Have Usability and Security Trade-offs in Mobile Financial Services become Untrustworthy?

Stephen Ambore
Department of Computing and Informatics
Bournemouth University
Dorset, UK
sambore@bournemouth.ac.uk

Christopher Richardson
Department of Computing and Informatics
Bournemouth University
Dorset UK,
cjrichardson@bournemouth.ac.uk

Huseyin Dogan
Department of Computing and Informatics
Bournemouth University
Dorset UK
hdogan@bournemouth.ac.uk

Edward Apeh
Department of Computing and Informatics
Bournemouth University
Dorset, UK
eapeh@bournemouth.ac.uk

The trade-off between Usability and Security has been well researched with various models proposed on how best to improve Usability without jeopardizing Security and vice visa. Usable Security has become a key factor in Mobile Financial Services (MFS), the new frontier for mobile phones utilisation. However, have the compromises gone too far? The trustworthiness of MFS system has already slowed down new adoption and impacted ongoing security trust issues and user confidence in spite of potential MFS benefits for its users. To understand this growing lack of trust with MFS, we need to comprehend the nature of Usable Security in assuring the behaviours of MFS users and determine the right trade-off to improve trust whilst facilitating future uptake. We conducted an empirical survey of 698 user's experience of MFS and here present our findings of this investigation for further synthesis towards proposing practical control elements to assure Usable Security in MFS.

Mobile Financial Services, Trust, Usability, Security, Usable Security, Cybersecurity

1. INTRODUCTION

Financial service is the new global frontier for mobile phones. Increasing numbers of customers now prefer banking through Mobile Financial Services (MFS); use of mobile phone as a means to conduct banking and other financial services (PwC, 2017). Moreover, the mobile platforms facilitate financial services to over 2 billion users, including a proportion of the world population that hitherto had no access to financial services (World Bank, 2018). The use of MFS as an alternative banking channel has also benefited regional banking by reducing the operational cost of online businesses (Sri and Gilang, 2015).

Whether serving as alternative banking channel or as the only means to access financial services, a wide range of mobile enabled financial solutions needs to be developed to meet the unique needs of each customer group. However, the increasing lack of trust in MFS has been a major challenge for customer adoption (Gao and Waechter, 2015). A contributing aspect is the lack of trust for MFS where Usable Security by design has become an important but compromised and often perceived as a failing component when deploying mobile security (Faily and Lacob, 2017). The MFS problem of Usable Security is not totally surprising, given the wide range of stakeholders in the MFS ecosystem (Ambore et al, 2016) on one hand and the "rush to mobile" on the other hand, which makes mobile solution developers focus more on meeting delivery targets (Ponemon, 2015) to the detriment of a usable and secure MFS solutions that should also meet the assured privacy needs of the end- user.

The current trade-off between Usability and Security has been studied in various contexts (Alshamsi, Williams and Andras, 2016). To understand the extent to why Usable Security is an essential component to the MFS domain, we need to comprehend its unique context and how to ensure the right balance between Usability and Security is deployed, specifically from the user's perspective.

Proceedings of British HCI 2018. Belfast, UK.

In recognition of Usable Security in mobile phone applications, Mobile Phone Operating System (OS) Original Software Developers (OSD) have published guidelines on Usability and Security at various levels (Ofcom, 2013). Though these guidelines are generally useful for users of Mobile OS and mobile application developers, many do not address the specific need of Usable Security for MFS.

This research provides an understanding of the key elements and comprehends the essential assurance issues and risk mitigation that Usable Security is required to provide MFS in order to establish trust from its user communities. The motivation of this work is to provide a Cybersecurity Countermeasure Framework and establish the principles for Usable Security for the assured use of MFS and thereby, improve its global adoption by increasing, sceptical public.

This paper highlights the results and understanding obtained from a survey of 698 users of MFS. It continues in Section 2 by reviewing related work. The methodology used for the research work is described in Section 3. Section 4 describes the results from this study. The paper concludes in Section 5 and also provides some direction for future work.

2. RELATED WORK

The trade-off between Usability and Security has been a subject intense discussion, the question of how to ensure security without compromising security has been the goal of many research works. For instance, Braz et al, (2007) developed a model called “Security Usability Symmetry” (SUS) which provides guidelines that acknowledge usability constraints and their potential impact on security in addressing the trade-off between Usability and Security.

In a paper advocating Security and Usability together during design to address any concerns with the trade-off between Usability and Security, Yee, (2004) opined that “conflicts between Security and Usability can often be avoided by taking a different approach to security in the design process and the design itself”. Similarly, an approach to predict trade-offs between Security and Usability for mobile application requirements engineering within the unique context of mobile computing, was proposed by Roh and Lee, (2017).

Analysing Security and Usability scenarios, Wang et al, (2017) proposed recommendations on improving security without jeopardising usability. A tool approach for collaboration between security and usability engineering was proposed by Faily and Iacob, (2017).

