Human Aspect in security of M-Commerce services in ICTD: A Siyakhula Living Lab Case Study

Marufu Anesu M.C., Sibanda Khulumani and Scott Mfundo S.

Department of Computer Science
University of Fort Hare, Private Bag X1314
Main Campus, Alice, 5700, South Africa
Tel: +27 40 602 2746, Fax: +27 86 248 9404

Abstract

This paper is a build up to a bigger work in progress which essentially looks at undertaking an extensive evaluation of security threats on M-Commerce platform usage in Information Communication technology for development (ICTD) contexts. This initiative will subsequently draw up a framework to inform deployment of such services and platforms in rural marginalized communities. As is commonly acknowledged that security requirements cannot be addressed by technical means alone, a significant aspect of protection comes down to the attitudes, awareness, behaviour and capabilities of the people involved. Likewise the aim of this work was to evaluate rural user's social habits and day-to-day interaction with mobile devices, in order to ascertain the human aspect as a source of threat in mobile device use. M-Commerce information and systems security seeks to provide: Confidentiality, Integrity, Availability, Non repudiation Authentication. We propose to use these security properties as metrics to investigate how security vulnerabilities were introduced by human to device interaction in our field of study. An ethnographic field study was performed under a Living Lab experience in order to understand the related problems and security issues on mobile phone and ICT usage in a marginalized community. Qualitative measures such as contextual inquiry, participant observation, focus and individual interviews were used during the field data collection. However, only preliminary results from field studies are described in this paper. This work however does not provide a concrete solution on how to secure M-Commerce systems but highlights some socio-technical suggestions that can be used in order to attain that goal. Product designers, service providers and all value chain providers must consider the discoveries noted in this paper in order to deliver successful ICT and mobile-based services to users in these areas.

Keywords: *M-Commerce Security; Mobile Device Security; Rural Marginalised Areas (MRA's); Living Lab, Siyakhula Living Lab; ICT, Threats and Vulnerabilities*

1. Introduction

Mobile transacting or Mobile Commerce (M-Commerce) has found 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 even in remote areas[1]. An information and communication technology for development (ICT4D) is a general term referring to the application of ICTs within the fields of socioeconomic development, international development and human rights [2]. A considerable number of mobile phones are now owned and used by people dwelling in resource constraint rural communities of emerging markets. This could be attributed to the idea that mobile phones provide a less expensive means to narrow the digital divide and because they only require basic literacy. This therefore makes them accessible to a large segment of the population across the world [3]. It is worth noting therefore that mobile phones have become essential tools for communication and information exchange in the last two decades [4].

Many people rely on their mobile phones in their personal lives as well as their businesses. As such, most mobile phone users exchange very sensitive and private information using their mobile phones. Likewise, it may be argued that although mobile use in M-Commerce platforms contribute to providing a cheaper and easier method of transacting for rural users, it is not without its challenges which among them security is of paramount importance. In [5] security was noted by the authors to be very critical to the success of M-Commerce and further research should be conducted in this area, in order to determine methods of making mobile transactions more secure. Further works from [6], [7], [8], [9], [10] also agree to the idea that security is a worthwhile endeavour to pursue in M-Commerce field. It is from such works and understanding that our work has sprung.

As is commonly acknowledged, security requirements cannot be addressed by technical means alone. A significant aspect of protection comes down to the attitudes, awareness, behaviour and capabilities of the people involved [11][12][13]. Indeed, people can potentially represent a key asset in achieving secure mobile use, 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. It is therefore the intention of this work to ascertain the human aspect as a source of threat in M-Commerce use through evaluation of their social habits and behavioural patterns in mobile phone use in order to suggest new solutions to support secure M-Commerce by rural users.

As described by [14] and [15], M-Commerce information and systems security seeks to provide: authentication, integrity, authorisation, availability and non-repudiation. We propose to use these security properties as metrics to investigate how security vulnerability is introduced by human to device interaction in our study field.

The rest of the paper is organized as follows: Section 2 briefly describes the related work; Section 3 outlines the description of our Study setup; the study site, study participants and the process of data collection used, the research methods, and analysis used. Section 4 presents the themes under investigation in alignment with the results. Finally, our paper ends with presenting study conclusion and future work.

