PhD-FHSE-2021-029
The Faculty of Humanities, Education and Social Sciences

DISSERTATION

Defence held on 21/09/2021 in Esch-sur-Alzette

to obtain the degree of

DOCTEUR DE L'UNIVERSITÉ DU LUXEMBOURG

EN PSYCHOLOGIE

by

Verena DISTLER

THE EXPERIENCE OF SECURITY IN HUMAN-COMPUTER INTERACTIONS: UNDERSTANDING SECURITY PERCEPTIONS THROUGH THE CONCEPT OF USER EXPERIENCE

Dissertation defence committee

Dr Vincent KOENIG, dissertation supervisor
Professor, University of Luxembourg

Dr Katharina KROMBHOLZ
Professor, CISPA Helmholtz Center for Information Security

Dr Gabriele LENZINI, Chair
Professor, University of Luxembourg

Dr Florian ALT
Professor, Bundeswehr University Munich

Dr Carine LALLEMAND, Vice Chair
Research Scientist, University of Luxembourg
Assistant Professor, Eindhoven University of Technology

The Experience of Security in Human-Computer Interactions: Understanding Security Perceptions Through the Concept of User Experience

Verena Distler

Abstract

In traditional interactions that do not rely on technology, most people are able to assess risks to their privacy and security and understand how to mitigate these risks. However, risk assessment and mitigation is more challenging when interacting with technology, and people's perceptions of security and privacy risks are not always aligned with reality. It is important for those who design technologies to understand how people perceive the security of technologies in order to avoid having their designs contribute to erroneous perceptions. Instead, interactions with technology should be deliberately designed to ensure that people do not over- or underestimate the security provided by the system.

This dissertation contributes to a better understanding of users' perceptions of security in human-computer interactions. It investigates which factors induce a perception of security and privacy risks and how user-centered design can influence these factors to deliberately design for or against perceived security.

I use a mixed-methods approach to address these objectives, including a systematic literature review, empirical data collection with focus groups, expert co-creation sessions, user tests in a controlled environment and a quantitative survey experiment.

The first research objective is to analyze how security and privacy researchers induce a perception of security and privacy risks with research participants. We conducted a systematic literature review and focused our analysis on study methods; risk representation; the use of prototypes, scenarios, and educational interventions; the use of deception to simulate risk; and types of participants. We discuss benefits and shortcomings of the methods, and identify key methodological, ethical, and research challenges when representing and assessing security and privacy risk. We also provide guidelines for the reporting of user studies in security and privacy.

The second research objective is to explore the factors that contribute to the acceptance of privacy and security risks in situations where people need to weigh the potential advantages of a technology against its associated privacy or security risks. We conducted a series of focus groups and highlighted the reasons why people accept compromises to their privacy and security, finding that perceived usefulness and the fulfilment of the psychological needs for autonomy and control were important factors. Our results suggest potential links between technology acceptance models and user experience models in the context of privacy-relevant interactions.

The third research objective is to design and evaluate examples of visible representations of security mechanisms, with a focus on encryption. We studied the effects of these visual and textual representations empirically to understand the impact of these visible security mechanisms on user experience, perceptions of security and users' understanding of encryption. We addressed this question in a series of studies, both lab studies and online experiments. In a vignette experiment, we find that more complex descriptions of encryption can lead to a better understanding and higher perceived security when designed carefully. However, we find no effect of novel visualizations of encryption on user experience (UX), perceived security or understanding of encryption.

The fourth objective is to explore how we might make the link from subjective experience to more secure behaviors. We introduce a new framework of security-enhancing friction design. The framework suggests helping users behave more securely by designing for moments of negative UX in security-critical situations while also ensuring that overall UX remains at an acceptable level to avoid disuse of secure technologies.

Overall, this doctoral dissertation contributes to research in the field of human-computer interaction, and more specifically, usable privacy and security. It improves our understanding of the methods used by researchers in the field of usable privacy and security use to create a perception of risk, and the factors that make people accept or reject certain privacy trade-offs. This dissertation also makes contributions to helping researchers and creators of technology understand how their designs influence perceptions of security, UX and understanding of encryption. This enables them to design for or against a perception of security, depending on the actual level of security provided by the technology. Finally, we conceptualize security-enhancing friction, a framework that suggests helping users to behave more securely by designing for moments of negative UX.

Acknowledgements

I express my gratitude to everyone who supported me while completing this doctoral dissertation.

I would like to thank my PhD advisor, Dr. Vincent Koenig, for his guidance throughout each stage of the process, fruitful discussions, and uplifting support. Thank you for your time and expertise over the years and for being an involved mentor.

I would also like to thank the members of my doctoral committee. I thank Dr. Carine Lallemand for transmitting her enthusiasm for research and providing valuable advice in many in-depth discussions. I thank Dr. Gabriele Lenzini for his insightful comments, which helped me advance in my research. Thank you both for your time and expertise.

I have had the pleasure of working and studying with great friends and colleagues. A special thank you to my wonderful colleagues at the HCI Research Group at the University of Luxembourg: Björn, Borce, Chris, Florence, Kerstin, Lorena, Luce, Sophie, and Vincent.

Thank you to Dr. Lorrie Cranor for the stimulating discussions and insightful guidance, as well as the warm welcome during my research stay. I also thank the members of the CyLab Usable Privacy and Security Laboratory for the discussions and kind welcome.

I express my gratitude to my friends and family for supporting me throughout my PhD. Special thanks to my parents, Andrea, Clara, Julia, Marc, and Tamara.

Thank you to the research participants who shared their time and experiences with me.

The research described in this dissertation was carried out with the support from the Fonds National de la Recherche under grant number PRIDE15/10621687.

Table of Contents

Chapter 1: Introduction **1**

1.1. Background 2

1.2. Overarching research objectives 8

1.3. Structure of the dissertation 9

1.4. Associated publications 11

1.5. References 12

Chapter 2: A Systematic Literature Review of Empirical Methods and Risk Representation in Usable Privacy and Security Research **17**

2.1. Abstract 17

2.2. Introduction 17

2.3. Background and related work 20

2.4. Research approach 24

2.5. Results 30

2.6. Discussion 56

2.7. Conclusion 68

2.8. Acknowledgements 69

2.9. Appendix 70

2.10. References 80

Chapter 3: How Acceptable Is This? How User Experience Factors Can Broaden Our Understanding of the Acceptance of Privacy Trade-Offs **95**

3.1. Abstract 95

3.2. Introduction 95

3.3. Research objectives 99

3.4. Methodology 100

3.5. Results 103

3.6. Discussion 110

3.7. Conclusion 118

3.8. Acknowledgements 119

3.9. Appendix 119

3.10. References 119

Chapter 4: Security – Visible, Yet Unseen? How Displaying Security Mechanisms Impacts User Experience and Perceived Security 125

4.1. Abstract 125

4.2. Introduction 125

4.3. Related work 126

4.4. Research objectives 129

4.5. Methodology 130

4.6. Results 134

4.7. Discussion 141

4.8. Conclusion 146

4.9. Acknowledgements 146

4.10. References 146

Chapter 5: Making Encryption Feel Secure: Investigating How Descriptions of Encryption Impact Perceived Security 151

5.1. Abstract 151

5.2. Introduction 151

5.3. Related work 152

5.4. Research objectives 155

5.5 Methodology 155

5.6. Results 161

5.7. Discussion 165

5.8. Conclusion 168

5.9. Acknowledgements 169

5.10. References 169

5.11. Appendices 172

Chapter 6: Complex, but in a good way? How to Represent Encryption to Non-Experts Through Text and Visuals – Evidence from Expert Co-Creation and a Vignette Experiment 173

6.1. Abstract 173

6.2. Introduction ... 173
6.3. Background ... 174
6.4. Research Objectives ... 182
6.5. Study 1: Iterative co-creation of representations of encryption with experts ... 183
6.6. Study 2: Vignette experiment with non-experts ... 188
6.7. Discussion ... 200
6.8. Conclusion ... 206
6.9. References ... 208
6.10. Appendices ... 215

Chapter 7: The Framework of Security-Enhancing Friction: How UX Can Help Users Behave More Securely ... 230

7.1. Abstract ... 230
7.2. Introduction ... 230
7.3. Existing security-enhancing interventions ... 231
7.4. Similarities and differences between existing security-enhancing interventions ... 235
7.5. Shortcomings of existing security-enhancing interventions ... 236
7.6. User experience, a good candidate to provide a nuanced understanding of subjective experience 237
7.7. Designing for negative experience and friction ... 238
7.8. Introducing security-enhancing friction ... 242
7.9. How to induce security-enhancing friction ... 248
7.10. How to measure the success of security-enhancing friction ... 250
7.11. Discussion ... 253
7.12. Conclusion ... 257
7.13. Acknowledgements ... 257
7.14. References ... 257

Chapter 8: Concluding Remarks ... 266

8.1. Synthesis of results ... 266
8.2. Contributions ... 270
8.3. Limitations and future work ... 273
8.4. Moving forward with the subjective experience of security in human-computer interactions ... 274

8.5. Conclusion 276

8.6. References 277

Chapter 1: Introduction

When interactions do not include technology, most people intuitively understand the risks to their privacy and security and how to protect against them. If we seek to tell somebody confidential information with other people in close proximity, we know that finding a separate room and closing the door will help keeping our information confidential. When sending a postcard, we are aware that the information we share can be read by anybody handling the postcard, while a letter in an envelope provides more confidentiality. In the past, wax seals could even provide authentication to one's writing, if the seal was unique to a sealer. A seal could also provide confidentiality, as a broken seal made it clear to the recipient that someone might have read or tampered with the letter. These examples are easily understood and, in most cases, yield accurate perceptions of security and privacy.

When humans interact with technology, it can be much harder to accurately evaluate the security of the interaction. When users of technology wish to share confidential information, the technological equivalent to closing the door on others listening in to your conversation is not immediately clear. Unencrypted communication can give the uninformed user the perception of sending a sealed letter, when really it might be more accurately compared to sending a postcard that can be read by others. Thus, interactions with technology may yield a subjective perception of security that is not warranted by the protections provided by the technology. Such inaccurately heightened mental representations of a system's protections can lead users to behave more insecurely than they might otherwise have. In contrast, an interaction that makes users feel unjustifiably insecure can induce them to use other products or services that feel more secure.

It is important to understand how people's perceptions of security are formed when interacting with technologies in order to obtain a nuanced understanding of their user experience (UX). A better understanding of the factors that induce certain subjective security-related experiences may help us better understand why people accept or do not accept certain compromises to their security and privacy, and engage in or do not engage in certain security-relevant behaviors. How people perceive the security of their interactions is subjective, and this subjective experience of security can be influenced by the various components of an experience, including the system people are using, the context in which their interaction is situated, or their previous experiences with similar interactions. This doctoral dissertation broadly aims to understand how people

subjectively perceive security in human-computer interactions. Understanding the determinants of security and privacy perceptions in human-computer interaction (HCI) can help guide future research and design people's perception of security in a way that is advantageous to the user. For instance, if people's perceived security is not aligned with the system state, we may want to design the interaction in a way that realigns their perceived security with what is warranted given the system state.

In this introductory section, I first provide a high-level overview of work in the area of security and privacy risk perceptions and relevant UX topics (Section 1.1). I invite the reader to refer to the respective chapters of this thesis for a deep dive into the previous work that is relevant for each chapter. Chapter 2 can be seen an extension of this background section, providing an original contribution, since it reports on a systematic literature review of 284 papers, including empirical studies in security and privacy over a 5-year period.

After presenting the background, I describe the overarching research objectives addressed in this dissertation (Section 1.2) and give an overview of the dissertation's structure (Section 1.3). I then outline the publications that are associated with this dissertation (Section 1.4).

1.1. Background

A significant body of research has studied user perceptions and behaviors in security and privacy-relevant contexts. In this section, I first introduce the concept of user experience, psychological needs theories, and technology acceptance models and their relation to security and privacy topics (Section 1.1.1). I then discuss research related to visible instances of security and their impacts on perceived security (Section 1.1.2). These topics transcend all chapters of this dissertation. Note that certain additional concepts (e.g., privacy trade-offs) are relevant only for certain chapters and are thus introduced in the respective chapter rather than in this overarching introduction.

1.1.1. Introducing user experience, psychological needs theories and technology acceptance to understand the experience of security-related interactions

In recent decades, HCI has become a highly relevant and timely field of research, as technologies increasingly enter various areas of people's lives. Usability has long been the prevalent concept in HCI user studies. Usability is typically defined as the "extent to which

a system, product or service can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use" (International Organization for Standardization, 1998). During the "third wave of HCI", the field expanded to focus more broadly user experience and non-work contexts (Bødker, 2006). Compared to usability, UX takes a broader view and considers a range of relevant psychological concepts when studying interactions with technology. Both instrumental and non-instrumental factors are taken into consideration (Hassenzahl, 2008). Instrumental factors of an experience are more goal-oriented (e.g., a user wants to send a message) than non-instrumental qualities, which are not directly goal-oriented, but can fulfil other needs (e.g., a user wants to talk to their family to fulfil their need for relatedness) (Hassenzahl, 2008). UX has become a core concept in HCI and can contribute to a nuanced understanding of how people perceive an interaction with technology. User experience can refer to different time spans, including anticipated UX (before usage), momentary UX (during usage), episodic UX (after usage) and cumulative UX (over multiple periods of use) (Roto et al., 2011). UX is related to psychological constructs such as emotions (Lopatovska & Arapakis, 2011) and psychological needs (Sheldon et al., 2001). Eudemonic aspects of UX have been used to describe the notion of striving to achieve one's personal best through an experience, which correlate with the non-instrumental (or "hedonic") qualities of experience (Mekler & Hornbæk, 2016).

UX can help understand both instrumental and non-instrumental factors of experience (Hassenzahl, 2008). Hassenzahl et al. (2008; 2010) suggested that the fulfillment of non-instrumental goals drives positive experience, along with the fulfillment of human needs such as autonomy, competence, security/control, relatedness, self-actualization/meaning, physical thriving, pleasure/stimulation, money/luxury, self-esteem and popularity/influence (Sheldon et al., 2001). The need for security, which is of particular interest for this dissertation and the field of usable privacy and security, has subdimensions; structure, predictability, presence of routines and habits, feeling safe from threats and uncertainties (Sheldon et al., 2001). We can apply UX work, including theories of psychological need fulfilment, to obtain a better understanding of security-related experiences.

The need for security and the concept of privacy are related. While a detailed definition of privacy is a far-reaching and ongoing discussion that falls outside the scope of this dissertation, it is often defined as individuals' ability to maintain control of their personal

information (Westin, 1968) and typically includes a notion of being able to decide and control the type of information about one's self or one's associations that one must reveal to others as well as under which circumstances and with which protections such revelations occur (Mason, 1986). From a user's perspective, privacy is thus related to the psychological need for security/control, which is defined as "feeling safe and in control of your life rather than feeling uncertain and threatened by your circumstances." (Sheldon et al., 2001, p. 339). For this reason, we apply perceived security as an umbrella term that links together the studies of this PhD thesis and encompasses the concept of privacy trade-offs. Privacy trade-offs can be seen as potential users of technologies evaluating and negotiating their need for security and control in interactions with technology.

Kraus et al. (2016, 2017) explored the use of psychological needs theories in the context of security and privacy. The authors found that security and privacy behaviors on smartphones are motivated by a number of psychological needs beyond the need for security (Kraus et al., 2016). Motivations for security actions include the need for meaningfulness, simulation, autonomy and competence (Kraus et al., 2017).

In usable privacy and security (UPS), users are often expected to adopt novel behaviors or technologies to improve their security or privacy. Some of these behaviors are adopted more easily, whereas others fail to gain traction with users. Technology acceptance models (TAM (Davis, 1985), UTAUT (Venkatesh et al., 2003)) and context-specific variations (e.g., Osswald et al., 2012; Pavlou, 2003) explain the factors that influence people's acceptance of technologies, including factors such as perceived usefulness, utility, social influence, and voluntariness of use. Hornbaek and Hertzum (2017) reviewed studies at the intersection of technology acceptance models and UX, concluding that many of these studies do not consider negative experiences and the fulfilment of psychological needs.

A note on terminology. Chapters 1 and 2 take a broader lens to explore the methods used by UPS researchers to induce a perception of risk and to understand how people rationalize their level of acceptance of privacy risks. The reader will thus find references to perceptions of security and privacy *risks* in Chapters 1 and 2. In Chapters 3 to 6, we then take a closer look at the impact visible representations of security mechanisms have on people's fulfilment of the need for security (Sheldon et al., 2001), which we refer to as *perceived security*. Chapter 7 then again takes a broader view and attempts to link UX to security *risk-taking behaviors.*

1.1.2. Visibility of security mechanisms and impact on security perceptions

Representing security mechanisms visually is challenging. Some security mechanisms need to be visible to end users, as users are expected to directly interact with them or they are displayed for legal reasons (e.g., authentication, verification, privacy permissions). However, other security mechanisms do not require direct user interaction and are thus often hidden from users' eyes (e.g., the presence of a secure channel). This has advantages; users are not slowed down by processing security-related information that is not needed to complete their primary task and do not need to understand the underlying security processes. However, users frequently over- or underestimate the security of a system they are using. Authors have described how instrumental the visibility of data collection is for people's development of "folk models" of what the system is doing (Rader & Slaker, 2017; Wash, 2010). They highlight that hiding the relationship between what the system is doing and what the user sees prevents the user from developing their own understanding and thus from making informed privacy decisions. Similarly, Spero and Biddle (2020) argue that concealing most security-relevant aspects of software inhibits the creation of mental models of security, which would allow users to behave more securely. They suggest that user security can be improved by building bridges between the user's security goals and the system's security state by making security information more salient in the user interface in a way that users find intelligible, thus leading to more secure behaviors. This confirms research suggesting that a lack of knowledge can cause certain security issues (Adams & Sasse, 1999), and can be summarized by the argument that security technologies should be visible, "available for inspection and examination" (Dourish et al., 2004). In the following, we highlight some of the research on visual representations of security mechanisms and how they relate to user perceptions, focusing on encryption-related interactions. We use the term "visible instances of security" to describe any visible representation of a security mechanism to users of a technology. A visible instance of security can encompass both visual and textual indicators (e.g., an image with a text caption).

One example of encryption protocols that many users are frequently exposed to is HTTPS. HTTPS is an encryption protocol that is used to implement confidential communications between parties whose identity is certified as trusted. Various studies have investigated

how to visualize the presence or absence of a HTTPS connection to users. Schechter et al. (2007) evaluated connection security indicators and warnings. They found that many participants failed to recognize the absence of a HTTPS indicator. Even when a warning page was displayed, many participants still took the risk and visited the website. Felt and colleagues (2015) later designed visual indicators for the presence or absence of HTTPS secure connections with the goal of improving understanding of these indicators as well as adherence to the secure behavior, which they defined as not visiting the untrusted website. The authors were not able to improve understanding of the security warning, but did improve adherence through opinionated design. Later, Felt et al. (2016) also designed new indicators for the presence or absence of HTTPS secure connections for browsers, and evaluated their effects in user studies. In a qualitative study on end users' and administrators' mental models of HTTPS, Krombholz et al. (2019) showed that end users often underestimated the security benefits of HTTPS. They also often ignored connection security due to general mistrust in the protection provided by HTTPS. In 2021, Chrome researchers published a blog post highlighting their previous research showing that the lock icon was often associated with a website being trustworthy, when really only the connection is secure (Panditrao et al., 2021). Due to this misalignment between how people interpreted the icon and the actual security property it intended to indicate, the researchers planned to run experiments with removing or replacing the lock icon. The results are not publicly available at present.

Similar situations to HTTPS arise with encrypted email, where the term "security" can have different meanings such as "confidentiality", "sender/receiver identity authentication", and for emailing and messaging specifically, "integrity of a message" and "end-to-end encryption". In Whitten and Tygar's (1999) seminal paper on the usability of PGP 5.0, usability issues made it difficult for non-expert users to make use of encrypted emails. Many novices were unable to successfully encrypt their emails even after more than an hour. Later work confirmed that usability problems influence the adoption of encryption in addition to social factors (e.g., being viewed as paranoid for encrypting emails) (Gaw et al., 2006). Ruoti and colleagues (2013) evaluated a webmail system that used security overlays with existing email services like Gmail. Their version of the tool was mostly invisible, with automatic key management and encryption. Their participants were mostly able to use the system without any training, but the security aspects were so invisible that some mistakenly sent out unencrypted messages and expressed concerns

about trusting the tool. The authors then conducted a study with a prototype that used manual encryption, which enabled participants to avoid mistakes and led to more trust in the system. Lausch et al. (2017) reviewed security indicators in the context of secure emails and found that adding certain images (e.g., postcards, closed envelopes, a torn envelope) yielded a relatively consistent interpretation. The authors also highlighted that a variety of indicators for encrypted email exist (as well as signed and unsigned email), making it difficult for users to understand their meaning.

More recently, research has also focused on end-to-end encrypted messaging applications such as Signal or WhatsApp. Researchers have often focused on authentication-related interactions, which users can have difficulties understanding or performing (Vaziripour et al., 2017), sometimes noting that inconsistent interface design and technical wording can make it difficult for users to use the technology as intended for better security (Abu-Salma et al., 2017). While usability issues have often been obstacles to the adoption of encryption technologies, Dechand et al. (2019) argue that another important problem may lie in how people perceive and understand security mechanisms, even when they are usable. They studied end-to-end encryption on WhatsApp as an example of a usable and secure end-to-end encryption solution and found that users' perception of the security provided was much more negative than justified. Indeed, participants underestimated the power of encryption and ignored the secure messaging application's notification about encryption, finding its wording hard to understand. Fassl et al. (2021) applied a user-centered design process to improve authentication ceremonies. Instead of incrementally improving existing ceremonies, they designed new ceremonies from scratch by employing a user-centered process that combined various user research methods. This approach took into account the social aspects of authentication ceremonies. While their approach did not result in better UX or usability, participants gained an improved understanding of the security implications of authentication ceremonies.

To synthesize, these examples deal with representations and implications of encryption, an ubiquitous security mechanism that underlies many daily interactions with technology but is usually largely invisible. Many of the studies explore user perceptions of encryption, often with the objective of improving the usability of these interactions or encouraging more secure user behaviors. An example of "improved" user behavior in the literature is to discourage users from visiting websites without a valid certificate (Felt et al., 2015) or enabling users to encrypt emails (Whitten & Tygar, 1999). While usability issues are still

relevant, others highlight that another important problem may lie in how people perceive and understand security mechanisms (e.g., Dechand et al., 2019). A user's perception of the security provided by a system is heavily influenced by what the interface reveals. Indeed, a growing body of research argues for more visible instances of security and privacy (e.g., Spero and Biddle, 2020). Previous research argues that making security and privacy processes more visible could help people have more realistic perceptions of security and privacy and thus of the risks of an interaction, eventually leading to more secure behaviors. But *how* to display security mechanisms to end users remains an open challenge in many contexts, and how such visible instances impact UX and security perceptions is an unsolved question that this dissertation contributes to answering.

We will now outline the overarching research objectives of this dissertation.

1.2. Overarching research objectives

This dissertation explores subjective perceptions of security and privacy. It addresses the questions of which factors induce perceptions of security and privacy risks and how user-centered approaches can contribute to designing these factors. Intentional design with respect to these factors could induce a perception of security or a lack thereof.

We study the factors that influence perceptions of security and privacy from four angles with the following high-level research objectives.

- The first objective is to analyze how security and privacy researchers induce a perception of security and privacy risks with research participants. To this end, we conduct a systematic literature review.
- The second objective is to explore the factors that contribute to the acceptance of privacy and security risks in situations where people need to weigh the potential advantages of a technology against its associated privacy or security risks. To this end, we conduct focus groups.
- The third research objective is to design and evaluate visible instances of security mechanisms, with a focus on encryption. In a series of studies, we investigate the effects of these visual and textual representations empirically to understand the impact of these more visible security mechanisms on user experience, perceptions of security and understanding.

- The fourth objective is to conceptualize security-enhancing friction, a framework that suggests helping users to behave more securely by designing for moments of negative UX in security-critical situations. We introduce the novel concept of security-enhancing friction, which allows the concept of user experience to be systematically integrated into empirical studies in the fields of usable privacy and security.

1.3. Structure of the dissertation

Chapter 1 provided a high-level overview of work pertaining to security and privacy risk perceptions and relevant UX topics and described overarching research objectives of this dissertation. We will now provide an outline of the structure of this dissertation, before listing the associated publications.

In Chapter 2, we conduct a systematic literature review of methods used in security and privacy studies with human participants to determine how researchers in the field of UPS represent security and privacy risk to research participants. From an initial sample of 633 papers published between 2014 and 2018, we systematically selected and analyzed 284 full-length papers. The analysis focused on methods; risk representation; the use of prototypes, scenarios and educational interventions; as well as deception and types of participants. We discuss the advantages and disadvantages of the methods used and identify key methodological, ethical and research challenges. This chapter makes theoretical/conceptual and methodological contributions (Wobbrock & Kientz, 2016), first and foremost by providing a systematic analysis of the methods used in UPS papers to induce the perception of privacy and security risks. We also provide a framework for systematically analyzing methods applied in UPS studies, with a focus on risk representation, and suggest guidelines for reporting empirical user studies. We identify methods, topics and user groups that are underrepresented in the UPS research literature and suggest potential directions for future UPS research.

In Chapter 3 of this dissertation, we explore factors that influence people's perceptions of security and privacy risks. We conducted focus groups with 32 participants in which we presented four scenarios with potential privacy trade-offs and asked participants to discuss whether they would be willing to accept the trade-offs described in these scenarios and for what reasons. This study gives rich empirical insights into how people perceive and evaluate privacy and security risks. It shows that the factors influencing the acceptance of

privacy trade-offs include a technology's perceived usefulness, context, previous experiences, perceived autonomy and control over the data being shared. On a theoretical level, the study helps address the inclusion of non-instrumental factors in the majority of acceptance models.

Building on these insights, in Chapters 4, 5 and 6, we then present studies that aim to understand how security mechanisms influence perceptions of security risks. In these studies, we focus on the visual display of encryption during data transmission, making a number of empirical contributions.

In Chapter 4, we qualitatively explore how visible security mechanisms in e-voting influence user perceptions of security risks. Two security mechanisms, vote verification and vote encryption, are displayed to users. This chapter contributes to existing knowledge on how displaying information on security mechanisms impacts people's UX, and we identify additional key factors that impact perceived security. We also provide some suggestions for the design of secure e-voting systems.

Chapter 5 studies which text-based descriptions of encryption are likely to enhance perceived security and gives practical suggestions on how researchers and designers can communicate encryption to non-expert users.

Chapter 6 investigates whether and how to best display encryption to non-experts during data transmission. We first collect security and HCI experts' ideas in an iterative co-creation process. We then evaluate these ideas using a large-scale vignette experiment with non-experts, in which we study the causal relationship between interface elements (visual representations and explanations of encryption) and perceived security, user experience and understanding of encryption. Our results show that the textual representation of encryption had a statistically significant and positive effect on perceived security and understanding, but not on UX. More complex text describing encryption resulted in higher perceived security and more accurate understanding. We did not find an effect of the visual representation of encryption.

All of these chapters primarily concern the study of subjective experiences in the context of security. In Chapter 7 of this dissertation, we propose to address the challenge of encouraging secure user behaviors by integrating the concept of UX into empirical usable privacy and security studies. We first compare and contrast existing security-enhancing interventions (e.g., nudges, warnings) through the lens of friction and build on these

insights to argue that it can be desirable to design for moments of negative UX in security-critical situations. We introduce the concept of security-enhancing friction, friction that reduces the occurrence of risk-taking behavior while ensuring that overall UX (after use) is not compromised. We demonstrate how this concept can be systematically integrated into empirical usable privacy and security studies, thus avoiding disuse of technologies with security interventions that are not compatible with acceptable UX. This chapter makes theoretical and methodological contributions to the literature.

Finally, we conclude by discussing the dissertation's findings and contributions and potential avenues for future research (Chapter 8).

1.4. Associated publications

Five chapters have been published in peer-reviewed venues, while Chapter 6 is under submission (see Table 1 for an overview). The published papers have been reformatted for the purposes of this dissertation.

Chapter	**Associated publication**	**Publication status**
Chapter 2	Distler, V., Fassl, M., Habib, H., Krombholz, K., Lenzini, G., Lallemand, C., Cranor, L., and Koenig, V. (2021). A Systematic Literature Review of Empirical Methods and Risk Representation in Usable Privacy and Security Research. *ACM Transactions on Computer-Human Interaction.*	*Accepted for publication*
Chapter 3	Distler, V., Lallemand, C., & Koenig, V. (2020). How Acceptable Is This? How User Experience Factors Can Broaden our Understanding of The Acceptance of Privacy Trade-offs. *Computers in Human Behavior*, 106, 106227. https://doi.org/10.1016/j.chb.2019.106227	*Published*
Chapter 4	Distler, V., Zollinger, M.-L., Lallemand, C., Roenne, P. B., Ryan, P. Y. A., & Koenig, V. (2019). Security – Visible, Yet Unseen? How Displaying Security Mechanisms Impacts User Experience and Perceived Security. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. Association for Computing Machinery. https://doi.org/10.1145/3290605.3300835	*Published*
Chapter 5	Distler, V., Lallemand, C., & Koenig, V. (2020). Making Encryption Feel Secure: Investigating how Descriptions of Encryption Impact Perceived Security. *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW),* 220–229. https://doi.org/10.1109/EuroSPW51379.2020.00037	*Published*
Chapter 6	Distler, V., Gutfleisch, T., Lallemand, C., Lenzini, G., Koenig, V. How to Represent Encryption to Non-Experts Through Text and Visuals? Putting Expert Ideas to the Test in a Vignette Experiment Among Non-Experts.	*Under review (minor revisions)*

Chapter 7	Distler, V., Lenzini, G., Lallemand, C., & Koenig, V. (2020). The Framework of Security-Enhancing Friction: How UX Can Help Users Behave More Securely. *New Security Paradigms Workshop 2020*, 45–58. https://doi.org/10.1145/3442167.3442173	*Published*

Table 1: Publications associated with this doctoral dissertation.

There are three related publications that are not chapters of this dissertation:

Distler, V., Lallemand, C., Koenig, V. (2018) Understanding human need fulfilment to support the design of secure experiences. Doctoral Consortium Paper at the 10th Nordic Conference on Human-Computer Interaction – NordiCHI '18 (Oslo, Norway, 2018).

Distler, V., Lallemand, C., Koenig, V. (2018) A UX Approach to Privacy and Security: the Impact of User, Contextual, and System-Related Factors. Extended Abstract Presented at the Workshop on Exploring Individual Differences in Privacy (CHI 2018).

Zollinger, M. L., Distler, V., Roenne, P., Ryan, P., Lallemand, C., & Koenig, V. (2019). User Experience Design for E-Voting: How mental models align with security mechanisms. Electronic Voting.

1.5. References

Abu-Salma, R., Krol, K., Parkin, S., Koh, V., Kwan, K., Mahboob, J., Traboulsi, Z., & Sasse, M. A. (2017). The Security Blanket of the Chat World: An Analytic Evaluation and a User Study of Telegram. *Proceedings 2nd European Workshop on Usable Security*. European Workshop on Usable Security, Paris, France. https://doi.org/10.14722/eurousec.2017.23006

Adams, A., & Sasse, M. A. (1999). Users are not the enemy. *Communications of the ACM*, *42*(12), 40–46. https://doi.org/10.1145/322796.322806

Bødker, S. (2006). When Second Wave HCI meets Third Wave Challenges. *Proceedings of the 4th Nordic Conference on Human-Computer Interaction 2006*, 9.

Davis, F. D. (1985). *A technology acceptance model for empirically testing new end-user information systems: Theory and results* [PhD Thesis]. Massachusetts Institute of Technology.

Dechand, S., Naiakshina, A., Danilova, A., & Smith, M. (2019). In Encryption We Don't Trust: The Effect of End-to-End Encryption to the Masses on User Perception. *2019 IEEE*

European Symposium on Security and Privacy (EuroS&P), 401–415. https://doi.org/10.1109/EuroSP.2019.00037

Dourish, P., Grinter, R. E., de la Flor, J. D., & Joseph., M. (2004). Security in the Wild: User Strategies for Managing Security as an Everyday, Practical Problem. *Personal and Ubiquitous Computing*, *8*.

Fassl, M., Gröber, L., & Krombholz, K. (2021). Exploring User-Centered Security Design for Usable Authentication Ceremonies. *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, 15.

Felt, A. P., Ainslie, A., Reeder, R. W., Consolvo, S., Thyagaraja, S., Bettes, A., Harris, H., & Grimes, J. (2015). Improving SSL Warnings: Comprehension and Adherence. *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, 2893–2902. https://doi.org/10.1145/2702123.2702442

Felt, A. P., Reeder, R. W., Ainslie, A., Harris, H., Walker, M., Thompson, C., Acer, M. E., Morant, E., & Consolvo, S. (2016). Rethinking Connection Security Indicators. *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*, 1–14. https://www.usenix.org/conference/soups2016/technical-sessions/presentation/porter-felt

Gaw, S., Felten, E. W., & Fernandez-Kelly, P. (2006). Secrecy, flagging, and paranoia: Adoption criteria in encrypted email. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 591–600). Association for Computing Machinery. https://doi-org.proxy.bnl.lu/10.1145/1124772.1124862

Hassenzahl, M. (2008). User experience (UX): Towards an experiential perspective on product quality. *Proceedings of the 20th Conference on l'Interaction Homme-Machine*, 11–15.

Hassenzahl, M., Diefenbach, S., & Göritz, A. (2010). Needs, affect, and interactive products – Facets of user experience. *Interacting with Computers*, *22*(5), 353–362. https://doi.org/10.1016/j.intcom.2010.04.002

Hornbæk, K., & Hertzum, M. (2017). Technology Acceptance and User Experience: A Review of the Experiential Component in HCI. *ACM Transactions on Computer-Human Interaction*, *24*(5), 1–30. https://doi.org/10.1145/3127358

International Organization for Standardization. (1998). *ISO 9241-11:1998. Ergonomic requirements for office work with visual display terminals (VDTs) –Part 11: Guidance on usability*.

Kraus, L., Wechsung, I., & Möller, S. (2016). *Exploring Psychological Need Fulfillment for Security and Privacy Actions on Smartphones*. https://doi.org/10.14722/eurousec.2016.23009

Kraus, L., Wechsung, I., & Möller, S. (2017). Psychological needs as motivators for security and privacy actions on smartphones. *Journal of Information Security and Applications*, *34*, 34–45. https://doi.org/10.1016/j.jisa.2016.10.002

Krombholz, K., Busse, K., Pfeffer, K., Smith, M., & von Zezschwitz, E. (2019). "If HTTPS Were Secure, I Wouldn't Need 2FA"—End User and Administrator Mental Models of HTTPS. *2019 IEEE Symposium on Security and Privacy (SP)*, 246–263. https://doi.org/10.1109/SP.2019.00060

Lausch, J., Wiese, O., & Roth, V. (2017). What is a Secure Email? *Proceedings 2nd European Workshop on Usable Security*. European Workshop on Usable Security, Paris, France. https://doi.org/10.14722/eurousec.2017.23022

Lopatovska, I., & Arapakis, I. (2011). Theories, methods and current research on emotions in library and information science, information retrieval and human–computer interaction. *Information Processing & Management*, *47*(4), 575–592. https://doi.org/10.1016/j.ipm.2010.09.001

Mason, R. O. (1986). Four Ethical Issues of the Information Age. *MIS Quarterly*, *10*(1), 5–12. https://doi.org/10.2307/248873

Mekler, E. D., & Hornbæk, K. (2016). Momentary Pleasure or Lasting Meaning?: Distinguishing Eudaimonic and Hedonic User Experiences. *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, 4509–4520. https://doi.org/10.1145/2858036.2858225

Osswald, S., Wurhofer, D., Trösterer, S., Beck, E., & Tscheligi, M. (2012). Predicting information technology usage in the car: Towards a car technology acceptance model. *Proceedings of the 4th International Conference on Automotive User Interfaces and Interactive Vehicular Applications*, 51–58.

Panditrao, S., O'Brien, D., & Stark, E. (2021, July 14). Increasing HTTPS adoption. *Chromium Blog*. https://blog.chromium.org/2021/07/increasing-https-adoption.html

Pavlou, P. A. (2003). Consumer Acceptance of Electronic Commerce: Integrating Trust and Risk with the Technology Acceptance Model. *International Journal of Electronic Commerce*, *7*(3), 101–134. JSTOR.

Rader, E., & Slaker, J. (2017). The importance of visibility for folk theories of sensor data. *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*, 257–270. https://www.usenix.org/conference/soups2017/technical-sessions/presentation/rader

Roto, V., Law, E., Vermeeren, A., & Hoonhout, J. (2011). User Experience White Paper. *Result from Dagstuhl Seminar on Demarcating User Experience, September 15-18, 2010*, 12.

Ruoti, S., Kim, N., Burgon, B., van der Horst, T., & Seamons, K. (2013). Confused Johnny: When automatic encryption leads to confusion and mistakes. *Proceedings of the Ninth Symposium on Usable Privacy and Security - SOUPS '13*, 1. https://doi.org/10.1145/2501604.2501609

Sheldon, K. M., Elliot, A. J., Kim, Y., & Kasser, T. (2001). What is satisfying about satisfying events? Testing 10 candidate psychological needs. *Journal of Personality and Social Psychology*, *80*(2), 325.

Spero, E., & Biddle, R. (2020). Out of Sight, Out of Mind: UI Design and the Inhibition of Mental Models of Security. *New Security Paradigms Workshop 2020*, 127–143. https://doi.org/10.1145/3442167.3442174

Vaziripour, E., Wu, J., O'Neill, M., Whitehead, J., Heidbrink, S., Seamons, K., & Zappala, D. (2017). Is that you, Alice? A Usability Study of the Authentication Ceremony of Secure Messaging Applications. *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*, 29–47. https://www.usenix.org/conference/soups2017/technical-sessions/presentation/vaziripour

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User Acceptance of Information Technology: Toward a Unified View. *MIS Quarterly*, *27*(3), 425–478. https://doi.org/10.2307/30036540

Wash, R. (2010). Folk models of home computer security. *Proceedings of the Sixth Symposium on Usable Privacy and Security - SOUPS '10*, 1. https://doi.org/10.1145/1837110.1837125

Westin, A. F. (1968). Privacy and freedom. *Washington and Lee Law Review*, *25*(1), 166.

Whitten, A., & Tygar, J. D. (1999). A Usability Evaluation of PGP 5.0. *Proceedings of the 8th USENIX Security Symposium*, 169–183.

Wobbrock, J. O., & Kientz, J. A. (2016). Research Contributions in Human-Computer Interaction. *Interactions*, 38–44.

Chapter 2: A Systematic Literature Review of Empirical Methods and Risk Representation in Usable Privacy and Security Research

Accepted for publication: Distler, V., Fassl, M., Habib, H., Krombholz, K., Lenzini, G., Lallemand, C., Cranor, L., and Koenig, V. (2021). A Systematic Literature Review of Empirical Methods and Risk Representation in Usable Privacy and Security Research. *ACM Transactions on Computer-Human Interaction.*

2.1. Abstract

Usable privacy and security researchers have developed a variety of approaches to represent risk to research participants. To understand how these approaches are used and when each might be most appropriate, we conducted a systematic literature review of methods used in security and privacy studies with human participants. From a sample of 633 papers published at five top conferences between 2014 and 2018 that included keywords related to both security/privacy and usability, we systematically selected and analyzed 284 full-length papers that included human subjects studies. Our analysis focused on study methods; risk representation; the use of prototypes, scenarios, and educational intervention; the use of deception to simulate risk; and types of participants. We discuss benefits and shortcomings of the methods, and identify key methodological, ethical, and research challenges when representing and assessing security and privacy risk. We also provide guidelines for the reporting of user studies in security and privacy.

2.2. Introduction

As the use of digital technology evolves, so does the number and the type of risks to which users and their data are exposed. Studying how people perceive those risks and what interventions will help people better understand and respond to them is thus an essential factor in achieving better security. To understand the extent to which study participants will take security- or privacy-protective steps often requires that participants are exposed to a scenario that provides realistic cues such that they will behave in the study in a similar way that they would behave in real life. This often requires exposing participants to real or simulated risk. Participants may be able to navigate menus, click buttons, and follow instructions to use a security tool such as an encrypted chat client or a web browser security

feature, but testing the effectiveness of such a tool often requires exposing participants to a real or simulated attack to determine how they will respond and whether the tool helps prevent them from being deceived by the attacker. Usable privacy and security (UPS) researchers regularly encounter challenges when they design studies – whether in the lab, online, or in-situ – that focus on people's perceptions of and response to security and privacy risks.

Since users usually have a primary objective that is not related to security or privacy, instructing participants to pay particular attention to privacy and security would lead to bias and "security priming" (Sotirakopoulos et al., 2011). Designing a realistic experience for a laboratory or online study of security and privacy risk is difficult. For additional realism, deception can be used to simulate attacks and to make participants believe they are at risk (Cranor & Buchler, 2014). When using deception, researchers must find a balance between preserving the realism of an attack and ethically exposing study participants to it. This is often achieved by debriefing participants about the deception promptly so they do not spend much time worrying about having been the victim of an attack or take unnecessary steps attempting to recover from a perceived attack.

In-situ studies are also challenging because attacks occur rarely and thus require collecting user activity logs over extended periods of time, potentially raising logistical and privacy concerns. In addition, observing real attacks without interfering and mitigating potential harm to participants can be ethically questionable. On the other hand, if researchers inject simulated attacks into a participant's real world activities, participants may become accustomed to being attacked for research purposes and may ignore real attacks.

These are just some of the challenges that researchers in usable privacy and security face when designing user studies; we describe these in more detail in Section 2.3.2. In light of these challenges, we investigated which methods researchers use for privacy and security studies that include human participants, with a particular focus on the approaches researchers use to represent risk. We conducted a systematic literature review of 284 full-length research papers published at five top conferences between 2014 and 2018, with the goal of accumulating the knowledge from a large body of studies and providing an analysis of the characteristics of empirical user studies in usable privacy and security. Systematic literature reviews efficiently integrate existing knowledge (Mulrow, 1994), and can aid in understanding the breadth of research on a topic. They can also be used to develop theories or conceptual background for subsequent research, and identify topics that require more

investigation (Paré et al., 2015). A better understanding of how risk is represented in privacy and security user studies will allow the community to critically assess and discuss the validity and ethics of different approaches, as well as help researchers as they design future studies.

Our literature review suggests that risk representation in the analyzed papers was mostly based on naturally occurring or simulated risk, varying with study methods and research objectives of the paper. Papers with an experimental objective mostly used simulated risk, and descriptive studies mostly relied on naturally occurring risk. Few studies relied only on mentioned risk or did not represent risk at all. Common tools used to represent risks to research participants included security/privacy-related tasks, prototypes, and scenarios. Deception, educational interventions, and incentives for secure behavior were only rarely used. Based on our systematic review, we discuss the implications of our findings and suggest guidelines for designing and reporting UPS user studies.

Our study makes the following contributions:

(1) A systematic review of the methods employed in UPS papers from 2014 to 2018 for inducing a perception of privacy and security risks.

(2) A structure for systematically analyzing methods in UPS studies, with a focus on risk representation.

(3) Identification of six approaches used in UPS studies (individually or in combination) for inducing a perception of risk: assigned tasks, prototypes, scenarios, deception, educational interventions, and incentives for secure behavior.

(4) Guidelines for designing and reporting UPS studies.

In this article, we first position our research within the broader context of related work in the field of usable privacy and security, considering previous literature reviews, methodological challenges faced by researchers in the field and how deception is used in UPS studies (section 2.3.). We then present the methods we used for this systematic literature review (section 2.4.). Next, we describe the approaches found in our literature review for representing risk to research participants (section 2.5.). We then discuss the choice of methods, participant recruitment and ethics, and consider limitations of our study (section 2.6.) before concluding (section 2.7.).

2.3. Background and related work

We review related work in three areas relevant to our study: UPS literature reviews, methodological challenges and risk representation in UPS research, and the use of deception when studying perceived risk.

2.3.1. Literature reviews in Usable Privacy and Security

Although several literature reviews have been conducted in areas related to usable privacy and security, none address the need for a systematic review of methodological issues specific to risk representation in UPS. Iachello and Hong (2007) summarize research on the topic of privacy in Human Computer Interaction, with a focus on current approaches, results, and trends. They identify future grand challenges in HCI and privacy, such as developing better ways of helping end-users manage their privacy, creating stronger analysis techniques and survey tools, or developing a theory of technology acceptance, specifically related to privacy. Garfinkel and Lipford (2014) review past UPS research and identify important research directions within UPS. They also describe important challenges of research in UPS, ranging from authentication, adversary modelling, system administration, consumer privacy, social computing, ecological validity, and teaching. Acquisti and colleagues (2017) review literature pertaining to privacy and security decision making with a focus on research assisting individuals' privacy and security choices with soft paternalistic interventions that nudge users toward more beneficial choices. The authors discuss potential benefits and shortcomings, as well as identify ethical, design, and research challenges.

In the subfield of authentication research, Biddle et al. (2012) provide an overview of published research in the area of graphical passwords, including usability and security aspects as well as system evaluation. Bonneau et al. (2012) evaluate two decades of proposals to replace text passwords for general-purpose user authentication. They provide a framework enabling researchers to evaluate the methods and to benchmark future web authentication proposals. Finally, Velásquez et al. (2018) present a systematic literature review of authentication schemes.

While a number of HCI papers have reviewed methods for user experience evaluation generally (Alves et al., 2014; Obrist et al., 2009; Pettersson et al., 2018), we know of no review of the methods used in UPS studies in particular. We fill this gap by reviewing

methods used in UPS studies from both the HCI literature and from specialized privacy and security publication venues, focusing on approaches to risk representation.

2.3.2. Methodological challenges and risk representation in Usable Privacy and Security

The methodological challenges in UPS are different from those in other focus areas of user-centred design. In particular, collecting data in an ecologically valid way remains particularly complex in UPS. While lab studies allow researchers to create a controlled environment and isolate the effect of certain variables, participants may face different threats and motivations than in the field. Using fictitious personal data rather than a participant's real data may reduce privacy risks but will impact the ecological validity of the study. In addition, simulated attacks in a lab environment will be experienced at a significantly higher rate than in a real-world setting, further jeopardizing ecological validity (Garfinkel & Lipford, 2014).

Another difficulty is that, for many relevant scenarios, security or privacy is not the primary goal of the individual, and thus any mention of security or privacy may prime participants and cause them to behave differently than they would normally (Egelman et al., 2007). In addition, it is difficult to simulate a situation in which users would both fulfil their primary tasks and respond to potential risks (Schechter, 2013).

A lab setting (as well as participant briefings, instructions, and research framing) can also frequently lead participants to state that they care more about security than they would in a real-world setting. Indeed, studies have found inconsistencies between what people say and the actions they actually take related to privacy and security (Egelman et al., 2007; Sotirakopoulos et al., 2011). Social desirability of privacy and security behaviors may play a role in this context (Egelman & Peer, 2015). Lastly, while the use of self-reported data about security and privacy behaviors can provide rich insights, these data can sometimes lack reliability for many reasons, including participants misremembering their past behaviors, or feeling uncomfortable making accurate disclosures.

UPS researchers use a variety of approaches to create a realistic experience of risk in their studies. In some studies, researchers introduce hypothetical scenarios and use role playing to simulate a real-life situation. Schechter and colleagues (Schechter et al., 2007) describe the use of role playing to create a perception of risk, but find that role playing has a significant negative effect on the security vigilance of study participants. Another

approach is the use of deception, which can be beneficial to understand how people react to attacks in a realistic setting, for instance by simulating the presence of an adversary (Cranor & Buchler, 2014) or by launching attacks on research participants (Egelman et al., 2007). While deceptive studies raise ethical concerns, these studies are often justified because it would be difficult or impossible to conduct some types of studies without deception, and harm to participants can be minimized through timely debriefing. For example, Cranor and Buchler (2014) argue that in the context of computer security warnings, it is important to use simulated attack scenarios to observe how participants respond to warnings when they have been led to believe they are actually at risk. Another approach is long-term in-situ studies. Forget et al. built the Security Behavior Observatory (SBO) to recruit and observe a panel of consenting home computer users, allowing for the study of security-related behavior in a real world setting (Forget et al., 2014).

2.3.3. The use of deception when studying perceived risk

Deception can be defined as deliberately misleading participants or not informing them about the purpose of the investigation, usually to avoid the possibility that responses might be given to meet perceived expectations of the researchers (*Deception Research – APA Dictionary of Psychology*, n.d.). In UPS studies, deception is often used to mislead participants so they believe the study is unrelated to security or that simulated risks are actually real. Generally, participants are debriefed promptly at the conclusion of the study to prevent psychological harm, for example from worrying about actual harm from simulated risks they have been misled to believe are real. Debriefing participants prevents mistrust in the researcher resulting from the use of deception (American Psychological Association, 2017).

Researchers have long emphasized the far-reaching ethical issues of studies using deception in psychological research, including a decrease of trust in researchers, lack of informed consent, and the insufficient effect of the debriefing (Baumrind, 1985). On the other end of the spectrum, Christensen (1988) argues that research participants often do not have negative feelings after participating in a deception experiment and that the acceptability of deception depends on the behaviors being investigated, the setting of the investigation (public vs. private place), and the outcome of the experiment. He concludes that deception should be avoided in studies investigating personal information or in studies that potentially harm the subject. Athanassoulis and Wilson (2009) argue that the fact that

a research study uses deception does not necessarily make it morally problematic. Rather, they suggest that ethics committees should focus on the reasonableness of withholding information from a participant, which is context-dependent.

In the field of Human-Computer Interaction, Adar and colleagues (2013) argue that deception is understudied and present a view of deception that takes into account motive (why deception happens), means (how deception is designed), and opportunity (when it works).

In the usable privacy and security community, the importance of rigorous reporting of deception has been underlined, including reporting how participants were debriefed, how they reacted, and how data was protected (Schechter, 2013). Deception is usually used to avoid security priming, which could impact participants' responses and reactions. Schechter et al. explored the effect of priming, where one experimental group was instructed to pay attention to security during the study which included banking tasks, while the other group was not "primed" in this way. The authors did not find a statistically significant difference between the groups (Schechter et al., 2007). Fahl et al., (2013) asked students to role-play that they had enrolled in a new university, and thus needed to create passwords. Similar to Schechter and colleagues, they did not find an effect of priming. Naiakshina et al., (2018) conducted an experiment with student developers, where half of the developers were primed to consider security when implementing the user registration functionality of a social network, while the other half were not primed. Contrary to the previously described studies, priming clearly had an effect on the number of participants who attempted to implement a secure solution. One should note, however, that while some of these studies use the notions of priming and deception almost interchangeably, we consider the lack of priming to be *partial disclosure* rather than *deception*, as described in detail in the results section.

In the quest to avoid priming participants, some deception studies do not ask participants for informed consent since informing them about the study could prime them. While most UPS studies undergo Institutional Review Board (IRB) or ethics board review, IRB approval does not guarantee that non-consenting participants do not feel violated, as described by Garfinkel and Lipford (2014). They emphasize that the question of consent in a field setting, where it is often avoided in an attempt to avoid priming participants, is a serious concern. The authors describe a study where the requirement for informed consent was waived through IRB approval, however, the experiment still resulted in

significant negative attention because participants resented being involved without their consent (Jagatic et al., 2007).

2.4. Research approach

2.4.1. Research Objectives

The goal of this paper is to summarize and extract knowledge from a large corpus of UPS work between 2014 and 2018. The objective is to analyze the characteristics of empirical studies in UPS to better understand how risk is represented in user studies and how researchers navigate the tension between realistic exposure to risk and ethical, legal, and practical considerations. We conduct a systematic literature review of a sample of recent papers published at top peer-reviewed UPS venues. We review the methods used in these studies and how they allow the authors to represent risk.

Our analysis focuses on three research questions:

RQ1: Which methods do researchers in the UPS community use?

RQ2: How do researchers in UPS represent risk?

RQ3: How do researchers in the UPS community use deception in their user study protocols?

The first two research questions cover the entire range of methods used by researchers in UPS and all types of risk representations (e.g., naturally occurring, simulated, mentioned, no intentionally designed risk perception), including an analysis of participant recruitment. Our third research question focuses on deceptive studies, examining the details of how deception is used. Based on our analysis we provide guidelines for researchers when designing and reporting UPS user studies.

2.4.2. Review Process

Our systematic literature review approach includes the following phases: (1) Identification, (2) Filtering, (3) Review, and (4) Analysis. In the identification phase we constructed the initial set of papers using keyword searches, during the filtering phase we checked whether the papers fulfilled our eligibility criteria, in the review phase we read all papers in detail and categorized them, and in the analysis phase we explored trends we observed during our review and developed guidelines for future UPS study design.

2.4.2.1. Phase 1: Identification of potentially relevant papers

Source selection

We selected the five most relevant peer-reviewed conference publication venues for UPS papers. We did not consider journal papers, as most UPS papers are published at conferences. We selected top tier privacy and security conferences that also invite UPS papers, namely ACM Conference on Computer and Communications Security (ACM CCS), IEEE Symposium on Security and Privacy (IEEE S&P), and USENIX Security Symposium (USENIX Security). In addition we included the Symposium on Usable Privacy and Security (SOUPS), a conference that focuses on UPS papers specifically. We also included the ACM Conference on Human Factors in Computing Systems (CHI), the top HCI conference where UPS papers are regularly published. Our selection of conferences includes three of the "big four" security conferences. We did not select the other big-four conference, the Network and Distributed Systems Security Symposium (NDSS), or the Privacy Enhancing Technologies Symposium (PETS) because they (a) have tended to publish fewer UPS papers than the other conferences, and (b) their publishers do not provide a searchable database of their papers. While UPS papers have also appeared in other top conferences in particular application areas such as The Web Conference and UbiComp, we limited our selection to conferences primarily focused on either security/privacy or HCI. As our focus is on current practices and methods, we only considered papers from the last 5 years. Since the publication year 2019 was still ongoing at the time of our data collection, we limited the search results to the period from 2014 to 2018.

Search procedure

We used the keyword search provided by the ACM Digital Library and the IEEE Computer Society Digital Library to construct our initial set of potentially relevant UPS papers in July 2019. As we are interested in UPS papers with a clear focus on user perceptions or behavior, we used a search query designed to select papers mentioning privacy or security in addition to at least one user-related term (user, usability, usable, user experience, UX) in title or abstract: *(privacy OR Security) AND (user OR usability OR usable OR ux OR "user experience").* We conducted a pilot in which we added specific terms related to security (e.g., encryption, passwords, authentication) to the search query. We decided against adding these terms as they retrieved only a small number of additional

papers, most of which were not relevant to our research questions. The search query resulted in 633 potentially relevant papers (shown in Table 1).

2.4.2.2. Phase 2: Filtering initial set of papers

The first author reviewed the titles and abstracts of the 633 papers identified in Phase 1 and removed papers that met one or more the following three exclusion criteria:

- Study does not involve any user data (data obtained directly as part of the study, data previously collected in other studies, or data obtained through naturally generated datasets).
- Paper is not a full conference paper (e.g., workshop paper, extended abstract). We decided to exclude such papers since it helped us avoid duplicates if a paper was first published as an extended abstract and later as a full paper. Short papers also tend to include less details on the methodology, and thus provide less insights into risk representations.
- Paper presents theoretical models or simulations without including a user study.

The first author coded all papers as to whether or not they met each of the exclusion criteria. In addition, the remaining authors double-coded 77 papers (12%). Cohen's kappa with the first author ranged between 0.80 (substantial agreement) and 1 (perfect agreement). Remaining conflicts were resolved in discussion. This resulted in 305 papers being removed and 328 advancing to Phase 3.

	CCS	IEEE S&P	USENIX Security	SOUPS	CHI	Total
Phase 1: Identification of potentially relevant papers	237	44	117	118	117	633
Phase 2: Papers filtered based on title and abstract to remove those without user data and those that are not full conference papers	194	20	87	0	4	305
Phase 3: Papers filtered after detailed review	15	4	5	3	17	44
Included Papers	28	20	25	115	96	284

Table 1: Exclusion of papers per round of exclusion and per publication venue.

2.4.2.3. Phase 3: Detailed review of the papers

The first three authors split up the 328 included papers between them. The first author read and coded 213 papers, the second and third author read and coded 72 and 41 papers respectively.

Based on the full paper, the authors excluded a total of 44 additional papers for the following reasons:

- User data was used purely to demonstrate the technical feasibility or effectiveness of a protocol (n=11).
- No user data was used (n=17).
- While the paper may mention privacy or security perceptions or behaviors, the authors did not design their study with the intention of studying privacy and security perceptions or behaviors (n=15).
- The publication was not a full paper (n=1).

The authors reviewed the remaining 284 papers (Table 1) in detail, filling out a spreadsheet row for each paper with information on the dimensions of our analysis structure. 22% (n=63) of papers were analyzed by two coders and any disagreements were discussed and resolved. All three coders participated in bi-weekly calls where they discussed unclear papers.

Our analysis includes the following dimensions which correspond to our research questions. Dimensions A-B describe the dataset, dimensions C-F respond to RQ1 (Which methods do researchers in the UPS community use?), dimensions G-M respond to RQ2 (How do researchers in UPS represent risk?) and dimension N responds to RQ3 (How do researchers in the UPS community use deception in their user study protocols?).

A. Publication Venue (Section 2.5.1.1.)

B. Topic: privacy-enhancing technologies, encryption, authentication, access control, privacy transparency and choice mechanisms, security indicators and warnings, social engineering, security perceptions, attitudes and behaviors, privacy perceptions, attitudes and behaviors, privacy and security for special populations, security for admins and developers, multiple topics (Section 2.5.1.2.)

C. Objective of the study: descriptive, relational, experimental, combination (Section 2.5.1.3.)

- Replication: yes, no, partial

D. Study method: survey, interview, experiment, focus group, workshop, analysis of existing data sets, log analysis, diary study, co-creation methods, vignette study, observation study, list experiment, vignette experiment, other (Section 2.5.1.4.)

E. Participants: representative sample, non-representative convenience sample, students, computer science students, developers, university employees, employees, security experts, other experts, MTurkers, Prolific, other crowdsourcing, Google Consumer Survey (GCS), Security Behavior Observatory (SBO), users of specific technology, disabled users, children or teenagers, women in particular, LGBTQ+, recruitment not mentioned, other (Section 2.5.1.5.)

- Number of participants

F. IRB or ethics board approval: ethics board approval, approved exempt, exempt from needing approval, not mentioned, corporate internal review, other (Section 2.5.1.6.)

G. Risk representation: naturally occurring, simulated, mentioned, no induced risk representation (Section 2.5.2.1.)

H. Risk response assessment: observational data, self-reported, assigned security or privacy task, assigned unrelated task, combination (Section 2.5.2.4.)

