Development of Usable Security Heuristics for Fintech

Stephen Ambore
Bournemouth University
Poole, Dorset, UK
sambore@bournemouth.ac.uk

Huseyin Dogan
Bournemouth University
Poole, Dorset, UK
hdogan@bournemouth.ac.uk

Edward Apeh
Bournemouth University
Poole, Dorset, UK
eapeh@bournemouth.ac.uk

Investments in cybersecurity over the years have led to the availability of strong technical countermeasures and innovations that are being increasingly leveraged to strengthen the security posture of financial services systems. The effort to improve the security posture of the human element of financial services systems has not matched the effort in developing technical countermeasures, thereby undoing the gains of the later. One area where such problem exist is in Fintech where emphasis is placed on developing innovative and secured technical financial models aimed at making financial services more accessible through the mobile phone. These Fintech solutions however have shortcomings in securing the human element. This study seeks to address this problem through the development of heuristics that can be applied in the evaluation or design of Usable Security in Fintech. This study developed twelve (12) initial Usable Security heuristics which were validated through expert review. The heuristics were developed through an iterative approach that comprises a survey of Fintech users, semi-structured interviews of Fintech solution providers and thematic analysis of relevant literature. The findings of the study show that application of the developed heuristic provides for Usable Security.

Usable Security. Fintech. Heuristics. Cybersecurity. Usability

1. INTRODUCTION

The high rate of mobile penetration, capability to generate insight from user data and the need for a better and personalized user experience in the use of financial services is driving the uptake of innovative models for financial services otherwise known as Fintech. Fintech refers to innovative models that enable the delivery of financial services in an agile manner (Mani, 2019, Addilah, 2019, Saksonova and Kuzmina-Merlino, 2017). These models leverage technologies like Application Programming Interface (API) Blockchain Technology, Biometry Technology, Artificial Intelligence, Data Analytics and Cloud to provide financial services to existing and new customer segment (EFInA, 2020).

In the UK, Fintech through challenger banks and neobanks like Monzo and Revolult are disrupting the financial services landscape (High, 2021). In response to this disruption, most incumbent banks now offer Fintech solutions to their customers through mobile financial services.

While Fintech has facilitated access to financial services in a cost-effective way, it comes with a secondary risk of cybersecurity to the customers. Fintech and digital platform provided a window for consumers to access financial services remotely during the lockdown occasioned by the COVID-19 pandemic in most countries where physical access to banks and stores were restricted. However, cyber fraud targeting Fintech increased during the same period (Glenny, 2021, Borrett, 2021).

Strong technological countermeasures like strong cryptographic algorithm, biometric authentication and improve methods to elicit informed consent exist to curb the growth of cybercrime. These technical countermeasures and innovation notwithstanding, cybercrime incidences still occur (Shetty, 2018). Most of these have been attributed to the human element who has been described as the "*weakest link"* in the security value chain because of their propensity to make errors or poor security decisions in the use of a system (Sasse et al., 2001, Pfleeger et al., 2014). Irrespective of the security controls put in place, the action or inaction of end-users can make a system susceptible to cyber-attacks. Analysing the psychological perceptions on why users make unsafe security decisions, West et al. (2009) posited that errors by end-users in the use of a system, and not sufficiently addressing human factor considerations during design are major contributors to cybersecurity risks. While investment in technical controls would help mitigate the risk of cybercrime, mitigating the vulnerability associated

with the *"weakest link"* is imperative to build security controls that do not discourage good use practice and further jeopardize security objectives. For instance, Hof (2015) argued that though technology controls exist to secure systems, they might not be designed with usability as a primary objective.

Security systems are not foolproof but strengthening the human element will further improve the security posture of Fintech. Fintech is an important innovation as it stands to provide access to financial services to over 1.7 billion people globally who currently do not have access to financial services (Asli et al., 2018). More so, as most banks continue to leverage the mobile phone to provide financial services, more customers will depend on Fintech to access service putting more customers and their transaction at risk of cybercrime.

This study adopts a sociotechnical approach to improve the cybersecurity posture of Fintech, by examining elements that can improve the human factor from the perspective of users and solution providers in the ecosystem. The study examined previous approaches adopted to improve cybersecurity from human perspectives and identified the need to develop heuristics that can be applied to improve Usable Security in Fintech, using a case study of mobile financial services. Heuristics are rules of thumb, for making inferences in an environment with limited time, knowledge or computational power (Hafenbrädl, et al., 2016).

While previous studies have developed heuristics, which were tested in other domains, to the best of our knowledge, no previous work exist on developing heuristics that will help evaluate and design Usable Security in Fintech (Feth and Polst, 2019).

Furthermore, early usability studies focused on improving user experience through usability inspection with a view to identifying usability problems (Nielsen, 1992). This study examined the Usable Security of Fintech from the perspective of the users and solution providers in the ecosystem.

The study presents an initial set of heuristics for the evaluation of Usable Security in Fintech. The recommendations of this study would serve as a guide for Fintech Developers, Systems Auditors, HCI and Cybersecurity experts looking to improve the security posture of Fintech solution.

The next section of this paper examines related work while section three (3) provides an overview of the methodology adopted in this study. Results of the studies conducted are provided in section four (4). A discussion on the findings and recommendation of the studies are contained in section five (5). The paper ends with a recommendation for future studies in section six (6).

2. BACKGROUND AND RELATED WORK

In this section, we reviewed prior work on improving the cybersecurity posture of systems with a focus on the human element. We then reviewed how Usable Security is evaluated and how it is incorporated into systems design. Furthermore, we reviewed various approaches adopted by previous studies in developing heuristics with a view to adapting the most appropriate approach into the study.

