) to get things done and provides a vital link to all of the dynamic interconnections.
- **Technology:** The technology element is composed of all the tools, applications and infrastructure that make processes more efficient.

The dynamic interconnections on the BMIS link the elements together and exert a multidirectional force that pushes and pulls in the midst of change. Actions and behaviours that occur in the dynamic interconnections can force the model out of balance or bring it back to equilibrium (Ena et al., 2010). The six dynamic interconnections are:

- **Governing:** Governing is the steering of the enterprise and demands strategic leadership. Governing incorporates ensuring that objectives are determined and defined, ascertaining that risks are managed appropriately, and verifying that the enterprise's resources are used responsibly.
- **Culture:** Culture describes a pattern of behaviours, beliefs, assumptions, attitudes and ways of doing things. It is created from both external and internal factors, and is influenced by and influences organizational patterns.
- **Enabling and support:** The enabling and support dynamic interconnection connects the technology element to the process element. Many of the actions that affect both technology and processes occur in the enabling and support dynamic interconnection.
- **Emergence:** Emergence which connotes surfacing, developing, growing and evolving—refers to patterns that arise in the life of the enterprise that appear to have no obvious cause and whose outcomes seem impossible to predict and control.
- **Human factors:** The human factors dynamic interconnection represents the interaction and gap between technology and people and, as such, is critical to an

---

information security program. Human factors may arise because of age, experience level and/or cultural experiences.

- **Architecture:** Security architecture is a comprehensive and formal encapsulation of the people, processes, policies and technology that comprise an enterprise's security practices. It is within the architecture dynamic interconnection that the enterprise can ensure defence in depth.

The elements and dynamic interconnections that form the basis of the BMIS model establish the boundaries of an information security program and model how the program functions and reacts to internal and external change. The BMIS provides the context in which frameworks such as (COBIT) and standards that enterprises currently use to structure information security program activities come together. Essentially, the model integrates frameworks and standards for information security, defining the boundaries of an information security program and how the program functions.

### **4.3 M-Commerce regulatory requirements and Acceptable Information security standards**

Information security plays an important role in protecting the assets of an organisation. Since no single formula will guarantee ultimate security, there is a need for a set of benchmarks or standards to help ensure that an adequate level of security is attained, resources are used efficiently, and the best security practices are adopted (HKSAR, 2008a). This chapter presents the various information security standards and regulations that are applicable to the M-Commerce sphere. These standards and regulations shall provide 1) a theoretical foundation of the proposed framework and 2) a base for development of informed deliverables (tangible outputs from the framework) complements with: ISO standards, NIST, COBIT, the BMIS, etc.

#### **4.3.1 ISO Standards**

ISO (International Organization for Standardization) is a global network that identifies what International Standards are required by business, government and society, develops them in partnership with the sectors that will put them to use, adopts them by transparent procedures based on national input and delivers them to be implemented worldwide (Standards, 2008). ISO standards distil an international consensus from the broadest possible base of stakeholder

---

groups. Expert input comes from those closest to the needs for the standards and also to the results of implementing them. In this way, although voluntary, ISO standards are widely respected and accepted by public and private sectors internationally. The importance of standards may be better appreciated by considering what would happen in their absence; they ensure that positive characteristics like durability, quality, efficiency, safety, privacy, security and environmental friendliness are reinforced (Standards, 2008).

ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization. These boards form the specialised systems for worldwide standardisation. In the field of information technology, ISO and IEC established a joint technical committee ISO/IEC JTC1, whose main task is to prepare international standards. Draft international standards adopted by the JTC1 are circulated to the national bodies for voting where 75% approval is sought. ISO/IEC JTC1 maintains an expert committee dedicated to the development of Information Security Management System (ISMS) family of standards. Through the use of the ISMS family of standards, organisations can develop and implement a framework for managing the security of their information assets including financial information, intellectual property, and employee details, or information entrusted to them by customers or third parties. These standards can be used to prepare for an independent assessment of their ISMS applied to the protection of information.

The ISO/IEC 27000-series numbering (“ISO27k”) has been reserved for a family of information security management standards derived from British Standard BS 7799. The ISO27k (ISO/IEC 27000-series) standards concern the protection of valuable information assets through information security, particularly the use of Information Security Management Systems (ISMSs). Justifiably this research shall be confined to standards under this set. Of paramount importance, different ISO standards shall be integrated into the ICTMS framework, at relevant levels of threat as discussed in later chapters.

The related ISO standards that were valuable for this research include

- ISO/IEC TR27015: (financial services)
- ISO/IEC TR 27015:2012
- ISO/IEC TR 27033-1 & 2 (Network Security)
- ISO/IEC TR 27032 (Cyber Security)
- ISO/IEC TR 27034 (Applications Security)



---

More information on these standards can be obtained from the ISO official site (<http://goo.gl/Ep5TkM>).

#### **4.3.2 National Institute for Standards and Technology (NIST) Special Publication (SP)**

NIST is a non-regulatory federal agency within the U.S. Department of Commerce. NIST's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve quality of life. As part of its mission, NIST supplies industry, academia, government, and other users with over 1,300 Standard Reference Materials (SRMs) (<http://goo.gl/xWP0s>). These artefacts are certified as having specific characteristics or component content, used as calibration standards for measuring equipment and procedures, quality control benchmarks for industrial processes, and experimental control samples (NIST Website). NIST has a database of the most recent publications, through which additional publications are added on a continual basis. One group of such publications is the Special Publications (SP) for various fields of study which include: Law Enforcement Technology (SP 480-XX), Computer Systems Technology (SP 500-XX), Industrial Measurement Series (SP 700-XX), Computer Security Series (SP 800-XX), Integrated Services Digital Network Series (SP 823-XX), among a host of others. Many of the publications to be considered in the ICTMS framework come from the SP 800 range.

Special Publications in the 800 series present documents of general interest to the computer security community. The SP 800 series provides a separate identity for information technology security publications. The SP 800 series entails work from ITIL's research, guidelines, and outreach efforts in computer security, and its collaborative activities with industry, government, and academic organizations. As with the ISO standards, specific NIST SP standards will have to be integrated into the ICTMS framework, at relevant threat mitigation levels.

#### **4.3.3 Adoption of Security Models into Proposed Framework**

With existing frameworks and standards not adequately addressing organizational culture or human factors, or providing for the unexpected (as the BMIS model does through the concept of emergence) this research adopted the BMIS model as the basis of construction of the ICTMS framework. Amalgamating the BMIS (and related frameworks like COBIT) to the

---

proposed ICTMS framework can form a holistic and dynamic approach to information security that is both predictive and proactive as it adapts to changes, considers the organizational culture and delivers value to the business.

The BMIS does not replace the many sources of security program best practices as is the case with the proposed ICTMS Framework. It does, however, provide a view of information security program activities within the context of the larger enterprise, to integrate the disparate security program components into a holistic system of information protection (Ena et al., 2010). Areas essential for the success of an information security program but not currently defined in frameworks and standards will be developed as part of the evolution of the BMIS. To obtain the maximum value from this model, it is important to understand that these dynamic interconnections may be affected directly or indirectly by changes imposed on any of the other components within the model, not just the two components linked at either end (Ena et al., 2010). This model presents a ground on which the ICTMS framework has been developed.

Some of the related frameworks, models and standards are currently not recognised (or in use) in the current M-Commerce landscape in South Africa. The noted standards were developed for different users and audience (in a different country); a technically different security environment to South Africa.

ICTMS Framework is unique as it is one-of-a-kind framework aimed at improving security of M-Commerce services as ICT4D initiatives for poverty alleviation. Unlike most frameworks, ICTMS framework takes an in-depth look at the lower security level issues that plague the M-Commerce transacting environment- a feature most frameworks fail to address. This research employs an empirical study of the issue, as shall be presented in chapter 5

#### **4.4 Concepts, Assumptions, Beliefs and Information Security Theories**

The following subsections present the Information Security (IS) theories that provided the fundamental foundation on which the ICTMS framework was built. Each subsection gives a brief discussion of what each theory is about, then points out how each aided in the development of the ICTMS framework.

---

#### **4.4.1 System theory**

A system is an organized collection of parts (or subsystems) that are highly integrated to accomplish an overall goal. The system has various inputs, which go through certain processes to produce certain outputs, which together accomplish the overall desired goal for the system. Systems theory is not a new concept. It was proposed in the 1940s by the biologist Ludwig von Bertalanffy (1950) and furthered by Ross Ashby (1964). According to systems theory, a system essentially consists of objects (physical or logical), attributes that describe the objects, relationships among the objects and the environment in which the system is contained (Ena et al., 2010). By the same concept M-Commerce is a mobile transacting system under the E-Commerce subset. In extension to the description of a system outlined earlier in this chapter, M-Commerce threat/vulnerability levels in the ICTMS Framework constitute logical objects, where attributes can be drawn to describe each object. These levels of vulnerability relate logically to each other and to the environment.

The success the systems approach has achieved in other fields bodes well for the benefits it can bring to security (ISACA, 2009). The often dramatic failures of enterprises to adequately address security issues in recent years are due, to a significant extent, to their inability to define security and present it in a way that is comprehensible and relevant to all stakeholders (ISACA 2009). Utilizing a systems thinking approach to the ICTMS framework will help service and content providers to address complex and dynamic security environments. The same approach will generate a beneficial platform for them to discover real security issues at the grass roots level other than at a higher managerial level. Although systems thinking can contribute to these beneficial outcomes, it is important to note that the ICTMS framework, which is based on systems theory, should be treated as part of the strategic plan for the information security program, not as a quick-fix solution for a broken program. Systems thinking should be seen as a long-term exercise that will ultimately aid the enterprise in achieving business goals (ISACA, 2009). The maturity of the information security program is often related to the maturity of the enterprise, which is linked to the degree to which systemic thinking is used in the organization. Systemic thinking paves the way for systemic processes.

#### **4.4.2 Defence in Depth**

Another concept considered in this research work is the Defence in depth. This is a strategy common to both military manoeuvres and information security. In both cases, the basic

---

concept of defence in depth is to formulate a multi-layered defence that will allow us to still mount a successful defence should one or more of our defensive measures fail. One important concept to note when planning a defensive strategy using defence in depth is that it is not a magic bullet. The number of security/defence layers put in place, or the number of defensive measures that are put in place at each layer, will not be able to keep every attacker out for an indefinite period of time, nor is this the ultimate goal of defence in depth in an information security setting (Andress, 2011). The goal is to place enough defensive measures between the important assets and the attacker so that an attack in progress can be identified, allowing administrators enough time to take more active measures to prevent the attack from causing further distraction. The ICTMS frameworks' levels/ modules of vulnerability align with a multi-layered defence in the Defence in Depth ideology. Each layer tries to discover vulnerabilities that can be explored by an attacker to a user carrying out a transaction. This ensures that at each level a solution or form of defence can be developed at each layer of the framework as a way to strengthen the defence of the whole M-Commerce security ecosystem.

#### **4.4.3 Intentional Culture of Security**

Creating an intentional security culture is a primary objective for the ICTMS Framework, as applied to information security. No security policies, standards, guidelines or procedures can foresee all of the circumstances in which they are to be interpreted. Therefore, if stakeholders or the intended users of M-Commerce systems are not grounded in a culture of security, there is potential for improper actions. Security should not be considered as adverse to the achievement of business objectives. If perceived as adverse, it becomes clear that security is a weak part of the overall culture of that system and allows security to be seen as prohibition rather than enablement. Among the rationales for a culture of security is the alignment of security with the enterprise as a whole.

Culture of security was defined in BMIS as a pattern of behaviours, beliefs, assumptions, attitudes and ways of doing things. It is emergent and learned, and it creates a sense of comfort. Culture evolves as a type of shared history as a group goes through a set of common experiences. Those similar experiences cause certain responses, which become a set of expected and shared behaviours. These behaviours become unwritten rules that, in turn, become norms that are shared by all people who have that common history.

---

The culture determines what an enterprise actually does about security (or any other objective) and not what it says that it intends to do. An effective security culture supports the protection of information while also supporting the broader aims of the enterprise. To sustain a security culture, it is critical to understand whether it was created in a purposeful manner or by “accident.” However, a culture of security is not an end in itself, but a pathway to achieve and maintain other objectives, such as proper use of information. The greatest benefit of a culture of security is the effect it has on other components within an M-Commerce system. It leads to greater internal and external trust, consistency of results, easier compliance with laws and regulations and greater value in the enterprise as whole (ISACA 2009).

In a related work Ross et al., (2011), discuss how to achieve a meaningful, intentional security culture. The same work provides information on the benefits of, and inhibitors to, a culture of security. It discusses positive and negative reinforcement strategies and the steps to take to achieve the right balance in a security culture program.

#### **4.5 Chapter Summary**

The chapter discussed existing security frameworks to determine components applicable to the ICTMS framework context. Essentially, work under this chapter set the stage for the framework inputs component in the ICTMS framework, which include: government regulations; IT governance frameworks and models; Regulatory standards and requirements; information system theories. The noted standards aid in the development of deliverables, as will be noted in the next chapter.

---

## **Chapter 5. ICT M-Commerce Security Framework (ICTMS Framework)**

The ICTMS is a framework this research proposes to address security issues that rural marginalised communities of South Africa encounter when using M-Commerce ICT solutions. This section presents the proposed security framework based on the adapted features discussed in the previous chapters (Chapters 2 and 4). The presentation of the proposed security framework starts with a summary of what the proposed security framework entails. This paves the way for a detailed discussion of the aspects that were noted and used as a development basis of the ICTMS framework. This is followed by a presentation of the framework's properties, structure, components and the functionality of those components. The framework validation will follow, and lastly a discussion of the significance and drawbacks of the ICTMS framework concludes the chapter.

### **5.1 Background**

The proposed ICTMS framework addresses M-Commerce security challenges by offering a way for enterprises to synthesise the frameworks and standards they are utilising to a formal technical framework they can follow. This helps to create a holistic information security programme that does more for the enterprise than traditional approaches in protecting users when transacting. The Framework complements, and does not replace, an organization's existing business or information security risk management process. Rather, those stakeholders responsible for deploying M-Commerce platforms can use its current processes and leverage the framework to identify opportunities to improve their organization's security risk management. Alternatively, an organization without an existing security programme can use the ICTMS framework as a reference when establishing one. The framework is generic, which means it may be applied in any context, but for the purposes of this research, it was applied within a rural context.

### **5.2 Valuable Security Framework Aspects Summarised**

The previous chapters (2 and 4) unearthed some aspects valuable in building the ICTMS framework. This section presents some of those aspects that are of interest in the development of the ICTMS framework.

---

### **5.2.1 Security is as strong as its weakest link.**

One of the most common analogies in the security community is that security is a chain, where a system is only as secure as the weakest link. Hence, one consequence is that the weakest parts of a system are the parts most susceptible to attack. M-Commerce system is most secure when:

- All policies, procedures, software and devices work together to provide a secure and adaptive system.
- Threats are contained at every point of entry.
- The M-Commerce security framework can automatically adapt to new and changing threats.

Attackers tend to go after low-security areas of the system. If they target a system for whatever reason, they will seek the path of least resistance. That means they will try to attack the parts of the system that look weakest, and not the parts that look strong. Even if they spend an equal effort on all parts of a system, they are far more likely to find points of potential access in the parts in need of improvement. Likewise, this research, in unison with other researchers' findings, noted that the human aspect provided the weakest link in the M-Commerce system within a rural setup (Arief & Besnard, 2004; Albrechtsen, 2007). The proposed framework therefore assists in identifying what can be perceived to be the weakest components of a typical M-Commerce system by performing a risk analysis, preferably through a case study, as was the case in this research project. The framework allows the M-Commerce security environment to be viewed in its simplest clusters (threat levels) which are analogous to the individual chain rings. From such a setup, the most serious risk should be addressed first, than the risk that seems easiest to mitigate. Once it is clear that some other component has a bigger risk, efforts can be focussed elsewhere. Later sections in this chapter discuss in detail the mitigation measures that can be employed to address the problem.

### **5.2.2 No one size fits all**

There is no "one size fits all" solution to information security. The security measures appropriate for an organisation/system/community depend on its circumstances and security environment. In this case a risk-based approach to decide what level of security is required can be adopted. As noted later in this chapter, the framework has dependent variables which can change the way the framework can assist in securing an M-Commerce system or related

---

ICT4D tool/initiative. These variables are 1) environment in which the framework is to be implemented and 2) the actual threats and vulnerabilities discovered in each tier of the 4 tiers of the framework. The reason why there is no “one size fits all” solution in security is: different systems are developed on different programming languages, on different platforms, for a different target audience, and a different environmental setup, where their principle of security is different (McCown, 2008). For this reason the framework needs to have components that truly scale, allow for growth or shrinkage, and provide flexibility for any specific needs. Most often these frameworks work in an intertwined relation to deliver a common result. Further, with multiple frameworks any organisation or value-added chain may be able to view a scenario from multiple perceptions, enabling a more informed decision-making process. This is done by assessing which framework provides a viewpoint which has not yet been used.

### **5.2.3 Security as an afterthought**

It is imperative for an M-Commerce value-added chain to protect the M-Commerce environment. Through tools, technology and awareness, M-Commerce participants from the service providers down to the end user must become proactive about security, instead of reactive, meaning they can know about and thwart a potential security issue before any damage is done. According to Tam (2012), security issues can have an impact regardless of company size – from the largest enterprise to the smallest to medium sized business. Therefore, getting a security plan in place early on is the key to avoiding a security breach incident. We noted in this study that most security issues are side effects of one illness: the participants in the value-added chain and the customers rarely think about security first. As noted in Appendix C, users do not consider security in their use of mobile phones. User practices, as discussed in our work (Marufu et al., 2013), indicate clearly how users take security for granted. From the developers’ standpoint, numerous patches are created to narrow the threats affecting the applications. McCown (2008) notes that priorities among software developers are usually focused on the following: 1) cook up applications quickly; 2) gain massive distribution; 3) get people to install it, and 4) monetise the application. Among customers the priorities would be: 1) saving money; 2) ease of use; 3) ease of installation; 4) enabling the business somehow (and save more money). In this state of affairs “little things” like security are bolted on once these applications are widely adopted. It is our view that



---

security would be better if companies and M-Commerce value-added chain players gave forethought to security threats and vulnerabilities.

As it stands, enterprises are in such a rush to adopt new technologies such as cloud computing, mobile devices and social media, that they often overlook the security risks. According to Ernst & Young's 14th annual Global Information Security Survey (2011), many companies were aware of the risks that new technology presents, yet they move ahead without implementing security controls.

Thus it is from this realisation that it is necessary that internet access points for rural users (even those not specific to M-Commerce transacting) should be made secure from the initial development. The framework can be seen as an enabler towards a culture of security from the initial phase before most ICTs find their way to these marginalised places. Security should not be considered down the years as an add-on, due to hackers taking a shift towards the M-Commerce platform in use in marginalised rural communities.

The Living Lab (LL) concept can be leveraged to push awareness campaigns. This in turn helps in fostering a culture of security within a marginalised community. The LL setup like the Siyakhula Living Lab (SLL), which offers communities literacy training programs, can be leveraged to launch awareness campaigns on safe use of ICTs. This would ensure that a security culture is fostered from an initial stage not only to be considered as an afterthought when ICTs have gained popularity and have widely penetrated these rural areas.

Although internationally accepted standards and frameworks help to fill the gap in the knowledge base, they traditionally have not looked at the enterprise as a system, considering things such as culture and emergence (Ena et al., 2010). While there are existing models for security, they have not taken a holistic approach or look at security systemically. The ICTMS framework is a holistic and modular threat mitigation approach to managing M-Commerce security for security issues, and fills the gap that other standards and frameworks have not.

Mobile device security in developing countries may be realised by ensuring that such devices are developed locally for the local target population. This ensures the security concerns on the mobile phones as M-Commerce enablers are catered for from the onset, not as an afterthought. When an organisation or community does not have control of the major element of the system process chain (mobile devices for M-Commerce value chain) security might be difficult to consider as an initial thought.

---

#### **5.2.4 Security and Human Considerations**

In spite of the implied focus on technology, achieving security in an area like M-Commerce is more than just a technical problem. It is increasingly involving the active participation of people in order to securely design, deploy, configure and maintain the systems (Furnell & Clarke, 2012). According to various researchers, (Arief & Besnard, 2004; Albrechtsen, 2007; Furnell & Clarke, 2012), security efforts that fail to consider how humans react to and use technology often do not deliver intended benefits. It is perhaps unsurprising to find much of the focus in IT and computer security being drawn towards the technical aspects of the discipline. However, it is increasingly recognised that technology alone cannot deliver a complete solution, and there is also a tangible need to address human aspects. At the core, it is up to the users to understand the threats they face and be able to use the protection available to them. Although this has not been entirely ignored, observations in this research work shows it has not received the level of attention that it merits in ICT4D contexts. For this reason the ICTMS Framework pays close attention to this phenomenon by dedicating a module on the threat mitigation level to human aspects that might affect security when transacting. Indeed, security surveys commonly reveal that the more directly user-facing aspects such as policy, training and education are prone to receiving significantly less attention than technical controls such as firewalls, antivirus and intrusion detection. The underlying reason for such disparity is that the human aspects are in many ways a more challenging problem to approach, not least because they cannot be easily targeted with a product-based solution (Furnell & Clarke, 2012).

### **5.3 Properties of the ICTMS Framework**

Before delving deep into the components of the ICTMS framework a discussion of some fundamental properties that the ICTMS framework was constructed on is necessary. An understanding of these properties paves the way for a greater understanding of the components of the ICTMS framework. These properties were crafted from a wide array of frameworks and an understanding of literature around information security

#### **5.3.1 Framework integration facets**

The ICTMS framework is not an isolated solution, nor does its existence envisage the replacement of already existing frameworks. Its potential lies in blending/ amalgamating with

---

existing security structures (frameworks, models). The ICTMS framework was built on the same fundamentals as the BMIS, with its main focus on the technology-people-process relationship. In essence this phenomenon allows the framework to act as an extension of these frameworks and *vice versa*; as they are built on the same fundamental principles of security. As indicated in the previous chapter, the related frameworks on which the ICTMS framework can be integrated to focus on a higher level of security mostly. The proposed ICTMS framework takes an in-depth approach into the lower-level security issues. The application of this framework is to address the security issues encountered by marginalised rural users when transacting.