I. Participants complete an assigned task (security- or privacy-related task, unrelated task, both, no task) (Section 2.5.3.1.)

J. Participants interact with prototype: yes, no (Section 2.5.3.2)

K. Participants asked to respond to one or more hypothetical scenarios: yes, no (Section 2.5.3.3)

L. Educational intervention: yes, no (Section 2.5.3.4)

M. Participants received an incentive for secure behavior: yes, no (Section 2.5.3.5)

N. Deception used: yes, no (Section 2.5.3.6)

- Type of deception: deception about the objective of the study, deception about the presence of risk, lack of consent
- Debriefing (for deception studies): yes, no

2.4.2.4. Phase 4: Analysis

In this phase, we explored the trends we observed during our review. We focused our analysis on how risk was represented and measured, and how researchers combined approaches for risk representation (assigned tasks, prototypes, scenarios, deception, educational interventions, incentives for secure behavior). We describe the results of this analysis in section 2.5.

2.4.3. Limitations

This paper is based on the analysis of a large corpus of papers. Although we report quantitative results on the frequency of papers with various attributes, we caution that our categorization of papers was somewhat of a subjective process, largely due to the fact that some authors did not provide complete information about their methods and that authors use terms like "deception" and "exempt" in inconsistent ways. Some papers fell into grey areas with details that could be interpreted in multiple ways. Such cases were resolved by discussion between the co-authors.

We took a number of steps to promote consistency between our coders in their interpretation of these papers. To arrive at our data set we double coded 12% of the papers according to our phase 2 exclusion criteria, an approach commonly used in systematic literature reviews to ensure the reliability of the inclusion/exclusion process. During the detailed analysis phase, we used bi-weekly calls of all coders to discuss ambiguous papers and ensure consistency. In addition, we also discussed difficult cases with the co-authors who were not otherwise participating in the coding process. Twenty percent of the papers were coded by two coders and conflicts were resolved through discussions, further clarifying any discrepancies in the coders' understanding of the categories. After all papers were coded, the first author also reviewed all code assignments to check for plausibility and consistency. Despite these efforts to maintain data accuracy, the frequencies and percentages in this paper are meant to describe trends in the data, rather than to be interpreted as exact indicators due to a certain level of subjective interpretation in the coding.

One might also question why we analyzed papers in the five-year period between 2014 and 2018, rather than including a longer time period. Since the publication year 2019 was still ongoing at the time of our data collection, we did not include papers from 2019. As our objective was to analyze recent research trends and methods in the UPS field rather

than taking a long-term, historic perspective, we limited the search results to the period from 2014 to 2018.

As described previously, we included papers from five top-tier peer-reviewed conferences that welcome UPS papers. While there are other venues that publish UPS papers (e.g., Network and Distributed System Security Symposium, The Web Conference, UbiComp), we limited our selection to conferences primarily focused on either security/privacy or HCI and that provided a searchable database. We also did not consider journals as most UPS papers are published at conferences and some that are published in journals are extended versions of conference papers. A search of the ACM "Transactions" journals found that we omitted relatively few papers by omitting journals. Nevertheless, a review of UPS papers in a wider array of journals might be insightful.

There were some types of data that we did not code for, but that should be considered for future research. For instance, future studies could investigate differences between online or in-person studies, and single-session versus longitudinal studies. A detailed analysis of where participants are located would also give compelling insights into certain geographic areas that are understudied. We did not analyse whether studies reference certain theories or frameworks (e.g., grounded theory, mental models, self-determination theory), which would be an interesting focus point for future research. Looking back at our results, we can also see that drawing tasks seemed to be used in some of the studies in our sample, and we have observed these tasks in more recent studies as well. We did not specifically focus on drawing tasks, but analysing how drawing tasks are used in UPS studies seems to be a relevant analysis to conduct. In our sample, we could see that a wide variety of compensation styles was employed, ranging from voluntary participation, to course credit, to raffles, to direct financial compensation, which we did not systematically compare and analyze. Future studies could analyze research participant compensation in UPS in more detail, and perhaps contribute to a "standard" of participant compensation. In addition, we recorded the number of participants in each study but did not record the number of experimental conditions. An analysis of participants per experimental condition and associated statistical power could provide added insights. Finally, our sample includes a number of studies that recruited experts as participants. We did not focus in detail on how experts contributed during their study participation.

2.5. Results

In this section, we first provide an overview of our data set and the methods used (responding to RQ1), and then focus on how researchers represent risk and assess participants' responses to risk in their studies. We describe the "tools" used by researchers to represent risks to research participants (prototypes, scenarios, educational interventions) and which study methods (e.g., experiments, surveys) coincide with which risk representation modes (RQ2). Finally, we analyze the use of deception (RQ3).

2.5.1. Data set description

In this section we provide an overview of our data set. We include descriptive statistics about the distribution of papers across venues and publication years. Further, we summarize high-level information about the papers, including the topics studied, research objectives, and study methods. In short, our data set included 284 UPS papers, with a large percentage published at SOUPS or CHI. The most frequent topics were authentication and privacy or security attitudes. Most of the papers had an experimental or descriptive objective and replications were rare. Experiments, interviews, and surveys were common study methods, and crowdsourcing and non-representative convenience samples were frequently used to recruit participants.

2.5.1.1. Publication venue

As shown in Table 2, the **most frequent conference venues** for UPS over the past five years, as defined by our search query, were SOUPS (n=115 included papers) and CHI (n=96). Not surprisingly, our data set includes almost all of the papers published at SOUPS during this time period, the only publication venue that specifically focuses on usable privacy and security topics. The papers were fairly well distributed across the five years of the study, as shown in the Appendix, Table 16.

	Papers published at conference (2014-2018)	Included papers	Percent included
SOUPS	119	115	97
CHI	2675	96	4
ACM CCS	664	28	4

USENIX Security	391	25	6
IEEE Security and Privacy	277	20	9

Table 2: Number of papers published at conference and papers included in our sample

2.5.1.2. Topics

Papers were coded into mutually exclusive, broad categories to obtain a high-level overview of frequently studied topics. The most frequently addressed topics in our analysis were *authentication* (25% of papers, n=72), followed by papers on *privacy perceptions, attitudes, and behaviors* (19%, n=55) and *security perceptions, attitudes, and behaviors* (16%, n=46). *Access control* (7%, n=20) and *security for admins and developers* (6%, n=18) were other frequent topics, as well as *encryption* (5%, n=15) and *privacy transparency and choice mechanisms* (5%, n=14). For the remaining topics, refer to Table 3. In section 2.5.2.3., we explain how risk was represented within each topic.

	Frequency	Percent
Authentication	72	25
Privacy perceptions, attitudes and behaviors	55	19
Security perceptions, attitudes and behaviors	46	16
Access control	20	7
Security for admins and developers	18	6
Encryption	15	5
Privacy transparency and choice mechanisms	14	5
Security indicators and warnings	12	4
Multiple	11	4
Privacy-enhancing technologies	11	4
Social engineering	10	4
Total	284	100

Table 3: Topics addressed in papers.

2.5.1.3. Objectives

We categorized papers according to their most important objective, which was either experimental, descriptive, or relational. Experimental research partitions participants into

equivalent groups and measures the influence of different experimental manipulations applied to each group (Stangor & Walinga, 2018). Descriptive research provides a snapshot or summary of participants and their opinions or behavior with respect to a particular context or setting. Relational research is designed to discover relationships among variables (Stangor & Walinga, 2018), for example the impact of certain demographics or past experiences on behavior. Overall, most included papers had an experimental (41%, n=115) or descriptive (31%, n=89) objective. 5% (n=13) of papers had a relational objective, and the remaining papers combined multiple objectives (see Appendix, Table 17). Note that we did not classify experimental research as combined with descriptive if descriptive results were used only to characterize the experimental population and were not an important objective of the study.

Replication studies appear to be rare in UPS. Our dataset includes 4 replications, and one partial replication. Replications were conducted for multiple reasons. For example, Bravo-Lillo et al. replicated the experimental methodology documented in an earlier study, but added new conditions (Bravo-Lillo et al., 2014). Another study replicated an earlier experiment in order to assess its robustness (Canfield et al., 2017).

2.5.1.4. Study methods

The papers from our sample predominantly used *experiments*, *surveys,* and *interviews*, or combinations of these study methods (see Table 4). We classify *experiments* as procedures where experimental conditions were manipulated, and the effect of this manipulation was measured. When study authors referred to an "online experiment" in their study, but without apparent experimental conditions, we instead classified the respective studies as *surveys*. *Surveys*, in our analysis, are different from *interviews* in that they usually took place in a written questionnaire form (on paper or online) without a conversation-style interaction between the researcher and the research participant. We coded experiments involving an oral debriefing phase as *experiments* only, not *experiments and interviews,* as we did not consider this debriefing phase an interview study in its own right, and debriefing phases were not always analyzed as rigorously as interview studies typically would be.

Less common study methods included analyses of existing datasets and log analysis. In addition, we found occasional use of focus groups, co-creation methods, list experiments,

observation studies, workshops, vignette studies, and diary studies. In section 2.5.2.2., we explain how risk was represented in studies using each method, and provide examples.

	Frequency	Percent
Experiment	99	35
Interview	36	13
Survey	34	12
Survey and Data Logs	12	4
Analyse Dataset	11	4
Survey and Interview	11	4
Experience Sampling Method	8	3
Survey and Experiment	8	3
Methods and Combinations with 5 or less occurrences	65	23

Table 4: Combinations of study methods in our sample (full table in Appendix, Table 18).

2.5.1.5. Participants

As shown in Table 5, the analyzed papers relied heavily on easily accessible populations, in particular crowdsourcing (n=106), non-representative convenience samples (n=79), and students (n=66). Most crowdsourcing studies used Amazon Mechanical Turk (n=86). Non-representative convenience samples here refer to recruitment of easily accessible, undefined population groups (e.g., through flyers in the neighborhood of the university, or general snowball sampling). In contrast, when researchers specifically recruited students, we used the separate category students. Users of specific technology (referring for instance to users of VR glasses, Android users, or users of specific social networks) were studied as well (n=37). Employees (n=33) also played a frequent role.

The number of participants varied considerably between studies, as shown in Appendix, Table 19. Interview studies tended to have the fewest participants among the frequently used study methods, with a median of 21 and a maximum of 200 participants. Surveys and log analysis studies tended to have many more participants. The median number of participants for surveys and log analysis was 307 and 100, respectively. However, some of these studies had over 10,000 participants.

Type of participants	Frequency

Crowdsourcing (incl. MTurk, Prolific, Google Consumer survey, other crowdsourcing)	106
Non-representative convenience sample	79
Students (incl. Computer Science)	66
Users of specific technology	37
Employees (incl. University employees)	33
Experts (security experts and other experts)	22
Other	13
Special user groups (incl. People with impairments, children or teenagers, women in particular, LGBTQ)	12
Developers	10
Representative sample	7
Security Behavior Observatory (SBO)	4
Recruitment not mentioned	3

Table 5: Number of papers that include a certain type of participants. One paper can include multiple types of participants.

We were interested in understanding to what extent underrepresented populations were studied in user-centred privacy and security studies and how researchers represented risk to them. For the purpose of this article, understudied populations include geographically rarely included populations (based on our sample from top-tier UPS venues), disabled persons, members of the LGBTQ+ community, certain age groups (older adults, children and teenagers), and any other special population that has not been widely studied. In total, 20 (7%) papers focused on these understudied populations, 8 of which include geographically understudied, 4 include people with disabilities, 4 papers include children, 2 include members of the LGTBQ+ community, 2 papers include survivors of intimate partner abuse.

2.5.1.6. IRB or ethics board approval

Recently, some publication venues have started requiring that authors mention ethics board reviews for all papers with human-subjects studies. However, this was not commonly required during the time period in which the papers we reviewed were published. About two-thirds of the papers we analyzed discussed IRB or ethics board

approval. 56% (n=159) of papers stated they had obtained approval or received exempt approval, 35% (n=99) did not mention whether they had approval, 4% (n=10) of papers were from an institution without approval procedure. The remaining papers either described a corporate internal review process, or claimed to be exempt from needing approval (see Appendix, Table 20). A number of papers that describe research conducted in the US stated that they were "approved exempt" or "received exempt approval." As this is actually a category of IRB approval in the US that requires review by the IRB, we include these in the papers that received approval and distinguish them from those that are exempt from needing approval. From talking to some of the study authors who did not mention IRB or ethics board approval in their studies, we learned that they did actually receive approval but did not mention it in their papers. It is likely that the percentage of papers that received IRB or ethics board approval is actually higher than what we report based on the statements in the papers.

2.5.2. How Risk is Represented and Measured

Many UPS studies focus on understanding how participants perceive security or privacy risk or how they use a tool or otherwise respond to a situation involving privacy or security risk. We were interested in how researchers represent risk to participants and how they approach the assessment of risk response. In addition, we investigated how risk was represented to understudied populations.

We categorized the way researchers represented risk to their participants. The categories included *simulated risk* (e.g., through the use of scenarios participants should imagine themselves in), *naturally occurring risk* (e.g., through observation or self-reported measures of naturally occurring behavior), *mentioned risk* (e.g., a questionnaire where participants were presented with hypothetical situations) or *no representation of risk*. In some cases, researchers using simulated risk in their studies did not inform participants about a scenario, but instead used deception to make a simulated risk appear to be naturally occurring; we classify these as simulated risk.

The majority of papers used either naturally occurring or simulated risk. Certain study objectives coincided with certain types of risk representation. For example, experimental studies used mostly simulated risk, and descriptive studies used naturally occurring risk.

In addition, risk representation also varied by topics. For instance, studies on privacy transparency and choice mechanisms and studies on authentication mostly used simulated

risk, while studies on access control, privacy-enhancing technologies, and security perceptions, attitudes and behaviors used mostly naturally occurring risk. Response to risk was measured mostly through self-reported measures, either on their own or in combination with observed measures. A smaller proportion of papers relied on purely observational measures.

2.5.2.1. Risk representation

We see that the vast majority of papers represent risk to participants in some way: 37% of papers used *naturally occurring risk*, 35% used *simulated risk*, 16% combined *multiple* approaches, 7% did not attempt to represent risk in any way to their participants, and only 6% *mentioned* risk to participants (Table 6).

	Frequency	Percent	Examples
Naturally occurring	105	37	A password reset email is sent to LinkedIn users, and its effectiveness is measured through an online survey of LinkedIn users (Huh et al., 2017). Threat modeling is introduced in an enterprise setting, and its effectiveness is evaluated (Stevens et al., 2018).
Simulated	98	35	Participants in an online experiment are asked to imagine they are creating a password for an account they "care a lot about, such as their primary email account." (Ur et al., 2017a) Developers are asked to roleplay and imagine they are responsible for creating the code for user registration and authentication of a social networking platform (Naiakshina et al., 2017a). Participants are asked to test a banking prototype for one week and are led to believe that the objective was to test the usability of the application (deception). After some days, the authors simulate a phishing attack to test the effect of personalized security indicators (Marforio et al., 2016).
Multiple	45	16	Participants in an online survey self-report behaviors in updating workplace passwords (naturally occurring), and their attitudes toward four password-management behaviors (mentioned) (Habib et al., 2018).
None	19	7	Researchers analyze multiple gesture recognizers and evaluate them based on various security criteria, and use pre-existing datasets to verify how well their prototype of a new authentication system works (Liu et al., 2017). Participants were asked to type sentences on phones provided to them by the researchers without knowing what the purpose was. The researchers used the data to understand the effect of participant movement on keystroke dynamics (Crawford & Ahmadzadeh, 2017).

Mentioned	17	6	In an online survey, participants are first provided with a description of the "legalese" language, and are then asked to encode clauses of a privacy policy in legalese terms (Sen et al., 2014).

Table 6: Risk representation and examples (N=284).

It might seem surprising that there are studies that do not attempt to create a perception of privacy and security risk. But indeed, there were studies that focused solely on the instrumental aspects of usability of a privacy or security tool. Fuller et al. (2017) tested the usability of cryptographically-protected search systems with participants who were not made aware of the privacy features. The authors evaluated participants' perception of the performance of the search system, rather than their perception of potential security and privacy risks. Others opted for evaluating users' perception of security practices. Oltrogge et al., (2015) conducted a survey with 45 developers for qualitative feedback on the implementation of TLS certificate pinning with the goal of creating a usable tool for implementing secure certificate validation. Chatterjee et al. (2016) had MTurk workers type leaked passwords under time pressure, yet without informing them about the security- and privacy-related rationale of the task. Lastly, some studies had participants talk about experiences without mentioning security or privacy, thus not creating any perception of risk. In all these studies, there was no attempt, indeed no need, to involve users in any security rationale and perception of risks.

2.5.2.2. Risk representation by study objective and method

Some risk representation approaches were frequently associated with particular study objectives, as shown in Figure 1. *Experimental* studies mostly use *simulated risk* (64%), *descriptive* studies frequently rely on *naturally occurring* (67%), while *relational* studies rely on *naturally occurring risk* (23%) and multiple risk *combinations* (46%).

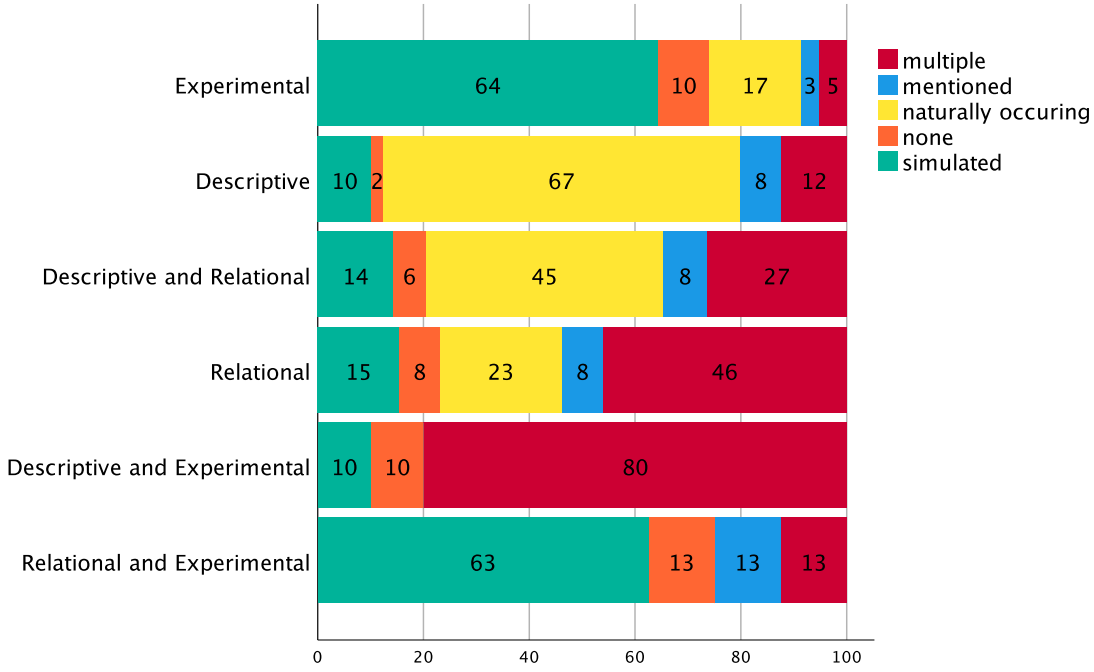


Figure 1: Crosstab Objective and Risk Representation (percentage of all studies with certain objective).

We observed that the approach to risk representation also varied considerably based on the type of study methods used, as detailed below.

Experiments

Most papers using only *experiments* used *simulated risk* (73%), as shown in Table 7, as this allowed researchers to introduce risk in a controlled way in all experimental treatments. However, 12% of experiments had *no representation of risk*. Indeed, some *experimental* studies had participants complete an *assigned security or privacy task*, yet with *no induced privacy and security risk* perception. In these cases, participants did not know that the task they were completing was privacy or security-relevant, and the authors did not intentionally create a perception of privacy and security risk. For instance, Shirvanian & Saxena, (2014) asked their participants to read out checksums, but did not inform participants as to why this was necessary. Similarly, in another study, participants were asked to transcribe audio-captchas, but they were not aware of what they were doing (Meutzner et al., 2015).

	Frequency	Percent
Simulated	72	73

None	12	12
Naturally occurring	9	9
Multiple	3	3
Mentioned	3	3

Table 7: Risk representation for experiments (papers that only use experiments, n=99)

One seemingly contradictory combination in the experimental category concerns a study with an *assigned security or privacy task*, yet *naturally occurring risk*. In this case, researchers collect and analyze participants' real passwords using semantic transformation, as well as their reasoning behind their habits (Hanamsagar et al., 2018). Given that participants used their own passwords to connect to their real accounts, the risk was naturally occurring even though the login task was assigned to them by the researchers.

Surveys

Papers that used a survey-based approach, most frequently used *naturally occurring* risk or *multiple* risk representations, but were less likely to *mention* or *simulate* risk, as shown in Table 8.

	Frequency	Percent
Naturally occurring	11	32
Multiple	9	27
Mentioned	5	15
Simulated	5	15
None	4	12

Table 8: Risk representation for surveys (papers that only use surveys, n=34)

When risk is naturally occurring, participants are asked about real-world behaviors in actual situations. For example, Felt et al. (2016) surveyed Chrome users about existing security indicators. Similarly, Redmiles and colleagues (2016) investigate how users' security beliefs, knowledge, and demographics correlate with their sources of security advice, and how all these factors influence security behaviors.

Studies with mentioned risk do not ask participants about their own experiences and also do not involve a scenario to simulate risk. For example, Eiband et al. (2017) presented

participants with a sketch depicting a person watching another person's screen to introduce the concept of shoulder surfing.

The difference between mentioned and naturally occurring risk can best be explained through a study that combines both mentioned and naturally occurring risk. Shay et al. (2014) for instance conducted a survey regarding account hijacking experiences. They first asked participants whether somebody had broken into one of their personal accounts. Participants who had experienced a compromise were asked about their experience (naturally occurring risk), those who had not yet experienced a compromise were asked to think about their primary personal email or social networking account throughout the survey. These participants were then asked about whom they were concerned might break into their accounts, how they thought accounts were compromised and other hypothetical questions. This second group was thus exposed to mentioned risk.

When risk was simulated in a survey study, a prototype or scenario was used. For instance, in a study by Karunakaran et al. (2018), participants were asked to imagine that they were victims of a data breach. This scenario simulated the risk.

In some cases, the survey was not situated in a privacy or security-relevant context for participants so we classify it as having no mention of risk. Oltrogge et al. (2015) for instance surveyed a sample of developers about their knowledge of certificate pinning, obstacles to pinning implementation, and how to help developers implement certificate pinning. Given that the questions concerned knowledge, obstacles, and wishes in general, there was no induced risk perception.

Interviews

Interviews most frequently used naturally occurring risk, as shown in Table 9, to investigate people's real-life privacy and security experiences.

	Frequency	Percent
Naturally occurring	26	72
Mentioned	4	11
Multiple	4	11
Simulated	2	6

Table 9: Risk representation for interviews (studies that only use interviews, n=36)

For instance, Rashidi and colleagues (2018) interviewed undergraduates to understand their real-life privacy workarounds in the context of pervasive photography. Similarly, Ahmed and colleagues (2015) interviewed people with visual impairments about their real-life privacy concerns. In another study with naturally occurring risk, kids played with connected toys in a lab setting with their parents present. The parents were interviewed about their mental model of the toys, with questions about parental controls, privacy, and monitoring of what the child says to the toy. The children were interviewed about their mental model of the toy and privacy perceptions, asking them if they thought the toy could remember what they told it, if they would tell the toy a secret, and whether their parents could find out what they told the toy (McReynolds et al., 2017). Naturally occurring risk was also used by two studies exploring security and privacy in an organizational context. Conway et al. (2017) interviewed bank employees about organizational privacy and security practices, and Haney et al. (2018) interviewed employees in a company for cryptographic products.

Interview studies with simulated risk typically use scenarios to *simulate* risk. For example, Vaniea et al. (2014) use a set of hypothetical scenarios to elicit stories about software update experiences. In this study the interviewer asked participants to imagine how they would respond to scenarios such as being prompted to restart an internet browser mid-task or seeing that a large number of urgent Windows updates were available. Sometimes interview studies combined *naturally occurring* risk with *simulated* risk. In one study, participants had to create passwords for three hypothetical websites while thinking aloud (simulated risk), and were then interviewed about their strategies, as well as general habits related to password creation (naturally occurring risk) (Ur et al., 2015).

Log Analysis

24 papers include the use of *log analysis,* and 4 papers use log analysis alone. Data logs usually use *naturally occurring risk*. One study, for instance, created and deployed a privacy-preserving advertising platform. The authors report on the number of opt-in users and describe their behavior by analyzing usage logs (Reznichenko & Francis, 2014).

Analysis of existing datasets

22 papers include the *analysis of existing datasets,* and 11 papers use the analysis of existing data sets alone. The analyses of datasets usually use *naturally occurring risk*. One

example is a study where researchers study the reaction to news articles by analyzing public comments (Fiesler & Hallinan, 2018).

Rarely used methods

Our data set includes eight *experience sampling* studies. Seven of the experience sampling studies used *naturally occurring risk*, and one used *simulated* risk. As an example for naturally occurring risk, Reeder et al. (2018) conducted an experience sampling study investigating people's reaction to web browser security warnings where they surveyed users in-situ (after being exposed to a warning) to understand their reasons for adhering or not to real warnings. Yang et al. (2016) conducted an experience sampling study using *simulated* risk. Participants were alerted multiple times a day to complete password creation or recall tasks. The passwords were for accounts that were used purely for the study, thus simulating the risk to participants.

Our data set includes six *focus group* studies, five of which combine focus groups with other methods. The majority of these papers use *naturally occurring risk*. For instance, (Sambasivan et al., 2018) conducted focus groups with 199 women from India, Pakistan, and Bangladesh focused on understanding how women perceive, manage, and control their personal privacy on shared phones. The authors identified five performative practices that participants employed to maintain individuality and privacy.

Our data set also includes three *diary* studies, all in combination with other methods, which use *naturally occurring or combinations of risk*. For example, Mare et al. (2016) gave participants smartwatches to log any authentication events as they went about their daily lives as part of a digital diary study.

We examined only three studies that used *workshops*, all in combination with other methods. The studies mostly *combined risk representation.* For example, Pearson et al. (2017) conducted workshops in which they presented design probes to explore the notion of "chameleon devices," mobile devices that blend into their background with the objective of making them more secure and private.

We examined two each of *vignette studies*, *list experiments*, and *co-creation studies*. The vignette studies were experimental studies that used *simulated risk*. For example, Votipka et al. (2018) conducted a *vignette* study to investigate user comfort level with resource accesses that happen in the background, without any visual indication of resource use. They find that both when and why a resource is accessed influences user comfort. The list

experiments *mentioned risk* to participants. For example, Usmani et al. (2017) conducted a list experiment to investigate the prevalence of social insider attacks, where attackers know their victims, and gain access to their account through directly using their device. The list experiment method allowed the authors to explore the sensitive topic of social insider attacks, finding that an estimated 24% of participants had perpetrated social insider attacks.

The *co-creation* studies used *simulated risk* and *naturally occurring risk*. For example, Egelman et al. (2015) created and evaluated a set of privacy indicators for ubiquitous sensing platforms. Using a crowdsourcing approach, they collected 238 sketches from participants based on 14 ubiquitous sensing concepts to understand how end users conceptualize the concepts. Using the themes identified in participants' sketches, the researchers then created icons for each concept and evaluated their comprehension rate in comparison to icons created by a designer. The icon sets performed similarly well at conveying the privacy concepts, with certain crowdsourced icons even outperforming designer-made icons.

2.5.2.3. Risk representation by topic

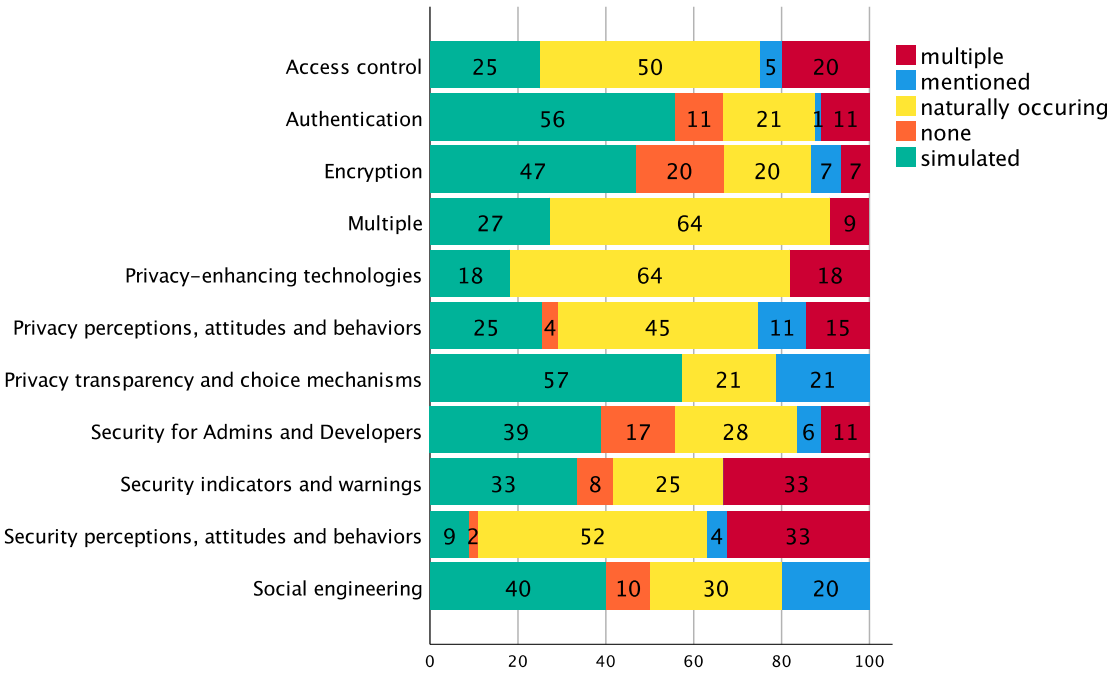


Figure 2: Crosstab Topic and Risk representation (percentage of all papers in topic).

Depending on the topic being studied, risk representation varied, as shown in Figure 2. Studies on *privacy transparency and choice mechanisms* and *authentication* mostly used simulated risk (57%). Studies on *access control*, *privacy-enhancing technologies,* and *security perceptions, attitudes and behaviors* applied mostly *naturally occurring risk* (50%, 64%, and 52% respectively).

Not surprisingly, studies on the topics that were mostly studied experimentally (Figure 2), such as *authentication*, *encryption*, *privacy transparency and choice mechanisms,* and *social engineering*, were more likely to use *simulated risk*, which is induced through the use of an experimental setup. On the other hand, studies on topics that frequently had descriptive objectives often applied *naturally occurring* or *mentioned* risk since descriptive methods usually offer less opportunity for risk simulation and are better suited to evaluate real-life risks or mentioned risks using methods such as interviews or surveys.

Additional analysis by topic, beyond risk representation, can be found in the appendix.

2.5.2.4. How response to risk is measured

We categorize papers based on their approach to collecting data about how participants perceive and respond to risks. We analyze whether papers use self-reported measures, observed measures, or combine both for data collection (Table 10).

	Frequency	Percent	Examples
Both observation and self-report	131	46	Authors combine semi-structured interviews and observe participants' use of a login procedure (Holz & Bentley, 2016). The researchers observed the participants and also asked questions about the authentication process. Participants were asked to create passwords in a lab setting, and were then interviewed about their process (Ur et al., 2015). Participants were observed and self-reported their experience.
Self-report	119	42	Researchers use a combination of interviews and a survey to identify privacy panic situations (Angulo & Ortlieb, 2015). Researchers conduct interviews with visually impaired participants to understand their privacy concerns and techniques to protect their privacy (Ahmed et al., 2015).

Observation	34	12	Researchers evaluate HTTPS adoption from a user perspective by collecting aggregate user metrics from major web browsers (Felt et al., 2017). Researchers analyze Twitter data to understand longitudinal exposure and withdrawal of socially shared data (Mondal et al., 2016).

Table 10: Approach to collecting data regarding risk response (N=284).

2.5.2.5. Understudied populations and risk representation and measurement

20 (7%) papers focused on understudied populations (see Section 2.5.2.5.). In terms of risk representation, 13 of these 20 papers used *naturally occurring* risk, 4 used *multiple* risk representations, 2 *mentioned* risk to research participants and 1 used *no* representation of risk. In line with this observation, 17 of these 20 studies had a *descriptive* or *descriptive and relational* objective and mostly used methods like *interviews* or *surveys*. Only 2 studies had an *experimental* objective (Lastdrager et al., 2017; Qahtani et al., 2018), suggesting that it is rare to assess the suitability of security and privacy tools for these populations. Lastdrager and colleagues (2017) study the effectiveness of anti-phishing training for children, and asked pupils to distinguish phishing emails from non-phishing emails after receiving training to recognize phishing. Qahtani et al. (2018) studied the effectiveness of fear appeals for the smartphone locking behavior of Saudi-Arabians, while also highlighting some of the methodological challenges of conducting research in Saudi-Arabia. Note that, while these populations are rarely included in the papers of our analysis, our sample of papers did not include specialized conferences that focus specifically on these populations. Nevertheless, there seems to be a research gap of these population groups at the venues we studied.

In comparison with these results, papers involving crowdworkers mostly relied on simulated risk, and, less frequently on naturally occurring or combinations of risk.

2.5.3. Tools for risk representation and measurement

In this section, we describe and analyze the "tools" UPS researchers use to represent risk to participants, focusing on assigned tasks, prototypes, scenarios, deception, educational interventions or incentives for secure behavior. We describe the characteristics and trends that were associated with these tools.

The majority of papers either used no assigned task or a security/privacy related task. Approximately a third of papers involved a prototype and almost a third of papers involved

a scenario. The use of deception was relatively rare in our sample and was associated with experimental studies and simulated risk. Only a small number (approximately 2%) of papers used educational interventions or incentives for secure behavior.

2.5.3.1. Assigned tasks

We categorize papers based on the tasks (if any) that are assigned to research participants. We analyze whether papers assign tasks to participants that are relevant to *security or privacy*, whether the tasks are *unrelated* to security or privacy, or whether *both* security and privacy related and unrelated tasks are used, as shown in Table 11. Not surprisingly, most papers that included an assigned task, assigned a task related to security or privacy. Sometimes participants were assigned tasks unrelated to security or privacy, often so that researchers could observe routine or incidental security tasks that participants had to perform as part of completing the assigned task without focussing participants' attention on security or privacy.

	Frequency	Percent	Examples
No assigned task	137	48	Participants' data logs are collected over multiple months to understand realistic security and privacy behaviors, and some of these participants are invited to participate in interviews (Forget et al., 2016). In an experience sampling study, participants answer to in-situ surveys throughout the day in response to certain trigger events related to permission settings (Bonné et al., 2017).
Security/privacy related task	102	36	Novice participants are instructed to attempt to send encrypted email (Ruoti et al., 2016). Participants are asked to use a new authentication method (Das et al., 2017).
Unrelated task	27	10	Participants are asked to perform unrelated tasks on an email platform. They are asked to find a certain email, schedule a calendar appointment and look up a contact. These tasks served as a reason for participants to login to the email platform, which was the interaction researchers were interested in (Holz & Bentley, 2016). Children are invited to the lab and asked to play with connected toys (McReynolds et al., 2017).

Both security/privacy related and unrelated task	18	6	Participants are asked to complete unrelated tasks that represent common smartphone activities (text entry activity, email reading activity). During the unrelated tasks, the participants were triggered mid-task to re-authenticate (S/P task) (Agarwal et al., 2016). In a developer study, participants were asked to complete coding tasks. One did not have direct security implications (URL shortener), and is thus an unrelated task. The other tasks had direct security implications (credential storage, string encryption) and are thus security-relevant tasks (Acar et al., 2017).

Table 11: Assigned tasks that participants were asked to complete (N=284).

2.5.3.2. Studies including prototypes

90 (32%) studies included a *prototype*, that is a new solution such as a textual message, an icon, or an interface that the authors present to participants, sometimes in a low-fidelity or non-interactive form. The risk representation of studies involving prototypes was usually simulated (54%) or naturally occurring (20%). 16% of the studies combined multiple ways of risk representation. For example, Vaziripour et al. (2018) made changes to the authentication ceremony in the secure messaging app Signal and evaluated the effect of these changes in a between-subjects experiment. Harbach et al. (2014) explored the effect of novel personalized security decision dialogues on the Android app installation process. Overall, studies involving prototypes follow the overall trends in the data with mainly convenience samples, many experimental and descriptive studies, and a high percentage of authentication papers. It is interesting to note that while prototypes appear in about a third of UPS studies we analyzed, the majority of the studies in our sample did not include prototypes, suggesting a focus on understanding user perceptions, attitudes, and behaviors as they relate to general concepts or to existing systems rather than proposed new solutions.

Studies involving prototypes were usually experimental (70%) or descriptive (16%). Risk response assessment for prototype studies usually included both self-reported and observed measures (68%), while 18% used self-reported measures alone and 14% used observed measures alone. Most studies that include prototypes study topics related to authentication (37%) or privacy perceptions, attitudes and behaviors (12%). 58% of papers including prototypes asked participants to complete security or privacy related tasks, 16% assigned no specific tasks, and 13% asked participants to complete unrelated tasks, 13%

asked participants to complete a combination of security and privacy-related and unrelated tasks.

2.5.3.3. Studies including scenarios

75 (26%) studies included *scenarios* in which the researchers asked participants to imagine themselves being in a certain situation. Studies involving scenarios mostly used simulated risk representation (64%) or combined multiple ways of representing risk (25%). A smaller proportion of the studies also used naturally occurring risk (9%). Several studies asked participants to imagine that their email account had been compromised and that they were asked to change the password (Komanduri et al., 2014; Melicher et al., 2016; Segreti et al., 2017; Shay et al., 2015; Ur et al., 2017b). Another study asked participants to play the role of managers responsible for access review in an organization (Jaferian et al., 2014). Hang et al. (2015) recruited participants in pairs who had a close relationship for a study on a secure fallback authentication scheme. The authors asked participants to engage in a roleplay, instructing one of them to play an adversary, whereas the other participant played a legitimate user.

Overall, scenarios were used by researchers as an easy way to simulate risk in a wide variety of research settings. For instance, scenarios were used in a lab setting by asking participants to roleplay and attempt to send each other a fictitious credit card number via secure messaging (Vaziripour et al., 2017). Scenarios could also be used in a survey or interview setting to introduce hypothetical scenarios that participants should situate themselves in, as used for instance in one study that presented interview participants with hypothetical scenarios related to software updates, in combination with probing questions (Wash et al., 2014).

2.5.3.4. Studies including an educational intervention

Seven papers included an *educational intervention*. Wash and Cooper (2018) attempt to educate their participants on how to detect phishing attempts, and Lastdrager et al. (2017) evaluate the effectiveness of anti-phishing training for children. Stevens et al. (2018) describe the effects of introducing staff of a digital defense organization to threat modelling, and Warshaw et al. (2016) use teaching sessions in an effort to improve adults' inference literacy (i.e., the beliefs and misconceptions people have about how companies collect and make inferences from their data). Two papers use informational videos to educate participants about smartphone locking (Albayram et al., 2017; Qahtani et al.,

2018). In one paper, participants first took part in a user test including three secure email systems, and in the post-study interview, the researchers described the actual security model of the system to the participants. After hearing these descriptions, participants were asked whether their opinions regarding any of the systems had changed (Ruoti et al., 2018).

Almost all of the papers including an educational intervention had an *experimental* objective (86%). In terms of risk representation, there was no clear tendency: two papers *mentioned* risk to research participants, two used *naturally occurring* risk and two *simulated* risk to their participants.

Although educational interventions were fairly rare, we observed (but did not code) a number of papers that included nudges or small interventions as part of a prototype tool. For example, several papers (Shay et al., 2015; Ur et al., 2017b) included interventions that provided feedback to users on password strength as part of a password-creation interface. These sorts of integrated interventions may be easier to deploy and more likely to be seen by users than a training program or educational video.

2.5.3.5. Studies including incentives for secure behavior

The field of behavioral economics frequently uses financial incentives to model real world incentives in an experimental setting. However, these seem to be relatively rare in UPS studies. Only five (2%) papers included financial incentives for secure behavior, usually with the intent of motivating participants to try to perform well on a security or privacy-related task that was part of the study. Indeed, all five papers included an *assigned security or privacy-relevant task*. Three of the papers used *simulated* risk, one used *combinations* of risk representation, and one *did not attempt* to simulate risk. All of the studies had an *experimental* objective, and four of them also included a *scenario* participants should situate themselves in. Two of the papers included *prototypes*. Four of the papers were related to *authentication* and one to *encryption*. None of these papers involved *deception*.

These studies all encouraged participants to try to perform well on their assigned security or privacy task by making a part of their compensation contingent upon successful completion. In the absence of this compensation structure, participants might not be motivated to try to perform the assigned task well as there would be no consequences for poor performance. A user who performs a real-world security task poorly risks a security-related consequence (e.g., an account compromise) or an inconvenience (e.g., having to

reset a forgotten password). A financial incentive provides a substitute risk to participants: the risk of losing the contingent compensation. For instance, Vaziripour et al. (2018) asked participants to complete the authentication ceremony of a secure messaging app, which they had attempted to improve for better usability. Participants received a base pay of $7, and they could receive a bonus of $3 if they managed to perform the task safely. Tan et al. (2017) conducted an online between-subjects experiment in which participants were asked to imagine they were an accountant who was requesting social security numbers from employees using a secure messaging system. Participants were asked to do a fingerprint verification for each request and researchers were interested in whether participants noticed mismatched fingerprints. As an incentive for fast and accurate performance, participants were told that the fastest 15% of participants who performed the task correctly would receive a $1 bonus in addition to a base compensation of $3. Similarly, Huh et al. (2015) simulated the PIN setup page of a made-up bank, informing participants that they would use the PIN for card purchases. Each participant was assigned a specific technique for memorizing the PIN, and they received an incentive of $0.25 if they came back later, and an additional $0.25 if they were able to remember the PIN.

Some security economics papers go a step further and use financial incentives as part of a model of participants' valuation of privacy or security protections. For example, in a UPS paper that was published at a conference on economics and computation (thus, not in our sample), Redmiles et al. (2018) gave participants a small deposit into an online account and offered them the opportunity to add two-factor authentication (2FA) to their account. They were told the probability that their account would be hacked and they would lose the balance, both with and without 2FA enabled. The researchers varied these probabilities across the experimental treatments and were able to observe whether participants made rational decisions about whether it was worth their time to enable 2FA.

2.5.3.6. Studies involving deception

Sixteen papers included *deception*, comprising between 4% and 10% of UPS papers from each of the five venues we studied. In five additional papers, authors referred to their own protocols as deceptive; however, we instead categorized them as *partial disclosure* to avoid priming participants to think about privacy and security specifically. For instance, one of the studies split software developers into two groups, which they refer to as "non-priming" and "priming". The non-priming group was told that the study was about API

usability, whereas the priming group was told that the study was about secure password storage. While the researchers called this deception, we are not considering studies that simply avoid priming participants as deception studies (Naiakshina et al., 2017b).

We first provide an overview of the characteristics of deception studies, before going into the details of how exactly participants were deceived and for which objectives. Ten papers describe a *debriefing procedure* that exposes the deception to participants at the end of the study, the remaining six papers do not describe any participant debriefing.

Papers involving deception typically mentioned IRB approval: 11 studies had *IRB or ethics board approval*, three studies were from an *institution without approval procedure*, one study went through an *ethics review in industry,* and one study *did not mention IRB-related information*.

The use of deception was highest for papers on *social engineering* (30% of papers in this category used deception) and *privacy transparency and choice mechanisms* (21% of papers in this category used deception). More information on the topics of deception studies can be found in Appendix, Table 21. 75% (n=12) of deception papers had an *experimental* objective, and measurements for papers including deception often combined *observed and self-reported measures* (50%). As shown in table 12, most deception studies were framed to avoid focusing participants on security or privacy tasks and most did *not use assigned tasks* (38%) or assigned only *unrelated tasks* (38%). As shown in table 13, the majority (69%) of papers involving deception used *simulated risk*. In terms of study methods, the majority of papers involving deception were based on an *experiment* (69%, see Appendix, Table 22).

	Frequency	Percent	Percentage of papers in that category that use deception
No assigned task	6	38	4
Unrelated task	6	38	22
Both security/privacy related and unrelated task	4	25	22
Security/privacy-related task	0	0	0

Table 12: Assigned tasks in deception studies (n=16).

	Frequency	Percent	Percentage of papers with each risk representation that use deception
simulated	11	69	11
naturally occurring	4	25	4
multiple	1	6	2
none	0	0	0
mentioned	0	0	0

Table 13: Risk representation of deception studies (n=16).

We categorized *deception* papers according to the *type of deception* they used in their study, as shown in Table 14. Sixteen were papers coded as deceptive, eight of these included *deception about the objective of the study*, four papers deceived participants about the *presence of risk* and in four papers, participants were *not aware they were participating in a study* (lack of consent).

A frequent approach was to deceive participants about the *objective of the study*. For instance, Marforio et al. (2016) instructed participants to use their online banking prototype for one week and simulated a phishing attack on the prototype on the fourth day. Similarly, in another study participants were led to believe that their objective was to evaluate browser extensions, but the authors performed a man-in-the-middle attack to spoof Google search results to ensure that only the experimental extensions were installed (Anderson et al., 2015). Participants were asked to find 20 weather extensions within the spoofed search results and evaluate their usability and aesthetics. Three of the manipulated search results at random present an unreasonable permission warning. The control group received conventional warnings that did not change their appearance, the treatment group received polymorphic warnings. The objective was to understand whether polymorphic warnings performed better at encouraging secure behavior.

Some papers deceived participants about the *presence of risk.* For example, Samat and Acquisti (2017) told participants that their information would be shared with a specified audience; however, the data was not shared with anyone outside the primary researchers of the study. In another study, the researchers sent Facebook friend requests from a "fake" account to participants before an interview study. They then confronted participants with inconsistencies in their self-reported interview answers and their observed reactions to the friend request (Rashtian et al., 2014). This study deceived participants because they did

not know that the friend request was part of the study. In addition, participants had not consented to a friend request being sent on Facebook as part of the study.

	Frequency	Examples
Deception about the objective of the study	8	Anderson et al., 2015; Marforio et al., 2016
Deception about the presence of risk	4	Rashtian et al., 2014; Samat & Acquisti, 2017
Lack of consent (deception about study participation)	4	Han et al., 2016; Hu & Wang, 2018; Wash & Cooper, 2018
Total	16	

Table 14: Types of deception studies and examples.

All four papers that did not obtain *consent* from their participants (shown in Table 15) were situated in the context of social engineering and three of them focused on attacks via email such as phishing or email spoofing (Han et al., 2016; Hu & Wang, 2018; Wash & Cooper, 2018). Two of these papers included real attackers among their non-consenting participants. The study of attackers in human-subjects experiments raises ethical issues that may warrant further exploration.

Han et al. (2016) leveraged a web honeypot to attract real attackers into installing phishing kits in a compromised web application. They then presented a sandbox designed to neutralize a phishing kit while keeping it functional. The approach was designed to preserve the victim's privacy, without interfering with the attack process in order to make sure that attackers can compromise the honeypot, install phishing kits, and conduct functional tests without being alerted about the sandbox configuration. The researchers collected and analyzed data from two-categories of unwitting study participants: attackers and victims. The study was conducted at a company and received approval from the company's legal department but not an ethics board. The authors do not describe a debriefing procedure.

Wash and Cooper (2018) sent four simulated phishing emails to university employees over a 30-day period. The employees did not know they were participating in a study. The first phishing email led to an education page where participants were educated about phishing. The authors tested the effectiveness of text variants that explained phishing to potential phishing victims. The study was IRB-approved and the authors discuss ethics. They explain that they did not obtain informed consent to avoid biasing the participants'

response to a phishing email. In addition, they did not debrief participants to prevent participants from thinking that all future phishing attempts are part of a research study. In contrast, a 2009 phishing study that also involved sending simulated phishing emails to a university community took a different approach, first recruiting participants for a study advertised as helping protect the university from identity theft, and later debriefing participants via email (Kumaraguru et al., 2009).

Hu and Wang (2018) describe a study in which participants took part in an online survey on their email usage. Participants were led to believe that this was the entire survey and they were done participating. However, 10 days later the participants were sent a spoofed email impersonating MTurk technical support. After the study, they were sent a debriefing email which explained the true purpose of the experiment and obtained informed consent retroactively. The study received IRB approval. We classified this as lack of consent as the participants had not consented at the time of their participation.

Sahin et al. (2017) tried to understand why a phonebot ("Lenny") was so successful in dealing with spam calls. They used a publicly available dataset of calls where spammers were deceived into thinking they were talking to a human, when in reality, they were talking to the phonebot. The study was conducted by a company and was not reviewed by an ethics board. Spammers were not debriefed either in this study or when the calls were originally recorded.

	IRB or ethics board approval	Ethics discussed	Participant debriefing	Mention of "deception"
PhishEye: Live Monitoring of Sandboxed Phishing Kits (Han et al., 2016)	No (Institution without approval procedure)	Yes	No	No
Who Provides Phishing Training?: Facts, Stories, and People Like Me (Wash & Cooper, 2018)	Yes	Yes	No	No
End-to-end Measurements of Email Spoofing Attacks (Hu & Wang, 2018)	Yes	Yes	Yes	Yes
Using chatbots against voice spam: Analyzing Lenny's effectiveness (Sahin et al., 2017)	Not mentioned	No	No (used existing dataset)	No

Table 15: Papers that did not obtain informed consent before the study began

2.6. Discussion

Our discussion focuses on four observations from our study. First, we discuss the choice of methods in our sample and how they correlated with certain types of risk representation. We also point to some methods that were rarely used in the papers we reviewed that may have advantages for UPS studies. Second, we discuss participant recruitment, including populations that appear to be understudied, and how risk was represented to them. Third, we discuss ethical issues faced in UPS studies, especially those involving deception or involving attackers as human subjects. Finally, we suggest guidelines for the reporting of empirical UPS studies, and propose a structure for their systematic categorization, with a focus on risk representation.

2.6.1. Choice of methods and risk representation

One of our research objectives was to explore how researchers navigate the tension between realistic exposure to risk and ethical, legal, and practical considerations. Overall, the choice of method usually coincided with certain types of risk representation. When picking a method, researchers will thus often face trade-offs with regards to the risk representation they can possibly use in their study design. This review can make such trade-offs more explicit so that researchers can choose accordingly. For instance, experimental studies and simulated risk often coincided, whereas descriptive studies often relied on naturally occurring or mentioned risk. Experimental setups lend themselves to simulating risky situations, for instance through the use of scenarios and prototypes that allow participants to situate themselves in a risky situation. On the other hand, descriptive studies frequently employ methods such as interviews or surveys, which offer less opportunity for risk simulation, but are highly suitable to study real-life risks or mention risky situations.

When measuring the response to risk, researchers frequently used self-reported measures alone or in combination with observed measures. One might think that a combination of self-reported and observed measures would always be the best choice, but the studies in our sample that used self-reported measures clearly focused on subjective perceptions, and did not have the objective of evaluating behavior. In these cases, self-reported measures were most suitable and least intrusive, for instance when understanding privacy panic situations (Angulo & Ortlieb, 2015) or evaluating people's privacy concerns and strategies they use to mitigate these concerns (Ahmed et al., 2015).

Naturally occurring risk was frequently used in self-report studies, for instance in a survey on sources of security advice and behaviors (Redmiles et al., 2016). Using self-report measures in studies involving naturally occurring risk can be a good option, as it minimizes logistical issues and allows participants to control what information they share with researchers. However, participants do not always self-report information accurately for a variety of reasons (e.g., social desirability bias, inaccurate memory). Direct observation of risk response usually offers the most accurate way to observe participants' responses to naturally occurring risk, but depending on the data being collected, it may pose logistical challenges. A study on private-by-design advertising (Reznichenko & Francis, 2014) for instance built a functional prototype of a privacy-preserving ad system, and ran into the challenge of incentivizing potential users to install the prototype on a large scale. They deployed their prototype by bundling it with a popular Firefox add-on that allows viewing documents (e.g., doc, ppt) in the browser without downloading them. Users updating this browser extension were asked whether they wanted to join the experiment, allowing the researchers to collect a large dataset using naturally occurring risk. Felt et al. (2017) used telemetry data from Google Chrome and Mozilla Firefox, which provides user metrics from a subset of users who opted in (for Firefox) or did not opt out (for Google Chrome) to understand the state of HTTPS adoption. As the users were using their browsers to carry out their real-life activities, the risk in this study was naturally occurring. Dunphy et al. (2015) used the Twitter Search API to collect "#password" tweets or the keyword "password," in combination with pronouns and possessive pronouns, to ensure that the data was connected to personal experiences. They collected 500,000 publicly available tweets, which they analyzed qualitatively. As the dataset was public and twitter users freely shared their thoughts on passwords, risk was naturally occurring.

Using *simulated* risk is often a good option when using participants' real accounts could be too invasive, for instance when the researchers would be able to see participants' real passwords, email inboxes, or bank account balances. Simulated risk was often induced through the use of scenarios, for instance by Ur et al. (2017b), who asked participants to imagine they are creating a password for an account they "care a lot about, such as their primary email account." Another example where simulating risk is necessary is when the phenomenon of interest doesn't often occur naturally or involves a prototype that has not yet been deployed. An example is a developer-centered study from Naiakshina et al.

(2017b), who asked a group of student developers who received a carefully designed set of instructions to imagine they were responsible for creating the user registration and authentication of a social networking platform. The authors told half of the participants that the study was about the usability of Java frameworks, while priming the other half by telling them that the study was about secure password storage. By situating all of the participants in the same context, and only varying the task instructions, the researchers were able to isolate the effect of the priming participants to think about security, demonstrating the advantage of simulated risk representation.

Mentioned risk was used rarely in our dataset. One example is a study evaluating the effectiveness of anti-phishing training with children. The authors first provided cybersecurity training for the children on a variety of security topics (e.g., phishing, hacking, cyberbullying). They then evaluated the ability of the children to detect phishing attempts. The authors did not create a scenario for the children and asked them to imagine a situation where they might be led to distinguish the legitimacy, but instead introduced the task as a "cybersecurity test," asking them to decide whether or not "action should be taken" (Lastdrager et al., 2017). If possible, in terms of risk representation, it seems preferable to attempt to simulate risk to research participants, which may explain that mentioned risk was comparatively rare. Simulating risks can help participants situate themselves in a hypothetical situation (e.g., through the use of scenarios, as described above), allowing them to comment on real-life motivations or obstacles that may play a role if they were exposed to the scenario in everyday life. In addition, simulating risks can feel more engaging for research participants, thus potentially leading to more in-depth insights.

Finally, a small number of studies used *no representation of risk.* These studies mostly focused on evaluating the usability of a prototype such as gesture recognizers (Liu et al., 2017) or keystroke dynamics (Crawford & Ahmadzadeh, 2017). While these prototypes are components of authentication systems, these studies focused only on evaluating usability of the prototypes on their own, without providing the context to participants and without any mention of risk. Nonetheless, it might still be relevant to simulate risk as it could impact participants' motivations to complete tasks correctly.

In our sample, researchers creatively combined a variety of tools aimed at helping participants perceive risk, ranging from scenarios and deception to incentives for secure

behavior. Educational interventions were tested, and prototypes were frequently used to create relatively realistic interactions for participants.

One takeaway from our analysis is that, while prototypes appear in about a third of the studies we analyzed, the majority of studies did not include prototypes. This might suggest a focus on understanding user perceptions, attitudes and behaviors in terms of general concepts or existing systems, rather than proposing and testing new solutions. Research that does not involve prototypes is often used to explore and define the problem space, as for example by Matthews et al., (2017), who studied privacy and security practices of survivors of intimate partner abuse. Exploring and defining a privacy- and security-related problem space holds much value, without necessarily proposing a new solution in the same paper. Exploratory UPS papers may eventually be followed-up with proposed solutions, either by the same authors or by others inspired by the exploratory paper.

Prototypes can also be a valuable tool even in more exploratory phases of research. Most studies involving a prototype in our sample had an experimental objective, but prototypes can be useful in combination with a variety of methods going beyond experiments. A prototype could for instance also be used to enhance the discussion in focus groups or interviews, or a deliberately imperfect prototype could serve as a basis that participants build upon in co-creation methods. Low-fidelity prototypes can be helpful to solicit more fundamental feedback on a scenario than a functional interface. Prototypes can also help participants situate themselves in hypothetical security or privacy-critical situations and make them seem more concrete, thus allowing researchers to explore participant reactions to the prototype as an artefact. Overall, the value of a prototype is also enhanced by the process that led up to its creation; user-centered approaches and extended pilot testing can improve the quality of the prototype that is ultimately exposed to research participants. The description of how prototypes and other tools were used in section 2.5.3. can provide inspiration for researchers planning UPS user studies.

Most of the papers we surveyed adopt traditional study methods: interview, experiment, and surveys. Methods such as focus groups, diary studies, vignette studies, list experiments, co-creation methods, and workshops were used only rarely. UPS studies, in this regard, do not diverge much from trends in HCI, where the same set of methods are most prevalent (Caine, 2016, Pettersson et al., 2018). Research on how to adapt a larger variety of HCI and design methods to the UPS field would help broaden the methodological spectrum currently used.

Some of the methods that do not occur frequently in our sample may nonetheless be useful to the UPS community and could hold potential for novel approaches to represent and measure risk. *Diary methods*, for instance, could help provide longitudinal insights into how participants perceive security or privacy risks over a longer time period. The method could be used for naturally occurring risks, but researchers might also equip participants with a new technology for the duration of the study and explore their long-term perceptions of security and privacy risks. Co-creation/participatory design and group methods can also hold advantages for use in UPS studies, we will consider these in the next two subsections.

2.6.1.1. Co-creation and participatory design methods

Methods including co-creation could help end users make an active contribution to the creation of effective privacy and security mechanisms and for instance help design more user-centred descriptions of privacy and security concepts. Such methods can hold value for UPS, in particular when the objective is to elicit and unveil user needs throughout the activity. Note that the creation of a final solution is usually not the objective of participatory or co-creative design methods. Quite frequently, participants are asked to create prototypes "in order for participants to gain knowledge for critical reflection, and provide users with concrete experience of the future design in order for them to specify demands for it" (Hansen et al., 2019). In terms of risk representation, co-design and participatory design activities can help users reflect and build upon the security and privacy risks that naturally occur in their lives, and contribute ideas leading to potential solutions. Going beyond naturally occurring risk, co-design and participatory design can also simulate or mention new risky situations to participants, helping researchers understand participant thought processes when exposed to risks.