While all these papers focused on enhancing the optimal Usability Security trade-off, other works have a different approach to addressing the concern. For instance, Adams and Sasse, (1999), looked at the roles of the end-user and impact of wrong perceptions of user behaviour in designing a user-centred security mechanism. They argued that security mechanism and policies that do not consider users’ work practices might lead to developing security mechanism that would result in insecure user behaviours.

The dimension of identifying internal and external threat elements that impact on Usability, Security or both was examined by Kainda et al, (2010). They proposed a model that would help in conducting Usability-Security analysis with the aim of identifying factors that affect Usable Security. While some of the factors identified by the model (effectiveness, efficiency etc) affect Usability alone, other factors (vigilance, motivation and social context, etc) impact on Security. Factors like memorability and knowledge affect both Usability and Security and as such are central to both.

Though user-centred design helps in improving Usable Security, Cranor and Buchler (2014) opinioned that the balance between Usability and Security would be gained from understanding the user decision-making process. They believe it is imperative for solution designers to consider the decision-making process to assign to users when designing a system.

In a study to identify Usability and Security issues in MFS with a bid to develop a solution to resolve them, Smith (2017) identified and presented criteria for Usable Security as identified by literature. While some were traditional criteria for Usability e.g. *effectiveness, efficiency, satisfaction* etc, criteria like *vigilance, trust, empowered user, feedback, awareness, motivation, context of use* and *user behaviour*; were identified as factors that affect Usable Security.

This examination of previous work carried out in Usable Security shows that various models have been proposed to address the Usability Security trade-off in the design and requirements gathering phase of solution development. The need to collectively address Usability and Security to improve this balance was also proposed. In order to ensure the designers’ intention meets the need of the end-user, it has been proposed that the “*weak link*” should be at the focus of designing a usable secure system. Furthermore, the examination revealed that in addition to traditional elements of Usability and Security, some elements exist that impact both Usability and Security.

Though previous research has provided insights on how to ensure that the Usability and Security balance does not result in a zero-sum outcome, the nature of Usable Security in MFS and the elements that affect them has not been investigated.

Furthermore, users of MFS bear the brunt of design decisions that impact Usable Security, it is therefore imperative (to Operators), to understand user behaviour in the use of MFS which when considered could improve design decisions that would lead to usable secure MFS.

This exploratory research orchestrates further understanding to identify observable and latent elements central to Usable Security in deployed MFS and how to improve trust in MFS based on information gathered from MFS users. The research also examines how user behaviour affects Usable Security of MFS.

3. METHODOLOGY

In order to better understand the impact of balance between Usability and Security in the use of MFS, we conducted an end-user survey. The survey questionnaires were distributed via electronic and paper-based correspondence. The completed questionnaires were then analysed and presented.

3.1 Survey Design

The survey questionnaire was developed based on Usability, Security and Usable Security criteria derived from literature that highlighted elements of Usability, Security and Usable Security (Wich and Kramer, 2015; Coursaris and Kim, 2006; Nielsen, 1995), Usability and Security related questionnaires from previous surveys (Mifsud, 2015; Lewis, 1995; Hoehle and Venkatesh, 2015), and critical examination of current threat landscape for MFS.

The population size for the survey was approximately 31 million; which is the number of unique bank accounts in Nigeria, the country of study. A sample size with 95% confidence level and 5% error rate based on Cochran's formulas, created an ideal sample size to satisfy the confidence level and error margin comes to 385 (Barlett, et al, 2001). A total of 698 responses were obtained at the close of the survey.

The survey was distributed electronically via social media (Facebook and WhatsApp), emails and could be completed using a PC, tablet or mobile phone. Hardcopy of the survey was also deployed.

The paper-based survey was piloted with 15 participants focus group, while the online version was piloted with a second focus group of 7 participants. The purpose of these pilots was to obtain feedback on the content, time demand for survey completion and to also test survey logic. Paper-based participants completed the survey in an average of 11 minutes while online participants completed the survey in an average of 9 minutes during the pilot phase.

3.2 Survey Feedback

The survey ran for 2 months. At the end of the survey period, 698 participants completed the questionnaire. 328 responses were obtained via electronic channels; while 370 paper-based surveys were completed and returned. In designing the online survey, a control was set to ensure only Mobile Financial Services users completed the survey. Rather than just exiting the survey, non-users were directed to a short survey that examined their reasons for not using MFS and required changes that would make them use MFS. Moreover, the survey feedback had 29 non-MFS users in total from which these 2 questions were not analysed as part of the survey. Furthermore, 53 of the paper-based responses had a large number of questions unanswered and were not considered for analysis. A total of 616 survey feedback responses were eventually analysed.

The survey was analysed using the Bristol Online survey, SPSS statistical package and Microsoft Excel 2016.

The first step in the survey was to cleanse the survey data. Although the deployed survey had 43 questions, due to the presence of multiple choice options and the 'others' option in some questions, a total of 106 unique variables were generated. The clean-up focused on 8 questions that allowed participants select more than one option in a question. For instance, a participant might use both an Apple phone and a Samsung phone to access MFS. A participant could also use several MFS products etc. It was thus necessary to account for all the various combinations in the data. At the end of the exercise, 65 clean variables were obtained.