2. Related Work

Some work is evident in the area of M-Commerce, cyber security awareness and mobile device use in the marginalized areas. Some of the work is actually done under LL environment which relates to the choice of using a Living Lab adopted by this research as well. Work by [16] described the development and deployment of an E-Commerce platform in Dwesa, the same area through which initial data collection was carried out for this research. Their work involved the implementation of an E-Commerce platform which can make a contribution to rural development and poverty alleviation in the area. However their work looked at an E-Commerce platform which was designed as a web application, to which security considerations were limited to desktop usage and not mobile usage. Even so the work is a valuable footstool for this work as it maps out some security considerations to be considered in creating an M-Commerce structure. More so, our work goes on further to take a direct assessment on the human aspect in security.

In [17] authors focused on promoting cyber security awareness towards the newly realised broadband capability and knowledge transfer within rural communities by means of a voluntary based training program. The cyber security awareness program modules in their work were divided into physical security, malware and malware countermeasures, safe surfing and social aspects of cyber security. However though this work can have great impacts on rural user awareness on cyber threats, less was mentioned in the area of human-to-mobile device interaction as a source of threat. Henceforth this work takes an angle towards exposing first the threats from human to device interaction before documenting the findings into a manual or awareness campaign. The paper roots its methodology approach in the Critical Social Theory (CST) adopted from related work by [18]. The author aims to contribute to on-going ICT for development (ICT4D) discourses by representing an African voice for international ICT policy interpretation and implementation.

In [19] authors tried to tackle the security issues from both technical and human perspectives; how computer attacks are performed, including how to gain illicit access, the types of attacks, as well as the potential damage that they can cause. They also uncovered sociological and psychological traits of attackers including their community, taxonomy, motives and work ethics. The work supports that humans play important roles in computer security. The paper however focused more on the attackers' side, a clear deviation from our work, which focuses more on the end user's (victims) of M-Commerce systems.

Whenever the human aspect is involved in security issues, culture has to be a part of it. A need to understand the cultural issues affecting security in large, distributed and heterogeneous systems, in this case M-commerce systems is essential. Authors in [20] present a model of security culture for e-Science, grounded both in the security literature and in empirical data from an e-Science project. From this model, we present five concepts, which have differing effects on security culture. Each concept is discussed in terms of how the literature treats it, and how it impacts security culture in practice. This discussion highlights differences and similarities between the two domains. It is from this work that a large part of our discussions are rooted.

3. Study Setup

For a better understanding of the current use of mobile phones and the security implications of user's interaction with their devices, we organized an ethnography field study in one rural community of South Africa under SLL. Through field studies, we tried to identify the different security vulnerabilities introduced by the human aspect. Data to be collected in the scope of highlighting the human aspect in compromising mobile devices (thereby 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 (Personal Identification Number) or passwords; 2) the security measures 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 (not limited to) social engineering, identity theft, twin evil attacks and literacy issues.

3.1 Participants and Site

We selected the Siyakhula Living Lab (SLL) located in the Eastern Cape Province of South Africa for our research study. The SLL is a joint initiative of the Telkom Centres of Excellence in the Departments of Computer Science at University of Fort Hare and Rhodes University. The SLL is currently running in the area around the Dwesa-Cwebe Nature reserve within the Mbashe Municipality. The Mbashe Municipality is a deep rural area situated along the Wild Coast of the Eastern Cape province of South Africa. The (initial) five villages targeted in the SLL are adjacent to the Dwesa-Cwebe area, which comprises the nature reserve and adjacent communities which are extended over a land area of approximately 153 square kilometres [21]. The reason we chose to carry out this study under a Living Lab context is that interaction with the rural communities is made easier since the platform for interaction is already in place. The LLs; SLL in particular, also offer better ICT infrastructure which equips rural users with a sense of readiness to engage in IT related issues and provide availability of fundamental ICT distribution channels. The targeted communities in SLL, by sheer size and because of political dynamics, represent a strategic emergent ICT market [22] for such M-Commerce platform security study. The SLL also enables the researchers to have a direct experience of the marginalized 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.
Our study consists 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). The idea was to have participants from literacy training classes at each of the two centres in the SLL. There are basically two centres one at Ngwane and the other at Nqabara at which computer literacy training courses are being held. Each class constituted at least a student, teacher or community member from schools affiliated to the SLL. Figure 1 shows the SLL Network Map and the a distribution of the centres in the Living Lab. Participants who converged at Nqabara came from Badi, Mevana, Kunene, and Nquba, while those at Ngwane were from Mpume, Nondobo, Ntubeni, Ngoma and Mtokwane.