Two papers in our sample used a form of co-creation. Egelman et al. (2015) asked crowdworkers to design icons to communicate what type of data devices with recording capabilities were currently recording. Adams et al. (2018) conducted a co-design study with Virtual Reality (VR) developers who were asked to contribute to a VR code of ethics on a shared online document.

2.6.1.2. Group methods

Few studies used group methods such as workshops and focus groups. However, workshops and focus groups hold the potential of gathering qualitative in-depth insights

into privacy and security attitudes that might help the community obtain even richer results. In comparison to interviews, which are already frequently used, such group activities allow researchers to confront and contrast different privacy and security attitudes and behaviors. By confronting various attitudes and behaviors, participants also naturally explain contradictions in their behavior and attitudes. This study method can help reveal how participants perceive naturally occurring risks and how they weigh advantages and disadvantages. Group methods are not limited to naturally occurring risks, however, they can also mention or simulate novel or futuristic risk situations. One could also imagine participants acting out scenarios with security or privacy risks in the group. Group methods can also provide insights on topics where users' attitudes seemingly contradict their behavior. Recent studies have used group methods in this way to understand privacy trade-offs better (Distler et al., 2020; Rainie & Duggan, 2015). These examples used multiple scenarios of potential privacy trade-offs that focus group participants should imagine themselves confronted with, for instance the possibility of using a smart thermostat that shares their data with undefined parties online. Focus group participants first noted advantages and shortcomings individually, and then discussed and confronted their opinions in the group setting.

Examples in our sample included Sambasivan et al. (2018) who conducted focus groups with women in South Asian countries to explore performative practices used to maintain individuality and privacy in contexts where devices were frequently borrowed and monitored by their social relations. Another paper used focus groups to understand how abusers in intimate partner violence exploit technology in order to gain a better understanding of threat models in this context and find mitigation strategies for such attacks (Freed et al., 2018).

2.6.2. Participant recruitment and risk representation

One remarkable observation of our sample showed that researchers often rely on easily accessible populations (e.g., MTurkers, convenience samples, students). While this is understandable from a researcher's point of view, including a more diverse set of research participants holds value, since minority groups often face specific risks in their daily life. Here, we discuss some approaches to including more understudied groups and provide some observations on the use of crowdworkers as UPS study participants.

2.6.2.1. Understudied groups

Within our sample of papers in top-tier security and privacy conferences which did not include special interest venues for these populations, non-Western populations, disabled persons, members of the LGBTQ+ community, and certain age groups (older adults, children and teenagers) were rarely studied. When these groups were included, they mostly participated in descriptive (rather than experimental) studies, such as interviews or surveys. Accordingly, risk representation was mostly based on naturally occurring risk. This means that most security or privacy tools are likely not tested by members of these groups, who might have special needs and thus might not be able to take advantage of their privacy and security-enhancing properties. They could also perceive or react to risks differently, further underlining the importance of including these groups. Other researchers may build on these results by striving to include understudied groups at all steps of research and design, including exploration, generation of ideas, and iterating on the development of prototypes and final tools. At SOUPS 2020, Fanelle et al. (2020) presented one such experimental study in which people with visual impairments tested the usability of audio captchas.

In addition to traditional recruitment approaches, such as contacting communities of understudied groups directly, using crowdsourcing solutions might hold potential. As the filtering options on crowdsourcing platforms such as Prolific Academic continue to become more fine-grained, researchers might take advantage of these filtering options to recruit understudied groups. Researchers should also make sure to advertise research in ways that are accessible to people with various types of impairments whenever possible. Including a wider variety of participants might also make it necessary to adapt the research methods to the abilities and strengths of the research participants, such as described for instance in research on participatory design with autistic children (Spiel et al., 2017).

2.6.2.2. Use of crowdworkers

In our sample, 106 papers used crowdsourcing platforms to recruit participants. Many of these papers in our sample discuss shortcomings of using crowdworkers in the limitations section, such as Tan et al. (2017) who point out that MTurkers are not representative of the general U.S. population. Habib et al. (2018) also recognize the limitations of using convenience samples such as MTurk, but point to research demonstrating that MTurk is a valid source of high-quality human subjects data (Kittur et al., 2008). Papers involving crowdworkers mostly relied on simulated risk, or, to a lesser extent, naturally occurring

or combinations of risk. Indeed, the use of crowdworkers does not exclude realistic risk representations, and researchers combine tools such as prototypes, scenarios, or educational interventions. Based on the sample of papers we analyzed, it appears that using crowdworking platforms has become an accepted practice for UPS studies, especially when researchers need to create a controlled experimental setup that requires sufficient statistical power, thus calling for large numbers of participants.

We did not systematically analyse compensation for crowdworkers, but we observed anecdotally that compensation seemed to vary substantially between studies, with one study, for example, compensating participants with $0.70 for a 10-minute survey on MTurk (Shrestha et al., 2016), and another study compensating participants $4 for a 10-to-15-minute MTurk study (Lyastani et al., 2018). While Prolific enforces payments of at least $6.50 per hour, MTurk does not currently enforce a minimum compensation. In addition to ethical concerns related to compensation for crowdworkers, low pay might also affect data quality and participants' willingness to disclose private information (Sannon & Cosley, 2018), thus potentially influencing the validity of UPS studies. A discussion of how to define "fair" compensation of crowdworkers who participate in UPS studies thus seems important.

2.6.3. Ethics

Here we focus on two ethical issues of particular importance for UPS studies: deception and use of attackers as human subjects in studies.

2.6.3.1. Deception

Based on our analysis, it seems that the tension between deception and ethics in UPS remains. In particular, the community is not consistent with the definition of deception. Five papers with broad or partial disclosure (not considered deception in our analysis) stated that they used deception, whereas not all papers that we coded as using deception stated that they did. We refer to studies with partial disclosure when the study objective was stated in a relatively broad manner to avoid priming participants. In one study for instance, the authors recruited participants "for a study on personal finance and credit bureaus" and purposefully omitted that they were specifically interested in Equifax or identity theft to avoid priming participants and limit self-selection bias (Zou et al., 2018). In another study, the researchers recruited Android users without mentioning that the study would focus on permissions (Harbach et al., 2014). Both these studies mention that they

use forms of deception, but we consider these instances of partial disclosure and not deception, as they did not mislead participants or withhold information important for them to understand their participation in the study. It is important to note that we discuss these papers with partial disclosure here because they referred to their own approaches as forms of deception. Unless a paper mentioned deception, we did not specifically look for partial disclosure; thus, we expect there may thus be many more papers with partial disclosure in our sample.

The community would profit from a clearer definition of what constitutes deception, and more discussion on what types of deceptions are ethically acceptable in UPS studies. Such a discussion should also include harm-mitigation strategies put in place by researchers, including the use of trained experimenters and requirements for strict debriefing protocols. In addition, clear reporting guidelines for deception studies should be established, as proposed in the next section (also refer to the list of guidelines in the Appendix).

Despite the utility of using deception to make study participants subjected to simulated risk believe they are actually at risk, we find relatively few studies that use deception. Some papers in our sample explain why they decided not to use deception in their studies, mostly pointing to the lack of necessity and avoidance of potential ethical concerns. Dechand et al. (2016) explain that they opted not to obfuscate the goal of their study since they wanted to find the best possible comparison of key-fingerprints in a security context, and the question of how to motivate users to do so was out of scope for their paper. Therefore, the authors argue that it was not necessary to use deception, and thus opted for what they call the "honest" approach. Similarly, Haque et al. (2014) argue that they did not use deception since it was not necessary for their study in which they created a scale to measure participants' comfort when constructing a strong password. The authors argue that given that since there was a relative lack of consequences (e.g., no embarrassment, no reason to respond dishonestly), they considered that it was unnecessary to hide the true intent of the study. Volkamer et al. (2018) also explain that they opted to avoid deception in their study, during which they observed people using ATMs in public. The authors explain that they intentionally avoided conducting a researcher-as-participant study, which uses deception and makes it more difficult to preserve anonymity of subjects. Instead, the authors decided to conduct a pure observation study without any type of deception, thus avoiding ethical concerns. Petracca et al., (2017) also do not use or mention deception in their paper, but describe an interesting approach that we consider partial disclosure. The

authors performed a lab study in which they evaluated the effectiveness of their authorization framework in supporting users in avoiding attacks by malicious apps. Before starting their experiment, the authors informed participants that attacks targeting sensitive audio or video data were possible during the interaction with the apps involved in the experimental tasks, but did not inform participants of the attack source. By revealing the possibility of attacks, yet without mentioning the attack source, the authors thus managed to simulate attacks without the use of deception.

2.6.3.2. Attackers as human subjects

When analyzing the use of deception in our sample, we found that in four papers, all related to social engineering, the authors did not obtain consent from their participants. Two of these papers included attackers as non-consenting participants (Han et al., 2016; Sahin et al., 2017). The inclusion of real (not simulated) attackers in UPS studies raises ethical questions. Some researchers might not think of attackers as research participants for which they require IRB approval or need to obtain informed consent, especially when they "only" analyze existing datasets (e.g., Sahin et al., 2017) or when observing the attackers' naturally occurring behavior (e.g., Han et al., 2016). Compared to general HCI research, the issue of including attackers as research participants seems somewhat unique to UPS and non-UPS security studies. However, researchers in criminology have discussed the ethical implications of including criminals, prisoners, or persons exhibiting potentially criminal behavior in their research. For instance, Ray et al., (2010) discuss the legal, ethical, and methodological considerations when studying child pornography offenders online. They underline that the Belmont Report, which provides ethical principles to which all researchers are bound, applies for all human subjects research, even when participants exhibit criminal behaviors. The report includes the principles of respect for persons, beneficence, and justice. The principle of respect for persons requires researchers to ensure that participants are autonomously and voluntarily consenting to take part in research. Beneficence requires researchers to minimize the risk of harm resulting from participation in research studies. The authors also discuss the tension between the legal perspective, which does not recognize participant privilege, and the ethical perspective, which requires the researcher to reduce the risk participants might incur from taking part in studies. Roberts & Indermaur (2003) discuss how signed consent forms, while usually required by human research ethics committees, can pose a threat to research participants in criminological research, especially offenders. Written documentation that

proves participation in a research study can threaten the offender's future wellbeing and create a barrier to participation. The authors thus suggest developing alternative approaches for obtaining informed consent. Furthermore, in UPS studies, it may be impossible to contact attackers to obtain permission to observe their illegal behavior for research purposes without scaring them away.

IRB review for studies with attackers as participants may focus on whether collecting data on attackers is done in a way that minimizes the potential that these unwitting participants are harmed, for example, by avoiding the collection of data that would allow the attackers to be identified, as identifying attackers is the job of law enforcement, but should be avoided by human-subjects researchers. In addition, identifying attackers will make them less likely to willingly participate in future research. Similar issues and remediations arise when unwitting participants are employees of a company being probed by UPS researchers. For example, a recent paper describing a study in which research assistants called customer service representatives (CSRs) at several mobile phone carriers to attempt to carry out "SIM swap attacks" includes an ethics section in which the authors explain that they did not record the phone calls with the CSRs and their notes on these calls do not include time of the call, any information that might help identify the CSR, or the phone number discussed on the call. In this way they minimized the chance that the CSRs (who in some cases made mistakes that allowed for successful attacks) might be identified by their employers (Lee et al., 2020).

The UPS community would profit from a constructive discussion on the ethics of research in which attackers (or other non-consenting people) are used as research participants. In contrast with research including criminal offenders, "attackers" in UPS do not always engage in criminal behavior -- e.g., an attacker may be someone who snoops on their friend's phone or a child who circumvents access controls put in place by their parents (Schechter, 2013b). Thus, a nuanced consideration of the ethical aspects is necessary. The discussion should also address the use of existing datasets that log attacker behavior without obtaining their consent.

2.6.4. Reporting user study methods

To analyze how researchers represent risk to their participants, it is essential to have a clear understanding of how the authors recruited participants, what the participants were told or led to believe, and how tasks or questions were framed. In some of the papers we

reviewed, these details were not clear, and we suggest improving reporting standards for better replicability and understandability of research. Conferences and journals should request (or require) more detailed reporting and encourage (and provide space for) the inclusion of research material (recruitment material, questionnaires, prototypes) in appendixes or as supplemental materials.

We suggest that the following questions should be answered for user studies in UPS (in addition to a typical description of the methods) to provide a clear understanding of risk representation and thus allow for an informed interpretation of the results. We also provide these questions in the form of a checklist in the appendix for researchers and reviewers to use.

- How were participants recruited?
- Were measures taken to include under-studied groups? If yes, what measures were taken?
- Was informed consent obtained? If yes, how?
- Did participants have an accurate understanding of when the data collection started and ended?
- Did participants receive a broad disclosure to avoid security or privacy priming? If so, what was it?
- In the participants' mind, whose data was at risk (if any)?
- Were participants led to believe something that was not the case (use of deception)?
- How did the research protocol mitigate potential harm to participants?
- What other ethical issues were discussed within the author team or the IRB and how were they treated?
- Did participants receive fair compensation? Report time needed for study participation and compensation. What constitutes fair compensation may also depend on factors such as the minimum wage in the area from which participants are recruited and the nature of the tasks they are asked to complete, as well as demographics and how challenging it is to recruit the target population (e.g., a student sample vs. senior doctors with a specific specialization). We suggest providing these details where relevant.
- Is the study protocol (including the instructions given to participants) available in the appendix?

In addition, we include a structure for categorizing UPS studies with respect to their methods and their treatment of risk. Publication venues that welcome research from the field of UPS (e.g., CHI, SOUPS, IEEE S&P, ACM CCS, USENIX Security) could use these guidelines to encourage better reporting of user studies. After reading a paper, reviewers should be able to easily categorize a paper according to these guidelines. This would improve the quality of user studies and encourage replicability and ethical approaches in user studies. In addition, it is useful for students to consider these guidelines as they read papers and start writing research papers of their own.

2.7. Conclusion

Studying how users of digital systems perceive privacy and security risks is a challenging endeavor for researchers and practitioners, who need to balance realistic risk representation and ethical concerns. Studying such questions in a context where research participants perceive no privacy and security risks would impact the validity of the study's results.

On the other hand, exposing people to realistic cyberattacks (e.g., having their identities or credit card numbers stolen) and letting them feel the cost of recovering a sense of normality after a crime, may be unethical unless done carefully to minimize the risk of harm. The issue is also intrinsically related to the use of deception in security research, a practice that seems inevitable in certain contexts to preserve the study validity and to avoid priming participants to look for or expect an attack. We conducted a systematic literature review investigating how recent research in UPS addresses this issue, analyzing 284 papers with regards to their study methods; how the study represents and assesses response to risk; and the use of prototypes, scenarios, educational interventions, and deception.

Important findings include that, across our sample, risk representation was mostly based on naturally occurring or simulated risk. Risk representation varied with the study methods and objectives of a paper. Papers with an experimental objective mostly used simulated risk, and descriptive studies mostly used naturally occurring risk. Response to risk was measured mostly through a combination of observed and self-reported measures, or self-reported measures on their own.

Researchers used a variety of "tools" to represent risk to participants. Security/privacy-related tasks were used in more than a third of the papers, and approximately a third of the papers involved a prototype. Scenarios were also frequently used to represent risk.

Deception was only rarely used to create a perception of risk, and only a small number of papers used educational interventions or incentives for secure behavior. In terms of participant recruitment, researchers frequently chose crowdworkers and non-representative convenience samples.

By reviewing the wide array of methods adopted by researchers interested in how users perceive privacy and security, we give an overview of the trade-offs researchers frequently face and present the community's response to them. Through a discussion of the advantages and shortcomings of the approaches used, our review helps the community be more cognizant of the plethora of different approaches for user studies in UPS, and of how papers discussed the validity of their approaches for risk representation and associated ethical choices. The systematic approach we followed allowed us to suggest guidelines for researchers who aim to report on user studies in privacy and security, and in particular, risk representation and assessment. In addition, we identify key methodological, ethical and research challenges.

Of course, there is no such thing as a "perfect" method. Rather, there is a large set of trade-offs to consider when choosing a research method. Our review of the methods in UPS studies offers transparency and improves the community's awareness of the adopted practices. We provide a checklist with methodological information we suggest should be included in all empirical UPS studies. On a larger level, we are convinced that fostering an ongoing discussion regarding methods and their potential to represent risk to participants will help the UPS community continuously improve towards a common understanding of valid, ethical and replicable science, and ultimately a richer understanding of how people behave in the presence of privacy and security risk.

2.8. Acknowledgements

We acknowledge support from the Fonds National de la Recherche (PRIDE15/10621687) and the Carnegie Corporation of New York.

2.9. Appendix

2.9.1. Guidelines for reporting of user studies in Usable Privacy and Security

Categorization of risk representation

We suggest the following shared vocabulary for describing the risk representation in UPS studies. UPS Venues can also ask reviewers to fill out this categorization and use it for descriptive statistics about the published studies.

Objective of the study *(check as many as apply)*

__ **Descriptive** - provides a snapshot of the current state of affairs

__ **Relational** - designed to discover relationships among variables

__ **Experimental** - participants are placed into multiple groups who experience different manipulations of a given experience so that the influence of each manipulation can be measured[1]

Risk response assessment method *(check as many as apply)*

__ **Observational data**

__ **Self-reported data**

__ **Assigned security or privacy task** - e.g., password creation, send encrypted message

__ **Assigned unrelated task** - e.g., drawing task, buy something on online store, other non-security or privacy-related tasks

Risk representation *(check as many as apply)*

__ **Naturally occurring risk** - e.g., through observation or self-reported measures of naturally occurring behavior

__ **Simulated risk** - e.g., through the use of scenarios participants should imagine themselves in

__ **Mentioned risk** - e.g., a questionnaire where participants were presented with hypothetical situations

__ **No induced risk representation**

Incentives for secure behavior

Were research participants incentivized to adopt a certain secure behavior, e.g., they would receive financial compensation if they managed to send an encrypted message?

__ yes __ no

Prototype

Does the study involve exposing participants to a prototype of any fidelity (interactive or non-interactive)? A prototype is defined as a new solution such as a textual message, an icon, or an interface.

__ yes __ no

Scenario

Do researchers ask participants to imagine themselves being in a certain situation?

__ yes __ no

Educational Intervention

Did the researchers attempt to educate research participants on privacy and security related topics?

__ yes __ no

[1] Definitions based on Stangor & Walinga (2018)

Checklist for Essential Methodological Details and Ethics

The following information should be clearly stated in usable privacy and security studies.

This checklist can be used by study authors and reviewers in usable privacy and security.

Recruitment

How exactly were participants recruited? E.g., flyers on university campus inviting students only, recruitment panel including parents in specific geographic area, undefined convenience sampling through flyers in an entire city, representative sample, purposive sample

Explain the recruitment strategy:
……..……..……..……..……..……..……..……..……..……..……..……..…….

Were measures taken to include under-studied groups (e.g., LGBTQ, older adults, kids, disabled persons…)?

__ yes __ no

Explain:
……..……..……..……..……..……..……..……..……..……..……..……..……..……..…….

Informed Consent

Was informed consent obtained?

__ yes __ no

If yes, how?
……..……..……..……..……..……..……..……..……..……..……..……..……..……..……..

Did participants have an accurate understanding of when the data collection started and ended?

__ yes __ no

Explain:
……..……..……..……..……..……..……..……..……..……..……..……..……..……..…….

Did participants receive a broad disclosure to avoid security or privacy priming?

Explain:
……..……..……..……..……..……..……..……..……..……..……..……..……..……..…….

Methodological Details

In the participants' mind, whose data was at risk (if any)?

Explain:
……..……..……..……..……..……..……..……..……..……..……..……..……..……..…….

Were participants led to believe something that was not the case (use of deception)?

Explain:
……..……..……..……..……..……..……..……..……..……..……..……..……..……..…….

How did the research protocol mitigate potential harm to participants?

Explain:
……..……..……..……..……..……..……..……..……..……..……..……..……..……..…….

Which other ethics issues discussed within the author team or the IRB and how were they treated?

Explain:
……..……..……..……..……..……..……..……..……..……..……..……..……..……..…….

Did participants receive fair compensation? Report time needed for study participation and compensation.

Time needed for participation: ……. Amount of compensation: ……

Replicability

Is the study protocol (including the instructions given to participants) available in the appendix?

__ yes __ no

2.9.2. List of included papers

We provide the list of included papers as supplemental material.

2.9.3. Dataset

We provide the full dataset as supplemental material.

2.9.4. Additional results

	Frequency	Percent
2014	43	15
2015	56	20
2016	54	19
2017	70	25
2018	61	22

Table 16: Number of included papers per year (N=284).

	Frequency	Percent
Experimental	115	41
Descriptive	89	31
Descriptive and Relational	49	17
Relational	13	5
Descriptive and Experimental	10	4
Relational and Experimental	8	3

Table 17: Objectives of the papers (N=284).

	Frequency	Percent
Experiment	99	35
Interview	36	13
Survey	34	12
Survey and Data Logs	12	4
Analyse Dataset	11	4
Survey and Interview	11	4
Experience Sampling Method	8	3

Survey and Experiment	8	3
Other	6	2
Data Logs	4	1
Survey and Analyse Dataset	4	1
Interview and Experiment	3	1
Interview and Focus Group	3	1
Interview and Other	3	1
Survey and Other	3	1
Observation and Interview	2	1
Experiment and Data Logs	2	1
Experiment and Other	2	1
Survey and Interview and Data Logs	2	1
Survey and List	2	1
Vignette	2	1
Workshop and Other	1	0.4
Focus Group	1	0.4
Survey and Data logs	1	0.4
Survey and Experiment and Analyse Dataset	1	0.4
Interview and Diary	1	0.4
Interview and Experiment and Analyse Dataset	1	0.4
Interview and Observation	1	0.4
Survey and Observation	1	0.4
Experiment and Analyse Dataset and Data Logs	1	0.4
Experiment and Focus Group	1	0.4
Observation	1	0.4
Survey and Co-creation	1	0.4
Survey and Interview and Analyse Dataset	1	0.4
Survey and Interview and Other	1	0.4
Survey and Workshop	1	0.4
Data Logs and Other	1	0.4

Experiment and Analyse Dataset	1	0.4
Experiment and Diary	1	0.4
Interview and Co-creation	1	0.4
Interview and Analyse Dataset	1	0.4
Interview and Data Logs	1	0.4
Interview and Workshop and Observation	1	0.4
Survey and Interview and Diary and Observation	1	0.4
Survey and Interview and Experiment	1	0.4
Survey and Interview and Experiment and Other	1	0.4
Survey and Interview and Focus Group and Analyse Dataset	1	0.4
Survey and Interview and Observation	1	0.4

Table 18: Combinations of study methods in our sample (N=284).

	Experiment (n=119)	Survey (n=85)	Interview (n=72)	Log Analysis (n=21)
Mean	653	846	29	774
Median	80	307	21	110
Std. Dev.	1514	1538	32	2882
Min	6	7	4	19
Max	9114	10763	200	13000

Table 19: Average number of participants per paper per study method.

	Frequency	Percent
Ethics board approval	159	56
Not mentioned	99	35
Institution without approval procedure	10	4
Corporate/Industry internal review process	10	4
Exempt from needing approval	4	1
Other	1	0.4
Multiple	1	0.4

Table 20: IRB or ethics board approval of papers (N=284).

	Frequency	Percent	Percentage of papers in that category that use deception
Authentication	3	19	4
Privacy perceptions, attitudes and behaviors	3	19	5
Privacy transparency and choice mechanisms	3	19	21
Social engineering	3	19	30
Security indicators and warnings	1	6	8
Security perceptions, attitudes and behaviors	1	6	2
Access control	1	6	5
Multiple	1	6	9
Total	16	100	

Table 21: Topics of deception studies

	Frequency	Percent	Percentage of papers using each method that used deception
Experiment	11	69	11
Analyse Dataset	1	6	9
Interview	1	6	3
Other	1	6	17
Survey and Experiment	1	6	13
Survey and Interview	1	6	9
Total	16	100	

Table 22: Study methods used in deception studies

2.9.5. Additional analysis by topics

As shown in Figure 3, most research topics had a dominant study objective. Access control, authentication, encryption, privacy transparency and choice mechanisms, social engineering, and security indicators and warnings are all investigated using experimental studies about two-thirds of the time. Papers that study privacy and security perceptions, attitudes and behaviors frequently use a descriptive objective (45% and 54%,

respectively). Studies of privacy-enhancing technologies and studies of multiple topics also tended to use a descriptive objective. Relational and combination objectives were not used frequently for any topic.

One might assume that in topic areas where experimental studies are predominant (*e.g., authentication, social engineering, security indicators and warnings*), researchers mostly seek to test and validate solutions, for instance new authentication schemes. While almost half (46%) of the *authentication* studies and 58% of papers on *security indicators and warnings* include a *prototype*, other topics with a large proportion of experimental studies (e.g., *social engineering*) do not include many prototypes. In these cases, the researchers might actually use experimental approaches to test and find difficulties users have with existing products. Research on topics with many descriptive studies (e.g., *privacy and security perceptions, attitudes and behaviors*) have a tendency to seek to describe the current state of affairs, without necessarily evaluating solutions in an experimental setting. Figure 4, which correlates the number of prototypes per topic, corroborates this hypothesis, showing that *privacy and security perceptions, attitudes and behaviors* indeed include very few prototypes (20% and 13%, respectively).

Figure 5 shows that *observation* occurs rarely on its own and that most topic areas rely on a combination of *self-reported and observed measures*. *Self-report studies* dominate two topic areas: *privacy perceptions, attitudes and behavior*s (71%) and *security perceptions, attitudes, and behaviors* (70%). *Authentication and social engineerin*g are the topics with the highest percentage of papers that use *observed* measures only (19%, 30%).

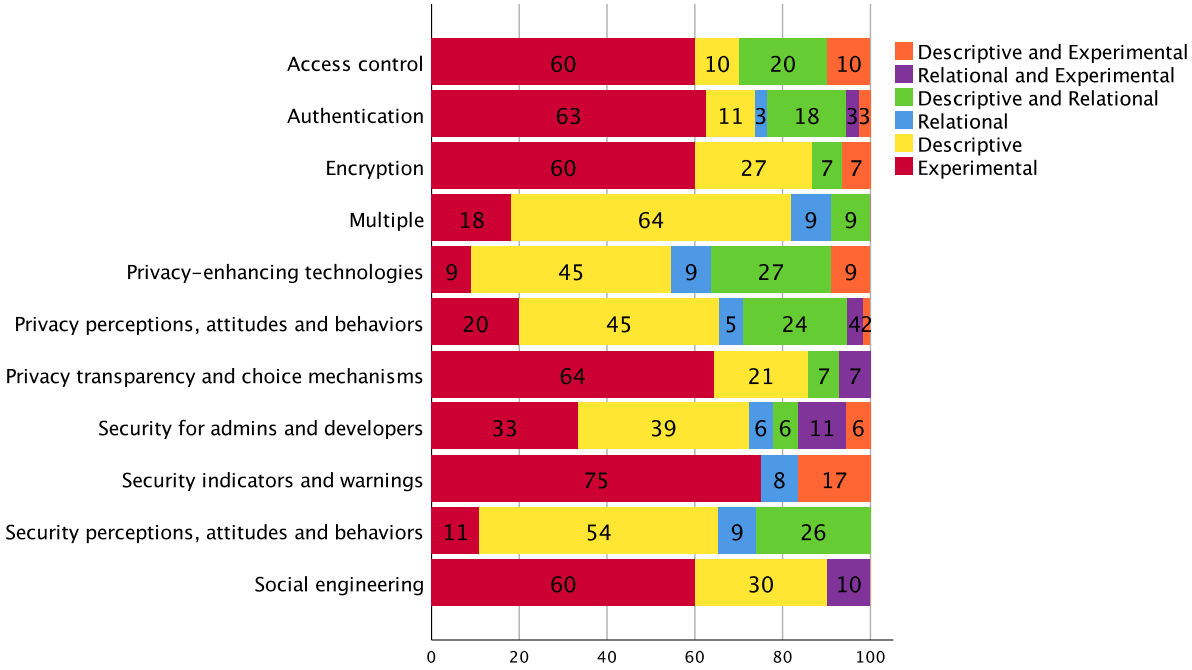


Figure 3: Crosstab research topic and objective (percentage).

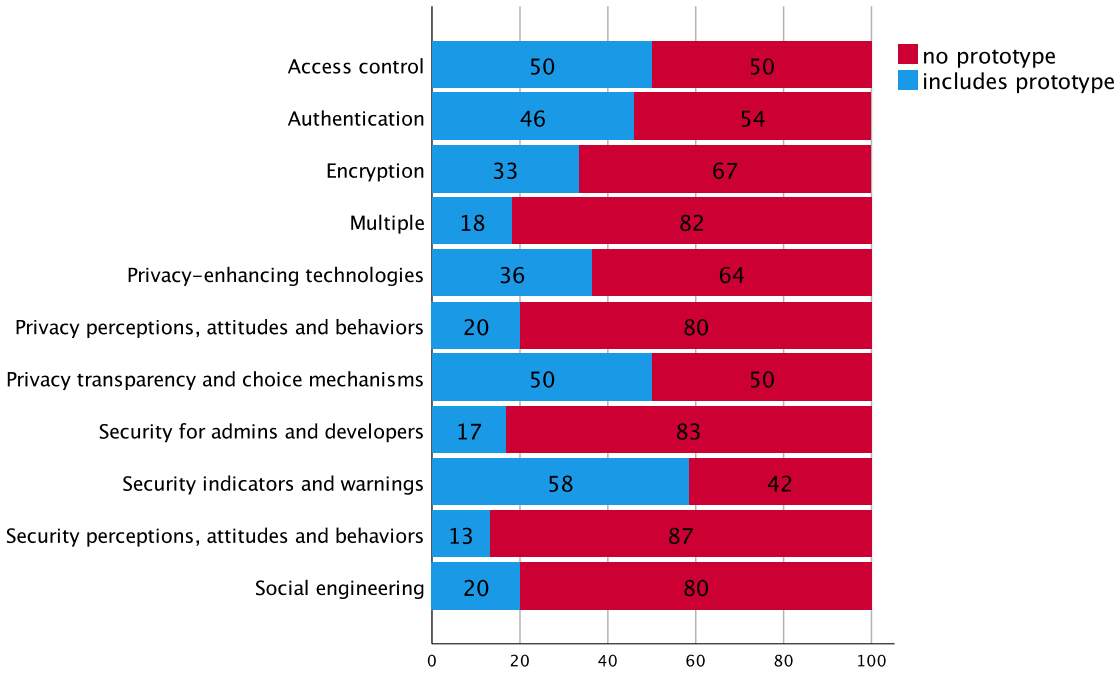


Figure 4: Proportion of studies including a prototype per topic.

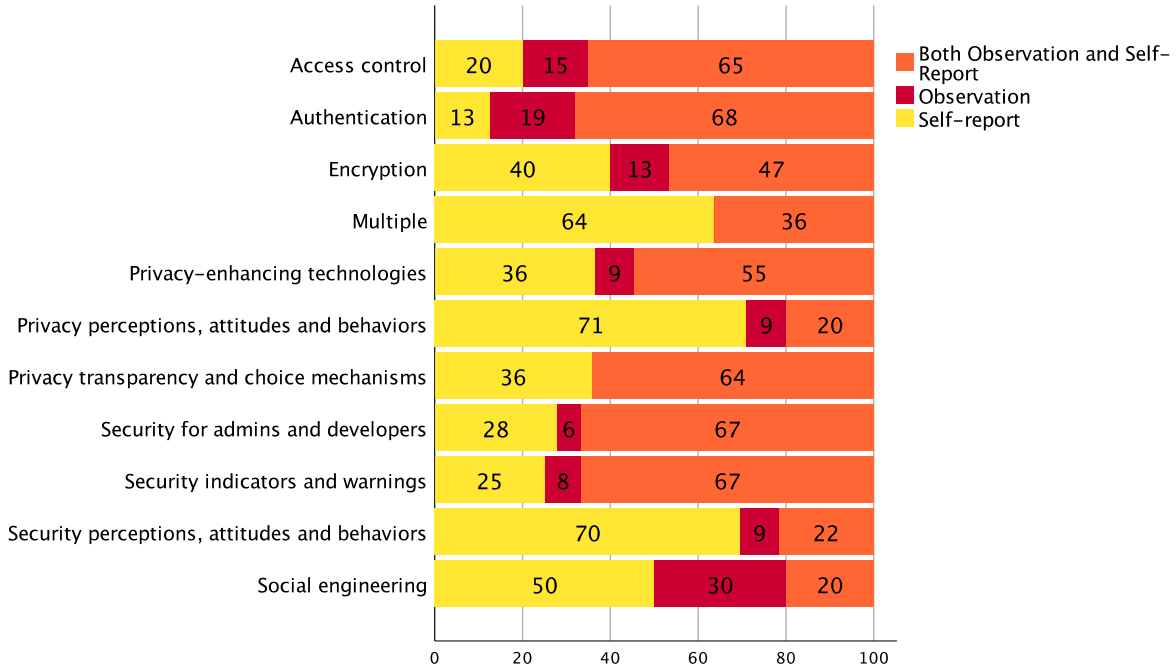


Figure 5: Crosstab Risk response assessment and Topic (percent of all studies on topic).

As shown in Figure 6, most topics appeared at all five of the venues we reviewed. However, a small number of topics were more likely to appear or not appear at certain venues. For example, papers on *privacy perceptions, attitudes and behaviors* were more likely to appear at CHI and rarely appeared at IEEE S&P or ACM CCS. Papers on *security perceptions, attitudes and behaviors* never appeared at IEEE S&P. Papers on the topics *security for admins and developers*, and *privacy-enhancing technologies* were rarely published at CHI. Papers on *security indicators and warnings* appeared only at CHI and SOUPS. Papers on *privacy transparency and choice mechanisms* and papers on *access control* never appeared at ACM CCS. SOUPS was the only venue that had published papers on all topic areas. Overall, our data show that certain topics were more likely to be published at certain publications venues over others. Our data does not show whether authors self-selected and did not submit papers at certain venues because the topics did not seem suitable, or whether reviewers at certain venues were likely to judge papers with certain research topics more favorably.

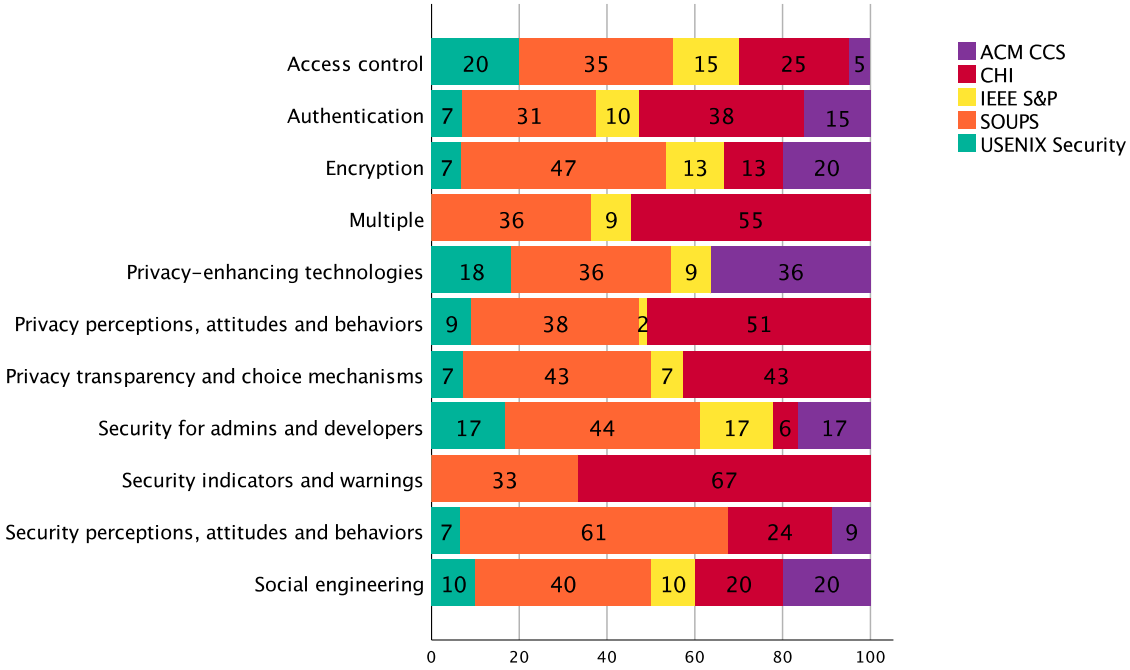


Figure 6: Crosstab Topic and Venue.

2.10. References

Acar, Y., Backes, M., Fahl, S., Garfinkel, S., Kim, D., Mazurek, M. L., & Stransky, C. (2017). Comparing the usability of cryptographic apis. *Proceedings of the 38th IEEE Symposium on Security and Privacy*.

Acquisti, A., Sleeper, M., Wang, Y., Wilson, S., Adjerid, I., Balebako, R., Brandimarte, L., Cranor, L. F., Komanduri, S., Leon, P. G., Sadeh, N., & Schaub, F. (2017). Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online. *ACM Computing Surveys*, *50*(3), 1–41. https://doi.org/10.1145/3054926

Adams, D., Bah, A., Barwulor, C., Musaby, N., Pitkin, K., & Redmiles, E. M. (2018). Ethics Emerging: The Story of Privacy and Security Perceptions in Virtual Reality. *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*, 427–442. https://www.usenix.org/conference/soups2018/presentation/adams

Adar, E., Tan, D. S., & Teevan, J. (2013). Benevolent deception in human computer interaction. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems - CHI '13*, 1863. https://doi.org/10.1145/2470654.2466246

Agarwal, L., Khan, H., & Hengartner, U. (2016). Ask Me Again But Don't Annoy Me: Evaluating Re-authentication Strategies for Smartphones. *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*, 221–236. https://www.usenix.org/conference/soups2016/technical-sessions/presentation/agarwal

Ahmed, T., Hoyle, R., Connelly, K., Crandall, D., & Kapadia, A. (2015). Privacy concerns and behaviors of people with visual impairments. *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, 3523–3532.

Albayram, Y., Khan, M. M. H., Jensen, T., & Nguyen, N. (2017). "...better to use a lock screen than to worry about saving a few seconds of time": Effect of Fear Appeal in the Context of Smartphone Locking Behavior. *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*, 49–63. https://www.usenix.org/conference/soups2017/technical-sessions/presentation/albayram

Alves, R., Valente, P., & Nunes, N. J. (2014). The state of user experience evaluation practice. *Proceedings of the 8th Nordic Conference on Human-Computer Interaction Fun, Fast, Foundational - NordiCHI '14*, 93–102. https://doi.org/10.1145/2639189.2641208

American Psychological Association. (2017). Ethical principles of psychologists and code of conduct (2002, amended effective June 1, 2010, and January 1, 2017). http://www.apa.org/ethics/code/index.html

Anderson, B. B., Kirwan, C. B., Jenkins, J. L., Eargle, D., Howard, S., & Vance, A. (2015). How Polymorphic Warnings Reduce Habituation in the Brain: Insights from an fMRI Study. *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, 2883–2892. https://doi.org/10.1145/2702123.2702322

Angulo, J., & Ortlieb, M. (2015). "WTH..!?!" Experiences, Reactions, and Expectations Related to Online Privacy Panic Situations. *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*, 19–38. https://www.usenix.org/conference/soups2015/proceedings/presentation/angulo

Athanassoulis, N., & Wilson, J. (2009). When is deception in research ethical? *Clinical Ethics*, *4*(1), 44–49. https://doi.org/10.1258/ce.2008.008047

Baumrind, D. (1985). Research Using Intentional Deception. *American Psychologist*, 10.

Biddle, R., Chiasson, S., & Van Oorschot, P. C. (2012). Graphical passwords: Learning from the first twelve years. *ACM Computing Surveys*, *44*(4), 1–41. https://doi.org/10.1145/2333112.2333114

Bonné, B., Peddinti, S. T., Bilogrevic, I., & Taft, N. (2017). Exploring decision making with Android's runtime permission dialogs using in-context surveys. *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*, 195–210. https://www.usenix.org/conference/soups2017/technical-sessions/presentation/bonne

Bonneau, J., Herley, C., Oorschot, P. C. van, & Stajano, F. (2012). The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes. *2012 IEEE Symposium on Security and Privacy*, 553–567. https://doi.org/10.1109/SP.2012.44

Bravo-Lillo, C., Cranor, L., Komanduri, S., Schechter, S., & Sleeper, M. (2014). Harder to Ignore? Revisiting Pop-Up Fatigue and Approaches to Prevent It. *10th Symposium On Usable Privacy and Security (SOUPS 2014)*, 105–111. https://www.usenix.org/conference/soups2014/proceedings/presentation/bravo-lillo

Caine, K. (2016). Local Standards for Sample Size at CHI. *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems - CHI '16*, 981–992. https://doi.org/10.1145/2858036.2858498

Canfield, C., Davis, A., Fischhoff, B., Forget, A., Pearman, S., & Thomas, J. (2017). Replication: Challenges in Using Data Logs to Validate Phishing Detection Ability Metrics. *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*, 271–284. https://www.usenix.org/conference/soups2017/technical-sessions/presentation/canfield

Chatterjee, R., Athayle, A., Akhawe, D., Juels, A., & Ristenpart, T. (2016). PASSWORD tYPOS and how to correct them securely. *2016 IEEE Symposium on Security and Privacy (SP)*, 799–818.

Cranor, L. F., & Buchler, N. (2014). Better Together: Usability and Security Go Hand in Hand. *IEEE Security Privacy*, *12*(6), 89–93. https://doi.org/10.1109/MSP.2014.109

Crawford, H., & Ahmadzadeh, E. (2017). Authentication on the Go: Assessing the Effect of Movement on Mobile Device Keystroke Dynamics. *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*, 163–173. https://www.usenix.org/conference/soups2017/technical-sessions/presentation/crawford

Das, S., Laput, G., Harrison, C., & Hong, J. I. (2017). Thumprint: Socially-inclusive local group authentication through shared secret knocks. *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, 3764–3774.

Deception Research – APA Dictionary of Psychology. (n.d.). Retrieved January 20, 2020, from https://dictionary.apa.org/deception-research

Dechand, S., Schürmann, D., Busse, K., Acar, Y., Fahl, S., & Smith, M. (2016). An empirical study of textual key-fingerprint representations. *25th USENIX Security Symposium USENIX Security 16)*, 193–208.

Distler, V., Lallemand, C., & Koenig, V. (2020). How Acceptable Is This? How User Experience Factors Can Broaden our Understanding of The Acceptance of Privacy Trade-offs. *Computers in Human Behavior*, *106*, 106227. https://doi.org/10.1016/j.chb.2019.106227

Egelman, S., Kannavara, R., & Chow, R. (2015). Is This Thing On?: Crowdsourcing Privacy Indicators for Ubiquitous Sensing Platforms. *Proceedings of the 33rd Annual*

ACM Conference on Human Factors in Computing Systems, 1669–1678. https://doi.org/10.1145/2702123.2702251

Egelman, S., King, J., Miller, R. C., Ragouzis, N., & Shehan, E. (2007). Security user studies: Methodologies and best practices. *CHI '07 Extended Abstracts on Human Factors in Computing Systems - CHI '07*, 2833. https://doi.org/10.1145/1240866.1241089

Egelman, S., & Peer, E. (2015). Scaling the Security Wall: Developing a Security Behavior Intentions Scale (SeBIS). *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, 2873–2882. https://doi.org/10.1145/2702123.2702249

Eiband, M., Khamis, M., von Zezschwitz, E., Hussmann, H., & Alt, F. (2017). Understanding Shoulder Surfing in the Wild: Stories from Users and Observers. *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, 4254–4265. https://doi.org/10.1145/3025453.3025636

Fahl, S., Harbach, M., Acar, Y., & Smith, M. (2013). On the ecological validity of a password study. *Proceedings of the Ninth Symposium on Usable Privacy and Security - SOUPS '13*, 1. https://doi.org/10.1145/2501604.2501617

Fanelle, V., Karimi, S., Shah, A., Subramanian, B., & Das, S. (2020, August). Blind and Human: Exploring More Usable Audio CAPTCHA Designs. *Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)*. https://www.usenix.org/conference/soups2020/presentation/fanelle

Felt, A. P., Barnes, R., King, A., Palmer, C., Bentzel, C., & Tabriz, P. (2017). Measuring HTTPS Adoption on the Web. *26th USENIX Security Symposium (USENIX Security 17)*, 1323–1338. https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/felt

Felt, A. P., Reeder, R. W., Ainslie, A., Harris, H., Walker, M., Thompson, C., Acer, M. E., Morant, E., & Consolvo, S. (2016). Rethinking Connection Security Indicators. *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*, 1–14. https://www.usenix.org/conference/soups2016/technical-sessions/presentation/porter-felt

Fiesler, C., & Hallinan, B. (2018). "We Are the Product": Public Reactions to Online Data Sharing and Privacy Controversies in the Media. *Proceedings of the 2018 CHI Conference*

on Human Factors in Computing Systems, 53:1--53:13. https://doi.org/10.1145/3173574.3173627

Forget, A., Komanduri, S., Acquisti, A., Christin, N., Cranor, L. F., & Telang, R. (2014). *Security Behavior Observatory: Infrastructure for long-term monitoring of client machines.* (p. 11) [Technical Report]. CMU-CyLab-14-009, CyLab, Carnegie Mellon University.

Forget, A., Pearman, S., Thomas, J., Acquisti, A., Christin, N., Cranor, L. F., Egelman, S., Harbach, M., & Telang, R. (2016). Do or Do Not, There Is No Try: User Engagement May Not Improve Security Outcomes. *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*, 97–111. https://www.usenix.org/conference/soups2016/technical-sessions/presentation/forget

Freed, D., Palmer, J., Minchala, D., Levy, K., Ristenpart, T., & Dell, N. (2018). "A Stalker's Paradise'': How Intimate Partner Abusers Exploit Technology. *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, 667:1--667:13. https://doi.org/10.1145/3173574.3174241

Fuller, B., Varia, M., Yerukhimovich, A., Shen, E., Hamlin, A., Gadepally, V., Shay, R., Mitchell, J. D., & Cunningham, R. K. (2017). Sok: Cryptographically protected database search. *2017 IEEE Symposium on Security and Privacy (SP)*, 172–191.

Garfinkel, S., & Lipford, H. R. (2014). *Usable Security: History, Themes, and Challenges*. Morgan & Claypool Publishers.

Habib, H., Colnago, J., Gopalakrishnan, V., Pearman, S., Thomas, J., Acquisti, A., Christin, N., & Cranor, L. F. (2018). Away From Prying Eyes: Analyzing Usage and Understanding of Private Browsing. *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*, 159–175. https://www.usenix.org/conference/soups2018/presentation/habib-prying

Han, X., Kheir, N., & Balzarotti, D. (2016). PhishEye: Live Monitoring of Sandboxed Phishing Kits. *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, 1402–1413. https://doi.org/10.1145/2976749.2978330

Hanamsagar, A., Woo, S. S., Kanich, C., & Mirkovic, J. (2018). Leveraging Semantic Transformation to Investigate Password Habits and Their Causes. *Proceedings of the 2018*

CHI Conference on Human Factors in Computing Systems, 570:1--570:12. https://doi.org/10.1145/3173574.3174144

Hang, A., Luca, A. D., Smith, M., Richter, M., & Hussmann, H. (2015). Where Have You Been? Using Location-Based Security Questions for Fallback Authentication. *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*, 169–183. https://www.usenix.org/conference/soups2015/proceedings/presentation/hang

Hansen, N. B., Dindler, C., Halskov, K., Iversen, O. S., Bossen, C., Basballe, D. A., & Schouten, B. (2019). How Participatory Design Works: Mechanisms and Effects. *Proceedings of the 31st Australian Conference on Human-Computer-Interaction*, 30–41. https://doi.org/10.1145/3369457.3369460

Haque, S. M. T., Scielzo, S., & Wright, M. (2014). Applying Psychometrics to Measure User Comfort when Constructing a Strong Password. *10th Symposium On Usable Privacy and Security (SOUPS 2014)*, 231–242. https://www.usenix.org/conference/soups2014/proceedings/presentation/haque

Harbach, M., Hettig, M., Weber, S., & Smith, M. (2014). Using Personal Examples to Improve Risk Communication for Security & Privacy Decisions. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 2647–2656.

Holz, C., & Bentley, F. R. (2016). On-Demand Biometrics: Fast Cross-Device Authentication. *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, 3761–3766. https://doi.org/10.1145/2858036.2858139

Hu, H., & Wang, G. (2018). End-to-end measurements of email spoofing attacks. *27th USENIX Security Symposium (USENIX Security 18)*, 1095–1112.

Huh, J. H., Kim, H., Bobba, R. B., Bashir, M. N., & Beznosov, K. (2015). On the Memorability of System-generated PINs: Can Chunking Help? *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*, 197–209. https://www.usenix.org/conference/soups2015/proceedings/presentation/huh

Huh, J. H., Kim, H., Rayala, S. S. V. P., Bobba, R. B., & Beznosov, K. (2017). I'm Too Busy to Reset My LinkedIn Password: On the Effectiveness of Password Reset Emails. *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, 387–391. https://doi.org/10.1145/3025453.3025788

Iachello, G., & Hong, J. (2007). End-User Privacy in Human-Computer Interaction. *Foundations and Trends® in Human-Computer Interaction*, *1*(1), 1–137. https://doi.org/10.1561/1100000004

Jaferian, P., Rashtian, H., & Beznosov, K. (2014). To Authorize or Not Authorize: Helping Users Review Access Policies in Organizations. *10th Symposium On Usable Privacy and Security (SOUPS 2014)*, 301–320. https://www.usenix.org/conference/soups2014/proceedings/presentation/jaferian

Jagatic, T. N., Johnson, N. A., Jakobsson, M., & Menczer, F. (2007). Social phishing. *Communications of the ACM*, *50*(10), 94–100.

Karunakaran, S., Thomas, K., Bursztein, E., & Comanescu, O. (2018). Data Breaches: User Comprehension, Expectations, and Concerns with Handling Exposed Data. *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*, 217–234. https://www.usenix.org/conference/soups2018/presentation/karunakaran

Kittur, A., Chi, E. H., & Suh, B. (2008). Crowdsourcing user studies with Mechanical Turk. *Proceeding of the Twenty-Sixth Annual CHI Conference on Human Factors in Computing Systems - CHI '08*, 453. https://doi.org/10.1145/1357054.1357127

Komanduri, S., Shay, R., Cranor, L. F., Herley, C., & Schechter, S. (2014). Telepathwords: Preventing weak passwords by reading users' minds. *23rd USENIX Security Symposium (USENIX Security 14)*, 591–606.

Kumaraguru, P., Cranshaw, J., Acquisti, A., Cranor, L., Hong, J., Blair, M. A., & Pham, T. (2009). School of Phish: A Real-World Evaluation of Anti-Phishing Training. *Proceedings of the 5th Symposium on Usable Privacy and Security (SOUPS 2009)*. https://doi.org/10.1145/1572532.1572536

Lastdrager, E., Gallardo, I. C., Hartel, P., & Junger, M. (2017). How Effective is Anti-Phishing Training for Children? *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*, 229–239. https://www.usenix.org/conference/soups2017/technical-sessions/presentation/lastdrager

Lee, K., Kaiser, B., Mayer, J., & Narayanan, A. (2020, August). An Empirical Study of Wireless Carrier Authentication for SIM Swaps. *Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)*. https://www.usenix.org/conference/soups2020/presentation/lee

Liu, C., Clark, G. D., & Lindqvist, J. (2017). Where Usability and Security Go Hand-in-Hand: Robust Gesture-Based Authentication for Mobile Systems. *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, 374–386. https://doi.org/10.1145/3025453.3025879

Lyastani, S. G., Schilling, M., Fahl, S., Backes, M., & Bugiel, S. (2018). Better managed than memorized? Studying the Impact of Managers on Password Strength and Reuse. *27th USENIX Security Symposium (USENIX Security 18)*, 203–220.

Mare, S., Baker, M., & Gummeson, J. (2016). A Study of Authentication in Daily Life. *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*, 189–206. https://www.usenix.org/conference/soups2016/technical-sessions/presentation/mare

Marforio, C., Jayaram Masti, R., Soriente, C., Kostiainen, K., & Čapkun, S. (2016). Evaluation of Personalized Security Indicators As an Anti-Phishing Mechanism for Smartphone Applications. *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, 540–551. https://doi.org/10.1145/2858036.2858085

McReynolds, E., Hubbard, S., Lau, T., Saraf, A., Cakmak, M., & Roesner, F. (2017). Toys That Listen: A Study of Parents, Children, and Internet-Connected Toys. *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, 5197–5207. https://doi.org/10.1145/3025453.3025735

Melicher, W., Kurilova, D., Segreti, S. M., Kalvani, P., Shay, R., Ur, B., Bauer, L., Christin, N., Cranor, L. F., & Mazurek, M. L. (2016). Usability and security of text passwords on mobile devices. *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, 527–539.

Meutzner, H., Gupta, S., & Kolossa, D. (2015). Constructing secure audio captchas by exploiting differences between humans and machines. *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, 2335–2338.

Mondal, M., Messias, J., Ghosh, S., Gummadi, K. P., & Kate, A. (2016). Forgetting in Social Media: Understanding and Controlling Longitudinal Exposure of Socially Shared Data. *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*, 287–299. https://www.usenix.org/conference/soups2016/technical-sessions/presentation/mondal

Mulrow, C. D. (1994). Systematic Reviews: Rationale for systematic reviews. *BMJ*, *309*(6954), 597–599. https://doi.org/10.1136/bmj.309.6954.597

Naiakshina, A., Danilova, A., Tiefenau, C., Herzog, M., Dechand, S., & Smith, M. (2017a). Why Do Developers Get Password Storage Wrong?: A Qualitative Usability Study. *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, 311–328. https://doi.org/10.1145/3133956.3134082

Naiakshina, A., Danilova, A., Tiefenau, C., Herzog, M., Dechand, S., & Smith, M. (2017b). Why Do Developers Get Password Storage Wrong?: A Qualitative Usability Study. *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, 311–328. https://doi.org/10.1145/3133956.3134082

Naiakshina, A., Danilova, A., Tiefenau, C., & Smith, M. (2018). Deception Task Design in Developer Password Studies: Exploring a Student Sample. *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*, 297–313. https://www.usenix.org/conference/soups2018/presentation/naiakshina

Obrist, M., Roto, V., & Väänänen-Vainio-Mattila, K. (2009). User experience evaluation: Do you know which method to use? *Proceedings of the 27th International Conference Extended Abstracts on Human Factors in Computing Systems - CHI EA '09*, 2763. https://doi.org/10.1145/1520340.1520401

Oltrogge, M., Acar, Y., Dechand, S., Smith, M., & Fahl, S. (2015). To Pin or Not to Pin—Helping App Developers Bullet Proof Their TLS Connections. *24th USENIX Security Symposium (USENIX Security 15)*, 239–254.

Paré, G., Trudel, M.-C., Jaana, M., & Kitsiou, S. (2015). Synthesizing information systems knowledge: A typology of literature reviews. *Information & Management*, *52*(2), 183–199. https://doi.org/10.1016/j.im.2014.08.008

Pearson, J., Robinson, S., Jones, M., Joshi, A., Ahire, S., Sahoo, D., & Subramanian, S. (2017). Chameleon devices: Investigating more secure and discreet mobile interactions via active camouflaging. *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, 5184–5196.

Petracca, G., Reineh, A.-A., Sun, Y., Grossklags, J., & Jaeger, T. (2017). Aware: Preventing abuse of privacy-sensitive sensors via operation bindings. *26th USENIX Security Symposium (USENIX Security 17)*, 379–396.

Pettersson, I., Lachner, F., Frison, A.-K., Riener, A., & Butz, A. (2018). A Bermuda Triangle? *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems - CHI '18*, 1–16. https://doi.org/10.1145/3173574.3174035

Qahtani, E. A., Shehab, M., & Aljohani, A. (2018). The Effectiveness of Fear Appeals in Increasing Smartphone Locking Behavior among Saudi Arabians. *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*, 31–46. https://www.usenix.org/conference/soups2018/presentation/qahtani

Rainie, L., & Duggan, M. (2015). *Privacy and Information Sharing*. Pew Research Center.

Rashtian, H., Boshmaf, Y., Jaferian, P., & Beznosov, K. (2014). To Befriend Or Not? A Model of Friend Request Acceptance on Facebook. *10th Symposium On Usable Privacy and Security (SOUPS 2014)*, 285–300. https://www.usenix.org/conference/soups2014/proceedings/presentation/rashtian

Ray, J. V., Kimonis, E. R., & Donoghue, C. (2010). Legal, ethical, and methodological considerations in the Internet-based study of child pornography offenders. *Behavioral Sciences & the Law*, *28*(1), 84–105. https://doi.org/10.1002/bsl.906

Redmiles, E. M., Kross, S., & Mazurek, M. L. (2016). How I Learned to Be Secure: A Census-Representative Survey of Security Advice Sources and Behavior. *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, 666–677. https://doi.org/10.1145/2976749.2978307

Redmiles, E. M., Mazurek, M. L., & Dickerson, J. P. (2018). Dancing Pigs or Externalities? Measuring the Rationality of Security Decisions. *Proceedings of the 2018 ACM Conference on Economics and Computation*, 215–232. https://doi.org/10.1145/3219166.3219185

Reeder, R. W., Felt, A. P., Consolvo, S., Malkin, N., Thompson, C., & Egelman, S. (2018). An Experience Sampling Study of User Reactions to Browser Warnings in the Field. *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, 512:1--512:13. https://doi.org/10.1145/3173574.3174086

Reznichenko, A., & Francis, P. (2014). Private-by-Design Advertising Meets the Real World. *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, 116–128. https://doi.org/10.1145/2660267.2660305

Roberts, L., & Indermaur, D. (2003). Signed Consent Forms in Criminological Research: Protection for Researchers and Ethics Committees but a Threat to Research Participants? *Psychiatry, Psychology and Law*, *10*(2), 289–299. https://doi.org/10.1375/pplt.2003.10.2.289

Ruoti, S., Andersen, J., Heidbrink, S., O'Neill, M., Vaziripour, E., Wu, J., Zappala, D., & Seamons, K. (2016). *"We're on the Same Page": A Usability Study of Secure Email Using Pairs of Novice Users*. 4298–4308. https://doi.org/10.1145/2858036.2858400

Ruoti, S., Andersen, J., Monson, T., Zappala, D., & Seamons, K. (2018). A Comparative Usability Study of Key Management in Secure Email. *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*, 375–394. https://www.usenix.org/conference/soups2018/presentation/ruoti

Sahin, M., Relieu, M., & Francillon, A. (2017). Using chatbots against voice spam: Analyzing Lenny's effectiveness. *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*, 319–337. https://www.usenix.org/conference/soups2017/technical-sessions/presentation/sahin

Samat, S., & Acquisti, A. (2017). Format vs. Content: The Impact of Risk and Presentation on Disclosure Decisions. *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*, 377–384. https://www.usenix.org/conference/soups2017/technical-sessions/presentation/samat-disclosure

Sambasivan, N., Checkley, G., Batool, A., Ahmed, N., Nemer, D., Gaytán-Lugo, L. S., Matthews, T., Consolvo, S., & Churchill, E. (2018). "'Privacy is not for me, it's for those rich women'": Performative Privacy Practices on Mobile Phones by Women in South Asia. *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*, 127–142. https://www.usenix.org/conference/soups2018/presentation/sambasivan

Sannon, S., & Cosley, D. (2018). "It was a shady HIT": Navigating Work-Related Privacy Concerns on MTurk. *Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems*, 1–6. https://doi.org/10.1145/3170427.3188511

Schechter, S. (2013a). *Common Pitfalls in Writing about Security and Privacy Human Subjects Experiments, and How to Avoid Them* (MSR-TR-2013-5). Microsoft Technical Report. https://www.microsoft.com/en-us/research/publication/common-pitfalls-in-writing-about-security-and-privacy-human-subjects-experiments-and-how-to-avoid-them/

Schechter, S. (2013b, July). The User IS the Enemy, and (S)he Keeps Reaching for that Bright Shiny Power Button! *Proceedings of the Workshop on Home Usable Privacy and Security (HUPS)*. https://www.microsoft.com/en-us/research/publication/the-user-is-the-enemy-and-she-keeps-reaching-for-that-bright-shiny-power-button/

Schechter, S. E., Dhamija, R., Ozment, A., & Fischer, I. (2007). *The Emperor's New Security Indicators*. 51–65. https://doi.org/10.1109/SP.2007.35

Segreti, S. M., Melicher, W., Komanduri, S., Melicher, D., Shay, R., Ur, B., Bauer, L., Christin, N., Cranor, L. F., & Mazurek, M. L. (2017). Diversify to Survive: Making Passwords Stronger with Adaptive Policies. *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*, 1–12. https://www.usenix.org/conference/soups2017/technical-sessions/presentation/segreti

Sen, S., Guha, S., Datta, A., Rajamani, S. K., Tsai, J., & Wing, J. M. (2014). Bootstrapping privacy compliance in big data systems. *2014 IEEE Symposium on Security and Privacy*, 327–342.