The survey questionnaire was segmented into 8 sections based on factors that affects both Usability and Security as summarised in (Smith, 2017) relationship between questions and ease of administration as follows:

i. Participants' details:

This section had 5 questions that sought to understand age, income and educational level of participants along with employment status and type of employment.

ii. Product Type and Means of Use:

This section gathered information on phone type, MFS type and means of access to the MFS products.

iii. Experience:

This section had 5 questions that sought to obtain feedback from user experience based on use of MFS. It also sought to understand user perception on the complexity of MFS and its end-user security mechanism.

iv. Awareness:

This section measures the awareness of privacy, products, roles and responsibilities of participants on the MFS they use.

v. Maintenance:

This section sought to understand user behaviour as regards basic application and phone housekeeping tasks and how it impacts on security and usability.

vi. Usability:

This section gauges user perception on various elements of usability of the MFS.

vii. Security:

This section sought to understand user perception on confidentiality, integrity and availability of MFS.

viii. Social Context:

The last section examines how social and environmental issues might impact on usable security.

ix. Stand out Questions:

Some standout questions not categorised in any of the previous sections were included in the survey. Questions were asked to gather information on participants whose MFS have been compromised in the past and their use behaviours. An 'additional feedback' section was included to capture any other thoughts.

3.3 Survey Analysis

With the survey data sets of 43,120 unique elements, it was imperative to approach the analysis of this survey in a way that would provide insight into the data, given the survey objectives which include:

i. Understanding observable and latent elements central to Usable Security in the use of MFS; and

ii. Impact of user behaviour on Usable Security

A review of available survey tools was performed with a view to understand the most suitable resource to answer the questions of this exploratory survey. The following tools were identified and used to conduct analysis of the data.

i. Descriptive Statistics.

This tool provided basic descriptive statistics e.g. frequency of the collated data. It helped to summarize and provide descriptive information about the collated data. It provided occurrence rates for responses, mean, median mode etc. The analysis of the data collated from this survey benefitted from descriptive statistics tool (how2stats, 2011).

ii. Correlation: Bivariate Analysis

This analysis sought to understand the relationship between variables in the survey, describe the effect that 2 or more phenomena occur together and their linkages. Since this research seeks to understand relationships between variables it would benefit from correlation. A bivariate analysis provided insight into the relationship between user privacy perception and privacy awareness (how2stats, 2011).

iii. Principal Component analysis (PCA)

Principal Component Analysis (PCA) is an exploratory multivariate analysis technique which seeks to describe the underlying structure in a data matrix (how2stats, 2011). PCA is a technique for investigating the interdependence within groups of variables. It is concerned with the relationships between observable variables and unobservable latent variables presumed to be generating the observations. In this research for instance, relationships between variables that would not have been apparent from the use of the tools previously discussed, were examined using PCA. PCA helped to expose latent variables not visible by using simple correlation techniques and cross tabulation.

In order to gain insight into group or related questions, an analysis of question clusters using PCA was implemented. This helped to simplify and reduce the number of variables needed to be analysed without any negative impact on the final output.

The results of the analysis are as described in the next section.

4. SURVEY RESULTS

4.1 User behaviour

An average MFS user is young, middle income and educated. 72.3% of the respondents were between 25-44 years, out of which 36.7% were between the ages of 35 to 44 years, while those between the ages of 25 to 34 years accounted for the 35.6%. Majority of MFS users (42.7%) have at least an undergraduate degree. This is understood given that the predominant MFS product used is Mobile

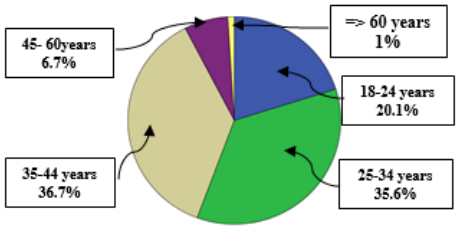

Figure 1.0: *Age distribution of respondent*

Banking, which presupposes respondents have bank accounts with some stream of income, but latch onto the use of MFS for convenience. Unstructured Supplementary Service Data (USSD), a cellular network communications channel is one of the leading platforms for MFS. USSD channel (30.8%) is only second to Mobile Banking (65.4%) in channels for conducting MFS. Figure 1.0 shows the age distribution of respondents.

MFS has three components; Mobile Money, which provides financial services to customers without access to banks, Mobile Banking; an alternative banking channel and Mobile Payment; using Mobile Money or Mobile Banking for payments. Adoption of Mobile Money amongst respondents was the lowest of all MFS products at 7.4%. However, 20% of the respondents (123) use Mobile Payment, Mobile Money and Mobile Banking products. 65% of the respondents have used MFS for 12 months and above. Only 13.3% of the respondents have used MFS for 6 months or less. Respondents overwhelmingly use Android and Windows to access MFS with only 14% using iOS-based phones to access the service.