### **5.3.2 Multi-layered modular approach**

The ICTMS framework adopts the multi-layered approach used in the onion-ring architecture. This architecture offers security by organising and matching access rights to increasing levels of responsibility and accountability (Wei et al, 2006b). This multi-layered approach resembles fundamental principles of the Defence in Depth ideology: a multi-layered defence that allows a successful defence to be mounted should one or more defence measures fail. This research classifies M-Commerce security threat-vulnerability-risks into four six: human behaviour and mobile device interaction security, mobile device security, M-Commerce access channel security, wireless network access control security, back end/server and database security (not covered in this research). These inspire the modular layers in the ICTMS framework discussed later in this chapter.

This modular approach has two main advantages. First, it allows the architecture to address the security relationship between the various functional blocks of M-Commerce transacting in a marginalised rural area context. Second, it permits a detailed evaluation and implementation of security solutions on a module-by-module basis, instead of attempting implementation on the complete architecture in a single phase. The products of this approach are realised in deliverables, namely, technical blueprints, user guidelines and recommendations. As a modular, loosely-coupled architecture, components can be upgraded or replaced as required to meet changing threats without having to re-architect the entire framework. It is this multi-layered modular approach that makes the ICTMS framework realise areas for future study for other researchers in the area of ICT security and M-Commerce systems development. Each module presents an in-depth analysis, thereby

---

unveiling the various issues and areas that can be further explored by future researchers from academia and industry.

### **5.3.3 Threat mitigation approach**

The framework's focus is pinned on threats encountered by users when using M-Commerce ICT initiatives. M-Commerce service providers who understand these threats can better decide where and how to deploy mitigation technologies. Without a full understanding of the threats involved in M-Commerce transacting security for users, less informed deployments tend to be implemented. By taking the threat-mitigation approach, this framework should provide M-Commerce service providers with information on making sound platform security choices. This approach enables the framework to be user-centred, thereby allowing for the suggestion of user specific guides and solutions. Awareness programs can as well be implemented as per necessity. It is a generalisation in this research that most of the threats and threat levels are the same for all users, which means the framework may be used in different setups, provided a few adjustments are carried out to fit the new required context.

### **5.3.4 Principles-based and open to continuous improvement**

As noted in previous sections, the proposed framework in this research was built on a strong foundation of theory in Information Security, from academia and industry research knowledge bases. Likewise the framework is based upon well-agreed information security principles. Further, there is no 'silver bullet' in information security that can alleviate all threats and vulnerabilities. Thus at every threat mitigation level an active role is required to ensure new threats are dealt with. The ICTMS framework serves as a pointer to areas where continuous improvement can be carried out on M-Commerce systems.

## **5.4 ICTMS Framework Architecture**

On an abstract level the framework has three major components, each comprising of further subcomponents: Framework input, Threat mitigation levels, and Deliverables. Refer to Figure5.1.

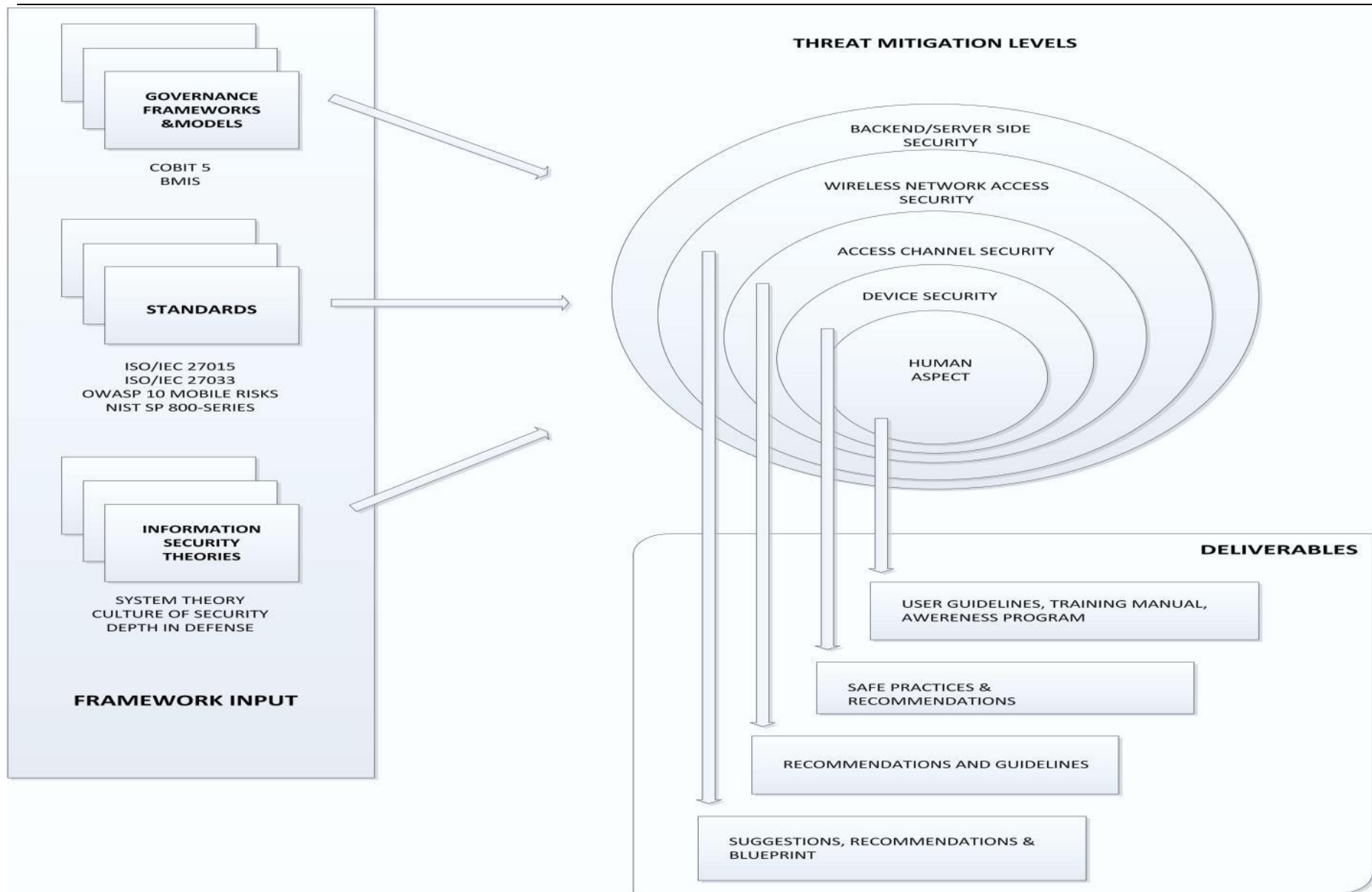


Figure 5.1: Components in the ICTMS Framework (Marufu & Sibanda, 2013a)



---

### **5.4.1 Framework input**

This component ensures that the framework is well positioned within a security environment in which it is set up to be used. The framework input component consists of three sub components: 1) Governance frameworks, Government Laws, Policies and Acts; 2) Standards and 3) Information Security Theories. Figure 5.1 indicates these three subcomponents of the framework and examples relating to each subcomponent. These input components create a platform where the actual core of the framework- the threat mitigation levels - is constructed.

Governance frameworks and models provide a structure on which the ICTMS framework integrates. Taking for example the COBIT framework, it provides a higher abstract level security for the M-Commerce value chain. In such a case deploying the ICTMS framework can be noted as an extension of these already-available security structures (frameworks and models) as it provides security down to the marginalised user conducting a mobile transaction.

Standards shown in Figure 5.1 provide guidelines to be followed in order to make security in each of the tiers of the ICTMS framework reach an acceptable threshold. Standards aid in developing informed deliverables in the framework. In addition, for each level/ tier of the framework's threat mitigation levels, different sets of recognised standards are employed to obtain a set of logical deliverables. A detailed view of how the standards do this can be traced in the next section. Examples of such standards used in this research include ISO/IEC TR 27015:2012, ISO/IEC TR 27033-1 & 2 (Network Security), ISO/IEC TR 27032 (Cyber Security), ISO/IEC TR 27034 (Applications Security), NIST SP800-127 (WiMAX security).

Information System Theories provide a deep background on the critical beliefs, assumptions, concepts and related work on the M-Commerce environment. Chapter 4 has a detailed discussion on some of the theories that were considered in the ICTMS framework.

### **5.4.2 Threat mitigation levels**

This component comprises five tiers/layers: Human Aspect, Device Security, Access Channel Security, Wireless Network Access Security, Backend/Server Side security. The layers were conceptualised from literature (Section 2.1). However, four levels

---

are considered in this research in order to narrow down the scope of the research in relation to the amount of time that was available to satisfy this work as a Master's thesis. Further, due to the restricted nature of the area the levels 5 and 6 seek to address, four levels are the current levels in the ICTMS framework. Although focus is on the first four layers, provision is made for the addition of more security layers. The option to adopt a "layered threat/vulnerability" component was discussed in Section 5.3.2. Each level has three main sections of analysis: 1) vulnerability discovery and assessment, 2) vulnerability and threat mitigation, 3) recommendations and suggestions. Firstly, threats and vulnerabilities are discovered, to which solutions to address the discovered threats follow, with the goal of solving them by specific solutions and recommendations. Each threat mitigation level requires different specific methods or techniques to be employed during the three stages of analysis, as will be discussed in later sections. At each respective threat mitigation level (1-4), mitigation of the threat also involves use of security standards that apply directly to them. For example, the network security level frameworks such as the Federal Information Processing Standards Publication 191, which presented Specifications for guidelines for the analysis Local Area Network (LAN) security. Such peer-reviewed standards can be incorporated to other security recommendations to make up deliverables aimed at addressing the discovered threats.

### **5.4.3 Deliverables**

This last component can be deemed the output component. Vulnerability assessment and threat discovery from each layer/ tier of the framework culminates in a deliverable, to alleviate the discovered vulnerabilities/threats. For instance, under the Human Aspect tier: some user guidelines on safe M-Commerce practices; a SLL training module section on M-Commerce and online safety; and an awareness program were developed. Details on deliverables were explained in detail under the discussions of each tier of the framework in section 5.5. It is significant to note that these deliverables do not suggest an ultimate solution to all the problems/ insecurities unearthed in each tier, but they pave the way to reducing risk, allowing for 1) a safer M-Commerce environment 2) better adoption of M-Commerce systems as ICT4D tools for poverty alleviation through improved trust. Henceforth, the deliverables that could be obtained by changing the study setup will change accordingly. These



---

deliverables are dependent variables: they depend on the rural setup in which the framework is deployed and the type of threats and vulnerabilities that would be unearthed in that rural setting.

The following section presents a detailed description of how the above components and subcomponents relate to each other and how they function to serve the required goal.

## **5.5 ICTMS Framework Functionality**

When considering functionality, the question that comes to mind is, what features should a comprehensive framework constitute? Patil (2008) suggested that a comprehensive information security framework should incorporate the following key elements:

- 1) Recommended sound security governance practices (e.g., organization, policies, etc.).
- 2) Recommended sound security controls practices (e.g., people, process, technology).
- 3) A guide to help reconcile the framework to common and different aspects of generally adopted standards (e.g., COBIT, HIPAA, etc.).
- 4) An analysis of risk or implications for each component of the framework.
- 5) A guide of acceptable options or alternatives and criteria, to aid in tailoring to an organizations operating environment.
- 6) A guide for implementation and monitoring.
- 7) Toolset for organizations to test compliance against the framework (e.g. HITRUST).

This section highlights how the ICTMS Framework incorporates these key elements. The approach adopted in this section links the aforementioned key elements of a comprehensive framework with the flow of thought introduced in the previous section (detailing how the components interact).

Figure 5.2 shows how the different components mentioned in the previous section interact.

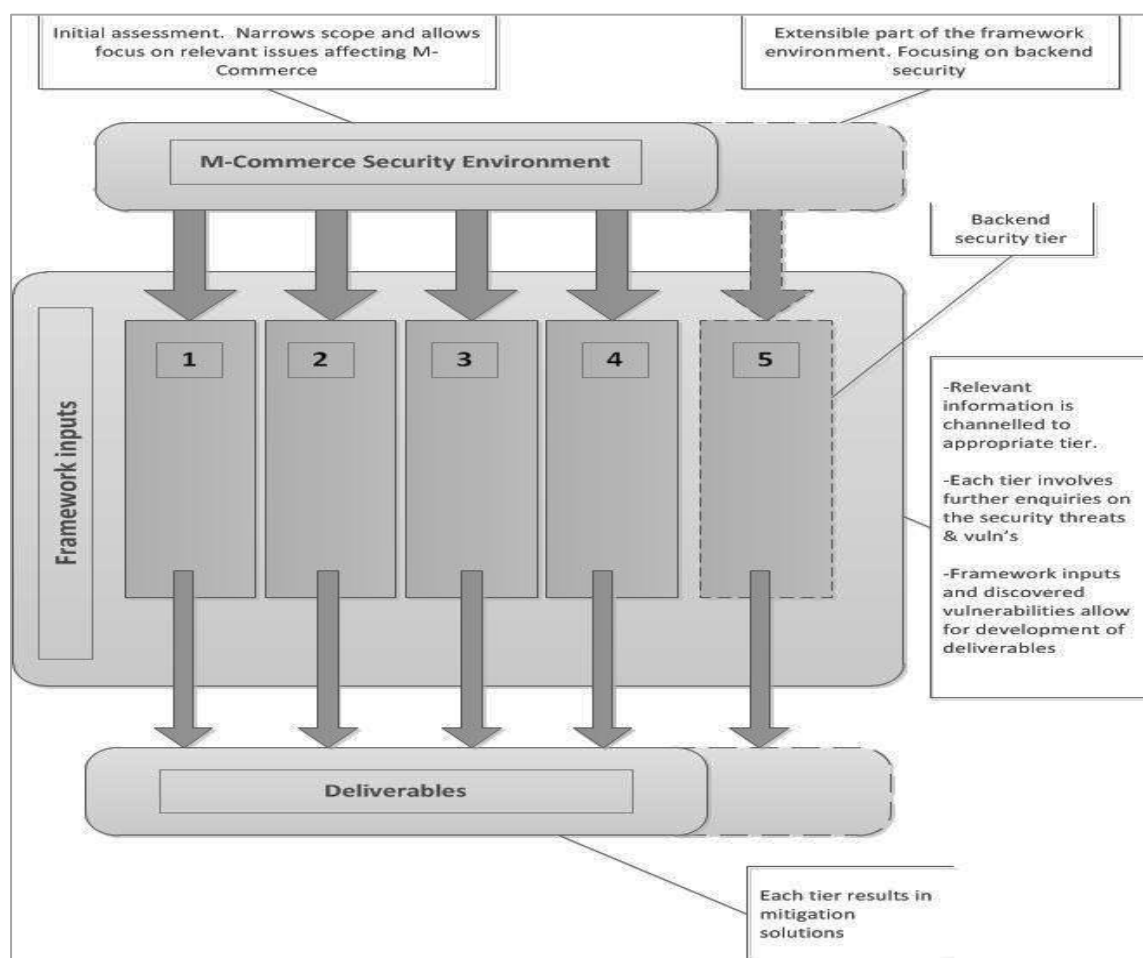


Figure 5.2: ICTMS Framework functioning components

### 5.5.1 M-Commerce security environment

The security environment incorporates all the background initial assessments. The segment also helps narrow the scope of analysis, allowing for a more focussed approach on the relevant security issues. Importantly this segment also allows the framework to be flexible to a change in environment by allowing new variables to be plugged into the framework mitigation threat level modules shown in Figure 5.2. The variables include information about governing laws, user behaviour, types of devices prevalent, type of network access, channels of transacting, etc. This segment involves qualitative tools for obtaining data. Of paramount importance, the number of modules in the lower segment (Figure 5.2) is determined and governed by the

---

outcome from this segment. At this juncture two of the key elements pointed out by Patil (2008) are addressed: (1) and (3).

### **5.5.2 Framework inputs**

Relevant information is channelled into the appropriate tier or module of the framework where further enquiries on the security threats are made. For instance, device security aspect information gathered on the M-Commerce ecosystem will be used to inform what vulnerability assessments to carry out in the *Device Security tier* of the ICTMS framework. These threat/vulnerability levels were made with a careful consideration of the “people, technology and process” principle, which in turn addresses the second of Patil’s key elements.

Thus, an investigation in this lower part of the model presented above involves technical methods of assessment (by mixed methods). Section 5.6.1 presents an assessment to this effect in depth. Each threat mitigation layer addresses Patel’s key elements (4), (5) and (6). The practical applicability of the proposed framework modelled in this section is presented as a case study scenario of a typical rural setup (Section 5.6). Following the discovery of threats and vulnerabilities through the assessments employed at each level, standards and models related to the tier are applied to inform on the mitigation measures. These related standards, models and Information security theories comprise the framework input (Figure 5.1). Thus if threats within the *Device Security tier* are noted, related standards, models and theories that ensure the threats are mitigated are employed. Later sections will elaborate on this aspect (Section 5.6.3).

### **5.5.3 Deliverables**

Deliverables are tangible solutions (artefacts, articles, software, and toolkits) that provide necessary capability to effect reasonable forms of mitigation to the threats/vulnerabilities that would have been discovered. These solutions are the result of combining best software, standards and framework models in a reasonable fashion to address the security challenge that would have been observed.

---

The following subsection demonstrates a typical case scenario (as a proof-of-concept) in which the ICTMS framework can be applied, to address M-Commerce security issues for rural users.

## **5.6 Application of the ICTMS Framework**

A case study was undertaken at the Siyakhula Living Lab at Dwesa in the Eastern Cape province of South Africa. The proposed ICTMS framework is applied in this case study scenario as a proof-of-concept. In so doing the researchers demonstrate how the major components of the proposed ICTMS framework function when applied to a rural setup. The strategy used in applying the framework to the case scenario follows the logic outlined in Section 5.5. Likewise, this section begins by giving a brief description of the scenario (the study setup, the participants involved and methods used to elicit data) followed by the outline of security functionalities required by the scenario. The description of how the framework provides the required functionalities presents the actual application of the framework to the scenario as a proof-of-concept.

Appendix A presents the study setup; discussing the sample, the instruments employed and how data were collected before outlining the importance and limitations of the data collected.

### **5.6.1 Rural M-Commerce Ecosystem**

The M-Commerce ecosystem has different variables at work with respect to context (Emmanuel & Muyingi, 2010; Chitungo & Munongo, 2013). Hence, an attempt was made to validate the threat mitigation levels in the proposed ICTMS framework to a practical rural setting, by presenting the current M-Commerce ecosystem within themes inspired by the threat/vulnerability levels modelled (Section 5.4). The aspects raising security concerns are noted thereafter. Data gathered during this phase include: 1) types of devices evident in these rural communities, 2) supporting network infrastructure for M-Commerce, 3) M-Commerce access channels in use, 4) willingness of the rural communities to engage in M-Commerce transactions, and 5) issue of trust in relation to security of M-Commerce transacting. To collect the data in this phase, a mixed method approach (qualitative measures and quantitative tools

---

such as contextual inquiry, participant observation, focus groups and questionnaires, (see Appendix A) was employed. The participants were from the literacy training classes from the SLL (see Appendix A). Appendix B presents a detailed discussion of the findings about the M-Commerce ecosystem within a rural setup. These findings show how transacting using mobile phones has reached the rural communities. Various other uses of mobile phones are being explored by users, making the M-Commerce ecosystem broad (as in peri-urban to urban setups) in terms of the viable vulnerability channels. This supports the significance of developing our proposed framework.

### **5.6.2 Threat and Vulnerability Framework Levels in a Rural Context**

Following the discovery of the M-Commerce security environment (using the guide in Section 5.5), contextualising the modelled security threat/vulnerability layers to a rural setting and the actual threat/vulnerability assessment was carried out. Assessing the applicability of each level of threat/vulnerability within the rural context aids in validating the relevance of each of these modelled framework layers. Hence, the different vulnerabilities that make M-Commerce unsafe and insecure for use by marginalised communities in the four threat/vulnerability mitigation levels were noted. The threat/vulnerability assessment (see Appendix C) provided for the development of deliverables which may be noted as a fulfilment of the nature of this study as applied research.

### **5.6.3 Threat and Vulnerability Mitigation (Provision for Framework Deliverables)**

To address the issues unearthed in the threat and vulnerability assessment, literature, related information security standards and lectures from security experts were used to construct the basis of the mitigation process. Appendix D presents a detailed account of the set of tools the security personnel within the M-Commerce value added chain can employ to understand and mitigate threats/vulnerabilities within the given context.

The case study was executed following the work flow detailed in Section 5.5. The findings in this chapter assisted in 1) establishing the state of affairs of the current rural M-Commerce ecosystem, 2) validating the applicability and relevance of the

---

threat/vulnerability mitigation levels modelled in Chapter 2 to the rural M-Commerce ecosystem, and 3) establishing the actual threats and vulnerabilities which led to an informed development of particular deliverables. Henceforth, the findings presented in this section sought to further strengthen the motivation behind developing a security framework in a rural context.

## **5.7 Validation of the ICTMS Framework**

The components of the framework were validated through development and application. Through development, a peer-reviewed theoretical foundation is applied to develop the framework model. Through application, the security threat levels were applied in a rural context to which threats and vulnerabilities were discovered by employing different techniques for each level. As pointed out earlier, several noteworthy research works were used for the construction of the threat/vulnerability mitigation security framework ICTMS in this study. These works include work presented in chapters 2 and 4, which facilitated the development and validation of the relevance of the framework threat/vulnerability mitigation levels.

