Human-Computer Interaction for Security Research: The Case of EU E-Banking Systems

Caroline Moeckel

Human-Computer Interaction for Security Research: The Case of EU E-Banking Systems

Caroline Moeckel, supervised by Xristine Faulkner

Faculty of Business, Department of Informatics
London South Bank University
103 Borough Road, London, SE1 0AA, UK
{moeckelc, xristine}@lsbu.ac.uk

Research Area. Human-Computer Interaction for Security (E-Banking)

Brief Description. This short paper highlights the interaction between security and usability in e-banking security and presents objectives and difficulties for studies in this field.

1 The Role of Security and Usability in Current EU E-Banking

E-Banking has undoubtedly become a key element in every modern bank's service portfolio during the last two decades. With its initial focus primarily on transactions, e-banking has now progressed towards an advanced online sales channel for financial products and most of today's e-banking platforms will be able to reproduce almost all services offered in bank branches [1]. But not only the strategic and commercial sides of e-banking have developed very far, also the e-banking security countermeasures employed have passed through several development stages, e.g. from simple password systems to sophisticated two-factor authentication approaches [4].

While the described innovation should generally be viewed as a positive one, current e-banking systems still show large failings in terms of their security and usability. These weaknesses are for example evident in a persistently high number of fraud cases for online banking, accounting for £46.7 million in 2010 (2009: £59.7, 2008: £52.5 [2]) solely in the UK [3]. The risk posed by banking fraud may also lead to a growing negative public perception or fear shown by customers. Alongside these security issues, some severe usability drawbacks can be observed in modern e-banking systems. While some of these may be related to the actual user interface design, a range of problems arise at system stages such as registration or business continuity. System lock outs or erroneously blocked transactions, like Barclaycard's fraud detection system flagging payments for London 2012 Olympic tickets as suspicious and declining them, are incomprehensible and frustrating to users. There are a range of similar cases, such as mentioned in [5] where card reader usability impedes security or in [6] where users prefer less secure solutions due to their apparently higher usability.

Security problems in this context may lead to substantial monetary losses or damage to reputation. However, usability shortcomings may also result in higher operational costs, for example when additional customer support is required through call centres or customers stop using the e-banking functions offered and revert to branch-based services. Furthermore, customers may prefer other financial institutions if their e-banking system seems to be more usable, e.g. if the bank forces the user to purchase a certain type of card reader. Due to the relative importance of e-banking for financial online product sales [1], usability may also directly affect revenue.

Considering the impact of security and usability as well as the examples and fraud statistics mentioned, the difficulty of combining the roles of security and usability in the context of e-banking becomes obvious. Although modern e-banking systems certainly provide sufficient protection levels and fulfil most functions expected from an internet-based bank branch, there is still a significant potential for improvement in the field of usable security. While the best possible protection against potential attacks and mitigation of threats is desirable from a security point of view, the proposed solution still has to be as usable as possible, which may ultimately require accepting a trade-off in security [7]. A range of security and usability problems in e-banking systems can be attributed to a conceptual mismatch of threats and countermeasures within the individual system - either at the cost of security when threats are not mitigated adequately by the employed countermeasures or at the cost of usability due to overly strict, hindering security measures not in line with the level of risk encountered. In addition, usability is often viewed as a separate entity and not considered at every stage of development, which may ultimately lead to decreased security or usability levels. Factoring in risk is crucial at this point as the risk level willingly accepted by a bank will influence the selection and design of their security countermeasures. Accepting certain calculated risks in this context may also be of benefit for usability, for example when allowing users to view their account balance after login in with a username-password combination and only enforcing complex security measures for higher-risk services such as transactions. Viewing security and usability purely as antagonists would be too one-dimensional [8], it is their interaction that needs to be understood and further defined for improving e-banking security.

There is a high degree of freedom in selecting countermeasures and designing systems in the context of e-banking and only a limited amount of regulatory guidelines on the issue. This is also underpinned by a large variation of different e-banking security systems currently observed across the European Union (EU) [1]. Although financial institutions are protecting themselves and their customers against a common global threat landscape, the systems currently in existence in the EU vary in terms of countermeasures employed and their respective usability.

Banks as well as academic researchers would therefore greatly benefit from more insights into the relationship between usability and security in the context of e-banking, particularly if these results could be translated into guidance applicable to real-world systems. Research in the area of usable security is generally limited due to the relative youth of the discipline [8]. In addition, there have been no academic or commercial efforts to create a comprehensive overview of the current e-banking security landscape in the European Union.

2 Benefits and Objectives of Research in the Field

To enhance usability in e-banking security, overcome current usability or security flaws and to ultimately improve e-banking systems, the understanding of the relationship between security and usability in this context needs to be further deepened, formalised and related to a real-world context. A lack of dedicated research methods for the field of usable security as well as the highly diverse sample of e-banking security solutions with different levels of security and usability in the current EU banking landscape indicate the potentially high value of a study in this area.

