Researching Sensitive HCI Aspects in Information Security: Experiences from Financial Services

Caroline Moeckel
Information Security Group
Royal Holloway, University of London
Egham Hill, Egham TW20 0EX
caroline.moeckel.2012@ live.rhul.ac.uk

ABSTRACT

Information security practitioners are tasked with protecting their organisation's assets and information – a sensitive area of work, especially in heavily regulated or critical infrastructure industries. Working directly with these individuals to learn more about HCI patterns and behaviours they display can be insightful, but not without challenges due to the perceived risk from sharing information involved. Ultimately, any public information may prove useful to potential attackers and actual risks can be difficult to quantify. This short position paper provides an introduction to the field before informally describing a number of experiences and observations made when working with financial services information security practitioners in a limited number of studies. This is followed by an indication of challenges and opportunities in this area to help enable potential discussions with other researchers and lastly a brief summary.

CHI'19 Extended Abstracts, May 4-9, 2019, Glasgow, Scotland, UK.

Sensitive Research, Practice, and Design in HCI Workshop 5 May, 2019

KEYWORDS

HCI; Sensitive Research; Information Security; HCISec; Usable Security; Financial Services

Common research themes
in HCISec and Usable Security
(based on [3])

- Realigning usability and security, e.g. human factors and user-centred design in security
- Authentication mechanisms, e.g. passwords or biometrics
- Secure systems, e.g. secure interaction design (for example to help prevent Phishing attacks)
- Privacy and anonymity systems, e.g. privacy issues in HCI and human-centred privacy
- Commercial approaches to usability and security experiences
- Research efforts in areas outside of usability and security touching on these areas or earlier works helping to define this discipline

BACKGROUND

Information security, its principles and processes aim to protect the confidentiality, integrity and availability of information. Learning about how humans operate in this space, whether in their private life or as an employee in an organisation, has been of interest to academic communities such as HCISec and Usable Security researchers, with dedicated conferences such as the Symposium on Usable Privacy and Security (SOUPS) [7] long in existence and traditional HCI conferences explicitly inviting submissions in this area (e.g. for Interact 2019 [4]).

Past research efforts in the area have addressed a multitude of topics (refer also to left column), ranging from usability studies of secure applications and systems, privacy concerns, evaluations of passwords and authentication solutions, user perspectives on security and usage of human-centred design and HCI methods in security – an excellent primer to the field is provided in 'Security and Usability - Designing Secure Systems that People Can Use' edited by Garfinkel and Cranor [3].

While many of these examples follow well-established routes and best practices in HCI research with a specific application to the field of information security, some HCI research for security can be identified as particularly sensitive and problematic in regard to ethical approval processes, ability to recruit participants and ultimately ways of publication. Although by no means a complete list of these affected areas of research, a few areas can be used as an example in this context. In-the-wild field studies, where security researchers simulate a realistic (but harmless) attack and usually deceive the participants about the real purpose behind the situation to learn more about the participant's behaviour in response to the attack, can be included here [6]. Although widely used and encouraged by the security community, purposeful vulnerability disclosure seems to carry a number of ethical challenges [5], with anecdotal evidence even hinting at assault against commercial security researchers after exposing security flaws [2].

Further to these examples, working directly with security practitioners in organisations around the topics of HCI and security may pose methodological challenges: from recruiting suitable participants, evaluating the risk of publication to ultimately gaining approval from both organisational side and academic institution. While some excellent examples of such research efforts exist as discussed in [1] for example, no best practice guidance and reference materials seem to be available at this point in time. This difficulty may be amplified for critical infrastructure sectors such as public health or telecommunications as well as heavily regulated industries such as financial services or pharmaceutical manufacturing.

Following this introduction and background section, a brief review of own past experiences in the field both as a researcher and participant is presented in this short position paper. This is intended to form a tangible and accessible discussion basis with other workshop participants, but also to potentially help shape practical recommendations and theoretical ideas for future research directions. Initial opportunities for next steps are included towards the end of this document as is a short summary with key take-away points.

EXPERIENCES FROM FINANCIAL SERVICES

This section provides a brief reflection with key experiences and observations made when working with a number of financial services practitioners (<20, manager/executive level) in two separate studies (a security persona set evaluation focus group and separate semi-structured interviews human/attacker-centric security) carried out last year (2018) to be shared with other workshop participants. This is supplemented by own past experiences and observations as a participant in financial services usability studies and other HCI concept studies. While limited in scale and hence expressiveness at this point in time, it would be interesting to discuss and compare these observations with others – it is also hoped that this will help prepare for guiding future research or lead to the production of best practice recommendations for similar studies if at all feasible.