The validation covered in this section involves using the information system components as the base concept. Information system resources can be defined as any organised combination of the following five resource components: hardware, software, data, networks, and people (Senior Scholars, 2007). Together, these components gather, transform, and disseminate information in an organisation (O'Brien, 2002). *People* make use of information systems to communicate using physical devices (*hardware*), information processing instructions and procedures (*software*), communications channels (*networks*), and stored databases (*data*). Similarly, the M-Commerce information systems that have these four non-human factor resource components will need to be protected by security measures to ensure their information quality and beneficial use, through which the business value of M-Commerce security can be achieved (O'Brien, 2002). Table 5.1 illustrates how the four ICTMS framework modules (layers) are interrelated to the resource components in information systems. The 'X' symbol signifies that the particular resource component has been covered in the ICTMS framework. As can be seen in Table 5.1, the hardware resource is covered by the modules (device security and network

security) of this framework. The software component is covered by three modules (human aspect, device security and access channel security). The network is covered by two modules (network security, and access channel security), while the data are covered by all four modules. The people resource in information systems is required in all the four modules as well. Since these resources are mutually dependent on each other and encompass the earlier layers, it can be concluded that the proposed framework does have high theoretical construct validity. This validation technique is adapted from the work of Wei et al., (2006a).

Table 5.1: Comparison of framework layers with the five resource components in information systems

	Hardware	Software	Network	Data	People
Human Aspect		X		X	X
Mobile Device Security	X	X		X	X
Access Channel		X	X	X	X
Wireless Access Network	X		X	X	X

## 5.8 Beneficiaries of the ICTMS framework

The Framework structure is designed to support existing aspects of business operations, and addresses M-Commerce security challenges users face by offering a way for enterprises to synthesise the frameworks and standards they are utilising to a formal technical framework they can follow. The following subsections establish which parties benefit from the proposed framework and how they benefit from it. The following examples provide options for using the ICTMS Framework.

### 5.8.1 Communicating Security Requirements with Stakeholders

The Framework provides a common language to communicate requirements among interdependent partners responsible for the delivery of critical M-Commerce

---

transacting platforms. The modular approach by the ICTMS framework aids in making the M-Commerce security environment simpler to understand. Depending on the role of the organisation in the M-Commerce value chain, the threat mitigation levels provide a guide to the security issues an organisation should address. From the fieldwork carried out, it can be noted how marginalised communities are in need of great ICT initiatives like M-Commerce, E-Health, etc., but lack an interface with the responsible value chain of the different services. In terms of security, marginalised communities would prefer a more direct audience with the service providers, where they can express their security concerns and build trust with them. This is supported by the data collected within this research. The ICTMS framework may be seen as a stepping stone in achieving such a dialogue in its first phase of operation (investigating the security environment).

Network administrators may also make use of the framework to establish which network components need attention in ensuring the network infrastructure and resources are secure.

### **5.8.2 Identifying Gaps for Future Research**

The Framework can be used to identify gaps where additional research would help organizations implement technologies or better address emerging threats. An organization going over the framework mitigation threat levels of the ICTMS framework may notice a level that they may have overlooked or particular threats/vulnerabilities that their current frameworks did not address. Researchers from both academia and industry can further explore these gaps. After pointing out the gaps, the organization might collaborate with technology leaders and/or standards boards to draft, develop, and coordinate standards, guidance, and practices to address the needs of potential adopters. These areas for improvement require continued focus. Although important, they are evolving areas that are yet to be developed or require further research and understanding. While tools, methodologies, and standards exist for some of the areas, they need to become more mature, available, and widely adopted.



---

### **5.8.3 M-Commerce User Considerations**

The framework was modelled around a rural community that is embraced by the presence of a living lab. Likewise application of the proposed framework will better suit related areas with living labs. The Framework is built and modelled around delivering an intentional culture of security for the end users of M-Commerce services in rural communities. This can be realised by the deliverables that each tier of the framework produces. Apart from all the deliverables, users should take a positive stance to protect themselves and their information when engaging in online activities. The human aspect is the main cornerstone of this research and likewise the ICTMS Framework. The framework is, therefore, structured to deliver the required solutions and ideas to tackle security issues targeting the mainstream M-Commerce users.

## **5.9 Significance of the ICTMS Framework**

An M-Commerce platform has many participants and has all the components such as software development, policies and procedures, incident management, business continuity management, regulations and audit etc. These components are called islands of security which cannot talk to each other and also do not work together (Patil, 2008). Therefore, a comprehensive information security framework is the answer for the components to work together, instead of having stand-alone components and systems. The same phenomenon can be noted in an M-Commerce value chain, where there are many participants employing different security strategies and implementations. A connected information security framework delivers practical guidance for everyday IT practices and activities, helping users establish and implement reliable, cost-effective IT services. In this case the ICTMS framework stands to look in-depth into four levels of threat and create a way in which the M-Commerce environment is more secure, by 1) best protecting or equipping users in using M-Commerce services, 2) providing a guide to service providers involved in pushing such M-Commerce platforms to these areas, 3) assisting further researchers willing to work on improving security in MRAs, 4) filling in the vacuum from upper-level security structures from M-Commerce platform developers to the lower-end user level. The ICTMS framework provides a

---

different perspective to the M-Commerce security environment. Further, in the current research we argue that, although it may be difficult to create a non-hackable system, the ICTMS framework will help in making these M-Commerce systems difficult to hack/ exploit.

Although these mentioned findings make the framework a positive step towards making ICT tools for development (specifically M-Commerce) more secure, we have noted some limitations that can be brought to light. The following section delves into these drawbacks and challenges.

### **5.10 Limitations of ICTMS Framework**

Unfortunately, while security frameworks can provide some help and value, all of them have drawbacks or weaknesses (IsecT, 2011). A weakness in most security frameworks is the narrow focus on a particular area, topic or approach. The argument is that security should take a holistic approach, with input from a variety of fields and a wide-ranging overview of the problem, as well as details suitable to the situation or environment. Unfortunately, it is not easy to document such a broad approach. The ICTMS main focus is on M-Commerce security environment in an ICT4D context. Some frameworks focus on details without considering anything about the overview. Likewise some take a management view and neglect the specifics and *vice versa*, while others focus on functional security, others on assurance mechanisms. This is the reason why frameworks should be used in an intertwined manner to provide a complementary impact on a given security objective.

It is worth noting at this juncture that the proposed framework in this research mainly focuses on the M-Commerce user to be the only *human aspect* it addresses, as other human aspect issues are assumed to be catered for by enterprise policy, security frameworks and models (COBiT, IBMS, etc.). If an M-Commerce platform lacks these supporting structures, implementation of the ICTMS framework may not live to fruition in ensuring safe M-Commerce transacting by marginalised communities. On the same note, use of ICTs as poverty alleviation tools would not be realised.

Another shortfall in the ICTMS Framework is that it was modelled to be implemented in a setup where the deliverables can be deployed or implemented, thus its focus towards those members within a LL/Telecentre environment that offers

---

literacy training to users (Section 6.4). This implies that a large population of the intended beneficiaries of this initiative will be left out in such a setup. The realised deliverables from the frameworks threat mitigation levels may only be available for marginalised M-Commerce users in a LL setup. The tiers/modules considered in this research work run as far as the wireless access network level and not beyond (for scalability of the research); assuming the backend is secure, which might not be the case.

The framework should be continuous and constantly upgraded. Thus a suggestion is to have an active online community to help develop further on this current framework. To address the areas for improvement the community must identify primary challenges; solicit input from stakeholders to address those identified challenges, and collaboratively develop and execute action plans for addressing the challenges.

The framework's core principals and behaviour cannot be modified, meaning that when you use a framework, you are forced to respect its limits and work the way it requires. Flexibility can break the core of a framework.

## **5.11 Chapter Summary**

This chapter has consolidated the entire security framework requirements gathered from literature (Chapter 2 and 3) into a model. The proposed framework's properties (Section 5.3) and architecture (Section 5.4) are then clearly defined. After demonstrating the functionality of the components in reference to its applicability the framework is then validated using two methods (through construction and through implementation). By construct the ICTMS framework is then validated on information system components and by choice of incorporating components from peer-reviewed sources. On the same wavelength, we presented application of the ICTMS framework in a case study scenario as a proof-of-concept. A case study of the SLL in the Dwesa/Cwebe area helped to demonstrate that the proposed security framework may be applied in a rural context. The case study strengthens the merit of the proposed ICTMS framework. The use of practical applicability eliminates misunderstandings about the scope and functionalities of the proposed security framework. The scenario was selected from ICT4D application domain to increase

---

the quality of generalization. Significance and limitations of the framework were then presented before this chapter summary.

The following chapter, Chapter 6, concludes this dissertation by presenting the contribution of the study, the summary of findings, and the conclusions and recommendations for future work.

---

## Chapter 6. Conclusion and Contribution

In this chapter, the dissertation is concluded by presenting summaries of the research findings and conclusions made by the study. The contributions made by the research, as well as recommendations for further research, are also presented. In the course of answering research questions outlined in Chapter 1, this dissertation presented different findings from each research sub-question. Each chapter of the dissertation, with the exception of Chapter 1 (Introduction) and Chapter 3 (Research Design and Methodology), addressed different research questions. This section presents a summary of the research findings reported in the dissertation. This is followed by a comprehensive section: threat/vulnerability levels; a main feature in the ICTMS framework.

### 6.1 Chapter Summary and Findings

The main objective of this study was to develop a security framework M-Commerce service provision in rural contexts. A framework in this study was defined as a brief set of ideas for organising a thought process about a particular type of thing. In the process of developing an M-Commerce security framework in a rural context, several research questions were set and answered.

The first research sub-question to be answered was: *What security aspects are related to M-Commerce as an ICT4D initiative?* Research activities pertaining to this research question were presented in Chapter 2. Security issues were classified into four levels of threat/vulnerability and related study works dissected to obtain the essential security aspects to be considered in developing a framework. The required components for developing the proposed framework were also established

The second sub-question to be answered was: *What are the requirements of an M-Commerce security framework?* The question was aimed at eliciting some framework development requirements from literature. Hence the essential components of a security framework were extracted from the literature and integrated into model building in Chapter 5. Security frameworks with essential components are adapted to satisfy the requirements of an M-Commerce security framework.

---

The third research sub-question to be answered was: *What existing security structures are related to the M-Commerce security?* The question was aimed at studying the existing security frameworks so as to determine components that could be used in building the proposed ICTMS framework. Chapter 4 presented these framework input components in the ICTMS framework, which include government regulations; IT governance frameworks and models; regulatory standards and requirements; information system theories. According to existing theory, there exist security frameworks that have some of the essential components of an M-Commerce security framework.

The fourth research sub-question to be answered was: *What are the components of a security framework for the M-Commerce security framework?* The aim of this question was to identify elements or components needed to compile a security framework from the existing security structures and M-Commerce security environment. These elements are presented in Section 5.2. These considerations aided in developing the framework properties in Section 5.3. Chapter 6 presents the case study that was used as proof-of-concept that the framework works by following a step by step process modelled in Section 5.5. The case study further validated the framework, pointing out to the types of threats that should be addressed within the four levels obtained from the literature review. Subsequently, these results of the case study further strengthened the threat/vulnerability levels of the framework.

This research was able to propose a framework which aims to 1) ensure secure transacting by marginalised users using M-Commerce initiatives, 2) provide a guide to M-Commerce value chain (Service providers, content developers etc.) involved in deploying M-Commerce platforms being used by rural users, by giving them a security insight of the M-Commerce environment in a rural context, 3) fill in the vacuum between the upper-level security structures from M-Commerce platform developers and the lower-level user end and 4) assist further researchers willing to work on improving security of ICTs.

## **6.2 Summary of Conclusions**

From the title of this document it is evident that the main objective of the study is to develop an M-Commerce security framework that can be used to address security

---

issues in an ICT4D setup. The move towards an M-Commerce security framework in an ICT4D context was motivated by the security challenges discussed in Chapter 2, as well as the non-existence of a security framework that satisfies the requirements of an M-Commerce security ecosystem outlined in Chapter 4.

From the research findings summarised in Section 6.1 above, the main research question can be answered at this point. The main research question of this dissertation was: How can an M-Commerce security framework be developed to solve security issues faced by marginalised rural users? The study came to the following conclusions based on the research findings and analysis presented in Chapters 4 and 5.

It was established in Chapter 2 that security vulnerabilities and threats span the whole M-Commerce spectrum, from the top layer to the bottom layer of the OSI network protocol stack, from machines to humans. The threats and vulnerabilities were classified into four main levels of security threats and vulnerability: mobile device security, human behaviour and device interaction (human aspect; [1a], [1b]), underlying network infrastructure/technologies (wireless network access channels [4]), and the M-Commerce access channel [3]. Coupled with the lack of a framework that directly deals with the security issues for a marginalised user, development of the ICTMS framework was argued to be necessary. The security framework solution should therefore provide security services to counter the abovementioned security threats.

Chapter 3 then maps out a plan on how the objectives were to be reached. The proposed security framework explained in Chapter 5 is the result of the research findings based on the four research sub-questions. In other words, the compiled ICTMS framework is the result of security aspects (sub-question 1), the requirements of a security framework (sub-question 2), the essential components of a security framework (sub-question 3), and the components of a security framework for the Semantic Web (sub-question 4).

ICTMS framework on an abstract level has three major components, each comprising of further subcomponents: Framework input, Threat mitigation levels, and Deliverables. A detailed account of the functionality of these components and sub-components was discussed in Chapter 5 (Section 5.4 and 5.5). After demonstrating the functionality of the components in reference to its applicability the

---

framework is validated using two methods (through construction and through application) (Section 5.5). The significance and drawbacks were also mapped out.

### **6.3 Recommendations for Further Research**

This section presents recommendations for further research based on the findings of the dissertation and the conclusions drawn. The study makes recommendations for improving the framework, further validation of the framework, investigating new security frameworks and investigating more requirements

#### **6.3.1 Improving the framework**

The proposed ICTMS framework utilises the established levels of threat/vulnerability within an M-Commerce ecosystem, outlined in Section 2.1. The framework can be improved by including the emerging functionalities and technologies. For instance, levels 5 and 6 suggested in section 2.1 would have to be incorporated. Within level 3 of the framework, more channels (NFC, IRV, etc.) would have to be addressed as more and more services find their way to marginalised areas of Africa. The framework can also be improved by considering different rural contexts: those rural areas without access to Living Labs or Telecentres to leverage the use of ICTs.

#### **6.3.2 Further validation of the framework**

The proposed ICTMS framework included the adaptation and integration of different components from different security frameworks. This conceptual adaptation and integration of the framework components was done, but without the criteria to validate the outcome. Further validation will improve internal accuracy of the framework. Further, the use of one case study does not allow for the generalisation of results that the framework works in a rural context. There is need to carry out more case studies to test the validity of the framework.



---

### **6.3.3 Investigating new security frameworks**

M-Commerce security and security of ICTs is currently an active research area, hence the need to investigate new security frameworks, standards and models currently being developed. This will effectively keep the model of the framework relevant to the ever-changing M-Commerce security ecosystem.

### **6.3.4 Investigating more requirements**

The requirements of a security framework for the Semantic Web were extracted from the existing security frameworks discussed in the literature review. Since M-Commerce in ICT4D contexts are still in the development stage and most M-Commerce applications are at research level, there is still room to extract new requirements of an M-Commerce security framework.

## **6.4 Closing remarks**

The idea of developing a framework, as the main output of this research is the answer for the components to work together, instead of having stand-alone components and systems. This research allowed for a better assessment of the vulnerabilities that usually affect marginalised M-Commerce users by employing the framework. This framework can be seen as a roadmap security enhancement plan for other ICT4D services which include but are not limited to M-Health, E-Judiciary, and E-Government. This is through the realisation that the services use merely the same technologies and are thereby exposed to the same vulnerabilities, threats and risks. The scope of research in M-Commerce security continues to grow with the introduction of new technologies and platforms to offer transacting capabilities. This makes the research area more and more interesting due to rising security problems.

---

## References

- Adesola, S.A., 2012. Alleviating Poverty through ICT as a means of Sustainable Socio-Economic Growth in Nigeria. *International Journal of Academic Research in Economics and Management Sciences*, 1(1), pp.89–98. Available at: <http://goo.gl/W2bWQl>.
- Ahuja, S.P. & Collier, N., 2010. An Assessment of WiMax Security. , 2010(May), pp.134–137.
- Albrechtsen, E., 2007. A qualitative study of users' view on information security. *Computers & Security*, 26(4), pp.276–289. Available at: <http://linkinghub.elsevier.com/retrieve/pii/S0167404806002033> [Accessed October 29, 2013].
- Al-zarouni, M., 2007. Introduction to Mobile Phone Flasher Devices and Considerations for their Use in Mobile Phone Forensics.
- Anand, S.V., 2007. *Mobile Application Security Framework for the Handheld Devices in Wireless Cellular Networks*,
- Andress, J., 2011. *The basics of information security : understanding the fundamentals of InfoSec in theory and practice*, Waltham: © 2011 Elsevier Inc.
- Apvrille, A., Caquot, A. & Antipolis, S., 2011. An Openbts Gsm Replication Jail For Mobile Malware. , (October), pp.1–9.
- Arief, B. & Besnard, D., 2004. Technical and Human Issues in Computer-Based Systems Security.
- Bailes, A., Brown, J. & Coley, L., 2006. M-Commerce Security : Issues , Trends , & Threats. *ISM* 4320, pp.1–14.
- Ben-asher, N. et al., 2011. On the need for different security methods on mobile phones. In *MobileHCI 2011*. Stockholm: ACM, pp. 465–473.
- Braund, P., 2006. Information and Communications Technology for Economic Development A Report on the Global E-Discussion Information and Communications Technology for Economic Development.
- Burgess, T.M., 2001. Guide to the Design of Questionnaires. *A general introduction to the design of questionnaires for survey research.*, University(1.1), pp.1–27. Available at: <http://goo.gl/DBjcT3>.
- Charles, B.L., Monodee, F. & Nurek, T., 2000. *The Critical Success Factors For Mobile Commerce: An Empirical Research paper*. University Of Cape town. Available at: <http://goo.gl/ctH1i>.
- Chikomo, K. et al., 2006. Security of Mobile Banking. Available at: [http://pubs.cs.uct.ac.za/archive/00000347/01/Security\\_of\\_Mobile\\_Banking\\_paper.pdf](http://pubs.cs.uct.ac.za/archive/00000347/01/Security_of_Mobile_Banking_paper.pdf).
- Chitungo, S.K. & Munongo, S., 2013. Extending the Technology Acceptance Model to Mobile Banking Adoption in Rural Zimbabwe. *Journal of Business Administration and Education*, 3(1), pp.51–79. Available at: <http://goo.gl/kuNS1X>.
- Clarke, R., 2008. A Risk Assessment Framework for Mobile Payments. In *21st Bled eConference eCollaboration: Overcoming Boundaries through Multi-Channel Interaction*. Bled, Slovenia, pp. 63–77.

- 
- CLUSIF, 2010. Web Application Security: Managing web application security risks. , (March).
- Cohen, D. & Crabtree, B., 2006. Qualitative Research Guidelines Project. *Robert Wood Johnson Foundation*. Available at: <http://goo.gl/bBoRJQ> [Accessed June 20, 2012].
- Couture, E., 2010. Mobile Security: Current threats and emerging protective measures. *The SANS Institute*, (InfoSec reading Room).
- Cuevas, C., Johnson, K. & DeLaGrange, T., 2011. MobiSec Live Environment DARPA Project. Available at: <http://goo.gl/8b38Z> [Accessed December 19, 2012].
- Dai, W. & Tang, Y., 2010. Research on Security Payment Technology Based on Mobile E-Commerce. *2010 2nd International Conference on Ebusiness and Information System Security*, pp.1–4. Available at: [http://ieeexplore.ieee.org/xpl/freeabs\\_all.jsp?arnumber=5473760](http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=5473760).
- Deepti, Khokhar, D. & Ahuja, S.P., 2012. A Survey Of Rogue Base Station Attacks In WiMAX. *International Journal of Advanced Research in Computer Science and Software Engineering Research*, 2(1), pp.1–5. Available at: [www.ijarcse.com](http://www.ijarcse.com).
- Dhir, A. et al., 2012. Design Guidelines for Pervasive Computing : Implications of Technology Use in Africa. *The Second IEEE International Workshop on Social Implications of Pervasive Computing, Lugano*, (March), pp.925–930.
- Diga, K., 2007. Mobile Cell Phones and Poverty Reduction : Technology Spending Patterns and Poverty Level Change among Households in Uganda. *Environment*, (December), p.4. Available at: [http://dev.mobileactive.org/files/file\\_uploads/Diga\\_2007.pdf](http://dev.mobileactive.org/files/file_uploads/Diga_2007.pdf).
- Dlamini, M.T., Eloff, J.H.P. & Eloff, M.M., 2009. Information security: The moving target. *Computers & Security*, 28(3-4), pp.189–198. Available at: <http://linkinghub.elsevier.com/retrieve/pii/S0167404808001168> [Accessed October 29, 2013].
- Duga, N. & Getachew, H., 2009. Mobile Services and ICT4D: To the Network Economy - Bridging the Digital Divide, Ethiopia's Case. *Addis Ababa University*, pp.1–7. Available at: <http://goo.gl/SWwqHZ> [Accessed May 23, 2012].
- Eiselen, R., Uys, T. & Potgieter, N., 2005. *Analysing survey data using SPSS13: A workbook*, Johannesburg: University of Johannesburg.
- Emmanuel, E.A. & Muyingi, H.N., 2010. Mobile Commerce Interaction Techniques for African Rural Economy Development : A Case Study for Dwesa.
- Ena, E.N.C. et al., 2010. The Business Model for Information Security (by ISACA). , pp.1–72. Available at: [www.isaca.org](http://www.isaca.org).
- Espiner, T., 2006. Phone Phishing Attack Hits US. Available at: <http://goo.gl/OYIrB> [Accessed May 10, 2013].
- EYGM, 2012. Mobile device security. *Insights on governance, risk and compliance*., (January).
- Fontana, A. & Frey, J.H., 2005. The Sage handbook of qualitative research. In N. . Denzin & Y. S. Lincoln, eds. *The interview: From neutral stance to political involvement*. Thousand Oaks, pp. 695–727.
- Freitas, H. et al., 1998. The Focus Group - A Qualitative Research Method: Reviewing The theory , and Providing Guidelines to Its Planning. , (010298), pp.1–22.