For research in this field, the following three main objectives can be identified:

1. creating a comprehensive overview and categorisation of e-banking security systems currently in real-world use throughout the EU,
2. understanding the relationship between security and usability in the context of e-banking as well as the potential influence of other factors such as cost and
3. extending the knowledge in the field of research methods for usable security as well as threat modelling with an applied example (e-banking).

3 Research Methods for Usable Security in E-Banking

For the case of security research, it needs to be understood that most organisations will not allow external researchers to access all details related to their security policies, specific solutions or products. This applies particularly to the very secretive banking sector, where publicised security flaws can translate into substantial financial losses, decreased trust or reputational problems. The expectation to work with real-world data on security within the organisation, e.g. number of security breaches encountered, investment on e-banking security or plans for future implementations, is therefore not entirely realistic. Ways to overcome this difficulty include using system analysis, e.g. of e-banking applications, customer or employee interviews and questionnaires or using data collected by professional or governmental organisations.

Secondly, research methods in the field of usable security have not fully matured yet and while various key publications [7] [8] in the area have hinted towards certain approaches such as threat modelling [9][10] or user testing, these need to be extended further and tested in various applied contexts. It is argued here that current usability evaluation methods do not fully account for the special nature of secure applications and software. This applies in particular for the example of e-banking, where a highly secure infrastructure has to provide simultaneously a high level of usability to its large number of non-expert users. This view is supported by key materials in this area, which criticise the adoption of usability methods by researchers in human-computer interaction for security (HCISec). Kainda et al. [7] notes that “the extent to which these apply to the field of HCISec is arguable given the fine balance between improving the ease of use of a secure system and potentially weakening its security”. Additionally, Cranor et al. [8] highlight the importance of “contextual information [...] in assessing the cost of the countermeasure to the system as a whole—this

includes financial, organizational, and user costs". This is by no means to say that usability evaluation methods should not be employed in a security context, since they may be beneficial through improving users' effectiveness, efficiency or satisfaction, but hints towards an integration of threats and vulnerabilities and surrounding factors.

4 Original Contribution and Future Work

A number of innovation factors valuable to banks will be included in this study. A framework for evaluating existent and future implementations of e-banking security will be devised for practical employment. Furthermore, the bank's position with all its related challenges will be taken into account rather than assessing the situation in a theoretical, unrealistic environment. In contrast to earlier studies, the interplay of security and usability without a separation of factors will be analysed, enabling the bank to understand the effects of changes in security or usability. In addition to introducing a new focus of user-centered design to e-banking security, this study will also give a detailed overview of the status of EU e-banking security.

Future work in this area could include exploring the mismatch between the customer's and the bank's perspective on e-banking security, further examining the data collected on e-banking security in Europe, learning more about the internal reasons that banks prefer certain countermeasures over others as well developing usability evaluation models specific to e-banking security.

References

1. Moeckel, C.: EU B2C E-Commerce in the Banking Sector. Diplomica, Hamburg (2008)
2. Financial Fraud Action UK: Fraud the Facts 2010, http://www.financialfraudaction.org.uk
3. UK Cards Association.: Fraud losses drop on UK card, cheques and online banking (March 2011), http://www.theukcardsassociation.org.uk/media_centre/press_releases_new/page/1323
4. Borchert, B.: Online-Banking Verfahren, http://www-ti.informatik.uni-tuebingen.de/~borchert/Troja/Online-Banking.shtml
5. Drimer, S., Murdoch, S.J., Anderson, R.J: Optimised to Fail: Card Readers for Online Banking. LNCS, vol. 5628, pp. 184-200. Springer, Heidelberg (2009)
6. Weir, C., Douglas, G., Richardson, T., and Jack, M. (2010). Usable security: User preferences for authentication methods in eBanking and the effects of experience. Interacting with Computers, vol. 22(3), pp. 153-164. Elsevier, New York (2010)
7. Kainda, R., Flechais, I. and Roscoe, A.W.: Security and usability: analysis and evaluation. In: 5th International Conference on Availability, Reliability and Security, pp. 275–282. IEEE Press, New York (2010)
8. Cranor, L.F. and Garfinkel, S.: Security and Usability - Designing Secure Systems That People Can Use. O'Reilly, Sebastopol, CA (2005)
9. Moeckel, C. and Abdallah, A.E.: Threat Modeling Approaches and Tools for Securing Architectural Designs of an E-Banking Application. In: 6th International Conference in Information Assurance and Security, pp.149. IEEE Press, New York (2010)
10. Moeckel, C. and Abdallah, A.E.: Understanding the Value and Potential of Threat Modeling for Application Security Design: An E-banking Case Study. In: Journal of Information Assurance and Security, vol. 6(4) [to appear]. Dynamic, Atlanta, GA (2011)