2.1 Improving Cybersecurity Posture Usable Security

Research efforts to strengthen the human element in the cybersecurity and HCI domain have focused on improving system usability as a means of improving the cybersecurity posture of systems. While early usability research focused on improving usability for users, some studies on improving the usability of security mechanism for Developers and Systems Administrators have been published (Nielsen, 92, Zurko and Simon,1996, Adams and Sasse, 1999, Wijayarathna, and Arachchilage, 2019).

The Mobile phone interface provides customers access to Fintech solution. Mobile Phone Operating System (OS) developers such as Microsoft, Android and Apple have published user interface design guides to facilitate the usability of applications that run on mobile phones (Android, 2018, Apple, 2018). Rule of thumb; otherwise known as the 10 heuristics for usability have also been proposed on how to ensure the usability of a system by users amongst others; preventing errors from occurring right from system design, providing a mechanism for timely feedback and provide necessary help and documentation on systems (Nielsen, 1995). Various usability models have also been developed. For instance, Harrison et al. (2013) proposed a usability model that considered the unique characteristics of mobile devices. Moreover, how Usability is designed in relation to Security is also important. While both Usability and Security are important, the way they are built into a system determines whether the implemented controls would meet the intended objective. The buttress to this argument, is the analogy of user authentication, Ferreira et al. (2009) posited that without a password, a system is more usable, and conversely, an authentication mechanism that frequently requests revalidation while highly secure might be less usable.

Various approaches have been proposed on how to design systems that are both highly secure and usable. A study by Bai et al. (2017) on balancing Usability and Security in the use of encrypted emails explained that encryption was difficult to use because of poor interface design and difficulty in key management. Furthermore, the paper reported the finding of a study that gauged participants understanding and how they valued Usability and

Security trade-off in email encryption. Factors like privacy, ease of use and trust were observed to influence Usability and Security trade-off decisions. Also, Cranor and Buchler (2014) advocated considering Usability and Security together during the design. The opinion was that the end-user decision-making process does affect the balance between Usability and Security. They placed the onus on system designers to actively consider which decision requirements are assigned to end-users.

In a bid to improve Usability while minimizing threat scenarios, a study to analyse factors affecting both Security and Usability together was conducted (Kainda et al., 2010). The study proposed a Usability-Security threat model that identified factors to focus on when evaluating Usability and Security attributes. The study identified *Effectiveness, Satisfaction*, *Accuracy* and *Efficiency* as attributable factors that affect Usability only. It also identified *Attention*, *Vigilance*, *Conditioning*, *Motivation* and *Social Context* as factors affecting Security only. However, *Memorability* and *Knowledge* affect both Usability and Security (Kainda et al., 2010).

In addition to the Usability and Security approaches discussed, Faily and Iacob (2017) proposed the use of a tool to ensure Usable Security. Their paper explains that the proposed tool; CAIRIS (Computer Aided Integration of Requirements and Information Security), facilitates the Usability Security engineering activity by providing the capability for persona development and threat modelling.

2.2 Usable Security Evaluation

To answer the question of how Usable Security can be evaluated in Fintech and how it could be incorporated in the design phase of Fintech solutions, we examined peer-reviewed Usable Security literature from 2010-2020. While some notable studies on system usability have been conducted in earlier years (Nielsen, 92, Zurko and Simon,1996, Adams and Sasse, 1999), the choice of papers was made to coincide with Fintech evolution and Usable Security research conducted in that period.

In a study to improve the usability of security measures Feth and Polst (2019) developed a heuristics-based usability evaluation model together with a model of how to apply the heuristics. The paper opined that the choice for heuristics was due to the reason that hard metrics for security are quite rare and difficult to apply in practice. To ensure the heuristics are human-centred, the heuristics incorporated HCD design principles. The intended audience of the heuristics are Developers and Systems Administrators (Feth and Polst, 2019). Similarly, in a study to address issues of consent data privacy concerns in health information system in the context of the social network paradigm, heuristics were developed to evaluate Usable Security on the system (Yeratziotis et al., 2012). In the same vein, Alarif et al. (2017) proposed a heuristics-based framework for evaluating E-Banking Security and Usability made up of 13 categories and 160 metrics (Alarif et al., 2017).

While the studies we referenced in this section, examined Usable Security evaluation in domains like health, and financial services, others were more component specific. For instance, Realpe et al. (2016) examined the Usable Security of user authentication, Eskandari et al. (2018) examined Usable Security of bitcoin key management, Green and Smith (2016) examined the usability of security APIs for developers and Schryen et al. (2016) examined the usability of CAPTCHAs.

Usable Security evaluation in the reviewed literature was carried out in three ways; experts review, user review, or systems analysis. A combination of user and expert review was also proposed (Nurse et al., 2011).

The studies reveal that heuristics are the most used usability inspection method and help identify errors that could be costly to address. While assessment of heuristics is at times considered unreliable. It often reveals problems that might otherwise affect system security (Yeratziotis et al., 2012).

2.3 Heuristics Development

While no single approach exists for developing heuristics, table 1.0 provides a guide to steps taken to derive heuristics from.

Table 1.0: *Usable Security Elements*

#	Steps	References
1	Derive heuristics from literature	Yeratziotis et al. (2012)
2	Refine heuristics	Feth and Polst, (2019)
3	Categorize heuristics	Nurse el al. (2011)
4	Revise for completeness and add more heuristics	Jiménez et al. (2012)
5	Prioritize Heuristics	Quiñones and Rusu (2017)

Usable Security evaluation has been conducted in several domains; however, none exist for the Fintech domain. This study seeks to develop heuristics for Usable Security evaluation in Fintech by adapting research effort in other domains to improve the security posture of Fintech from the human element perspective, using mobile financial services as a case study. In addition to evaluating the usability of user interface design by heuristics principles, usability metrics also exist for that purpose. For instance, the System Usability Scale (SUS) and the Quality in Use Integrated Map (QUIM) have been used to measure the usability of user

interface design in specific application domains (Brooke,1996, Seffah et al., 2001, Sivaji et al., 2011).