Shay, R., Ion, I., Reeder, R. W., & Consolvo, S. (2014). "My Religious Aunt Asked Why I Was Trying to Sell Her Viagra": Experiences with Account Hijacking. *Proceedings of the 32Nd Annual ACM Conference on Human Factors in Computing Systems*, 2657–2666. https://doi.org/10.1145/2556288.2557330

Shay, R., Ur, B., Bauer, L., Christin, N., Cranor, L. F., Forget, A., Komanduri, S., Mazurek, M. L., Melicher, W., & Segreti, S. M. (2015). A Spoonful of Sugar?: The Impact of Guidance and Feedback on Password-Creation Behavior. *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems - CHI '15*, 2903–2912. https://doi.org/10.1145/2702123.2702586

Shirvanian, M., & Saxena, N. (2014). Wiretapping via mimicry: Short voice imitation man-in-the-middle attacks on crypto phones. *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, 868–879.

Shrestha, B., Shirvanian, M., Shrestha, P., & Saxena, N. (2016). The Sounds of the Phones: Dangers of Zero-Effort Second Factor Login Based on Ambient Audio. *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, 908–919. https://doi.org/10.1145/2976749.2978328

Sotirakopoulos, A., Hawkey, K., & Beznosov, K. (2011). On the challenges in usable security lab studies: Lessons learned from replicating a study on SSL warnings. *Proceedings of the Seventh Symposium on Usable Privacy and Security*, 3.

Spiel, K., Malinverni, L., Good, J., & Frauenberger, C. (2017). Participatory Evaluation with Autistic Children. *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, 5755–5766. https://doi.org/10.1145/3025453.3025851

Stangor, C., & Walinga, J. (2018). Introduction to Psychology-1st Canadian Edition.

Stevens, R., Votipka, D., Redmiles, E. M., Ahern, C., Sweeney, P., & Mazurek, M. L. (2018). The battle for New York: A case study of applied digital threat modeling at the enterprise level. *27th USENIX Security Symposium (USENIX Security 18)*, 621–637.

Tan, J., Bauer, L., Bonneau, J., Cranor, L. F., Thomas, J., & Ur, B. (2017). Can unicorns help users compare crypto key fingerprints? *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, 3787–3798.

Ur, B., Alfieri, F., Aung, M., Bauer, L., Christin, N., Colnago, J., Cranor, L. F., Dixon, H., Emami Naeini, P., Habib, H., & others. (2017a). Design and evaluation of a data-driven password meter. *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, 3775–3786.

Ur, B., Alfieri, F., Aung, M., Bauer, L., Christin, N., Colnago, J., Cranor, L. F., Dixon, H., Emami Naeini, P., Habib, H., & others. (2017b). Design and evaluation of a data-driven password meter. *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, 3775–3786.

Ur, B., Noma, F., Bees, J., Segreti, S. M., Shay, R., Bauer, L., Christin, N., & Cranor, L. F. (2015). "I Added '!' at the End to Make It Secure": Observing Password Creation in the Lab. *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*, 123–140. https://www.usenix.org/conference/soups2015/proceedings/presentation/ur

Usmani, W. A., Marques, D., Beschastnikh, I., Beznosov, K., Guerreiro, T., & Carriço, L. (2017). Characterizing Social Insider Attacks on Facebook. *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, 3810–3820. https://doi.org/10.1145/3025453.3025901

Vaniea, K. E., Rader, E., & Wash, R. (2014). Betrayed by updates: How negative experiences affect future security. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 2671–2674.

Vaziripour, E., Wu, J., O'Neill, M., Metro, D., Cockrell, J., Moffett, T., Whitehead, J., Bonner, N., Seamons, K., & Zappala, D. (2018). Action Needed! Helping Users Find and Complete the Authentication Ceremony in Signal. *Proceedings of the Fourteenth Symposium on Usable Privacy and Security*, 17.

Vaziripour, E., Wu, J., O'Neill, M., Whitehead, J., Heidbrink, S., Seamons, K., & Zappala, D. (2017). Is that you, Alice? A Usability Study of the Authentication Ceremony of Secure Messaging Applications. *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*, 29–47. https://www.usenix.org/conference/soups2017/technical-sessions/presentation/vaziripour

Velásquez, I., Caro, A., & Rodríguez, A. (2018). Authentication schemes and methods: A systematic literature review. *Information and Software Technology*, *94*, 30–37. https://doi.org/10.1016/j.infsof.2017.09.012

Volkamer, M., Gutmann, A., Renaud, K., Gerber, P., & Mayer, P. (2018). Replication Study: A Cross-Country Field Observation Study of Real World PIN Usage at ATMs and in Various Electronic Payment Scenarios. *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*, 1–11. https://www.usenix.org/conference/soups2018/presentation/volkamer

Votipka, D., Rabin, S. M., Micinski, K., Gilray, T., Mazurek, M. L., & Foster, J. S. (2018). User Comfort with Android Background Resource Accesses in Different Contexts. *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*, 235–250. https://www.usenix.org/conference/soups2018/presentation/votipka

Warshaw, J., Taft, N., & Woodruff, A. (2016). Intuitions, Analytics, and Killing Ants: Inference Literacy of High School-educated Adults in the US. *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*, 271–285. https://www.usenix.org/conference/soups2016/technical-sessions/presentation/warshaw

Wash, R., & Cooper, M. M. (2018). Who Provides Phishing Training?: Facts, Stories, and People Like Me. *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems - CHI '18*, 1–12. https://doi.org/10.1145/3173574.3174066

Wash, R., Rader, E., Vaniea, K., & Rizor, M. (2014). Out of the Loop: How Automated Software Updates Cause Unintended Security Consequences. *10th Symposium On Usable Privacy and Security (SOUPS 2014)*, 89–104. https://www.usenix.org/conference/soups2014/proceedings/presentation/wash

Yang, Y., Clark, G. D., Lindqvist, J., & Oulasvirta, A. (2016). Free-form gesture authentication in the wild. *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, 3722–3735.

Zou, Y., Mhaidli, A. H., McCall, A., & Schaub, F. (2018). "I've Got Nothing to Lose": Consumers' Risk Perceptions and Protective Actions after the Equifax Data Breach. *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*, 197–216. https://www.usenix.org/conference/soups2018/presentation/zou

Chapter 3: How Acceptable Is This? How User Experience Factors Can Broaden Our Understanding of the Acceptance of Privacy Trade-Offs

Published as: Distler, V., Lallemand, C., & Koenig, V. (2020). How Acceptable Is This? How User Experience Factors Can Broaden our Understanding of The Acceptance of Privacy Trade-offs. *Computers in Human Behavior*, 106, 106227. https://doi.org/10.1016/j.chb.2019.106227

3.1. Abstract

Privacy is a timely topic that is increasingly scrutinized in the public eye. In spite of privacy and security breaches, people still frequently compromise their privacy in exchange for certain benefits of a technology or a service. This study builds on both technology acceptance (TA) and user experience (UX) research in order to explore and build hypotheses regarding additional dimensions that might play a role in the acceptability of privacy tradeoffs that are not currently accounted for in TA models. Using four scenarios describing situations with potential privacy trade-offs, we conducted a focus group study with 8 groups of participants (N = 32). Our results suggest that factors influencing privacy trade-offs go beyond existing TA factors alone. A technology's perceived usefulness plays an important role, as well as dimensions related to context, previous experiences, perceived autonomy and the feeling of control over the data being shared.

3.2. Introduction

Technologies nowadays are able to perform complex tasks in most areas of people's lives, and many of these tasks may impact users' privacy. Privacy is defined as the ability of individuals to maintain control of their personal information (Westin, 1968). Privacy also relates to the notion of voluntariness, referring to the type of information about one's self or one's association that a person must reveal to others, under which circumstances and with which protections (Mason, 1986). The matter has indeed gained high topicality and public attention. Privacy initiatives such as the General Data Protection Regulation (GDPR) in the European Union aim at improving the regulatory landscape and establish, amongst other measures, the principle of "privacy by design".

When confronted with technologies, users' privacy behavior regularly reflects conscious or unconscious decisions on whether they accept privacy trade-offs, which involve sharing some level of personal data in exchange for using a product or service (Rainie & Duggan, 2015). While technology acceptance models offer a framework for studying acceptance, they have shortcomings such as the absence of psychological needs and negative emotions. Moreover, while factors about users, systems, tasks and organization context are widely recognized as important, many papers on technology acceptance do not address them (Hornbæk & Hertzum, 2017).

Our research leads to the following contributions:

- It adds to knowledge on factors influencing the acceptability of privacy trade-offs and gives insight into the non-instrumental aspects affecting acceptance of privacy-relevant technology, including autonomy, control, context-related factors. Thereby, it helps addressing the lack of non-pragmatic aspects (e.g., hedonic aspects, psychological needs, values) as those offered by UX frameworks, in the majority of acceptance models.
- It describes implications for the design of privacy-relevant systems.

3.2.1. Technology acceptance models

Technology acceptance can be defined as the judgement, attitude and behavioral reactions toward a product (Schade & Schlag, 2003). Technology acceptance models aim at explaining users' intention to use a system, mostly as a result of perceived usefulness (similar to performance expectancy) and perceived ease of use (similar to effort expectancy). These factors are at the basis of the first technology acceptance model (TAM) developed by Davis (1985), which has been extensively used and adapted to numerous contexts. Other influencing factors were introduced in later models, such as social influence. The UTAUT (unified theory of acceptance and use of technology (Venkatesh, Morris, Davis, & Davis, 2003)) hence describes behavioral intention to use a system as dependent on performance expectancy, effort expectancy and social influence. In its updated version UTAUT2 (Venkatesh, Thong, & Xu, 2012), three new constructs, specific to consumer adoption, were introduced: hedonic motivation, price value and habit.

Application areas of acceptance models include for instance smart home technologies (Paetz, Becker, Fichtner, & Schmeck, 2011), social media (B. C. F. Choi & Land, 2016),

health care records (Angst & Agarwal, 2009; Egea & González, 2011) or online tax (Wu & Chen, 2005).

3.2.2. Distinguishing user experience and usability

Usability traditionally focuses on "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" (ISO 9241-11). User experience (UX), on the other hand, takes a broader approach in which task performance is put into perspective with additional aspects, including emotive, subjective and temporal factors of UX, going beyond instrumental facets (Hassenzahl & Tractinsky, 2006). The subjective meaning of an experience, emotional aspects (Desmet & Hekkert, 2007) as well as the context within which the interaction occurs (e.g., organizational/social setting, voluntariness of use, etc.) are within the scope of UX (Hassenzahl & Tractinsky, 2006). While usability is per se is goal-oriented, UX as a concept can also entail experiences with no performance expectations. Hassenzahl (2008) describes this multifactorial nature of UX using a distinction between instrumental (or "pragmatic") qualities and non-instrumental (or "hedonic") qualities of experience.

3.2.3. Links between technology acceptance models and user experience

Pragmatic, or instrumental, quality describes a "product's perceived ability to support the achievement of do-goals" (i.e., tasks) (Hassenzahl, 2008) Hedonic quality refers to a product's perceived ability to support the achievement of "be-goals", such as "feeling safe" or "feeling competent" for instance (Hassenzahl, 2008). UX research also takes into account emotional, subjective and temporal aspects of interaction (Hassenzahl & Tractinsky, 2006),

It has been suggested that hedonic motivation might be a critical factor influencing behavioral intention in consumer-based contexts (Venkatesh et al., 2012). Human needs are are considered drivers of positive experiences (Hassenzahl, 2008; Sheldon, Elliot, Kim, & Kasser, 2001). The most relevant psychological needs have been narrowed down to autonomy, competence, security, relatedness, popularity, stimulation and security (Hassenzahl, 2008; Sheldon et al., 2001). The need for security is defined for instance as "feeling safe and in control of your life rather than feeling uncertain and threatened by your circumstances" (Sheldon et al., 2001). The fulfilment of psychological needs can be measured using a standardized questionnaire (Sheldon et al., 2001), and methods for

qualitative assessment have been developed as well (Lallemand, 2015). Recent studies have applied psychological needs theories to the context of security and privacy (Distler et al., 2019; Kraus, Wechsung, & Möller, 2016, 2017).

It is important to stress that there are overlaps between UX and acceptance models. The TAM (Davis, 1985) for instance includes perceived usefulness (utility as defined by Shackel and Richardson (1991)) and perceived ease of use (similar to usability as defined by ISO 9241-11), and adaptations of the existing models to various contexts include some hedonic aspects (Al-Sharafi, Arsha, Abu-Shanab, & Elayah, 2016; Osswald, Wurhofer, Trösterer, Beck, & Tscheligi, 2012) such as perceived security, perceived safety or self-efficacy. Other extensions of the TAM have found that trust has a positive effect on behavioral intention to use, while usefulness, security and privacy perceptions influenced trust (Al-Sharafi et al., 2016; Venkatesh & Bala, 2008). Acceptance models thus partially cover certain mostly pragmatic UX factors, whereas other UX constructs such as psychological needs fulfilment are not yet included (Hornbæk & Hertzum, 2017), even though a strong tendency on their importance exists (Hassenzahl et al., 2013; Hornbæk & Hertzum, 2017).

3.2.4. The acceptability of privacy trade-offs

Privacy trade-offs can be defined as circumstances under which people would "share personal information or permit surveillance in return for getting something of perceived value." (Rainie & Duggan, 2015).

The acceptability of compromising one's privacy in exchange for certain advantages has been studied under various angles. The theory suggests that people's intention to disclose personal information depends on a privacy calculus, in which competing factors are assessed and users try to maximize the positive and minimize the negative consequences (Wottrich, van Reijmersdal, & Smit, 2018). The privacy calculus takes into account perceived privacy risk, privacy concerns, personal internet interest and internet trust (Dinev & Hart, 2006). This model has since been used in the context of social networks (Dienlin & Metzger, 2016; Krasnova, Veltri, & Günther, 2012), mobile devices (Keith, Thompson, Hale, Lowry, & Greer, 2013) and ecommerce (Luo, Li, Zhang, & Shim, 2010).

Some studies have also looked at discrepancies between user attitude and their actual behavior, a phenomenon called the privacy paradox (Norberg, Horne, & Horne, 2007),

challenging the assumption that privacy-related decision-making is purely rational (Acquisti & Grossklags, 2005; Tsai, Egelman, Cranor, & Acquisti, 2011).

However, a large amount of factors play a role when studying privacy trade-offs. For instance, Rainie and Duggan (2015) studied the acceptance of privacy trade-offs in six different scenarios. Each scenario introduces the possibility of using a new technology offering certain advantages, which at the same time might also create a privacy risk. Participants' acceptance depended on a number of factors, such as trust in the company offering the deal, what happens to the data after it is collected and how long the data are retained. Both the conditions of a trade-off, as well as the circumstances of the participants' lives play a role. The potential availability of data to third parties was also a consideration.

In summary, technology acceptance models assess users' intention to use a system through factors such as performance and effort expectancy. The inclusion of non-pragmatic user experience factors, such as psychological needs, into acceptance models has been considered relevant (Hornbæk & Hertzum, 2017) and the consciousness and rationality of privacy trade-offs has been challenged. There is thus a strong rationale to include factors that are not based on rationality, again underlining the relevance of UX for this topic. More research is therefore needed on the reasons which influence users' acceptance of privacy trade-offs in different contexts, investigating the influence of both acceptance and UX factors.

3.3. Research objectives

Users sometimes accept certain privacy-related shortcomings in exchange for potential benefits of a technology. It is currently unclear whether technology acceptance models can be directly applied to privacy- and security-critical contexts, or whether important factors would be missing. The objective of this study is thus to explore and build hypothesis on additional dimensions which impact the acceptability of privacy-relevant technologies, thereby taking an interdisciplinary approach that contributes to bridging UX and TA models. Most TA models currently lack links to UX models. In particular, various hedonic qualities of experience are missing, such as psychological need fulfilment, which can provide a way of understanding the motivations behind the aims of use, or social factors (Hornbæk & Hertzum, 2017).

Our study addresses the following research question: To what extent can we use UX factors to complement technology acceptance models to be more applicable to the context of privacy-related technologies?

3.4. Methodology

We used a qualitative approach in order to obtain in-depth insights helping us understand to what extent UX factors can be used to complement technology acceptance models in the context of privacy-relevant technologies. A qualitative approach is well suited in this context to generate hypotheses on whether additional dimensions might be missing in the existing acceptance models. Qualitative studies also allow researchers to acquire an understanding of the situations in which technology is used (Blandford, Furniss, & Makri, 2016) and to discern the meaning people assign to processes and structures in their lives (Miles, Huberman, & Saldana, 2014). We used focus groups because group interactions force participants to question their beliefs and eventually to argument in order to defend their opinions (Krueger & Casey, 2014). To do so, they often rely on personal stories and also describe the values underlying their viewpoints. In addition, focus groups allow for factors outside the classical scope of acceptance models to show their relevance.

3.4.1. Participants

Thirty-two participants (17 men, 15 women) from different cultural and socioeconomic backgrounds participated in focus groups discussions. We created eight groups of a manageable size: two IT-literate expert groups, two student groups with non-IT related majors, and four groups of the general population. Experts and non-experts participated in separate groups to avoid experts influencing the other participants' opinions. The expert groups were recruited using the authors' professional networks while the student groups were recruited at the university. Recruitment within the general population was conducted using social network groups of local municipalities. Participants received a financial compensation. The average age of our participants was 33 years (Min = 19, Max = 55). Our sample covered various educational backgrounds. The participants had a multitude of nationalities.

3.4.2. Procedure

We conducted eight focus groups, of which four took place in a face-to-face setting and four online, allowing us to reach people beyond the geographical area of the university.

Each group comprised 4 to 5 participants who did not know each other. The sessions were administered in January 2018, during a single week in order to reduce the potential impact of a privacy-related information that would have spread in the news. The face-to-face focus groups took place at the university, each session lasting about an hour. For the online focus groups, we decided to opt for Facebook, a tool that our participants were familiar with. We gave them the possibility to create a fake Facebook account in case they did not want their real name to appear in the focus group discussion, but only one participant used this possibility. The focus group discussion took place in a "private Facebook group", so that only the facilitator and the participants could access the discussion. All focus groups (online and offline) were conducted by the same facilitator who was a UX expert, working in the field of usable security, and trained in qualitative methods. This ensures high consistency with regards to the facilitations style and adherence to ethics standards.

Participants were presented a selection of technology use scenarios derived from Rainie and Duggan's report (2015). Given that we adopted a focus group approach, we chose to remove two of the scenarios used in their original study so we would have sufficient time to have an in-depth discussion for all scenarios without exceeding the one hour limit. The four scenarios we selected clearly described each situation with its advantages and disadvantages (Table 1). We selected one scenario ("free social media") describing a technology that is broadly used already, while the remaining three scenarios are still rather innovative. All of the scenarios describe a potential situation in which a technology could provide some benefits in exchange for the user sharing different types of data. In the following, we will refer to acceptability of these scenarios (the prospective judgement toward a technology which has not been experienced yet (Schade & Schlag, 2003)) rather than acceptance, given that the described technologies have not yet been used by our participants under the specific conditions mentioned.

Participants first commented on each scenario individually by writing down the pros and cons. Once all participants had written down their opinions on each scenario individually, a group discussion on the acceptability of the described technologies followed. Participants were instructed to comment on the reasons why they thought a scenario was acceptable or unacceptable, and to discuss various opinions. In order to get a rich picture of the factors influencing privacy-related acceptability, participants were not constrained to only discussing privacy-related issues, but their opinions on the acceptability in general,

privacy concerns were discussed only if they emerged naturally. The facilitator ensured that all participants contributed to the discussion and shared their viewpoint.

3.4.3. Qualitative content analysis process

A transcription of all focus group data was prepared to facilitate further analysis. The qualitative analysis process broadly followed Braun and Clarke's (2006) thematic analysis approach. They describe six phases of thematic analysis, starting with (1) familiarisation with the data, (2) a generation of initial codes and (3) searching for themes. After, (4) themes are reviewed and then (5) defined and named. Lastly, (6) a report is created. For the present study, after transcribing and familiarising themselves with the data, the first author generated initial codes using a bottom-up approach and searched for themes. The author then organized the themes in an affinity diagram, in order to map them with regards to the factors known from acceptance and UX frameworks. At this point, the other authors reviewed the themes and their links to the theory as suggested by the first author. The authors then discussed any disagreements and agreed on a final set of themes and their links to acceptance and UX theory.

Scenario	Description
Office surveillance cameras	"Several co-workers of yours have recently had personal belongings stolen from your workplace, and the company is planning to install high-resolution security cameras that use facial recognition technology to help identify the thieves and make the workplace more secure. The footage would stay on file as long as the company wishes to retain it, and could be used to track various measures of employee attendance and performance."
Sharing health information	"A new health information website is being used by your doctor's office to help manage patient records. Your participation would allow you to have access to your own health records and make scheduling appointments easier. If you choose to participate, you will be allowing your doctor's office to upload your health records to the website and the doctor promises it is a secure site."
Smart thermostat	"A new technology company has created an inexpensive thermostat sensor for your house that would learn about your temperature zone and movements around the house and potentially save you on your energy bill. It is programmable remotely in return for sharing data about some of the basic activities that take place in your house like when people are there and when they move from room to room."
Free social media	"A new social media platform is being used by your former high school to help manage communications about a class reunion. You can find out the basic information about the reunion over email, but your participation on the social media site would reconnect you with old friends and allow you to communicate more easily with those who are attending. If you choose to participate, you will be creating a profile using your real name and sharing a photo of yourself. Your access to the service is free, but your activity on the site would be used by the site to deliver advertisements it hopes will be appealing to you."

Table 1: Description of the scenarios from Rainie and Duggan (2015) used in the present study (French translation available in the supplementary material).

3.5. Results

In the following, participant codes are assigned to the verbatims. Participants 1-16 took part in face-to-face focus groups, participants 17-32 in online focus groups (Expert groups: P1-P4 and P17-P21, Student groups: P5-P8 and P22-P25, General population: P9-P16 and P26-P32).

3.5.1. Office surveillance cameras scenario

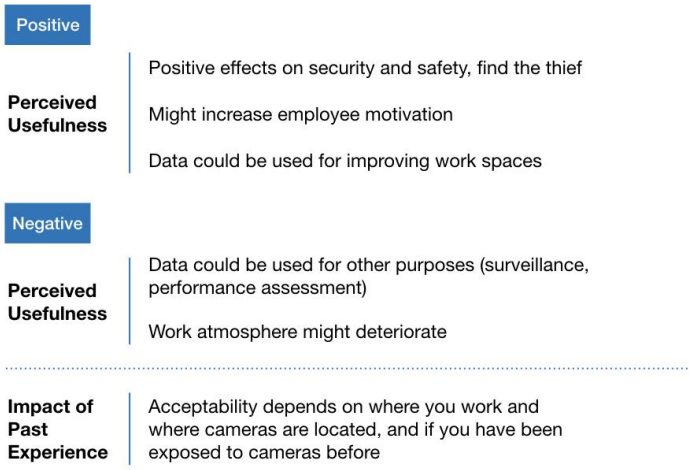


Figure 1: Most used arguments in favour of and against acceptability of the scenario "office surveillance cameras".

Perceived usefulness

On the positive side (Figure 1), participants stated that the office cameras might improve security and safety, and that they might help find the thief (as presented in the scenario). A few of them also argue that office cameras might positively impact employee motivation for instance by discouraging non work-related activities: *"Company controls employees, so no free-riders are watching Netflix during the working time." (P6, Student)*

Another positive aspect mentioned, perhaps more surprising as it does not relate to any part of the scenario, was that data about office occupancy and flow of people could be used as a basis for improving the design of work spaces: *"In a good way, it could be used to improve work experience, and the design of work spaces." (P1, Expert)*

Negative aspects were overall prominent in group discussions about this scenario, with participants fearing that data could be used for other purposes than security, such as surveillance of employees or performance assessment. These uses were perceived as intrusive, and some participants thought that security was mainly used as a pretext to introduce employee surveillance.

"It is not acceptable because it goes beyond the initial objective of finding the thief, which I am ok with, but if it is also for monitoring people [...] it goes beyond the acceptable, especially if the cameras use facial recognition." (P12, General population)

"I would feel like the company uses a phony reason in order to execute a plan that aims at monitoring and judging employees without their knowledge." (P19, Expert, in the context of surveillance cameras)

"It is not only about how we work, but also what we eat for lunch and who we are talking to." (P7, Student)

Lastly, participants indicated that cameras would deteriorate the work atmosphere and end up having negative consequences on the productivity of employees:

"It creates an atmosphere of mistrust and of "big brother is watching you." This is bad for the work atmosphere too, so I am not sure that the objective of performance will be reached by this mean." (P15, General Population)

Context

Most of the participants agree that the acceptability of these surveillance cameras depends on the type of work done, and the location of the cameras:

"There are certain places where it is required [...], like hotels, sports centers, something like this." (P7, Student)

"It is not acceptable in office corridors or office rooms. Entrances and reception lobby is fine." (P23, Student)

Impact of past experiences

Participants having worked in specific places, such as shops or hotels, declared being used to it and therefore having less issue with the acceptability of the scenario: *"But for me, I am fine. I mean I was always working in a company where there were cameras*

everywhere, because I was working in a hotel and we had to be protected, so I am fine with that." (P6, Student)

3.5.2. Sharing health information scenario

Figure 2: Most used arguments in favour of and against acceptability of the scenario "health information".

Perceived usefulness

A majority of participants thought that the increased efficiency when taking appointments and improved communication between doctors were positive aspects of this scenario (Figure 2). Another argument, mentioned several times, in favour of using the health information platform was that online banking worked: *"We are slowing down the evolution of the [e-health record] system because of security questions, which can be managed. The banks are doing it well!" (P19, Expert), "I feel like bank accounts are more secure" (P9, General Population)*

This led to discussions about the sensitivity of bank data as compared to health data: *"It is the same thing with bank account data. I prefer that someone knows my medical data rather than my bank account." (P10, General Population), "Bank data is not as sensitive as health data." (P32, General Population)*

Eventually, a question that also occupied our participants was the added value of sharing the data. Some found that it might be preferable to only enable patients to book appointments online, without in return obliging them to share their medical data on the platform.

Perceived control and autonomy

Participants appreciated that patients would have more control over their medical data. The importance of free consent was emphasised by participants, who acknowledge the fact that using the health information platform was not mandatory in the scenario. One should *"not be obliged to enrol" (P11, General Population)* and *"Personal consent is required." (P24, Student)*

A considerable number of participants were concerned about what happened to their data. They wondered who could gain access to it and were concerned about hacking*: "Even if it is secure, there will always people who can [hack the health data], there is always someone who is smarter. They can crack anything anyhow." (P13, General Population)*

Some mitigated that fear by stating that the current medical system might already be flawed: *"Well, there are IT security flaws, that's what I noticed, but at the same time [at the moment] I'm pretty sure that my data is already digitized and stored on a server somewhere and I'm not even sure where they are [...]." (P15, General Population)*

On the technical side, some expert participants also found that there was not enough information on the security mechanisms that were used to make the platform secure. This expert would for example double check how secure the platform is: *"If my doctor "promises" that the site is secure, I will not take his word for it, but I'll dig into the actual security." (P18, Expert)*

Context and user-related factors

Participants were worried that health data might be used against them in different contexts, including insurance companies, pharmaceutical industries and discrimination of potential employers due to health issues: *"Insurance companies could use the data against me as in the US, but also banks or other organisations." (P1, Expert)*

In the group discussions, it was emphasised that the acceptability of this platform also depended on how severe one's health issues are, mentioning for example HIV and its stigmatisation in society: *"There are many diseases that some people would want to keep to themselves. Especially in the case of HIV patients." (P23, Student)*

3.5.3. Smart thermostat scenario

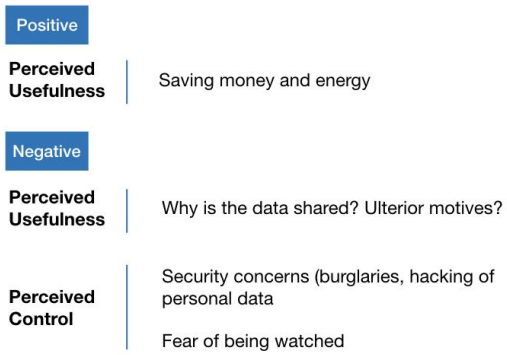


Figure 3: Most used arguments in favour of and against acceptability of the scenario "smart thermostat".

Perceived usefulness

A considerable number of participants mentioned energy and financial savings as advantages of this scenario (Figure 3). This is in line with previous research (Paetz et al., 2011) stating that monetary benefits were a crucial driver for adoption of electricity demand regulating smart home devices. Some participants did not see any disadvantages to the scenario: *"To me this is acceptable, it absolutely doesn't disturb me, on the contrary [...]. It is not intrusive to me." (P9, General Population)*

The groups also reflected upon which amount of money would justify the trade-off of having movement data shared, yet there was no consensus on the price value of the savings: *"I would probably use it, if it helps me save a lot of money on my electricity bill. But if it is 10€ a month, not really." (P6, Student)* In another focus group, one participant underlined that even small amounts of money are important. *"That's 120€ a year, that's not nothing!" (P10, General Population)*

Eventually, a considerable number of participants questioned the motives for sharing the data: *"Why does there have to be data sharing? If I have a system here, it can be local. Why do I need to share this - with whom? It does not say it here." (P16, General Population)*

"Energy consumption is not negotiable: it should not be a return for a favor." (P2, Expert)

Perceived control

Some indicated that tech companies might combine data from different sources and make predictions. The trustworthiness of the company was sometimes questioned.

"I feel like this is almost voyeurism. Sharing data on the rooms in which someone is present, this is extremely personal. And when we see that Facebook can predict a divorce 2 years in advance and that it knows more than the national institute of statistics, we quickly imagine the statistics and predictions made possible by tracking people's presence in the rooms of their house." (P17, Expert)

"The company should be prevented to pair this data with any other data." (P24, Student)

"I don't agree with the fact that I don't know who has access to my data, or for what purpose they will be used, if they will be sold etc." (P15, General Population)

On another negative side, a large number of participants mentioned security concerns, some also considering the potential scaling of burglaries: *"Imagine if you hack an entire district and you know the right moment for break-ins in the entire district." (P32, General Population)*

Context

Overall, participants often stated that more information on the kind of data being collected would need to be specified. Acceptability of the device would therefore depend on how "private" or "sensitive" the type of data shared was perceived by the participants: *"If it is in any way identifying or giving out any information, personal or non-personal data about any of my rhythms or things I do in my house then I would not want to do it." (P3, Expert)*

3.5.4. Free social media scenario

Figure 4: Most used arguments in favour of and against acceptability of the scenario "free social media".

Perceived usefulness and enjoyment

On the positive side (Figure 4), our participants emphasized the enjoyable aspects of social media which make it easy to stay in touch with peers. Other positive remarks referred to the free use of the platform.

More surprisingly, many participants also underlined the advantages of targeted ads, even though this seems hard to admit for some people and led to interesting discussions on profiling. Reacting to a previous comment on the interest of targeted ads, one of the expert participants stated: *"This is something I also wanted to add but then I thought no, I don't want to write this down. But there are some ads I actually like. And there are very often some ads that are so well targeted that I am very happy to discover them. I usually say "Oh come on, that's just another ad…" and then I think "They know me well!"" (P1, Expert)*

The multiplication of accounts was an important negative aspect related to the introduction of "just another social network".

Perceived autonomy

Several participants appreciated that one was not obliged to use the platform.

On the negative side (Figure 4), a large number of participants indicated that they found too many ads intrusive and annoying. However, they also thought that it is the responsibility of the user to not share sensitive data and to not click on unwanted ads, as stated for instance by this participant: *"Whoever is using it has to be extremely careful in the information they are posting online. At the moment you post it online, it's online forever." (P23, Student)*

Some participants also used this argument to make the point that people who did not like their data being shared were free not to use the platform. *"I am not a dangerous person, I don't write anything about bombing, or drugs and stuff. So for me it is ok, I am fine that WhatsApp will share my data if they need. But for some people [...] they feel unprotected. But then they don't have to use it." (P6, Student)*

Perceived control

Some participants did not appreciate the lack of control of the data they shared on social media. Many participants also reported feeling "*observed*, *followed*" *(P9, General*

Population), and mentioned that such a platform should not be advertised as being free, because users "pay" with their data: "*Can we fight against the language of "FREE social media" or "FREE service"? Because simply put, it is not free. We are a file of data, used for statistics, products and so on." (P24, General Population)*

Impact of past experiences

Many also found it acceptable because they already use similar social networks: *"For me this scenario is acceptable because it is the same configuration as Facebook, which I use regularly." (P28, General Population) - "I thought the same thing, given that I use Facebook I cannot say that this type of social platform is not acceptable." (P27, General Population)*

Participants also considered spam one risk of signing up to the social network, but this was not enough to make the scenario unacceptable, given that they were already used to spam. *"The downside is that it will be spam on your email of course, but come on, we have so much already, and I think it is ok." (P6, Student)*

Context and user-related factors

A few participants however distinguished the difficulties of "vulnerable" users who might not be able to differentiate ads from other types of content. *"My sister has a mental disability, when she sees ads I don't think she reacts like me. She would not be really aware that it is an ad." (P15, General Population)*

Participants felt that they were not important enough to be targeted on social media. *"But come on, I am not a famous or popular person, so I don't have this fear that this data will really be used against me." (P6, Student)*

3.6. Discussion

Our content analysis shows that both acceptance factors and UX factors played a role for participants. Perceived usefulness and ease of use are used in all acceptance models (with similar factors in UX models), while perceived enjoyment, perceived autonomy and the influence of past experiences are linked to hedonic aspects of UX.

3.6.1. Perceived usefulness, ease of use and perceived enjoyment

Across all technology acceptance models, Davis' (1985) dimensions of perceived usefulness and perceived ease of use (or related notions such as performance expectancy and effort expectancy in the UTAUT model (Venkatesh et al., 2003, 2012)) were considered as major factors explaining behavioral intention to use a system. These factors are comparable to pragmatic qualities of experience in UX models. In the present study, these aspects were indeed discussed extensively across scenarios and seemed to have a strong impact on participants' intention to use or accept the systems. While most participants could clearly see the added value of the health records (improved efficiency of the current scheduling system), the thermostat's usefulness was questioned with regards to the amount of energy saved and the necessity of sharing data. The social network's usefulness was also frequently challenged due to the fact that it did not seem substantially advantageous compared to existing platforms. Similarly, the surveillance cameras were not perceived as useful, and related shortcomings did not outweigh the disadvantages.

Interestingly, when the perceived usefulness of a system was not immediately clear to participants (e.g., the smart thermostat would actually not require any network connection to achieve its mission), one could sometimes note a feeling of mistrust, participants feeling like the company could have a hidden agenda: an apparently innovative technology could be a pretext for getting their data.

Perceived ease of use, on the other hand, was hardly discussed by our participants. Apart from rare mentions to the fact that some technologies could exclude part of the population (mainly the elderly), usability has not been used as an argument in favor or against the acceptability of a scenario. We hypothesize that the nature of the scenarios – rather vague and with no reference to interaction design - made it difficult for participants to imagine perceived ease of use either as a barrier or a facilitator.

3.6.2. Perceived enjoyment

Our participants rarely mentioned enjoyment as a relevant factor. The acceptability of the health data scenario for instance was explained with pragmatic aspects (similar to Rainie and Duggan., 2015) and pleasure was not mentioned as a relevant advantage of using an online health platform, which is in line with research by Tavares and Oliveira (2016) who found out that patients do not perceive the use of electronic health record portals as enjoyable. Performance expectancy and effort expectancy (which is comparable to the benefits identified by our participants) on the other hand had a significant impact on the

adoption of online health record platforms. While the smart thermostat has been described by some participants as "innovative", one could not observe a role for perceived enjoyment in that scenario either. In line with Krasnova et al., (2012), performance aspects (saving money / energy) again took the lead here. The closest "hedonic" dimension in the discussions was linked to individuals' values of preserving energy in order to promote a more sustainable way of consuming energy. The fact that perceived enjoyment was rarely mentioned as a relevant factor might also relate to the fact that hedonic factors, while crucial for choice, are only rarely acknowledged at an overt, rational level. This phenomenon is particularly strong when there is a need for justification and an explicit trade-off between hedonic and pragmatic (Diefenbach & Hassenzahl, 2011).

3.6.3. Perceived autonomy and perceived control

Hedonic UX factors linked to perceived autonomy and control were addressed in all focus groups. The importance of having a free choice of using a technology was highlighted across all scenarios. A frequent argument was also the fact that, if people did not want their data to be sold or used for other purposes, they are not obliged to use a technology. The lack of choice in the office camera scenario, as well as the uncertainty related to what data is collected and by whom it might be watched or used, was often mentioned as a barrier to acceptability.

The need for autonomy can be linked to voluntariness of use, which is one of the moderators of technology acceptance in the UTAUT model (Venkatesh et al., 2003). Beyond voluntariness, perceived control over the information that might be shared to third-parties seems to be one of the main UX factors impacting acceptability. This does not come as a surprise, given that control is a crucial factor in UX needs theories (e.g., (Hassenzahl et al., 2010; Sheldon et al., 2001)), which are considered relevant to technology acceptance (Hornbæk & Hertzum, 2017). A recurring position in all focus groups was for instance that people are keeping the control over what they decide to share on social media. Students and experts mostly felt in control over the information they post, therefore explaining their high level of acceptability. When participants expressed that they perceived the level of control as low, it was mostly linked to low acceptability: *"I don't agree with the fact that I don't know who has access to my data, or for what purpose they will be used, if they will be sold etc." (P15, General Population, in the context of the smart thermostat scenario)*

3.6.4. Perceived risks vs. benefits: a complex balance

As mentioned in the literature review, models of privacy calculus take into account perceived privacy risk and privacy concerns (Dienlin & Metzger, 2016; Dinev & Hart, 2006) and suggest that people's intention to disclose personal information depends on a privacy calculus, in which competing factors are assessed and users try to maximize the positive and minimize the negative consequences (Wottrich et al., 2018).

In the present study, the perceived privacy risk was dependent on the scenario. While in the health data scenario the risk of a privacy breach was frequently cited as a concern, in the social media example, the majority of our participants did not really fear that someone might use their data against them. Interestingly, mostly participants in the expert groups mentioned the risk that companies might combine data of different services and make predictions on that basis. This might indicate a low awareness of these practices within "layman" users, and therefore a lower perceived privacy risk impacting their intentions to use specific systems.

It is noteworthy that surveillance cameras were mostly assessed as acceptable by students. As they are not directly concerned by this scenario, one might assume that the perceived risks or disadvantages are low and distant. On the contrary, the very low acceptability ratings of other participants for this scenario might be explained by the fact that the risk of theft is rather small and hypothetical as compared to the immediate and consequent disadvantages employees would experience. It is therefore the perceived benefit that is assessed as too low to be relevant as a trade-off. This is in line with Hallam and Zanella (2017) who found that privacy breaches (in this case security incidents) might seem rather distant and hypothetical, and thus influence behavior less than short-term consequences.

3.6.5. The influence of previous experiences

Previous experiences form users' expectations, which then strongly influence users' early evaluations of the usability and enjoyment of a service (Kujala, Mugge, & Miron-Shatz, 2017) and thus play an important role in UX. A relevant observation made during the study refers to the use of personal anecdotes to explain one's opinion, such as the last time a participant went to the doctor and had to wait for a long time, which seemed to strongly influence her acceptance of online health records and their promise of increased efficiency. The same argument was employed in the context of office surveillance cameras, where previous exposure to such practices were used to explain why the participant found the

scenario acceptable. Interestingly, these types of reasoning were very frequently used during the discussion phase, but never written down during the individual phase. It seems that past experiences played an important role in participants' acceptability of technology and were used to illustrate and argue during the discussion phase. These past experiences described either critical incidents (e.g., especially satisfying or dissatisfying experiences in relation to the topic) or ordinary experiences that are integrated as a habit (e.g., cameras when working in a hotel or in a shop). In the first case, it seems like the incidents strongly influenced attitudes and behavior as a way to cope with the frustration or irritation felt. The second case might be close to the habit factor described by Venkatesh et al. (2012) who state that "the passage of chronological time can result in the formation of differing levels of habit depending on the extent of interaction and familiarity that is developed with a target technology" (p. 161). In addition, the self-consistency bias (Luu & Stocker, 2018) also became apparent in how participants viewed past experiences. Participants exhibited consistent judgements between the past use of a technology (e.g., social media) and why they thought a similar scenario was acceptable: *"given that I use Facebook I cannot say that this type of social platform is not acceptable" (P27, General Population).*

Our findings therefore tend to confirm that feedback from previous experiences indeed influences beliefs and future behavioral performance (Ajzen, 2011; Venkatesh et al., 2003, 2012). Note that these previous experiences are not to be understood necessarily as experiences with technology (acceptance models usually define "experience" as an opportunity to use a target technology (Venkatesh et al., 2012)), given that a negative experience with a "human" service can result in a more positive attitude towards a technology that would increase its efficiency.

At another level, many participants expressed a sort of resignation regarding advertisements, stating that they were so omnipresent that adding another service with ads did not make a real difference. This might point to the phenomenon of privacy fatigue (H. Choi, Park, & Jung, 2018) which refers to exhaustion and cynicism related to managing one's privacy and which has been shown to have a strong influence on privacy-related behavior.

3.6.6. The links between technology acceptance and user experience in the context of privacy trade-offs

In summary, our results show that both acceptance factors and UX factors played a role when judging the acceptability of privacy trade-offs. Pragmatic factors such as perceived usefulness were crucial factors for our participants. Hedonic qualities, namely the psychological needs of autonomy and control, also had a strong impact on the perceived acceptability of the scenarios. Our objective of studying non-pragmatic UX aspects that impact acceptance was partly reached. Some hedonic aspects of UX played a role in our study, such as perceived autonomy and control, but the results are non-conclusive with regards to other hedonic aspects. While relying on the scenarios provided by Rainie & Duggan (2015) came with the advantage of using accepted and validated materials on one hand, this material might simply not trigger the necessary emotions to make more far-reaching claims about e.g,. hedonic and enjoyment aspects. We nevertheless believe that these findings are promising and point towards the added value of including users' needs such as autonomy and control in the study of the acceptability of privacy trade-offs. By understanding users' needs, and by supporting their fulfilment through interaction, we can create positive experience and influence users' intention to use a system.

3.6.7. Individual judgement vs. group discussions

Given that our participants wrote down their perceived advantages and shortcomings of the scenarios individually before the group discussion, we observed that certain aspects were mostly written down, but hardly addressed in the group setting. In the first place, many of the advantages people mentioned individually and which were directly retrievable from the scenarios were not addressed in the groups. This might be due to the fact that these advantages are less controversial and therefore need less discussion, however one might also hypothesize that participants were less convinced of these advantages and mainly wrote them down because they were easily available in the scenario. This phenomenon sheds light on one of the advantages of the focus group methodology. While individually, participants had a tendency to write down the advantages that were easily available, the group discussion phase pushed them to explain further and argue their points of view and to concentrate on the most salient aspects. The social desirability bias might also have influenced participants to focus more on certain aspects, but our homogeneous groups mitigated a part of this bias by helping participants feel at ease expressing their

opinions. This also highlights the importance of including both individual and group measures in order to limit this bias.

3.6.8. Limitations

The goal of our study was to go beyond the pragmatic aspects currently covered by most acceptance models to explore the reasons why people accept privacy in certain contexts and build hypotheses regarding additional factors impacting acceptance. We used a qualitative approach, which typically does not have the objective of providing generalizable findings (Leung, 2015) but rather to explore new areas and develop hypotheses (Miles et al., 2014). While we thus do not claim that our results are generalizable, we believe that our analysis speaks beyond the scope of this study. The validity of this research was maximized by sampling a diverse set of participants based on the criteria of nationality, age range and work experience. The coherence of our results with existing theory supports their potential generalizability.

We used a focus group approach in order to provide rich explanations for acceptance of privacy trade-offs. This approach also allowed us to capture diverse viewpoints and observe the reactions of participants who were confronted to privacy concerns that differed from their own. Creating groups of students, experts and groups of the general population has allowed us to understand trends within these groups, which might be explored further in future studies.

Although every effort has been made to ensure the validity of our findings, the present study is subject to limitations that point to opportunities for future research. First, the rationality of privacy-related decisions has been challenged (Acquisti & Grossklags, 2005) and the link between acceptance and actual usage is not clear. A focus group setting that encourages logical explanations might induce a more analytical and rational thinking than might be observed in real-life settings where individuals might not discuss these settings prior to their behavior. However, this limitation was taken into account in the study design. While focus group discussions cannot predict behavior in an absolutely accurate way, they did indeed provide us with important insights into factors impacting privacy behavior. One might point to novel approaches to collecting privacy-relevant data, such as text mining methods using real online customer reviews (Rese, Schreiber, & Baier, 2014), which might be relevant when exploring privacy trade-offs as they actually study acceptance of systems in use and not only the projection of acceptability. Their limitation however is that people

usually report particularly satisfying or dissatisfying experiences, also called critical incidents.

From a methodological perspective, we are aware that certain arguments occur frequently because they were obvious from the scenario descriptions. We have highlighted these apparent arguments in the results section and have discussed the salience of arguments by comparing those who were produced individually versus during the discussion.

Our sample composition also presents inherent limitations, as a qualitative approach using focus groups usually does not reach a sample representative of the entire population. While the inclusion of contrasting groups (experts, students, general population) is already an asset of the present study, we did for instance not include teenagers or retired persons in our sample. This might be relevant for future work as some demographics have been shown to influence privacy-decisions (Rainie & Duggan, 2015). Cultural differences might also play an important role in privacy. Despite the fact that we had a diverse set of participants in terms of nationalities represented, the sample for each nationality was too small to derive any conclusions; we did not control for cultural bias.

For the online focus groups, we used Facebook as a platform, which excluded those who did not have a Facebook account or did not want to participate in a discussion group on this social network. This limitation was partially mitigated through the use of face-to-face focus groups.

3.6.9. Future work and recommendations for updated technology acceptance models in the context of privacy trade-offs

Taking into account these limitations, and building on the promising findings, we are planning for future work to include a quantitative questionnaire. It will allow us to exploit the results of this qualitative study and reach a more representative sample of the population over a number of different channels to exclude biases linked to the use of one social network only. The questionnaire will also take into account UX needs so as to further verify ties with UX, and the privacy paradox with the goal of evaluating not only the acceptability of the scenarios, but also the alignment of this acceptability with real-life actions. We also believe that future studies should conduct a more in-depth research on the influence of the human needs (Hassenzahl et al., 2010; Hornbæk & Hertzum, 2017; Sheldon et al., 2001) as these theoretical models and related design tools might be a great support for designers trying to cope with users' privacy concerns. In a health context,

Angst and Agarwal (2009) have for instance shown that even potential users with high levels of privacy concern can change their attitudes positively if message framing is adapted accordingly.

In order to support the inclusion of these theoretical models into practice, we recommend that design teams should strive to understand users' **needs** in the context of privacy trade-offs. Supporting fulfilment of these needs through the interaction might well influence users' privacy trade-offs and intention to use a system. Our results show that the needs of **autonomy and control** have an important influence on the acceptability of privacy-relevant technologies as participants wanted to be free to choose whether they wanted to use a technology, and they felt uneasy with the loss of control of their data. When creating an integrated model that bridges UX and TA research for application in the context of privacy-related technologies, the impact of these concepts should be closely investigated in detail. While in our study, autonomy and control were prevalent, design teams should also use existing tools to explore other needs that are relevant for their experience (e.g., UX Needs Cards (Lallemand, 2015)).

Another relevant UX factor when designing privacy-relevant experiences is the influence of **past experiences.** One should thus explore which past experiences users compare one's product or service to. Benchmarking such comparable experiences can help understand users' mental models and design their experience accordingly. In addition, closer examination of the self-consistency bias in the context of privacy trade-offs seems worthwhile.

Our study also shows that the acceptance of privacy trade-offs is highly context-dependent. We recommend that design teams studying acceptance should explore context-related factors in the design process, for example using tools such as contextual inquiry (Holtzblatt & Beyer, 2016) and synthesizing through user journey maps (Kalbach, 2016).

3.7. Conclusion

In the present study, we conducted focus groups with 32 participants in order to understand factors influencing their privacy trade-offs in four different use scenarios and to match these factors to both acceptance and UX frameworks. Our contribution consists in the rich qualitative insights elucidating the factors that influence the extent to which users accept privacy trade-offs, pointing to a selection of ties between acceptance and UX factors. While this calls for further research, it also points out that pragmatic aspects alone are

insufficient for explaining privacy trade-offs; a prominent example is that of "control" or "autonomy" suggesting that factors outside the conceptual space of technology acceptance dimensions are just as relevant. This further illustrates how human behavior is likely to depend not only on security and privacy awareness and that designers need to consider the technology and experience design as a whole instead of focusing on single aspects.

At a larger level, we expect the results of this study to contribute to the development of user-centred privacy initiatives and to the enrichment of current theoretical models of technology acceptance with additional aspects drawn from the field of UX.

3.8. Acknowledgements

We acknowledge support from the National Research Fund under grant number PRIDE15/10621687. We thank the anonymous reviewers for their feedback.

3.9. Appendix

Supplementary data to this article can be found online at https://doi.org/10.1016/j.chb.2019.106227.

3.10. References

Acquisti, A., & Grossklags, J. (2005). Privacy and rationality in individual decision making. *IEEE Security and Privacy Magazine*, *3*(1), 26–33. https://doi.org/10.1109/MSP.2005.22

Ajzen, I. (2011). The theory of planned behaviour: Reactions and reflections. *Psychology & Health*, *26*(9), 1113–1127. https://doi.org/10.1080/08870446.2011.613995

Al-Sharafi, M. A., Arsha, R. A., Abu-Shanab, E., & Elayah, N. (2016). The Effect of Security and Privacy Perceptions on Customers' Trust to Accept Internet Banking Services: An Extension of TAM. *Journal of Engineering and Applied Sciences 11(3):545-552*, 9.

Angst, C. M., & Agarwal, R. (2009). Adoption of Electronic Health Records in the Presence of Privacy Concerns: The Elaboration Likelihood Model and Individual Persuasion. *MIS Quarterly*, *33*(2), 339–370. https://doi.org/10.2307/20650295

Blandford, A., Furniss, D., & Makri, S. (2016). Qualitative HCI research: Going behind the scenes. *Synthesis Lectures on Human-Centered Informatics*, *9*(1), 1–115.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Choi, B. C. F., & Land, L. (2016). The effects of general privacy concerns and transactional privacy concerns on Facebook apps usage. *Information & Management*, *53*(7), 868–877. https://doi.org/10.1016/j.im.2016.02.003

Choi, H., Park, J., & Jung, Y. (2018). The role of privacy fatigue in online privacy behavior. *Computers in Human Behavior*, *81*, 42–51. https://doi.org/10.1016/j.chb.2017.12.001

Davis, F. D. (1985). A technology acceptance model for empirically testing new end-user information systems: Theory and results (PhD Thesis). Massachusetts Institute of Technology.

Desmet, P., & Hekkert, P. (2007). Framework of Product Experience. *International Journal of Design*, *1*(1).

Diefenbach, S., & Hassenzahl, M. (2011). The dilemma of the hedonic – Appreciated, but hard to justify. *Interacting with Computers*, *23*(5), 461–472. https://doi.org/10.1016/j.intcom.2011.07.002

Dienlin, T., & Metzger, M. J. (2016). An Extended Privacy Calculus Model for SNSs: Analyzing Self-Disclosure and Self-Withdrawal in a Representative U.S. Sample. *Journal of Computer-Mediated Communication*, *21*(5), 368–383. https://doi.org/10.1111/jcc4.12163

Dinev, T., & Hart, P. (2006). An Extended Privacy Calculus Model for E-Commerce Transactions. *Information Systems Research*, *17*(1), 61–80. https://doi.org/10.1287/isre.1060.0080

Distler, V., Zollinger, M.-L., Lallemand, C., Roenne, P. B., Ryan, P. Y. A., & Koenig, V. (2019). Security—Visible, Yet Unseen? *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, 1–13. Glasgow, Scotland Uk: ACM.

Egea, J. M. O., & González, M. V. R. (2011). Explaining physicians' acceptance of EHCR systems: An extension of TAM with trust and risk factors. *Computers in Human Behavior*, *27*(1), 319–332. https://doi.org/10.1016/j.chb.2010.08.010

Hallam, C., & Zanella, G. (2017). Online self-disclosure: The privacy paradox explained as a temporally discounted balance between concerns and rewards. *Computers in Human Behavior*, *68*, 217–227. https://doi.org/10.1016/j.chb.2016.11.033

Hassenzahl, M. (2008). User experience (UX): Towards an experiential perspective on product quality. *Proceedings of the 20th Conference on l'Interaction Homme-Machine*, 11–15. ACM.

Hassenzahl, M., Diefenbach, S., & Göritz, A. (2010). Needs, affect, and interactive products – Facets of user experience. *Interacting with Computers*, *22*(5), 353–362. https://doi.org/10.1016/j.intcom.2010.04.002

Hassenzahl, M., Eckoldt, K., Diefenbach, S., Laschke, M., Len, E., & Kim, J. (2013). Designing moments of meaning and pleasure. Experience design and happiness. *International Journal of Design*, *7*(3).

Hassenzahl, M., & Tractinsky, N. (2006). User experience—A research agenda. *Behaviour & Information Technology*, *25*(2), 91–97. https://doi.org/10.1080/01449290500330331

Holtzblatt, K., & Beyer, H. (2016). *Contextual design: Design for life*. Morgan Kaufmann.

Hornbæk, K., & Hertzum, M. (2017). Technology Acceptance and User Experience: A Review of the Experiential Component in HCI. *ACM Transactions on Computer-Human Interaction*, *24*(5), 1–30. https://doi.org/10.1145/3127358

Kalbach, J. (2016). Mapping experiences: A complete guide to creating value through journeys, blueprints, and diagrams. O'Reilly Media, Inc.

Keith, M. J., Thompson, S. C., Hale, J., Lowry, P. B., & Greer, C. (2013). Information disclosure on mobile devices: Re-examining privacy calculus with actual user behavior. *International Journal of Human-Computer Studies*, *71*(12), 1163–1173. https://doi.org/10.1016/j.ijhcs.2013.08.016

Krasnova, H., Veltri, N. F., & Günther, O. (2012). Self-disclosure and Privacy Calculus on Social Networking Sites: The Role of Culture: Intercultural Dynamics of Privacy Calculus. *Business & Information Systems Engineering*, *4*(3), 127–135. https://doi.org/10.1007/s12599-012-0216-6

Kraus, L., Wechsung, I., & Möller, S. (2016). *Exploring Psychological Need Fulfillment for Security and Privacy Actions on Smartphones*. https://doi.org/10.14722/eurousec.2016.23009

Kraus, L., Wechsung, I., & Möller, S. (2017). Psychological needs as motivators for security and privacy actions on smartphones. *Journal of Information Security and Applications*, *34*, 34–45. https://doi.org/10.1016/j.jisa.2016.10.002

Krueger, R. A., & Casey, M. A. (2014). *Focus Groups: A Practical Guide for Applied Research* (5th Edition). Retrieved from https://books.google.fr/books?id=APtDBAAAQBAJ

Kujala, S., Mugge, R., & Miron-Shatz, T. (2017). The role of expectations in service evaluation: A longitudinal study of a proximity mobile payment service. *International Journal of Human-Computer Studies*, *98*, 51–61. https://doi.org/10.1016/j.ijhcs.2016.09.011

Lallemand, C. (2015). Towards consolidated methods for the design and evaluation of user experience. University of Luxembourg, Luxembourg.

Leung, L. (2015). Validity, reliability, and generalizability in qualitative research. *Journal of Family Medicine and Primary Care*, *4*(3), 324–327. https://doi.org/10.4103/2249-4863.161306

Luo, X., Li, H., Zhang, J., & Shim, J. P. (2010). Examining multi-dimensional trust and multi-faceted risk in initial acceptance of emerging technologies: An empirical study of mobile banking services. *Decision Support Systems*, *49*(2), 222–234. https://doi.org/10.1016/j.dss.2010.02.008

Luu, L., & Stocker, A. A. (2018). Post-decision biases reveal a self-consistency principle in perceptual inference. *ELife*, *7*, e33334. https://doi.org/10.7554/eLife.33334

Mason, R. O. (1986). Four Ethical Issues of the Information Age. *MIS Quarterly*, *10*(1), 5–12. https://doi.org/10.2307/248873

Miles, M. B., Huberman, A. M., & Saldana, J. (2014). *Qualitative Data Analysis*. Retrieved from https://books.google.lu/books?id=3CNrUbTu6CsC

Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs*, *41*(1), 100–126.