- 
- Fuller, M., 2005. M-Commerce and Security. , pp.1–14. Available at: <http://goo.gl/0WZ9i> [Accessed August 20, 2012].
- Furnell, S. & Clarke, N., 2012. Power to the people? The evolving recognition of human aspects of security. *Computers & Security*, 31(8), pp.983–988. Available at: <http://linkinghub.elsevier.com/retrieve/pii/S0167404812001228> [Accessed October 29, 2013].
- Goudar, A., 2010. *Mobile Transactions and Payment Processing (MPHASIS an HP company)*, New York, New York, USA. Available at: <http://goo.gl/Brj0UL>.
- Grami, A. & Schell, B.H., 2004. Future Trends in Mobile Commerce : Service Offerings , Technological Advances and Security Challenges. , pp.1–14. Available at: <http://goo.gl/vd8XE>.
- Grobler, M. et al., 2011. Towards a cyber security aware rural community. In *Proceedings of the 2011 Information Security for South Africa (ISSA) Conference*. Johannesburg: Institute of Electrical and Electronics Engineers ( IEEE ), pp. 1–7. Available at: <http://goo.gl/680YtV>.
- Gumbo, S. et al., 2012. Living Lab Methodology as an Approach to Innovation in ICT4D : The Siyakhula Living Lab Experience. In P. Cunningham & M. Cunningham, eds. *IST-Africa 2012 Conference Proceedings*. Dar es Salaam: IIMC International Information Management Corporation, pp. 1–9.
- Gururajan, R.A.J., 2006. A Discussion On Security Risks In Mobile Commerce. *e-Business Review*,, 7(2), pp.1–14.
- Hancock, B., 1998. An Introduction to Qualitative Research An Introduction to Qualitative. *Trent Focus for Research and Development in Primary Health Care An*, ((Updated 2002) Copyright of the Trent Focus Group).
- Heeks, R., 2009. The ICT4D 2.0 Manifesto: Where Next for ICTs and International Development? *Development Informatics Working Paper Series*, (42), pp.1–35. Available at: [http://www.sed.manchester.ac.uk/idpm/research/publications/wp/di/documents/di\\_wp42.pdf](http://www.sed.manchester.ac.uk/idpm/research/publications/wp/di/documents/di_wp42.pdf).
- HKSAR, 2008a. An Overview Of Information Security Standard; Government of the Hong Kong Special Administrative Region. , (February).
- HKSAR, 2008b. *Web Application Security*, Hong Kong.
- Howie, D., Koivisto, A. & Sauvola, J., 2001. A hierarchical framework model of mobile security. *12th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications. PIMRC Proceedings (Cat. No.01TH8598)*, 1, p.A–56–A–60. Available at: <http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=965391>.
- Hsieh, C., 2007. Mobile Commerce : Assessing New Business Opportunities. , 7(1), pp.87–100.
- Hui, T., 2011. Security Framework for Mobile Commerce. *Energy Procedia*, (13), pp.8602–8608.
- Humaidi, N. & Balakrishnan, V., 2012. The Influence of Security Awareness and Security Technology on Users ' Behavior towards the Implementation of Health Information System : A Conceptual Framework. , 35.
- ICASA, 2011. COBIT 5 A Business Framework for the Governance and Management of IT. Available at: <http://www.isaca.org/COBIT/Pages/COBITFramework.aspx> [Accessed May 17, 2012].
-

- 
- ISACA, 2009. An Introduction to the Business Model for Information Security. *University of Southern California's Marshall School of Business Institute for Critical Information Infrastructure Protection*, pp.1–27.
- IsecT, 2011. Information security compliance. *IsecT Ltd*, (March), pp.1–10. Available at: <http://goo.gl/xV05Hv> [Accessed September 20, 2012].
- Jansen, W. et al., 2007. A Unified Framework for Mobile Device Security Vlad Korolev.
- Jansen, W. & Ayers, R., 2007. Guidelines on Cell Phone Forensics Recommendations of the National Institute of Standards and Technology. *Nist Special Publication*, 800(101), pp.1–104. Available at: <http://csrc.nist.gov/publications/nistpubs/800-101/SP800-101.pdf>.
- Jansen, W. & Scarfone, K., 2008. *Guidelines on Cell Phone and PDA Security Recommendations of the National Institute of Standards and Technology*, Gaithersburg. Available at: <http://goo.gl/SfB1L>.
- Jha, R.K. et al., 2012. Detection and Fortification Analysis of WiMAX Network : With Misbehavior Node Attack. , 2012(June), pp.353–367.
- Jha, R.K. & Dalal, U.D., 2011a. Security analysis of WiMAX network: With Misbehavior Node attack. *2011 World Congress on Information and Communication Technologies*, pp.391–398. Available at: <http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6141278>.
- Jha, R.K. & Dalal, U.D., 2011b. Security analysis of WiMAX network: With Misbehavior Node attack. *2011 World Congress on Information and Communication Technologies*, pp.391–398. Available at: <http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6141278>.
- Jiang, E.P., 2012. Designing a Framework for Network Security Protection. *World Academy of Science, Engineering and Technology*, 66, pp.928–932.
- Jobodwana, Z.N., 2009. E-Commerce and Mobile Commerce in South Africa : Regulatory Challenges. , 4(4), pp.287–298.
- Joubert, J. & Belle, J. Van, 2009. The Importance of Trust and Risk in M-Commerce : A South African Perspective. In *Pacific Asia Conference on Information Systems (PACIS) PACIS 2009 Proceedings*. pp. 1–14. Available at: <http://goo.gl/WbKnxY>.
- Kark, K. et al., 2007. Defining a High-Level Security Framework. *Forester Research: For Security & Risk Professionals*. Available at: <http://goo.gl/0zY7B>.
- Kennedy, D., 2010. *Social Engineering Toolkit (Devolution)*, Available at: <http://www.social-engineer.org>.
- Khanyile, S. & Abdullah, H., 2012. *COBIT 5 : an evolutionary framework and only framework to address the governance and management of enterprise IT*,
- Kmal, D. & Abdullah, S., 2009. Build A Framework to Optimize M-Commerce Security Abstract : *Tikrit Journal of Pure Science*, 15(2), pp.123–127. Available at: <http://goo.gl/l8uJ9>.
- Kothari, C.R. & Garg, G., 2014. Research Methodology: An Introduction. In *Research Methodology : Methods and Techniques*. p. 470. Available at: <http://goo.gl/Vsj8T4>.
- Krueger, R.A., 2002. Designing and Conducting Focus Group Interviews. *Developing questions for focus groups*. Thousand Oaks, CA:, (October).

- 
- Languepin, O., 2010. How mobile phones can help reduce poverty. Available at: <http://thailand-business-news.com/news/top-stories/26596-how-mobile-phones-can-help-reduce-poverty>. [Accessed May 22, 2012].
- Lee, C., Kou, W. & Hu, W.-C., 2005. *Mobile Commerce Security and Payment Methods* C. Lee, W. Kou, & W.-C. Hu, eds., Idea Group Inc.
- Mark, H., 2007. People, Process and Technology. *Transaction World Magazine*, 6(9). Available at: <http://goo.gl/w5ZqX> [Accessed March 24, 2013].
- Marufu, A.M.C. & Sibanda, K., 2013a. An M-Commerce Security Framework for ICT4D Contexts. In R. Volkwyn, ed. *Southern Africa Telecommunication Networks and Applications Conference (SATNAC)*. Spier Wine Estate, Stellenbosch, Western Cape, South Africa, pp. 271–276.
- Marufu, A.M.C. & Sibanda, K., 2013b. Mobile Device Threats and Vulnerabilities as M-Commerce Enablers for Marginalised Communities : Siyakhula Living Lab. In *15th Annual Conference on World Wide Web Applications*. Cape Peninsula University of Technology: OpenJournals Publishing., pp. 1–14.
- Marufu, A.M.C., Sibanda, K. & Scott, M. S., 2013. Human Aspect in security of M-Commerce services in ICTD : A Siyakhula Living Lab Case Study. *International Journal of Computer Science Issues*, 10(5), pp.25–33. Available at: <http://goo.gl/8SwO7C>.
- Mathias, C.J., 2009. Mobile security threats. *Techtarget*. Available at: <http://goo.gl/JGsgIZ> [Accessed April 20, 2013].
- Maxim, M. & Pollino, D., 2002. *Wireless Security*, McGraw-Hill Professional.
- Mbaya, I.R., Science, M.O.F. & Science, C., 2007. Towards A Security Framework For The Semantic. , (November).
- McCown, C., 2008. Framework for Secure Application Design and Development: Foundation, Principles and Design Guidelines.
- Meng, J. & Ye, L., 2008. Secure Mobile Payment Model Based on WAP. *2008 4th International Conference on Wireless Communications Networking and Mobile Computing*, (March), pp.1–4. Available at: [http://ieeexplore.ieee.org/xpl/freeabs\\_all.jsp?arnumber=4680310](http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=4680310).
- Mennecke, B.E. & Strader, T.J., 2003. *Mobile Commerce: Technology, Theory and Applications* 1st ed., London: IDEA Group Publishing.
- Merwe, P.B. Van Der, 2003. *Mobile Commerce Over Gsm: A Banking Perspective On Security*. University of Pretoria.
- Miller, C., Mulliner, C. (2009). Fuzzing the Phone in your Phone. Black Hat USA 2009 Mobile
- Mouton, J., 2001. *How to succeed in you Master's and Doctoral Studies: A South African Guide and Resource Book* 1st ed. M. Hittge & A. Thorne, eds., Pretoria, South Africa: Publishers, Van Schaik.
- Muchenje, T., 2008. *Investigation of Security Issues on a Converged WiFi and WiMAX Wireless Network Master of Science Tonderai Muchenje*. University of Fort Hare.
- Mulhall, A., 2003. In the field: notes on observation in qualitative research. *Journal of advanced nursing*, 41(3), pp.306–13. Available at: <http://www.ncbi.nlm.nih.gov/pubmed/12581118>.
-

- 
- Networks, J., 2012. Security For The New Layered End-to-End Security Solutions for Mobile Network Operators. , 2012, pp.1–4.
- Networks, J., 2010. White Paper Mobile Security — Why The Time Is Now Mobile Carriers Must Implement Security Now to Protect the New Wave of Mobile.
- O'Brien, J., 2002. *Management Information Systems: Managing Information Technology in the E-Business Enterprise*, New York, NY, USA: Irwin Professional Pub.
- Olivier, M.S., 2004. *Information Technology Research: A practical guide for Computer Science and Informatics* 2nd ed., Pretoria, South Africa: Van Schaik Publishers.
- Osman, H. & Taylor, H., 2008. Towards a Reference Model for M-Commerce over Ad Hoc Wireless Networks. , pp.1–14.
- Pade, C. et al., 2009. *Siyakhula Living Lab -Baseline Study*, Available at: <http://goo.gl/JDOvvl>.
- Patil, J., 2008. *Information Security Framework: Case Study Of A Manufacturing Organization*. Mercy College.
- Ross, S.J. et al., 2011. Creating a Culture of Security ISACA and IT Governance Institute® (ITGI®) Affiliates and Sponsors, ed. , pp.1–251.
- Ruggiero, P. & Foote, J., 2011. *Cyber Threats to Mobile Phones*, US-CERT Resources.
- Saraydaryan, J., Benali, F. & Ubeda, S., 2009. Comprehensive Security Framework for Global Threads Analysis. *IJCSI International Journal of Computer Science Issues*, 2, pp.18–32.
- Savenye, W.C. & Robinson, R.S., 1996. Qualitative Research Issues And Methods : An Introduction For Educational Technologists. In pp. 1045–1072. Available at: <http://goo.gl/wfRT8p>.
- Sawyer, J., Eston, T. & Johnson, K., 2012. Smart Bombs: Mobile Vulnerability and Exploitation. Available at: <http://goo.gl/iaS0k> [Accessed November 20, 2012].
- Schlegel, R. et al., 2011. Soundcomber : A Stealthy and Context-Aware Sound Trojan for Smartphones. In *Proceedings of the 18th Annual Network and Distributed System Security Symposium (NDSS)*. NNDS, pp. 17–33. Available at: <http://goo.gl/gBNwJ>.
- Senior Scholars (2007) AIS Senior Scholars Forum Subcommittee on Journals: A baseket of six (or eight) A\* journals in Information Systems Archived at [<http://home.aisnet.org/associations/7499/files/SeniorScholarsLetter.pdf>.]
- Schwidorski-Grosche, S. & Knospe, H., 2002. Secure mobile commerce. *Electronics Communication Engineering Journal*, 14(5), p.228. Available at: <http://link.aip.org/link/ECEJE9/v14/i5/p228/s1&Agg=doi>.
- Sharma, R.K., Sharma, R. & Raj, S., 2011. Confronts And Issues In M-Commerce [ A Business On Mobile And Net Approach ]. , 4(1), pp.51–55.
- Singel, D. & Preneel, B., 2003. The Wireless Application Protocol ( WAP ) \*. , (September), pp.1–10.
- Siochruí, S.Ó. & Girard, B., 2005. *Community-based Networks and Innovative Technologies : New models to serve and empower the poor*,
- Slyke, C. Van & Belanger, F., 2002. *Introduction to electronic business technologies.*, New York, NY, USA: John Wiley & Sons, Ltd.
-

- 
- Sreenivasan, J. & Mara, U.T., 2010. A Conceptual Framework on Mobile Commerce Acceptance and Usage Among Malaysian Consumers : The Influence of Location , Privacy , Trust and Purchasing Power 2 Problem Statement. , 7(5), pp.661–670.
- Standards, S., 2008. UNIT 2 SECURITY FRAMEWORK. , pp.38–62.
- Summary, A.E., 2008. Boosting Economic Growth and Poverty Reduction ICT in Africa. *ICT in Africa*, (April 2008).
- Tam Vu, (2012), Anatomy of an Attack – Why You Need to Consider Security in the Cloud, Filed in Cloud Industry Insights Published on May 23rd, 2012 [<https://www.rackspace.com/blog/the-anatomy-of-an-attack-interactive/>]
- Team, U.-C.C.R., 2010. *Technical Information Paper-TIP-10-105-01 Cyber Threats to Mobile Devices*,
- Thomas, G.D.A., 2007. *A Framework for Secure Mobile Computing in Healthcare* by. Nelson Mandela Metropolitan University.
- Tiwari, R. & Buse, S., 2007. *The Mobile Commerce Prospects: A Strategic Analysis of Opportunities in the Banking Secotr*, Hamburg.
- Tsalgatidou, A. & Veijalainen, J., 2000. Mobile Electronic Commerce : Emerging Issues The Wireless Application Protocol ( WAP ). , pp.477–486.
- Tuff, D., 1985. Focus Group Research — Methods And Practices.
- Varshney, U. & Vetter, R.O.N., 2002. Mobile Commerce : Framework , Applications and Networking. , pp.185–198.
- Verma, P., 2011. Pentesting Mobile Applications. *ClubHack 2011 Hacking and Security Conference*. Available at: <http://goo.gl/ySGuQ> [Accessed November 20, 2012].
- ViaForensics, 2012. Santoku. Available at: <http://goo.gl/4fBBO> [Accessed December 20, 2012].
- von Bertalanffy, L.; General System Theory: Foundations, Development, Applications, George Braziller, 1976
- Wei, J., Liu, L.C. & Koong, K.S., 2006a. An onion ring framework for developing and assessing mobile commerce security. *Int. J. Mobile Communications*,, 4(2), pp.128–142.
- Wei, J., Liu, L.C. & Koong, K.S., 2006b. An onion ring framework for developing and assessing mobile commerce security. , 4(2), pp.128–142.
- Weidman, G., 2012. *Introducing the Smartphone Penetration Testing Framework*,
- West, D.M., 2013. Alleviating Poverty: Mobile Communications, Microfinance and Small Business Development Around the World. *Issues in Technology Innovation*, (May 2013), pp.1–12.
- World Wide worx, 2011. The Mobile Internet in South Africa. *Mobility 2011*.
- Yazdanifard, R., Sayed, M. & Elkhair, A., 2011. Mobile Commerce and Related Mobile Security Issues. , 9, pp.198–201.
- Yeh, J., Hu, W.-C. & Lee, C., 2009. Security Issues and Possible Countermeasures for a Mobile Agent Based M-Commerce Application. , pp.2614–2632.



---

Yusoff, A.Y. & Lim, S.Y.P., 2003. ICT FOR DEVELOPMENT ( ICT4D ) Understanding ICT4D Thematics in Malaysia : A Sourcebook. , (December).

Zaballos, A. et al., 2010. Testing Network Security Using OPNET. , pp.1–5.

Zefa, A.B., 2010. ICT for Development : sustainable technology-supported participatory development for poverty alleviation in the context of digital divides ICT for Development : sustainable technology-supported participatory development for poverty alleviation in the cont. , (2009), pp.1–35.

Zhang, R. & Hilton, T., 2012. The Characteristics and Technical Foundations of Mobile Commerce. *Issues in Information Systems*, 13(2), pp.394–396.

Zhang, Y. & Wildemuth, B.M., 2005. Unstructured Inrerviews. , (1998), pp.1–10.



University of Fort Hare  
*Together in Excellence*

---

## Appendices



## Appendix A: Case Study Setup

The case study was conducted in the Siyakhula Living Lab (SLL). The SLL communities are situated in and around the Dwesa Nature Reserve in the former Transkei of South Africa. The area is approximately 40km from the town of Willowvale in the Eastern Cape, along the Wild coast. It is very rural, with only dusty road networks, no running or plumbed water, only pit toilets, and limited (yet increasing) access to electricity. The Living Lab (LL) approach used in the SLL has and continues enabling effective innovation within the ICT4D space (Gumbo et al. 2012) which has inspired the choice of this study research area. The choice was also inspired by the idea that interaction with the rural communities is made easier as an existing platform for interaction is already in place. The SLL also enables the researchers to have a direct experience of the marginalised rural reality. This brings a crucial understanding of the rurality context to our work, allowing for a study that is relevant and well positioned to meet the M-Commerce security needs of the communities.

### Participants

Data was collected from mobile phone users within the Dwesa/Cwebe area. Participants constituted 77.27% females to 22.73% males (from the questionnaires). The field study consisted of three main stakeholders also referred as study participants i.e., students (age group between 16-25 and not working), community members (none teaching and mostly staying at home), teachers/educators (all age groups). Figure 0.1 shows a graph depicting the age distribution among the participants.

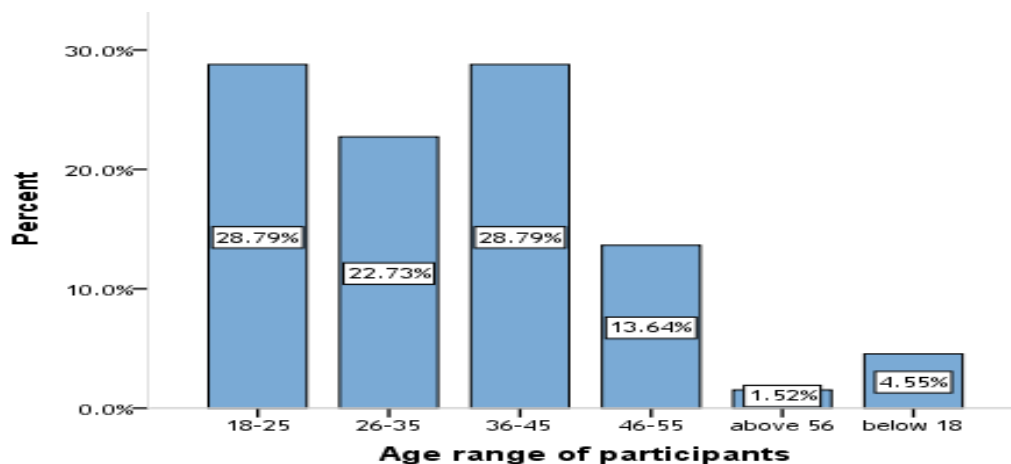


Figure 0.1: Study participants' age range demographics

Based on the responses to a few demographic questions it was possible to find certain differences among the participants. Figure 0.2 shows the classification of the participants with respect to their monthly income.

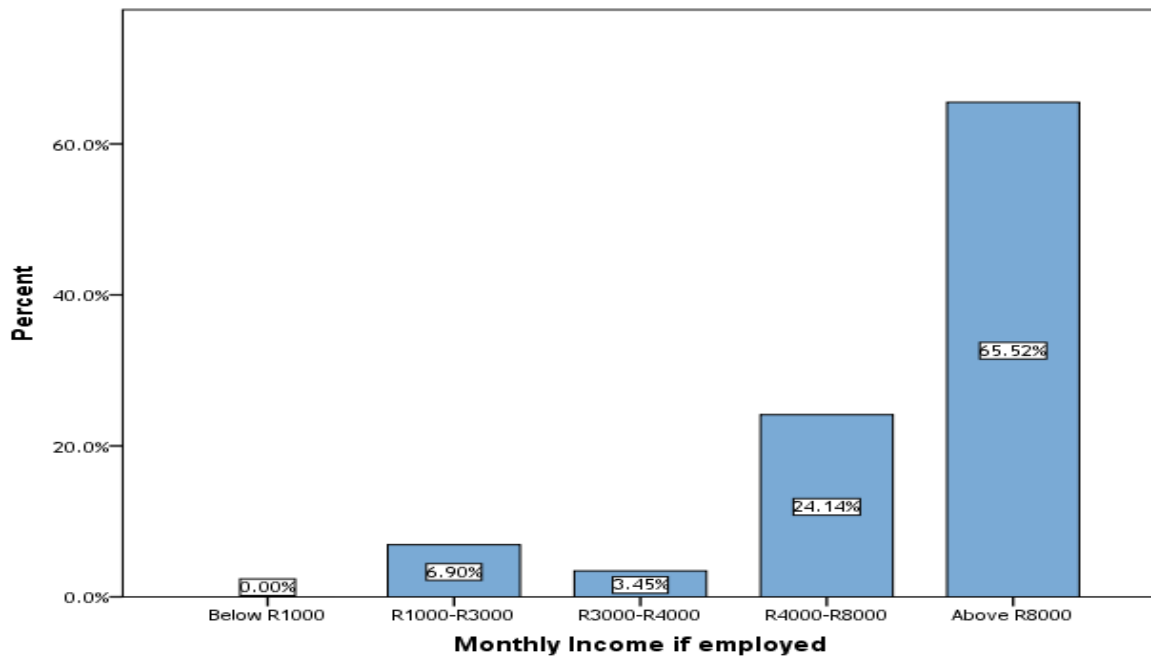


Figure 0.2: Distribution of monthly income of employed participants

The idea was to include participants from literacy training classes conducted by SLL at each of the two centres, as interaction was already established (between the researchers and the participants) during the training classes. There are basically two centres one at Ngwane and the other at Nqabara at which computer literacy training courses are held. Each class constituted at least a student, teacher or community member from schools affiliated to the Siyakhula Living Lab. Figure 0.3 of the Siyakhula Living Lab Network Map shows a visual presentation of the distribution of the centres in the Living Lab. Participants who converged at Nqabara would be those from Badi, Mevana, Kunene, and Nquba, while those at Ngwane where from Mpume, Nondobo, Ntubeni, Ngoma and Mtokwane.