The study also takes into cognisance existing frameworks and models for Usability and Security evaluation that can be leveraged to address risk identified by Open Web Application Security Project (OWASP) in a Fintech context (OWASP, 2016).

3. METHODOLOGY

The Usable Security heuristics for cybersecurity for Fintech was developed in three (3) iterations and validated by expert interviews. The first iteration was based on a survey of 698 Fintech users. The second iteration was based on a semi-structured interview of thirty-seven (37) participants, comprising Fintech solution providers and Bank Chief Information Officers (CIOs). The third Iteration was based on a thematic analysis of Usable Security evaluation papers published between 2010 to 2020 and an analysis of cybersecurity and Usable Security related framework and procedure. The heuristics developed as an outcome of these iterations were then validated through an interview of fourteen (14) cybersecurity and Usable Security experts.

3.1 Study Design

As described in section two (2), no single approach exists for developing heuristics. However, to ensure we address the major objective of this study which is leveraging human factor approaches to improve Usable Security in Fintech, we designed a study that considered the perspective of key stakeholders in the ecosystem, while taking cognisance of related efforts from literature and industry, this approach in addition to providing heuristics that would improve Usable Security, facilitates traceability from developed heuristics to practical problem it seeks to address. Table 2 provides an overview of the approach adopted in this study.

Table 2: *Study Approach*

Steps	**Study Method**	**Analysis Approach**	**Output**
Iteration 1	Survey of 698 fintech users	Principal Component Analysis	5 Usable Security Heuristics
Iteration 2	Semi-Structured interview of 37 fintech providers	Thematic Analysis Card sorting	5 Usable Security Heuristics
Iteration 3	Systematic Literature Review Document Analysis	Thematic Analysis	12 Usable Security Heuristics
Consolidated heuristics	Synthesized heuristics	Synthesis	Consolidated heuristics
Validation	Experts interview	ANOVA	Experts feedback on heuristics

3.2 Iteration 1: User Survey

The objective of the user survey was to gain understanding of observable and latent constructs that affect Usable Security for users of Fintech. To conduct this study, a survey instrument consisted of forty-three (43) questions. The questions consisted of thirty (30) Likert-type statements anchored by a five-point scale, ranging from 1 (‘‘strongly disagree” or “Never”) to 5 (‘‘strongly agree” or “always”). The remaining instrument constitutes twelve (12) multiple choice questions and one open-ended question.

The instrument was segmented into nine (9) sections for ease of administration. The questionnaire was then distributed both electronically and paper based. The electronic question was created using Bristol Online Survey (BOS), a survey tool made available by the university library of the authors, and circulated via email, and social media via WhatsApp and Facebook. Hard copies were distributed by hand to market placing targeting audience without social media presence. The study was aimed at Fintech users who use Mobile Financial Services solutions. The questionnaires were distributed to 1000 respondents in Nigeria. However, only 698 completed questionnaires were returned. Table 3 provides a summary of profile of survey participants.

Table 3: *User survey participants profile*

Age	%
18-24	20
25-34	35.6
35-44	36.7
45-60	6.7
= or > 61	1.0
Educational Qualification	%
Primary School Certificate	0.5
Secondary School Certificate	8.4
Diploma	12.3
Undergraduate Degree	42.7
Postgraduate Degree	35.2
Others	0.8
Monthly income	%
< = N 20,000	18.2
N 21,000 – N 50,000	15.6
N 51,000 - N 100,000	20.3
N 101,000 - N 250,000	23.4
N 251,000 - N 500,000	14.9
>= N 501,000	7.6

*1 US Dollars = 315 Nigerian Naira

Principal Component Analysis (PCA) was then conducted on the data collated from the survey to

identify elements central to Usable Security. In this research, PCA helped to expose latent variables not visible by using simple correlation techniques and cross-tabulation (Abdi and Williams, 2010).

3.3 Iteration 2: Study of Fintech Solution Providers and Bank CIOs

The objective of this study was to identify Usable Security elements that impact the practices of Fintech solution providers. Semi-structured interview participants are developers of Fintech and Bank CIOs. The recruitment process for the Developers was based on crowdsourcing from various online forums for Fintech solution providers and recommendations from financial services solution providers. Some participants were recruited from www.upwork.com, which provides the ability to filter and contact participants who met the set criteria. The website also provided verifiable evidence of past experiences of participants and their real identities. Sixty (60) participants were recruited but interviews were eventually conducted for twenty-two (22) participants. Four (4) of the participants were from the USA, Eight (8) from Asia, Seven (7) from Africa, two (2) from Europe and one (1) from the Middle East. The average years of experience for participants was eight (8) years. The most years of experience by any participant was fifteen (15) years, while the least number of years of experience by any participant was four (4) years. Irrespective of years of experience, participants have all worked on several successful Fintech projects. Ten (10) participants were Mobile Application Developers, six (6) were either Testers or Quality Assurance experts and three (3) had Governance related qualifications, like Project Management and Solution Architects. One (1) of the participants was a User Interface Design expert while two (2) were Business Relationship and Business Analysis experts. It should be noted that the skills mentioned above were primary expertise, as a number of the participants have played multiple roles in past projects.

The second group consisted of fifteen (15) Banking CIOs who have participated in the deployment of Mobile Financial Services making it a total of thirty-seven (37) participants for the study. The interviews were conducted over three (3) months.