3.2 Research Methods

For our research we applied the observation technique 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

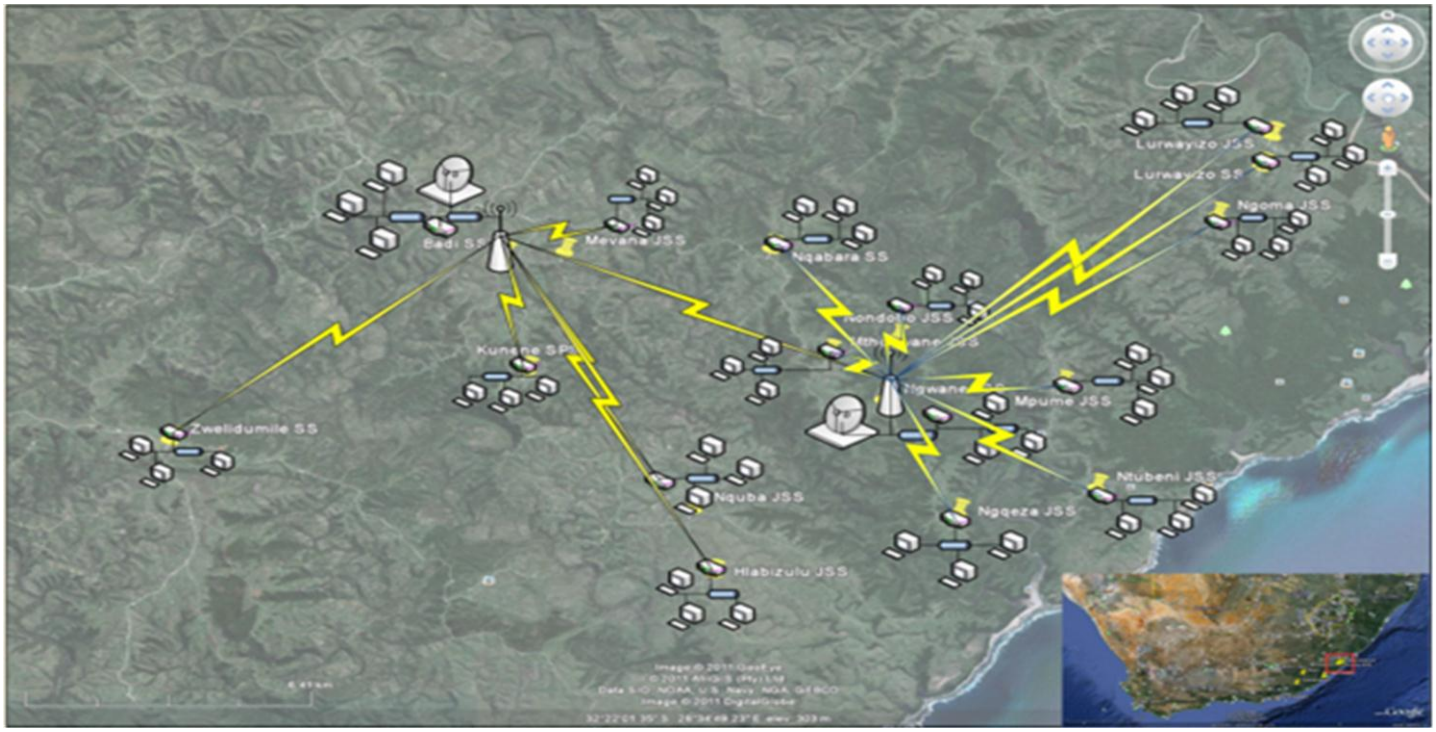

Figure 1: Siyakhula Living Lab Network

a better understanding of mobile device use in an ICTD context 4) to gain new insights or to 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, 4) 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. During the field study, field notes were written to capture and preserve indigenous meanings. To do so, we tried to recognize and limit reliance upon preconceptions about members' lives and activities. We tried to be responsive to what others were concerned about. But while field notes are about others, their concerns and doings gleaned through empathetic immersion, they necessarily reflect and convey the ethnographer's understanding of these concerns and doings [16].

After building rapport with the community members through the literacy training courses at both centres we used the observation technique to gather data on how the users interacted with their handheld devices and how security vulnerabilities may be introduced. We tried to obtain inferences from the way in which the cultural context shapes participants' perceptions about personal data, data use, mobile devices and institutional trust.

The types of mobile devices being used were also noted for the purposes of cross referencing with a baseline study that was carried out in [23]. This was done to determine if the type of device used might influence the type of security measures a user may use and also with the interfacing aspect.

