Towards Usable Online Banking Security

Mathias Mujinga[1] and M.M. Eloff[2]
School of Computing
University of South Africa
South Africa
{[1]mujinm, [2]eloffmm}@unisa.ac.za

***Abstract*–Security technologies are making advances in protecting valuable information systems assets such as data and networks. Data centres can employ state-of-the-art cryptographic algorithms and networks can be protected by the most advanced firewalls. However, this is of no use if the users that these systems are intended to assist in their day-to-day work find them obstructive. This is a serious problem facing information security experts, because traditionally more attention was focused on the functionality of systems – especially security systems – with little or no consideration to the usability of such systems. Achieving total security is impossible, as security is a moving target. There are, however, noticeable advances in developing security technologies that enhance the functional aspects of a security system so as to mitigate the ever-increasing sophisticated threats that prevail in today's internet environment. The main challenge is getting the buy-in of users and embedding their behaviour in a real security culture where they take responsibility and show accountability. This task is extremely challenging and proving nearly impossible, since human behaviour cannot be predicted or guaranteed. This research-in-progress looks at highlighting and finding ways to improve the usability of online banking security systems. We will investigate the design principles and human capabilities in terms of the effort needed to use security systems securely.**

Keywords – Usability, Usable security, User experience

I. INTRODUCTION

Online security is a major concern for organisations as well as their clients who conduct business online. A number of studies found the lack of trust and perceived (security) risk to be major concerns for consumers making online purchases [1, 2, 6] and doing online banking. Achieving total security is impossible, as security is a moving target. There are, however, noticeable advances in developing security technologies that enhance the functional aspects of a security system so as to mitigate the ever-increasing sophisticated threats that prevail in today's internet environment. The main challenge is getting the buy-in of users and embedding their behaviour in a real security culture where they take responsibility and show accountability. This task is extremely challenging and proving nearly impossible, since human behaviour cannot be predicted or guaranteed.

II. PROBLEM STATEMENT

The software design of applications can go a long way in determining the usability of those applications. Design plays a major role in security applications, where security is not the primary production task. Flechais, Mascolo and Sasse [4] highlighted the importance of integrating security and usability with the requirements and design process. Furnell [5] found design flaws in the usability of security features in Microsoft Word and argued that it was difficult to discover these security tools. He also found no explanation of how they were used to achieve specific security goals. Research has since shown noticeable gains in shaping human behaviour through training and education. The latter can be complemented by taking the behaviour of users into account when designing and developing security systems. The limitations inherent in humans and identified by cognitive psychology must be recognised and taken into consideration.

This research is a work in progress. It looks at various aspects (identified from different research areas) of achieving the ultimate goal of designing usable security systems that users can embrace. It involves taking into account interface design principles and human capabilities when it comes to what the system demands from the users. This will help to reduce the tendency of users to bypass security merely because of the effort needed to comply with security mechanisms. The research tries to diminish the vulnerability of online users – both to old and new sophisticated online security threats – that are increasingly being developed and targeting these unsuspecting users. We examine the relationship between efforts being made to educate and make users aware of these threats and find out why the users are still vulnerable. We hypothesise that the technology developed for users to counter online security threats are not usable, hence users cannot use them effectively. This leads to the questions below.

III. RESEARCH DESIGN

The research question of this work rests on three axes – online banking, security and usability, as shown in Figure 1. The ultimate desirable position is to have online banking services that users can use with minimum effort and without errors, hence secure and usable online banking.

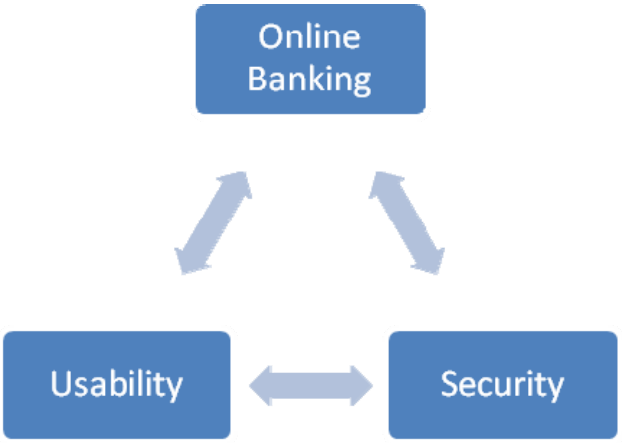

Figure 1. Three axes of secure online banking

Our research question is formulated as follows: *How usable is online banking security and can usable online banking security be secure?*