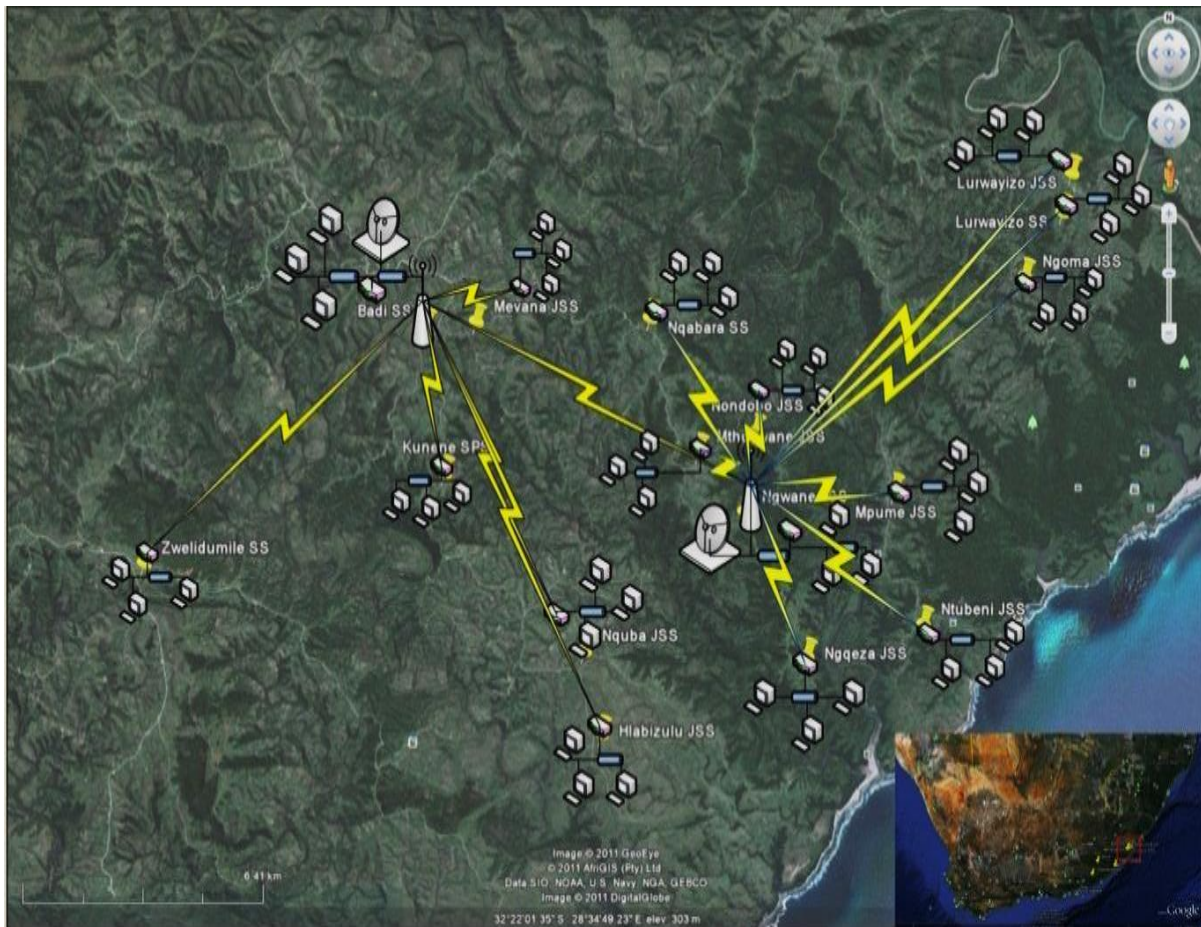


Figure 0.3: Siyakhula Living Lab Network Setup -Dwesa Area (<http://goo.gl/2pcSHL>)

## Instruments/ Methods

Under each phase (and subsequent level) a relevant set of instruments and method were used, depending on the type of data to be collected. This section describes the instruments that were employed to gather data at each of the four objectives.

This section discusses in detail the tools that have been mentioned in the previous section presenting 1) the background information to each tool/technique, 2) the type of information the tool was used to gather 3) the reason why the specific tool was used by referencing commonly known methodology experts and 4) the actual steps in which the required tool was used.

### *Observation Technique*

Not all qualitative data collection approaches require direct interaction with people. Observation is a technique that can be used when data collected through other means can be of limited value or is difficult to validate (Hancock, 1998). For example, in interviews participants may be asked about how they behave in certain situations but there is no guarantee that they actually do what they say they do (Mulhall, 2003).

Although an interview or questionnaire can be employed, the information that would have been obtained is what people thought was going on than what actually is going on. Through the Observation technique it was possible to ascertain whether what people say they do and what they actually do in reality match. More so, the Observation technique was used to 1) build rapport with informants, 2) provide a better platform to later cross-check information and possible differences between what people do and what they say they do, 3) get a better understanding of mobile device use in the ICT4D context 4) gain new insights or discover things that people may not wish to reveal in interviews, or may be not asked about in surveys and may not have thought of mentioning, 5) gather data on how the users interacted with their handheld devices and how security vulnerabilities may be introduced.

To facilitate the Observation technique some field notes, videos and photos/pictures were taken. Techniques employed for collecting data through Observation included:

*Written descriptions:* observations of people, and their interaction with their mobile devices were made. Notes were taken of these observations. Limitations of this are similar to those of trying to write down interview data as it occurs (Hancock, 1998). First there is a risk that the researcher will miss out on observations because he is writing about the last thing he noticed. Secondly, the researcher may find his attention focusing on a particular event or feature because they appear particularly interesting or relevant and miss things which are equally or more important but their importance is not recognised or acknowledged at the time.

*Video recording:* this freed the observers from the task of making notes at the time and allows events to be reviewed time after time. One disadvantage of video recording noted by (Hancock, 1998) is that the actors in the social world may be more conscious of the camera that they would be of a person and that their behaviour will be affected. They may even try to avoid being filmed. This problem can be lessened by having the camera placed in a fixed point rather than carried around. However, this means that only events in the line of the camera can be recorded limiting the range of possible observations. For this reason the use of

a camera was very minimal as we did not want a change mobile users behaviour and interaction with their mobile devices.

*Photographs:* Photographs are a good way of collecting observable data of phenomena which can be captured in a single shot or series of shots. For example, photographs of prevalent mobile devices among the participants were captured.

### *Focus groups*

A focus group is a qualitative data collection method in which one or two researchers and several participants meet as a group to discuss a given research topic (Freitas et al., 1998). These sessions are usually tape recorded, and sometimes videotaped. The moderator (one researcher) leads the discussion by engaging the participants to respond to open-ended type of questions – questions that require an in-depth response rather than a single phrase or word (Tuff, 1985; Freitas et al., 1998). Appendix H shows the picture display of the two focus groups carried out.

Focus groups were used in this aspect because 1) they yield a large amount of information over a relatively short period of time; 2) they are effective for accessing a broad range of views on our specific topic, as opposed to achieving group consensus, and 3) acts as an enabling tool in developing drafts of interviews and/or questionnaires 4) can be used effectively in conjunction with other qualitative methods. Group dynamics stimulate conversation and reactions. Within this research, focus groups are typically one method among many that were used to create a complete picture of how lack of enhancing M-Commerce systems affects a community of people. Use of focus groups contributes to this broad understanding by providing well-grounded data on mobile phone use, social norms, the pervasiveness of these norms within the community, and people's opinions about their own values over the M-Commerce environment.

The fundamental data collected by this technique were the transcripts of the group discussions and the moderator's reflections and annotations. Together with the Observations technique and the semi-structured questionnaires, the focus groups aided this preliminary research to ascertain human aspect as security loopholes, and even illuminated the results of other data obtained in a baseline study of the SLL on mobile device use (Pade et al., 2009)

In order to design a comprehensive focus group schedule some research documentation and papers on the area were read, and ideas and skills were developed to carry out the actual focus groups and collect data. One such document which offered a most comprehensive basic structure is the work of (Krueger, 2002).

### *Interviews*

Interviews are a widely used tool to access people's experiences and their inner perceptions, attitudes, and feelings of reality (Zhang & Wildemuth, 2001). Based on the degree of structuring, interviews can be divided into three categories: structured interviews, semi-structured interviews, and unstructured interviews (Fontana & Frey, 2001). In this section we will focus on semi-structured interviews and unstructured interviews as qualitative research methods for data collection.

Unstructured interviewing is recommended when the researcher has developed enough of an understanding of a setting and his or her topic of interest to have a clear agenda for the discussion with the informant, but still remains open to having his or her understanding of the area of inquiry open to revision by respondents (Cohen & Crabtree, 2006). Because these interviews are not highly structured and because the researcher's understanding is still evolving, it is helpful to anticipate the need to speak with informants on multiple occasions.

Development of rapport and dialogue is essential in unstructured interviews. Due to this reason voice recordings were done to avoid the problems considered in jotting notes.

The interview guide was developed iteratively - questions were developed, tested, and then refined based on what was learnt from the literature survey (e.g. on the SLL network setup information).

### *Questionnaires*

A questionnaire is a group or sequence of questions designed to elicit information from an informant or respondent when asked by an interviewer or completed unaided by the respondent (Savenye & Robinson, 1996). There are three types of questionnaires; unstructured, structured and semi structured questionnaires. An unstructured questionnaire is a tool used by an interviewer who engages with a participant, asking questions about a particular topic or issue. A guide of questions is created to direct the interview, where the specific questions and the sequence in which questions are asked are not precisely determined



in advance (Burgess 2001). A structured questionnaire, on the other hand, is one in which the questions asked are precisely decided in advance. When used as an interviewing method, the questions are asked exactly as they are written, in the same sequence, using the same style, for all interviews. Nonetheless, the structured questionnaire can sometimes be left a bit open for the interviewer to amend to suit a specific context. A semi structured questionnaire is a mix of unstructured and structured questionnaires. Some of the questions and their sequence are determined in advance, while others evolve as the interview proceeds.

The questionnaires were created from similar questionnaires that deal with similar topics following a literature survey for similar studies that have been conducted. In that way we avoided re-inventing the wheel. Hence the steps we adopted for developing our questionnaire were taken from (Burgess 2001; Eiselen et al. 2005)

After the field work, data from the questionnaires was processed, analysed, and presented in the form of a report in the work (Marufu et al. 2013). For analysis both dummy tables and software assisted-analysis using IBM's SPSS software program employed. The great advantage of using a computer lies in its ability to do several kinds of analysis in a relatively short time. An appropriate, useful and interesting way to present the obtained results in the form of graphs and tables can therefore be realised.



## Appendix B: M-Commerce Ecosystem within a Rural Setup

### Mobile Phone Ownership

Mobile phones are enablers of M-Commerce transacting. Results obtained from the empirical study confirmed what literature from various researchers had suggested (Dhir et al., 2012), (Pade et al. 2009) that mobile devices have managed to penetrate to even previously inaccessible marginalised rural areas. From the results obtained during a quantitative survey in this research work (Figure 0.4), 90.3% of the participants had mobile phones, 3.03% had two, while 6.06% had none. The data also indicated that the prevalent phones are feature phone Nokia phones (78.13%).

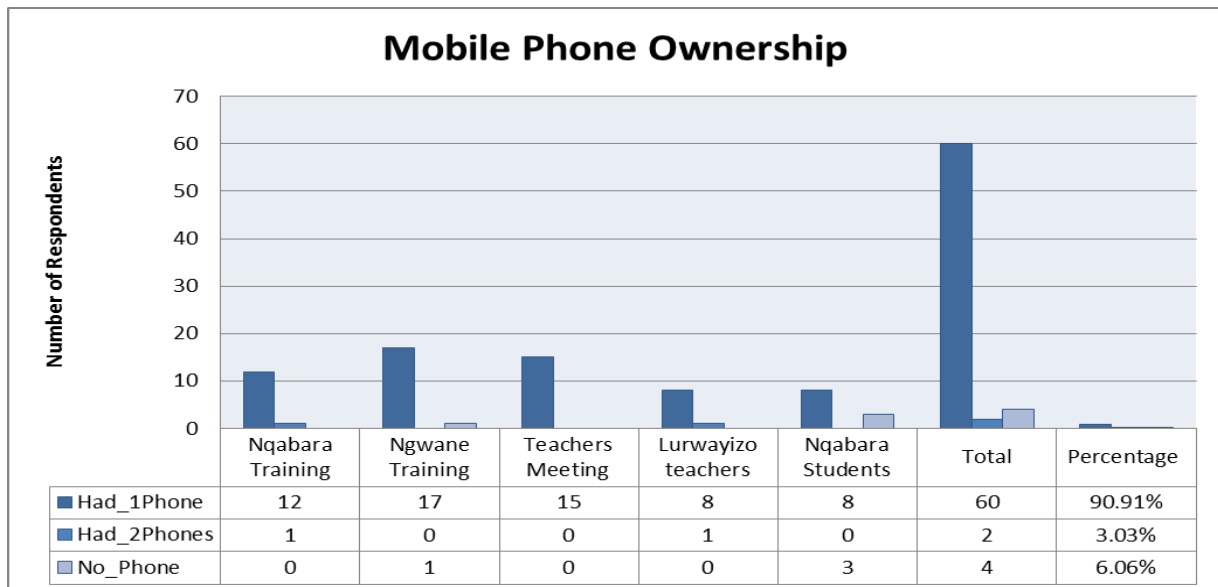


Figure 0.4: Mobile phone presence among the participants

In addition to the results depicted in Figure 0.5, Appendix G gives a visual display of the other mobile phone brands with smartphone capabilities that were also noted in the initial findings prior to the quantitative. Further enquiry indicated that affordability was the main reason for lack of mobile phones. However, although mobile phones are penetrating to MRAs, cost remains an important factor. Due to this reason, purchase of mobile phones would be based on their affordability over functionality aspects which include usability, security, encryption etc. This survey also shows an even distribution of ownership of mobile

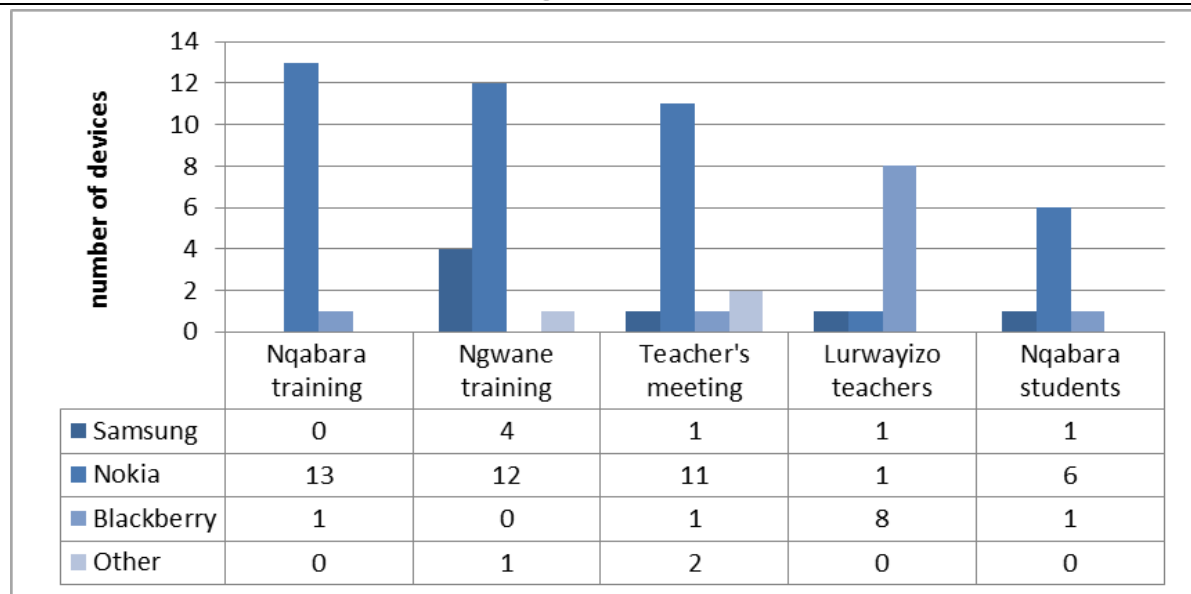


Figure 0.5: Mobile phone prevalence

devices across different age groups and occupations: students, educators and community members. Teachers prove to be the main pioneers of new technology.

According to Networks 2010; Marufu & Sibanda 2013b; the type of mobile phone has bearing on the type and level of security a device would present for the mobile transacting users. Table 6.1 presents a detailed account of the specific models of brands presented in Figure 0.4. Most of the devices presented are feature phones, not capable of providing critical security features (such as data encryption, remote wiping, strong authentication schemes, etc.) which render them as a possible weak link in the M-Commerce system chain described in Section 2.2. It should also be noted that the feature phones are less susceptible to the recent trend of malware affecting smartphones, which sets apart a rural context from a developed area. However with an increase in affordability of “smartphone-like” phones and the gradual phasing out of old technology, an influx of high end smartphone devices is inevitable to the rural areas in the near future. Observations displayed in Appendix G indicate signs of penetration of some high end phones, though to a lower extent.

Table 0.1: Mobile phone brand prevalence

Participants	Nokia Models	Samsung Models	BlackBerry Models	Other
Ngwane Training	X2,X1, Asha, C1,C2,E2120, 1616,1282,5130C	C2222, E250, GT B-3210	-	AG
Nqabara Training	C1,X2,RH-112, RM-614(C3)	-	Curve-8520	-
Lurwayizo Teachers	X2,X3,E63,E250, 7100	S5300	-	-
Nqabara Students	X2, Asha	GT-53653	9300	
Teachers Meeting	X2, 5310,	E250	Torch- 9800	MTN ztee MOBOT

### Obtaining a Mobile device

Results indicate that the participants acquired their devices from different sources. Apparently, majority of participants did not have the liberty to purchase the mobile phones themselves, which meant none of them had an option to assess the device (for security or functionality). Since most of these devices are inherited from a relative or close friend, a huge security concern is raised on whether this device will be safe for the new user to use in transacting over M-Commerce platforms. Considering how personal information, including financial information is being stored on the mobile devices, passing on of an old phone to a relative or friend may have some security concerns in this field of M-Commerce. Participants were asked who had bought the mobile phones they were using and the graph below shows their responses. With the introduction of technology it is also possible that an intentional malware infected device is sold by an attacker with the intention of later retrieving financial information from the victim.

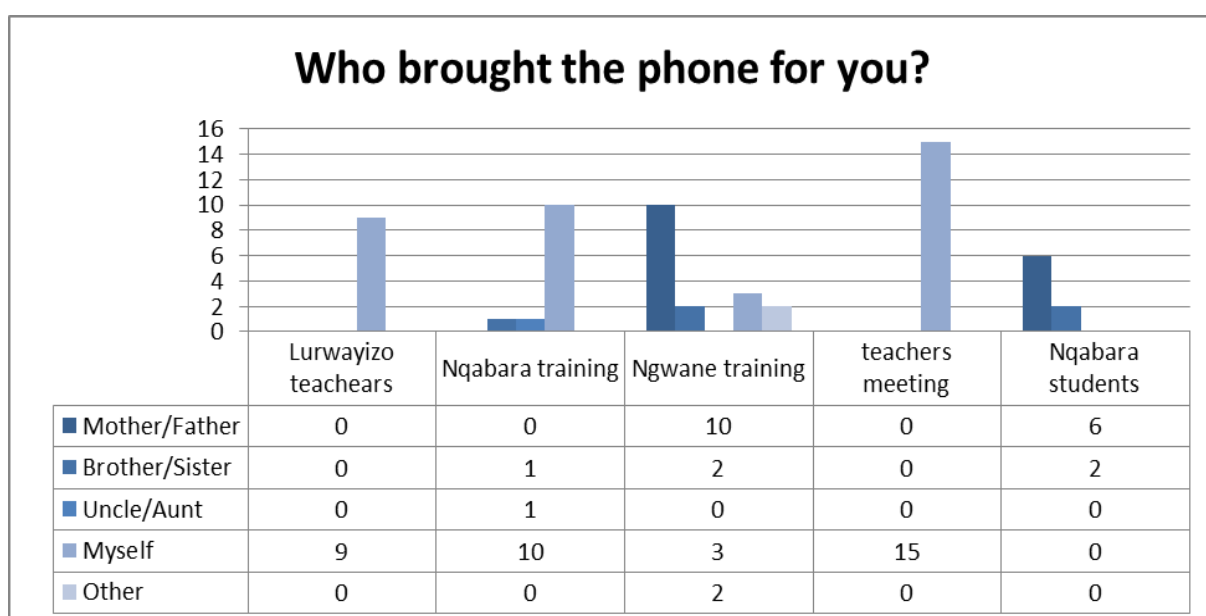


Figure 0.6: Sources of devices the participants are using

A follow up question was asked to the participants to understand if the mobile phone they had was a new device or a second hand acquisition. The graphs below show 86% of the participants obtained a new device while 14% got a second-hand device. An interpretation of this observation is the likelihood of security being compromised through the passing on of a mobile device or purchasing a “second hand” device is minimal. Although minimal efforts should still be made to eradicate the chances of an old device having malware passed on to elicit financial and personal data from recipient.