The observation method paved way for the focus groups that were then held in the same context. Focus groups were used in this study because 1) they could yield a large amount of information over a relatively short period of time; 2) they were an effective tool for accessing a broad range of views on our specific topic, as opposed to achieving group consensus, and 3) could act as an enabling tool in developing drafts of interviews and/or questionnaires and 4) could be used effectively in conjunction with other qualitative methods (observations). More so, the group dynamics stimulate conversation and reactions. Within this research, use of focus groups is typically one method among many that we chose 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. It is a situation described as triangulation, which is the use of two or more different methods, in a complementary way, for the same research subject [].

Ethnography study was carried out in a period of about 5 months. The collected data was analysed using grounded theory method [24]. Based on the study findings, appropriate adjustments were made to our original study. Some questions were modified and added in order to know more about the unclear facts.

During our ethnography field study, we practiced a pure qualitative research methodology where a set of qualitative methods were combined in order to gain rich user data. We practiced observation, focus and contextual inquiry for performing this triangulation. Table 1 lists the number of people who participated and their respective literacy training centres and their areas of residence.

Table 1: Participants in the focus groups at Ngwane and Nqabara in the SLL

Participants	Focus Group Centre	
	Ngwane	Nqabara
Students	3	1
Teachers	6	6
Community Members	2	3

In our study, we took certain precautionary steps to avoid any possible bias in our data collection process. For example, to reduce the gap between researchers and participants, engagement was done in the literacy training sessions prior to the commencement of the actual data collection. In writing field notes, we gave special attention to the indigenous meanings and concerns of the people studied. However, even after taking these precautionary steps, we still faced some challenges for example, most of the participants are fluent in isiXhosa and have difficulty in expressing themselves well in English, and hence translation was required from time-to-time as the facilitators were not fluent in isiXhosa. A colleague fluent in isiXhosa language assisted in the transcription of focus group recordings.

4. Study Results

The results section is divided into two main sub-sections: Observations and Focus groups, and results obtained from the respective tools of collection are presented respectively. Table 2 shows the mapping of the obtained themes to principles of security which were violated from user activity.

Table 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

4.1 Observations

4.1.1 Phone/device penetration

High end smartphones have managed to penetrate into this community, with special mention going to a Samsung galaxy S2 model at Ngwane. This widens the range of devices that would be under scrutiny for security vulnerabilities. The participants had at least one cellphone on them, which may actually indicate the idea of mobile devices becoming more affordable. Lower end devices with weak encryption capabilities were also noted but their prevalence was not as preconceived (were expected to be the dominant devices, which was not exactly the case). 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 high end smartphones where noted in with the highest being a Samsung galaxy S2.

4.1.2 Threat from user behaviour

In both centres placing a cellphone on the workbench 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. 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. The use of password or PIN as mobile device locking facilities was not a common practice. Most devices with a Bluetooth facility were not fully secured due to user unawareness and/or ignorance.

4.2 Focus Groups

This section is presented into sections showing the different themes that were noted in the focus groups. Table 2 shows a mapping of the themes in the focus groups to the elements of security adopted in this work

4.2.1 Theft/ Loss of mobile devices

The first challenge is that mobile devices are by design small and portable which can result in loss or theft of the device. While their size is good for day to day usability and convenience it is not as good then when it comes to security. As pointed before modern mobile devices contain more and more sensitive information creating a need to protect the sensitive data on the phone even if it is lost or stolen [13]. Under this theme we were looking to find out a number of possible security issues that may expose user privacy through device loss or theft. Data collected included how often the devices were being lost or stolen, the measures the participants were employing to protect data on the devices or device loss/ theft. At both centres mobile device loss was a norm especially for those users who travel a lot with public transport. As was picked from the observations users behave in a way that seemed to support the reason of the device being lost or stolen. For instance during the literacy training classes most 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. But as one member pointed out and we subscribe to; safety of one's mobile phone is up to the individual of that mobile phone. Some participants at Ngwane even suggested the use of purses and bags, but in the end they even adhered to the idea that even with that, there was no guaranteed way to keep devices from being lost or stolen as some may be taken from one with their consent by robbers. As a measure of protecting the data on the devices, use of PIN's and passwords remained synonymous to most members. One member in Nqabara stated the need to register a SIM card to a device on purchase of a new device as a security measure. But as was also noted, a good number of the participants never really had that option as they got the devices from a relative as a gift usually. This also is ceasing to be an option as some acts in place are now ensuring that a device is not locked to a specific network provider. Moreover, an aware user is a secure user. Regardless of the make or model of a device, keeping data

secure comes down to how one uses and maintains the device.