Mobile application download is the predominant way to setup MFS, with 71.3% of the respondents setting up MFS service on their devices by downloading from authorized application stores. A third party set up the service for 15.9% of the respondents while 4.1% of the respondents could not explain how the MFS they used was setup.

PIN is a leading authentication mechanism for MFS. About 20% of the respondents use Multi Factor Authentication (MFA) to access the MFS they use. PIN with 71.6% is the most predominant authentication mechanism, though most times used in combination with token.

Mobile Network Operator (MNO) data plan is the most preferred means of accessing MFS. 62.6% of the respondents use both Wi-Fi and MNO data plan to access MFS, but more often than not use MNO data.

Convenience (29.7%), ease of use (30.3%) and availability of service (33.8%) are the leading influencers that made respondents choose to use MFS service.

Complexity as against insufficient knowledge is the major cause of transaction errors in the use of MFS. 24.5% of the respondents often experience transaction errors when using MFS. 20.9% of the respondents often perform a single task several times due to the complexity of the MFS. Respondents generally disagree (81.1%) that insufficient knowledge on the use of MFS makes them to conduct a single task several times.

Unstable internet service frustrates MFS users. 65.2% of the respondents said poor or fluctuating internet service frustrates them the most when using MFS. Unsatisfactory level of support from operators (31.7%) and lack of transaction feedback (26.1%), are other major sources of frustration. 63.4% of the respondents share the same phone they use for MFS with others. 29% of the respondents use the same PIN they use for authenticating their mobile phones to authenticate MFS transactions on their phone. 26.6% of the respondents write their authentication details somewhere on their phones to enable easy recall.

MFS users claim not to like security controls that are complex. 78.8% of the respondents believe PIN authentication alone is sufficient to secure their MFS transactions. However, when asked if they would need an additional level of authentication (53.3%) answered in the affirmative. Most respondents (30.8%) cannot differentiate real Mobile applications from rouge ones. Most respondents have no knowledge of Cyber threats that can affect MFS users like Ransomware, smishing, and Mobile Malware. Figure 2.0 shows a distribution of end-user understanding of rogue applications.

However, respondents claim to have an average

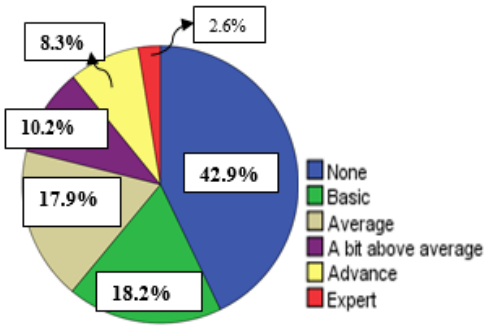

Figure 2.0: *User knowledge of Rogue applications*

knowledge level on privacy. Most participants are ignorant of the connection between update of mobile phone Operating System (OS) and periodic update of MFS applications on the security of the system. 87.5% of the respondents do not agree that the security of MFS transactions depends on the update of their mobile phone OS. Furthermore, 84.4% of the respondents indicated that the security of the MFS they use does not depend on how frequently the MFS application is updated.

Respondent claim to prefer security to ease of use in MFS. Respondents preferred a secure transaction (66.6%) than an easy to use MFS system. Nevertheless, they would also prefer if the security control is easy to use.

4.2 Principal Component Analysis (PCA) Result

To conduct the PCA, we first conducted a cluster analysis on a group of variables. Cluster analysis is

a multivariate method which aims to classify objects based on certain similarities into groups (Cornish 2007, Hair et al, 1998).

In conducting the clustering analysis, variables that sought to analsye the same factors were placed in the same group. Each group was then jointly analysed in such a way as to reveal insights that might not be obvious in analysing single variables. For instance, analysing a single variable for effects of poor network on Usable Security provided some insight into the impact of network on usable security, analysing other environmental concerns together would provide deeper insight into the impact of environmental factors in general on usable security.

6 clustered groups were classified as shown in in table 1.0 below.

Table 1.0: *Description of grouped classification used for cluster analysis*

Sn	Group	Description	Short Name
1	Complexity of system	Gauging user perception on complexity of MFS and its security mechanism	Complexity
2	Awareness of privacy	Awareness of privacy in use behaviour of MFS.	Privacy
3	End-user patching	User behaviour in maintaining updated OS, application and antivirus	Patching
4	Usability	User perception on usability of MFS	Usability
5	Security	User perception on security of MFS	Security
6	Environmental Impact	Impact of environmental factors on usable security of MFS	Env

PCA results described in the rest of this section are based on cluster analysis of the groups in table 1.0.