This question is expanded into the following research sub questions:

1. *Is there a security problem with online banking and to what extent?*
2. *Is the online security technology sufficient to mitigate security breaches?*
3. *Do human factors and usability issues compromise online security?*
4. *How can human behaviour be altered to mitigate online security threats?*
5. *What do consumers prefer – seamless or visible security?*

Research design is the roadmap of the entire research project that outlines choices to be made at each stage of the project. This section will go into details about how this research will be conducted; starting from the underlying philosophical assumptions, data collection and analysis techniques. We present the research design using the research 'onion' adapted from literature and breaks it down in accordance with the choices we make at each stage. Figure 2 depicts the research 'onion' [23] and our choices at each layer.

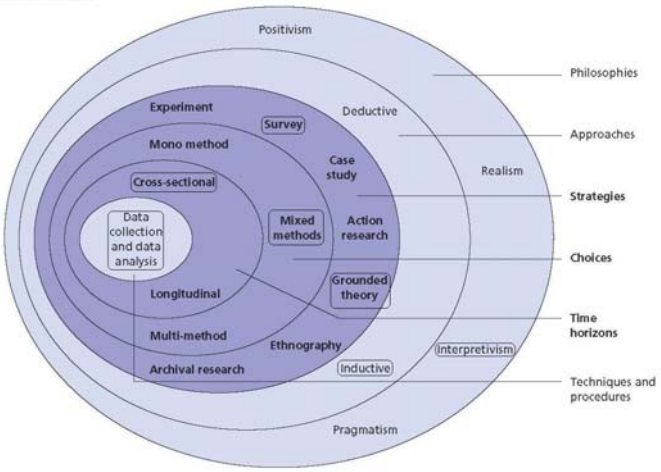

Figure 2. The research 'onion' (Saunders *et al.*, 2009)

IV. Philosophical Assumptions

This research adopts the interpretivist philosophical worldview on how knowledge is extracted. We will study the phenomenon of what influences the behaviour of users of online banking services and look at their interaction with online security technologies. Furthermore, we aim to investigate the design principles that the developers applied to these technologies and check if usability was considered.

Locke [7] described interpretive (and related constructivist) paradigms as having an interest in understanding the world of lived experience from the point of view of those who live it. Hence the concern was with a subjective reality. Researchers working in this paradigm focused on particular situated actors who they construed as composing meaning out of events and phenomena through prolonged processes of interaction that involved history, language and action.

The current research will adopt the inductive approach, whereby we do not start with any theory but develop one as we collect and analyse data. The deductive approach will also be used, but to a lesser extent.

V. Research Strategy

Our research strategies will be grounded theory (qualitative) and survey (quantitative). This will channel our research to follow a mixed-method approach, with qualitative research being more dominant. Grounded theory is a strategy of inquiry in which the researcher derives a general, abstract theory of a process, action, or interaction grounded in the views of participants. This process involves using multiple stages of data collection and the refinement and establishing of interrelationship of categories of information [8]. Glaser and Strauss [9] are regarded as the originators of grounded theory. In their 1967 publication they argued that researchers should strive not only to test theories but to discover new theories. Hence the book provides guidelines on the process of discovering new theories for sociologists. Two primary characteristics of this design are the constant comparison of data with emerging categories and the theoretical sampling of different groups to maximise the similarities of and differences between information [10].

The survey strategy is usually associated with the deductive approach. This allows you to collect quantitative data which you can analyse quantitatively using descriptive and inferential statistics. Questionnaires will be used to confirm or disapprove the findings obtained. We plan to question a representative sample of online banking users, and will correlate the findings with the heuristic evaluation findings by field experts.

VI. Methodology

Since we intend to use surveys and grounded theory, our reseach will be based on the mixed-method approach. According to Saunders *et al.* [6], this is the general term to describe when both quantitative and qualitative data collection techniques and analysis procedures are used in a research design. Mixed-method research uses both quantitative and qualitative data collection techniques and analysis procedures –either at the same time (parallel) or one after the other (sequentially), but it does not combine them.

The mixed-methods approach has advantages, such as bringing together the best of both methods, providing more evidence than either quantitative or qualitative research alone, and helping to answer questions that cannot be answered by either of the approaches alone. It provides a bridge across otherwise adversarial divides between quantitative and qualitative researchers, encourages the use of multiple worldviews or paradigms, and is practical since the researcher is free to use all methods possible to address a research problem [11].