4.2.2 Mobile device repairs

Under this theme, it was our intention to try to find out; who the participants and members of the community consulted when faced with challenges in operating their mobile devices, to which they take the devices to for repairs, and what level of trust they have for such places? Among the answers that we got from the participants at both centres, some consultations were evident from a majority of the participants. In response to the first question we found out that they consulted students (for teachers), one's own children, mobile phone retailers, the user manual, colleagues or family members. Of interest is the response we got from one participant at Ngwane: "I take it to anybody who can repair or help me…"At the same centre suggestions of calling the customer care of the service provider, and buying another one were also mentioned.

We learnt that in case of device malfunction these devices are taken to repairmen in the nearest towns or cities. Most repairmen are found in Willowvale, were contact with the majority of the rural users is established. When devices are taken for repairs there, they are most of the times left behind with the repairmen. The members in the focus groups acknowledged and stated that the process was not secure. One participant at Nqabara who had past encounters with these repairmen points out how untrustworthy such places are for mobile device repairs. Due to desperation and a lack of secure trustworthy alternatives, participants still take their devices to the mentioned places.

It was our observation henceforth that major security concerns were raised under this theme. It was noted, if bogus repairmen could get the custody of a device they would be able to search for personal plus important details on the device or even install applications (for example Soundminer [25]) that can listen 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 can be used. Not saying that this was observed to be the direct case but, if mobile device use is to be considered secure such issues are supposed to be addressed in the Security Plan on M-Commerce use by rural users.

4.2.3 Device Sharing

Under this theme we tried to ascertain if some security threats may be introduced by some user activities, in this case; sharing of the mobile device. The first impression we got from the floor in both sessions was that the members did not share their devices to which we later discovered that the majority of the participants did share. As with the observations and informal interviews the most occurring answer was that at least someone could answer their calls in cases where they are absent. This was surely the case as some echoed statements like "my kids can answer my phone." People who confirmed to sharing the mobile device noted sharing it with their kids, colleagues, siblings, spouses, and one's boyfriend/girlfriend. Among those who said they shared one even mentioned that she even allowed her siblings to take the device with them and then return it. At Ngwane however some even stated that they did not share (even in cases where she's helping someone else, the person can only use it in their presence). We also noted that most if not all participants who shared devices, did not employ the use of a password which seemed to be a security concern in cases were the trusted party decides to abuse the trust.

4.2.4 Use of Passwords and PINs

A major security weakness that occurs in mobile use is the lack of user awareness. The typical user is not aware that their actions have security implications. A typical user will not worry about securing their phone through a locking mechanism, or they will not ensure that transactions are secure before proceeding. This can lead to the spread of viruses or leaking of sensitive data. Under this theme we were trying to find out 1) how the participants felt about use of passwords and PINs as security, and 2) if they encountered any problems in storing or memorising the password. At the session at Nqabara most of the members attributed to memorising the password as a real problem. One actually stated she resolved not to use any password as a result. We noted a bit of confusion as some of the participants did not know whether their devices had a PIN or password facility or not. Recalling the PIN is an evident challenge and one user had this to say: "common numbers for example my date of birth as no one will obviously forget his/her date of birth".

Some however stated memorisation of passwords was not a big challenge as they try to eliminate the challenge of memorising by simply using date of birth, sibling's name, or even ID numbers. Besides being easy to recall these participants felt it was safe to use as well stating: "I used to use my date of birth number now my ID number…" and "I use my bank number as my security code, so that nobody knows the number…". These practices may leave the users greatly exposed as stated before, as most perpetrators of cyber-crimes are aware that users make use of their personal information for their password.

When we enquired on how the participants felt about replacing regular passwords with the use of biometrics, we noticed that there was a general impression that there are doubts in the new technologies about authentication. One, at Nqabara was quick to suggest: "if security can be done

by a human being, then a human being can change that thing". More sentiments suggested lack of trust on the use of the thumbs as an authentication mechanism, pointing out exposure to identity theft in cases where databases with their information are breeched. At Ngwane we noticed the majority of the participants were a bit confused with the use of biometrics despite explanation of the concept to them. In the end most agreed to the use of biometrics, but this could have been to pressure to conform to other people's views.