87.99% of the respondents believe the MFS system is complex. To obtain this feedback, 4 questions were clustered and analysed together. These questions sought to understand task completion rate, error rates, number of tries before successful completion of a task and reasons for the multiple attempts. 10.7% however believe the system is easy to use; whereas 1.3% of the respondents were indifferent. Out of the respondents who say the MFS they use is complex to use, the largest group of participants who find the system complex to use are within the 35 to 44 years age bracket. Those within the age range of 18 to 24 years find it easy to use. However, 68.02% of the respondents are satisfied with the usability attributes of MFS. 53.73% of the respondents believe the security of the MFS they use is adequate. Table 2.0 shows the distribution of perception of complexity. Gaps between perception on understanding of privacy and demonstration of privacy in practice exist. While 78.9% of respondents claimed to have a basic to expert level knowledge on privacy, 79.71% of the respondents did not demonstrate understanding of privacy and its implication in the use of MFS products, based on use behaviour. For instance, respondents that claim an above average knowledge of privacy and its implication on the use of MFS still share their phones with friends and family. They use the same PIN for their phones and MFS, they also write authentication details for the MFS on their phones. Table 3.0 shows the distribution of privacy based on use behaviour.

Table 2.0: *Complexity*

		Frequency	Percent	Cumulative Percent
Valid	easy	66	10.7	10.7
	Neutral	8	1.3	12.0
	complex	542	88.0	100.0
	Total	616	100.0	

Table 3.0: *Privacy*

		Frequency	Percent	Cumulative Percent
Valid	high privacy	125	20.3	20.3
	low privacy	491	79.7	100.0
	Total	616	100.0	

Though respondents cannot directly link the impact of updating their mobile OS, mobile applications or antivirus to the security of MFS, 82.63% of respondents update their phone operating system, Mobile applications and phone antivirus as at when due.

60.2% of respondents believe environmental issues like weak internet network strength, incoming phone calls during transactions, environment of use and low battery life have an impact on security and usability of MFS. 20% of the respondents believe these factors do not impact on usability and trust while another 19.3% were indifferent.

Majority of those with high degree of trust on MFS (61.9%) did not receive any training or sensitization before they commenced use of the system. Awareness and training might mean different things. It might also mean that training was not sufficient.

4.3 Observable Variables

This section shows the relationship between observable variables and unobservable latent variables generating the observations, based on PCA analysis. Table 4.0 shows the descriptive statistics of the observable factors.

Table 4.0: *Descriptive statistics of observable usable security factors*

Descriptive Statistics

	Mean	Std. Deviation	Analysis N
Complexity	31.67	6.622	616
Privacy	6.75	2.586	616
Patching	19.14	5.670	616
Usability	8.60	2.461	616
security	6.68	1.915	616
Env	6.29	1.717	616

As shown in table 4.0, *Complexity* has a mean of 31.67 and a variation of 6.622. *Complexity* also shows the highest deviation. *Patching* has the second highest mean and accounts for the second highest deviation. While user behaviour on *Security* and *Env*, show the least deviation.

The PCA correlation matrix shows that all 6 observable variables have a direct or inverse relationship. Table 5.0 shows the result of the PCA correlation matrix.

Table 5.0 shows that *Usability and Security* have the highest positive correlation factor of 0.552, *Complexity* has a negative correlation with both *Usability* (-0.302) and *Security* (-0.302). This implies *Complexity* has an impact on both *Usability* and *Security*. The more complex the system is, the lower the Security and Usability of the system and vice versa. The coefficient of correlation of *Privacy* to *Usability* is 0.173, while that *Privacy* to *Security* is 0.165. This implies that participants' level of privacy based on system use also has a positive correlation on both *Usability* and *Security*. The higher a participant's level of privacy in using MFS, the higher the Usability and Security of the system. The coefficient of *Privacy* variable to *Usability* is 0.249 while the coefficient of *Patching* variable to *Security* is 0.264. This shows that regular updates of phone OS, apps and antivirus correlate with higher level of Usability and Security.

In summary, system complexity, privacy, frequency of updates, and level of trust are correlated with both Usability and Security. Correlation between components is further depicted by a scatter plot as shown in figure 3.0.