This research will use a heuristic evaluation tool to perform a usability analysis. It will investigate the problem of online security usability from two perspectives, namely the designers or developers of security technology and the ultimate users of this technology. To get a complete picture of the research problem, we propose the use of mixed methods, so that one method will complement the other. We will collect data from both groups; in other words, the users' data will be collected using quantitative and qualitative data collection tools, while data from designers will be collected using qualitative tools only. The data from security designers will be used to determine whether the design process incorporates usability design principles and users' capabilities. Grounded theory will help this study to discover the underlying problems through direct contact with the social world being studied and it will momentarily put aside *a priori* theorising. This is not to say that core theories in the field of study will be ignored.

Another source of data in this study will be interviews and questionnaires. The interviews will be of a semi-structured as well as an unstructured format. According to Saunders *et al.* [6] the researcher has a list of themes and questions to be covered in semi-structured interviews, although these may vary from interview to interview. On the other hand, unstructured interviews are informal and are often used to explore in detail a general area in which the researcher is interested. These are often referred to as 'in-depth interviews'.

Our participants in conducting interviews will be banking security designers or developers. For the purposes of this study, this group will include information technology and communications (ICT) personnel, such as chief technology officers (CTO) and technicians. We intend to use questionnaires in the form of an online survey tool to collect data from online banking users.

VII. Scope and Limitations

The scope of our research will be limited to the usability of online banking security technology and we will use South Africa's four major banks to gather the relevant data. The study will develop a framework for usable online banking security by gathering data from two groups of online banking security participants, namely users and developers. This data will be used in conjunction with already researched design principles for usable security so as to come up with a framework as a proof of concept. The proof of concept will be evaluated by means of the usability inspection method of heuristic evaluation.

Heuristic evaluation is an informal method of usability analysis where a number of evaluators are presented with an interface design and asked to comment on it. This is done by looking at an interface and trying to come up with an opinion about what is good and bad about it [14]. Heuristic evaluation uses the following ten general principles for user interface design [13]:

1. Visibility of system status
2. Match between system and the real world
3. User control and freedom
4. Consistency and standards
5. Error prevention
6. Recognition rather than recall
7. Flexibility and efficiency of use
8. Aesthetic and minimalist design
9. Help for users to recognise, diagnose, and recover from errors
10. Help and documentation

The study will evaluate the framework against these principles as its baseline.

VIII. Usability

In 1990, usability was defined by the Institute of Electrical and Electronics Engineers (IEEE) as "the ease with which a user can learn to operate, prepare inputs for, and interpret outputs of a system or component" [15]. Later on, the International Standards Organization (ISO) developed two major categories of standards on usability, namely a product-oriented approach and a process-oriented approach. The process-oriented approach's definition of usability is "the extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use" [16]. Product-oriented usability was defined in [17] as "the capability of the software product to be understood, learned, used and attractive to the user, when used under specified conditions". In this context the attributes that a product requires for usability depend on the nature of the user, the task and the environment. For the purposes of this study we will use product-oriented usability. Usability is not a one-dimensional property of a user interface. In fact, Nielsen [12] defined usability in terms of five quality components: learnability, efficiency, memorability, errors and satisfaction

IX. Security Usability

Karat, Brodie and Karat [18] identified four unique aspects of Human-Computer Interaction (HCI) design that presents challenges and opportunities. Firstly, since security is not the main goal of users, they want it to be transparent and they still want to be in control of the situation. Secondly, security which is often designed with highly trained technical users in mind is now supposed to be used by a totally different type of user. Thirdly, usability is a bigger problem in security since complexity is at the heart of many security systems. Lastly, systems must be designed to allow easy and effective updates.

According to Sasse and Flechais [21], most users fail to display the required behaviour when using security. The following reasons are put forward for this view: users are unable to behave as required, or they simply do not want to behave in the way required. The impossible password demand in many standard security policies is an example of users being unable to behave as required. Sasse and Flechais [21] furthermore argued that some users fail to comply simply because the required behaviour is awkward, not because it is too difficult.

Security system design can go a long way to alleviate the 'human problem'. Security components of applications that are not primarily developed for security purposes are usually not placed on the forefront of the user interface [1]. Furnell also concluded that the security solutions that users need are mostly available but not easy to find and use. After being discovered, the functionality aspects have to be understood by the user through the user interface. Shneiderman and Plaisant [19] proposed eight 'golden rules' for interface design, namely strive for consistency; cater for universal usability; offer informative feedback; design dialogs to yield closure; prevent errors; permit easy reversal of actions; support internal locus of control, and reduce short-term memory load. Katsabas, Furnell and Dowland [20] suggested the preliminary guidelines below for which applications must follow so that effective and usable presentation of security functionality can be achieved:

- Provide visible system state and security functions.
- Ensure that security could be easily used.
- Make it suitable for advanced as well as first-time users.
- Avoid technical vocabulary or advanced terms.
- Handle errors appropriately; allow customisation without the risk of being trapped.
- Make it easy to set up security settings, suitable security help and documentation.
- Make the user feel protected – security should not reduce performance.