Osswald, S., Wurhofer, D., Trösterer, S., Beck, E., & Tscheligi, M. (2012). Predicting information technology usage in the car: Towards a car technology acceptance model. *Proceedings of the 4th International Conference on Automotive User Interfaces and Interactive Vehicular Applications*, 51–58. Portsmouth, New Hampshire: ACM.

Paetz, A.-G., Becker, B., Fichtner, W., & Schmeck, H. (2011). Shifting Electricity Demand with Smart Home Technologies—An Experimental Study on User Acceptance. *30th USAEE/IAEE North American Conference Online Proceedings, Washington DC, 9-12 October 2011.*, 19.

Rainie, L., & Duggan, M. (2015). *Privacy and Information Sharing*. Pew Research Center.

Rese, A., Schreiber, S., & Baier, D. (2014). Technology acceptance modeling of augmented reality at the point of sale: Can surveys be replaced by an analysis of online reviews? *Journal of Retailing and Consumer Services*, *21*(5), 869–876. https://doi.org/10.1016/j.jretconser.2014.02.011

Schade, J., & Schlag, B. (Eds.). (2003). *Acceptability of Transport Pricing Strategies: An Introduction*. Retrieved from https://www.emeraldinsight.com/doi/pdfplus/10.1108/9781786359506-001

Shackel, B., & Richardson, S. J. (1991). *Human factors for informatics usability*. Cambridge university press.

Sheldon, K. M., Elliot, A. J., Kim, Y., & Kasser, T. (2001). What is satisfying about satisfying events? Testing 10 candidate psychological needs. *Journal of Personality and Social Psychology*, *80*(2), 325.

Tavares, J., & Oliveira, T. (2016). Electronic Health Record Patient Portal Adoption by Health Care Consumers: An Acceptance Model and Survey. *Journal of Medical Internet Research*, *18*(3), e49. https://doi.org/10.2196/jmir.5069

Tsai, J. Y., Egelman, S., Cranor, L., & Acquisti, A. (2011). The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study. *Information Systems Research*, *22*(2), 254–268. https://doi.org/10.1287/isre.1090.0260

Venkatesh, V., & Bala, H. (2008). Technology Acceptance Model 3 and a Research Agenda on Interventions. *Decision Sciences*, *39*(2), 273–315. https://doi.org/10.1111/j.1540-5915.2008.00192.x

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User Acceptance of Information Technology: Toward a Unified View. *MIS Quarterly*, *27*(3), 425–478. https://doi.org/10.2307/30036540

Venkatesh, V., Thong, J., & Xu, X. (2012). Consumer Acceptance and Use of Information Technology: Extending the Unified Theory of Acceptance and Use of Technology. *MIS Quarterly 36(1):157-178*, 22.

Westin, A. F. (1968). Privacy and freedom. *Washington and Lee Law Review*, *25*(1), 166.

Wottrich, V. M., van Reijmersdal, E. A., & Smit, E. G. (2018). The privacy trade-off for mobile app downloads: The roles of app value, intrusiveness, and privacy concerns. *Decision Support Systems*, *106*, 44–52. https://doi.org/10.1016/j.dss.2017.12.003

Wu, I.-L., & Chen, J.-L. (2005). An extension of Trust and TAM model with TPB in the initial adoption of on-line tax: An empirical study. *International Journal of Human-Computer Studies*, *62*(6), 784–808. https://doi.org/10.1016/j.ijhcs.2005.03.003

Chapter 4: Security – Visible, Yet Unseen? How Displaying Security Mechanisms Impacts User Experience and Perceived Security

Published as: Distler, V., Zollinger, M.-L., Lallemand, C., Roenne, P. B., Ryan, P. Y. A., & Koenig, V. (2019). Security – Visible, Yet Unseen? How Displaying Security Mechanisms Impacts User Experience and Perceived Security. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems.* Association for Computing Machinery. https://doi.org/10.1145/3290605.3300835

4.1. Abstract

An unsolved debate in the field of usable security concerns whether security mechanisms should be visible, or blackboxed away from the user for the sake of usability. However, tying this question to pragmatic usability factors only might be simplistic. This study aims at researching the impact of displaying security mechanisms on User Experience (UX) in the context of e-voting. Two versions of an e-voting application were designed and tested using a between-group experimental protocol (N=38). Version D displayed security mechanisms, while version ND did not reveal any security-related information. We collected data on UX using standardised evaluation scales and semi-structured interviews. Version D performed better overall in terms of UX and need fulfilment. Qualitative analysis of the interviews gives further insights into factors impacting perceived security. Our study adds to existing research suggesting a conceptual shift from usability to UX and discusses implications for designing and evaluating secure systems.

4.2. Introduction

Security concerns are becoming increasingly critical and pervasive. In 2018, security breaches continue to increase in cost and size [23] and the average total cost of a data breach amounted to $3.86 million, an increase of 6% from 2017. For critical systems such as election systems, the impact of security breaches goes far beyond financial cost, which has led the US Department of Homeland Security to declare the election system “critical infrastructure” highlighting its crucial importance to national security and economy [13].

Security research is thus of strategic importance, but while technical security has traditionally been well studied, human factors have long played a limited role in security

research. There has however been a growing understanding that many security breaches can be linked to "human error" [8] oftentimes because the system interfaces with its users in an insecure way and violates basic principles of psychology and security economics [17]. The field of usable security addresses this issue.

Research has discussed whether there is an inherent trade-off between security and usability [10] given that security introduces barriers to action, while HCI attempts to remove such obstacles. Automated approaches of security, which remove security decisions from the hands of the users, have thus emerged [12, 31]. However, this view has been challenged [32, 45], Norman [32] for example emphasised that appropriate technology can make some systems easier to use while enhancing security. It has also been shown that the lack of knowledge can be a root of security issues [3]. From a UX perspective, security can be an enabling factor and a significant part of UX [34] and the importance of taking into account UX factors has been underlined [9].

In this study, we take a user-centred perspective to security to investigate the impact of communicating security mechanisms on UX. We adopted a mixed-methods approach that combined user tests with semi-directive interviews, investigating both overall User Experience as well as psychological needs fulfilment.

This paper makes the following main contributions to the HCI community:

- Our findings extend existing knowledge on how displaying information on security mechanisms impacts people's UX.
- We identify additional key UX factors that impact perceived security.
- We propose actionable guidelines to support the design of secure systems for researchers and practitioners.

4.3. Related work

Different fields of research have adopted different definitions of security. Security can refer to personal security, physical security and computer security [30]. In the context of IT, security can be defined as the limited effects of an attacker trying to make a system fail [36]. This is coherent with many traditional definitions of security which typically refer to security mechanisms such as passwords or encryption [30]. These definitions are mostly concerned with systems or situations, whereas the definition of security in UX Design is concerned with the perceived security humans experience when interacting with

such system. A definition that is often used in UX has its origin in psychological needs theories, which define the need for security as “feeling safe and in control of your life rather than feeling uncertain and threatened by your circumstances” [20].

A related concept is privacy, which mostly focuses on either (1) the right to isolation or (2) the right to control information about oneself. Palen and Dourish [35] characterise privacy as “the continual management of boundaries between different spheres of action, and degrees of disclosure within those spheres”. These boundaries change with context.

4.3.1. Usable security: towards a stronger inclusion of User Experience

Usability is traditionally concerned with improving “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.” (ISO 9241-11)

In comparison, User Experience (UX) focuses less on task performance and puts a stronger emphasis on emotive, subjective and temporal aspects that play a role when users interact [37]. UX takes into account both hedonic (non-instrumental) and pragmatic (instrumental) qualities of experience [29]. Pragmatic qualities can be seen as similar to the aspects measured by usability. Users' frequent non-compliance with security procedures, combined with their difficulties using security mechanisms, have led some to believe that security and usability are inherently in conflict [7]. Other studies suggest that security and usability are interrelated in a complex way and trade-offs must be balanced [16].

Dunphy and colleagues [11] proposed that ideas from experience-centered design can help researchers in the security domain understand context-specific user behaviours, gain insights into subjective user perceptions of security or privacy and create theories about how technologies fit into people's lives. Studies have also underlined the need to take into account users' values in addition to experiential factors [9].

Pagter and Petersen [34] suggested the strategic use of explicit security actions to design for engaging experiences that are perceived as secure. They demonstrated that security can be a visible, enabling factor for experience, rather than a nuisance.

Studies have also shown that it is important to take into account psychological needs as a part of UX, given that fulfilment of psychological needs has been shown to contribute to a positive UX [18, 41]. The most relevant needs were narrowed down to autonomy, competence, relatedness, popularity, stimulation and security [18].

4.3.2. Visibility of security mechanisms and UX

Security mechanisms are often hidden away from the user [10]. While this approach has the advantage that users are not required to understand the underlying security mechanisms, it has been shown that lack of knowledge can be the root of certain security issues [3], and authors have argued that instead of being "transparent", security technologies should be "highly visible, available for inspection and examination seamlessly as a part of work" [10].

The effectiveness of displaying security mechanisms has been questioned, Schechter and colleagues [39] showed for instance that users mostly did not correctly interpret the lack of security indicators, such as HTTPS indicators or authentication images. In their study, even though the website showed increasingly important signs that it was not secure, no participant adopted "secure behaviour" and withheld their password. Their work thus seems to indicate that security indicators do not necessarily modify users' behaviour. Ferreira and colleagues [15] showed that context and beliefs play a role in users' security decisions regarding visible security indicators.

Fahl et al. [14] studied the usability and perceived security linked to encrypting Facebook messages, investigating different combinations of manual and automatic encryption and key management. Studies outside the scope of security indicate that the degree of visibility of a system's functioning might impact trust. Kizilcec [25] studied the impact of algorithmic transparency on trust in the context of peer-assessment. Participants who had received a lower grade than expected trusted the grading algorithm less, unless the algorithm was explained to them. On the contrary, when too much information on the algorithm was provided, trust was eroded.

4.3.3. Security and UX of e-voting

Paper voting systems have several shortcomings, some of which are of pragmatic nature (e.g., waiting times [42]), others are linked to security weaknesses. To respond to security-related and pragmatic concerns, researchers have developed end-to-end verifiable e-voting schemes (e.g., [4, 38]).

Privacy, in the context of e-voting, is defined by ballot-secrecy, receipt-freeness and coercion-resistance. Ballot-secrecy means that the system must not reveal the vote for a given voter. Receipt-freeness indicates that there is no information, or receipt, that can

directly prove a vote. Coercion-resistance means that a voter is able to cast a vote freely, even if a coercer can interact with the voter before, during and after casting.

Verifiability, on the other hand, should enable voters to check that their vote was cast-as-intended, recorded-as-cast and tallied-as-recorded. There is a distinction between individual verifiability, which means that voters can verify their own votes, and universal verifiability, which allows any observer of the election to verify the correctness of the result of the election.

In response to these security requirements, various voting systems have been developed. While these methods may solve some security problems that are associated to traditional paper voting, they also introduce some added complexity to the voting process [2]. Acemyan et al. [2] compared the usability of three voting systems, and found out that they were exceptionally difficult to use. In the first step of using the voting systems, casting a vote, only 58% of the participants were able to successfully cast a vote across all three systems. Overall satisfaction was low. For the second step of these voting systems, the verification phase, completion rates were even lower. The authors emphasise the importance of voting systems to be not only secure, but also usable.

Other studies have pointed towards a correlation between perceived security and acceptance of a voting method [44], thus pointing towards the relevance of investigating fulfillment of the need for security.

Going beyond usability, the UX of e-voting systems has only been studied to a limited extent. In this paper, we study the impact of displaying security mechanisms on User Experience in the context of e-voting. This use case is illustrative of an application in a high-stakes environment, yet nevertheless targeted at the general population. Some might view voting as a rare occasion, yet it is a frequent interaction considering all types of elections (e.g., citizenship, in a work or school context, associations). E-voting can thus be a regular, high-stakes interaction for most people. We use it here as a representative of security-relevant technologies and will discuss the underlying implications of our findings for the design of such systems.

4.4. Research objectives

An important debate in the field of usable security concerns whether security mechanisms should be made visible to users or rather stay invisible to improve systems' usability.

Knowing more about the impact of making security elements visible in different contexts will inform the design of security-relevant technologies to trigger optimal experiences. This study thus aims to address this challenge by adopting a more comprehensive UX perspective beyond usability concerns only.

The present study addresses the following research questions:

- RQ1: What is the impact of displaying encryption-related security mechanisms on UX?
- RQ2: What is the impact of displaying verifiability-related security mechanisms on UX?

Building on RQ1 and RQ2, we will derive actionable guidelines to support the design of secure experiences.

4.5. Methodology

4.5.1. Participants

38 participants took part in our study (19 male, 19 female). In order to ensure that all participants had comparable prior voting experiences, only persons who held the voting right and had participated in at least one political election were selected.

The average age was 35.4 years (Min = 19, Max = 73, SD = 12.45). Participants were recruited in online groups on social networks of nearby cities where users exchange practical information. We recruited a diverse sample of laypersons who were unknown to the researchers. 13% held no diploma or a diploma below the A-levels, 29% had obtained the A-Levels degree, 21% held a college degree, 18% a Bachelor's degree, 16% a Master's degree and 3% had a PhD.

There were 19 participants per group. Groups were assigned to ensure high similarity between conditions (age, gender, education), thus controlling for extraneous variables.

4.5.2. Procedure

We conducted 38 user tests and semi-structured interviews in summer 2018. Each session took approximately 1 hour. Participants gave informed consent and were compensated for their time.

The sessions were split up into 4 phases:

1. **Voting phase:** Participants cast a vote via the application.
2. **Post-voting UX evaluation:** The UX of phase (1) is evaluated through:
    a. *two questionnaires:* UEQ [28] and UX needs scale [27]
    b. a semi-structured interview.
3. **Verification phase:** Participants verify that their vote has been taken into account using the same app.
4. **Post-verification UX evaluation:** The UX of phase (3) is assessed using the same procedure as in phase (2).

Both the interview and questionnaires were administered twice i.e., once after the voting phase (T1), and once after the verification phase (T2). This repeated measure allows to explore users' thoughts about the voting and the verification phase in a separate manner given that verification has no direct equivalent in paper voting.

We combined questionnaires and interviews in order to gather both structured data (following a UX framework and allowing us to compare UX across versions D/ND and phases T1/T2) and deep insights formulated in users' own words.

In order to improve the ecological validity of our lab study, we introduced a scenario which participants should envision themselves in. This in-sitro approach consists in the recreation of elements of a real use situation in a lab setting, thus increasing the level of realism of lab studies [26]. We asked participants to imagine that the next national elections were about to take place, and that they had decided to vote online. They received some basic information regarding the candidates they could choose from for their election, as well as “official” letters which were personalized to each participant giving them the login details for the application. All sessions were facilitated by one of two trained facilitators in order to ensure high consistency with regards to the facilitation style. All participants casted their vote successfully and no major issues were encountered by participants in the two groups.

Special attention was paid to security priming, which is a common bias in usable security studies [16]. We attempted to avoid priming our participants by explaining that the goal of the study was merely to understand the UX of the application. In the interviews, no reference to security was made until the very end of the study.

4.5.3. Material

4.5.3.1. Standardized UX Scales

We used two standardized questionnaires as a measure of UX: the User Experience Questionnaire (UEQ, [28]) and the psychological needs scale (original questionnaire [41] adapted by Lallemand and Koenig [27]).

The UEQ measures overall attractiveness, pragmatic (instrumental) and hedonic (non-instrumental) qualities of experience. The pragmatic qualities subscales include perspicuity, dependability, efficiency. Hedonic qualities include stimulation and novelty subscales. The items are presented in the format of 26 contrasted pairs of words separated by a 7-points scale (ranging from -3 to 3) as exemplified here:

Attractive ○ ○ ○ ○ ○ ○ ○ Unattractive

The UX needs are a further UX measure which focuses on the fulfilment of psychological needs. Multiple studies show that fulfilment of psychological needs might be a driver of positive experience [19, 41]. The 30-items scale measures the fulfilment of the needs for competence, autonomy, security, pleasure, relatedness, influence and self-actualizing. While we were mostly interested in the needs of security, competence and autonomy, we administered the questionnaire including all needs in order to avoid security priming. We asked the participants to rate the fulfilment of their psychological needs using a 5-points Likert scale (from 1 Not at all to 5 Extremely). After having checked the reliability of each UX need subscale, we computed mean scale values for each need by averaging the respective items for each participant. Statistical analyses have been conducted using SPSS v24. Effect sizes are reported following Cohen's convention.

4.5.3.2. Interviews

The questions in the first interview (at T1, after the voting phase) concerned the overall impression participants had, any difficulties they might have encountered, and how they perceived the e-voting experience compared to paper voting. Trust in the application was also discussed. A free discussion followed, with the participant explaining their rationale. In the second interview (at T2, after the verification phase), participants were asked the same questions again, with additional questions pertaining to the verification phase. Questions regarding the perceived security were only asked at the very end of the session (in the end of the evaluation phase at T2) in order not to bias participants' earlier responses to refer mainly to security. A bottom-up content analysis of recurring topics followed, which were subsequently organised in an affinity diagram. The categories that were

obtained using the bottom-up analysis were closely related to the UX frameworks as deployed in the questionnaires, namely hedonic and pragmatic qualities, with additional factors identified, namely contextual factors and past experiences. Our objective was to understand how these factors impacted perceived security.

4.5.3.3 The e-voting smartphone application

We developed an Android application for the existing e-voting protocol Selene [38]. Selene is an end-to-end verifiable voting scheme that avoids voters having to handle an encrypted ballot and instead provides each person with a unique tracking number. This number allows voters to verify that their vote has been counted in a list of all votes. It thus takes a different approach from most voting schemes, which require users to handle an encrypted ballot in order to verify that their vote has been included in the tally.

Using the technical specifications of Selene, we created low- and high-fidelity prototypes, which we iteratively tested on end users and improved following a user-centered design process. In order to study the visibility of security mechanisms, two versions of the app were developed (screenshots in the additional material):

- *Version D* displays the employed security mechanisms (e.g., encryption or decryption) to the user through waiting screens (e.g., "currently encrypting your vote") and additional explanations as shown in Figure 1 and Figure 2.
- *Version ND* does not display any security mechanisms to the user. There were no waiting screens that informed users of the ongoing encryption. No explanations were given regarding the technical security mechanisms in place.

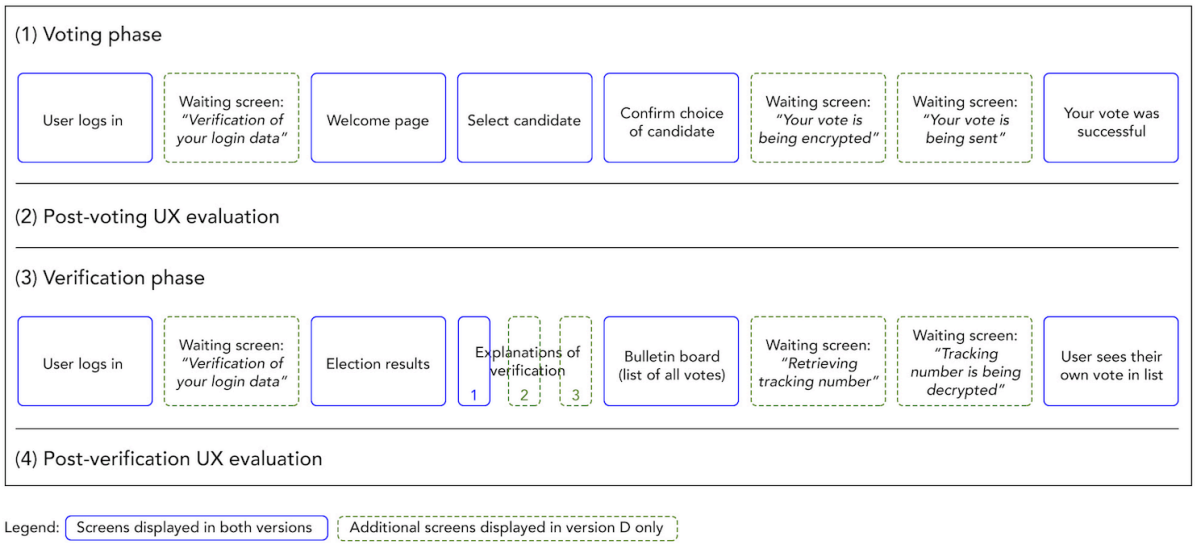


Figure 1: A conceptual overview of the differences between version D and ND of the app.

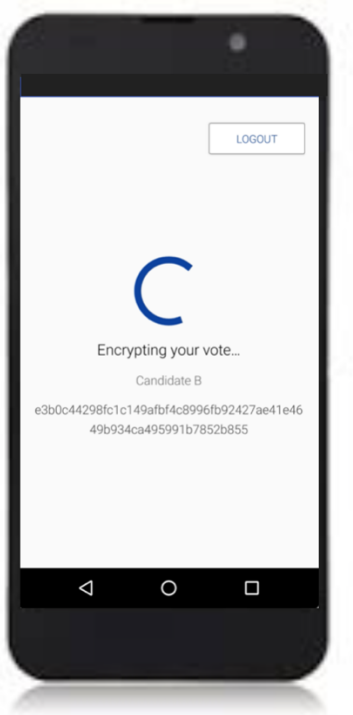


Figure 2: One of the screens displaying the security mechanisms of the app in version D during phase 1 (voting phase). No such informative screens were shown in version ND.

There were thus two main instances of security mechanisms that were made visible in the application: encryption/decryption processes (between-subject design, only in version D) and verification (within-subject design, present in both versions yet with more explanations in version D), in addition to the authentication phase.

4.6. Results

4.6.1. Impact of displaying security mechanisms on UX

4.6.1.1. User Experience Questionnaire

Both versions of our application scored above average on the UEQ (according to [40]) with average means of 1.12 (*SD* = 0.82) for version D and 1.05 (*SD* = 0.86) for version ND as shown in Table 1. Overall, respondents assessed version D (with visible security mechanisms) as slightly better than version ND. As shown in Figure 1, version D (at T1, *M* = 0.95, *SD* = 0.72) scored higher on hedonic aspects than version ND (*M* = 0.60, *SD* = 0.98) with a small effect size (*d* = 0.41). Version ND at T1 scored slightly higher for

pragmatic aspects (*M* = 1.64, *SD* = 1.41) than version D (*M* = 1.50, *SD* = 1.26), yet with a negligible effect size. At the subscale level, results indicate that Perspicuity (e.g., understandable/not understandable, difficult to learn/easy to learn) was experienced higher in version ND (*M* = 2.16, *SD* = 1.29) than in version D (*M* = 1.90, *SD* = 1.30, *d* = -.23). The hedonic subscale Perceived Novelty was significantly higher (t(36) = 2.20, *p* = .035) in version D (*M* = 1.31, *SD* = 1.09, version ND: *M* = 0.33, *SD* = 1.30) with a moderate effect size (*d* = 0.67).

4.6.1.2. Psychological Needs Questionnaire

This section focuses on the needs for Competence, Autonomy and Security. While these were the needs we were mainly interested in, we still collected data for all needs to avoid security priming. Our participants assessed the fulfilment of their need for Security as higher in version D (*M* = 3.80, *SD* = 0.71) than in version ND (*M* = 3.51, *SD* = 1.00) with a small effect size (*d* = 0.34). Similarly, the need for Competence was perceived higher in version D (*M* = 3.85, *SD* = 0.68) than in version ND (M = 3.54, SD = 1.35,d = 0.29). Both in version D and ND of the app, the feeling of Competence was higher after the voting phase than after the verification phase. The levels of perceived Autonomy were very similar for both versions (Version D: *M* = 4.05, *SD* = 0.69, Version *ND*: *M* = 4.13, *SD* = 0.81). No notable differences between versions were found regarding the fulfilment of pleasure, relatedness and influence. At the item level, the item "I felt I understood how things worked" (part of Security scale) was significantly higher inversion D (*M* = 4.32, *SD* = 1) than in version ND (*M* = 3.63, *SD* = 1.07, t(36) = 2.04, *p* = .049). In order to explore the relationships between the need for security and the other UX factors, we computed Pearson's correlation coefficients. We first explored the links between the fulfilment of the need for Security and the need for Competence (feeling capable and effective in one's actions) and found an overall moderate correlation for both version D and ND combined, (r(36)= .62, *p* = .001). While the two needs were not correlated in version D, they were strongly correlated in ND, (r(17) = .73, *p* = .001) and especially at T2 (r(17) = .87, *p* =.001). No significant correlation was found between Security and Autonomy for both versions D and ND, nor for Security and Pragmatic Quality or Security and Attractiveness. Last, Security and Hedonic Quality were moderately correlated at T2 only for version ND (r(17)= .49, *p* = .033). Regarding demographic factors, age was negatively correlated with all UX factors (Hedonic qualities: r(36) = -.30, *p* = .068, pragmatic qualities: r(36) = -.35, *p* = .031, attractiveness: r(36) = -.37, *p* = .024). Age was

also negatively correlated with perceived security yet in version D only (r(17) = -.42, p = .077). No significant correlation was found between age and the need for security in version ND. In version ND, age was negatively correlated with competence (r(17)= -.43, p = .077). No statistically significant difference was found with regards to participants' education level.

	Vers. D		Vers. ND			
	M	*SD*	*M*	*SD*	*d*	*p*
UEQ/Overall	1.12	0.82	1.05	0.86	0.08	0.810
UEQ/Hedonic	0.95	0.72	0.60	0.98	0.41	0.214
UEQ/Pragmatic	1.50	1.26	1.64	1.41	-0.11	0.741
UEQ/Attr.	1.18	0.69	1.18	0.92	0	0.997
Needs/Competence	3.85	0.68	3.54	1.35	0.29	0.371
Needs/Autonomy	4.05	0.69	4.13	0.81	-0.10	0.748
Needs/Security	3.80	0.71	3.51	1.00	0.34	0.304

Table 1: Summary of questionnaire results for both UEQ and needs questionnaire.

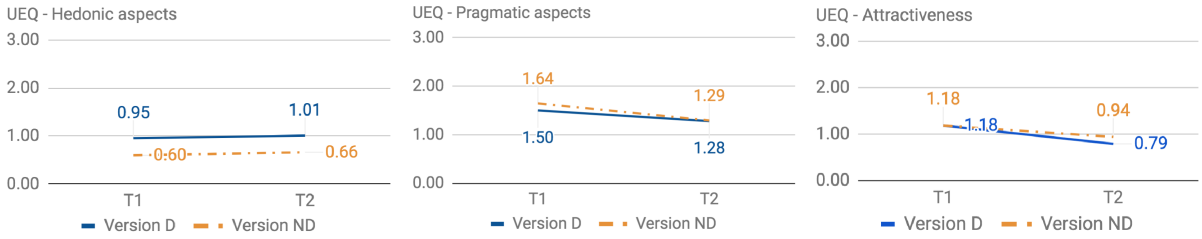


Figure 3: Results of User Experience Questionnaire (Version D: display of security mechanisms, Version ND: no display of security information. For statistically non-significant results, effect size was reported)

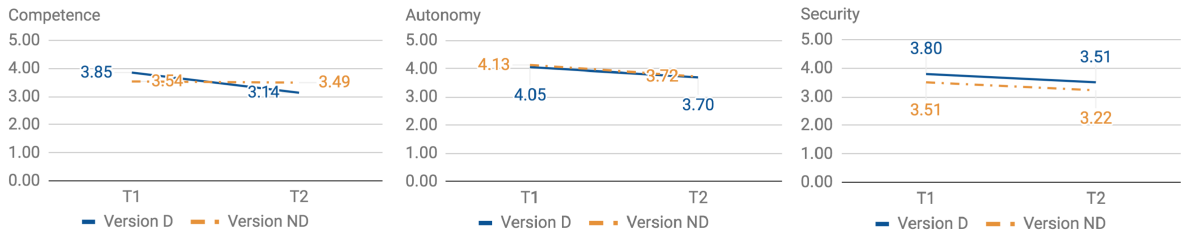


Figure 4: Results of psychological needs questionnaire (Version D: display of security mechanisms, Version ND: no display of security information)

4.6.2. UX factors impacting perceived security of e-voting

The results of the interviews were analysed using a content analysis of recurring topics and shed light on additional factors impacting the UX with a special focus on aspects

pertaining to the perceived security of participants. No notable differences emerged between the participant groups who had used version D and those who had used version ND. We thus report these findings with no distinction of the experimental group participants belonged to.

We studied three instances of visible security: the display of encryption, verification and the authentication phase. We will first report these findings, before describing additional factors that played an important role in the experience: general security concerns, the impact of pragmatic qualities, contextual factors and past experiences.

4.6.3. Impact of displaying encryption

Many participants who had used **version D** of the application did not consciously see or pay attention to the security mechanisms displayed to them. Most of those who did notice the mechanisms however felt reassured: “I like seeing that there is encryption, it is good to remind people that their data is secure and not hacked, and there is no HTTPS like in a browser.” (P35). “When I see ‘encryption ongoing’, that's reassuring.” (P17).

One participant who had used version D explicitly stated that they would choose seeing security-related information if they had a choice: “If I had the possibility to choose if I want to have access to this transparency for both encryption and verification, I would choose this [transparent] version.” (P32) The same participant even pushed for more transparency: “I like when it's open source, like this everyone can see if it is secure”.

In **version ND**, some participants perceived the process as too quick and easy. This left them with a feeling of uneasiness although they did not necessarily link it to the lack of security information. Few participants specifically referred to a lack of feedback in version ND, but P5 for instance found that there was not enough information: “I feel like user feedback is missing, usually I like having some little things telling me that it is secure.”

4.6.4. Impact of the verification phase

The verification phase is an unknown concept to most end-users, with no direct equivalent in real-life. In the application, there was a list of all votes that had been counted for the election. These votes are completely anonymous, only the user of the app can see their own vote for verification. The application explained vote verification to participants in an understandable way, which was validated in pre-tests. The results regarding verification were contradictory. Many participants expressed that vote verification was positive. “This

might be better than the current voting system where my vote completely disappears. It is reassuring." (P29), but many also did not see any advantage to verifying: "I am confused, I don't know what this is good for. A confirmation that my vote has been counted would have been sufficient." (P30).

Interestingly, verification, a mechanism designed to increase vote security, decreased many participants' perceived security: "I am less confident now [after the verification phase]." (P26)

While many participants simply did not see any use to vote verification, some expressed strong concerns regarding vote anonymity during this phase. Even though they had understood that their vote was still private, the fact of seeing all anonymized votes in a list gave them the impression that their vote was suddenly less confidential. One participant compared seeing the anonymized list of votes to opening the curtain of a voting booth, revealing the person's back, strongly emphasising that "just seeing a little bit is already too much. There is information one does not want to have." (P32)

Some participants compared the verification phase to the counting of votes in paper voting: "When I go to see the counting of votes, I know that the persons counting did it correctly. Here [with verification on the app] I don't have this certainty. On the internet, I am not convinced." (P24).

4.6.5. The importance of the authentication phase

Many participants described the authentication phase as critical for their perceived security, and interestingly, many participants believed that a secure authentication phase was sufficient to create security: "As soon as there were the login codes, I felt secure. Like online with the credit card icon, I felt secure." (P27)

Some participants suggested alternative authentication methods, such as using a digital fingerprint or two factor authentication to improve the overall security of the application. "In order to improve my trust, maybe there should be a log in with a digital fingerprint. I don't see anything else." (P25). These insights show that a carefully designed authentication phase can impact the perceived security of an entire application.

While the focus of this study was to examine the impact of displaying these instances of security, qualitative analysis showed that the participants' general security concerns played a role in their perception of the security mechanisms and the e-voting application as a

whole. Moreover, pragmatic qualities, contextual factors and past experiences contributed to their experience. We will describe these results in the following.

4.6.6. Security concerns

When asked whether they had any security concerns while using the e-voting application, many participants reported not having any: “About the security? No, nothing has come to my mind.” (P27) When prompted, they were unsure of security risks and described a general feeling of vulnerability when using technologies. A large number of participants mentioned some general security concerns, such as hacking, which they perceived as inherent to technologies in general and thus not something that can be avoided: “Yes, of course it is always possible to be hacked. That's not something I think about.” (P16). Most participants were unsure of the security risks linked to using smartphone apps. “Security questions? No. But it remains technology. Can there be leaks on an application? I think it might be hacked?” (P23)

Other security concerns either referred to human threats such as others voting instead of the legitimate person (“What if someone votes instead of me?” (P19)) or general technical threats linked to using the internet or smartphones; “For sure this is quicker, but I am not a fan of the internet. I think it's vulnerable, even if it is secure.” (P24). “Nothing is ever secure, nowhere.” (P28)

4.6.7. Pragmatic qualities

Our qualitative analysis showed that pragmatic aspects play an important role in the experience of e-voting. Our participants found the application practical, easy to use and understandable, with an appropriate design. “It was very quick and clear, you couldn't fall off track. It does its job.” (P3). They mentioned that e-voting in general might increase the vote turnout, and that it might mitigate some of the security problems of paper voting. On the negative side, our participants expressed concern for certain population groups: “I am very engaged with elderly people and I see the difficulties they have with IT. When I put myself in their shoes, it is complicated. Except if someone is next to them to help them vote on their phone, but what about vote secrecy?” (P19)

Interestingly, some participants stated that the ease of use gave them the impression that the application was trustworthy: “Given that it's easy to use I would trust it more.” (P32)

Pragmatic qualities did not only have a positive impact however. Surprisingly, participants found that the e-voting application was too easy to use: “It's easy but frustrating, you don't have to go anywhere, you just push a button and that's it. It is too quick”(P30). And lastly, there were also participants who stated that even though they did not really trust the app, they would still use it for practical reasons.

4.6.8. Contextual factors

Some contextual factors impacted our participants' UX when e-voting. First, many participants mentioned that receiving their login ID and password in letters gave them a feeling of security: “Receiving this by paper mail is reassuring.” (P2) Some however mentioned security concerns regarding paper mail, for example with regards to roommates or family members who might access their login details. Many participants were also reassured by the fact that the application had been issued by a governmental authority “I didn't wonder about security. If it is an app from the government, I thought that it must be secure”.

4.6.9. Past experiences

Participants consistently compared e-voting to paper voting. The symbolic value of casting a paper vote was important to them: “It's symbolic to go into the voting booth. I miss the symbolic aspect with e-voting, I think it would be a pity if we all voted on our phones.” (P23). Participants mentioned that they liked the personal contact when paper voting (“At the polling station we talk about our opinions, we discuss with people” (P27)). However, other participants mentioned that e-voting offered relief of the social pressure they experience at polling stations: “This is extremely anonymous, there is no pressure like at the polling station with the people behind you. On the smartphone, you can hardly be judged. This makes me feel more in security when voting.” (P15)

Participants also often referred to past experiences in other domains when evaluating the UX of the e-voting application. Banking apps were often used as an example for secure applications that everyone uses. Again, the organisation issuing the application was an important factor impacting perceived security: “If the app is from this bank, then it must be secure.” (P11) Some participants also explained that they were aware of potential security failures of banking apps, but underlined that the practical aspects of using a banking app were predominant: “I use the banking app, but I know that I am not safe.

There are people who get hacked. When something like this exists and it's practical, one uses it." (P16)

This is similar to the trust participants expressed in the e-voting application, which was grounded in its practicality and ease of use.

Other examples participants compared e-voting to were official administrative procedures which they completed online, such as tax returns: "I already do a lot of things online, my tax returns for example. It saves a tremendous amount of time. When it's easy to use, it suits me fine." (P27)

4.7. Discussion

4.7.1. Why designing for usability alone is insufficient: How displaying security mechanisms impacts UX

The first research question of the present study had the objective of investigating how displaying security mechanisms impacts User Experience. Both versions showed good scores for pragmatic quality, and it is noteworthy that all of our participants were able to successfully cast their vote compared to 58% for the e-voting systems tested by Acemyan and colleagues [2]. While these studies are comparable to a limited extent (e.g., slight differences in study design, contextual factors might have changed during four years), it is noteworthy that the voting applications tested in their study were not designed in a user-centred approach, pointing towards the value of adopting a UX process when creating e-voting applications.

In version ND, participants had less information to process since no security information was given to them. While this might have advantages for the efficiency and overall usability of a system, usability can also have downsides, as one of our participants explained: "Voting becomes banal. It is very quick, I am not for it." (P23). Making the process quicker and smoother might cause perceived security to decrease. Indeed, the need for security was slightly less fulfilled in version ND and the interviews show that the security mechanisms felt reassuring to participants. While many participants using version D of the app did not report seeing the security mechanisms, we hypothesise that the presence of security information, combined with the additional waiting time it introduced had a positive impact on the hedonic quality of the experience and on perceived security. Lower usability due to more visible encryption might thus be correlated with higher

perceived security. This hypothesis is in line with a study by Fahl and colleagues [14] who found the highest usability in the versions of their prototype that included either no display of security, where encryption was completely automated, or a combination of manual encryption and automatic key management. Similarly to our study yet not assessed using the same metrics, “security feeling” was highest in the versions with the lowest usability scores, which included some extent of manual encryption or key management.

Previous studies have investigated the usability of e-voting systems [2, 5, 44], but there is a dearth of research that takes into account UX in the context of e-voting. While usability is an important indicator and prerequisite for such systems, our study and related work thus indicate that the goal of making security-relevant technologies more usable alone is insufficient to create a positive UX. Dependent on the experience designers want to create, adopting a usability perspective alone might even be detrimental to the objective, given that usability does not take into account critical factors such as perceived security. Moreover, while a lack of usability will result in users' dissatisfaction, a good level of usability will not necessarily trigger satisfaction. This is what is commonly referred to as a hygiene factor as compared to motivational factors [20, 21].

The UX approach might provide insights into context-specific user behaviour, into subjective perceptions of security and privacy and create theories about how technologies fit into people's lives [11]. While the SUS [6] scale is most commonly used in the usable security community, more recent UX scales like the UEQ [28] allow researchers and practitioners to understand hedonic qualities of experience, in addition to the pragmatic quality (comparable with the measure supported by the SUS).

Ideas from experience-centered design might help researchers in usable security gain a deeper understanding of context-dependent behaviors and subjective user perceptions [11] due to a stronger focus on emotive, subjective and temporal aspects [37]. Beyond supporting the inclusion of UX-criteria in usable security studies, we believe that a conceptual change away from usability to UX would allow for a more holistic understanding of security-relevant experiences.

4.7.2. Transparency: a double-edged sword for UX

Including transparency is necessary to provide people with the means to understand the security implications of the configuration of technologies at their disposal, and it should be expressed in terms that correspond to users' activities and needs at the time [10].

Dourish et al. [10] suggest that security technologies should be highly visible and available for inspection.

In the present study, we investigated the impact of making security mechanisms visible on UX. There were three instances of security that were made visible in our application: two main instances of the display of encryption-related processes and the verification phase, in addition to the authentication phase.

The verification phase was studied as a security mechanism that is required in e-voting with the objective of making the voting process verifiably secure both at the individual and the universal level. As stated by Olembo and Volkamer [33], "user interaction for verifiability is required in verifiable e-voting systems, and therefore understanding is critical." (p. 173). Verification thus requires user interaction which is an important difference between these types of transparency given that the display of the encryption-related processes does not require any interaction.

The first way of providing transparency, the display of encryption and decryption processes, was embodied in version D of the application. As described above, this version showed overall more positive results in terms of UX and needs fulfilment, even though many participants reported not consciously having processed the display of the security mechanisms. This result is similar to Fahl and colleagues [14], in whose study manual key management (also implying a more visible security mechanism) equaled lower usability scores, but also higher perceived security. The authors suggested that the complexity of a mechanism might increase a user's perceived security, and that an entirely invisible and effortless protection mechanism might not generate a feeling of security. It is also noteworthy that participants using version D felt like they understood how things worked significantly better than in version ND, pointing to a potential improvement of understanding of the functioning of the app.

The second research question concerned the impact of displaying verifiability-related security mechanisms on UX. The verification phase yielded ambivalent reactions, even though the explanations were carefully worded and pre-tested. Overall, UX was assessed as better before the verification phase, and many participants did not understand the utility of seeing their own vote within the entire list of votes on the bulletin board. Some participants reported feeling more insecure, while others felt reassured that their vote had been counted towards the election result. The verification phase introduces some friction

to the process by requiring an additional interaction of the user which is not directly aligned with their objective at the time of use. Verification has no direct equivalent in real life users can base their understanding on, it has been considered an “unnatural concept” for users [44]. The verification process is however necessary from a security standpoint, it is thus important to design this process in a way that supports UX and perceived security.

Referring back to Dourish and colleagues [10], more research is needed to investigate how verification can be communicated even better for those participants for whom seeing the list of votes was a perceived mismatch with their need at the time, which was to check that their vote (and their vote only) had been recorded correctly.

A discrepancy was noteworthy in this context. Introducing a certain degree of complexity by displaying the encryption and decryption process had a negative impact on pragmatic aspects, but a positive impact on overall UX. This result is promising given that it indicates that displaying security mechanisms such as encryption, while not necessarily improving usability, might improve overall UX. Displaying information about encryption might also contribute to users' understanding of encryption processes who often have misconceptions about the latter [1]. The verification phase, in contrast, had a negative effect on UX, and it had, according to the interviews, the shortcoming of not being aligned with the users goals at the moment. This example demonstrates that transparency needs to be provided in a meaningful and purposeful way that is aligned with users' goals.

4.7.3. Limitations and future work

The present study has also shown some limitations. While great efforts were made to maximize the validity of our study (e.g., use of scenarios and elements simulating a real election such as official personalised letters), the fact that it took place in a lab setting might have increased participants' feeling of security [39, 43] and partially biased the evaluation of UX on specific aspects (e.g., social factors) which are harder to assess in a controlled environment [27].

In our study we used two versions of the same smartphone application. Future studies should investigate the impact of a larger diversity of visualisations of security mechanisms on UX. Another aspect that was not addressed by our study are cultural aspects that might impact UX, including perceived security (e.g., for countries where voting is linked to higher risks). Similarly to previous literature [33], our study takes a western perspective and future studies should investigate cultural differences linked to e-voting perceptions.

4.7.4. Recommendations for the design of security-relevant technologies

We suggest the following recommendations for researchers and designers who have the objective of improving the UX and perceived security of security-relevant technologies.

Do not assume users necessarily have security concerns: Users do not necessarily have many concerns regarding IT security. One should therefore avoid the security-priming bias by not prompting participants to think about security topics.

Be aware that users do not always have the required knowledge to assess a system's security level: Many users have a limited knowledge of security but have a general feeling that new technologies can bear security risks, often referring to the general risk of "hacking". Design teams should explore users' security knowledge and iteratively test security-relevant processes on the target population.

Take advantage of users' beliefs about the authentication phase for enhancing technical security: Users often refer to the perceived security of the authentication phase (when applicable) as a proxy for overall security and seem to be willing to invest more efforts at this stage to safeguard their security. Designers might thus introduce additional authentication security measures if necessary (e.g., biometrics, 2 Factor Authentication).

Include contextual factors as essential aspect of experience / security design: When forming an opinion of the perceived security of an application, users take context into account. The experience of any system starts before the interaction and users rely on related information (e.g., which organisation or authority issued the app) to make the choice of using a system or not. Exploring users' needs through contextual inquiry [22]and synthesizing them through user journey maps [24] safeguards the integration of contextual factors during the design process.

Benchmark comparable experiences likely to act as users' reference points: Users also use past experiences to make sense of their current experience. One should therefore carefully investigate potentially related experiences to understand the elements that impact perceived security. Some of these elements may then be transferred to one's project.

Use transparency in a purposeful way and consider the relevance of trade-offs between usability and other experience related factors: Transparency (in the sense of displaying security mechanisms) can shape perceived security either for the sake of a more optimal experience or for adding friction when user awareness of security is critical. One should adopt a larger conceptual model when designing security relevant technologies, not

limited to usability. Design and evaluation methods should support this more comprehensive perspective: an example of this would be replacing usability scales such as SUS or QUIS with more recent UX scales (e.g., UEQ used in the present study) when assessing systems' qualities.

4.8. Conclusion

The present study aims to address the debate of whether security mechanisms should be visible to users using a more comprehensive UX approach that goes beyond usability alone. It makes three main contributions. First, it builds on existing knowledge on how displaying information on security mechanisms impacts people's UX. Second, it identifies UX factors that impact perceived security. The results have shown that factors impacting UX and perceived security go beyond usability aspects, which supports the inclusion of such factors into usable security studies. Our study adds to existing research suggesting that a conceptual shift from usability to User Experience might bring substantial added value to the field of usable security. Our third contribution thus consists in suggesting a number of recommendations for design and research in usable security. The results of this study are thus promising, and we expect the results to contribute to future studies which investigate to what extent displaying information on security mechanisms can be an enabling factor to UX.

4.9. Acknowledgements

We thank the anonymous reviewers for their constructive feedback. We acknowledge support from the National Research Fund (FNR) under grant number PRIDE15/10621687. PBR was partly supported by the FNR INTER-Sequoia project which is joint with the ANR project SEQUOIA ANR-14-CE28-0030-01. MLZ was supported by the INTER-SeVoTe project.

4.10. References

[1] Abu-Salma, R., Redmiles, E.M., Ur, B. and Wei, M. 2018. Exploring User Mental Models of End-to-End Encrypted Communication Tools. *Proceedings of the 8th USENIX Workshop on Free and Open Communications on the Internet (FOCI)* (Baltimore, MD, Aug. 2018), 8.

[2] Acemyan, C.Z., Kortum, P., Byrne, M.D. and Wallach, D.S. 2014. Usability of voter verifiable, end-to-end voting systems: Baseline data for Helios, Prêt à Voter, and Scantegrity II. *The USENIX Journal of Election Technology and Systems*. 2, 3 (2014), 26–56.

[3] Adams, A. and Sasse, M.A. 1999. Users are not the enemy. *Communications of the ACM*. 42, 12 (Dec. 1999), 40–46. DOI:https://doi.org/10.1145/322796.322806.

[4] Adida, B. 2008. Helios: Web-based Open-Audit Voting. *USENIX security symposium* (2008), 335–348.

[5] Bederson, B.B., Herrnson, P.S., Niemi, R.G., Lee, B. and Sherman, R.M. 2003. Electronic Voting System Usability Issues. *NEW HORIZONS*. 5 (2003), 8.

[6] Brooke, J. 1996. SUS-A quick and dirty usability scale. *Usability evaluation in industry*. 189, 194 (1996), 4–7.

[7] Cranor, L.F. and Garfinkel, S. 2004. Guest Editors' Introduction: Secure or Usable? *IEEE Security Privacy*. 2, 5 (Sep. 2004), 16–18. DOI:https://doi.org/10.1109/MSP.2004.69.

[8] Cranor, L.F. and Garfinkel, S. 2005. Realigning Usability and Security. *Security and Usability*. O'Reilly Media, Inc.

[9] Dodier-Lazaro, S., Sasse, M.A., Abu-Salma, R. and Becker, I. 2017. From Paternalistic to User-Centred Security: Putting Users First with Value-Sensitive Design. *Workshop on Values in Computing. 09 May 2017* (2017), 7.

[10] Dourish, P., Grinter, R.E., de la Flor, J.D. and Joseph., M. 2004. Security in the Wild: User Strategies for Managing Security as an Everyday, Practical Problem. *Personal and Ubiquitous Computing*. 8, (2004).

[11] Dunphy, P., Vines, J., Coles-Kemp, L., Clarke, R., Vlachokyriakos, V., Wright, P., McCarthy, J. and Olivier, P. 2014. Understanding the Experience-Centeredness of Privacy and Security Technologies. (2014), 83–94.

[12] Edwards, W.K., Poole, E.S. and Stoll, J. 2008. Security automation considered harmful? *Proceedings of the 2007 Workshop on New Security Paradigms - NSPW '07* (New Hampshire, 2008), 33.

[13] Elections - Critical Infrastructure: *https://www.eac.gov/election-officials/elections-critical-infrastructure/*. Accessed: 2018-09-20.

[14] Fahl, S., Harbach, M., Muders, T., Smith, M. and Sander, U. 2012. Helping Johnny 2.0 to encrypt his Facebook conversations. *Proceedings of the Eighth Symposium on Usable Privacy and Security - SOUPS '12* (Washington, D.C., 2012), 1.

[15] Ferreira, A., Huynen, J.-L., Koenig, V., Lenzini, G. and Rivas, S. 2015. Do Graphical Cues Effectively Inform Users? *Human Aspects of Information Security, Privacy, and Trust*. T. Tryfonas and I. Askoxylakis, eds. Springer International Publishing. 323–334.

[16] Garfinkel, S. and Lipford, H.R. 2014. *Usable Security : History, Themes, and Challenges*. Morgan & Claypool Publishers.

[17] Gollmann, D., Herley, C., Koenig, V., Pieters, W. and Sasse, M.A. 2015. Socio-Technical Security Metrics (Dagstuhl Seminar 14491). *Dagstuhl reports*. 4, 12 (2015), 28.

[18] Hassenzahl, M. 2008. User experience (UX): towards an experiential perspective on product quality. *Proceedings of the 20th International Conference of the Association Francophone d'Interaction Homme-Machine on - IHM '08* (Metz, France, 2008), 11.

[19] Hassenzahl, M., Diefenbach, S. and Göritz, A. 2010. Needs, affect, and interactive products – Facets of user experience. *Interacting with Computers*. 22, 5 (Sep. 2010), 353–362. DOI:https://doi.org/10.1016/j.intcom.2010.04.002.

[20] Hassenzahl, M., Eckoldt, K., Diefenbach, S., Laschke, M., Len, E. and Kim, J. 2013. Designing moments of meaning and pleasure. Experience design and happiness. *International Journal of Design*. 7, 3 (2013).

[21] Herzberg, F. 1976. One More Time: How Do You Motivate Employees? *Job Satisfaction — A Reader*. M.M. Gruneberg, ed. Palgrave Macmillan UK. 17–32.

[22] Holtzblatt, K. and Beyer, H. 2016. *Contextual design: Design for life*. Morgan Kaufmann.

[23] IBM Security Services 2018. *The 2018 Cost of a Data Breach Study by the Ponemon Institute*.

[24] Kalbach, J. 2016. *Mapping experiences: A complete guide to creating value through journeys, blueprints, and diagrams*. O'Reilly Media, Inc.

[25] Kizilcec, R.F. 2016. How Much Information?: Effects of Transparency on Trust in an Algorithmic Interface. (2016), 2390–2395.

[26] Kjeldskov, J. and Skov, M.B. 2007. Studying Usability In Sitro: Simulating Real World Phenomena in Controlled Environments. *International Journal of Human-Computer Interaction*. 22, 1–2 (Apr. 2007), 7–36. DOI:https://doi.org/10.1080/10447310709336953.

[27] Lallemand, C. and Koenig, V. 2017. Lab Testing Beyond Usability: Challenges and Recommendations for Assessing User Experiences. *Journal of Usability Studies*. 12, 3 (2017), 22.

[28] Laugwitz, B., Held, T. and Schrepp, M. 2008. Construction and Evaluation of a User Experience Questionnaire. *HCI and Usability for Education and Work*. A. Holzinger, ed. Springer Berlin Heidelberg. 63–76.

[29] Mahlke, S. 2008. *User experience of interaction with technical systems*.

[30] Mathiasen, N.R. and Bødker, S. 2008. Threats or threads: from usable security to secure experience? *Proceedings of the 5th Nordic conference on Human-computer interaction: building bridges* (2008), 283–289.

[31] Montesino, R. and Fenz, S. 2011. Information Security Automation: How Far Can We Go? *2011 Sixth International Conference on Availability, Reliability and Security* (Vienna, Austria, Aug. 2011), 280–285.

[32] Norman, D.A. 2009. When security gets in the way. *interactions*. 16, 6 (Nov. 2009), 60. DOI:https://doi.org/10.1145/1620693.1620708.

[33] Olembo, M. and Volkamer, M. eds. 2013. *Human-Centered System Design for Electronic Governance: Lessons for Interface Design, User Studies, and Usability Criteria*. IGI Global.

[34] Pagter, J.I. and Petersen, M.G. 2007. A Sense of Security in Pervasive Computing—Is the Light on When the Refrigerator Door Is Closed? *International Conference on Financial Cryptography and Data Security* (2007), 383–388.

[35] Palen, L. and Dourish, P. 2003. Unpacking "Privacy" for a Networked World. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (2003), 129–136.

[36] Pieters, W. 2006. Acceptance of voting technology: between confidence and trust. *Trust Management, 4th International Conference, iTrust 2006, Pisa, Italy, May 16-19, 2006* (2006), 283–297.

[37] Roto, V., Law, E., Vermeeren, A. and Hoonhout, J. 2011. User Experience White Paper. *Result from Dagstuhl Seminar on Demarcating User Experience, September 15-18, 2010* (Feb. 2011), 12.

[38] Ryan, P.Y., Rønne, P.B. and Iovino, V. 2016. Selene: Voting with transparent verifiability and coercion-mitigation. *International Conference on Financial Cryptography and Data Security* (2016), 176–192.

[39] Schechter, S.E., Dhamija, R., Ozment, A. and Fischer, I. 2007. The Emperor's New Security Indicators. (May 2007), 51–65.

[40] Schrepp, D.M. 2018. User Experience Questionnaire Handbook. (2018), 15.

[41] Sheldon, K.M., Elliot, A.J., Kim, Y. and Kasser, T. 2001. What is satisfying about satisfying events? Testing 10 candidate psychological needs. *Journal of personality and social psychology*. 80, 2 (2001), 325.

[42] Smith, S.W. 2003. Humans in the loop: Human-computer interaction and security. *IEEE Security & Privacy Magazine*. 1, 3 (May 2003), 75–79. DOI:https://doi.org/10.1109/MSECP.2003.1203228.

[43] Sotirakopoulos, A., Hawkey, K. and Beznosov, K. 2011. On the challenges in usable security lab studies: lessons learned from replicating a study on SSL warnings. *Proceedings of the Seventh Symposium on Usable Privacy and Security* (2011), 3.

[44] Winckler, M., Bernhaupt, R., Palanque, P., Lundin, D., Leach, K., Ryan, P., Alberdi, E. and Strigini, L. 2009. Assessing the usability of open verifiable e-voting systems: a trial with the system Prêt à Voter. *Proceedings of ICE-GOV* (2009).

[45] Yee, K.-P. 2002. User interaction design for secure systems. *International Conference on Information and Communications Security* (2002), 278–290.

Chapter 5: Making Encryption Feel Secure: Investigating How Descriptions of Encryption Impact Perceived Security

Published as: V. Distler, C. Lallemand, & V. Koenig. (2020). Making Encryption Feel Secure: Investigating how Descriptions of Encryption Impact Perceived Security. 2020 *IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, 220–229. https://doi.org/10.1109/EuroSPW51379.2020.00037

5.1. Abstract

When communication about security to end users is ineffective, people frequently misinterpret the protection offered by a system. The discrepancy between the security users perceive a system to have and the actual system state can lead to potentially risky behaviors. It is thus crucial to understand how security perceptions are shaped by interface elements such as text-based descriptions of encryption. This article addresses the question of how encryption should be described to non-experts in a way that enhances perceived security. We tested the following within-subject variables in an online experiment (N=309): a) how to best word encryption, b) whether encryption should be described with a focus on the process or outcome, or both c) whether the objective of encryption should be mentioned, d) when mentioning the objective of encryption, how to best describe it, e) whether a hash should be displayed to the user. We also investigated the role of context (between subjects). The verbs “encrypt” and “secure” performed comparatively well at enhancing perceived security. Overall, participants stated that they felt more secure not knowing about the objective of encryption. When it is necessary to state the objective, positive wording of the objective of encryption worked best. We discuss implications and why using these results to design for perceived lack of security might be of interest as well. This leads us to discuss ethical concerns, and we give guidelines for the design of user interfaces where encryption should be communicated to end users.

5.2. Introduction

Effective communication about security is crucial to shape security perceptions purposefully and, ultimately, to reduce risky behaviors. Indeed, when interfaces communicate security states in a potentially misleading way, people may misinterpret the protection offered by a tool, which may hinder adoption [2]. Efforts to model

misalignment between a user's mental model and the system's security state [17, 24] show that lack of alignment can lead to “false sense of insecurity”, or on the contrary, a “false sense of security” [24]. While previous work shows that visible indicators of encryption, in their case a waiting screen displaying "encrypting your vote" and a hash, may have a positive impact on perceived security [12], it is currently unclear precisely *how* encryption should be communicated to people with the goal of triggering perceived security.

To address this objective, we conducted an online experiment with 5 within subjects variables: a) wording of encryption, b) process or outcome-focused description (or both), c) whether the objective of encryption should be mentioned, d) when mentioning the objective of encryption, how to best describe it, e) whether a hash should be displayed to the user. To understand whether the perceived security of these options depended on context, we used three contexts as a between subjects variable (online banking, e-voting, online pharmacy).

This paper makes the following contributions:

- We present a relative ranking of the perceived security of various text samples describing encryption to users.
- We provide suggestions to support the communication of encryption to users in a way that enhances perceived security.

5.3. Related work

Improving the user-friendliness of encryption has been important concern in the usable security and privacy community given that encryption approaches sometimes demand too much user effort and thus do not lead to adoption. More convenient encryption approaches are frequently seen as “good enough” for everyday use [4]. Interestingly, the adoption of secure messaging applications depends largely on social factors, rather than security and privacy concerns [8].

Going beyond improving the usability and UX of encryption tools, there is an ongoing debate in the usable security and privacy community on whether security mechanisms such as encryption should be visible to users. Consensus has not been reached so far, and the answer seems to be “it depends”. When users cannot see underlying security mechanisms, the advantage is that they do not need to understand what the security mechanisms entails. The resulting lack of knowledge can however lead to security-

relevant misunderstandings [3], and some authors have argued that security and privacy should be highly visible [13] and scrutable [21] in order to keep the human in the loop [23].

5.3.1. Consequences of invisible and ineffectively communicated encryption

Wu and Zappala [26] describe how the invisibility of encryption can lead people to make up their own, frequently inaccurate or outright wrong, mental models (or "folk models" [25]) of encryption. Such incorrect mental models and misaligned security perceptions can cause security problems when users need to interact with encryption, such as sending out unencrypted messages or emails mistakenly [22] or using less secure channels because encrypted messaging apps are not perceived as secure [16].