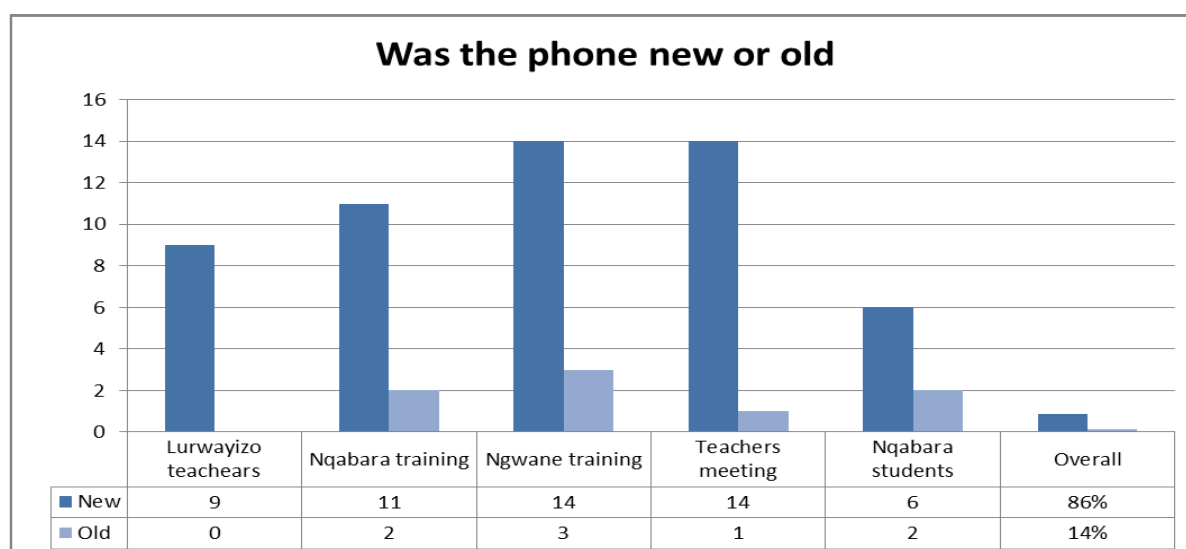


Figure 0.7: The state of phone on first use by participants

## Mobile device as storage device

More so, it was also noted how mobile phones are used as storage devices in most instances in marginalised rural areas. This can have serious repercussions on the M-Commerce systems considering the stored data includes sensitive user banking username and PIN codes in stored memory. When the participants were asked through a questionnaire where they stored their mobile files (pictures, videos, contacts, etc.) from selected options: SD card, Phone memory, Laptop, Desktop, USB, Elsewhere. Figure 0.8 below shows their responses. Graph shows majority of the participants store their files and data in the mobile phone and SD card respectively.

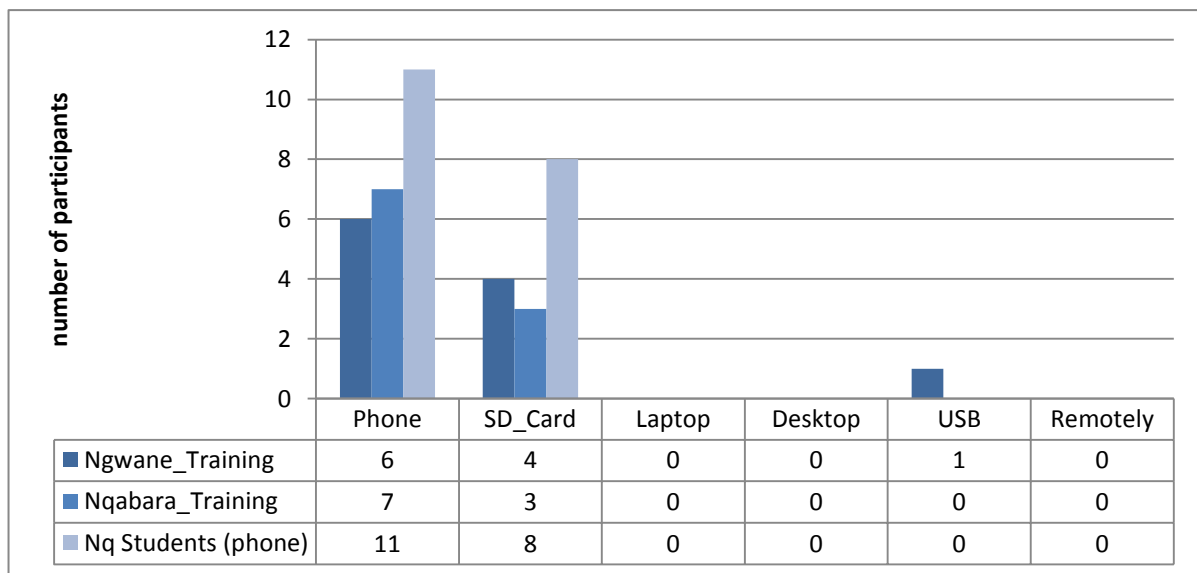


Figure 0.8: Where users store most of their data

A focus group that was carried out prior to issuing out the Questionnaire confirmed what was obtained by the follow up questionnaire.

## Services accessed with mobile phones

Figure 0.9 shows the services that the participants made use of on their mobile devices. Some participants were not sure of the existence/ absence of some of these features on their devices. The type of service accessed by the user using the mobile phone has a great chance of introducing some vulnerability to the user personal financial information.

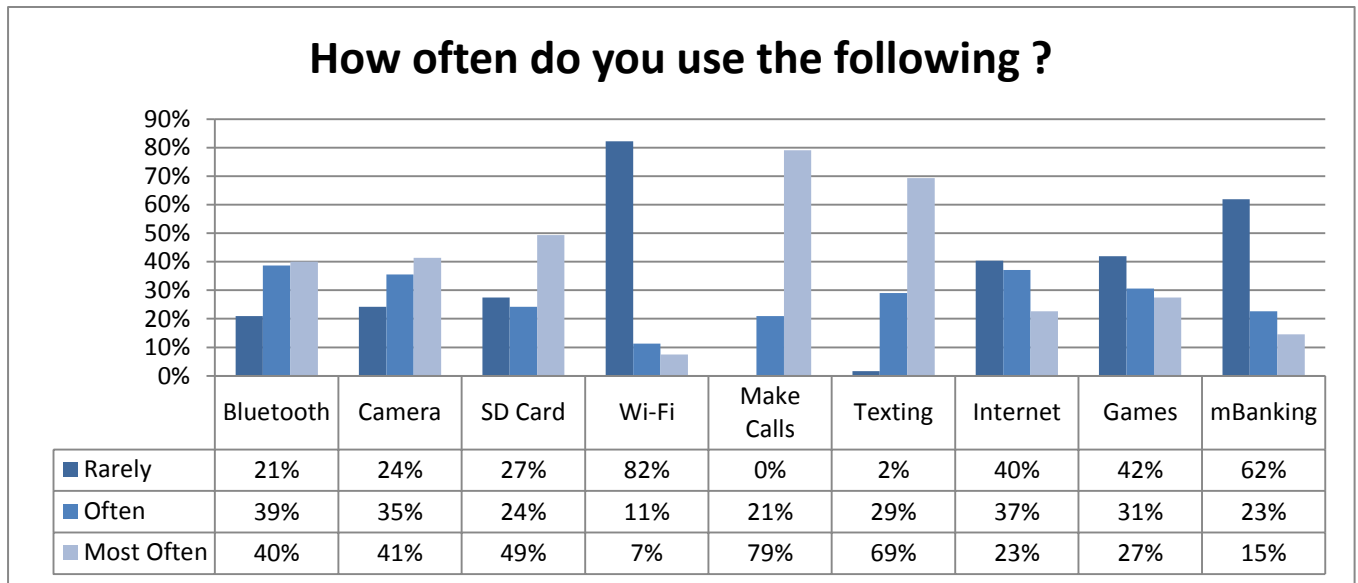


Figure 0.9: Mobile phone usage by participants

Mobile usage by the participants indicated that Wi-Fi, Internet, Games and M-Banking are the most rarely used services with percentages of 82%, 40%, 42% and 62%. This can be attributed to the types of mobile phones that there are available to the participants. The devices are low end, which means they are not capable of offering or processing the aforementioned services. The most used features on the mobile phones were noted to be: making calls, texting, SD memory use, camera and Bluetooth respectively.

*Mobile device storage:* mobile phones are used as a backup and data storage device for pictures, music, personal documents, etc. As a result the majority of the community members use mobile phones with SD card slot as a removable storage devices, introducing a potential vector malware can be distributed from mobile device to mobile device through desktops. If an attacker can leverage such a situation, they can execute an effective malware that has capability to spread effectively and also elicit data from a wide array of mobile devices.

*Bluetooth:* sharing of media files through Bluetooth was widely noted during Observations. Likewise, in the survey 79% (39% often and 40% most often respectively) of participants indicated that they often used mobile phones, while 21% rarely used it. The reason behind rare use can be attributed to unavailability of Bluetooth services on the mobile phones. Overall, a malware that can be developed and target the Bluetooth channel for its propagation and effective distribution (e.g. botnet-like malwares) may have serious repercussions on the M-Commerce ecosystem within a rural setup. Moreover, Bluetooth use in this rural setup is

not necessarily different from the use in developed places, but is worthwhile noting within the security framework developed in this research study.

*Wi-Fi:* Most of the mobile phones that were prevalent were incapable to make use of Wi-Fi provided by the Network providers and SLL Network to allow mobile transacting. Due to that reason, this of lack of capability to connect to Wi-Fi resources reduces the number of M-Commerce channels that are currently available to the rural community. Likewise the M-Commerce ecosystem can be noted as less susceptible currently to network targeting malware or threats. However a threat mitigation framework being proposed in this research should provision for these types of threats, as further penetration of smartphone devices to rural areas in the near future may make the threat a reality.

*Texting and Calling:* text and voice data mining sensory malware have gained substantial popularity in recent research. Although texting and calling are the most common activities users make use of, it would be difficult for malwares to cause a great risk to these channels, because of the low computation capability of most of the current devices. This leaves social engineering as an effective channel bearing serious connotations on security surrounding the M-Commerce ecosystem. Hence there is need to address this in the proposed framework.

*Internet access:* survey showed how the internet was fast becoming part of the participants' lives. Likewise as was established by (Grobler et al. 2011) that accessing internet using mobile phones comes with the same consequences as using a computer or a laptop; it is therefore necessary that users are advised to apply all basic safe surfing best practices on mobile phones as well. The proposed framework inspires the provision of deliverables that seek to address these issues.

Overall, although the results indicate a significant change in mobile phone usage, rural users remain unaware of the extra resources a mobile phone can provide, such as, access to government information, banking services, and Internet access. Hackers and attackers may leverage on this lack of knowledge and expertise to perform a widespread attack on mobile phone platforms in the future. Together with the arguments raised in this subsection it is necessary to develop a security framework that will help protect marginalised rural community users when transacting with such a volatile M-Commerce environment.



## Trust of M-Commerce Systems

Participants were asked if they trusted using the following M-Commerce services: M-Banking, M-Payment, Buying Airtime and Cloud based services (Figure 0.10)

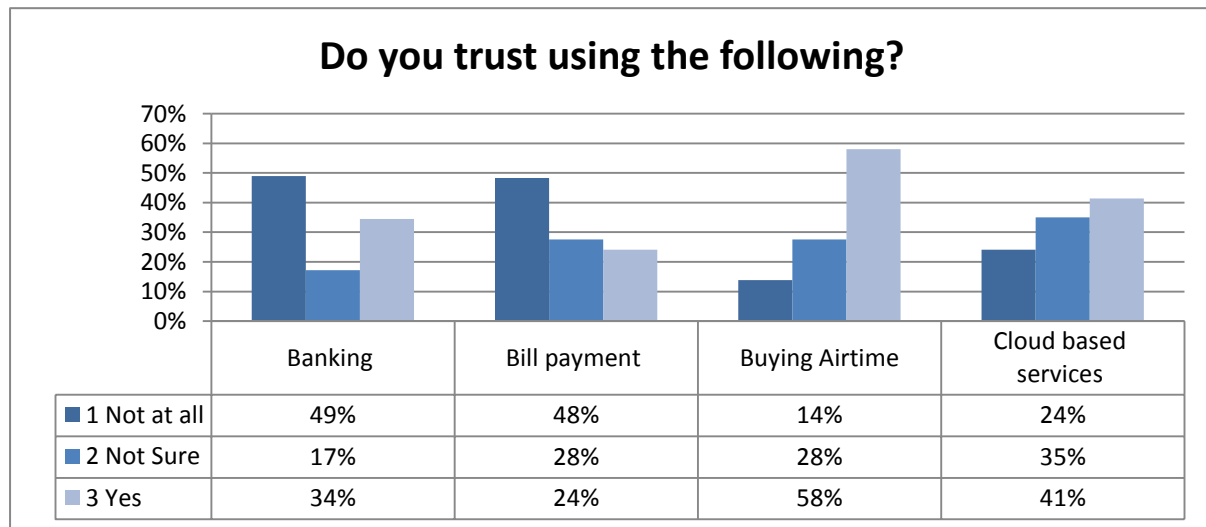


Figure 0.10: User trust levels towards use of mobile services

Bill payment was the list popular M-Commerce transacting on the list including M-Banking, airtime purchases and cloud based services. Airtime Buying was the most popular form of M-transacting with 58% confirming carrying it out. The main reason was that the transaction involved relatively less amounts of money. A considerable percentage; 49% and 48% of participants confirmed they did not use banking and bill payment respectively. Further enquiries showed that users were unaware of these services. In a case where the participants understood the service, their choice not to use the platform was attributed to lack of trust in the platform. Indeed trust is a huge factor in adoption of ICTs like M-Commerce. M-commerce transactions are often characterised by complex technology, anonymous vendors, lack of transparency and convoluted interactions between stakeholders. Trust becomes more important in situations of increased uncertainty in M-Commerce. Trust is a big issue and if these systems are going to be adopted, some major breakthrough is required to make sure trust with the systems is established. Security threats must not therefore leave room for doubt to users of M-Commerce products. Focus group carried out prior to the questionnaires indicated how users were confident with carrying out M-Commerce only for small amounts of money. Since trust issues relate in depth to security, our work emphasises on the strengthening M-Commerce security environment in an attempt to improve adoptability.

## **Siyakhula Living Lab Network Setup**

Siyakhula Living Lab (SLL) network is a community-wide broadband network that connects a number of distributed access networks (DANs), housed on school properties, within the various communities it operates. The entire network spans approximately 20 square kilometres and uses WiMAX technologies from Alvarion to share/distribute Internet access (via VSAT solutions from Telkom and Internet Solutions) as well as other services such as VoIP and shared local web content (for the purposes of education mainly, but with a view to increasing local services to other areas too, such as Health, Commerce and Governance). Internet access in the SLL is provided through the use of VSAT technologies. Via the broadband islands deployed in the SLL, communities have access to various services such as email, VoIP, the Internet and the TeleWeaver multi-service platform. In order to support the SLL's objectives and provide the community with access to ICTs, a local loop access network (creation of two interconnected broadband islands) was deployed to the Dwesa-Cwebe area. WiMAX technologies were used to build the local loop while VSAT technology is used to link the communities to the Internet. This setup creates a valuable channel for marginalised users to engage in M-Commerce through the network facility. Security of SLL network is thereby noted to be important in this research as compromise of the network security may hinder transacting by marginalised communities using it for M-Commerce transacting.

There are two VSAT service providers present in the SLL network. One of the VSAT units binds to a real world IP address space, thereby allowing connection to core router at Ngwane from outside of the SLL network. The VSAT unit at Badi does not bind any real world IP space, hence is not accessible from the outside of the network unless an SSH tunnel is created. Currently this has not been done, but is possible. Hence currently only access to the Ngwane router is possible, allowing the network administrator to perform maintenance to the core router or the Edubuntu servers or other servers running within the LAN at Ngwane. Likewise, if an attacker gains access to the Ngwane router through the VSAT unit binding a real world IP, serious security breaches may be encountered.

There are two BreezeMAX micro base stations, one at Ngwane and the other at Badi. The choice for these sites to house the base stations was due to their geographical proximity. More so, the WiMAX base station at Ngwane is a Mobile WiMAX unit (802.16e), which

means the unit is capable of handling true mobility rather than just nomadic users. However, there is no true mobility as yet, as there is an omni-directional antenna. For true mobility to be realised there is need for at least two sector antennas to do hand-over (which is the definition of true mobility). True mobility can be a beneficial feature to M-Commerce transactions over this infrastructure. To note is also this increase in mobility capabilities is proportional to security issues the network system may face. A Fixed WiMAX unit (802.16d) base station is present in Badi. This base station is the old base station that was housed at Ngwane before SAAB Grintek sponsored the expansion. This base station is not capable of mobility; although nomadic users are possible. This unit is suited to fixed wireless installations and much easier to configure. It can be done via the AlvariStar software or via a telnet session making remote configuration possible. However, since there is currently no remote access to the Badi School it is not possible to have remote access. Basically with respect to security, gaining access remotely to the Badi base stations may be a difficult task for an attacker.

Hence the two WiMAX base stations work in a Point to Multi-Point configuration. Meaning that they both have omni-directional antennas and the signal radiates out at 360 degrees uniformly. The schools that are then able to see their nearest base station connect to that base station using what are known as Customer Premises Equipment (CPE). With the new mobile base station the CPEs are wireless routers, with the old base station the CPE are wireless bridges and require the installation of separate routers in order to allow the school computers and even mobile phones to connect to the network.

The schools connected to Ngwane have CPEs which behave as wireless routers. However, because of their design they do not allow traffic from the outside to pass through into the LAN at the school. This means that remote access to those schools' internal servers is not possible. IP forwarding is possible; but the available CPEs do not implement standard IP forwarding. Therefore, if IP forwarding is enabled on the CPE, the school's servers linked to that CPE will no longer be accessible remotely. CPEs at the schools which connect to Badi are an older generation of CPEs, hence there are not able to run as wireless routers, why they operate as bridges. Likewise, due to this reason there have separate routers behind the bridges at each school. Mikrotek 750G RBs are currently being used.

The above mentioned security issues are explored more in detail later on in this chapter. The following section shall also dissect the second part of the network from the telecom fraternity.

### **Telecommunications Networks**

There are no fixed line telecommunications infrastructures in the area at all, but there is relatively decent GSM coverage with 3G access in places (Pade et al. 2009). Cellphones are the most common modern ICT used in rural areas and they appear to have increased in availability in the last two to three years, as only a few people owned cellphones four years ago (Marufu & Sibanda, 2013b). A variety of factors influence the choice of network (Vodacom, Cell C, MTN) for cellphones quite apart from connectivity and coverage (for instance, most people use MTN rather than Vodacom, which has better connectivity through the Vodacom network tower in Mpume). These factors include word of mouth, peer influence, and the cost of the package.

Cellphones are the prevailing modern ICT in rural areas, and so they are targeted by our study as a tool that could support development there (a view generally shared by other researchers in the field of ICT for development). However, even though cellphone use has soared and proved its worth in developing countries, network providers often appear sceptical about rollout in rural areas (Siochrú & Girard, 2005). They do serve some rural areas, but ‘coverage does not necessarily mean access to poorer sections of the community.

The baseline study of the same area revealed that most local owners of mobile phones used the MTN network (58%), with the rest on Vodacom (40%) except for one person on a third network, Cell C. This obviously has changed over the years with the growth of other network providers like Cell C. MTN was preferred even though the Vodacom network tower was built within Mpume, giving a better signal; but the Vodacom tower suffered from frequent electrical blackouts. Figure 0.11 shows a range of factors influencing the choice of network in Mpume where network coverage was the greatest factor.

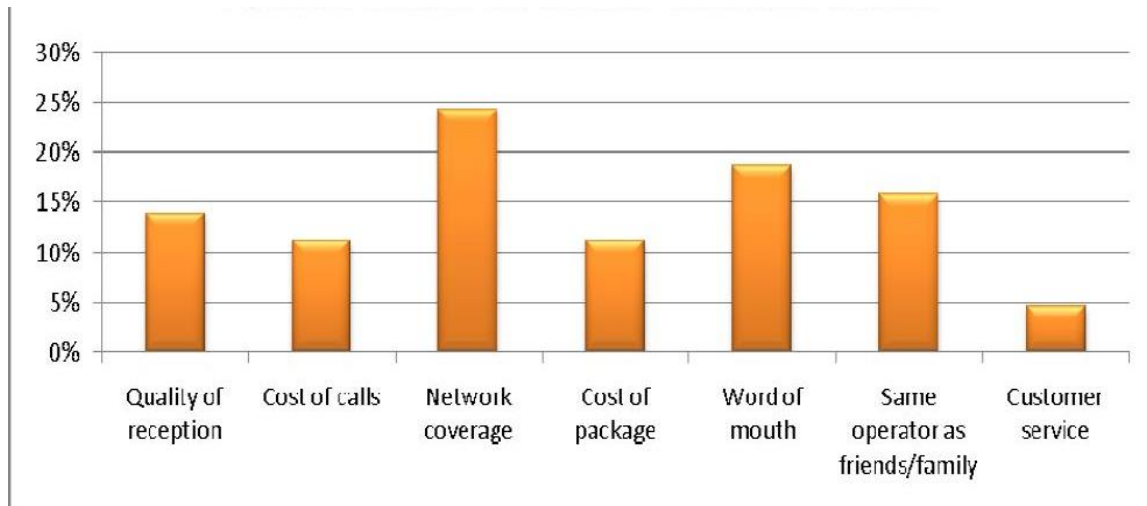


Figure 0.11: Factors influencing network choice (Pade et al 2009))

The type of Network infrastructure that is deployed also affects the issue of security. Most telecom service providers have GSM and EDGE as common infrastructures in those places. The main thrust of the framework should address these network infrastructures. Not much work shall be done on investigating security threats, but literature and standard recommendations shall be made as the framework also addresses M-Commerce platforms running over these networks.

## **Appendix C: Threat and Vulnerability Assessment**

### **Threats and vulnerabilities associated with the human aspect/user interaction with mobile device**

As noted in the Chapter 2, serious security issues can be realised from the way users as human beings interact with each other and with the mobile phones within an M-Commerce transaction. We sort to analyse the different security vulnerabilities introduced by the human aspect. Data to be collected in the scope of highlighting the human aspect in compromising M-Commerce systems security included; 1) the day to day use of the handheld devices which may introduce some vulnerabilities; from general internet use, transacting, sharing of the device with other users, taking the device for repairs and use of PIN/passwords; 2) the security measures the users employ to protect valuable information on the device from being stolen, lost or misused; 3) social aspects that may undermine the security which include and are not limited to social engineering, identity theft, twin evil attacks and literacy issues.