As a researcher

For the limited examples mentioned, the following experiences and observations can be noted in this context:

- Generally, financial services security practitioners were passionate, seemed keen to talk about their ways of working and were willing to comment on prototypes/research examples.
- However, there was a relatively high drop-out rate with some participants ultimately not agreeing to have their data used for research/publication (10-15% of initial participants).
- Employees at analyst or assistant level seemed more reluctant to take part from the start or ended participation early (risk perception?).
- Sign-off via email for gathered data and insights to be used in publication seem to work well for this audience and satisfy the need for risk management from their side. An objective risk assessment seemed difficult for the researcher in this position.
- Recruitment of participants from financial start-up companies rather than established financial services organisations proved difficult.

As a participant

For the limited examples mentioned, the following experiences and observations can be noted in this context:

- Often, testing seems to be technically difficult and complex to set up (e.g. new mobile concepts and prototypes), but amount of resulting data and analysis may be limited.
- No dedicated risk assessment seemed to have been undertaken or had been provided to participants before start of the study/experiment.

- Risks or potential outcomes to the study did not seem to play a major role or were not shared with participants.
- There seems to be high levels of informal/ad-hoc studies (via e.g. short surveys), whereas larger scale external studies involving customers would be managed through a third-party handling recruitment and taking care of legal aspects (for commercial HCI studies in financial services).
- Email seems to be the preferred medium to share participant information and follow-up once the study had been completed (comfort vs need for evidence).

CHALLENGES & OPPORTUNITIES: WHERE TO NEXT?

From this small sample of cases and related observations, several challenges can be highlighted and potentially warrant further discussion. Provided the sensitive nature of information security in a large financial services organisation, the current treatment and presentation of risk requires further enquiry – at this point, it is indicated that recruitment and participation rates may be hindered, but there may also be a wider impact on ethical and legal aspects of research. Another challenge to overcome seems to be the ability to recruit participants from non-traditional, new entrants to the market – it is unclear whether risk perception plays a role in this context, but it could be that for these organisations, the risk of giving away potentially sensitive information outweighs potential benefits.

On the other hand, there are already some aspects and practices that seem to work for this particular setting of information security and financial services. Using email communications and exact sign-off procedures for the results to be published seems to work well to reduce perceived risks. Overall, given the sensitive area of work these practitioners carry out, the level of engagement was encouraging and pro-research, which is likely to originate from the research-driven culture found in information security.

SUMMARY

While working directly with information security practitioners in heavily regulated industries such as financial services can be hugely rewarding and insightful, considering present challenges may help to improve research practice in the field. Whether it is a more proactive perspective on risk, strengthening current best practices or learning from other subject areas, there seem to be several opportunities and routes to develop and progress from here. Discussing common and similar challenges, but also different perspectives and opposite opinions, with other workshop participants would serve as an excellent starting point for moving towards positive changes in practical research involving information security practitioners in e.g. financial services.

REFERENCES

[1] Louise Axon, Bushra Alahmadi, Jason R. C. Nurse, Michael Goldsmith and Sadie Creese. 2018. Sonification in Security Operations Centres: What do Security Practitioners Think? In *Proceedings of 2018 Workshop on Usable Security (USEC) at Network and Distributed System Security Symposium (NDSS*). https://www.cs.ox.ac.uk/files/9802/2018-USEC-NDSS-aangc-preprint.pdf.

[2] Guise Bule. 2019. Researcher Assaulted by a Vendor After Disclosing a Vulnerability. https://www.secjuice.com/security-researcher-assaulted-ice-atrient/

[3] Simson Garfinkel, Lorrie Cranor. 2008. Security and Usability - Designing Secure Systems that People Can Use. O'Reilly Media.

[4] International Conference on Human-Computer Interaction (INTERACT). https://interact2019.org.

[5] Andrea M. Matwyshyn, Ang Cui, Angelos D. Keromytis, Salvatore J. Stolfo. 2010. Ethics in security vulnerability research. IEEE Security & Privacy, Volume 8, Issue 2, March-April 2010. DOI: 10.1109/MSP.2010.67.

[6] Rasha Salah El-Din. 2012. To Deceive or Not to Deceive! Ethical Questions in Phishing Research. In *Proceedings of BCS HCI 2012 Workshops, HCI Research in Sensitive Contexts: Ethical Considerations*. https://ewic.bcs.org/upload/pdf/ewic_hci12_ec_paper2.pdf.

[7] Symposium on Usable Privacy and Security (SOUPS). https://www.usenix.org/conference/soups2019.