In addition to impacting mental models of encryption, lack of visible encryption can also influence trust and perceptions of the security of a tool. Ruoti and colleagues [22] tested prototypes of two versions of a private email system, one where technical details were hidden (e.g., key management and encryption), whereas the other version did show such information. The authors found that invisible security details (automatic key management, automatic encryption) led some users to mistakenly send out unencrypted messages, and some users doubted the trustworthiness of the email system. The authors then conducted user studies with an alternative prototype that used manual encryption. The users accepted extra steps of cutting and pasting ciphertext themselves and had more trust in the system. The authors suggest that more visible encryption may be a way to foster greater trust. Distler and colleagues [12] described similar results when comparing an e-voting application with visible encryption with a second version, where encryption was invisible. While the version with visible encryption performed worse in terms of pragmatic aspects of UX (i.e., usability), it seemed to qualitatively create a more favorable reaction for overall User Experience (UX) and perceived security.

Mental models of the security of messaging apps are often erroneous, as shown by Gerber et al. [16] who investigated how people perceive the security of end-to-end encryption for the messaging app WhatsApp in an interview study. They found that about half of the participants thought that even with E2E encryption, messages were still available in plain text to third parties. This perception that messages could be eavesdropped led to a lack of trust towards WhatsApp. The authors suggest implementing a user interface that makes E2E encryption processes more graspable for the user and increases transparency about

the business model and the encryption protocol, which is not publicly available yet. The creation of metaphors with the objective of improving user understanding of encryption also seems to be a promising direction for future research, however, Demjaha et al., [10] showed that using metaphors can sometimes do more harm than good, and the authors underline the difficulties of explaining encryption to users.

Similar problems are pointed out by Abu-Salma and colleagues [1] who analyzed the user interface of the secure messaging app Telegram. The interface design showed various issues, including the use of inconsistent terminology and not making all security features clear to the user. A later study showed that users lacked both trust in and awareness of encryption in secure messaging tools, even though the tool explitely informed them that encrpytion was used [9].

Communication with end users in the context of connection security seems to be similarly challenging as shown in a qualitative study on end user and administrator mental models of HTTPS. Users often confuse encryption with authentication and tend to underestimate the security benefits of HTTPS. When comparing the mental models of encryption of end users to administrators, end users have a more conceptual understanding, whereas administrators' understanding is more protocol-based [18].

5.3.2. How to communicate security concepts and encryption

How security concepts such as encryption should be communicated to users remains an ongoing debate. Bultel and colleagues [6] proposed various ways of teaching security concepts including various encryption modes to children or non-expert adults in an understandable manner. However, in many contexts, it is not always realistic to include full explanations of the details of encryption protocols to users who want to achieve their primary goal, unrelated to encryption. Efforts to communicate encryption in a concise manner has been made in the context of browser security indicators which communicate that data is sent through an encrypted communication protocol. Felt and colleagues found that the strings “secure” and “https” performed best at conveying security to users, accompanied by a green lock [14]. The level of detail that should be communicated to users can be difficult to define. In the warning literature [19], studies have shown that explicit (full and precise) information creates a greater perception of risk, better comprehension of the safety issues and people remember more explicit warnings [19].

Overall, it seems that visible instances of encryption may be beneficial for perceived security [12, 22] and that interface design has an important impact on people's perceived security of encryption [16]. In particular, text describing encryption-related processes often lacks consistency [1] and should be made more graspable to users for better perceived security [16].

5.4. Research objectives

The objective of this study is to better understand how to describe encryption in a way that gives a feeling of perceived security to users. Given that user understanding and perceived security do not necessarily coincide, we wanted to disentangle the goals of optimizing for user understanding and perceived security. Our objective was thus not to improve user understanding of encryption, rather, we aimed at investigating the impact of various ways of wording encryption in user interfaces on perceived security. We address the following research question: How should we describe encryption to users to create perceived security through user interfaces?

5.5 Methodology

We conducted a mixed design online experiment, including both an in-between subjects variable (text samples) and a between subjects variable (context). All experimental variables are described in 5.5.2. Material, details on participants can be found in 5.5.3. Participants.

5.5.1. Procedure

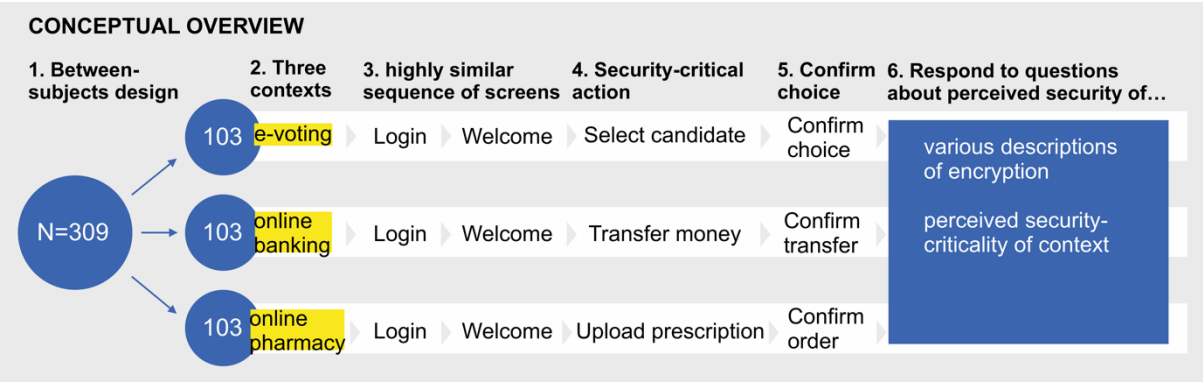


Figure 1: Overview of the study design (a separate subset of this dataset, addressing another research question, has been separately analyzed by [11])

An overview of the study design is presented in Figure 1. Participants viewed various screens simulating the use of a smartphone app. In each of these contexts, we focused on the moment where the user has to send critical data (vote, money transfer, medical prescription). At this security-critical moment (shown in more detail in the appendix), participants had to confirm whether the information was correct. Finally, they were presented with various text samples (described in "Material") which they rated on a Likert scale of perceived security from 1 (not secure at all) to 10 (very secure). An example of how the question was presented to participants is shown in Figure 2, the full questionnaire is provided as supplementary material. We then asked participants how security-critical their experimental use context was in their opinion on a scale from 1 (not security-critical) to 10 (very security-critical).

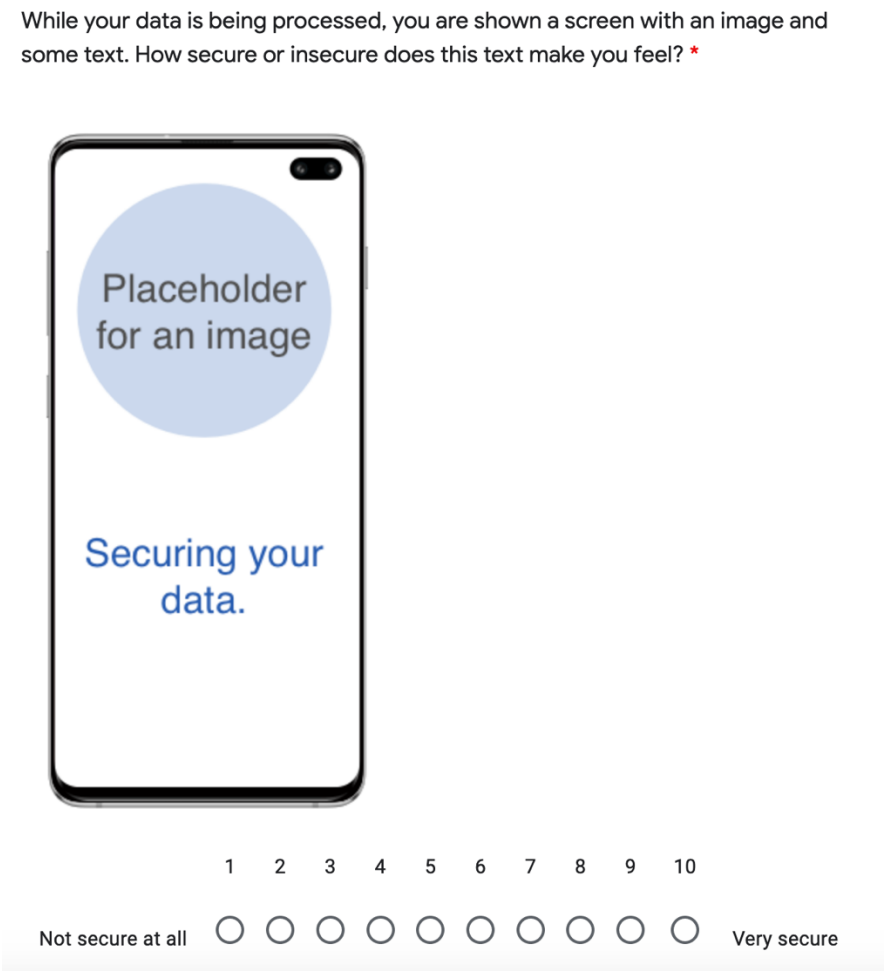


Figure 2: Sample question as presented to participants.

Question order and answer options were randomized. This paper focuses on the part of the questionnaire that addresses the perceived security of various ways of describing encryption. A separate subset of this dataset, addressing another research question

concerning the perceived security of a selection of icons, has been separately analyzed by [11]. The subset of data analyzed in the present article includes only questions regarding the textual description of encryption, which were asked after the questions concerning the perceived security of icons. Given that all participants were exposed to the same icons (in random order) before answering to the questions about the perceived security of textual descriptions of encryption, we have ensured that any potential bias relating to previously answering questions about the icons was the same across all participants.

5.5.2. Material

5.5.2.1. Text samples (Within subjects)

We investigated the best wording to communicate encryption for perceived security. The objective was to keep the text samples short and concise, aiming to foster perceived security rather than technical understanding. We conducted a literature review to inform the selection of the text samples used in our experiment. The text samples were additionally reviewed by a group of seven usable security and UX experts, and subsequently pre-tested and refined with the target population in qualitative pre-tests (N = 15).

In summary, we tested 5 aspects related to possible descriptions of encryption, as shown in Table 1:

	Variable	Options
a)	Wording of encryption	3 text samples
b)	Focus on process or outcome of encryption	3 options (Table 2)
c)	How to describe the objective of encryption	3 text samples
d)	Display or omit objective of encryption	Display or omit
e)	Hash	Display or omit

Table 1: Summary of the variables and answer options, details in the text

a) Wording of encryption

First, we studied how to word encryption in a way that conveys security. We used the following answer options (screens in Figure 3):

- securing your data (or vote/transaction)

- encrypting your data (or vote/transaction)
- translating your data (or vote/transaction) to secret code

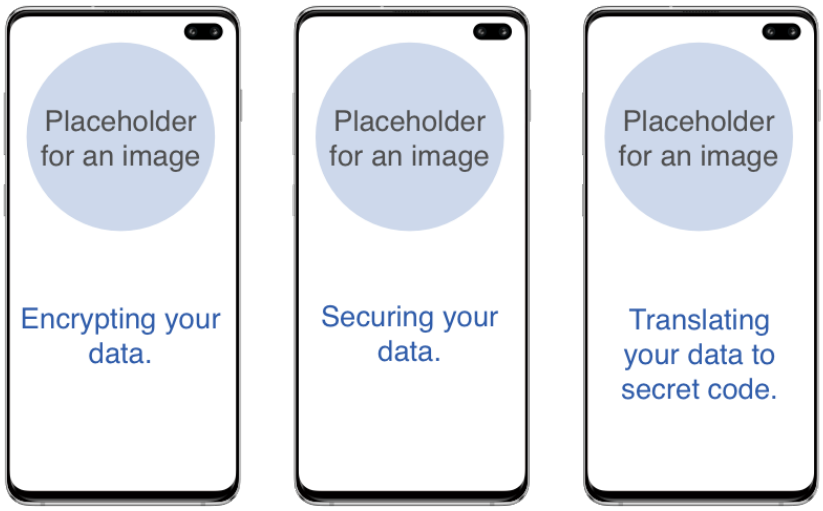


Figure 3: Participants rated the perceived security of each text sample on a scale from 1 (not secure at all) to 10 (very secure).

The verbs "encrypt" and "secure" were based on previous research [14], where they evoked perceived security.

b) Focus on process or outcome of encryption

As displayed in Table 2, participants selected whether (1) process-oriented wording, (2) results-oriented wording, or (3) a combination of both made them feel more secure.

(1)	(2)	(3)
Encrypting your data.	Your data is encrypted	Encrypting your data → Your data is now encrypted.

Table 2: Does process-oriented wording (1), results-oriented wording or (3) a combination of both make people feel more secure?

c) How to describe the objective of encryption

We were interested in the impact of explicitness [19] on perceived security and wanted to understand if the objective of encryption should be mentioned to the user when designing for perceived security. Explicit information, in this context, can be defined as full and precise information [19].

For cases where describing the objective of encryption was necessary, we wanted to understand how to describe encryption in a way that enhances perceived security. We

strived to keep these explanations short and concise, as recommended in the warning literature [19] so that users would realistically be able to read them in a smartphone app. We avoided technical jargon, which is usually not a good way to achieve explicitness for a general target audience [19].

The three versions we tested were:

Your vote is now encrypted / secure / translated to secret code...

- ... to mask your data from being viewed and read.
- ...to protect it during transit.
- ...so that only authorized parties can read it.

d) Display or omit objective of encryption

After finding out which option felt most secure in the previous question, the next question addressed whether perceived security was higher when participants were presented with the goal of encryption or when this information was omitted. The participants chose whether overall, they preferred being presented the objective of encryption, or not.

e) Display or omit hash

In addition to the previously mentioned wordings regarding encryption, we also wanted to know whether participants felt more secure when a hash was displayed or whether the opposite was the case. We thus asked them to choose the screen they felt was more secure between one with a hash and one without a hash (see Figure 4).

Figure 4: Participants had to choose whether they felt more secure when seeing a hash or without this information.

5.5.2.2. Context (Between subjects)

Within our experimental design, each participant was randomly assigned to one of three use contexts. In all contexts, participants were placed in a realistic scenario in which they had to take a context-dependent, security-critical action. These scenarios were (1) voting for the next national elections online (2) transferring money on a banking app (3) ordering medication through the app of an online pharmacy. All three contexts used a very similar sequence of screens so that the context was the only major factor that varied between use contexts (see Appendix, Table 7). We purposefully kept the color scheme and visual design consistent and neutral across use contexts. We did not use any official-looking logos to ensure the logo did not act as a confounding factor.

5.5.3. Participants

309 participants took part in our study. The average age was 34.8 years (Min = 18, Max = 76, SD = 12.6). Participants were sampled through the crowdsourcing platform Prolific. Peer and colleagues [20] found that Prolific participants produced data quality that was comparable to MTurk's and tends to include more diverse samples. We recruited 309 adult UK citizens who were randomly split into three experimental groups of 103 participants. Each experimental group was assigned to a different security-critical context (see "Procedure").

5.5.3.1. Pre-tests

We conducted 3 pre-tests with 5 participants each. In these pre-tests, we asked Prolific participants to comment on the difficulty and understandability of the questionnaire, what they liked and disliked about the questionnaire. We also gathered feedback on the adequacy of the compensation, and asked them to give feedback to improve the questionnaire. This also allowed us to refine the smartphone screens shown to the participants. We excluded anyone who had participated in pre-tests, and no participant could partake in more than one group.

5.5.3.2. Ethics

The study has received prior approval by our university's ethics committee. Participants gave informed consent. We did not use deception. The compensation of this study (GBP 2.20 / ca. USD 2.90 for 15 minutes) equals GBP 8.80 / ca. USD 11.60 per hour, thus exceeding Prolific's minimum compensation of GBP 6.50 / ca. USD 8.50.

5.5.4. Data analysis

For qualitative analyses, the first author used inductive coding to create the codebook in consultation with the other authors. We did not exclude any data points given that responses were of satisfactory quality, all datasets were complete, and all qualitative answers were valid. We used an alpha level of .05 for all statistical tests. While we can conclude from the normality tests of the residuals that they don't follow a normal distribution, visually verifying the distributions of the residuals on a histogram shows that they are quite symmetrical and the analysis of variance is known to be a robust method in that case. We provide the ANOVA tables[2].

5.6. Results

5.6.1. Security-criticality

There was a significant effect of context on criticality $F(2,306) = 4.25$, $p = .015$. Online banking was perceived as significantly more security-critical than the online pharmacy ($p = .012$) (see Table 3). No significant difference with voting could be observed ($p = .149$). No significant difference between voting and the online pharmacy could be observed ($p = .575$).

Context	Mean	SD	Min	Max
e-voting	8.88	1.62	4	10
Online Banking	9.28	1.13	4	10
Online Pharmacy	8.67	1.76	1	10
Total	*8.94*	*1.54*	*1*	*10*

Table 3: Criticality of contexts (1 = not security critical, 10 = very security-critical, N = 103 per context)

[2] Link to ANOVA tables

5.6.2. Wording of encryption, focus on process or outcome of encryption (a) and b))

In summary, the verbs encrypt and secure were perceived as significantly more secure (Table 4) than "translating to secret code" (described in more detail hereafter).

Process-focussed wording We conducted a univariate analysis of variance to understand whether there was an effect of the textual indicator on perceived security and whether there was an effect of the experimental group (e-voting, online banking, online pharmacy). There was no significant effect of context on perceived security at the $p < .05$ level, $F(2,918) = .76$, $p = .469$. The version of the text however had a significant effect $F(2,918) = 100.6$, $p < .001$. An interaction between context and version of text could not be demonstrated, $F(4,918) = 1.48$, $p = .208$.

Result-focussed wording There was a significant effect of context on perceived security, $F(2,918) = 3.24$, $p = .040$. The version of the text also had a significant effect, $F(2,918) = 158.00$, $p < .001$. An interaction between context and version of text could not be demonstrated, $F(4,918) = .66$, $p = .620$. Post-hoc tests showed that the perceived security was significantly higher in the pharmacy use case compared to the banking use case ($p = .033$). Post-hoc tests showed that for both process-focussed and result-focussed wording, the verbs "encrypt" and "secure" significantly outperformed "translating to secret code" ($p < .001$, Tukey HSD). In both cases, no significant difference between "encrypt" and "secure" was observed ($p = .985$ process-focussed, $p = .240$ results-focussed).

Process-oriented wording, results-oriented wording, or a combination of both (b) For 63% of participants, seeing information on the process, followed by information on the result was perceived as more secure than seeing either option in isolation (26% found result-focussed wording more secure, 11% found process-focussed wording more secure). There was no significant difference between the contexts ($\chi 2$ (2, $N = 309$) = 8.33, $p = 0.080$).

Verb used	Process-focused or results-focused	Text communicating encryption	Mean	SD
Encrypt	Process-focused	"Encrypting your transaction."	6.61	2.198
	Result-focused	"Your transaction is now encrypted."	7.19	2.198
Secure	Process-focused	"Securing your transaction."	6.56	2.010
	Result-focused	"Your transaction is now secure."	7.40	2.114
Translate to secret code	Process-focused	"Translating your transaction to secret code."	4.44	2.289
	Result-focused	"Your transaction is now translated to secret code."	4.42	2.555
Total	*Process-focused*		*5.87*	*2.390*

	Result-focused		*6.31*	*2.657*

Table 4: Descriptive statistics of perceived security of textual indicators. 10 equals highest possible perceived security, 1 lowest perceived security.

5.6.3. How to describe the outcome of encryption for perceived security (c)

There was no significant effect of context on perceived security, $F(2,918) = .24$, $p = .786$. The version of the text had a significant effect, however: $F(2,918) = 17.69$, $p < .001$. An interaction between context and version of text could not be demonstrated $F(4, 918) = .87$, $p = .482$. Post-hoc Tukey HSD tests showed that the wording "...so that only authorized parties can read it" ($M = 6.65$, $SD = 2.41$) significantly outperformed "...to mask your data from being viewed and read." ($p < .001$) and "to protect it during transit." ($p < .001$) (see Table 5). The latter two versions did not differ significantly with regard to their perceived security ($p = .120$).

Text Version	Mean	SD
Your transaction is now [...] so that only authorized parties can read it	6.65	2.42
Your transaction is now [...] to mask your data from being viewed and read.	5.90	2.39
Your transaction is now [...] to protect it during transit.	5.52	2.35
	6.02	*2.43*

Table 5: Perceived security of three text versions communicating the result of encryption (10 equals highest possible perceived security, 1 lowest perceived security).

5.6.4. Display or omit objective of encryption (d)

Overall, 63% of participants felt more secure not knowing about the goal of encryption. In the context of voting, more participants preferred knowing about the goal of encryption (45% compared to 37%), but the difference was non-significant ($\chi 2(2, N = 309) = 4.55$, $p = .110$).

5.6.5. Display or omit hash (e)

A majority of participants (72%) felt more secure notseeing the hash. There were no significant differences between the contexts ($\chi 2(2, N = 309) = .22$, $p = 0.895$).

5.6.6. Why People want to know or prefer not to know about the goal of encryption

As shown in Table 6, analysis of qualitative answers showed that those who **preferred not being told** about about the goal of encryption stated that on the one hand, they preferred straight-to-the-point information (see Table 6) and on the other hand, it made them worry about security problems they had not previously thought about.

Participants who perceived the **display of the goal of encryption as more secure** did so because they felt better informed about the process and they thought that it sounded more professional.

Displaying the goal of encryption…	Responses	Representative Verbatims
Is unnecessary, keep itsimple	36%	"I only need to know my data is secure at all times, not the reason why." (P72) "Simple to read, gets the point across, no useless information." (P301)
Makes me feel better informed	22%	"Because it makes it clearer what is being encrypted and why." (P182) "I would like to be told whether or not my data will be protected and know what/who would be able tosee my data." (P79) "Because it's not just random terminology that doesn't mean anything. It explains why these processesare happening to your data which makes me feel as though security is paramount in the process." (P239)
Makes me worry	18%	"I really don't know. It's weird. You'd think the more transparency the better, but actually, I'd rather just do the whole "ignorance is bliss" thing and just not think about the risks involved in sharing my data showing the reason for encryption provides an extra layer of worry that I was never worried about untilit was mentioned." (P82)
Sounds safer and moreprofessional	13%	"I feel secure cause the info tells me my data is being protected." (P143)

Table 6: Why participants felt more secure seeing / not seeing the goal of encryption. Percentages do not add up to 100% because only frequent codes are listed.

5.6.7. Summary of Results

a) Wording of encryption: The verbs "encrypt" and "secure" outperformed "translating to secret code".

b) Focus on process or outcome of encryption: Most participants preferred seeing information on the process of encryption, followed by information on the result.

c) How to describe the objective of encryption: Participants thought that, "...so that only authorized parties can read it" felt most secure as an objective of encryption.

d) Display or omit objective of encryption: 63% of participants felt more secure when they were not told about the objective of encryption.

e) Display or omit hash: 72% felt more secure when not seeing the hash.

5.7. Discussion

5.7.1. How to Describe Encryption to Users to Evoke Perceived Security

5.7.1.1. Wording

This study addresses the question of how to describe encryption in a way that triggers perceived security. Both "encrypting your transaction" and "securing your transaction" were perceived as significantly more secure than "translating your transaction to secret code." Indeed, the use of slightly technical vocabulary (encrypting, securing) felt reassuring and professional for participants. Previous research in the context of HTTPS indicators also found that "secure" yielded a high number of participants who felt at least somewhat safe, and the lowest number who felt not safe at all [14]. Future studies could address even more variations of wordings, such as more "extreme" statements (e.g., "highly secure"), however such descriptions might have a negative effect on the perceived security of expert users, who might thus want more information on the actual security of the system. Another relevant question for future work concerns the applicability of these results going beyond graphical interfaces, such as reassuring descriptions of encryption for voice interactions.

5.7.1.2. Level of detail

In our study, user perception was different when they were presented with details on the objective of encryption. Participants felt that mentioning the transfer of data, as well as mentioning the possibility of their data being viewed and read, made them worry about security more than they would have without this information. This aligns with results from the warning literature, which found that a higher level of "explicit" (full and precise) information leads to greater perception of risk or hazard [19]. While creating a greater perception of risk is intended for effective warnings, a designer's intention when communicating encryption might be the opposite, aiming to reassure users. In this case,

one option might thus be to opt for a lower level of explicitness, which has the downside of potentially not informing the user sufficiently. Indeed, 63% of participants stated that they felt more secure not knowing about the objective of encryption. While this is the majority, it is worth mentioning that the remaining 37% felt reassured and kept in the loop when seeing the objective of encryption. Future studies might address whether this concerns a particular population group (e.g., more tech savvy users), or whether in certain contexts users might be more interested in receiving more detailed information on the security process.

5.7.1.3. Phrasing the objective of encryption

Rather than completely omitting any explicit information on the objective of encryption, designers might also choose to inform users, but ideally word the advantages of encryption in a positive, rather than directly threat-related way when designing for perceived security. Compared to "[...] to mask your data from being viewed and read." and "Your transaction is now [...] to protect it during transit.", "Your transaction is now [...] so that only authorized parties can read it" was perceived as significantly more secure than information relating to "data being viewed and read" or "to protect it during transit". We hypothesize that this is due to the fact that the information focuses on the positive result of encryption, rather than potential threats during data transmission. This is coherent with previous research emphasizing that displays of security mechanisms should be meaningful for users and aligned with their goals [12], which was not the case for the majority (63%) of our users who felt more secure not seeing the goal of encryption.

5.7.2. Use of results to design for a lack of perceived security

While the first reaction to these results may be to discard any text samples that did not create a feeling of perceived security, there is value in understanding which descriptions of encryption evoke a negative reaction, a lack of perceived security. For instance, mentioning data transmission and the possibility of data being viewed and read created a sense of worry for our participants. Previous work has shown that users sometimes show a false sense of security, when it is not warranted by a secure system state [24]. Understanding the interface elements that give people a sense of perceived insecurity may allow us to design interactions that lower their perceived security in order to avoid a false sense of security that may lead to risky behaviors.

Experience design can thus be used to purposefully design moments of doubt and reflection when it is in the interest of the user, but further research is needed to understand the nuances of such design interventions and how to best apply them. In addition, ethical implications of such design approaches need to be considered.

5.7.3. Ethical implications and potential for misuse

When using experience design to either design for or against perceived security, malicious actors can use these insights to purposefully create a sense of security for unsafe websites. While we cannot prevent such misuse, we believe that a deeper understanding of how interface elements influence security perceptions is also valuable for benevolent actors. In particular, any design will impact user perceptions of the security of an interface, be it intentional or unintentional.

Nevertheless, we believe that a further discussion of how experiential design aiming to change security perceptions can be considered a subtle persuasive design technique [15] and should adhere to according ethical guidelines [5], similar to reflections in the field of warnings [7] would be of value to the community.

5.7.4. Limitations

This study has some limitations. We used a simulation of a smartphone application, rather than asking participants to download an application on their phone. This trade-off was carefully weighed in advance and allowed us to control the participants' exploration process of the app and to ensure that participants unwilling to download apps on their phones could still participate in the study. Participants also did not put any real personal information at risk, which allowed us to avoid any potential harm to the participants, but it might also have increased their perceived security. Lastly, we cannot be sure whether all participants knew the name of the medication used in the pharmacy context (a medication used to treat depression), which may have impacted their perception of the criticality.

One might argue that some of the text samples were more familiar to participants than others, such as “securing” data. The word encryption, on the other hand, is a well-established term in security research and one might thus assume that it results in higher perceived security for participants than more novel options (e.g., “translating to secret

code"). While these are valid assumptions, no empirical evidence exists thus far, and it is compelling to deliver results to substantiate these intuitions.

We chose to use a simple ANOVA instead of a mixed model for repeated measures for reasons of parsimony. Given that all our significant results are highly significant, the tests can be considered powerful enough. We also conducted a mixed model analysis, which we provide [3].

5.7.5. Recommendations for the design of indicators for perceived security

Based on these results, we suggest the following recommendations for researchers and designers who have the objective of communicating encryption to users in way that enhances perceived security:

- When describing encryption with the intention to improve perceived security on an interface, text should be short and overly technical elements avoided for perceived security.
- When informing users of the result of encryption with the intent to improve perceived security, designers should be careful to avoid a strong focus on data transmission or third parties accessing data. Instead, the positive result of encryption seems to evoke a more positive response.
- Designers may choose to mention the threats a security measure protects users against with the purpose of creating moments of doubt and reflection when it is in the interest of the user. In this case, ethical concerns should be considered and misinforming the user must be avoided.

5.8. Conclusion

This study addresses the timely question of how to describe encryption to users in a way that maximizes perceived security. It gives insights into the perceived security various textual samples evoke, demonstrating that text should be short and slightly technical for perceived security. While users overall did not feel more secure when knowing about the objective of encryption, framing the result of encryption in a positive way seems promising. We also discuss why using these results to design for perceived lack of security

[3] Link to mixed model analysis

might be useful. We discuss ethical implications, and provide guidelines for describing encryption. We expect the results of this work to contribute to the design of secure systems by making a step towards more reassuring descriptions of encryption, and at a larger level, security systems that keep users in the loop in an experience-centered way.

5.9. Acknowledgements

We thank our shepherd Dr. Katharina Krombholz and the anonymous reviewers. We acknowledge support from the National Research Fund (FNR) under grant number PRIDE15/10621687. We also thank Etienne Le Bihan for his feedback.

5.10. References

[1] Ruba Abu-Salma, Kat Krol, Simon Parkin, Victoria Koh, Kevin Kwan, Jazib Mahboob, Zahra Traboulsi, and M. Angela Sasse. The security blanket of the chat world: An analytic evaluation and a user study of telegram. In *Proceedings 2nd European Workshop on Usable Security.* Internet Society.

[2] Ruba Abu-Salma, M. Angela Sasse, Joseph Bonneau, Anastasia Danilova, Alena Naiakshina, and Matthew Smith. Obstacles to the adoption of secure communication tools. In *2017 IEEE Symposium on Security and Privacy (SP),* pages 137–153. IEEE.

[3] Anne Adams and Martina Angela Sasse. Users are not the enemy. *Commun. ACM,* 42(12):40–46, December 1999.

[4] Wei Bai, Moses Namara, Yichen Qian, Patrick Gage Kelley, Michelle L. Mazurek, and Doowon Kim. An inconvenient trust: User attitudes toward security and usability tradeoffs for key- directory encryption systems. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016),* pages 113–130. USENIX Association.

[5] Daniel Berdichevsky and Erik Neuenschwander. 1999. Toward an ethics of persuasive technology. *Commun. ACM* 42, 5 (May 1999), 51–58. DOI:https://doi-org.proxy.bnl.lu/10.1145/301353.301410

[6] Bultel, Xavier, et al. "How to explain modern security concepts to your children." *Cryptologia* 41.5 (2017): 422-447, 2017.

[7] Kenzie A Cameron and David M DeJoy. The persuasive functions of warnings: Theory and models. In Michael S Wogalter, editor, *Handbook of Warnings*, pages 301–312. CRC Press.

[8] Alexander De Luca, Sauvik Das, Martin Ortlieb, Iulia Ion, and Ben Laurie. 2016. Expert and non-expert attitudes towards (secure) instant messaging. In *Proceedings of the Twelfth USENIX Conference on Usable Privacy and Security (SOUPS '16).* USENIX Association, USA, 147–157.

[9] Sergej Dechand, Alena Naiakshina, Anastasia Danilova, and Matthew Smith. In Encryption We Don't Trust: The Effect of End-to-End Encryption to the Masses on User Perception. In *2019 IEEE European Symposium on Security and Privacy (EuroS&P),* pages 401–415, Stockholm, Sweden, June 2019. IEEE.

[10] Albese Demjaha, Jonathan Spring, Ingolf Becker, Simon Parkin, and Angela Sasse. Metaphors considered harmful? An exploratory study of the effectiveness of functional metaphors for end-to-end encryption. In *Proceedings 2018 Workshop on Usable Security,* San Diego, CA, 2018. Internet Society.

[11] Verena Distler, Carine Lallemand, and Vincent Koenig. The power of visual indicators perceived security and interpretation of icons. under submission.

[12] Verena Distler, Marie-Laure Zollinger, Carine Lallemand, Peter B. Roenne, Peter Y. A. Ryan, and Vincent Koenig. Security - visible, yet unseen? In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems, CHI '19*, pages 605:1–605:13, New York, NY, USA, 2019. ACM.

[13] Paul Dourish, E. Grinter, Jessica Delgado de la Flor, and Melissa Joseph. Security in the wild: User strategies for managing security as an everyday, practical problem. *Personal Ubiquitous Comput.*, 8(6):391–401, November 2004.

[14] Adrienne Porter Felt, Robert W. Reeder, Alex Ainslie, Helen Harris, Max Walker, Christopher Thompson, Mustafa Embre Acer, Elisabeth Morant, and Sunny Consolvo. Rethinking connection security indicators. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*, pages 1–14. USENIX Association.

[15] Bj Fogg. Persuasive computers: perspectives and research directions. In *Proceedings of the SIGCHI conference on Human factors in computing systems - CHI '98,* pages 225–232. ACM Press.

[16] Nina Gerber, Verena Zimmermann, Birgit Henhapl, Sinem Emeröz, and Melanie Volkamer. Finally johnny can encrypt: But does this make him feel more secure? In *Proceedings of the 13th International Conference on Availability, Reliability and Security*

- *ARES 2018,* pages 1–10. ACM Press.

[17] Adam Michael Houser. Mental models for cybersecurity: A formal methods approach.

[18] Katharina Krombholz, Karoline Busse, Katharina Pfeffer, Matthew Smith, and Emanuel von Zezschwitz. " if https were secure, i wouldn't need 2fa"-end user and administrator mental models of https. In *2019 IEEE Symposium on Security and Privacy (SP),* pages 246–263. IEEE, 2019.

[19] Kenneth Laughery R and Smith Danielle Paige. Explicit information in warnings. In M Wogalter, editor, *Handbook of Warnings*, pages 605–615. CRC Press.

[20] Eyal Peer, Laura Brandimarte, Sonam Samat, and Alessandro Acquisti. Beyond the turk: Alternative platforms for crowdsourcing behavioral research. *Journal of Experimental Social Psychology,* 70:153–163, 2017.

[21] Rader, E. and Slaker, J. 2017. The importance of visibility for folk theories of sensor data. *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)* (2017), 257–270.

[22] Scott Ruoti, Nathan Kim, Ben Burgon, Timothy van der Horst, and Kent Seamons. Confused johnny: when automatic encryption leads to confusion and mistakes. In *Proceedings of the Ninth Symposium on Usable Privacy and Security - SOUPS '13*, page 1. ACM Press.

[23] S.W. Smith. "Humans in the loop: Human-computer interaction and security." *IEEE Security & privacy* 1.3 (2003): 75-79.

[24] Borce Stojkovski, Itzel Vazquez Sandoval, and Gabriele Lenzini. Detecting misalignments between system security and user perceptions: a preliminary socio-technical analysis of an e2e email encryption system. In *2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, pages 172–181. IEEE, 2019.

[25] Rick Wash. Folk models of home computer security. In *Proceedings of the Sixth Symposium on Usable Privacy and Security - SOUPS '10,* page 1. ACM Press.

[26] Justin Wu and Daniel Zappala. When is a tree really a truck? exploring mental models of encryption. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018),* pages 395–409, Baltimore, MD, August 2018. USENIX Association.

5.11. Appendices

5.11.1. Link to full questionnaires

Onling banking questionnaire

e-voting full questionnaire

Online pharmacy full questionnaire

5.11.2. Security-critical action depending on context

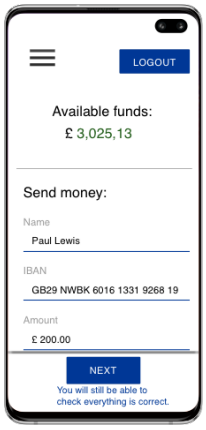
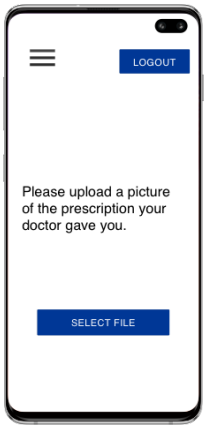
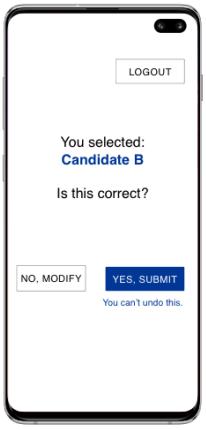
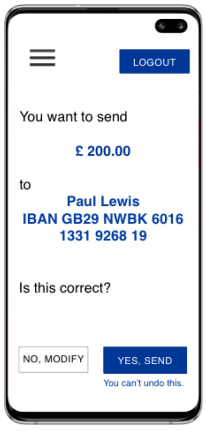
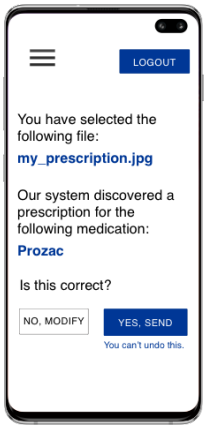
<table>
<tr><td colspan="3">Step 4: Security-critical action</td></tr>
<tr><td>e-voting</td><td>Online banking</td><td>Online pharmacy</td></tr>
<tr><td> 
</td><td> 
</td><td> 
</td></tr>
<tr><td colspan="3">Step 5: Confirm choice</td></tr>
<tr><td> 
</td><td> 
</td><td> 
</td></tr>
</table>

Table 7: Detailed view of step 4 and 5 in Figure 1: Depending on context, the security-critical action varied. The table shows the respective security-critical action for each context. (a separate part on another topic of the questionnaire was analyzed by [11])

Chapter 6: Complex, but in a good way? How to Represent Encryption to Non-Experts Through Text and Visuals – Evidence from Expert Co-Creation and a Vignette Experiment

Under review.

Co-authors: Verena Distler, Tamara Gutfleisch, Carine Lallemand, Gabriele Lenzini, Vincent Koenig.

6.1. Abstract

An ongoing discussion in the field of usable privacy and security debates whether security mechanisms should be visible to end-users during interactions with technology, or hidden away. This paper addresses this question using a mixed-methods approach, focussing on encryption as a mechanism for confidentiality during data transmission on a smartphone application. In study 1, we conducted a qualitative co-creation study with security and Human-Computer Interaction (HCI) experts (N = 9) to create appropriate textual and visual representations of the security mechanism encryption in data transmission. We investigated this question in two contexts: online banking and e-voting. In study 2, we put these ideas to the test by presenting these visual and textual representations to non-expert users in an online vignette experiment (N=2180). We found a statistically significant and positive effect of the textual representation of encryption on perceived security and understanding, but not on user experience (UX). More complex text describing encryption resulted in higher perceived security and more accurate understanding. The visual representation of encryption had no statistically significant effect on perceived security, UX or understanding. Our study contributes to the larger discussion regarding visible instances of security and their impact on user perceptions.

6.2. Introduction

Streamlining people's interactions with technology might help improve usability but can led to some unintended secondary effects in the context of security and privacy. In the quest to make interactions more "user-friendly", security mechanisms have often been hidden away from users under the rationale that they can introduce barriers to action, while Human-Computer Interaction (HCI) designers attempt to remove such barriers (Dourish

et al., 2004). Accordingly, automated approaches of security that remove security decisions from the user's hands have emerged (Edwards et al., 2008).

But when users do not need to interact with security, they likely also do not need to understand security processes. This lack of understanding can lead to security issues (Adams & Sasse, 1999). Authors thus reasoned that security technologies should be highly visible and available for inspection (Adams & Sasse, 1999), with some explaining that only by making security-related actions and their consequences more visible, users are able to form accurate mental models about the security of an interaction (Spero & Biddle, 2020). Some authors also argued that security can even act as an enabling factor and a significant part of positive user experience (Pagter & Petersen, 2007).

To investigate these questions, in the present paper we focus on the security mechanism encryption, applied to provide confidentiality during data transmission on a smartphone application. To understand user perceptions, we investigate three concepts. First, we are interested in perceived security, which we define as how secure or insecure an experience felt to the research participant (see section 6.6.1.1.). Second, we research user experience, which we define and discuss in section 6.3.3., and measure using the UEQ-S measurement (Schrepp et al., 2017). Third, we investigate the understanding of the security mechanism encryption based on a set of exploratory questions designed by security experts for non-expert users (described in section 6.6.1.1.). In the following, we will frequently refer to "understanding" as a shorter form of "understanding of the security mechanism encryption" for better readability.

This paper is organized as follows. In section 6.3., we introduce the background for our research, including research on visual representations of security mechanisms, use contexts of our research, and work on measuring subjective experiences. In section 6.4., we explain the research objectives. We then describe the iterative co-creation of representations of encryption with experts in section 6.5. (study 1), and the vignette experiment with non-experts in section 6.6. (study 2). Section 6.7. discusses the results of our work, before concluding in section 6.8.

6.3. Background

The question of how to represent security mechanisms visually remains a challenge. In the following, we use the term "visible instances of security" to describe any visible

representation of a security mechanism to the user of a technology. A visible instance of security can encompass both visual and textual indicators (e.g., an image with some text).

Icons have long been used in graphical user interfaces to convey information (Blattner et al., 1989) and have the potential of being universally understood, even though sometimes, a range of different meanings can be attributed to a single icon (Rogers, 1989). As early as in 1999, Wiedenbeck (1999) evaluated the learnability of an application using buttons with text labels, icons, or a combination of both, measuring both the success of novice users learning how to use the application and measuring users' attitudes toward the application. Performance was best when using text labels only, or when combining icons with text labels; performance using the icon-only interface was much poorer. Ease of use was perceived as better for the icon-label interface, and perceived usefulness was higher for the icon-only and icon-label interfaces. This study seems to show that a combination of textual and visual representation may be most suited to convey information.

In the following, we will describe some of the research on visual representations of security mechanisms, and how they relate to user perceptions.

6.3.1. Research on visual representations of security mechanisms and perceptions

One instance of encryption protocols that should be familiar to many is HTTPS. It is used for implementing confidential communications towards interlocutors whose identity is certified as trusted[4]. Various studies explored how to visualize the presence of an HTTPS connection (resp. the lack thereof) to inform users whether they are transmitting sensitive data e.g., credit card numbers securely (resp. or insecurely) or to someone trusted (resp. or untrusted)[5].

Schechter et al. (2007) evaluated different connection security indicators and warnings, finding that participants failed to recognize the absence of a HTTPS indicator. Even when a warning page was displayed, suggesting that it may be unwise to visit a untrusted website whose certificate is invalid or expired, potentially suggesting that the website is not what it claims to be or that its identity was certified a long time ago and might have changed, many participants still took the risky action of visiting the website. The authors confirm

[4] HTTPS also has the goal of authenticating the identity of the server for the reason that "secure" messages should be confidential but also sent to the intended recipient and not, despite confidentially, to an imposter.

[5] The potential issues are (1) their data will be sent in clear and can be read if the protocol is HTTP, or, (2) if the protocol is HTTPS, will be sent encrypted but to a recipient who may be who it claims to be (e.g., Amazon), but the certificate is invalid, or the recipient is not who it claims to be.

prior findings that users seem to ignore HTTPS indicators and warnings. Felt and colleagues (2015) later designed visual indicators for the presence / absence of HTTPS secure connections, with the goal of improving understanding of these indicators, as well as adherence to the secure behavior, which they defined as not visiting the untrusted website. The authors were not able to improve understanding of the security warning, but improved adherence through opinionated design. Later, Felt et al. (2016) also designed new indicators for the presence / absence of HTTPS secure connections for browsers, and evaluated their effects on users. The authors indicate HTTPS in green with a padlock and the text "secure", HTTP in grey with a circle icon (resembling an "information" symbol) and the text "not secure", and invalid HTTPS in red with a triangle with an exclamation mark, and the text "not secure". The selection was implemented by Google Chrome. In a 2021 blog post, Chrome researchers highlighted previous research showing that the lock icon was often associated with a website being trustworthy, when really only the connection is secure (Panditrao et al., 2021). Due to this misalignment between people's interpretation of the icon and the actual security property it intended to indicate, the researchers planned to run experiments with removing or replacing the lock icon. The results are not publicly available at present.

Similar situations as with HTTPS arise with encrypted email. Also here "security" stands for several meanings such as "confidentiality", "sender/receiver identity authentication" and peculiarly to emailing and messaging,"integrity of a message", and "end-to-end encryption". Once more, this multifaceted role of the term "security" has given rise to several misunderstandings, while being a source of great confusion among users. The technical difficulty to make the whole encryption mechanism working as intended, which often requires users to perform additional actions such as creating and managing encryption keys on top of writing and sending messages, did not help the cause of securing the email, and encryption is still rarely used by laypersons. That said, even the goal of informing users of the presence of a mechanism to ensure the confidentiality of their messages through encryption has not been easy. As early as in Whitten and Tygar's (1999) seminal paper on the usability of PGP 5.0, usability issues made it difficult for non-expert users to make use of encrypted emails. In their study, most novices were unable to successfully encrypt their emails in a 90 minutes time period. Later work confirmed that usability issues, in addition to social factors (e.g., being viewed as paranoid for encrypting emails) play a role in the adoption of encryption (Gaw et al., 2006). Ruoti et al. (2013)

evaluated a webmail system that uses security overlays with existing mailing services like Gmail. Their version of the tool was mostly invisible with automatic key management and encryption. Their participants were mostly able to use the system without any training, but the security aspects were so invisible that some mistakenly sent out unencrypted messages, and were concerned about trusting the tool. The authors then conducted a study with a prototype that used manual encryption, which enabled participants to avoid mistakes and led to more trust in the system. Lausch et al. (2017) reviewed security indicators in the context of secure emails and found that adding images of postcards, closed envelopes, and a torn envelope may warrant further work since they offered a relatively consistent interpretation. The authors also highlighted that the security indicators for encrypted email in different applications are mostly padlocks, but a variety of indicators exist for encrypted email (as well as signed and unsigned email), making it complicated for users to understand their meaning. They did not study text in association with the icons.

More recently, secure communication has often expanded to also include end-to-end encrypted messaging applications such as Signal or Whatsapp. Fahl et al. (2012) studied the usability and perceived security when encrypting Facebook messages, comparing combinations of manual and automatic encryption and key management. The authors found the highest usability in the versions of their prototype that included no display of security, where encryption was completely automated, or a combination of manual encryption and automatic key management. Researchers have often focused on authentication-related interactions, which users can have difficulties understanding or performing (Vaziripour et al., 2017), sometimes noting that inconsistent interface design and technical wordings can make it difficult to use the tools securely and as intended by the designers (Abu-Salma et al., 2017). A recent study by Fassl et al. (2021) explored a user-centered design process to improve usable authentication ceremonies. Instead of incrementally improving existing ceremonies, they employed a user-centered process to design new ceremonies from scratch in collaborative design workshops, followed by a security evaluation to narrow the design space, an iterative storyboard prototyping approach to improve usability, and an online evaluation. This user-centered approach took into account the social aspects of authentication ceremonies. While their approach did not result in better UX or usability, participants gained an improved understanding of security implications of authentication ceremonies.

A study on textual descriptions of encryption during data transmission in multiple contexts found that the verbs "secure" and "encrypt" were perceived as relatively secure, but the study did not combine the text samples with images or icons (Distler et al., 2020). While privacy icons do not serve to represent an underlying security mechanism per se, some of the insights from studies on how to represent privacy concepts are relevant to our study. A study on the design of privacy icons (Cranor, 2021) also demonstrated the importance of placing link text next to the icons for participants to understand what it meant. It is also important to consider different user groups as the usability of icons also differs between different age groups, with older adults needing more time to select icons, but giving the same number of correct responses in a navigation task (Dosso & Chevalier, 2021).

In this article, we will focus on the security mechanism "encryption", a mechanism that is ubiquitously used to ensure secure digital communications, yet mostly invisible in the user interface. We will focus on encryption as a mechanism used mostly for confidentiality during data transmission on a smartphone application. We will address the question of how to display this security mechanism in two contexts, e-voting, and online banking when optimizing the experience for perceived security, UX, and understanding. We will now describe examples where visible representations of encryptions were empirically assessed with end-users in these two contexts, and then situate our study conceptually.

6.3.2. Security mechanisms in specific use contexts

In the present paper, we focus on the visual representation of encryption used for confidentiality during data transmission in two use contexts, e-voting and online banking. We will now introduce some previous work on visible instances of security mechanisms in the contexts of e-voting and online banking, as well as factors that were found to influence security perceptions in previous work.

6.3.2.1. E-voting

E-voting is a high-stakes use context where encryption is used to ensure vote confidentiality, together with other cryptographic mechanisms that are often employed to ensure a trustworthy electronic election process, for instance, to help users and authorities verify that votes are not lost, tampered with, or selectively discarded, and that the vote counting has not been compromised. Elections have a complex work and information flow, and it is hard for citizens to have a detailed picture of the whole process, with or without the use of security mechanisms which, of course, complicate the picture. In the following,

we will focus on e-voting using a smartphone application; technology-supported voting at the polling station is out of scope for our purposes.

Existing e-voting applications can be hard to use and not always perceived as secure by the users. While vote verification is considered a cornerstone of secure elections, it also often leads to usability issues (Acemyan et al., 2014). Note that in this paper we focus on the security mechanisms in place when the user casts a vote; other cryptographic processes, such as those involved in the verification step (e.g., ensuring that a vote has been cast, cast as intended, counted as cast and similar properties) are instead out of scope for our purposes.

Remote e-voting is already used in some countries, for instance Estonia (Alvarez et al., 2009; Vassil et al., 2016) and Switzerland (Petitpas et al., 2020). A study compared the usability of multiple e-voting schemes and demonstrated that insufficient usability led to a considerable proportion of participants unable to cast a vote across voting systems, and many were unable to verify whether their vote had been taken into account. Overall satisfaction was low (Acemyan et al., 2014). A coercion-resistant e-voting with transparent verifiability protocol is “Selene” (Ryan et al., 2016). Selene allows voters to verify their vote using a tracking number to find their vote in clear on a bulletin board, providing a simple approach to vote verification. Distler et al. (2019) describe the design of an e-voting application based on the existing e-voting protocol Selene in two versions, one of which displays more security-related information to users. The version with “more information” (“version D”) included a visual of encryption, whereas the other version displayed no encryption-related information. In addition, version D also included more explanation about the vote verification process. Their results suggest that the version displaying more information may perform better overall in terms of UX and psychological need fulfilment, even though they caution to interpret these results carefully since results were statistically non-significant, potentially due to a relatively small sample size for intergroup comparisons, suggesting that more work is needed. Marky et al. (2018) evaluated the usability of different implementations of the Benaloh challenge for cast-as-intended vote verification, comparing three approaches. Based on their results, the authors recommend using the mobile approach for deployment during elections, and using the automatic approach for those who do not own a smartphone or similar device.

6.3.2.2. Online banking

In most European countries, e-voting is not routinely used for major political elections, online banking is a more common and more frequent interaction than voting for many people. Online banking can take place on a computer, using the browser, on a smartphone or other mobile devices, often using either a mobile application or the browser, in addition to various options for two-factor authentication that are frequently used (e.g., a second smartphone application, codes to be received via SMS, or a separate hardware token). This combination of options for online banking can make it difficult for users to accurately assess the presence or absence of security mechanisms during the interaction.

Online banking is also perceived as security-critical by users (Distler et al., 2020) and previous studies have found that perceived security and trust had a positive impact on the acceptance of online banking (Damghanian et al., 2016). Perceived risk had no significant effect on the acceptance of online banking, but on trust in online banking. Authors have argued that banks should take better steps to persuade their customers about the security and usefulness of their online banking systems (Özlen & Djedovic, 2017). Khan et al. (2017) investigated the acceptance of online banking in a developing country, Pakistan. The authors found that perceived security, as well as performance expectancy, facilitating conditions, habit, and privacy value were important antecedents of behavioral intentions. A study in the context of financial technology (Lim et al., 2019) found that perceived security and knowledge have an effect on users' confirmation (the extent to which the users' expectation of a service are fulfilled) and the perceived usefulness of a mobile fintech payment services, but perceived security did not directly impact on user satisfaction and continual intention to use.

The studies above have in common that researchers evaluate subjective experiences, and frequently, attempt to design for a user-friendly interaction that users understand and perceive as secure. How to measure such subjective perceptions is a challenge that can in part be addressed through the concept of user experience.

6.3.3. Measuring subjective experience through user experience

The evaluation of people's interactions with technology is a challenge that was traditionally addressed by the field of usability, but the concept has shifted to the broader concept of user experience. Usability focuses on the users' ability to achieve their goals effectively, efficiently and to their overall satisfaction (International Organization for Standardization, 2018). Authors have argued that a certain level of usability is necessary

as a basis for a positive experience (Hassenzahl et al., 2013), but will not necessarily lead to a positive experience on its own. In addition to users being able to achieve their tasks, user experience also takes into account the non-instrumental qualities that many experiences fulfil (Hassenzahl, 2001). These non-instrumental qualities refer to functions an interaction fulfils that are not directly goal oriented, but instead could fulfil psychological needs such as feeling connected to others (relatedness) or self-actualization (Sheldon et al., 2001). Adopting user experience as a frame of reference can help obtain a broader understanding of how users perceive an interaction. An efficient way to measure UX are standardized scales such as the Attrakdiff (Hassenzahl et al., 2003) or the User Experience Questionnaire (UEQ) and its shorter versions, the UEQ-S (Laugwitz et al., 2008; Schrepp et al., 2017).

In addition to UX, we also measure perceived security and understanding of the security mechanism encryption, as described in section 6.6.1.1. Conceptually, we see security perceptions as related to the psychological need for security (Sheldon et al., 2001). The measurement of understanding of an interaction, or, in our case, of the security mechanism encryption, is more difficult to situate within the framework of UX, but understanding is often highly relevant in usable privacy and security (UPS) contexts where misunderstandings can lead to security issues.

6.3.4. Summary

There is a growing body of research that calls for more visible and transparent communication of security mechanisms to end-users. Dourish et al. (2004) have argued that security technologies should be visible to users, to provide people with the means to understand the security implications of the current configuration of technologies they are using. This visibility should be expressed not as mathematically-grounded concepts of cryptography, but in terms that are adapted to the users' activities and needs at the time. Rather than making information about security mechanisms available when the user requests it, it should be available as a part of every activity in the system (Dourish & Redmiles, 2002), similar arguments being reiterated more recently, stating that displaying security mechanisms more clearly could help improve users' mental models and understanding of the security state of their interaction (Spero & Biddle, 2020). Pagter and Petersen (2007) suggested that security mechanisms could in fact become a significant part of positive experiences by providing a perception of security. Indicators for the

presence of the security mechanism encryption have been tested in contexts such as connection security indicators, encrypted email, encrypted messaging applications and e-voting, frequently finding that people's understanding was inaccurate and not always inducing perceived security (Acemyan et al., 2014; Distler et al., 2019). Perceived security was also an important factor for the acceptance of online banking (Damghanian et al., 2016; Özlen & Djedovic, 2017). Going beyond the perceived security, people's understanding of the security mechanisms in place is also an important aspect to consider, to ensure that their understanding is as accurate as possible and avoid erroneous mental models. Finally, people's user experience, as a broader measure of people's overall impressions of the interaction, is a promising concept to provide additional information with regards to the subjective experience of security-critical interactions.

Despite existing user studies of various encryption technologies, the HCI and UPS communities mostly lack concrete guidelines on how to communicate many of these security mechanisms to end-users. Current practices also sometimes lead to misunderstandings of the security provided by a system. In particular, previous work does not describe causal relationships between specific textual and visual representations of the security mechanism encryption on perceived security, UX and understanding. In addition, existing work mostly focuses on one specific use context and implications on how to display the security mechanism encryption are thus not necessarily transferable to other contexts. In the present paper, we test the indicators in two contexts, e-voting and online banking. These are relevant use cases for our purposes, as both rely on security mechanisms and can make use of visual and textual indicators to enhance users' experience during interactions.

We will now describe how we will contribute to closing these gaps.

6.4. Research Objectives

The main aim of this research is to evaluate the effects of textual and visual representations of encryption on non-experts' perceived security, UX and understanding. Our research design involved two studies, with the purpose of study 1 being to inform the design of our vignette experiment in study 2.

In our first study (section 6.5.), we involved experts from the fields of security, privacy and HCI to develop ideas on how to communicate encryption to non-experts via textual and visual representation:

- RQ1: How do HCI and security experts suggest to display the security mechanism encryption to non-expert users using textual and visual representation in the context of e-voting and online banking?

The first study allowed us to obtain the visual and textual representations for our main study; in our second study (section 6.6.), we tested the impact of these representations on non-experts' perceived security, UX and understanding in a vignette experiment, comparing the use contexts e-voting and online banking.

- RQ2: What is the effect of *visual* representation of encryption on perceived security, user experience and understanding of the security mechanism encryption?
- RQ3: What is the effect of *textual* representation (including the complexity of text) of encryption on perceived security, user experience and understanding of the security mechanism encryption?

We also address an additional methodological question. Since to the best of our knowledge no measurement of understanding of encryption exists in prior research, we explore how we might measure non-experts' understanding of the security mechanism encryption across both studies (sections 6.5. and 6.6.). Based on experts' suggestions in study 1, we created a measurement for understanding of encryption in study 2 and included it in the vignette experiment. We further openly asked participants what they thought our exploratory understanding questions were intended to measure and analyze the answers to this question.

6.5. Study 1: Iterative co-creation of representations of encryption with experts

To address our first research question, we conducted multiple co-creation activities with security and HCI experts to find out how we may best represent the security mechanism encryption to non-expert users and how we may measure understanding of encryption. The study was approved by our institution's ethics board, and experts provided informed consent. To define the visual and textual representations of encryption, we used an iterative design process, where experts were confronted with previous experts' ideas and opinions. Figure 1 shows the four stages of our iterative design process.

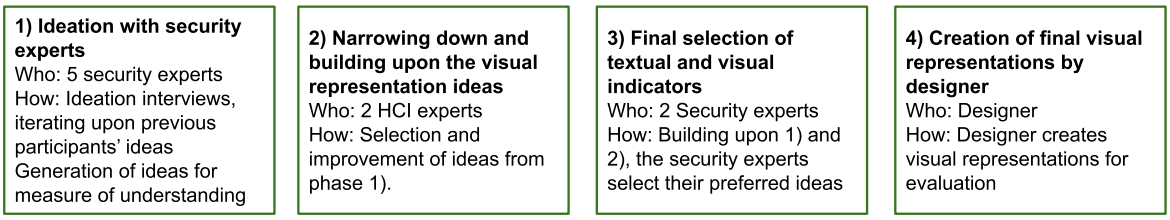


Figure 1: Summary of methodology study 1

6.5.1. Ideation with security experts

6.5.1.1. Participants

In this first phase, five security experts were recruited for an ideation session. The experts were three PhD Candidates, one Postdoctoral Researcher and one Full Professor. The PhD Candidates had between 0 and 5 years of experience in the field, the Postdoctoral Researcher between 5 and 10 years, and the Full Professor more than 10 years of experience. The experts participated in sessions of 1-1.5 hours each and were compensated with 40€ for their time. The participants were not part of the author team and recruited through the personal network of the first author. Four of the ideation sessions took place in the user lab, and one remote. We pre-tested the protocol; it worked as intended and we only made minor changes to the protocol, allowing us to include the pilot participant into the final set of security expert participants.