Considering how social engineering is on the high as a password one can easily see the users lack awareness of the repercussions of their actions. A possible solution for overcoming the lack of user awareness is to have the wireless carriers offer security training or provide a security awareness pamphlet when a user purchases a mobile device. There will always be people who refuse to read a pamphlet or pay attention to security training but the more people that are aware of the risks the more likely the risks will be reduced. This reason leads to the suggestion of employing a culture of security approach discussed later on. Also, the mobile device manufacturers should be held responsible for making the devices a secure as possible by default. Currently many security features are either disabled by default or are set to the lowest security setting. If manufacturers set their device security defaults to a secure setting then users will always have some level of protection even if they decide not to further configure the phone.

4.2.5 Internet Use and Safety

At this level it was brought to the focus group facilitators' attention that a majority of the participants employed their mobile devices to access the internet and its services. The participants were therefore asked about their surfing habits (which services they accessed, through which sites, if any use of mobile apps was done to access these internet services and which applications they were familiar with). We also established that mobile transacting was a norm among some of the participants with activities including: money transfers (via MPESA); purchasing and transfer of airtime, making online mobile payments (of electricity bills) etc. In general surfing for news and information through mobile browsers, social networking (e.g. Facebook), access of email services and communication were part of the list of activities noted in both focus group sessions conducted. Cellphone banking was a main M-Commerce service that the people engaged in. We also noted that the use of mobile apps was another source of threat to user information as most users downloaded applications from unsafe sources over the internet. It was also noted that the internet is fast becoming part of the participants' lives. Likewise as was established by [21] 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. Users are further advised to install and frequently update the mobile phone anti-virus software and other security related software as well as the mobile phone patches.

4.2.6 M-Commerce Transacting and Trust Issues

This study being part of a bigger work in progress which essentially looks at undertaking an extensive evaluation of security threats on M-Commerce platform usage in ICTD contexts is was essential to: 1) find out how the participants and members in marginalized areas feel about paying for goods and services using a cellphone, and 2) to identify if there were trust issues on conducting such transactions using mobile devices.

In both sessions we got mixed sentiments in response to the first objective; some felt its better than queuing for services, as services are made accessible without hustles. Some pointed the idea of M-Commerce being actually cheaper and accessible than traditional commerce in some instances. They felt it really helps as they usually encounter transport problems and takes time than just doing it online. However we came to learn that the impression most rural users get is that these banking systems are not secure or safe. One participant at Ngwane explicitly suggested the real threat is at the bank or service provider's end, and not necessarily at the end user side.

Trust is a big issue and if M-Commerce systems are going to reach their fullest potential. Likewise some major breakthrough is required to make sure trust through improved security within the systems is established. Some even suggested that they can only transact using small amounts of money. In the case of mobile banking or internet banking, they suggest it is the bank personnel who are the real perpetrators of most bank scams and fraud.

The focus groups also reviewed a usual occurring trend of losing money unscrupulously through the banks and financial institutions where money "is just transferred" without user or customer consent. In addition, there was a great worry that their personal information is all over the internet (online) - in need of clarification by responsible parties into who has what access to their information and why. Special mention of some governmental departments was stated to be the likely source distributing the information.

It was also established that participants and other members of the community regularly receive numerous calls by different people or companies through whom they do not know where they got their numbers from. These anonymous callers usually would tell them their details and ask them to confirm and provide some information. We noted this down to be a typical social engineering scam.

Furthermore, from the user behaviours and focus groups we established that the users must be made aware of the repercussions of their actions when utilizing their mobile devices. They must understand the losses that they may incur if proper precautions are not followed. The best method would be providing guidance to the user when they purchase the device.