To collect the data to address the intensions in this objective a mixture of a set of qualitative measures and quantitative tools such as contextual inquiry, participant observation, focus groups and questionnaires were used. The participants (as described in the Sample section) were from the literacy training classes from the SLL. First the human aspects were noted using Observation technique. This was followed by focus group set up in the two SLL literacy training centres. Thereafter, an initial pilot study was carried out with one group of trainees and the two centres conducting literacy training. After a pilot study, the necessary changes and reviews were made to the instruments before the actual data collection was done on another group of participants.

As part of the results we managed to show the human aspect security loopholes. Main themes were noted in the focus groups. Table below shows the mapping of the themes in the focus groups to the elements of security adopted in this research.

Table 0.2: Focus group themes mapping to elements of security

Systems Security	Confidentiality	Integrity	Availability	Non repudiation	Authentication
Theft/Loss of Device	X				X
Mobile Device Repairs	X	X	X		X
Device Sharing	X				X
Password and PIN Use	X	X			X
Internet and Safety					
Transacting via M-Commerce	X	X	X	X	X

It was noted that mobile device loss was a norm especially for users travelling a lot with public transport. More so, users' practices also add to the reasons of the device loss or theft. For instance during the literacy training classes held in the Dwesa SLL (where data was collected) a considerable number of mobile devices were placed on the work benches, with little attention, which suggested that the environment may have been more trusted. This trust may be abused and used by perpetrators to obtain the devices and pursue their agenda. Another major security issue that was noted was the lack of user awareness in mobile phone use. For example a number of the participants did not know whether their devices had a PIN or password facility or not. The typical user is not aware that their actions have security implications. Recalling the PIN/password for user authentication on the mobile phone was an evident challenge; users end up not equipping their mobile phones with any of the authentication mechanism. To navigate away from such a problem users resort to using their date of birth, sibling's name, or even ID numbers. These practices may leave the users greatly exposed, as most perpetrators of cyber-crimes are aware that users make use of their personal information for their password. It was learnt that when users face mobile phone malfunction, these devices are taken to repairmen in the nearest towns or cities. When devices are taken for repairs, they are usually left behind with the repairmen. If a device is left in the custody of bogus repairmen, personal and important details on the device may be compromised. Data is elicited through installations of applications like Soundminer that listens for sensitive data on the phone and post it to the perpetrator. Data elicitation through some open source tools like MOBILedit! Forensic, EnCase, FTK, Cellebrite and Sleuthkit is also possible. We observed Collectivist cultural norms -were sharing of mobile devices was common, and perceptions that mobile devices can be used to store personal data and that no-one else will make use of

or retrieve that data. In addition, a considerable number of participants, who shared devices did not employ the use of a password, thereby presenting a great security concern in cases where the trusted party decides to abuse the trust.

Additional interesting findings on how marginalised users expose themselves to security risks within the M-Commerce ecosystem can be obtained in (Marufu & Sibanda, 2013). The M-Commerce security obviously has less focus on the end user human aspect, evident by user unawareness.

### **Threats and vulnerabilities associated with the handheld devices**

This objective required analysis of security vulnerabilities on the mobile devices as main enablers for M-Commerce. Data to be gathered on how handheld devices compromise M-Commerce systems security included: 1) a background on the type of devices in such areas 2) mobile devices operating systems' security/ vulnerabilities; 4) devices' current security mechanisms to protect user data 6) Use of Mobile Antivirus Solutions (is use of antiviruses an efficient way to protect MRA users), usability, OS platform of residence, availability to rural users.

In a baseline study that was carried out (Pade et al. 2009) in the same study area, information about the mobile phones in use was made available. However, in order to carry out an informed research, current data on devices in use was gathered through Observation technique, and use of questionnaires to obtain validating data.

Literature review was performed to ascertain the security vulnerabilities that are prevalent on mobile phones as M-Commerce enablers. In this section we looked at data storage and protection, user authentication, supporting technologies use (Bluetooth, Wi-Fi), Software App's as areas affecting mobile phone security. A deep analysis of Malware and Applications are beyond the scope of this section as they fall under Level III section of the framework.

An in-depth analysis through literature review was carried out to ascertain how the principles of security are undermined by the handheld devices in use and how they can be mitigated. Potential risks presented by mobile phones as M-Commerce enablers are presented in the results section and a discussion of channels data can be elicited from devices was noted in a published article linked to this research. Recommendations of an ideal M-Commerce "fit" device are made after considering the characteristics a typical device is to have.



It was noted that the “Device” and the “Human Aspect” components of Threat/Vulnerability levels in the ICTMS framework are difficult to clearly separate as the human aspect is still in play. More so considering how there is a presence of many vendors creating mobile devices it is difficult to carry out a threat/vulnerability analysis. However, by mixed method approach, an array of channels through which data can be elicited from handheld devices in marginalised communities thereby compromising the M-Commerce platform, was noted.

The common type of devices that were observed were low end devices (feature phones). This means, the current types of devices in such marginalised areas are not capable of providing demanding security features like data encryption, remote tracking, device wiping, and antivirus installations among others. Although that may be the situation, low end devices are less susceptible to other security risks like malware (which mainly target smartphone). However, security of these low end devices is still a necessity.

Theft and loss of unencrypted devices or devices without a password was noticed as the greatest vector to data loss on the device. More so, participants’ mobile phones had a number of built-in configuration settings and security features that often went unused due to user unawareness. Hence, we established that, understanding and taking full advantage of the facilities offered by these mobile phones is an important step towards establishing a comprehensive set of security safeguards.

Poor authentication schemes, which provide a hindering factor to users securing their devices was also acknowledged. This is coupled with low literacy and ignorance among the users. Overall, authentication practices are not a norm among the rural users, as they are seen as an irritating feature to ease of use. In addition, we learnt that users shared their mobile phones regularly. Although mobile sharing will not be an effective vector for penetration to mobile phone data elicitation, it pointed an interesting observation. We noted development of mobile device which allows mobile sharing through individual login platform could be a solution to the problem of sharing of device containing sensitive information.

Bluetooth use was common on most mobile phones. It can be noted that after simple Bluetooth sniffing techniques were run 78% of the devices with Bluetooth functionality where not regularly turned off or had a default password on them. We managed, with the owner’s permission to control the devices using Bluesnarf. These discoveries and more that were made at this level are presented in our related paper (Marufu & Sibanda 2013b). The same article also presents a detailed discussion on the above summarised ways in which

personal data and financial information can be elicited from handheld devices when rural marginalised users are transacting.

### Threats and vulnerabilities on M-Commerce access channel

In this section analysis of security vulnerabilities on the main channels through which M-Commerce platforms are being access was carried out. Hence initially an enquiry was made on the prevalent channels currently in use by communities in the SLL. Literature Review as well as a mixture of qualitative techniques (focus groups) and quantitative techniques was employed to gather this data. This initial enquiry resulted in a choice to focus on four channels of access: SMS, USSD, Web-based applications and Mobile based applications. Access to carry out a detailed security assessment of some of these channels is restricted, which narrowed most findings and analysis to be based on literature surveys and informal enquiries. Hence literature survey was carried out on all the above listed channels.

The major M-Commerce enabling channels of access that were noted are SMS, USSD, Mobile App and web app. The minority of rural users participate in M-Commerce transacting using mobile apps. Main logical reason derived was the types of mobile phones prevalent in such an area are low end feature phones, incapable of running additional third party applications. This phenomenon enables this research to infer that this channel would have low chances of being used by attackers to solicit users' personal and financial details.

Social engineering is a serious channel though which M-Commerce users can be manipulated to give away their personal details and Participants were asked how often they received calls or SMS's asking them to confirm/send in their personal details. Figure 0.12 shows a graph with their responses.

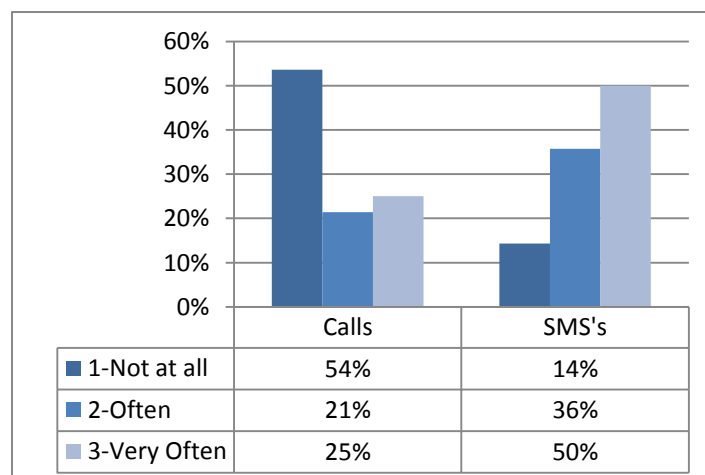


Figure 0.12: Frequency participants received spam

Evidently participants confirmed that they receive spam calls and SMSs often. A follow up question was asked to the participants to enquire if they confirmed to any of the above requests.

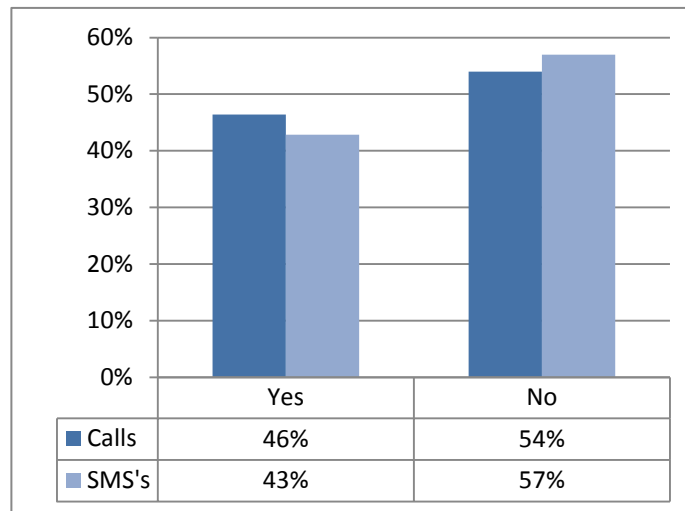


Figure 0.13: Frequency participants responded to the spam calls or SMSs

Figure 0.13 shows that majority of the participants, (54% and 57% respectively) did not respond to the calls or SMSs they received on their devices.

### **Threats and Vulnerabilities in the network access technologies enabling M-Commerce**

Literature survey, desktop surveys and data scrapping techniques were carried out to find which networks are in place for M-Commerce transacting by rural users. Emphasis therefore put on the network technologies and infrastructure under the SLL and three main network service providers.

Second assessment in this section was focused on discovering the security issues prevalent on the above mentioned network systems over which M-Commerce transacting are evident. For the mobile networks literature and desktop survey were carried out to find out various ways in which security of the access mobile network technologies may be compromised. A semi-structured questionnaire was prepared and put through to the SLL network administrator and a WiMAX specialist at Saab Grientek.

A detailed and critical literature survey on the overview and comparison of the Wi-Fi and WiMAX wireless (access network technologies employed in the SLL) was presented as

background knowledge and understanding into converged wireless network. Each of these two networks was then analysed in terms of both strength and weakness in their security implementations.

To identify the threats/vulnerabilities present within the network infrastructure in use by the community members within the Dwesa Siyakhula Lab enquiries through interviews to the network administrator, Ingrid was carried out. Initial question was posed to ascertain if M-Commerce transacting could be supported by the current structure and what the drawbacks would be. Ingrid indicated that M-Commerce transacting was possible, but it had more to do with the type of mobile device the rural community users of Dwesa had than the network infrastructure. She iterated that no-one in Dwesa has WiMAX enabled mobile phones hence access in that view is currently impossible. On a broader view, there are not many WiMAX enabled phones available in South Africa at all. However if the network access is through the Wi-Fi hot spots, she responded that it is possible to conduct an M-Commerce transaction, provided, the community users have a Wi-Fi enabled cellphone. Ingrid suspected that there are not many smart phones in Dwesa and that there will be a far greater number of S40 phones which are not Wi-Fi enabled, which was in alignment to the survey results presented in Section 5.1.

The aforementioned suggestions by (Muchenje, 2008) were not implemented in the expanded network. When asked if there were any measures were being implemented in the SLL, Ingrid indicated that a PPPoE network on top of the wireless network connecting all the schools used to be run, but the installation of the new Mobile WiMAX base station during the SLL network upgrade made that complicated to do. Furthermore, none of the students seemed to understand PPPoE, making it more complicated for them to work with the network. The old WiMAX base station at Badi could implement the original PPPoE that was used when it was at Ngwane, but, again there would be need for the network users to understand PPPoE. Thus, in order to promote ease of use of network resources by users, it was ideal not to implement it. What this implies for the current network system is that the security issues unearthed on the previous network system in a work by (Muchenje, 2008) are still present. Ingrid also confirmed our suspicion that when the SLL network was upgraded, not much security considerations were taken into perspective. She was also asked about any other specific security measures that were being employed on the SLL network. It was learnt that not much security is being implemented, although there is a possibility to setup an AAA Radius server

with the WiMAX base station. According to Jaco van Zyl from Grintek WiMAX does not work well with the open source radius server, FreeRadius. He said it would need to be worked on and possibly it would make a good Masters project to try and implement FreeRadius with the WiMAX network in order to add proper authentication into the network. In terms of WiMAX security, the network administrator also reported that the only main security measure that is prevented is rogue WiMAX CPE joining the network. This is done by only allowing known CPE MAC addresses to receive IP space in the network. So if an attacker is to setup their own WiMAX CPE and try to connect to the network, it will fail as the CPE would not be assigned an IP address as the MAC address of the device would be unknown. Also, the routes in the network statically configured, therefore traffic would not be able to flow to or from the rogue CPE. General impression noted was that security is not much of a serious issue in network infrastructures in such a rural place. Moreover, the initial literature survey indicated that the VSAT unit at Ngwane binds real world IP address space which allows connection to core router at Ngwane from outside of the SLL network. Ingrid was asked if there was a chance that this could be a point of entry by a hacker (if the system was supporting M-Commerce transaction on a regular basis). She confirmed that this could be a point of entry, but the attacker would first have to know the IP address (which is not published it anywhere). Then they would need to know at least one of the user names of people who have an account on that core router. Once they find out a user name (which is difficult to do) they would then have to implement brute force attacks in order to attempt to guess their passwords. Ingrid concluded that with Root SSH access disallowed on the core router, hacking in to this core router is technically doable but it's a non-trivial exercise. A general impression that noted is that security is not considered in rural marginalised setups as a serious issue. Some arguments about this issue are discussed in the framework chapter.

A port scan was carried out to confirm the types of threat/vulnerability that the network components could face. After running Net scan Android vulnerability scanner from a Mobile device: 12 addresses where found (12.6 seconds) The following table shows the discovered devices in the IP range of 192.168.2.1 – 192.168.2.254: Opened ports, port numbers and vulnerability.



Table 0.3: Presence of open ports within the Ngwane base station

IP address	Presence of Opened Ports	Opened Port Numbers
192.168.2.1	X	22,111,789
192.168.2.2	X	22, 25, 53, 80, 111, 389, 789
192.168.2.4	X	22, 53, 111, 443, 623, 789
192.168.2.5	X	22, 111, 789
192.168.2.6	X	22, 111, 789
192.168.2.7	X	22, 111, 789
192.168.2.50	X	23, 80,433
192.168.2.104	X	22, 80, 433
192.168.2.106	X	22, 80,443, 623
192.168.2.110	-	-
192.168.2.185	-	-
192.168.2.202	X	135, 139, 445

This selected case study scenario highlights several security aspects that have to be dealt with in the proposed security framework. The following subsection discusses the layers of the threat mitigation component of the ICTMS framework, bringing out how each component functions in addressing the security issues unearthed.

## **Appendix D: Threat and Vulnerability Mitigation**

### **Human Aspect Level Security**

Security is a human issue and people (users) can represent a significant part of the problem. Before educating user's or creating awareness programs and strategies, one should understand the extent that social engineering and related attacks are perceived by the users. The case study indicated how social engineering poses a serious threat to marginalised rural users. Hence, to combat social engineering attacks on users, the Human Aspect module of the ICTMS framework suggests an active penetrative testing stance by use of Social engineering Toolkit (SET). This social engineering toolkit is a project named Devolution, and it comes with Backtrack as a framework used for penetration testing. SET was created and written by the founder of TrustedSec. It is an open-source Python-driven tool aimed at penetration testing around Social-Engineering. SET is a popular platform; has been presented at large-scale conferences including Blackhat, DerbyCon, Defcon, and ShmooCon. With over two million downloads, SET is the standard for social-engineering penetration tests and supported heavily within the security community (Kennedy, 2010). From a security standpoint, it is more a collection of tools and techniques that range from negotiation, sales, psychology and ethical hacking. While social engineering can include physical security the SET framework focuses on the art of manipulating people to achieve a goal. The goal involves showing a LL or related ICT access centre where weaknesses may lie with training of rural users of ICTs (not only M-Commerce) in developing a culture of security. Use of SET within a LL setup may help in discovery of the social engineering attacks, with the intention of formulating a defence against them before the actual villains do so. A similar tool that can be employed to address social engineering is the Smartphone Penetration Testing (SPF) framework, described in detail in the next section. Deploying of such a system would require a regular dedicated administrator or helpdesk, so that its positive contributions live to fruition.

Furthermore, it was necessary to educate the marginalised community users on the different M-Commerce platforms security guidelines with the aim of securing their information and money. Likewise three deliverables were developed to ensure user awareness and education: user guidelines, training manual (within the SLL), and awareness program template. Deliverables were obtained by incorporating some standards. A good security awareness

program should educate users about policies and safe practices with information technology (IT). Users should receive information about who to contact if they discover a security threat and how to handle confidential information. Regular training is particularly necessary in a LL setup. However, confirming how well the awareness program is working can be difficult. The most common metric would be looking for a downward trend in the number of incidents over time. Security issues on the human aspect present no easy answers/solutions. Thus, although user education can help; the framework recommends employing every measure that can help make the user community aware of security and social engineering issues. Teachers at the schools (as they are pioneers of new technologies) can have lunchtime presentations about security. The administrator or LL management may also engage in posting security-related news articles on SLL community member's mailing lists. There is a need to make available a sounding board for users' questions on security about things that do not seem quite right. In this research three methods are suggested and these are: 1) developing an online help desk, 2) creating an online database or repository of video tutorials for local users created in a native language (isiXhosa), and 3) training an active member of the community responsible of conducting regular vulnerability assessments in the LL environment. The National Institute of Standards and Technology (NIST) have a publication with templates and guides for what should go into a security awareness training program.

### **Device Level Security**

Mobile phone penetration rate in a marginalised rural community has increased and continues to increase. Use of the mobile devices as transaction enabling tools was also evident. However, a considerable number of users did not employ any device security procedures (data encryption and password/PIN) to protect data. Clearly there are security vulnerabilities that are prevalent on mobile phones as M-Commerce enablers and a need to address the issues before M-Commerce systems can be deemed secure in a rural context is vital. Product designers, platform developers, service providers and all value chain providers must consider these needs in order to deliver successful ICT and mobile-based services to users in these areas. Some user safe-use guideline was established and distributed into the SLL members. Requirements of a secure mobile phone were defined for users to refer to on purchase of a device that may be used for M-Commerce.



Moreover, a number of mobile device testing software, addressing threats and vulnerabilities introduced by mobile devices is available. Most of these solutions seek to secure the whole mobile security environment while some are individual tools for specific threat analysis. Examples of penetrative testing tools and tools sets include: MobiSec, SANTOKU, SPF, etc.

SPF framework is an open source solution for integrating the assessment of smartphones into penetration testing. Such a solution allows security teams and penetration testers to assess the security posture of the smartphones in an environment. Bulb Security developed the open source Smartphone Penetration Testing Framework to solve this problem as a part of the DARPA cyber fast track program (Weidman, 2012). The framework provides a selection of remote, client side, and social engineering based exploitation attacks. For example, the framework sends a text message to a potential victim disguised as typical advertisements that come from vendors with a link included. When users click on the link they are directed to a framework controlled web server that launches a client side attack against the smartphone browser.

To carry out penetrative testing the MobiSec framework by SecureIdeas and Santoku platform by viaForensics can be complementarily employed. The MobiSec Live Environment provides a single environment for testers to leverage the best of all available open source mobile testing tools, as well as the ability to install additional tools and platforms, that will aid the penetration tester through the testing process as the environment is structured and organized based on an industry proven testing framework (Cuevas et al. 2011) (ViaForensics, 2012). An advantage of these platforms is that they are open source and have active online communities offering news, tutorials, and zero day exploits to test out for an administrator. An ICT4D context will benefit more from such a setup as the software can be acquired easily on line free of charge.

Furthermore, researchers have come up with general guidelines for securing data that can help IT and users keep mobile data secure (Mathias, 2009). Use of these tips and tricks as a foundation for mobile device security is then used to craft a security program that works.

## **M-Commerce Access Channel Security**

Access channels lay within the responsibility of the M-Commerce value added chain (the content providers, platform developers, etc.). The deliverables this research produced were recommendations.

### ***SMS and USSD***

In a work (Chikomo et al. 2006) discusses some of the security shortfalls, GSM network, SMS/GPRS protocols and security problems with current banks mobile banking solutions. Their work also discusses two channels of relevancy (as noted in Chapter 3) in our research work: the SMS and GPRS. Some proposed solutions for these problems are documented in the same publication. The results from these proposed solutions proved to provide secure and economic communications between the mobile application and the bank servers. The proposed solutions allow the users to bank using secure SMS and GPRS. However, some work can still be done on their work to ensure sure safe use of SMS and GPRS systems. It is an area of further study and research as well. From this research's point of view, there is need for the value added chain to take an active role to educate the users and make them aware of the various schemes that attackers employ to gain financial and personal information.

### ***Application Development***

On the issue of software development (McCown, 2008) presented a common framework that encompasses and adheres to basic tenets of information security. The proposed framework includes: 1) the basics; what you need to know before writing a single line of code, 2) fundamental rules to be followed when writing the code 3) best practices- proven and successful methods for implementing the code. In web applications, OWASP provides a standard set of risks that every developer should be aware of. Both Native apps and Web apps need to be safe and secure from the conception of their idea to development and use. The following sections dissect further the recommendations this research unearthed.