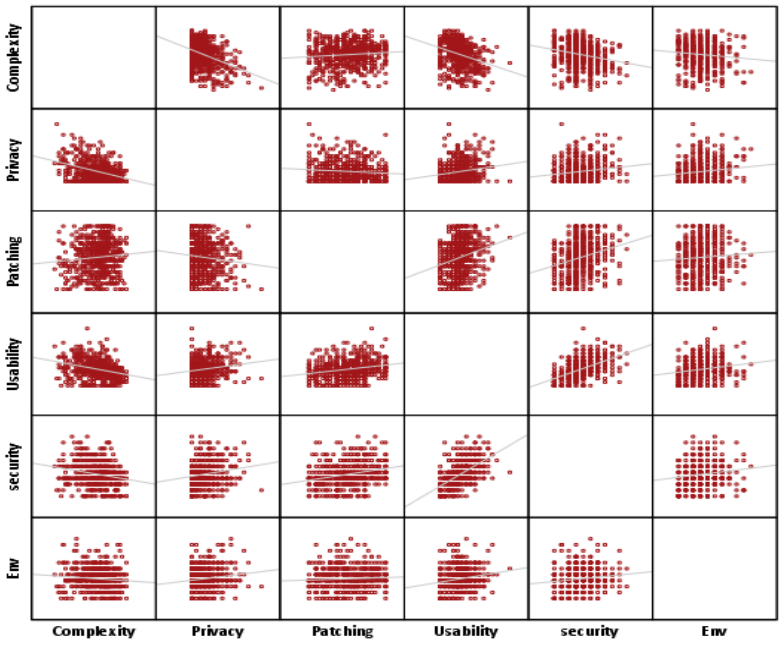

Figure 3.0: *Scatter Plot showing correlation between component*

4.4 Latent Variables

Kaiser-Meyer-Olkin (KMO) measure of sampling adequacy of 0.638 indicates proportion of variance in entire variables (Williams et al, 2010). Standard deviation measured the proportion of independent variables; in this case, KMO measures the variation of interdependence of all observable variables. The

result from the KMO Bartlett's test of sphericity shows that for the 616 respondents being analysed, 64% of them have certain commonality. However, about 36% variation exists amongst respondents. 38% have distant opinions.

Component matrix analysis of the 6 observable variables (*Complexity, Privacy, Patching, Usability, Security* and *Env*) against the 4 latent variables revealed that there was a correlation between the first latent component and all 6 observable variables. The first component loads heavily on Usability and Security. It has a strong positive

***Table 5.0**: PCA Correlation Matrix*

Correlation Matrix

	Complexity	Privacy	Patching	Usability	security	Env
Complexity	1.000	-.376	.092	-.302	-.216	-.096
Privacy	-.376	1.000	-.100	.173	.165	.135
Patching	.092	-.100	1.000	.249	.264	.062
Usability	-.302	.173	.249	1.000	.552	.174
security	-.216	.165	.264	.552	1.000	.136
Env	-.096	.135	.062	.174	.136	1.000

According to KMO results, the sampling adequacy had 36% variation, this implies only 64% of the variation has been explained. To optimize the model to account for 80% of the variables, correlations on latent components were examined. Table 6.0 shows KMO Bartlett's test results.

***Table 6.0:** KMO Bartlett's test*

KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.638
Bartlett's Test of Sphericity	Approx. Chi-Square	494.897
	df	15
	Sig.	.000

Further analysis shows that 4 latent variables cumulatively account for 82.751% variation. This

***Table7.0:** Component Matrix*

	Component			
	1	2	3	4
Usability	.800			
security	.760			
Complexity	-.580	.535		
Patching	.313	.735		.540
Privacy	.487	-.606		.525
Env	.373		.920	

Extraction Method: Principal Component Analysis.

implies that in addition to the 6 observable variables discussed earlier, some latent variables that impact Usable Security in the use of MFS exist. Table 7.0 shows the component matrix analysis of observable variables against latent variables (components).

correlation coefficient of 0.8 on *Usability* and 0.76 on *Security*. It has a negative correlation of -0.58 on *Patching* and a low positive correlation on *Complexity* (0.31), *Privacy* (.049) and *Env* (0.37) respectively.

The second latent component loads positively on *Complexity* (0.535) and *Patching* (0.735). However, it loads negatively (-0.606) on *Privacy*. The second component does not show correlation on *Usability and Security* and *Env*.

The third component loads positively on *Env* (0.92) and has no correlation with the other 5 observable variables.

The fourth component loads only on 2 observable variables; *Privacy* and *Patching*.

As part of the PCA, a pattern matrix analysis and a structure matrix analysis were further conducted to gain more insight into the latent component, both matrixes revealed further correlation between the latent variables and the observable variables. The pattern matrix showed that *Complexity* has a bipolar loading while the second component loads heavily on *Patching* and a weak positive loading on *Complexity*. The third component loads heavily on *Privacy* and negatively on *Complexity*.

5. DISCUSSIONS

From the survey results, there was no evidence to show that age or income level has a direct effect on usable security; however, results obtained showed that younger people are more likely to forget their MFS login credential when compared to older people (60 years and above). This might not be unconnected with the fact that younger people might have the need to recall many login

credentials which might affect memorability, while older people might have fewer applications to worry about.

No significant difference was observed between participants who have been using MFS for over 12 months and participants who have used the solution for a shorter period.

Most users download applications they use from Mobile apps stores and majority of the users are unable to differentiate between real applications and rogue applications. Even though popular application stores like Apple store and Google Play store have controls, the possibility of jail-breaking or rooting exists. Users at times receive forwarded hyperlinks to sites where they can download certain applications from. While in terms of Usability this is preferable to downloading from the application stores, the risk of introducing mobile malware is further heightened. End-users should be educated on the need to download applications from only authorised sources to mitigate the risks of mobile malware attacks.

Some respondents use multifactor authentication to access MFS, which is a good security control. However, the multiplicity of authentication credentials used by users for various phone applications makes majority of respondents save authentication information on the same phone they use and also share with family and friends, thereby introducing new security concerns. This behaviour seems to be predominant among the age range 25 to 44 years, who incidentally have the highest population of MFS users based on this survey.