6.5.1.2. Procedure

The facilitator guided the experts through a number of questions and tasks. First, the experts were invited to explore ways of describing encryption to non-expert users while explaining their thought process. Next, we asked the experts to generate ideas for questions they might ask non-experts to measure whether they had understood encryption being used during data transmission. We asked the experts to explain their thought process for the questions they came up with.

Then, the experts were presented with three visual representations that are, or could be, used to represent security concepts (hand-drawn images of padlock, shield, database with a key, see Figure 2). We used hand-drawn images to alleviate any concerns about not being able to draw "well enough" in the next stage of the procedure. They were asked to rank these in terms of how well they represented encryption and to discuss critically what they liked and disliked about the visual representations.

Finally, the experts were asked to generate at least three ideas of visual representations of encryption, going beyond the common ones we asked them to critique. While the first expert participant was only presented with the three initial visual representations, the second expert was asked to critique the same three visual representations, plus the visual representations expert 1 had come up with. Expert 3 critiqued the initial visual representations, plus the visual representations experts 1 and 2 had come up with, and so on. Thereby, the experts built upon the ideas of previous experts, resulting in a rich collection of ideas for visual representations of encryption. Before presenting the previous experts' ideas, we redrew them so that they could not recognize a colleague's handwriting and would not hesitate to critique their ideas.

Figure 2: Hand-drawn images of padlock, shield and database with key that experts were asked to critique.

6.5.1.3. Results

The experts mainly critiqued that the padlock and the shield seemed too unspecific to indicate a security mechanism such as encryption, and associated the third icon with a database rather than any specific security mechanism. They also critiqued and built upon the previous' experts' ideas as shown in Table 3 (appendix), which demonstrates the evolution of the visual indicators through the various stages of study 1.

The experts also suggested a variety of explanations of encryption, as well as ideas on questions that they might ask a non-expert to evaluate their understanding of encryption as a security mechanism. Using the pool of potential questions intended to measure understanding of encryption, we selected a set of questions (mainly excluding any repetitive questions) and presented these to a security expert for feedback and improvement. We then presented this improved set of questions to another security expert, who also suggested improvements. This iterative process led to six questions intended to

evaluate whether participants' mental model corresponds to an interaction secured by encryption (see Supplemental Material).

Overall, the experts suggested focusing on questions that evaluated the most important implications of encryption, as they would not expect non-experts to be able to explain how encryption worked specifically. We use these suggestions for how to evaluate understanding of the security mechanism encryption in study 2 (see Section 6.6.1.1.).

6.5.2. Narrowing down and building upon the visual representation ideas with HCI experts

In this step, our objective was to narrow down and improve the large number of ideas of visual representation generated by the security experts in Phase 1.

6.5.2.1. Participants

We recruited two HCl experts from the personal network of the authors (not part of the author team) to take part in a 1.5 hours conference call. One of the experts had between 0 and 5 years of experience, the other between 5 and 10 years of experience in HCI. Their main expertise did not lie in the field of usable privacy and security. The experts were compensated with 40€ for their time.

6.5.2.2. Procedure

In the meeting, the experts were first presented with all the visual representations, and asked to individually think about which ones were most promising for use in a smartphone application (not in a tutorial context, but presented briefly as part of a smartphone interaction). They could also choose to modify visual representations they thought were promising but could be improved on certain aspects. After the individual task, both experts were asked to converge their opinions in a shared document and discuss which visual representations to keep, remove or modify. This phase yielded a set of visual representations that were deemed suitable for smartphone interactions and a set of recommendations on how to change visual representations to be more user-friendly. Using the HCI experts' suggestions, the first author created modified versions and presented them to the HCl experts for feedback the day after the initial call.

6.5.2.3. Results

Overall, the experts mainly opted to exclude representations that seemed too complex for being viewed only briefly in the context of a smartphone application, as these seemed more appropriate for tutorial-style interactions. They also asked to standardize the way certain components were visualized (e.g., by always using the same visual representation to represent a polling station or bank).

6.5.3. Final selection of textual and visual indicators

6.5.3.1. Participants

In this phase, we recruited two security experts (one postdoc and one PhD researcher) who had not participated in the previous stages. One of the experts had between 0 and 5 years, the other between 5 and 10 years of experience in the field of security respectively. Participation took 20-30 minutes and was asynchronous. The experts were compensated with 20€ for their time.

6.5.3.2. Procedure

We created a shared worksheet to be filled out by our security experts participants. The participants were first presented with all the expert ideas on how to describe encryption to non-experts and asked to highlight their favorite ideas out of the eight options. Then, we asked them to build upon these ideas to create a textual description of encryption with a low level of detail; as well as a description with a high level of technical complexity (yet still accessible for non-experts). Then, we presented the visual representations that stemmed from phase two and asked the expert to select their four favorite visuals and explain their selection.

6.5.3.3. Results

As a result, we obtained six favorite visual representations of encryption. The experts also built upon all previous ideas to create explanations of encryption with varying levels of detail. We (the authors) selected and combined their preferred descriptions; one used only the term encryption (“Encrypting your data”), and two with higher levels of complexity: “Encrypting your data. Encrypting your data ensures that only your intended recipients can read your data.” and “Encrypting your data using a digital key. Others require this key to read your data, and we made sure that only your intended recipients know it.”

6.5.4. Creation of final visual representations by designer

We used the online platform Fiverr.com to find a designer to create the visual representations. We used the same color scheme for all visual representations for consistency and went through one additional iteration with the designer to simplify and standardize the visual representations, while closely representing the experts' ideas. Table 3 (appendix) shows how the expert visual indicators evolved through the stages of this study.

6.6. Study 2: Vignette experiment with non-experts

In the second study, our objective was to evaluate how well the experts' ideas communicated encryption to non-expert users, addressing research questions 2 and 3. Anyone who has not received formal training or work experience in information security or cryptography is considered a non-expert for the purpose of our study.

We tested all the combinations of textual and visual representation brought forward by the experts in a vignette experiment. Vignette experiments combine the advantages of survey and experimental research (Auspurg & Hinz, 2015). Respondents are typically presented with descriptions of hypothetical scenarios, which are experimentally manipulated by the researcher. The method is extensively applied to study normative judgements and behavioral intentions (Wallander, 2009). The experimental design allows achieving high internal validity because the variation in the observed outcome variables can be solely attributed to the experimental manipulation of vignette characteristics. Moreover, the vignettes are assigned randomly to respondents, thus the effect of vignette characteristics on outcome variables should be independent from respondent characteristics. Using a vignette experiment allows us to provide causal evidence regarding the relationship between visual and textual representations of encryption and our three dependent variables (perceived security, UX, and understanding).

6.6.1. Research design

To test the effect of the visual and textual representations of encryption on our outcomes of interest, we conducted an online vignette experiment in February 2021 which was approved by our institution's ethics board. Our experiment considers two contexts where security concerns are highly relevant: e-voting and online banking. We investigated the impact of these combinations on people's perceived security, UX and understanding of

the security mechanism encryption used mainly for confidentiality during data transmission.

Participants were randomly assigned to either the e-voting version of our survey, or the online banking version (split-half experiment, see Figure 3). Within each context, after providing informed consent, the participants were shown a series of images of smartphone screens aimed at helping them envision being in the specific scenario (i.e., having to make a bank transfer or voting for a candidate).

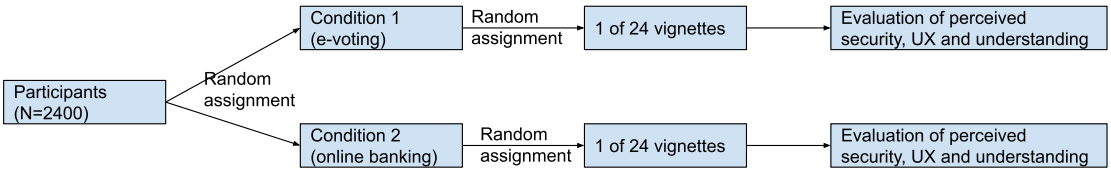


Figure 3: Overview of the study design (not shown: demographic questions).

Our vignettes exhibited the encryption part of the data transmission process in each context. They were integrated as one image of a smartphone screen into the series of smartphone screens. The vignettes varied experimentally in the values of two dimensions: the visual and textual presentation of encryption. Both dimensions were based on the expert productions in study 1. Table 1 provides an overview of the values of textual presentation of encryption and Table 2 provides the same information regarding the visual presentation of encryption. "No text" in Table 1 means that in this condition no textual representation was displayed. Instead, the visual was presented on its own unless they were assigned to the vignette that combined no text and no visual (i.e., where neither a text nor visual was shown). This condition thus represents a common case in current smartphone applications, where no visual indicators of encryption are shown to users. The respondents who were assigned to this vignette were shown the series of smartphone screens without the vignette. Instead of displaying the vignette, the confirmation screen was directly shown to participants. We used this condition as our control condition. Figure 4 shows an example vignette with the combination Text ID 4 und Visual ID 2. The experimental design resulted in 24 (4x6) vignettes, representing all possible combinations of visual and textual representations of encryption. We employed a between-subjects design. Each participant was exposed to one randomly assigned vignette only. Such an approach decreases the risk of the respondents detecting the objective of the experiment

and avoids, for example, learning effects. In each context, this vignette was followed by an image of a smartphone screen confirming the success of the interaction.

Text ID 1	*No text*
Text ID 2 (technical term "encryption")	Encrypting your data.
Text ID 3 (lower complexity)	Encrypting your data. Encrypting your data ensures that only your intended recipients can read your data.
Text ID 4 (higher complexity)	Encrypting your data using a digital key. Others require this key to read your data, and we made sure that only your intended recipients know it.

Table 1: Values of the experimental variable: textual representations of encryption.

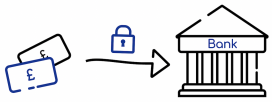
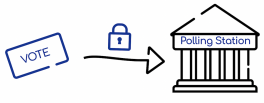
ID	Visual ID 1	Visual ID 2	Visual ID 3
Online banking	*No visual representation*		
e-voting	*No visual representation*		
ID	**Visual ID 4**	**Visual ID 5**	**Visual ID 6**
Online banking			
e-voting			

Table 2: Values of the experimental variable: visual representations of encryption.

Figure 4 shows an example vignette with the combination Text ID 4 und Visual ID 2. Out of the 24 vignettes, one consisted of the combination no text and no visual. This condition thus represents a common case in current smartphone applications, where no visual indicators of encryption are shown to users. The respondents who were assigned to this vignette were shown the series of smartphone screens without the vignette. Instead of displaying the vignette, the confirmation screen was directly shown to participants. We used this condition as our control condition.

After participants had looked at all of the images of smartphone screens, we then asked them to rate (1) the perceived security, (2) the UX of the simulated interaction (3), and their understanding of the security mechanism encryption used mainly for confidentiality during data transmission. We provide the full questionnaire as Supplemental Material.

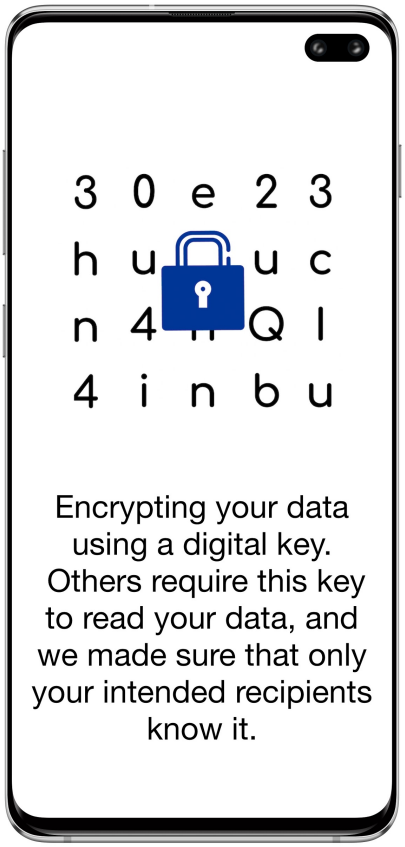


Figure 4: Sample vignette, combination of Text ID 4 and Visual ID 2.

6.6.1.1. Measurements

Perceived security.

We measured perceived security ("How secure or insecure did this experience feel to you?") on a scale of 1 (not secure at all) to 10 (very secure).

User Experience.

We evaluated UX with the 8-items short version of the UEQ, the UEQ-S (Schrepp et al., 2017) which measures UX in two dimensions: pragmatic quality and hedonic quality. Each dimension is measured with a 7-point semantic differential scale with four items. Pragmatic quality of experience is measured with the differentials obstructive/supportive, complicated/easy, inefficient/efficient, confusing/clear. Hedonic quality is measured with the differentials boring/exciting, not interesting/interesting, conventional/inventive, usual/leading edge. For our analysis, we generated two mean value indices representing the two dimensions.

Understanding of the security mechanism of encryption.

Finally, we used an exploratory measure of understanding of the security mechanism encryption resulting from study 1. Participants rated how much they agreed or disagreed with the single items on a 5-point scale for the following question items. Since it is an exploratory measure, respondents were given the option "not sure":

- The connection is protected so that hackers cannot steal the data I'm sending.
- I am using a secure communication channel.
- Even if someone steals the data that I am sending, they won't be able to see what it means.
- Nobody can impersonate me unless they know my digital key.
- Nobody can see what I am sending without holding my digital key.
- My actions on the application are not revealed by someone listening in on the channel.

We reversed the scale such that higher values on the 5-point scale meant more agreement or, in other words, that participants thought that the interaction was secured by encryption. We generated a mean value index based on the six items. Observations for the option "not sure" were counted as missing values. For respondents with missing values, the mean understanding was calculated based on the items for which valid information was

available. However, we applied weights that assign higher values to respondents who rated all six items (i.e., either agreed or disagreed to all six items) when constructing the index. For instance, a participant who answered all six items without selecting "not sure" would be given the full weight of 1, a participant who answered "not sure" on three out of six questions would be given a weight of 0.5. Respondents with missing values (i.e., not sure) on all six items were assigned the weight of 0 and thus were excluded from the analysis (N=99). We used this weighted mean value index to measure understanding of encryption in our analysis. This approach allows us to use as much of the available information as possible without unnecessarily reducing the sample size.

To further assess the quality of our measurement of understanding, we asked participants what they thought the "understanding" questions meant in an open-ended question ("In your own words, what was the question above about?").

6.6.1.2. Recruitment and participants

We invited a sample of 2400 participants from Prolific who were based in the UK. Prolific allows researchers to recruit potential participants according to specific selection criteria. Participants are notified through the recruitment platform once they are eligible to take part in a research study. In terms of recruitment criteria, we did not specify constraints regarding gender, education or other factors. The included participants were notified automatically and redirected to the survey. The sample was non-representative. Note, however, that a representative sample is not necessary to achieve internal validity with experimental data. We recruited 2400 participants with the objective of obtaining 50 answers per vignette in both contexts (2*50*24=2400), which the literature suggests as the rule of thumb to obtain enough statistical power (Auspurg & Hinz, 2015). We excluded anyone who had participated in pre-tests of the study. The data collection period took one day in early 2021.

In total, 2,457 respondents started the survey and 2,417 completed the survey (i.e., answered all questions). We excluded respondents who had previously worked or studied in a field related to cybersecurity from further analysis. We also excluded respondents who did not pass the attention check questions. For any participants who filled out the survey twice (presumably by saving the link to our survey), we excluded their second participation from our analysis and kept the first time they participated. Finally, we excluded respondents who had not answered all the relevant questions from further

analysis (i.e., who dropped out before answering the questions related to our dependent variables). Our analytic sample included 2180 participants, of which 1087 were randomly assigned to the context of e-voting, and 1093 were randomly assigned to online banking.

The participants were 68.8% women, 30.7% men, the remainder being non-binary and a gender that was not listed (0.5%). Participants were 38 years old on average (SD=12.5). Around 55% of the respondents have a university degree (Bachelor or higher).

6.6.1.3. Experimental data

Since we employed a between-subjects design, our data comprises 2180 vignette ratings from 2180 respondents. A Chi-Square Test of Independence between vignettes and context revealed a non-significant result, suggesting that the split-half experiment worked. On average, each vignette was evaluated 45 times (e-voting: 45 times; banking: 46 times). Tables 4 and 5 (appendix) show that all bivariate correlations between the values of our two vignette variables are close to zero ($r < 0.1$) and not statistically significant, ensuring efficient estimation. Similarly, all correlations between the values of our vignette variables and key observed respondent characteristics (education, age) were close to zero ($r < 0.1$) and not statistically significant, indicating that the randomization worked. The only exception is respondent gender, of which single values correlated significantly with one value of visual representation, but these correlations were also close to zero (see Tables 4 and 5). We performed robustness checks to test the influence of respondent characteristics on our findings (see Section 6.7.).

In both contexts, respondents used the whole answer scale for the dependent variables and the distribution of ratings was left-skewed for perceived security, UX (pragmatic quality), and the weighted index for understanding, thus tending towards more positive values on the respective scales (see Figures 9-12, and 15-16 in the appendix). Hedonic quality of UX was symmetrically distributed in both contexts (Figures 13 and 14 in the appendix).

6.6.1.4. Data analysis

To analyse our experimental data, we conducted Ordinary Least Squares (OLS) regressions using robust standard errors to account for heteroskedasticity. We estimated separate models for our dependent variables (UX pragmatic, UX hedonic, perceived security, and understanding) and the two contexts. We first estimated the overall effect of textual and visual representation of encryption on each of our dependent variables. We

then estimated the effects of the single values of textual and visual representation for each dependent variable in a second model. If we found statistically significant effects, we tested whether the effects of textual and visual representation varied between contexts in a third set of models. These models were conducted based on the full sample and including an interaction term between the variable indicating the context and the variables indicating textual and visual representation. We performed several analyses to assess the robustness of our findings (see our discussion in section 6). We provide these additional analyses as supplemental material.

Regarding the qualitative analysis, we categorized all qualitative answers about what participants thought the understanding questions were aimed at. Once the initial codebook was created, we conducted a test session with 8 HCI experts, who applied the codes to a subset of 400 answers. They commented on any codes they thought were unclear and suggested improvements, which we used to update the codebook. Using the updated codebook, we then conducted a double-coding session with an HCI expert who double-coded the answers from 250 participants (11% of answers). Since there was a large number of codes and potential combinations, the probability of agreement by chance was low. We thus used a simple measure of percentage agreement. We defined agreement between coders as the exact same combination of codes. For the questions assessing qualitative answers to the understanding question, the two coders achieved an agreement of 86%.

We provide the syntax files used for analysis and the data (with potentially harmful meta data removed), as well as our annotated analysis, as supplementary material.

6.6.2. Results

6.6.2.1. Bivariate correlations between dependent variables

We found a statistically significant and positive correlation between UX and perceived security in both the context of e-voting (pragmatic, r= 0.40; hedonic, r=0.36; 5% significance level) and online banking (pragmatic, r=0.46; hedonic, r=0.29; 5% significance level). Thus, higher values on UX mean higher values on perceived security in both contexts.

There is a statistically significant and positive correlation between perceived security and understanding in both contexts (e-voting, r = .56; banking, r=0.40; 5% significance level), meaning that the better the understanding, the higher the perceived security.

Overall, the size of the correlation is moderate suggesting that our three dependent variables capture distinct dimensions of the interaction.

6.6.2.2. Experimental evidence

Perceived security

Table 6 (appendix) shows the results of OLS regressions predicting perceived security regarding the overall effects of text and visual representation. In both contexts, we observed a positive and statistically significant overall effect of text representation (compared to no text) on perceived security. The effect was highly significant ($p < 0.001$) in the banking context and significant at the 5%-level in the e-voting context. When looking at the single values of text representation (see Table 7), "lower complexity" and "higher complexity" showed statistically significant and positive effects in the banking context (both $p < .001$). Figure 5 shows the results graphically. Lower complexity text increased perceived security by almost one scale point (0.74), similarly, high complexity text increased perceived security by 0.70 compared to no text. The difference between the two effects was not statistically significant. Although we observed the same pattern in the e-voting context, the effect sizes were slightly smaller than in the banking context. Moreover, we only found a statistically significant effect of high complexity (5%-level). The values of the visual representation of encryption showed relatively small effects on perceived security, which were not statistically significant in both contexts.

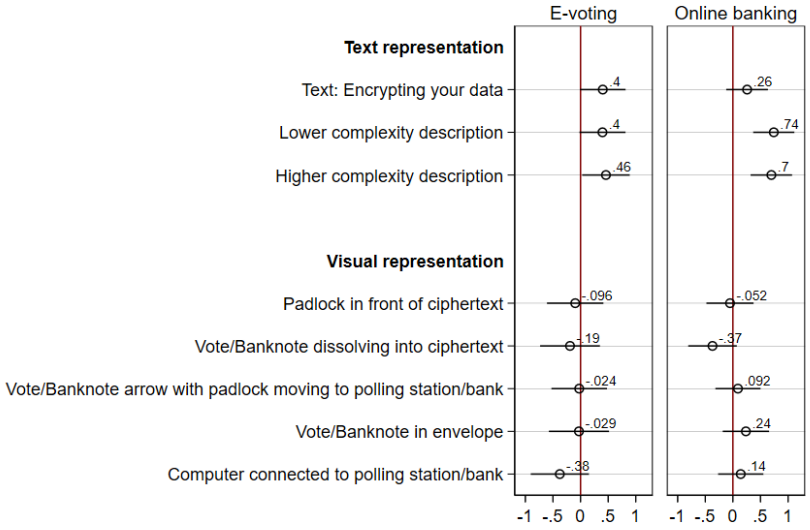


Figure 5: Coefficient plot: single effects of vignette values on perceived security. N=1,087 in e-voting, N=1,093 in online banking.

Table 8 (appendix) shows the results of a regression model including an interaction effect between context and textual representation. The interaction effect suggested slightly more positive effects of lower and higher complexity in the banking contexts compared to the e-voting contexts, but was not statistically significant. Thus, our results do not suggest substantial differences in the effects of text presentation between the two contexts. Since we found no substantial and significant effects of visual presentation in any of the two contexts, we did not estimate a model including an interaction of visuals and context.

In summary, we found evidence that textual representation of encryption increases perceived security while visual representation has no effect.

User experience (UX)

Pragmatic quality of user experience (UX-PQ): In both contexts, the overall effect of text and visual presentation were close to zero and not statistically significant (see Table 9 in the appendix). We observed similar results regarding the effects of the various versions of text and visuals on UX-PQ (see Table 10). The effects were relatively small and not statistically significant (see also Figure 6, which shows the results graphically). Some of the effects of the versions of visual presentation showed a negative sign, suggesting a decrease in UX-PQ. In both contexts, none of the observed effects were statistically significant. The only exception is the padlock in front of ciphertext (visual ID 2), which had a statistically significant negative yet small effect on UX-PQ in the context of banking ($p<0.01$).

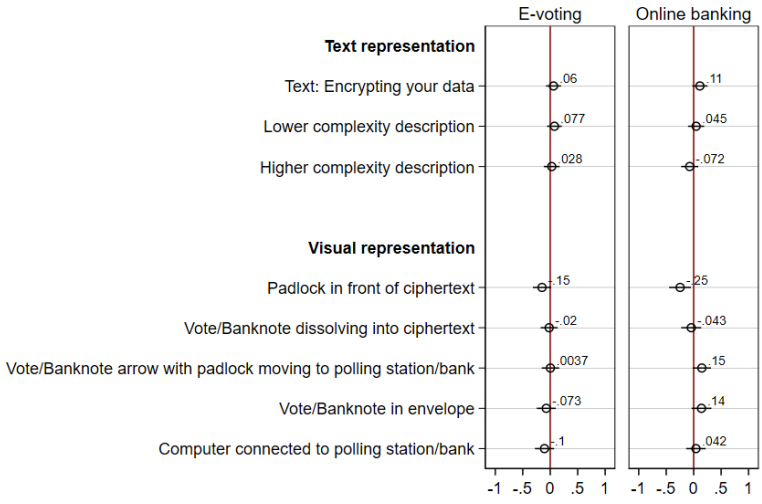


Figure 6: Coefficient plot: single effects of vignette values on UX-PQ. N=1,087 in e-voting, N=1,093 in online banking.

Hedonic quality of user experience (UX-HQ): Regarding the overall effects of text and visual presentation, we observed relatively small and non-significant effects in both contexts (see Table 11). Similarly, we observed relatively small and close-to-zero effects of the versions of text and visual presentation of encryption on UX-HQ in both contexts (see Table 12 in the appendix). Some of those showed negative signs, however, the effects were not statistically significant in most cases. We found a statistically significant and positive effect of visual representation ID 4 (vote/banknote arrow with padlock moving to polling station/bank) on UX-HQ in the context of voting ($p<0.05$). We provide the coefficient plot for the versions of the text and visuals in Figure 7.

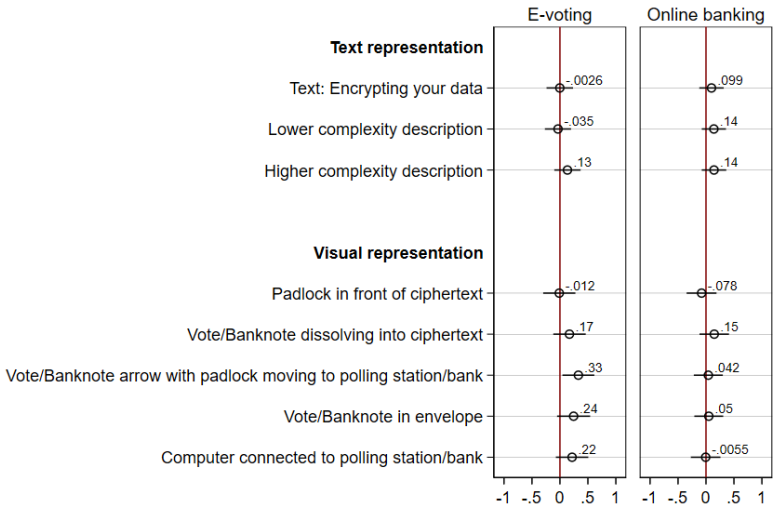


Figure 7: Coefficient plot: single effects of vignette values on UX-HQ. N=1,087 in e-voting, N=1,093 in online banking.

Overall, we found little evidence suggesting that textual and visual representations impact UX, with two exceptions: padlock in front of ciphertext regarding UX-PQ in the context of banking, and vote/banknote arrow with padlock moving to polling station/bank regarding UX-HQ in the context of voting.

Understanding

Table 13 (appendix) shows the results regarding understanding of encryption. The textual representation of encryption had a statistically significant and positive overall effect on understanding of encryption in both contexts (e-voting: $p < 0.001$; online banking: $p < 0.001$). We found no statistically significant overall effect of visual representation and the effect was close to zero in both contexts (see also Figure 20 in the appendix). When looking at the single values of text (see Table 14 for the full model and Figure 8 for the

graphical presentation of results), Text version 3 (highest complexity) has the strongest positive effect (similar to our results regarding perceived security) in both contexts. In the context of e-voting, the difference between the effect of higher complexity and lower complexity as well as the simplest version "encrypting your data" vs. no text was statistically significant ($p < 0.05$ and $p < 0.001$, respectively). In the context of online banking, only the difference between higher complexity and the simplest text version as well as between lower complexity and the simplest version was statistically significant. The difference between the effects of higher and lower complexity was not statistically significant.The visual representation of encryption had no statistically significant effect on understanding in both contexts. All effects were relatively small.

Similar to our results regarding perceived security, the interaction terms between context and text was not statistically significant and rather small in both contexts, suggesting that the effect of text on understanding does not vary in a relevant way between the two contexts (Table 15).

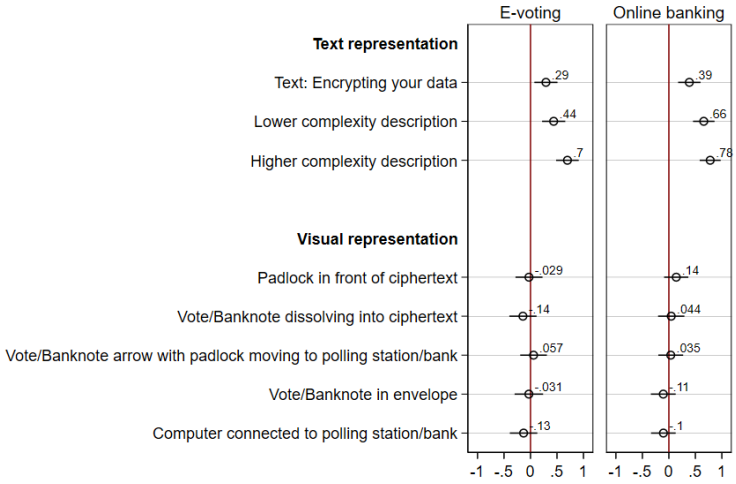


Figure 8: Coefficient plot: single effects of vignette values on understanding. N=1,087 in e-voting, N=1,093 in online banking.

In summary, we found evidence that a textual representation of the security mechanism encryption increases the understanding of encryption. In both contexts, more complex textual representations had the greatest influence, although we found no relevant differences between high complexity and low complexity, at least in online banking.

To synthesize, our results show that UX-PQ and UX-HQ are positively correlated with perceived security, as is our measure of understanding encryption. The textual

representation of encryption had a statistically significant and positive overall effect on both perceived security and understanding of encryption in both contexts, with more complex versions of the text having a greater influence. The visual representation of encryption had no substantial or statistically significant effect on any of our dependent variables.

6.6.2.3. Results of qualitative analyses

We will now describe the qualitative results obtained from the open-ended questions to complement our understanding of participant perceptions.

Since the "understanding" questions were exploratory, we asked participants what they thought these questions were about (commonly referred to as "face validity"). 65% of answers mentioned that they were about security in general, followed by encryption (19%) and hacking (14%), as well as authentication (3%), impersonation (3%) and fraud (2%).

Most of these concepts are closely related to encryption during data transfer, which can, for instance, provide confidentiality and protection from fraud, hacking or impersonation to a certain degree. The only concept which one can argue is not necessarily related to encryption during transmission is authentication which participants frequently related to login details. In the qualitative answers, we could see that participants who mentioned authentication seemed to mix up the "digital key" mentioned in the description of encryption with a password. We also explored the terms participants used to qualify these concepts. Participants mostly thought that the question aimed at exploring their feelings, knowledge, thoughts, understanding and perceptions.

Overall, these qualitative results show that our participants thought that our understanding questions measured concepts closely related to what we intended to measure, albeit they often expressed this more generally as a notion of overall security.

6.7. Discussion

In this section, we reflect on the three research questions of this paper. First, we discuss our results regarding the expert co-creation study (RQ1). Second, we discuss the results from our vignette experiment (RQ2 and RQ3). Next, we discuss the exploratory measure of understanding brought forward by our experts, and reflect on its usefulness. We also discuss the limitations of the present work and suggest directions for future research.

6.7.1. Generating ideas for visual and textual representation of encryption using a multidisciplinary panel of experts

The results from study 1 answered RQ1 and provided us with the elements needed to inform study 2. Expert insights are used in a variety of studies in usable privacy and security, for instance in order to compare their behaviors with non-expert behaviors (Busse et al., 2019; Ion et al., 2015), their security perceptions compared to non-experts (Gallagher et al., 2017), or to compare the security concerns experts had as compared to non-experts (Murillo et al., 2018). In this article, we used a different approach and did not compare expert and non-expert behaviors, perceptions or understanding. Instead, we recruited a mix of security and HCI experts and asked them to generate ideas in an iterative co-creation process. We found this approach helpful, in particular by asking the experts to build upon the earlier experts' ideas, which encouraged them to go beyond the ideas that first came to their mind. This approach differs from a recent study using co-design methodologies with non-expert users (Fassl et al., 2021). The authors highlight that the initial framing of the security threat and task heavily influenced participants' ideas for solutions. This difficulty when using co-design methods for displays of technical security with non-experts led us to avoid using the non-experts to come up with ideas of how to display encryption as we would have needed to explain what encryption is first. However, explaining encryption to non-experts is a non-trivial task and there is limited work on how to best do this. This paper makes a contribution to this gap. Both our approach and co-design methodologies with non-experts seem suitable to put the user at the centre in the design of user-centered displays of security, but our iterative approach of combining expert knowledge from multiple domains (study 1), followed by a an evaluation with non-experts (study 2) might be more suitable for technical topics where co-design with non-experts is initially difficult since they are not familiar with the subject matter and empirical guidance on how to create a common frame of reference is lacking.

6.7.2. Putting expert ideas to the test: experimental results of the effects of visual and textual representations on dependent variables

The results from study 1 informed study 2, which addressed RQ2 and RQ3. We found that the visuals had no statistically significant effect on any of our dependent variables, while the version of the text had a statistically significant effect on perceived security and understanding. We might have expected the visual representations to be "intuitive" ways

of displaying the security mechanism of encryption to users, not requiring any reading and able to convey a "great deal of information concisely" (Blattner et al., 1989, p. 12). However, our study does not confirm such assumptions that visuals are necessarily more intuitive ways of displaying information. Previous work frequently measured the effects of icons and text in terms of observed measures such as task completion times or error rates. For instance, Huang et al. (2019) compared two experimental groups of older adults, one of which interacted with an ATM interface that only used text, and one of which used an interface that combined icons and text. Task completion (measured in terms of use of the help button and number of steps required to complete a task) was better for the participants in the group that saw both icons and text, although effect size remained relatively small. Similarly, Majrashi (2020) found that combining text with icons in a smartphone menu led to faster task completion times and fewer mistakes. Both studies did not measure any subjective indicators of experience, as was done in this study. In other studies that included self-report measures of experience, the combination of visual representation with text labels, as well as text-only led to better learnability and ease of use (Wiedenbeck, 1999). In work on the visuals representing privacy choices, it was also necessary to add a text to the icon for research participants to understand their meaning (Cranor, 2021). Note that, based on these studies, one might have expected the visual indicators to have a positive effect in our study when combined with textual indicators, but this was not the case – even when combined with textual indicators, the visuals had no statistically significant effects. Our results were however in line with research that found that textual indicators have a positive effect on user perceptions (Cranor, 2021; Wiedenbeck, 1999).

We can hypothesize on the reasons why there was no significant effect in our study. All of our visuals were novel to users since they were based on the expert iterations in study 1. This novelty might require participants to engage in greater mental efforts to process the visuals which have no previously assigned meaning. Indeed, previous work has found familiarity to be a relevant factor for the guessability of physical safety warning signs, for instance (Chan & Ng, 2010) and is generally considered relevant for the speed and accuracy with which icons and objects can be identified (McDougall et al., 2016). Wogalter et al. (2006) also describe the different symbol-to-concept relationships, from representational symbols that directly or closely relate to the represented concept, to more abstract or arbitrary symbols, with a more distant relationship to the concept. A sign with

a crossed out match would be an example of a representational symbol, directly displaying the meaning of "do not light a match". In our case, such direct representation was not possible as encryption does not have an equivalent, well-known real-world concept that could be visualized to represent encryption. The digital processes represented by the visuals are not always familiar to non-experts, for instance the concept of data transmission in visual IDs 4 and 6. Also note that many of these studies investigate performance measures such as number of errors participants make or completion time. Self-report measures with a focus on variables such as UX and perceived security are comparatively rare, we cannot exclude that the tested visual representations might have an effect on measured variables that were out of scope of this study.

In our study, more complex text had a positive effect on understanding of the security mechanism encryption and at least in the online banking sector also on perceived security. Considering that more complex text introduces friction to the interaction by introducing additional information and an additional step compared to our control condition, our work lends some empirical support to work arguing that introducing some friction into experiences may create more mindful experiences (Cox et al., 2016). Recent work also made an argument for "security-enhancing friction", friction that encourages users to behave more securely (Distler et al., 2020). The friction introduced through the descriptions of encryption can be seen as friction that helped improve the understanding of encryption, which is in itself a positive result for the security of our users. Of course, our work does not allow us to make statements about behaviors.

6.7.3. The challenges of creating an exploratory measure of understanding of encryption

In our studies, we created and used an exploratory measurement of understanding for encryption. We asked experts which questions they might ask non-experts to evaluate whether they had understood that encryption was being used, upon which we iterated twice with other security experts. We then used these question items in study 2 as an exploratory measure of understanding. Our qualitative analysis shows that these questions were mostly perceived by non-experts as measuring security in general or encryption. The answers suggesting that the items measured security in general did not provide any details about the security mechanism providing the security, but they seemed to understand the general implication of providing protection to some degree. One possibility for these results is that

participants lack the necessary vocabulary to associate our six items with encryption and therefore associate these items with the more familiar term security. However, it might also be the case that the six items capture security perceptions in addition to understanding. Also, the answer option "not sure" was used relatively frequently, although no question item seemed to stand out in terms of difficulty to provide an answer (approximately 20% of participants for each question item). These ratings could indicate that the participants did not understand the question, or they might have understood the question, but were not sure about its answer. For these respondents, we might have over- or underestimated understanding of encryption. As a robustness test for our weighted mean value index of understanding, we generated an index excluding all observations for "not sure" and re-estimated our models using this index as a dependent variable. These analyses did not reveal substantial changes in our findings. We provide this additional analysis as supplemental material.

6.7.4. Limitations and future work

Our study has some limitations and open questions for future work remain.

Visual and textual representations

There are some limitations related to the visual representations we used. The visual indicators we evaluated were closely based on the HCI and security expert ideas and were not redesigned by an icon designer following guidelines for icon design. A previous study compared crowdsourced security indicators by non-experts with designer-drawn icons. In their evaluation, the crowdsourced indicators performed no worse, and sometimes better than the designer-drawn icons (Egelman et al., 2015), providing some support to our approach. However, future work could redesign the icons following icon design guidelines and evaluate the effectiveness. We also tested the vignettes in the particular context of a smartphone interaction, a context for which the visual representations may have included more details than is typical in such interactions. While the visuals did not have a significant effect in this context, we cannot exclude that they might have positive effects in, for example, a tutorial setting aimed at teaching non-experts about encryption, a potential avenue for future studies. We also did not test animated designs, which is an open question for future research. Future work could address the effect of familiarity with visuals on user perceptions, for instance using eye tracking to investigate how fast people are able to react

to the visuals, and whether they react more efficiently to indicators that are commonly used.

Some limitations need to be acknowledged regarding the textual representations. Our study focused not only on textual representations of encryption in general but also the degree of complexity of textual representations. Complexity was defined based on technical concepts introduced in each version of text, but other characteristics of textual representations might have an effect on our outcomes of interest. For example, future studies could explore the impact of text length in addition to the mentioning of technical concepts. In our study, more complex text provided more details on the ongoing process, which made more complex text longer. Thus, we cannot clearly separate the effect of text length and technical terms. Also, the number of technical concepts in one text might additionally play a role, which could be assessed in future work.

Overall, a promising result of our study is that complex, carefully designed descriptions of encryption had a statistically significant effect on perceived security and understanding. We hope to see more work in the future on how to design text that describes technical security concepts to non-experts in a user-centred way.

Generalizability

A potential limitation of the present work concerns the generalizability of our results to real-world interactions with technology. Our participants were encouraged to pay close attention and might have paid less attention in a real-life context. Thus, we might have overestimated the effect of textual representations on our dependent variables in the vignette experiment. Nevertheless, as discussed, our results are in line with previous studies finding an effect of textual representations on perceptions and/or performance. It would be relevant for future studies to implement varying representations of security mechanisms in real-life use contexts, where participants might pay less attention to the details of a smartphone application, and compare the results to our outcomes. Also, the generalizability of our results is further limited to the textual and visual representations used in our design (including the general layout of our vignettes such as color), but other relevant combinations of text and visual representations might exist. These could be assessed in future research.

Measuring understanding of encryption

For our exploratory measure of understanding, we, as well as our experts, found it challenging to define what level of understanding of such a technical concept we could expect non-experts to have. A challenge of measuring understanding of encryption is to make sure that the wording of the questions stays sufficiently non-technical for non-expert users, but at the same time measures the intended concept. Given that understanding of encryption constitutes a relevant concept for many security-relevant interactions, future work should continue iterating upon our exploratory items. For example, although we had conducted qualitative pre-tests of the questionnaire, more extensive qualitative investigation of the "understanding" items should reveal the reasons for participants' frequent selection of "not sure" as an answer. Overall, we think that the items were a useful first step in measuring general understanding of encryption, but we acknowledge the exploratory nature of our measurement and that further research is needed to validate and further develop this study's measurement of understanding.

Theoretical concepts

Our study also leaves some open questions on a theoretical level. Indeed, typical models of UX (Hassenzahl, 2008; Mahlke, 2008) and instruments assessing UX (Hassenzahl et al., 2003; Laugwitz et al., 2008) do not include indicators for understanding of underlying processes or perceptions of security. While psychological need theories include the need for security as drivers of satisfying events (Sheldon et al., 2001), assessment is relatively broad and thus difficult to apply in the field of usable privacy and security. But of course, the field of usable privacy and security has long extended beyond the concept of usability and includes a broad scope of research; for instance aiming to improve user understanding and perceptions of security (Abu-Salma et al., 2018; Distler et al., 2019; Spero & Biddle, 2020) or applying co-design methodologies for security processes (Fassl et al., 2021). In the future, it would be relevant to see work theorizing on the links between UX and usable privacy and security, reflecting on the extent to which the broad range of issues addressed by the field of usable privacy and security can be addressed under the umbrella of UX. The field would further profit from empirical work assessing the relationship between the concepts of understanding, user experience and understanding, strengthening our theoretical knowledge of user perceptions in the context of security-relevant interactions.

6.8. Conclusion

There is an ongoing debate whether security mechanisms should be visible or hidden away from users. User-centered design typically aims to let users complete their tasks as easily and quickly as possible (Krug, 2000), leading to many security mechanisms being hidden away from the user, who thus have no indication they are happening in the background. This lack of visibility can backfire when users lack understanding of security processes, potentially leading to security issues (Adams & Sasse, 1999) and leaving users unable to form accurate mental models of the security of a system (Spero & Biddle, 2020). Authors have thus argued that security should be highly visible and ready to be inspected by users (Adams & Sasse, 1999).

Our study brings empirical evidence to the ongoing discussion "should security mechanisms be visible or hidden away from users" by answering two main research objectives. First, we addressed the question of how HCI and security experts suggest displaying encryption to non-expert users using textual and visual representation, using an iterative co-creation process (see section 4). Second, we wanted to understand what the effects of the resulting visuTal and textual indicators are on perceived security, user experience and understanding, comparing two use contexts: e-voting and online banking. To this end, we conducted an online vignette experiment with non-expert users to test the effect of the representations on our outcomes of interest (see section 5).

In summary, the textual representation of encryption significantly increased both perceived security and understanding of encryption in both use contexts. More complex text describing encryption resulted in higher perceived security and more accurate understanding. Representing encryption through text thus seems to be a promising solution to improve understanding and improved security. Overall, we found little differences in our results between the two use contexts. We found no statistically significant or substantial effect of textual representations on UX. Finally, visual representations of encryption had no statistically significant effect on any of our dependent variables.

Overall, our study contributes to the larger discussion regarding visible instances (including text and visuals) of security and the impacts they may have on user perceptions. Our study supports the hypothesis that more visible instances of security support more accurate understanding (Spero & Biddle, 2020), but also, perceived security. We also attribute this effect to the extensive design phase of the tested vignettes with a multidisciplinary panel of experts; as well as pre-tests that enabled us to improve upon any expert suggestions that participants perceived as confusing. We therefore interpret our

results as an encouragement to carefully design and pre-test technical descriptions for improved understanding and perceived security in a user-centered way.

While the vignette experiment is a frequently used methodology to measure normative judgements, attitudes, and behavioral intentions in sociology (Wallander, 2009), to the best of our knowledge, it has rarely been applied to evaluate interface designs in UPS contexts (Al-Natour et al., 2020) or other HCI contexts (Vance et al., 2015). Our work demonstrates that this method can be applied to empirically evaluate details of interface design. Its strength lies in the results that give insights into the causal relationship between visual and textual design choices and outcome indicators, free from confounding factors.

Our results demonstrate the relevance of measuring the effects of user interface elements such as visual and textual indicators on facets of experience such as perceived security, UX and understanding. We hope that future work will provide more empirical research-based guidance on how displays of technical security might look when optimizing these user-centered indicators going beyond UX alone and including security perceptions and understanding.

6.9. References

Abu-Salma, R., Krol, K., Parkin, S., Koh, V., Kwan, K., Mahboob, J., Traboulsi, Z., & Sasse, M. A. (2017). The Security Blanket of the Chat World: An Analytic Evaluation and a User Study of Telegram. *Proceedings 2nd European Workshop on Usable Security*. European Workshop on Usable Security, Paris, France. https://doi.org/10.14722/eurousec.2017.23006

Abu-Salma, R., Redmiles, E. M., Ur, B., & Wei, M. (2018). Exploring User Mental Models of End-to-End Encrypted Communication Tools. *Proceedings of the 8th USENIX Workshop on Free and Open Communications on the Internet (FOCI)*, 8.

Acemyan, C. Z., Kortum, P., Byrne, M. D., & Wallach, D. S. (2014). Usability of voter verifiable, end-to-end voting systems: Baseline data for Helios, Prêt à Voter, and Scantegrity II. *The USENIX Journal of Election Technology and Systems*, *2*(3), 26–56.

Adams, A., & Sasse, M. A. (1999). Users are not the enemy. *Communications of the ACM*, *42*(12), 40–46. https://doi.org/10.1145/322796.322806

Al-Natour, S., Cavusoglu, H., Benbasat, I., & Aleem, U. (2020). An Empirical Investigation of the Antecedents and Consequences of Privacy Uncertainty in the Context

of Mobile Apps. *Information Systems Research*, *31*(4), 1037–1063. https://doi.org/10.1287/isre.2020.0931

Alvarez, R. M., Hall, T. E., & Trechsel, A. H. (2009). Internet Voting in Comparative Perspective: The Case of Estonia. *PS: Political Science & Politics*, *42*(03), 497–505. https://doi.org/10.1017/S1049096509090787

Blattner, M. M., Sumikawa, D. A., & Greenberg, R. M. (1989). Earcons and Icons: Their Structure and Common Design Principles. *Human-Computer Interaction*, *4*(1), 11. Computers & Applied Sciences Complete.

Busse, K., Schäfer, J., & Smith, M. (2019). Replication: No one can hack my mind revisiting a study on expert and non-expert security practices and advice. *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*.

Chan, A. H. S., & Ng, A. W. Y. (2010). Investigation of guessability of industrial safety signs: Effects of prospective-user factors and cognitive sign features. *International Journal of Industrial Ergonomics*, *40*(6), 689–697. https://doi.org/10.1016/j.ergon.2010.05.002

Cox, A. L., Gould, S. J. J., Cecchinato, M. E., Iacovides, I., & Renfree, I. (2016). Design Frictions for Mindful Interactions: The Case for Microboundaries. *Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems - CHI EA '16*, 1389–1397. https://doi.org/10.1145/2851581.2892410

Cranor, L. F. (2021). Informing California privacy regulations with evidence from research. *Communications of the ACM*, *64*(3), 29–32. https://doi.org/10.1145/3447253

Damghanian, H., Zarei, A., & Siahsarani Kojuri, M. A. (2016). Impact of Perceived Security on Trust, Perceived Risk, and Acceptance of Online Banking in Iran. *Journal of Internet Commerce*, *15*(3), 214–238. https://doi.org/10.1080/15332861.2016.1191052

Distler, V., Lallemand, C., & Koenig, V. (2020). Making Encryption Feel Secure: Investigating how Descriptions of Encryption Impact Perceived Security. *The 5th European Workshop on Usable Security (EuroUSEC)*, 10.

Distler, V., Lenzini, G., Lallemand, C., & Koenig, V. (2020). The Framework of Security-Enhancing Friction: How UX Can Help Users Behave More Securely. *New Security Paradigms Workshop 2020*, 45–58. https://doi.org/10.1145/3442167.3442173

Distler, V., Zollinger, M.-L., Lallemand, C., Roenne, P. B., Ryan, P. Y. A., & Koenig, V. (2019). Security—Visible, Yet Unseen? *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, 1–13.

Dosso, C., & Chevalier, A. (2021). How do older adults process icons during a navigation task? Effects of aging, semantic distance, and text label. *Educational Gerontology*, *47*(3), 132–147. https://doi.org/10.1080/03601277.2021.1886634

Dourish, P, Grinter, R. E., de la Flor, J. D., & Joseph., M. (2004). Security in the Wild: User Strategies for Managing Security as an Everyday, Practical Problem. *Personal and Ubiquitous Computing*, *8*.

Dourish, Paul, & Redmiles, D. (2002). An Approach to Usable Security Based on Event Monitoring and Visualization. *Proceedings of the 2002 Workshop on New Security Paradigms*, 75–81. https://doi.org/10.1145/844102.844116

Edwards, W. K., Poole, E. S., & Stoll, J. (2008). Security automation considered harmful? *Proceedings of the 2007 Workshop on New Security Paradigms - NSPW '07*, 33. https://doi.org/10.1145/1600176.1600182

Egelman, S., Kannavara, R., & Chow, R. (2015). Is This Thing On?: Crowdsourcing Privacy Indicators for Ubiquitous Sensing Platforms. *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, 1669–1678. https://doi.org/10.1145/2702123.2702251

Fahl, S., Harbach, M., Muders, T., Smith, M., & Sander, U. (2012). Helping Johnny 2.0 to encrypt his Facebook conversations. *Proceedings of the Eighth Symposium on Usable Privacy and Security - SOUPS '12*, 1. https://doi.org/10.1145/2335356.2335371

Fassl, M., Gröber, L., & Krombholz, K. (2021). Exploring User-Centered Security Design for Usable Authentication Ceremonies. *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, 15.

Felt, A. P., Ainslie, A., Reeder, R. W., Consolvo, S., Thyagaraja, S., Bettes, A., Harris, H., & Grimes, J. (2015). Improving SSL Warnings: Comprehension and Adherence. *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems - CHI '15*, 2893–2902. https://doi.org/10.1145/2702123.2702442

Felt, A. P., Reeder, R. W., Ainslie, A., Harris, H., Walker, M., Thompson, C., Acer, M. E., Morant, E., & Consolvo, S. (2016). Rethinking Connection Security Indicators. *Twelfth*

Symposium on Usable Privacy and Security (SOUPS 2016), 1–14. https://www.usenix.org/conference/soups2016/technical-sessions/presentation/porter-felt

Gallagher, K., Patil, S., & Memon, N. (2017). New Me: Understanding Expert and Non-Expert Perceptions and Usage of the Tor Anonymity Network. *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*, 385–398. https://www.usenix.org/conference/soups2017/technical-sessions/presentation/gallagher

Gaw, S., Felten, E. W., & Fernandez-Kelly, P. (2006). Secrecy, flagging, and paranoia: Adoption criteria in encrypted email. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 591–600). Association for Computing Machinery. https://doi-org.proxy.bnl.lu/10.1145/1124772.1124862

Hassenzahl, M. (2001). The Effect of Perceived Hedonic Quality on Product Appealingness. *International Journal of Human-Computer Interaction*, *13*(4), 481–499. https://doi.org/10.1207/S15327590IJHC1304_07

Hassenzahl, M. (2008). User experience (UX): Towards an experiential perspective on product quality. *Proceedings of the 20th Conference on l'Interaction Homme-Machine*, 11–15.

Hassenzahl, M., Burmester, M., & Koller, F. (2003). AttrakDiff: Ein Fragebogen zur Messung wahrgenommener hedonischer und pragmatischer Qualität. In G. Szwillus & J. Ziegler (Eds.), *Mensch & Computer 2003* (Vol. 57, pp. 187–196). Vieweg+Teubner Verlag. https://doi.org/10.1007/978-3-322-80058-9_19

Hassenzahl, M., Eckoldt, K., Diefenbach, S., Laschke, M., Len, E., & Kim, J. (2013). Designing moments of meaning and pleasure. Experience design and happiness. *International Journal of Design*, *7*(3).

Huang, H., Yang, M., Yang, C., & Lv, T. (2019). User performance effects with graphical icons and training for elderly novice users: A case study on automatic teller machines. *Applied Ergonomics*, *78*, 62–69. https://doi.org/10.1016/j.apergo.2019.02.006

International Organization for Standardization. (2018). *Ergonomics of human-system interaction—Part 11: Usability: Definitions and concepts (Standard No. 9241-11:2018)*. https://www.iso.org/obp/ui/#iso:std:iso:9241:-11:ed-2:v1:en

Ion, I., Reeder, R., & Consolvo, S. (2015). "...No one Can Hack My Mind": Comparing Expert and Non-Expert Security Practices. *Eleventh Symposium On Usable Privacy and*

Security (SOUPS 2015), 327–346. https://www.usenix.org/conference/soups2015/proceedings/presentation/ion

Khan, I. U., Hameed, Z., & Khan, S. U. (2017). Understanding Online Banking Adoption in a Developing Country: UTAUT2 with Cultural Moderators. *Journal of Global Information Management*, *25*(1), 43–65. https://doi.org/10.4018/JGIM.2017010103

Krug, S. (2000). *Don't make me think!: A common sense approach to Web usability*. Pearson Education India.

Laugwitz, B., Held, T., & Schrepp, M. (2008). Construction and Evaluation of a User Experience Questionnaire. In A. Holzinger (Ed.), *HCI and Usability for Education and Work* (Vol. 5298, pp. 63–76). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-540-89350-9_6

Lausch, J., Wiese, O., & Roth, V. (2017). What is a Secure Email? *Proceedings 2nd European Workshop on Usable Security*. European Workshop on Usable Security, Paris, France. https://doi.org/10.14722/eurousec.2017.23022

Lim, S. H., Kim, D. J., Hur, Y., & Park, K. (2019). An Empirical Study of the Impacts of Perceived Security and Knowledge on Continuous Intention to Use Mobile Fintech Payment Services. *International Journal of Human–Computer Interaction*, *35*(10), 886–898. https://doi.org/10.1080/10447318.2018.1507132

Mahlke, S. (2008). *User experience of interaction with technical systems* [Doctoral dissertation.].

Majrashi, K. (2020). Performance of mobile users with text-only and text-and-icon menus in seated and walking situations. *Behaviour & Information Technology*, 1–19. https://doi.org/10.1080/0144929X.2020.1795257

Marky, K., Kulyk, O., Renaud, K., & Volkamer, M. (2018). What Did I Really Vote For? *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems - CHI '18*, 1–13. https://doi.org/10.1145/3173574.3173750

McDougall, S., Reppa, I., Kulik, J., & Taylor, A. (2016). What makes icons appealing? The role of processing fluency in predicting icon appeal in different task contexts. *Applied Ergonomics*, *55*, 156–172. https://doi.org/10.1016/j.apergo.2016.02.006

Murillo, A., Kramm, A., Schnorf, S., & Luca, A. D. (2018). "If I press delete, it's gone"—User Understanding of Online Data Deletion and Expiration. *Fourteenth Symposium on*

Usable Privacy and Security (SOUPS 2018), 329–339. https://www.usenix.org/conference/soups2018/presentation/murillo

Özlen, M. K., & Djedovic, I. (2017). Online banking acceptance: The influence of perceived system security on perceived system quality. *Journal of Accounting and Management Information Systems*, *16*(1), 164–178. https://doi.org/10.24818/jamis.2017.01008

Pagter, J. I., & Petersen, M. G. (2007). A Sense of Security in Pervasive Computing—Is the Light on When the Refrigerator Door Is Closed? *International Conference on Financial Cryptography and Data Security*, 383–388.

Panditrao, S., O'Brien, D., & Stark, E. (2021, July 14). Increasing HTTPS adoption. Chromium Blog. https://blog.chromium.org/2021/07/increasing-https-adoption.html

Petitpas, A., Jaquet, J. M., & Sciarini, P. (2020). Does E-Voting matter for turnout, and to whom? *Electoral Studies*, 102245. https://doi.org/10.1016/j.electstud.2020.102245

Rogers, Y. (1989). Icons at the interface: Their usefulness. *Interacting with Computers*, *1*(1), 105–117. https://doi.org/10.1016/0953-5438(89)90010-6

Ruoti, S., Kim, N., Burgon, B., van der Horst, T., & Seamons, K. (2013). Confused Johnny: When automatic encryption leads to confusion and mistakes. *Proceedings of the Ninth Symposium on Usable Privacy and Security - SOUPS '13*, 1. https://doi.org/10.1145/2501604.2501609

Ryan, P. Y., Rønne, P. B., & Iovino, V. (2016). Selene: Voting with transparent verifiability and coercion-mitigation. *International Conference on Financial Cryptography and Data Security*, 176–192.

Schechter, S. E., Dhamija, R., Ozment, A., & Fischer, I. (2007). *The Emperor's New Security Indicators*. 51–65. https://doi.org/10.1109/SP.2007.35

Schrepp, M., Hinderks, A., & Thomaschewski, J. (2017). Design and Evaluation of a Short Version of the User Experience Questionnaire (UEQ-S). *International Journal of Interactive Multimedia and Artificial Intelligence*, *4*, 103. https://doi.org/10.9781/ijimai.2017.09.001

Sheldon, K. M., Elliot, A. J., Kim, Y., & Kasser, T. (2001). What is satisfying about satisfying events? Testing 10 candidate psychological needs. *Journal of Personality and Social Psychology*, *80*(2), 325.

Spero, E., & Biddle, R. (2020). Out of Sight, Out of Mind: UI Design and the Inhibition of Mental Models of Security. *New Security Paradigms Workshop 2020*, 127–143. https://doi.org/10.1145/3442167.3442174

Vance, A., Lowry, P. B., & Eggett, D. (2015). Increasing Accountability Through User-Interface Design Artifacts: A New Approach to Addressing the Problem of Access-Policy Violations. *MIS Quarterly*, *39*(2), 345–366. https://doi.org/10.25300/MISQ/2015/39.2.04

Vassil, K., Solvak, M., Vinkel, P., Trechsel, A. H., & Alvarez, R. M. (2016). The diffusion of internet voting. Usage patterns of internet voting in Estonia between 2005 and 2015. *Government Information Quarterly*, *33*(3), 453–459. https://doi.org/10.1016/j.giq.2016.06.007

Vaziripour, E., Wu, J., O'Neill, M., Whitehead, J., Heidbrink, S., Seamons, K., & Zappala, D. (2017). Is that you, Alice? A Usability Study of the Authentication Ceremony of Secure Messaging Applications. *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*, 29–47. https://www.usenix.org/conference/soups2017/technical-sessions/presentation/vaziripour

Wallander, L. (2009). 25 years of factorial surveys in sociology: A review. *Social Science Research*, *38*(3), 505–520. https://doi.org/10.1016/j.ssresearch.2009.03.004

Whitten, A., & Tygar, J. D. (1999). A Usability Evaluation of PGP 5.0. *Proceedings of the 8th USENIX Security Symposium*, 169–183.