Along the same line, Sasse and Flechais [21] argued that security applications must be goal and task driven, since human behaviour is goal driven [20]. Hence, the effective and efficient execution of tasks, which helps the user to attain goals, is a key principle for the design of successful systems. This led Payne *et al*. [22] to conclude that *security tasks must be designed to support production tasks and they must not conflict with production tasks*. Users need to understand and accept the need for security and be motivated to comply with it so as to avoid the inclination to shortcut security [21]. Weirich and Sasse [23] identified the following beliefs and attitudes that are held by most users who fail to comply with security policies:

- Users do not believe they are personally at risk.
- Users do not believe they will be held accountable for not following security regulations.
- The behaviour required by security mechanisms conflicts with social norms.
- The behaviour required by security mechanisms conflicts with users' self-image.

Changing user behaviour is a multi-faceted task that inherently needs to take a number of aspects into consideration. These include human memory capabilities, user perceptions, organisational and personal goals and HCI design principles. Therefore the design of usable security systems is a task that needs the effort of people from disparate disciplines.

X. User Experience

Recently, designers of information systems have come to realise that usability alone does not guarantee the success of a product. The trend has been to design for user experience. User experience (UX) is the way a person feels about using a product, system or service. User experience highlights the experiential, affective, meaningful and valuable aspects of human-computer interaction and product ownership, but it also includes a person's perceptions of the practical aspects of a system, such as its utility, ease of use and efficiency. User experience is subjective in nature, because it is about an individual's feelings and thoughts about the system. User experience is also dynamic, because it changes over time as the circumstances change. We intend to incorporate some aspects of UX in our study.

XI. Related Work

Recently researchers started looking at the interaction of security and usability. Some research has been conducted looking at different aspects of the usable security phenomenon. The works range from evaluating specific security applications for usability to designing heuristics for usability evaluation. Below we provide brief critiques of some of these works.

Whitten and Tygar [24] conducted one of the first security usability tests by evaluating the usability of PGP 5.0, an encryption program. They did a cognitive walkthrough analysis together with a laboratory user test to evaluate whether PGP 5.0 can be successfully used by cryptography novices to achieve effective electronic mail security. The analysis revealed that the program had a number of user interface design flaws that rendered it unusable to novice users. A need was therefore identified to develop and apply user interface design principles and techniques for security. Whitten and Tygar's study forms the baseline for most usability studies.

AlZomai, AlFayyadh, Jøsang and McCullagh [25] conducted a study on the usability of transaction authorisation in online banking systems by looking at current authentications that involve re-authentication of users through out-of-band channels for each transaction. Assuming the reliability of the mobile telephone network and the vigilance of the user in checking the SMS before entering the OTP, this system is secure. However, the usability of the system becomes poor because the user is required to verify a number of such messages, due to the mental load required. The findings illustrate that a significant proportion of users do not carefully verify the OTP SMS messages before entering the authorisation code on the terminal. This implies that the method protects against certain attacks while still being vulnerable to other obvious attacks.

Casaló, Flavián and Guinalíu [26] analysed the influence that perceived web site security and privacy, usability and reputation have on consumer trust in the context of online banking. They described the positive effects of security and

privacy, usability and reputation on consumer trust in a web site in the online banking context. While this study analysed web site security and privacy, usability and reputation, as well as their perceived impact on consumer trust, our study will concentrate at the usability of the security mechanisms used on these websites in the context of online banking.

One area of concern for usability in security is password complexity. Simple passwords are highly usable to users because they are easy to remember but also very insecure since they can be cracked in seconds. Extensive research work done in this area has mostly focused on password usability, with some works suggesting image-based authentication methods.

XII. Conclusion and Contribution

Understanding why users overlook security mechanisms will not only help in the formulation and enforcement of security policies, but also contribute to the design of such security technologies. A healthy security culture can be created by taking into consideration human aspects that make it difficult for users to comply with security requirements. The eventual expected outcome of the present research is a framework for the design of usable online banking security. Such a framework will incorporate design principles for usable online security and will be tested using the heuristic evaluation method.