Card sorting technique helped in arriving at the key factors that affect Usable Security from the perspective of the stakeholders (Nurmuliani, et al., 2004). Three (3) Information security experts conducted the card sorting exercise which culminated in the identification of Usable Security heuristics from the second iteration. An online tool UsabiliTest, (Usabilitest, 2018) was used to conduct the card sorting exercise, the tool provided a user-friendly graphic user interface for card sorting and allowed participants to choose between open, closed or hybrid card sorting options.

3.4 Iteration 3: Literature review

Iteration one (1) and two (2) revealed elements central to Usability and Security and threw up a question on how Usable Security is evaluated and designed. The 3rd iteration of the study was designed to answer the question.

The process included the development of a search strategy and six search strings. The literature search was conducted in the following sources: Sources: ACM Digital Library, USENIX, Science Direct, IEEE Explorer Digital Library, Scopus, Google Scholar, Springer, ResearchGate. Only peer-reviewed papers published in English language between 2010 to 2020 were in scope for the studies. Eighty-eight (88) peer-reviewed papers were identified from the search and analysed using Thematic Analysis. Analysis of Usable Security framework was also conducted as part of the process.

3.5 Consolidation and Validation of Heuristics

This paper adapted the approach presented by Yeratziotis et al. (2012) and Feth and Polst (2019) and integrated the findings from all three iterations, giving rise to a set of heuristics principles and their descriptions.

Twelve (12) heuristics principles together with descriptions and derived heuristics were subjected to expert validation. The validation was conducted in the form of a semi-structured interview. Thirty (30) experts were contacted however, at the end of the validation period fourteen (14) participants took part in the validation, four (4) of the participants are experts based on the USA, four (4) in Nigeria, four (4) in UK, one (1) in Italy and the last one in Lithuania. While six of the experts are cybersecurity experts, seven work in the Human Computer Interaction (HCI) domain and one works in both. Of the fourteen participants, four work in the Financial Services sector, two in the Health sector, one in the Payment industry space, one from the Defense, others from Academia and freelance.

To validate the heuristics, a semi-structured interview with four (4) sections and twenty-nine (29) questions were deployed. All the interviews were conducted virtually as it was conducted during the COVID-19 pandemic where physical contact was restricted.

4. RESULT

This study culminated in the development of twelve (12) Usable Security heuristics validated by experts. In addition to the heuristics, this section present findings from the studies leading to the development of the heuristics.

4.1 Iteration 1 Result

Principal Component Analysis (PCA) conducted on the data from the survey of 698 Fintech users indicated that out of the total number of respondents been analysed certain commonalities exist in 64% of them. The PCA also identified some observable components that when analysed in a correlation matrix exhibit certain correlations. Based on a comparison of the initial eigenvalues of the six (6) observable component, and extraction sums of square loadings, four (4) components explain 82.76% of the variation. An analysis of the PCA correlation matrix showed the relationship between the six (6) observable matrices. The analysis shows that Usability and Security have the highest positive correlation factor of 0.552, complexity variable has a negative correlation with both Usability (-0.302) and Security (-0.302). The coefficient of end-user privacy variable to Usability is 0.249 while the coefficient of end-user patching variable to security is 0.264. Furthermore, the relationship between the observable and latent factors was analysed using the model generated through the pattern matrix. The first latent component of the matrix loads heavily on Usability (0.869) and Security (0.841) but loads negatively on complexity (-.388). The second component loads positively on Patching and Complexity, while the third component loads only on Environment, while the last component loads heavily on Privacy and inversely on Complexity.

Based on PCA conducted on the data, five (5) heuristics were derived from the study as follows:

4.1.1 Complexity of System
The element addresses the complexity of security controls. While this was identified as a Usability attribute, participants believe addressing this will both improve Usability and Security. Furthermore, the study revealed that though the response from participants indicated that the system was not complex when the aggregate tasks that determine complexity were measured, the result showed the contrary.

4.1.2 Awareness of Privacy
Most participants indicated that they had more than an above-average knowledge of privacy. However, this differed in practice as participant phone use behaviours show a poor understanding of privacy. These participants store and use their logon credential in such a way that jeopardizes the security of their Fintech applications.

4.1.2 End-User patching
Lack of ensuring timely critical update poses a risk for Fintech users. While participants intuitively demonstrated a good habit of ensuring timely critical update on their devices, most are not aware of how this affects security.

4.1.3 Environmental Impact
While other factors results from direct user behaviour, this element measures the impact of factor external to the user and its impact on Usable Security. External factors like the environment of use might constitute a distraction to participants and has an impact on both Usability and Security of the system.

4.1.4 Usability and Security
Usability and Security are factors that have also been identified by participants to impact cybersecurity in Fintech. Furthermore, in ensuring a balance between Usability and Security in Fintech, our result show that Security concerns have more impact on trust than Usability concerns.

4.2 Iteration 2 Result

The heuristics derived from the first iteration were from the perspective of Fintech users, to ensure the final heuristics take cognisance of key stakeholders in the ecosystem, we conducted a second iteration of the study intending to identify more specific elements from the perspective of Fintech solution providers, that could further improve Usable Security in Fintech. To that effect, we conducted a semi-structured interview of Fintech solution development team (22) and bank Chief Information Officers (15), the rest of the section details the findings of the study.

Most development team members tend to play multiple roles. In one instance, a Developer was responsible for User Experience (UX) design, Security and Testing, in another instance a Developer was responsible for all processes from requirements gathering to documentation. While this might shorten development time, it might eliminate checks and balances that might have an impact on Usable Security of the final product. Furthermore, the study revealed that the level of awareness of stakeholders on Usable Security has an impact on how requirement for developing a solution are gathered. End-users are often not aware of what is technically and functionally feasible in securing a system before the development of the solution, as such depend on the development team to address security requirements in the system. However, users can provide input on how to improve usability when a prototype is made available.