MFS users prefer Security above Usability. Convenience and ease of use attract most users to MFS. Though users think MFS is complex to use, they prefer a secure MFS solution to one that is easy to use. However, they would also prefer if the security controls put in place to protect MFS are less complex.

Environmental factors impact both the Usability and Security of MFS services. Users believe poor network, low battery, incoming calls to their phones while conducting MFS transactions affect Usability and Security of the system.

Though most users of MFS are ignorant of the links between regular updates of Mobile phone O/S, applications and phone antivirus to Security and Usability of the system, they tend to update as soon as new updates are available.

Knowledge of privacy does not translate to behaviours that exhibit understanding of the implications of privacy. Users generally have an understanding of privacy, but this does not reflect in behaviours of the use of MFS.

There was no correlation between training and secure use of MFS. Most users that exhibit high level of trust in the existing MFS system did not receive any form of training on MFS before or after they commenced use of the system.

Users that exhibit high level of trust on the system possess the following characteristics based on survey analysis:

- They believe the transaction limits set on MFS is sufficient;
- They believe their MFS transactions are protected from unauthorised disclosure irrespective of their past experience;
- They believe their MFS transactions are accurate and consistent through-out its life-cycle; and
- They are satisfied with the reliability of the MFS system.

There is a high degree of correlation between Usability and Security in the use of the MFS. Usability attributes like *effectiveness*, *efficiency* and *learnability* affect Security attributes like *confidentiality*, *availability* and *integrity* of MFS system.

The PCA analysis shows that complexity of system, and awareness of privacy, Usability and Security are observable variables that affect Usable Security. While end-user exhibit good patching behaviour, they cannot relate the need to regularly update their mobile phones to its effect on security.

The PCA further reveals that in addition to observable variables that affect Usable Security, some indirect factors exist in MFS user behaviour that affect Usable Security. One of these components has a positive correlation with Usability and Security while others have positive or inverse correlation to some observable variables.

6. CONCLUSIONS

While previous studies have focused on understanding Usable Security trade-off from design perspective, this research examined the trade-off by analysing MFS user behaviours. The study revealed that users are capable of inherently exhibiting good security behaviours. For instance, users regularly update mobile phone OS, mobile applications and phone antivirus even when they do not understand the relationship between regular systems update to system security. Also, most users did not receive any training on how to use MFS or its security controls but figured out a safe way to use the system, even when it seemed complex.

MFS users prefer Security above Usability. Though users prefer less complex security controls, they would forego Usability for Security in the use of MFS, as a security failure would likely lead to financial loss.

Usable Security of MFS impacts user behaviours and causes users to act in less secure ways. For instance, users store MFS login credentials on their phones and also share the same phones with family and friends. User awareness can be used to address this risk; however, the research has shown that user awareness does not always translate to good user security behaviour. This might be due to the usability of the awareness material or the gap between learning and awareness in practice.

Furthermore, the study has shown through the behaviours of users of MFS that complexity of the MFS system, awareness of privacy by users, usability, security and environmental factors are central to Usable Security in the use of MFS. The study also revealed that latent variables that impact Usable Security in the use behaviour of MFS exist.

While Usability and Security trade-off is an important consideration during design and it is generally accepted that a right balance between Usability and Security would encourage good user behaviours, this study has shown that users of MFS will trade Usability for Security, even though they would prefer less complex security mechanism. The study has also revealed that users are inherently capable of good security behaviours even when the security mechanism seems a bit complex.

Ensuring an optimal balance between Usability and Security might not be sufficient to address the trust gap in the use of MFS. To address the gap, user perception on the complexity of MFS and its security mechanism should be considered. Also, user awareness on privacy in the use of MFS, and the impact of environmental factors like internet network connectivity strength should also be considered. In addition to the aforementioned factors, latent elements in the use of MFS exist that have impact on the right balance between Usability and Security. Putting the same emphasis on these factors as currently done in ensuring an optimal balance between Usability and Security can lead to a cost-effective usable secured MFS.

7. FUTURE WORK

This study focused on understanding the impact of user behaviour on Usable Security and trustworthiness in the use of MFS. There is a need for a formal framework that will seek to address the identified factors that impact Usability and Security and consequently trust in the use of MFS. Future studies will seek to explore how to develop this framework.

8. REFERENCES

Adams, A., & Sasse, M. A. (1999). Users are not the enemy. Communications of the ACM, 42(12), 40-46.

Alshamsi, A., Williams, N., Andras P., (2016), The Trade-off Between Usability and Security in the Context of eGovernment: A Mapping Study, BCS Human Computer Interaction Conference 2016. https://www.researchgate.net/publication/310624156_The_Trade-off_Between_Usability_and_Security_in_the_Context_of_eGovernment_A_Mapping_Study. (Retrieved March, 2018)

Ambore, S. Richardson, C. Dogan, H, Apeh, E. Osselton, D. (2016). A “Soft” Approach to Analysing Mobile Financial Services Socio-Technical Systems. Proceedings of British HCI 2016.