One method of providing guidance would be to provide a pamphlet or booklet along with the device that details all the security features on the phone and what settings should be utilized. The booklet should also detail what a user should be aware of when making transactions on their phone. For example, they should be shown how to verify that they are making secure connections and they are not being tricked by an attacker. This method of providing guidance may not be followed by all users. In order to ensure that all users receive some sort of guidance, the mobile device should also have warnings appear on screen when a user performs a potentially harmful action. For example, if the user attempts to disable the password feature then the phone should make them aware of the repercussions by displaying a warning on the screen that the user must agree to before continuing on. As demonstrated by social engineering, a gullible user could be an Achilles' heel of system security. For that reason, it is necessary to educate the marginalised community users of the different M-Commerce platforms so that they will follow security policy guidelines and do their best to help maintaining the security of their information and money. [13] emphasises the importance of information security awareness and training. He also recommends steps and procedures that one needs to take in order to avoid being a victim of a social engineering attack. This research therefore led to the development of some user guidelines and a training module for the SLL. More so, each participant of an M-Commerce platform is an important actor for ensuring security. Participants, as appropriate to their roles, should be aware of the relevant security risks and preventive measures, assume responsibility and take steps to enhance the security of information systems and networks. This can be achieved by shaping the marginalised communities towards a culture of security- defined by ICASA as a pattern of behaviours, beliefs, assumptions, attitudes and ways of doing things that promotes security. A culture of security is and must be a joint endeavour, from the government through to the M-Commerce service providers, down the value added chain to the ordinary user in a community such as Dwesa.

Promotion of a culture of security will require both leadership and extensive participation and should result in a heightened priority for security planning and management, as well as an understanding of the need for security among all participants. Security issues should be topics of concern and responsibility at all levels of government and business and for all participants. The Guidelines by Organisation for Economic Co-Operation and Development (OECD), and ICASA constitute a foundation for work towards a culture of security throughout society [26]. This will enable participants to factor security into the design and use of all information systems apart from M-Commerce. They propose that all participants adopt and promote a culture of security as a way of thinking about, assessing, and acting on the operations of information systems and networks.

It is important to note that, 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 dynamic interconnections within an enterprise. 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 [27].

In [13][28], the author discusses how to achieve a meaningful, intentional security culture. It provides information on the benefits of, and inhibitors to, a culture of security. It further discusses positive and negative reinforcement strategies and the steps to take to achieve the right balance in a security culture program

5. Conclusion and Future Work

In this study, we have presented the results of our ethnography study, organized in the SLL. The aim of this study was to evaluate the human aspect as a source of threat in mobile device use in marginalised communities. It was evident after this study that the security threats are real and need to be addressed. There is a growing demand for understanding the needs and expectations of users dwelling in resource constraint, rural regions of different emerging markets. Ensuring appropriate attention and support for the needs of users should be seen as a vital element of a successful security strategy. User guidelines and a SLL M-Commerce Security training manual are deliverables as output from this study. The major limitation of our existing study was great focus on one set of participants that was attending the literacy training sessions. There is a possibility that some more data or user experiences where left out in such an approach. This study showed some interesting results to be incorporated to the ICTD M-Commerce Security Framework in progress. The approach used in this work can be seen as a roadmap security evaluation plan for other ICTD services which include but not limited to, M-Health, E-Judiciary, and E-Government. We envisage the creation of a framework which can be used by to inform the value added chain on deployment of such services and platforms in rural marginalized communities.

6. Acknowledgments

This work is based on the research undertaken within the Telkom CoE in ICTD supported in part by Telkom SA, Tellabs, Saab Grintek Technologies, Easttel, Khula Holdings, THRIP, NRF SA and GRMDC. The opinions, findings and conclusions or recommendations expressed here are that of the authors and none of the above sponsors accepts any liability whatsoever in this regard

7. References

[1] A. Dhir, I. Moukadem, N. Jere, P. Kaur, S. Kujala, and A. Ylä-jääski, "Ethnographic Examination for Studying Information Sharing Practices in Rural South Africa," no. c, pp. 68–74, 2012.

[2] R. Heeks, "The ICT4D 2.0 Manifesto: Where Next for ICTs and International Development?," *Dev. Informatics Work. Pap. Ser.*, no. 42, pp. 1–35, 2009.

[3] A. Dhir, N. Jere, P. Kaur, M. Heiskala, I. A. Albidewi, and D. M. Alghazzawi, "Design Guidelines for Pervasive Computing : Implications of Technology Use in Africa," no. March, pp. 925–930, 2012.

[4] M. Ahmed, J. Penney, S. Ikki, A. Salami, T. Bath, M. A. Allah, and S. Mansour, "Threats to Mobile Phone Users ' Privacy," pp. 709–737, 2009.

[5] B. L. Charles, F. Monodee, and T. Nurek, "The Critical Success Factors For Mobile Commerce: An Empirical Research paper," University Of Cape town, 2000.

[6] M. Uk, "Challenges in Mobile Electronic Commerce," in *Proceedings of IeC 2000. 3rd Int. Conf. on Innovation through E-Commerce*, 2000, no. 1.