Participants identify Agile as the predominant methodology used during the development of Fintech applications for mobile phones. Participants believe the Agile development method helps to achieve both Usability and Security objectives as it tends to reveal security loopholes at the early stages of development before it becomes expensive to correct. According to another participant, Agile provides for continuous interaction between clients and development team, facilitating the chances of

deploying an acceptable solution. Participants also agree that development methodology alone was not sufficient to guarantee Usable Security. To achieve Usable Security, both Usability and Security must be deliberately planned into the development process.

Though standard usability and threat scenarios were considered during design, there seemed to be no clear-cut documented usability needs or requirements from customers, Developers depend on business requirements specifications, which regards security as a non-functional requirement. Usability considerations mostly come to the fore during testing. Usability testing is consistently done by in-house teams representing user interest, typically with automated testing tools. In general, there seemed to be no defined approach or minimum expectation during testing. Participants noted that tests must not only be conducted on end-user facing Fintech applications but also on the back-end servers. As one participant puts it "*Mobile apps with financial nature depend heavily on the back-end processes to accomplish tasks, for instance, where a user requests for an Account Statement or transactions, the front-end mobile app must wait for results from the back-end processes to complete before displaying to the user, as such, testing the efficiency of the back-end processes is therefore paramount to the success of the mobile deployment*". However, participants believe testing back-end and ensuring its security is the responsibility of the financial services provider. While functionalities, layouts and user experiences were designed by the development team, they depend on whatever back-end security infrastructure exists.

In deploying Fintech, solution providers are expected to comply with standards and guidelines specified by regulators in addition to payment industry standards like the Payment Card Industry Data Security Standard (PCI DSS). Based on the interviews, it was observed that development teams are guided by various generic development standards, security standards and government regulations. Controls against non-compliance to existing standards include penalties like fines and being placed on the policy violation list. By far the most potent control for ensuring compliance to standards as identified by participants is the reputational risk to the solution provider due to lack of adherence to standards.

While most participants agree that based on experience, Usability and Security should be considered together at every phase of Fintech solution development and deployment, some participants thought otherwise. For instance, one participant believed that a trade-off between Usability and Security should not be the focus during the development of Fintech. The focus he said should be on minimizing the possibility of threat scenarios and maximizing the accessibility of usability scenarios, with more attention given to minimizing threat scenarios. Another participant suggested a risk-based approach whereby the tilt should depend on where the risk lies. The use of analytics to continuously refine Usability and Security was also suggested. Another participant believed that the development team should worry more about Security and allow the users to worry about Usability because no matter the effort developers put in ensuring the balance, users will always have the final say on what is truly usable.

4.2.1 Card Sorting Results

A thematic analysis of the semi-structured interview data revealed factors that affect Usable Security from the perspective of the participants. Using card sorting techniques, the factors were categorized by three (3) Information Security experts and presented herewith as Usable Security heuristics from supply-side stakeholders.

(i) Security and Usability: Eighty-Two (82) of the cards sorted identified security and usability as a factor that should be addressed to improve the security posture of Fintech. Thirty (30) of the eighty-two (82) cards were related to security assurance, fifteen to security, and the rest to usability.

(ii) Design: Participants believe system design is a very important element for improving Usable Security in Fintech. Twelve (12) of the cards identified design as a factor affecting Usable Security.

(iii) Communication: Communication and feedback in Fintech transaction affect user confidence and trust in the use of the solution. Thirteen (13) cards identified communication as an important Usable Security element for Fintech.

(iv) Quality: Quality relates to the correct elicitation and coding of user requirements and the testing of the solution based on these requirements. Eleven (11) of the cards identified quality as an important Usable Security element for Fintech.

(v) Operations and Infrastructure: Environmental factors outside the control of the user, but within the control of the solution providers have an impact on the security of the Fintech applications. Twenty-nine (29) cards identified this factor as an element.

4.3 Iteration 3 Result

The first two iterations identified Usable Security heuristics from the perspective of stakeholders in the system. This iteration examines existing work from other domains with a view for identifying elements

that can be applied to improve Usable Security in Fintech. Based on thematic analysis of Usable Security evaluation literature from 2010 to 2020, and an analysis of Usability and Security frameworks, the following heuristics were identified in Table 4.

Table 4: *Usable Security Elements*

#	Heuristic	Reference
1	Integrity	Gaehtgens et al. (2017) Feth and Polst (2019) Yeratziotis et al. (2012)
2	Proportionality	Feth and Polst (2019) Yeratziotis et al. (2012)
3	Transparency	Realpe et al. (2016) Feth and Polst (2019) Gaehtgens et al. (2017) Yeratziotis et. Al. (2012)
4	Empowerment	Alarifi et al. (2017) Melicher, et al. (2016) Feth and Polst (2019) Yeratziotis et al. (2012)
5	Identity	Gaehtgens et al. (2017) Feth and Polst (2019)
6	Reliability	Uzun et al. (2011) Alarifi et al. (2017) Hof (2015)
7	User Support	Feth and Polst (2019) Yeratziotis et al. (2012) Hof (2015)
8	Accessibility	Feth and Polst (2019) Hof (2015)
9	Authenticity	Yeratziotis et al. (2012) Khan (2015) Kainda, R., et al. (2010)
10	Compliance	Alarifi et al (2017)
11	Alignment	Hof (2015) Khan (2015)
12	Freedom	Hof (2015) Khan (2015)

4.3.1 Consolidate Heuristics Principle

This section presents a mapping of heuristics from the three () iterations. Usable Security as a factor from iteration one and two was not included as the entire heuristics is meant to address Usable Security. Table 5 shows Usable Security elements derived from the three iterations.