Barlett, J. E., Kotrlik, J. W., & Higgins, C. C. (2001). Organizational research: Determining appropriate sample size in survey research. Information technology, learning, and performance journal, 19(1), 43.

Benjamin, J.S, (2017) Mobile Financial Services: A Usable Security study of the user pathway, Bournemouth University M.Sc. Thesis.

Braz, C., Seffah, A., & M’Raihi, D. (2007). Designing a trade-off between Usability and Security: a metrics based-model. In IFIP Conference on Human-Computer Interaction (pp. 114-126). Springer, Berlin, Heidelberg.

Cornish, R. (2007). Statistics: Cluster analysis. Mathematics Learning Support Centre.http://www.statstutor.ac.uk/resources/uploaded/clusteranalysis.pdf (Retrieved 16th March, 2018)

Coursaris, C., & Kim, D. (2006). A qualitative review of empirical mobile usability studies. AMCIS 2006 Proceedings, 352.

Cranor, L. F., & Buchler, N. (2014). Better together: Usability and Security go hand in hand. IEEE Security & Privacy, 12(6), 89-93.

Faily, S., & Iacob, C. (2017). Design as Code: Facilitating Collaboration between Usability and Security Engineers using CAIRIS. In 2017 IEEE 25th International Requirements Engineering Conference Workshops (REW) (pp. 76-82). IEEE.

Hair, J. F., Black, W. C., Babin, B. J. Anderson, R. E., & Tatham, R. L. (1998). Multivariate data

analysis (Vol. 5, No. 3, pp. 207-219). Upper Saddle River, NJ: Prentice hall.

Hoehle, H. and Venkatesh, V. (2015) Mobile Application Usability: Conceptualization and Instrument Development. MIS Quarterly Vol. 39 No. 2, pp. 435-472.

How2stats, (2011) http://www.how2stats.net/p/home.html (Retrieved December, 2017).

Kainda, R., Flechais, I., & Roscoe, A. W. (2010). Security and usability: Analysis and evaluation. In Availability, Reliability, and Security, 2010. ARES'10 International Conference on (pp. 275-282). IEEE.

Lewis, J. R. (1995) IBM Computer Usability Satisfaction Questionnaires: Psychometric Evaluation and Instructions for Use. International Journal of Human-Computer Interaction, 7:1, 57-78.

Mifsud, J. 2015, Usability Metrics – A Guide to Quantify the Usability of Any System, https://usabilitygeek.com/usability-metrics-a-guide-to-quantify-system-usability (Retrieved June, 2017).

Nielsen, J. (1995). 10 usability heuristics for user interface design. Nielsen Norman Group, 1(1).

Ofcom, (2013), Study into the implications of Smartphone operating system security, https://www.ofcom.org.uk/__data/assets/pdf_file/0016/76111/goode_intelligence_report_o1.pdf. (Retrieved March, 2018).

Ponemon Institute Research, (2015). Report on The State of Mobile Application Insecurity., Sponsored by IBM Independently conducted by Ponemon Institute LLC Publication Date: February 2015.

PwC, (2017), Don ’t take it to the bank: What customers want in the digital age. https://www.pwc.com/us/en/financial-services/publications/assets/pwc-fsi-whitepaper-digital-banking-consumer-survey.pdf.(Retrived 14th March, 2018)

Roh, W., and Lee, S. W. (2017). An Ontological Approach to Predict Trade-Offs between Security and Usability for Mobile Application Requirements Engineering. In 2017 IEEE 25th International Requirements Engineering Conference Workshops (REW) (pp. 69-75). IEEE.

Sri, R. and Gilang, R.P. (2015), The Influence Of Mobile Banking Transaction Used On Cost Reduction Of SMEs Employers International Conference on Economics and Banking https://www.researchgate.net/publication/299963777_The_Influence_Of_Mobile_Banking_Transaction_Used_On_Cost_Reduction_Of_SMEs_Employers (Retrieved March, 2018).

Wang, Y., Rawal, B., Duan, Q., & Zhang, P. (2017, February). Usability and Security Go Together: A Case Study on Database. In Recent Trends and Challenges in Computational Models (ICRTCCM), 2017 Second International Conference on (pp. 49-54). IEEE.

Wich, M., and Kramer, T. (2015). Enhanced human-computer interaction for business applications on mobile devices: a design-oriented development of a usability evaluation questionnaire. In System Sciences (HICSS), 2015 48th Hawaii International Conference on (pp. 472-481). IEEE.

Williams, B., Onsman, A., and Brown, T. (2010). Exploratory factor analysis: A five-step guide for novices. Australasian Journal of Paramedicine, 8(3).

World Bank, (2018), The Global Findex Database, 2014, Measuring Financial Inclusion around the World, http://www.worldbank.org/en/programs/globalfindex. Retrieved March, 2017. (Retrieved 16th March, 2018).

Yee, K. P. (2004). Aligning security and usability. IEEE Security & Privacy, 2(5), 48-55.