References

[1] C. M. K. Cheung, L. Zhu, T. Kwong, G. W. W. Chan and M. Limayem, "Online consumer behavior: A review and agenda for future research," in *Proceedings of the 16th Bled eCommerce Conference, Bled,* 2003, pp. 9-11.

[2] A. M. Aladwani, "Online banking: a field study of drivers, development challenges, and expectations," Int. J. Inf. Manage., vol. 21, pp. 213-225, 2001.

[3] M. Sathye, "Adoption of Internet banking by Australian consumers: an empirical investigation," *International Journal of Bank Marketing,* vol. 17, pp. 324-334, 1999.

[4] I. Flechais, C. Mascolo and M. A. Sasse, "Integrating security and usability into the requirements and design process," *International Journal of Electronic Security and Digital Forensics,* vol. 1, pp. 12-26, 2007.

[5] S. Furnell, "Why users cannot use security," *Comput. Secur.,* vol. 24, pp. 274-279, 2005.

[6] M. Saunders, P. Lewis and A. Thornhill, *Research Methods for Business Students.* Prentice Hall, 2009.

[7] K. D. Locke, *Grounded Theory in Management Research.* SAGE Publications Ltd, 2001.

[8] K. Charmaz, *Constructing Grounded Theory: A Practical Guide through Qualitative Analysis.* USA: Sage Publications, Inc., 2006.

[9] B. G. Glaser, A. L. Strauss and E. Strutzel, "The discovery of grounded theory; strategies for qualitative research," *Nurs. Res.,* vol. 17, pp. 364, 1968.

[10] J. W. Creswell, *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches.* USA: Sage Publications, Inc, 2009.

[11] J. W. Creswell and V. L. P. Clark, *Designing and Conducting Mixed Methods Research.* USA: Sage Publications, Inc, 2011.

[12] J. Nielsen, *Usability Engineering.* Morgan Kaufmann, 1993.

[13] J. Nielsen, "Ten usability heuristics," *Useit.Com,* 1990.

[14] J. Nielsen and R. Molich, "Heuristic evaluation of user interfaces," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems: Empowering People,* 1990, pp. 249-256.

[15] IEEE Std 610.12, "IEEE Standard Glossary of Software Engineering Terminology," vol. 121990, 1990.

[16] ISO 9241-11, "Ergonomic requirements for office work with visual display terminals (VDTs): Guidance on usability," *ISO Standards,* 1998.

[17] ISO/IEC 9126-1, "Software Engineering - Product Quality - Part 1: Quality Model," *ISO,* 2001.

[18] C. M. Karat, C. Brodie and J. Karat, "Usability design and evaluation for privacy and security solutions," in *Security and Usability: Designing Secure Systems that People can use*, L. F. Cranor and S. Garfinkel, Eds. USA: O'Reilly Media Inc., 2005, pp. 47 - 74.

[19] B. Shneiderman and C. Plaisant, *Designing the User Interface: Strategies for Effective Human-Computer Interaction.* USA: Pearson Education, 2010.

[20] D. Katsabas, S. Furnell and P. Dowland, "Using Human Computer Interaction principles to promote usable security," 2005.

[21] M. A. Sasse and I. Flechais, "Usable security," in *Security and Usability: Designing Secure Systems that People can use*, L. F. Cranor and S. Garfinkel, Eds. USA: O'Reilly Media Inc., 2005, pp. 13 - 30.

[22] S. C. Payne, S. S. Youngcourt and J. M. Beaubien, "A meta-analytic examination of the goal orientation nomological net." *J. Appl. Psychol.,* vol. 92, pp. 128, 2007.

[23] D. Weirich and M. A. Sasse, "Pretty good persuasion: A first step towards effective password security in the real world," in *Proceedings of the 2001 Workshop on New Security Paradigms,* 2001, pp. 137-143.

[24] A. Whitten and J. D. Tygar, "Why johnny can't encrypt: A usability evaluation of PGP 5.0," in *Proceedings of the 8th USENIX Security Symposium,* 1999, pp. 169–184.

[25] M. AlZomai, B. AlFayyadh, A. Jøsang and A. McCullagh, "An exprimental investigation of the usability of transaction

authorization in online bank security systems," in *Proceedings of the Sixth Australasian Conference on Information Security-Volume 81*, 2008, pp. 65-73.

[26] L. V. Casaló, C. Flavián and M. Guinalíu, "The role of security, privacy, usability and reputation in the development of online banking," *Online Information Review*, vol. 31, pp. 583-603, 2007.