Table 5: *Usable Security Elements*

#	Iteration		
	One	**Two**	**Three**
1		Quality	Integrity
2	Complexity	Quality	Proportionality
3		Design	Transparency
4	Awareness of privacy		Empowerment
5			Identity
6	Environmental	-Design -Communication -Operations and Infrastructure	Reliability
7	-Awareness of privacy -Patching		User Support
8	Complexity		Accessibility
9			Authenticity
10			Compliance
11			Alignment
12			Freedom

The detail of the twelve (12) identified heuristics and their description is as shown below:

(i) **Integrity:**

This factor address controls against the unauthorized modification of transaction data. It consists of measures put in place for data protection.

- Derived heuristics:
  - *a) Protected area should be inaccessible to unauthorized users*
  - *b) System should automatically test and install the required software update without making the system more vulnerable or less usable*

(ii) **Proportionality:** Ensure security controls are proportionate to users' knowledge, time, transaction type and cognitive ability.

- *Derived heuristic:*
  - *a) System supports both novice and expert users*
  - *b) Users should be able to customize security to meet their individual preferences*

(iii) **Transparency:** Ensure security controls and practices are comprehensible, verifiable and accessible for the user.

- *Derived heuristics:*
  - *a) System security status should be obvious to use irrespective of knowledge of the security mechanism*

b) Users should be able to understand what security mechanism is active.

(iv) **Empowerment:** Enable users to express their systems security needs in the most efficient way

- *Derived heuristics:*

a) User should be able to customize security preferences

b) User should be able to reverse certain security choices.

(v) **Identity:** Ensure that users can be uniquely identified and verified with a high level of assurance

- *Derived heuristics:*

a) Authentication options designed in a way to keep the cognitive load of users low

(vi) **Reliability:** Ensure service consistency and functionality on facilitating effective communication and feedback for user transactions and security actions

- *Derived heuristics:*

a) The system should communicate error and transaction status to users in an understandable manner.

(vii) **User Support:** Ensure measures are put in place to support and educate users on the use of the system and security controls without additional cognitive workload on users.

- *Derive heuristics:*

a) Security operations should be easy to learn and apply irrespective of user cognitive ability.

b) Only relevant security information should be provided

(viii) **Accessibility:** Ensure the system and security control do not discriminate against any user

- *Derived heuristic:*

a) The security mechanism should have consideration for accessibility,

b) A visually impaired user should be able to differential a genuine from a rogue Fintech application

(ix) **Authenticity:** Ensure the system has valid certificates and the information should be available on the interface of use.

- *Derived heuristics:*

a) System should alert users when they are interacting with non-trustworthy sources

(x) **Compliance:** Ensure system and security control complies with extant policies, guidelines

- *Derived heuristics:*

a) Test conditions and scenarios should address compliance to extant policies and regulations

(xi) **Alignment:** Ensure security mechanisms aligns with the usual flow of user activities, mental model and cognitive ability

- *Derived heuristics:*

a) Security controls should not add to the cognitive workloads of the user

(xii) **Freedom:** Ensure security mechanisms guarantee a certain degree of freedom to users

- *Derived heuristics:*

a) Security control should not limit user option in the use of the application

4.4 Heuristics Validation

All fourteen (14) experts that participated in the validation of the heuristics agreed on the importance of all twelve (12) heuristics and provided feedback they believe would further strengthen the heuristics. This section provides results from the heuristics validation interview.

One expert suggested “Consistency” might be a better description of the heuristics currently labelled “*Integrity*” as also addresses consistency of transaction throughout its life cycle. An expert noted that *Proportionality* might be difficult to implement as a decision needs to be made as to whether it should be implemented as a dynamically aware system or coded into the system during the design phase. Affordance was suggested as a more suitable description for *User Support.* Experts noted that it was important to take care that end-users were not burdened with too much documentation as it would counteract the objective of Usability. Experts recommended that *Compliance* should be further decomposed to address contractual requirements, legal requirements and regulatory standards. Experts recommended the merging of *Integrity* and *Reliability* and *Authenticity* and *Iden tity*.

ANOVA was carried out to determine differences in the mean perception of respondents by country and sector. The perception was gauged for when the factors are used to evaluate Usable Security and when they are used as a guide to design Usable Security into the system. Response from four experts was deleted from the model because they did not complete this section of the questionnaire. Table 6 below shows the descriptive statistics of the model.

Table 6: *Descriptive Statistics*

Descriptives

		N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
						Lower Bound	Upper Bound		
Weighted_Evaluation	Nigeria	2	33.00	.00	.00	33.00	33.00	33.00	33.00
	UK	3	28.33	8.08	4.67	8.25	48.41	19.00	33.00
	US	4	33.25	.50	.25	32.45	34.05	33.00	34.00
	Lithuania	1	33.00	.	.	.	.	33.00	33.00
	Total	10	31.70	4.47	1.41	28.50	34.90	19.00	34.00
Weighted_Design	Nigeria	2	33.00	.00	.00	33.00	33.00	33.00	33.00
	UK	3	29.67	9.45	5.46	6.19	53.15	19.00	37.00
	US	4	37.00	2.94	1.47	32.32	41.68	33.00	40.00
	Lithuania	1	33.00	.	.	.	.	33.00	33.00
	Total	10	33.60	5.76	1.82	29.48	37.72	19.00	40.00

The model shows that the mean of Nigerian experts is thirty-three (33) with a standard deviation of zero (0) while UK experts have a standard deviation of 8, which shows a more divergent view, the value is smaller for US experts.

ANOVA test was conducted to test the statistical significance of the elements when used for evaluation and when applied to design.

Table 7 shows the detail of the ANOVA test conducted. The test shows that there was no statistically significant difference between groups was determined by one-way ANOVA ($F(3, 6) = 0.74$, $p = .565$). No statistically significant difference, in the perception of the respondent.