[7] S. I. Sheikh, "MASTER ' S THESIS Mobile Commerce," Luleå University of Technology, 2006.

[8] R. A. J. Gururajan, "A Discussion On Security Risks In Mobile Commerce," *E-bus. Rev.*, vol. 7, no. 2, pp. 1–14, 2006.

[9] A. Grami and B. H. Schell, "Future Trends in Mobile Commerce : Service Offerings , Technological Advances and Security Challenges."

[10] A. Bailes, J. Brown, and L. Coley, "M-Commerce Security : Issues , Trends , & Threats," *ISM 4320*, pp. 1–14, 2006.

[11] S. Lineberry, "The Human Element : The Weakest Link in Information Security," *J. Account.*, vol. 204, no. 5, pp. 44–49, 2007.

[12] I. Arce, *The weakest link revisited [information security]*, vol. 1, no. 2. 2003, pp. 72–76.

[13] K. D. Mitnick and W. L. Simon, *The art of deception: Controlling the Human Element of Security*. Wiley.com, 2001, pp. 1–105.

[14] M. Fuller, "M-Commerce and Security," 2005. [Online]. Available: http://goo.gl/0WZ9i. [Accessed: 20-Aug-2012].

[15] C. Lee, W. Kou, and W.-C. Hu, *Mobile Commerce Security and Payment Methods*. Idea Group Inc, 2005, pp. 292–316.

[16] L. Dalvit, "The Deployment of an e-Commerce Platform and Related Projects in a Rural Area in South Africa," vol. 1, no. 1, pp. 9–18, 2007.

[17] M. Grobler, Z. Dlamini, S. Ngobeni, and A. Labuschagne, "Towards a cyber security aware rural community," in *Proceedings of the 2011 Information Security for South Africa (ISSA) Conference.*, 2011, pp. 1–7.

[18] K. Krauss, "Towards Self-Emancipation in ICT for Development Research : Narratives about Respect , Traditional Leadership and Building Networks of Friendships in Rural South Africa Towards Self-Emancipation," vol. 4, no. 2, 2012.

[19] B. Arief and D. Besnard, "Technical and Human Issues in Computer-Based Systems Security."

[20] S. Faily, I. Fléchais, and S. Culture, "A Model of Security Culture for e-Science," 2003.

[21] R. Palmer, H. Timmermans, and D. Fay, "From Conflict to Negotiation Nature-based development on the South African Wild Coast.," HSRC Press, Pretoria, 2002.

[22] S. Gumbo, H. Thinyane, M. Thinyane, A. Terzoli, and S. Hansen, "Living Lab Methodology as an Approach to Innovation in ICT4D : The Siyakhula Living Lab Experience," in *IST-Africa 2012 Conference Proceedings*, 2012, pp. 1–9.

[23] C. Pade, R. Palmer, M. Kavhai, and S. Gumbo, "Siyakhula Living Lab -Baseline Study," no. April. pp. 1–88, 2009.

[24] B. Glaser and A. Strauss, "The discovery of grounded theory," *Strategies for Qualitative Research.* 1967.

[25] R. Schlegel, K. Zhang, X. Zhou, M. Intwala, A. Kapadia, and X. Wang, "Soundcomber : A Stealthy and Context-Aware Sound Trojan for Smartphones," in *Proceedings of the 18th Annual Network and Distributed System Security Symposium (NDSS)*, 2011, pp. 17–33.

[26] C. O. F. Security, V. Une, and C. D. E. La, "OECD Guidelines for the Security of Information Systems and Networks."

[27] E. N. C. Ena, B. L. I. Ng, U. P. P. Ort, and H. Factors, "The Business Model for Information Security (by ISACA)," 2010.

[28] S. J. Ross, J. Stewart-Rattray, B. Cameron, C. Dimitriadis, W. Goucher, N. Kromberg, O. Sveen, V. Poole, and R. Sethi, "Creating a Culture of Security." © 2 0 1 1 I S A C A, pp. 1–251, 2011.

M.A.C Marufu: is a researcher in the department of Computer Science at University of Fort Hare and is presently studying towards his Master of Science degree at the same institution. He attained his undergrad and honours degrees at the University of Zimbabwe. His research interests include Mobile security, Penetrative testing, M-Commerce and ICT4D

K. Sibanda: is a researcher and senior lecturer in the Department of Computer Science at the University of Fort Hare.

M.S Scott is the Head of Department, a researcher and lecturer in the Department of Computer Science at the University of Fort Hare.