### ***Mobile Web Applications***

Tools recommended in this research work to address Web application threat discovery includes Arachni. Arachni is an Open Source, feature-full, modular, high-performance Ruby

framework aimed towards helping penetration testers and administrators evaluate the security of web applications. It is smart, it trains itself by learning from the HTTP responses it receives during the audit process and is able to perform meta-analysis using a number of factors in order to correctly assess the trustworthiness of results and intelligently identify false-positives. Arachni uses various techniques to compensate for the widely heterogeneous environment of web applications. These include a combination of widely deployed techniques (taint-analysis, fuzzing, differential analysis, timing/delay attacks) along with novel technologies (rDiff analysis, modular meta-analysis) developed specifically for the framework. This allows the system to make highly informed decisions using a variety of different inputs; a process which diminishes false positives and even uses them to provide human-like insights into the inner workings of web applications.

More so, on Web app security, (CLUSIF, 2010) suggests best practices for creating secure web applications that organisations should apply to develop applications offering a level of security in line with activity-specific risks. OWASP also provides a set of some practices which should be considered in developing Web applications. INSIGHTS-Ernst & Young recommends assessing web-based mobile apps by performing the testing from the perspective of an anonymous user as well as with privileges of the various authenticated users roles in the application (EYGM, 2012). This can be accomplished using traditional web browser on a PC with a standard application security assessment tool set. Scans of the web servers to identify information level vulnerabilities are important, but due to permission and unavailability of such platforms for researchers to explore, this research does not include such an assessment. These scan results should be used to identify common application issues such as those listed in the OWASP Top 10.

A non-intrusive analysis of the website can be performed, including checking content by mirroring the entire site and then checking for client-side code vulnerabilities. Using input generated from the analysis phase, proprietary tools should dynamically test the web server components for common web server and web application vulnerabilities, such as SQL injection, cross-site scripting, cross-site request forgery and directory structure. Also, execution of commercial and public domain tools should be used as deemed necessary. The results from the vulnerability scans should be assessed to identify probable vulnerabilities (false positive reduction). During the next phase, vulnerabilities should be validated through attempts to exploit the vulnerability and other analysis.

### *Mobile Native Applications*

Depending on an application's functionality, testing can be done either in a simulator or on a physical device, or both. During the assessment, of the application's functionality, any internal logic controls and external connections are ascertained.

Applications developed for mobile devices provide challenges to testing not present in traditional applications. For example, mobile devices have limited direct access to low-level processes and exception logs. The devices also support application interaction with GPS, cameras, Bluetooth, WAP and other technologies not present in traditional PCs. To address these challenges, Ernst & Young uses two testing methods:

*Simulators:* Each platform provides developers with an SDK for application development and simulators of different model phones for testing and debugging purposes. These tools can also allow a tester to analyse and test applications in a variety of configurations and devices without the restrictions of a physical device. A benefit to testing within simulators is that code does not need to be signed by a trusted party to execute within the simulator.

*Physical device:* Testing on a physical device provides access to a number of features not available in a simulator, such as SMS, GPS, camera and Bluetooth (depending on the emulator used for simulation). However, testing is restrained because of the lack of access to the underlying OS and application signing requirements.

Because mobile applications vary in many respects, the same document pencils out some suggested steps in carrying out these steps. M-Commerce application developers can carry out their own application security testing before deploying them for public use.

### **Wireless Network Access Security**

Converged wireless infrastructure can be a major contributor to ICT services like M-Commerce. That being the point, security is a serious issue that should be addressed. From a glance it is not feasible that anyone would have the cunning desire to go war-driving through a rural community in deep former Transkei for instance. Likewise one obvious argument will be that robust complex security measures are not that necessary in rural marginalised areas as low literacy does not warrant the feasibility of attacks occurring. We argue it is dangerous, though, to design security that is only "good enough" to hold up against non-technical

intruders. Do we really need to be concerned about black-hat hackers and war drivers in rural Africa?

Where there is a need, people tend to develop skills around it (and the skills to make money from it). War driving tools are freely and easily available on the internet, as are tools required to take advantage of numerous other security exploits. With the increase of internet use and no adequate culture of security, serious problems lie ahead in the future. A little knowledge goes a long way when it comes to hacking, and the days of assuming someone has to be a computer expert to be a security risk are over.

More so, stating that data security is less important in developing African countries than it is in more developed countries sounds as if it is acceptable to adhere to lower standards of quality in these developing countries than it is for developed countries. If use of a WPA2 encryption is a high standard for a residential router in a developing country, then a school in deep rural setting should have it too. We argue that even if data stored on a system seems unworthy of tight security, potential intruders may be after other network resources (or create botnets out of such vulnerable systems). A bot, or web robot, is an automated malware program that scans blocks of network addresses and infects vulnerable computers. A network of these infected computers—numbering in the hundreds of thousands or even millions—is called a botnet (robot network), and each computer becomes connected to a command-and-control server operated by the criminal. Once the botnet is in place, it can be used in distributed denial of service (DDoS) attacks, proxy and spam services, malware distribution, and other organized criminal activity. Botnets can also be used for covert intelligence collection, and terrorists or state-sponsored actors could use a botnet to attack Internet-based critical infrastructure. And, they can be used as weapons in ideology campaigns against their target to instigate fear, intimidation, or public embarrassment. An example is the Coreflood a virus key-logging program on a botnet, that allows cyber thieves to steal personal and financial information by recording unsuspecting users' every keystroke. Such scenarios show how important security should be enforced from the offset in any network.

In such a rural setup where bandwidth is scarce and sometimes billed by volume, it may also not be wise to make an expensive VSAT Internet connection available to passers-by on the street. With some of these areas located close to holiday destinations or recreational facilities (Dwesa Nature Reserve for instance) such situations should be catered for. Network

resources and systems open to such natural resources can deal a massive blow on the future of these ICT initiatives in poverty alleviation and development.

Thus, as developing countries transition to a broadband digital world based on information flow, they must ensure security of the data, networks and systems, and build market and user trust in the use of ICTs for a range of online services, applications and transactions. This trust is the enabler that will encourage governments, the private sector and users alike to innovate and realize the transformational potential of ICTs in a connected world. Lack of a secure and trusted environment would lead to delayed adoption of ICTs, putting developing nations at a disadvantage in participating in global innovation, education, and commercial networks.

Although security is a critical issue in e-business, it is often impossible to measure its effectiveness in real life because of the network administrators' fears or prejudice. In order to find a solution to this particular issue, once more simulation opens the path to solving problems that are hard to fix in real life. In order to improve and support network security development it is important to consider the help that OPNET can provide in testing security performance before its deployment. OPNET is extensive and powerful simulation software with wide variety of possibilities enabling the possibility to simulate entire heterogeneous networks with various protocols. Work by (Zaballos et al. 2010) gave an overall view of all the devices and techniques available within the OPNET Modeller related to security. Framework advises on the use of a network modeller to test and come up with security solutions before implementing a network for the marginalised rural communities as security should not be viewed as an add-on/ after-thought.

It is common practice in modern cyber security analysis to separately utilize real systems of computers, routers, switches, firewalls, computer emulations (e.g., virtual machines) and simulation models to analyse the interplay between cyber threats and safeguards. In contrast, Sandia National Laboratories has developed novel methods to combine these evaluation platforms into a hybrid testbed that combines real, emulated, and simulated components (Van Leeuwen, Brian, et al., 2010). The combination of real, emulated, and simulated components enables the analysis of security features and components of a networked information system. When performing cyber security analysis on a system of interest, it is critical to realistically represent the subject security components in high fidelity. In some experiments, the security component may be the actual hardware and software with all the surrounding components represented in simulation or with surrogate devices. Sandia National Laboratories developed



a cyber testbed that combines modelling and simulation capabilities with virtual machines and real devices to represent, in varying fidelity, secure networked information system architectures and devices. If the aforementioned works can provide such great capabilities, future researchers working on network security in ICT4D infrastructures by leveraging on the previous works to assess the vulnerabilities and threats that would need to be addressed. This in turn can result in an accessible threat mitigation methodology.

In relation to the GSM network as a solid structure on which different channels are hosted, Malware has capability to evade and destroy the network infrastructure thereby affecting the different access channels of transacting noted in this research. A fake GSM operator using the open source OpenBTS project can be used to help analyse mobile malware live while being sure the malicious programs are not inadvertently propagated on the network of a real operator. There is work already carried out by (Apvrille et al. 2011) that explains how to set up our GSM network and then how to use it for the analysis of mobile malware. Area for future work would be simulating not only a live GSM network but all telecommunication networks through which M-Commerce transactions traverse and test malware vulnerability.



## **Appendix E: Questionnaire on Mobile Phone Usage**

Hello! ☺ Anesu Marufu and Thoba Lose here, researchers with the Siyakhula Living Lab, based at the University of Fort Hare. We are currently conducting a study on mobile phone usage patterns amongst the Dwesa Community. We now wholeheartedly invite you to take part in our study. We would like to assure you that there are no right or wrong answers and we are interested in YOUR OPINION. Would it be convenient for you to take a few minutes of your time to answer the questions that follow? Thank you. ☺

The data collected will be used in research purposes. **YOUR PRIVACY IS OF TOP PRIORITY.**





## Section 1

1. Gender:

<input type="checkbox"/>	Male
<input type="checkbox"/>	Female

2. Age:

<input type="checkbox"/>	Below 18
<input type="checkbox"/>	18 – 25
<input type="checkbox"/>	26 – 35
<input type="checkbox"/>	36 – 45
<input type="checkbox"/>	46 - 55
<input type="checkbox"/>	Above 56

3. Employment Status:

<input type="checkbox"/>	Employed
<input type="checkbox"/>	Unemployed
<input type="checkbox"/>	Self-Employed

**SKIP Q4. IF UNEMPLOYED**

4. Monthly Income (R ):

<input type="checkbox"/>	Below R1000
<input type="checkbox"/>	R1000 – R3000
<input type="checkbox"/>	R3000 – R4000
<input type="checkbox"/>	R4000 – R8000
<input type="checkbox"/>	Above R8000

5. Where do you stay (Village)?

\_\_\_\_\_



## Section 2

6. Do you own a mobile phone?

<input type="checkbox"/>	Yes
<input type="checkbox"/>	No

If NO,

7. Why?

<input type="checkbox"/>	Affordability (Cost)
<input type="checkbox"/>	See no use
<input type="checkbox"/>	Cannot use a mobile phone
<input type="checkbox"/>	Other

If YES,

8. What **BRAND** is your mobile phone?

<input type="checkbox"/>	Nokia
<input type="checkbox"/>	BlackBerry
<input type="checkbox"/>	Samsung
<input type="checkbox"/>	Other

9. What **MODEL** of the brand is it (e.g. Nokia X2, BlackBerry Curve, and Samsung E250)?

\_\_\_\_\_

10. How would you rate your mobile phone's battery life?

1=Poor; 2=Fair; 3=Good

<input type="checkbox"/> 1	<input type="checkbox"/> 2	<input type="checkbox"/> 3
----------------------------	----------------------------	----------------------------

11. Which of the following services do you have on your phone, and how often do you use them?

1=Not at all; 2=Often; 3= Very often

<input type="checkbox"/>	Bluetooth	<input type="checkbox"/> 1	<input type="checkbox"/> 2	<input type="checkbox"/> 3
<input type="checkbox"/>	Camera	<input type="checkbox"/> 1	<input type="checkbox"/> 2	<input type="checkbox"/> 3
<input type="checkbox"/>	Memory Card	<input type="checkbox"/> 1	<input type="checkbox"/> 2	<input type="checkbox"/> 3
<input type="checkbox"/>	Wi-Fi	<input type="checkbox"/> 1	<input type="checkbox"/> 2	<input type="checkbox"/> 3
<input type="checkbox"/>	Calls	<input type="checkbox"/> 1	<input type="checkbox"/> 2	<input type="checkbox"/> 3
<input type="checkbox"/>	Texting	<input type="checkbox"/> 1	<input type="checkbox"/> 2	<input type="checkbox"/> 3
<input type="checkbox"/>	Internet	<input type="checkbox"/> 1	<input type="checkbox"/> 2	<input type="checkbox"/> 3
<input type="checkbox"/>	Gaming	<input type="checkbox"/> 1	<input type="checkbox"/> 2	<input type="checkbox"/> 3
<input type="checkbox"/>	M-Banking	<input type="checkbox"/> 1	<input type="checkbox"/> 2	<input type="checkbox"/> 3



12. What do you do on most your mobile phone, and how often?

1=Rarely; 2=Often; 3=Very Often

	Making Calls	1	2	3
	Texting (SMS)	1	2	3
	Taking Pictures	1	2	3
	Instant Messaging (e.g. mxit, 2go, WhatsApp)	1	2	3
	Emails	1	2	3
	Social Networks (e.g. Facebook, Twitter)	1	2	3

13. What do you store most on your mobile phone?

1=Rarely; 2=Least Often; 3=Very Often;

	Contacts	1	2	3
	SMS	1	2	3
	Pictures	1	2	3
	Music	1	2	3
	Videos	1	2	3

14. Do you have an Antivirus on your mobile phone?

	Yes
	Not Sure
	No

15. Your mobile operator is?

	Vodacom
	MTN
	Cell C
	8ta
Other	

16. Are you satisfied with the overall performance of your mobile operator?

	Yes
	No

17. If NO, why are you not satisfied?

	Cost of making calls
	Cost of SMS
	Poor network coverage
	Customer care services
	Not secure
Other	



18. Are you on:

<input type="checkbox"/>	Pre-Paid
<input type="checkbox"/>	Contract

If on **CONTRACT**, GO TO Q23.

19. If on **PRE-PAID**, how often do you buy airtime?

<input type="checkbox"/>	Everyday
<input type="checkbox"/>	Once a week
<input type="checkbox"/>	Monthly
<input type="checkbox"/>	Other

20. How do you get the airtime?

<input type="checkbox"/>	In a shop/vendors
<input type="checkbox"/>	Through mobile transfer (e.g. Me2U)
<input type="checkbox"/>	Through mobile banking

21. Recharge amount:

R

22. Do you typically use up all your airtime?

<input type="checkbox"/>	Yes
<input type="checkbox"/>	No

23. If on **CONTRACT**, what is your average billing per month?

R



### Section 3

24. Who bought the mobile for you?

	Father/Mother
	Brother/Sister
	Uncle/Aunt
	Myself
Other	

25. Was it new or old?

	New
	Old

26. What was the most important reason for purchasing your mobile phone?

	Gives you the 'convenience' of calling anytime.
	It makes you easily accessible
	It is easy to communicate with friends
	No Landline, so you preferred a mobile phone.
	For information access
	For business reasons
Other	

27. Would you share you mobile phone with someone?

	Yes
	No

28. Why?

\_\_\_\_\_

29. What frustrates you the most about you mobile phone?

	Storage Space
	Battery Life
Specify	



## Appendix F: Focus Group Interviewing

### **Welcome:**

*Good morning and welcome to our session. Thanks for taking the time to join us to talk about enhancement of security and privacy in M-Commerce systems in the county. My name is Anesu Marufu and assisting me is ..... We're both with the University of Fort Hare. We are currently undertaking a research on how best people and users in this area can be best protected when using mobile phones/ cell phones when buying goods and services using these devices. We are here therefore to talk to you as the residence of this area to get know what you like, what you don't like, and how security of the programs might be improved. We intend to have discussions like this with several groups around the Eastern Cape region.*

### **Definition of terms**

- Mobile phone/Cellphone > Mobile Commerce
- Examples

### **Results will be used for**

*You've probably noticed the camera and voice recorder. We're recording the session because we don't want to miss any of your comments. People often say very helpful things in these discussions and we can't write fast enough to get them all down. The reports will go back to the county extension staff to help them plan future programs.*

### **You were selected because**

*You were invited because you are local residence and you have a better perspective of how cellphones are used in this area. You are the best people as well to help shed more light on how different things on the technologies can be changed to make mobile device more secure.*

### **Guidelines**

- No right or wrong answers, only differing points of view
- We're recording, one person speaking at a time
- We're on a first name basis
- We won't use any names in our reports. You may be assured of complete confidentiality.
- You don't need to agree with others, but you must listen respectfully as others share their views
- Rules for cellular phones and pagers if applicable. For example: We ask that you turn off your phones or pagers. If you cannot and if you must respond to a call please do so as quietly as possible and rejoin us as quickly as you can.
- My role as moderator will be to guide the discussion
- Talk to each other

### **Questions**



A. Information of the mobile device

- 1) What type of information do you have on your mobile devices?
- 2) Do you feel the information on your mobile device is i) important ii) safe?

B. Theft/Loss of Device

- 1) What or who influences your decision to purchase a mobile device? Did you buy it yourself or someone did it for you
- 2) How often do you lose the devices?
- 3) How do you try to prevent loss or theft of the device?

C. Mobile device repairs

- 1) When we have problems in operating our cellphones, who do we consult?
- 2) When making cellphone repairs where do we take the devices? Are you trusting of these people?

D. Mobile sharing

- 1) How often do you share your mobile device?
- 2) Which people do you trust to share your cellphones with?
- 3) Is there any specific way to protect personal information do you consider?

E. Use of PINs, Password (1<sup>st</sup> explain a PIN & password)

- 1) How do you feel about using a password to protect your information
- 2) Any problems in storing/memorising the password? How do you remember a password?

F. Interfacing and ease of use (1<sup>st</sup> explain use of biometric systems)

- 1) Do you feel replacing passwords with biometrics for instance would be better?

G. Internet use and safety


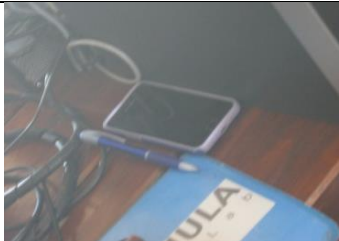








- 1) How often do you visit the internet using cellphones?
- 2) Which type of sites do they usually visit?
- 3) Which applications are they familiar with? (Give examples, Whatsapp, Facebook messenger, BBM etc.)How often do you use these applications?
- 4) How often they make downloads of apps, pictures, attachments, upgrades, etc.

H. M-Commerce trust

- 1) How do you feel about paying for goods and services using a cellphone?
- 2) Do you feel you can trust the security of conducting such a transaction online?



## Appendix G: Mobile phones Prevalence Observations

NQABARA FOCUS GROUP	NGWANE FOCUS GROUP	SHORT NOTES
		High end smartphones have also managed to penetrate into this community, with among them a special mention of a Samsung S2 at Ngwane. All the participants had atleast one cellphone on them.
		In both centres placing a cellphone was a norm and from the few conversations held, the environment feels safe to leave one's device on the work bench in a room with a lot of people.
		Enquiries on penetration of smart devices revealed that there is high readiness to embrace new technology.  Teachers in the community are the pioneers of new technologies
		In both centres a lot of Black Berry mobile devices were noted and seemed to be the most common device noted at both centres.  Most devices with a blue tooth facility where not fully secured.
		Lower end devices were also noted but the numbers or prevalence among the members was not as preconceived.





## Appendix H: Focus Group Picture Display

Table 0.4: Picture display of focus groups carried out at two training centres in SLL

NQABARA FOCUS GROUP	NGWANE FOCUS GROUP
 A group of people are seated in a room with computer monitors in the background. A woman in a blue jacket is holding a document and speaking to the group.	 A group of people are seated in a room with a wooden door and a whiteboard in the background. They are engaged in a discussion.
 A group of people are seated on the floor in a room with a wooden floor. A man in a white shirt is speaking to the group.	 A group of people are seated in a room with large windows in the background. They are engaged in a discussion.



## Appendix I: Safe Mobile Phone Use Guidelines

### SAFE MOBILE PHONE USE GUIDELINES

#### A. THE BASICS



- 1) When buying a mobile phone, consider its security features
- 2) Configure the device to be more secure; use of authentication on the device (PINs & Passwords)
- 3) Maintain physical control of the device, especially in public or semi-public places.
- 4) Take the mobile phone to reliable and trustable repairmen.

#### B. DATA & INFORMATION

- 1) Avoid keeping sensitive information, such as personal and financial account information
- 2) If the presence of sensitive data is not avoidable, the data should be kept in a suitable encrypted form until required. Some devices do support built-in encryption capabilities.
- 3) Avoid giving out personal information to suspicious calls/SMSs or emails.
- 4) Delete all information stored in a device prior to discarding it/ giving it away
- 5) Disable interfaces that are not currently in use, such as Bluetooth, infrared, or Wi-Fi.
- 6) Set Bluetooth-enabled devices to non-discoverable.
- 7) Avoid joining unknown Wi-Fi networks and using public Wi-Fi hotspots.



#### C. ONLINE ACTIVITY

- 1) Limit exposure of your mobile phone number especially online.
- 2) Be choosy when selecting and installing apps.
- 3) Do not follow links sent in suspicious email or text messages.
- 4) Be careful when using social networking applications.
- 5) Configure web accounts to use secure connections
- 6) Use antivirus software solutions





## Appendix J: Safe Practices Transacting Online

### HOW TO PROTECT YOURSELF WHILE TRANSACTING ONLINE – WEB APPLICATION

While enjoying the convenience of modern web applications and application services, end-users should take active steps to protect themselves. In many transactional web applications, it is not uncommon for customers to sign or agree to a “Terms and Conditions” statement, in which customers agree that the web application provider not be liable for any loss or damage that may occur due to any security compromise of the customer’s account.

#### Common safeguards for end-users:

- 1) Don’t login to critical web applications from a public computer.
2. Don’t cache your username and password in the workstation.
3. Remember to logoff at the end of a session.
4. Use different sets of logins and passwords for different web applications and services.
5. Regularly change your passwords used in critical web applications if a one-time password is not supported.
6. Report abnormal behaviour to the service provider immediately.
7. Ensure that the operating system and system components like Internet Explorer (browser) are fully patched and up to date.
8. Install a personal firewall as well as anti-virus software with latest virus signatures. Any anti-virus software should be good enough to detect malware such as keyloggers.
9. Don’t download software or plug-ins from unknown sources.