Table 7: *ANOVA*

		Sum of Squares	df	Mean Square	F	Sig.
Evaluation	Between Groups	48.68	3	16.23	.74	.565
	Within Groups	131.42	6	21.90		
	Total	180.10	9			
Design	Between Groups	93.73	3	31.24	.92	.488
	Within Groups	204.67	6	34.11		
	Total	298.40	9			

5. DISCUSION AND CONCLUSION

The Usable Security heuristic principles presented in this work seeks to improve the usability of security mechanisms in Fintech applications. The heuristics developed can be applied to evaluate the Usable Security of existing systems or as a guide to design Usable Security during Fintech application development. While heuristics are generally developed from existing literature, extensive work was conducted to develop heuristics from a sociotechnical perspective. The approach adopted facilitates heuristics traceability and reduce cybersecurity risk associated with the human element in the use of Fintech applications.

This study argued that cybersecurity issues still affect Fintech despite the availability of strong technical countermeasures. The proposed heuristics do not intend to replace existing technical countermeasures but make them more usable to end-users irrespective of their knowledge of the systems, security controls and physical ability.

The fourteen (14) experts that validated the heuristics all agree that the heuristics are apt in achieving the study objective but suggested that some of the elements could be merged, while the derived heuristics under each are retained. The experts also opined that the heuristics can be used in a Fintech sandbox process as criteria to ensure the Usable Security of the final product.

The suitability of the heuristics for evaluation of Fintech and design of Fintech solution was ascertained by participants. However, the level of importance was different for some element when used for evaluation compared to when used for design. Also, the view of the importance of each element was dependent on the domain of the evaluator, while HCI professionals tend to rank HCI related elements higher, security experts tend to rate security inclined elements higher. Irrespective of the level of priority given to the element by each group, they all emphasised the importance of all elements in the evaluation of Usable Security.

The development heuristics would be of benefit to Fintech Developers, Systems Auditors and Systems Administrators and end-users of Fintech solutions.

6. FUTURE WORK

This study has answered the research question of how to evaluate Usable Security in Fintech using a case study of mobile financial services, by developing twelve (12) Usable Security heuristics using an iterative approach that took cognisance of key players in the sociotechnical system.

Future work will involve using heuristics to evaluate Fintech solutions and compare them side by side with other usability heuristics. To determine how the heuristics will serve as a design guide, a hackathon will be organised where the heuristics principles will be used to guide development and then compared to existing development practices.

7 REFERENCES

Abdi, H. and Williams, L.J., (2010). Principal component analysis. Wiley interdisciplinary reviews: computational statistics, 2(4), pp.433-459.

Abdillah, L. (2019, December). An Overview of Indonesian Fintech Application. In The First International Conference on Communication, Information Technology and Youth Study (I-CITYS2019), Bayview Hotel Melaka, Melaka (Malacca), Malaysia.

Alarifi, A., Alsaleh, M., & Alomar, N. (2017). A model for evaluating the security and usability of e-banking platforms. *Computing*, *99*(5), 519-535.

Asli, D., Klapper, L., Singer D., Ansar, S. and Hess, J, (2018), The Global Findex Database 2017: Measuring Financial Inclusion and the Fintech Revolution. Washington, DC: World Bank. doi:10.1596/978-1-4648-1259-0. License: Creative Commons Attribution CC BY 3.0 IGO.

Android, (2018). Android user interface development beginners guide, 2018. http://index-of.es/Android/Android.User.Interface.Development.Beginner.Guide.pdf. (Retrieved 22nd March 2021)

Apple, (2018). Human Interface guidelines. https://developer.apple.com/ios/human-interface-guidelines/overview/themes/, (Retrieved 22nd March 2021)

Bai, W., Kim, D., Namara, M., Qian, Y., Kelley, P. G., & Mazurek, M. L. (2017). Balancing security and usability in encrypted email. *IEEE Internet Computing*, *21*(3), 30-38.

Borrett, A. (2021). Techmonitor, Covid-19 has increased cybersecurity risk to the fintech ecosystem, https://techmonitor.ai/technology/cybersecurity/cybersecurity-risk-fintech-ecosystem (Retrieved 26th April, 2021)

Brooke, J. (1996). others,"SUS-A quick and dirty usability scale," Usability Eval. *Ind*, *189*, 4-7.

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

Enhancing Financial Innovation and Access (EFInA), (2020) FinTech Landscape and Impact Assessment Study

Eskandari, S., Clark, J., Barrera, D., & Stobert, E. (2018). A first look at the usability of bitcoin key management. *arXiv preprint arXiv:1802.04351*.

Faily, S., & Iacob, C. (2017, September). 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.

Ferreira, A., Rusu, C., & Roncagliolo, S. (2009). Usability and Security patterns. In *2009 Second International Conferences on Advances in Computer-Human Interactions* (pp. 301-305). IEEE.

Feth, D., & Polst, S. (2019). Heuristics and models for evaluating the usability of security measures. In *Proceedings of Mensch und Computer 2019* (pp. 275-285).

Gaehtgens, F., Allan ,A., Zlotogorski, M., Buytendijk,F. (2017). Definition: Digital Trust. Gartner research Published: 24 May 2017 **ID:** G00329409.

Glenny, M., (2021). Financial Times, Pandemic accelerates growth in cybercrime. https://www.ft.com/content/49b81b4e-367a-4be1-b7d6166230abc398?desktop=true&segmentId=d8d3e364-5197-20eb-17cf-2437841d178a#myft:notification:instant-email:content (Retrieved 29th April, 2021)

Gorski, P. L., & Iacono, L. L. (2016). Towards the Usability Evaluation of Security APIs. In *HAISA* (pp. 252-265).

Green, M., & Smith, M. (2016). Developers are not the enemy!: The need for usable security apis. *IEEE Security & Privacy*, *14*(5), 40-46.

Hafenbrädl, S., Waeger, D., Marewski, J. N., & Gigerenzer, G. (2016). Applied decision making with fast-and-frugal heuristics. *Journal of Applied Research in Memory and Cognition*, *5*(2), 215-231.

Harrison, R., Flood, D., & Duce, D. (2013). Usability of mobile applications: literature review and rationale for a new usability model. *Journal of Interaction Science*, *1*(1), 1-16.

High M, (2021). Monzo, Revolut and more - the rise of UK fintechs, https://www.fintechmagazine.com/venture-capital/monzo-revolut-and-more-rise-uk-fintechs (retrieved 8th May, 2021)

Hof, H. J. (2015). User-centric IT security-how to design usable security mechanisms. *arXiv preprint arXiv:1506.07167*.

Hof, H. J. (2015). Towards enhanced usability of it security mechanisms-how to design usable it security mechanisms using the example of email encryption. *arXiv preprint arXiv:1506.06987*.

Jiménez, C., Rusu, C., Roncagliolo, S., Inostroza, R., & Rusu, V. (2012). Evaluating a methodology to establish usability heuristics. In *2012 31st International Conference of the Chilean Computer Science Society* (pp. 51-59). IEEE.

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

Khan, H., Hengartner, U., & Vogel, D. (2015). Usability and Security perceptions of implicit authentication: convenient, secure, sometimes annoying. In *Eleventh Symposium On Usable Privacy and Security ({SOUPS} 2015)* (pp. 225-239).

Mani V, (2019), Cybersecurity and Fintech at a Crossroads, ISACA Journal / Issues / 2019 / Volume 1

Melicher, W., Kurilova, D., Segreti, S. M., Kalvani, P., Shay, R., Ur, B.,and Mazurek, M. L. (2016). Usability and Security of text passwords on mobile devices. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems* (pp. 527-539).

Nielsen, J. (1992). Finding usability problems through heuristic evaluation. In *Proceedings of the SIGCHI conference on Human factors in computing systems* (pp. 373-380).

Nurmuliani, N., Zowghi, D., & Williams, S. P. (2004). Using card sorting technique to classify requirements change. In *Proceedings. 12th IEEE International Requirements Engineering Conference, 2004.* (pp. 240-248). IEEE.

Nurse, J. R., Creese, S., Goldsmith, M., & Lamberts, K. (2011). Guidelines for usable cybersecurity: Past and present. In *2011 third international workshop on cyberspace safety and security (CSS)* (pp. 21-26). IEEE.

OWASP Mobile Top 10, (2016) https://owasp.org/www-project-mobile-top-10/ (Retrieved 7th May, 2021)

Pfleeger, S. L., Sasse, M. A., & Furnham, A. (2014). From weakest link to security hero: Transforming staff security behavior. *Journal of Homeland Security and Emergency Management*, *11*(4), 489-510.

Quiñones, D., & Rusu, C. (2017). How to develop usability heuristics: A systematic literature review. *Computer standards & interfaces*, *53*, 89-122.

Realpe, P. C., Collazos, C. A., Hurtado, J., & Granollers, A. (2016). A set of heuristics for usable security and user authentication. In *Proceedings of the XVII International Conference on Human Computer Interaction* (pp. 1-8).

Saksonova, S., and Kuzmina-Merlino, I. (2017). Fintech as financial innovation–The possibilities and problems of implementation.

Sasse, M. A., Brostoff, S., & Weirich, D. (2001). Transforming the 'weakest link'—a human/computer interaction approach to usable and effective security. *BT technology journal*, *19*(3), 122-131.

Schryen, G., Wagner, G., & Schlegel, A. (2016). Development of two novel face-recognition CAPTCHAs: a security and usability study. *Computers & Security*, *60*, 95-116.

Seffah, A., Kececi, N., & Donyaee, M. (2001). QUIM: a framework for quantifying usability metrics in software quality models. In *Proceedings Second Asia-Pacific Conference on Quality Software* (pp. 311-318). IEEE.

Shetty M., (2018), Banks warn of new mobile malware, 232 banking apps in danger. https://timesofindia.indiatimes.com/business/india-business/banks-warn-of-new-mobile-malware/articleshow/62436145.cms. (Retrieved May 12, 2018).

Sivaji, A., Abdullah, A., & Downe, A. G. (2011). Usability testing methodology: Effectiveness of heuristic evaluation in E-government website development. In 2011 Fifth Asia Modelling Symposium (pp. 68-72). IEEE.

Usabilitest, (2018). https://www.usabilitest.com/. (Retrieved 31st August 2018)

Uzun, E., Saxena, N., & Kumar, A. (2011). Pairing devices for social interactions: a comparative usability evaluation. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 2315-2324).

West, R., Mayhorn, C., Hardee, J., & Mendel, J. (2009). The weakest link: A psychological perspective on why users make poor security decisions. In *Social and Human elements of information security: Emerging Trends and countermeasures* (pp. 43-60). IGI Global.

Wijayarathna, C., & Arachchilage, N. A. G. (2019). Why Johnny can't develop a secure application? A usability analysis of Java Secure Socket Extension API. *Computers & Security*, *80*, 54-73.

Yeratziotis, A., Pottas, D., & Van Greunen, D. (2012). A usable security heuristic evaluation for the online health social networking paradigm. *International Journal of Human-Computer Interaction*, *28*(10), 678-694.

Zurko, M. E., & Simon, R. T. (1996). User-centered security. In *Proceedings of the 1996 workshop on New security paradigms* (pp. 27-33).