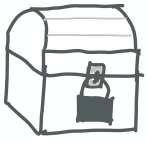
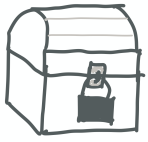
Wiedenbeck, S. (1999). The use of icons and labels in an end user application program: An empirical study of learning and retention. *Behaviour & Information Technology*, *18*(2), 68–82. https://doi.org/10.1080/014492999119129

Wogalter, M. S., Silver, N. C., Leonard, S. D., & Zaikina, H. (2006). Warning Symbols. In M. S. Wogalter (Ed.), *Handbook of Warnings* (pp. 159–176). CRC Press. https://doi.org/10.1201/9781482289688

6.10. Appendices

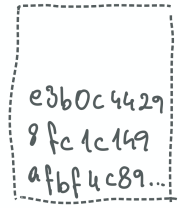
6.10.1. Expert co-creation – Additional Details

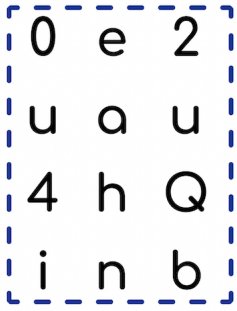
Below, we summarize the results from the expert ideation phase (1), the selection and improvement with HCI experts (2), the final selection by security experts (3), and the final visual representations that were created by a designer (4). The last column shows the visual representations that we used for the visual representations in the vignettes.

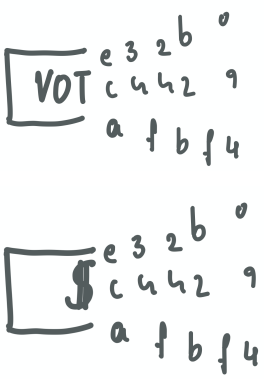
1) First ideation with security experts	2) Selection and improvement with HCI experts	3) Final selection of visual representations	4) Final visual representations by designer
			
			
			
			
			

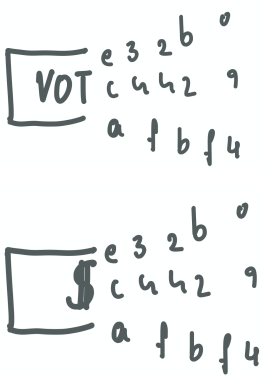
e3b0c4429
8fc1c149
afbf4c89...

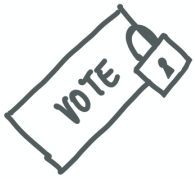
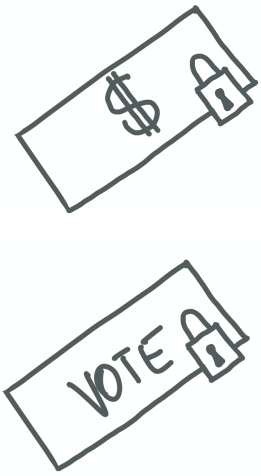
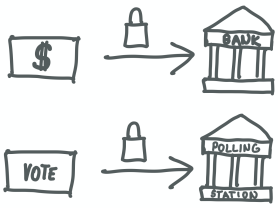
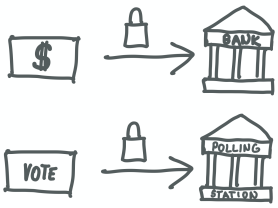
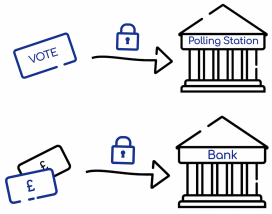
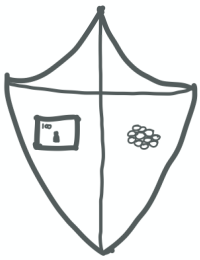
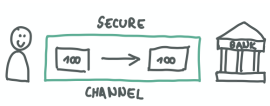
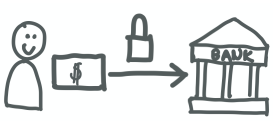
the actual ciphertext

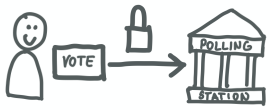
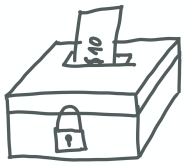
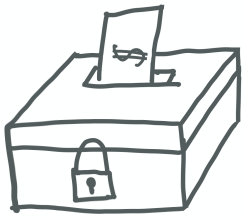
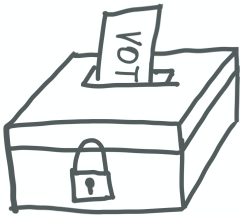
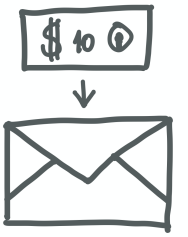
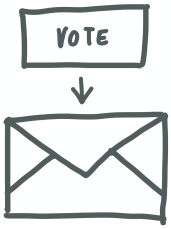
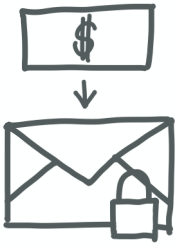
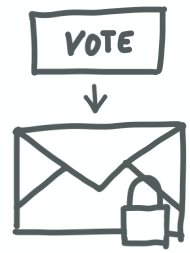
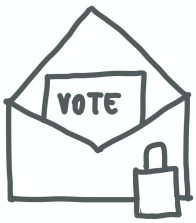
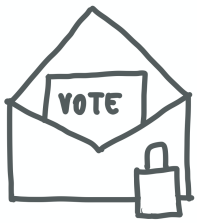








 VOTE	 $ VOTE		
 VOTE			
 VOTE 1 VOTE 2 VOTE 3			
 BANK	 BANK VOTE POLLING STATION	 BANK VOTE POLLING STATION	 VOTE Polling Station Bank
			
 SECURE CHANNEL BANK	 BANK		

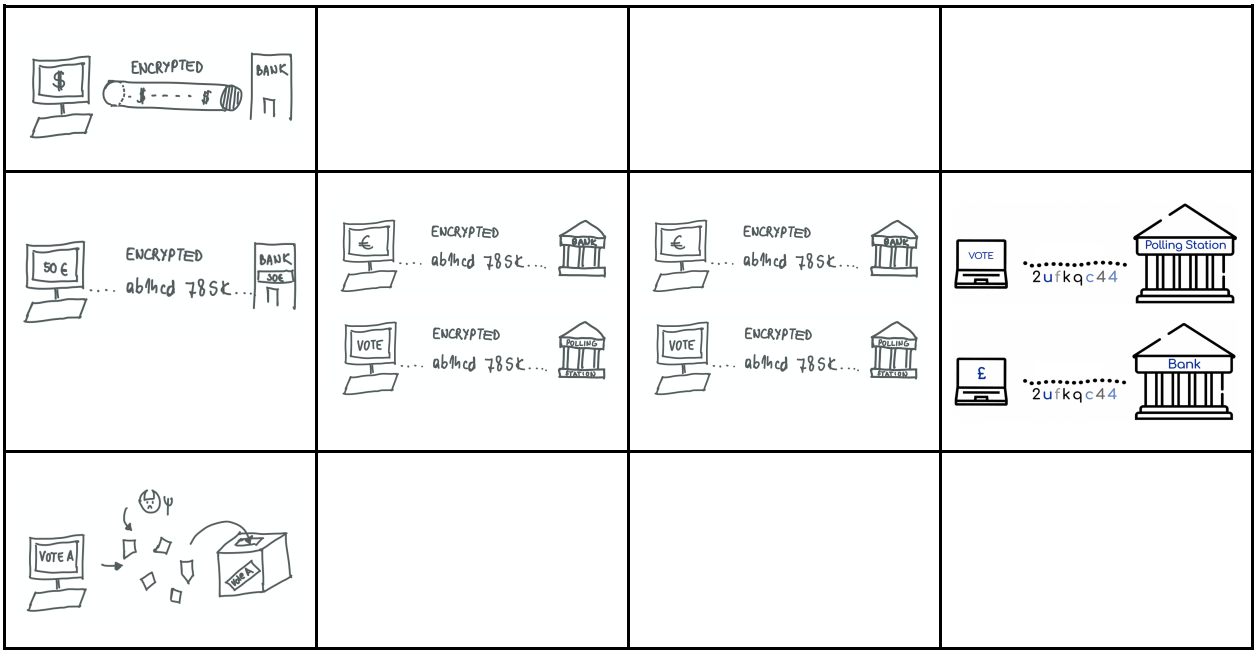


Table 3: Iterations of the visual representations of encryption

6.10.2. Correlations

	Text_1	Text_2	Text_3	Text_4	Visual_1	Visual_2	Visual_3	Visual_4	Visual_5	Visual_6	Male	Female	Non-binary	Gender not listed	Univ. education	Age
Text_1	1.00															
Text_2	-0.32*	1.00														
Text_3	-0.32*	-0.35*	1.00													
Text_4	-0.32*	-0.34*	-0.34*	1.00												
Visual_1	-0.07*	0.05	0.00	0.01	1.00											
Visual_2	0.02	0.04	-0.04	-0.03	-0.21*	1.00										
Visual_3	0.05	-0.06*	0.01	0.00	-0.20*	-0.19*	1.00									
Visual_4	0.05	-0.03	0.00	-0.02	-0.21*	-0.20*	-0.19*	1.00								
Visual_5	-0.04	-0.00	-0.02	0.06*	-0.21*	-0.19*	-0.19*	-0.19*	1.00							
Visual_6	-0.02	0.01	0.03	-0.03	-0.21*	-0.20*	-0.19*	-0.20*	-0.20*	1.00						
Male	-0.01	-0.02	0.04	-0.01	-0.01	-0.03	0.08*	-0.03	-0.02	0.02	1.00					
Female	0.01	0.02	-0.04	0.01	0.01	0.03	-0.09*	0.03	0.03	-0.01	-0.99*	1.00				
Non-binary	-0.00	-0.01	-0.01	0.02	0.00	0.01	0.05	0.01	-0.03	-0.03	-0.05	-0.10*	1.00			

Gender not listed	-0.02	-0.02	-0.02	0.05	-0.01	-0.01	0.07*	-0.01	-0.01	-0.01	-0.02	-0.04	-0.00	1.00		
Univ. education	0.00	-0.04	-0.00	0.04	-0.02	0.00	0.03	0.03	-0.04	-0.00	-0.05	0.05	-0.02	0.03	1.00	
Age	0.00	0.01	-0.01	-0.00	0.02	-0.01	0.03	0.00	0.02	-0.06*	0.08*	-0.07*	-0.03	-0.00	-0.04	1.00

Pairwise correlations between values of vignette variables (as dummies) and respondent gender (as dummies for each category), university education (Bachelor degree and higher as dummy), and age (continuous). Pearson's correlation coefficient. * $p < 0.05$

Table 4: Bivariate Correlations of Vignette Values for Online Banking

	Text_1	Text_2	Text_3	Text_4	Visual_1	Visual_2	Visual_3	Visual_4	Visual_5	Visual_6	Male	Female	Non-binary	Univ. education	Age
Text_1	1.00														
Text_2	-0.33*	1.00													
Text_3	-0.35*	-0.34*	1.00												
Text_4	-0.33*	-0.32*	-0.33*	1.00											
Visual_1	-0.04	0.02	-0.00	0.03	1.00										
Visual_2	0.06	-0.01	-0.02	-0.03	-0.20*	1.00									
Visual_3	-0.02	-0.02	0.04	0.00	-0.20*	-0.21*	1.00								
Visual_4	-0.00	0.06*	-0.03	-0.03	-0.21*	-0.22*	-0.22*	1.00							
Visual_5	0.01	-0.00	0.01	-0.01	-0.18*	-0.19*	-0.19*	-0.20*	1.00						
Visual_6	-0.00	-0.04	0.00	0.04	-0.19*	-0.20*	-0.20*	-0.21*	-0.18*	1.00					
Male	0.06	-0.02	0.01	-0.05	-0.05	-0.03	-0.01	0.08*	0.01	-0.00	1.00				
Female	-0.06	0.02	-0.00	0.05	0.05	0.03	0.00	-0.08*	-0.01	0.01	-0.99*	1.00			
Non-binary	-0.01	0.02	-0.01	-0.01	-0.03	-0.03	0.04	0.00	0.05	-0.03	-0.04	-0.10*	1.00		
Univ. education	-0.01	-0.00	0.05	-0.04	-0.03	-0.00	0.03	0.03	0.02	-0.04	-0.05	0.04	0.06	1.00	
Age	-0.02	0.08*	-0.05	0.00	0.02	-0.02	0.01	0.07*	-0.06	-0.02	0.09*	-0.08*	-0.03	-0.06*	1.00

Pairwise correlations between values of vignette variables (as dummies) and respondent gender (as dummies for each category), university education (Bachelor degree and higher as dummy), and age (continuous). Pearson's correlation coefficient. * $p < 0.05$

Table 5: Bivariate Correlations of Vignette Values for E-Voting

6.10.3. Distribution of rankings

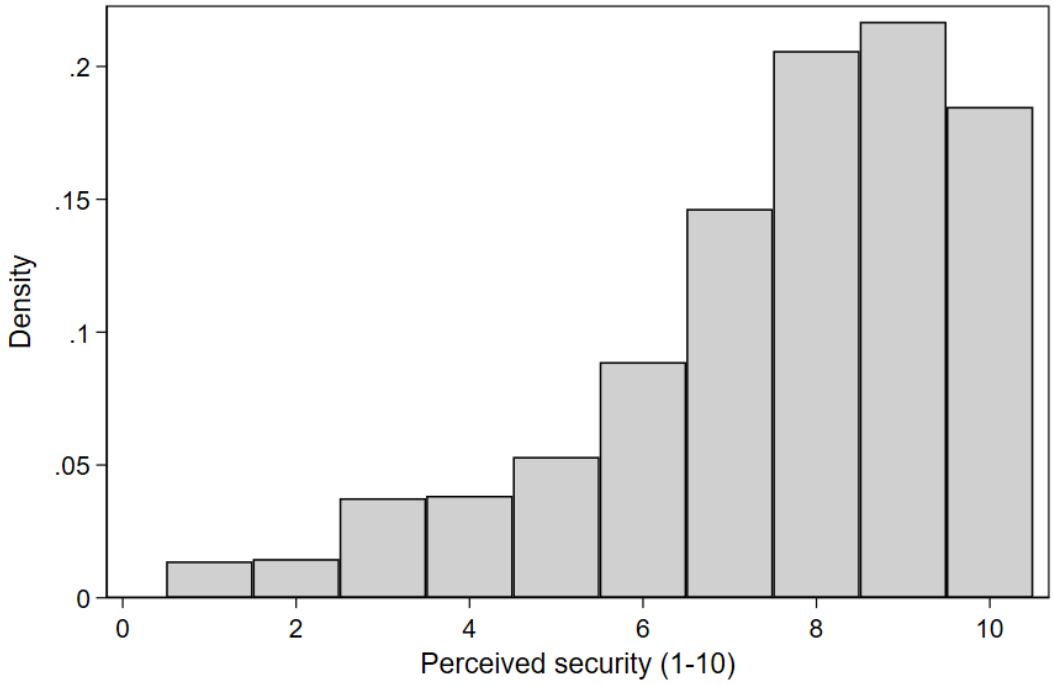


Figure 9: Distribution of rankings of perceived security in online banking context. N=1,093

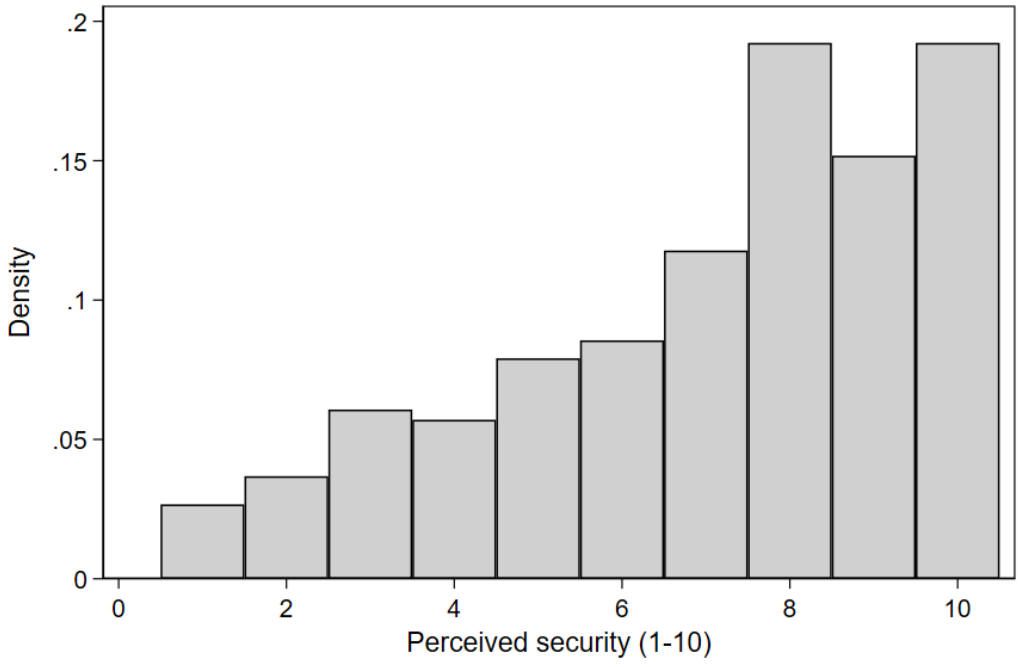


Figure 10: Distribution of rankings of perceived security in e-voting context. N=1,087

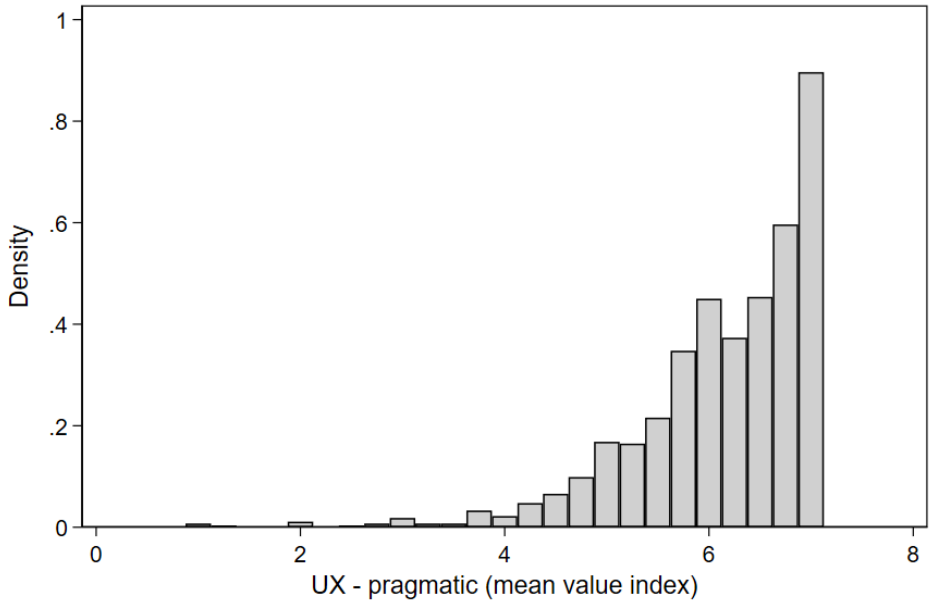


Figure 11: Distribution of rankings of pragmatic quality of UX in online banking context. N=1,093

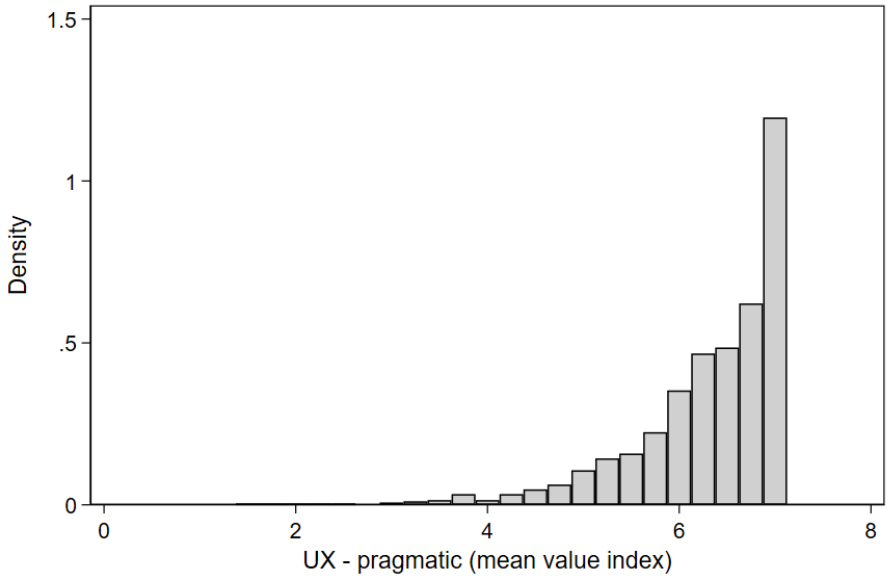


Figure 12: Distribution of rankings of perceived pragmatic quality of UX in e-voting context. N=1,087

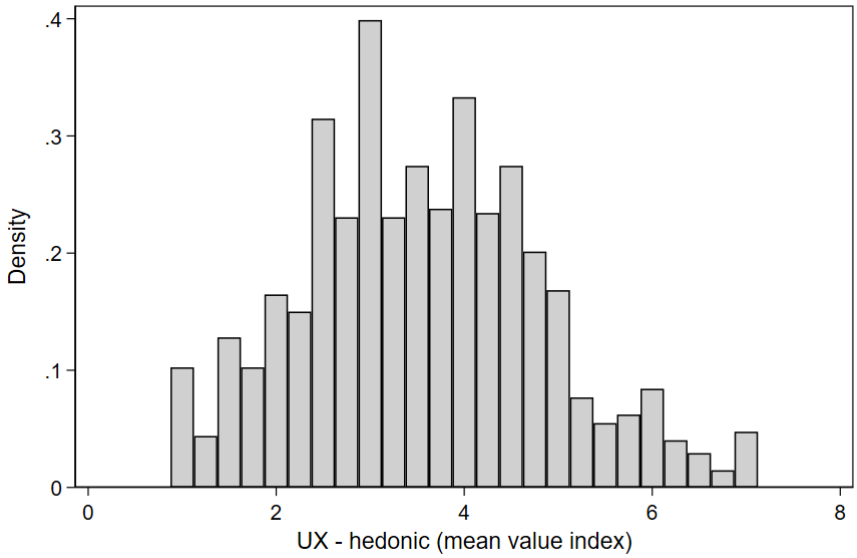


Figure 13: Distribution of rankings of hedonic quality of UX in online banking context. N=1,093

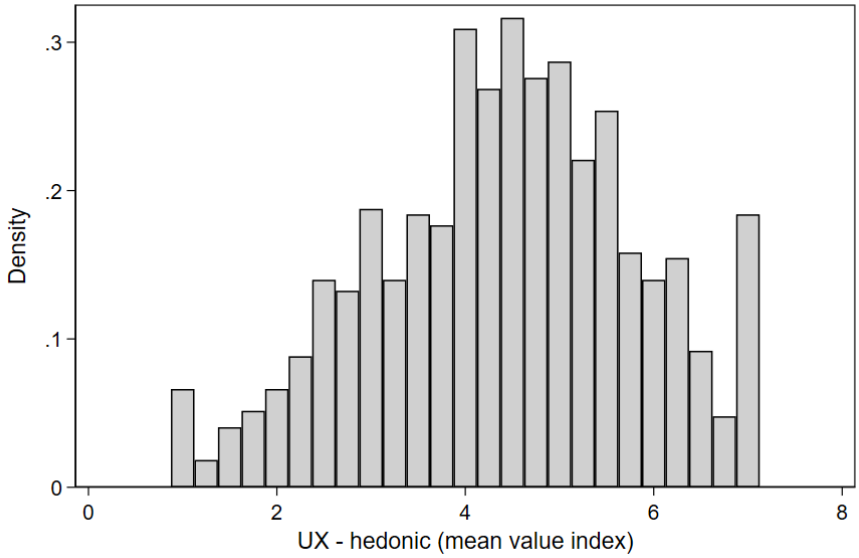


Figure 14: Distribution of rankings of hedonic quality of UX in e-voting context. N=1,087

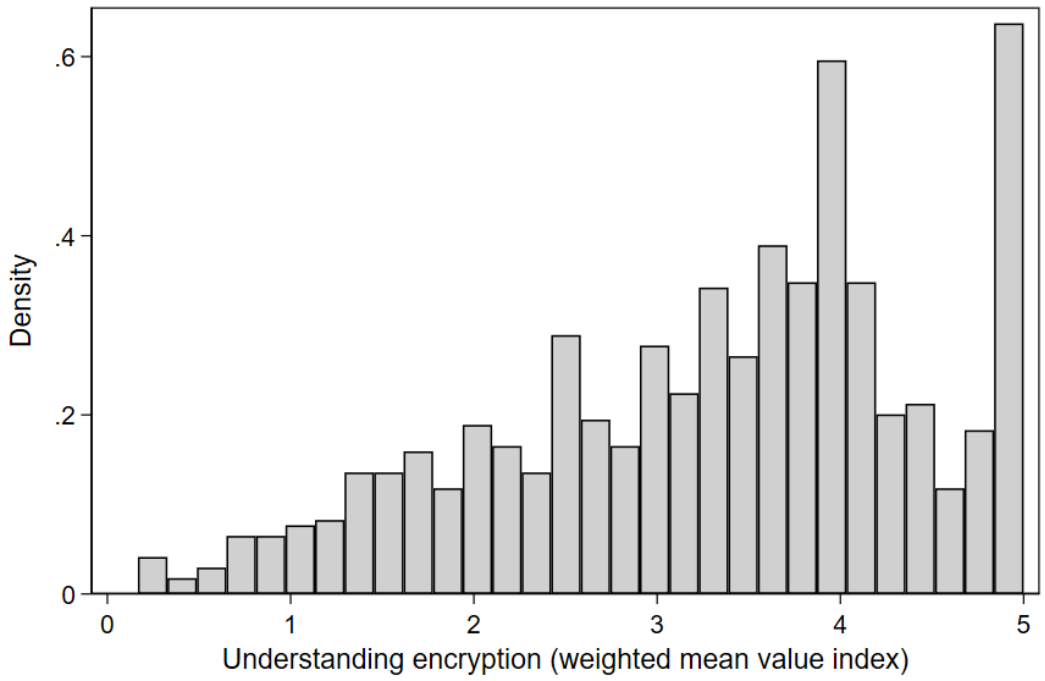


Figure 15: Distribution of rankings of understanding of encryption in online banking context. N=1,093

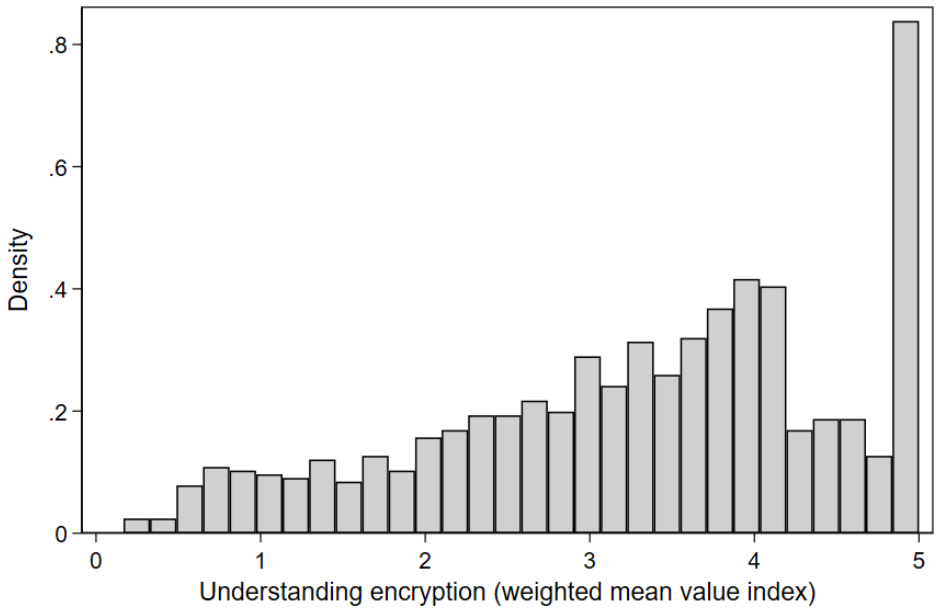


Figure 16: Distribution of rankings of understanding of encryption in e-voting context. N=1,087

6.10.4. Regression tables

	Voting		Banking	
Text representation	0.415*	(0.173)	0.590***	(0.165)
Visual representation	-0.143	(0.209)	0.029	(0.162)
Constant	6.882***	(0.230)	7.102***	(0.198)
Observations	1087		1093	

N= 1,087 in e-voting, N=1,093 in online banking. Dependent variable: perceived security (scale 1-10). Robust standard errors in parentheses.

$^{+}$ $p < .10$, * $p < .05$, ** $p < .01$, *** $p < .001$

Table 6: Perceived security – overall effects of textual and visual representation

	Voting		Banking	
Text: Encrypting your data	0.402+	(0.210)	0.257	(0.192)
Lower complexity description	0.397+	(0.212)	0.741***	(0.189)
Higher complexity description	0.460*	(0.220)	0.696***	(0.192)
Padlock in front of ciphertext	-0.096	(0.260)	-0.052	(0.218)
Vote/Banknote dissolving into ciphertext	-0.191	(0.276)	-0.370+	(0.224)
Vote/Banknote arrow with padlock moving to polling station/bank	-0.024	(0.257)	0.092	(0.208)
Vote/Banknote in envelope	-0.029	(0.277)	0.235	(0.214)
Computer connected to polling station/bank	-0.376	(0.269)	0.142	(0.209)
Constant	6.877***	(0.231)	7.134***	(0.197)
Observations	1087		1093	

N= 1,087 in e-voting, N=1,093 in online banking. Dependent variable: perceived security (scale 1-10). Robust standard errors in parentheses

$^{+}$ $p < .10$, * $p < .05$, ** $p < .01$, *** $p < .001$

Table 7: Perceived security - single effects of the values of textual and visual representation

	Model with interactions	
Text: Encrypting your data	0.408+	(0.210)
Lower complexity description	0.401+	(0.212)
Higher complexity description	0.458*	(0.219)
Online banking	0.376+	(0.210)

Text: Encrypting your data # Online banking	-0.139	(0.285)
Lower complexity description # Online banking	0.351	(0.284)
Higher complexity description # Online banking	0.246	(0.291)
Padlock in front of ciphertext	-0.069	(0.169)
Vote/Banknote dissolving into ciphertext	-0.269	(0.177)
Vote/Banknote arrow with padlock moving to polling station/bank	0.038	(0.165)
Vote/Banknote in envelope	0.110	(0.173)
Computer connected to polling station/bank	-0.107	(0.168)
Constant	6.809***	(0.185)
Observations	2180	

N= 2,180. Dependent variable: perceived security (scale 1-10). Robust standard errors in parentheses

$^{+}p < .10$, $^{*}p < .05$, $^{**}p < .01$, $^{***}p < .001$

Table 8: Regression table for perceived security with interactions

	Voting		Banking	
Text representation	0.060	(0.058)	0.036	(0.062)
Visual representation	-0.066	(0.065)	0.006	(0.072)
Constant	6.309***	(0.072)	6.099***	(0.080)
Observations	1087		1093	

N=1,087 in e-voting, N=1,093 in online banking. Dependent variable: UX-pragmatic quality, mean value index based on four items. Robust standard errors in parentheses

$^{+}p < .10$, $^{*}p < .05$, $^{**}p < .01$, $^{***}p < .001$

Table 9: Pragmatic quality of UX (UX-PQ) – overall effects of textual and visual representation

	Voting		Banking	
Text: Encrypting your data	0.060	(0.070)	0.114	(0.071)
Lower complexity description	0.077	(0.068)	0.045	(0.074)
Higher complexity description	0.028	(0.073)	-0.072	(0.079)
Padlock in front of ciphertext	-0.149+	(0.085)	-0.246*	(0.102)
Vote/Banknote dissolving into ciphertext	-0.020	(0.079)	-0.043	(0.093)
Vote/Banknote arrow with padlock moving to polling station/bank	0.004	(0.081)	0.149+	(0.085)
Vote/Banknote in envelope	-0.073	(0.089)	0.143	(0.092)
Computer connected to polling station/bank	-0.104	(0.089)	0.042	(0.090)

Constant	6.314***	(0.072)	6.102***	(0.079)
Observations	1087		1093	

N=1,087 in e-voting, N=1,093 in online banking. Dependent variable: UX-pragmatic quality, mean value index based on four items. Robust standard errors in parentheses

$^{+}p < .10$, $^{*}p < .05$, $^{**}p < .01$, $^{***}p < .001$

Table 10: Pragmatic quality of UX (UX-PQ) - single effects of the values of textual and visual representation

	Voting		Banking	
Text representation	0.040	(0.098)	0.124	(0.090)
Visual representation	0.187	(0.114)	0.030	(0.102)
Constant	4.223***	(0.130)	3.435***	(0.118)
Observations	1087		1093	

N=1,087 in e-voting, N=1,093 in online banking. Dependent variable: UX-hedonic quality, mean value index based on four items. Robust standard errors in parentheses

$^{+}p < .10$, $^{*}p < .05$, $^{**}p < .01$, $^{***}p < .001$

Table 11: Hedonic quality of UX (UX-HQ) – overall effects of textual and visual representation

	Voting		Banking	
Text: Encrypting your data	-0.003	(0.121)	0.099	(0.111)
Lower complexity description	-0.035	(0.119)	0.141	(0.111)
Higher complexity description	0.134	(0.120)	0.143	(0.112)
Padlock in front of ciphertext	-0.012	(0.147)	-0.078	(0.136)
Vote/Banknote dissolving into ciphertext	0.170	(0.148)	0.147	(0.134)
Vote/Banknote arrow with padlock moving to polling station/bank	0.330*	(0.145)	0.042	(0.132)
Vote/Banknote in envelope	0.244	(0.150)	0.050	(0.132)
Computer connected to polling station/bank	0.217	(0.148)	-0.006	(0.135)
Constant	4.228***	(0.130)	3.433***	(0.118)
Observations	1087		1093	

N=1,087 in e-voting, N=1,093 in online banking. Dependent variable: UX-hedonic quality, mean value index based on four items. Robust standard errors in parentheses

$^{+}p < .10$, $^{*}p < .05$, $^{**}p < .01$, $^{***}p < .001$

Table 12: Hedonic quality of UX (UX-HQ) - single effects of the values of textual and visual representation

	Voting		Banking	
Text representation	0.471***	(0.092)	0.600***	(0.088)

Visual representation	-0.057	(0.101)	0.012	(0.090)
Constant	3.015***	(0.120)	2.839***	(0.110)
Observations	1029		1052	

N=1,087 in e-voting, N=1,093 in online banking. Dependent variable: Understanding of encryption, weighted mean value index based on six items. Robust standard errors in parentheses

$^{+}p < .10$, $^{*}p < .05$, $^{**}p < .01$, $^{***}p < .001$

Table 13: Understanding of encryption – overall effects of textual and visual representation

	Voting		Banking	
Text: Encrypting your data	0.291**	(0.112)	0.386***	(0.108)
Lower complexity description	0.437***	(0.111)	0.659***	(0.104)
Higher complexity description	0.697***	(0.109)	0.780***	(0.101)
Padlock in front of ciphertext	-0.029	(0.130)	0.139	(0.117)
Vote/Banknote dissolving into ciphertext	-0.143	(0.131)	0.044	(0.127)
Vote/Banknote arrow with padlock moving to polling station/bank	0.057	(0.128)	0.035	(0.119)
Vote/Banknote in envelope	-0.031	(0.137)	-0.105	(0.119)
Computer connected to polling station/bank	-0.130	(0.133)	-0.103	(0.119)
Constant	3.008***	(0.119)	2.841***	(0.110)
Observations	1029		1052	

N=1,087 in e-voting, N=1,093 in online banking. Dependent variable: Understanding of encryption, weighted mean value index based on six items. Robust standard errors in parentheses

$^{+}p < .10$, $^{*}p < .05$, $^{**}p < .01$, $^{***}p < .001$

Table 14: Understanding of encryption - single effects of the values of textual and visual representation

	Model with interactions	
Text: Encrypting your data	0.296**	(0.112)
Lower complexity description	0.435***	(0.111)
Higher complexity description	0.699***	(0.109)
Online banking	-0.115	(0.111)
Text: Encrypting your data # Online banking	0.085	(0.155)
Lower complexity description # Online banking	0.219	(0.152)
Higher complexity description # Online banking	0.074	(0.148)
Padlock in front of ciphertext	0.057	(0.087)
Vote/Banknote dissolving into ciphertext	-0.051	(0.091)

Vote/Banknote arrow with padlock moving to polling station/bank	0.049	(0.087)
Vote/Banknote in envelope	-0.070	(0.090)
Computer connected to polling station/bank	-0.116	(0.089)
Constant	2.982***	(0.100)
Observations	2081	

N=2,180. Dependent variable: Understanding of encryption, weighted mean value index based on six items. Robust standard errors in parentheses

$^{+}$ $p < .10$, * $p < .05$, ** $p < .01$, *** $p < .001$

Table 15: Regression table for understanding of encryption with interactions

Chapter 7: The Framework of Security-Enhancing Friction: How UX Can Help Users Behave More Securely

Published as: Distler, V., Lenzini, G., Lallemand, C., & Koenig, V. (2020). The Framework of Security-Enhancing Friction: How UX Can Help Users Behave More Securely. *New Security Paradigms Workshop 2020*, 45–58. https://doi.org/10.1145/3442167.3442173

7.1. Abstract

A growing body of research in the usable privacy and security community addresses the question of how to best influence user behavior to reduce risk-taking. We propose to address this challenge by integrating the concept of user experience (UX) into empirical usable privacy and security studies that attempt to change risk-taking behavior. UX enables us to study the complex interplay between user-related, system-related and contextual factors and provides insights into the experiential aspects underlying behavior change, including negative experiences.

We first compare and contrast existing security-enhancing interventions (e.g., nudges, warnings, fear appeals) through the lens of friction. We then build on these insights to argue that it can be desirable to design for moments of negative UX in security-critical situations. For this purpose, we introduce the novel concept of security-enhancing friction, friction that effectively reduces the occurrence of risk-taking behavior and ensures that the overall UX (after use) is not compromised.

We illustrate how security-enhancing friction provides an actionable way to systematically integrate the concept of UX into empirical usable privacy and security studies for meeting both the objectives of secure behavior and of overall acceptable experience.

7.2. Introduction

Users are exposed to privacy and security risks on a daily basis, and as technology becomes more pervasive, security risks linked to technology use continue to increase [25]. Usable privacy and security (UPS) researchers have developed a wide variety of security-enhancing interventions (e.g., nudges [1], warnings [2, 19], attractors [8, 9], fear appeals [50]) aiming to help users stay secure and protected by avoiding risky behaviors. In this paper, we aim to identify similarities and differences between these interventions, as

security-enhancing interventions are often studied separately, making it difficult to compare their effects. Additionally, there is no standardized way of measuring the effects of such security-enhancing interventions. In particular, there is a lack of systematic measurement of experiential factors, which could provide a nuanced understanding of why interventions correlate with certain behavioral outcomes, and overall experience is not always assessed.

We argue that the field of user experience (UX) can help respond to these challenges, as it holds rich insights into emotional, subjective and temporal aspects that affect how a user perceives their interactions with systems [52]. We believe that applying the concept of friction to address security- and privacy-relevant risk-taking behaviors is a promising direction and a highly relevant way of bridging UX and UPS. We thus introduce the concept of *security-enhancing friction* and describe actionable ways to transfer the concept into practice using the large variety of UX methods already available.

This article makes the following contributions:

- We compare and contrast existing security-enhancing interventions through the lens of friction design.
- We introduce the concept of security-enhancing friction and explain how it can help reduce or prevent risk-taking behaviors while keeping overall UX at an acceptable level, thus further bridging the disciplines of UPS and UX.
- We suggest practical guidelines for the use of UX methods to gain a better understanding of the underlying reasons for privacy- and security-relevant behaviors. In so doing, we contribute to consolidating the objectives of "better security" and "better UX" by developing a framework that integrates both.

7.3. Existing security-enhancing interventions

UPS researchers have designed a large variety of interventions to help people avoid risk-taking behaviors. For the purpose of this article, we term these attempts "security-enhancing interventions", interventions that intend to reduce, avoid, or correct risk-taking behavior. In the following sections, we summarize important attempts that have been made to encourage more secure behavior. The cited studies are meant to be illustrative rather than exhaustive. In selecting which publications to include, we conducted a search of the ACM Digital Library and gave particular attention to studies appearing in top-tier conferences and journals.

7.3.1. Nudges

Thaler and Sunstein [56] describe nudges as thoughtful "choice architecture" that can be used to direct users in beneficial directions, that is, to guide them to make decisions that are beneficial to them, without restricting freedom of choice. Nudging acknowledges that subtle differences in system design (e.g., defaults, saliency of features, or feedback) can impact users' behavior, leading to better or worse outcomes for users [1]. In privacy and security, nudges can guide users to make more privacy-conscious choices. For instance, on social networks, users who attempt to post content publicly can be nudged to reconsider their privacy settings [1]. Another example stems from Twitter, where users are nudged to check their application access settings right after changing their password. This makes it more likely that users will take the suggested action. Nudges can be considered an instance of "soft paternalism" that supports decision-making without restricting the user's choices. Nudges have also been applied to direct users towards more secure public wireless networks [57] and to encourage users to make more privacy-conscious decisions on Facebook and mobile permissions interfaces [61, 62, 64]. Peer et al. [45] studied the impact of personalizing nudges to match people's decision-making styles, rather than using "one-size-fits-all" nudges, and found that personalized nudges can lead to stronger passwords.

Frik et al. [21] explored the use of commitment devices to nudge users towards complying with security mitigations. A commitment device is a mechanism that allows the "present self" to commit to a future action, so that the "future self" is more likely to follow through later. They find that giving people the opportunity to take action at a later time may increase compliance with security mitigations.

Renaud and Zimmermann [51] address the ethical questions related to nudging, which is usually based on the premise that nudging should be done for the good of the nudgee, rather than "for profit" or other objectives that are not beneficial to the nudgee, as criticized by the opponents of nudging. Of course, simply "avoiding" nudges is not a realistic option, since there is no such thing as a neutral choice architecture [1]. For instance, in the context of GDPR consent notices, Utz et al. [59] describe how graphical interface properties such as the position, type of choice and content framing influence people's consent choices. Renaud and Zimmermann [51] suggest a number of guidelines for ethical nudging based on the principles of ethical research: respect for others, beneficence, justice, scientific integrity and social responsibility.

7.3.2. Fear appeals

Fear appeals attempt to scare people into taking a particular recommended action to secure their information and devices [50]. The rationale is that emotions can help prompt action, with fear being a powerful emotion. Fear appeals have been applied in various contexts, including phishing [30] and smartphone locking behavior [3, 48]. Renaud and Dupois [50] point out, however, that strong emotions can backfire, lead to adverse outcomes and be ethically questionable. The authors also emphasize the wide variety of measurements used to evaluate the effectiveness of fear appeals, ranging from post-appeal attitudes, general attitudes, behavioral intentions and attitudes, actual behavior and attitudes, attention and behavioral outcomes. This lack of consensus on what needs to be measured makes it difficult to compare the efficacy of fear appeals across different studies, leading the Renaud and Dupois to call for a recommended experiment design protocol that would make it easier to compare studies.

In addition, it is unclear whether fear appeals actually succeed in inducing fear, with many studies relying on a one-item measure that has been found insufficient to evaluate whether fear was induced [7].

7.3.3. Warnings

Warnings usually aim to remind users about security risks, and are displayed to users when there is a potential threat to information security [63]. While some warnings merely alert users to the presence of a hazard, the most effective warnings generally provide clear instructions about how to avoid it. Effective warnings must capture users' attention and convince them to take an action to avoid or mitigate a hazard [12].

Warnings are frequently used in UPS, for instance in the context of SSL/TLS warnings, where they are intended to guide confused users to a safe path of action [19].

Another case in which warnings seem to produce security-enhancing results comes from a study by Gorksi and colleagues [23], who asked software developers to complete a short set of programming tasks; they were either assigned to the control group (no warnings) or to the test group, which worked with an API version that integrated security warnings providing secure programming tips. The developers who were exposed to the security warnings created significantly more secure code than the developers in the control group. A later participatory design study with software developers found that design guidelines for end-user warnings are only partially applicable to warnings for developers, who were

interested in details such as message classification, title message, code location, link to detailed external resources and color [22].

While warnings have proven effective in many contexts, users become habituated when they are exposed to a large number of warnings. In a 2013 study on SSL, malware and phishing warnings in Chrome and Firefox, Chrome users were significantly more likely to ignore SSL warnings than Firefox users [2]. The authors hypothesize that this might be because Chrome did not have an exception storing mechanism for certificate errors, which could result in many false positives (warnings that are displayed in non-risky situations) and produce habituation, which the authors called "warning fatigue". Both polymorphic warnings and attractors aim to counteract warning fatigue, or habituation following repeated exposure to warnings, and encourage users to pay increased attention to warnings or other messages.

7.3.4. Polymorphic warnings

In order to force users to pay attention to warnings and prevent habituation effects, polymorphic warnings intentionally delay and continuously change the form of the required user inputs [10]. The results demonstrated that users took fewer unjustified risks when presented with polymorphic dialogues compared to traditional warnings. "Audited" polymorphic dialogues, dialogues that warn users that their answers will be forwarded to auditors, who can then quarantine users who provide unjustified answers, performed even better in terms of security, but were not perceived as acceptable. Polymorphic dialogues seem to be more resistant to habituation than static warnings [60], and multiple studies have measured their effect in terms of brain response (functional magnetic resonance imaging or fMRI) [5, 60].

7.3.5. Attractors

Attractors are user interface modifications that attempt to draw users' attention to the most important information for decision-making. These attractors can either be purely visual, or temporarily inhibit dangerous behaviors to redirect users' attention to salient information [9]. Attractors that require the user to interact with the salient information (e.g., retype parts of information) were found to be resistant to habituation [8]. Similarly, Karegar and colleagues [32] investigated the effect of interaction modes and habituation on user attention to privacy notices, concluding that that certain types of interactions (e.g., drag and drop, checkboxes) performed best at getting users' attention.

7.4. Similarities and differences between existing security-enhancing interventions

The security-enhancing interventions described above vary in their level of disruptiveness. To acknowledge these varying levels of disruptiveness, we suggest that security-enhancing interventions can be classified on a scale from high friction to low friction, similarly to how Cranor [12] suggested that "communications that are relevant for security tasks" could be classified on a scale from active (interrupt user's primary task) to passive (available to the user, but easily ignored).

While some of the security-enhancing interventions above are undoubtedly "high friction" and interrupt the user's primary task (warnings, polymorphic warnings), others can be located anywhere on the scale and can take more or less disruptive forms (attractors, fear appeals, nudges) as shown in Figure 1.

Figure 1: Scale of security communications from low friction (no interruption, easily ignored) to high friction (interruptive, cannot be ignored).

Table 1 compares and contrasts existing security-enhancing interventions using the following criteria: the objective the intervention is intended to meet, the intended friction, and how and when the effectiveness of the intervention is measured.

Intervention and Objective	Intended friction	Sample evaluation measures	Time of measurement		
			During	After	Long-term
Nudges – Direct users to more privacy- and security-conscious choices	Low ◂—▸ High	Behavioral intention [57, 64], behavioral data [4, 61, 62], usefulness, willingness to use [62], level of comfort [62, 64], creepiness, perceived control of information disclosure, perceived relevance of information requested, privacy concern [64], understanding, reaction after multiple nudges [4]	[4]	[4, 57, 62, 64]	[61]

Fear appeals – Direct users to more privacy- and security-conscious choices using fear		Perceived vulnerability [30], perceived security [30], fear [30, 48], response efficacy [3, 30, 48], self-efficacy, response costs [3, 30, 48] S/P concerns [3, 48], perceived severity [3, 48], behavior [3, 48], perceived data value [3]		[3, 30, 48]	[3, 48]
Warnings – Direct users to a choice that prevents a specific hazard		Behavioral data (adherence with warnings) [2, 16, 19, 23, 46] understanding of threat source, data risk, and false positives [19], thoughts during exposure to warning, comprehension, attitudes and beliefs, motivation and behavior [16]	[2, 16, 19, 46]	[16, 19, 23, 46]	[16, 19]
Polymorphic warnings – Direct users to a choice that prevents a specific hazard while avoiding habituation effects		Behavioral data (adherence with warnings) [10]; time for completing tasks [10], brain response [5, 60], mouse cursor tracking [5], eye tracking [60]	[5, 10, 60]	[5, 10]	[60]
Attractors – Draw users' atten tion to the most important information		Behavioral data (adherence to recommended action), survey questions on whether participants clicked and whether their decision was informed [9]	[9]	[9]	

Table 1: A comparison of security-enhancing interventions according to their objective, intended friction (representing a range), sample evaluation measures and time of measurement. Note that the intended friction can be lowered through habituation: The first time a user is exposed to a warning, friction may be high, but as they continue to be exposed, habituation could make the friction appear lower.

7.5. Shortcomings of existing security-enhancing interventions

Table 1 compares the interventions' similarities and differences, making some shortcomings apparent:

- The interventions address different focus areas, and are usually studied separately. This makes it hard to compare effectiveness across approaches.
- The sample studies evaluate success very differently, there is no systematic measurement of experiential factors that could provide a nuanced understanding of why interventions correlate with the intended behavioral outcomes, or why they fail.
- The time of measurement also differs substantially across approaches, with most measuring success after exposure. Habituation is not always measured.

- Finally, the interventions are often studied with a focus on the behavioral outcome, that is, whether participants take the intended action; the overall experience and acceptance of the security-enhancing intervention are not always assessed. However, security interventions can lead to negative emotions (e.g., annoyance, circumvention, resignation, avoidance) and could, in the worst-case scenario, lead users to stop using the services that apply such interventions to improve security. Such potential negative outcomes are not always controlled for and mitigated.

In light of the aforementioned difficulties that many security interventions face, we argue that the design of security interventions should build on research from the fields of psychology and user experience, which provide in-depth insights into users' emotions and psychological needs as well as the temporal aspects of the user experience. Building upon these concepts to work towards more secure user behaviors holds the potential to address existing shortcomings.

Therefore, in this paper, we integrate UX theory, in particular research on friction and negative experience, with security research to present a novel, interdisciplinary concept to address the described challenges: security-enhancing friction.

First, it is essential to provide a short overview of UX theory.

7.6. User experience, a good candidate to provide a nuanced understanding of subjective experience

User experience (UX) focuses on emotional, subjective and temporal aspects that play a role when users interact with systems [52], taking into account both hedonic (non-instrumental) and pragmatic (instrumental) qualities of experience [40, 41]. Pragmatic qualities are similar to the aspects measured by usability, which has traditionally focused on improving “the extent to which a product can be used by specified users to achieve specified goals with effective-ness, efficiency and satisfaction in a specified context of use” (ISO 9241-11). Pragmatic qualities can also be described as “a product’s perceived ability to support the achievement of do-goals” [37], such as sending a text message to someone. Pragmatic qualities relate to the functionality and utility of the product, while hedonic qualities refers to a product’s perceived ability to support the achievement of “be-goals”, such as “being competent” or “being special”. Hassenzahl [27] argues that the fulfilment of be-goals is the driver of experience, meaning that hedonic quality contributes

directly to the core of positive experience. The fulfilment of do-goals can often be seen as a means to fulfilling be-goals. Standardized scales for measuring UX include the Attrakdiff scale, which measures UX along the dimensions of hedonic and pragmatic qualities [28] and the UEQ, which evaluates UX along the dimensions of attractiveness, perspicuity, efficiency, dependability, stimulation, and novelty [36].

Positive experiences are considered to result from fulfilling the human needs for autonomy, competence, security, relatedness, self-actualization/meaning, physical thriving, pleasure/stimulation, money/luxury, self-esteem and popularity/influence [55]. UX is a multi-faceted concept, and security-enhancing interventions can impact different dimensions of UX to varying degrees. For instance, we can hypothesize that an attractor (described in Section 7.3.5.) that temporarily inhibits an action could create a moment of negative UX, since the pragmatic quality (achievement of do-goals) of the experience is momentarily compromised, but a carefully designed attractor might not have a negative impact on the overall experience, given that the user's psychological needs for security and competence are fulfilled thanks to the slower interaction. A momentary interruption in the user's action does not necessarily have a negative impact when the user reflects back on the experience.

Thus, when discussing UX, it is important to be conscious of the fact that UX can refer to various time frames (Figure 2). Depending on the context, researchers might be interested in momentary UX (a specific change in feeling during an interaction), episodic UX (perceptions related to a specific usage period) or cumulative UX (views on a system after having used it for a while) [52].

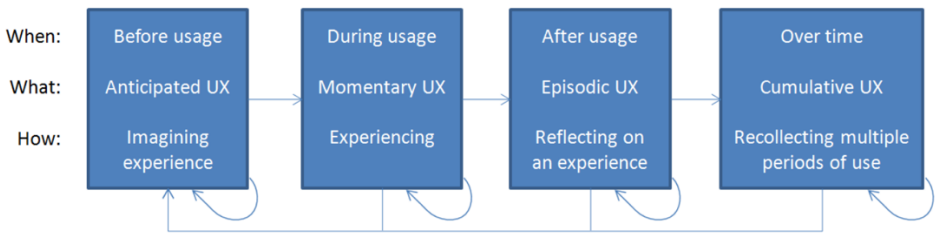


Figure 2: The temporal dynamics of UX [52].

7.7. Designing for negative experience and friction

UX theory and practice tend to focus on positive experiences, leaving many open questions on how negative experiences are created and the effects they may have. To apply UX

theory in UPS, we need to take a closer look at negative experiences. In this section, we describe work on negative experiences and build on these examples to illustrate what security-enhancing friction might look like.

Fokkinga and Desmet [20] suggest enriching UX by purposefully involving negative emotions in user-product interaction. They develop the rich experience framework, which combines a negative stimulus that triggers a negative emotion (e.g., anger, sadness, frustration) with protective frames. Their approach involves three steps, in which the designer decides (1) which negative emotion to incorporate into the design, (2) how and when to elicit it and (3) which protective frame to use. The protective frame is defined as an element that takes away the unpleasant aspects of the negative emotions to allow the user to enjoy their beneficial aspects. For example, seeing a lion triggers fear in most people. Adding a protective frame (a cage) to the experience makes it a positive experience. Without fear, the experience would not be enjoyable, as an empty cage would be dull. The authors suggest that there are four types of protective frames: the safety-zone frame (people perceive negative a stimulus but feel protected from it), the detachment frame (people observe an event without participating in it, e.g., watching a movie), control frame (people are in the danger zone but trust they have the skills to protect themselves from harm) and the perspective frame. The perspective frame provides a window to the wider implications of a situation. For instance, one participates in a charity run and feels tired, yet the experience is positive since the pain contributes to an important cause.

Cox and colleagues [11] also highlight that designing friction into interactions by introducing “microboundaries” can have positive effects. The authors define microboundaries as interventions that provide a small obstacle that prevents users from rushing from one context to another by creating a brief moment of reflection. They define design frictions as points of difficulty encountered during users’ interaction with a technology and describe their potential advantages, such as reducing the likelihood of errors in data entry tasks or supporting health behavior change. They suggest that introducing friction into experiences can disrupt automatic, “mindless” interactions with positive effects, which seems relevant for the security context. The authors compare microboundaries to a smaller version of keeping a credit card encased in a block of ice: you can still get the card out and make purchases, but the time needed for the ice to melt away allows you to think about whether you really want to spend the money.

Studies on design friction indicate that friction might be a powerful way to help people avoid undesirable behaviors, such as wasting electricity [34] or procrastination [35], and instead adopt a "desirable" behavior (help the user attain their goals, living a more energy-efficient life). In order to help people engage in their desired behaviors (e.g., working out or cleaning) instead of procrastinating, Laschke et al. design an object that introduces friction when the user procrastinates by dropping a puck representing the desired task to the floor [35]. This friction intervention induced reflection about procrastination and behavioral change. Another study [34] designed friction to combat standby power consumption by creating a caterpillar-like object connected to a device's power cord. It "breathes slowly" during normal power consumption, but friction is introduced as soon as the device is left in standby mode, wasting energy. The caterpillar starts twisting awkwardly, creating a link between the abstract concept of energy use and the consequences for the environment. The authors suggest using feedback designed to create situational friction as a way of disrupting routines and suggesting alternative courses of action, while still being perceived as acceptable and meaningful [34]. In some instances, friction can intentionally slow down and interaction to reassure users. For example, a time bar indicating the progress of sending an email can reassure people that their email is being sent; it also provides room for an undo in case of a quick change of mind or a "send" pressed by mistake.

We define friction as follows:

Friction is a momentary perturbation in an otherwise uninterrupted interaction that a user has with a system that does not compromise the user's experience in the long run or disrupt the user's trust in the service.

In Section 7.8.1., we will reflect on how friction can be used to discourage insecure behaviors in digital spaces, but for the time being, let us consider examples of friction that are already used to discourage unsafe behavior in the physical world, for example, while driving.

7.7.1. Friction in the physical world

Figure 3 shows an example of friction in the physical world. **Speed bumps** are commonly used to discourage drivers from going too fast by introducing friction into the road that the driver cannot avoid. In theory, the option to speed is still open to the driver, but it is easier and more comfortable to adopt the safe behavior of slowing down than to opt for the unsafe

option. Another interesting attribute of the pictured speed bump is that it allows bicycles to pass by on the side without slowing down. We can see this as symbolic for different types of users, some of which need to be exposed to friction to adopt better behaviors, while others do not. It is also important that friction is used in contexts where it is useful (e.g., speed bumps before pedestrian crossings) rather than in places where it may seem superfluous.

Figure 3: Friction in the physical world: speed bumps are used to encourage vehicles to adopt the safer behavior: slowing down. In digital spaces, friction can help encourage a large variety of secure behaviors beyond slowing users down. (Picture by the authors)

If the driver understands the reason of the bumper, for example, close to a school, they may eventually adopt that behavior automatically. In general, however, it is not required that users understand the reason of a friction, or even that they realize the presence of friction, for the friction to have an effect on the users' behavior. A modern ATM machine that delays a user's taking back the money only after they removed the card, eventually will change how users act while withdrawing money, having helped them to grow the habit to expect to see and take back the card first and then the money, which is the reason why the friction was introduced in the first place.

Of course, this example of friction in the real world has some limitations that we can overcome in digital spaces. In this example, the behavior we want to discourage is speeding, and the intended behavior is driving more slowly. In the digital world, simply slowing users down would not always be our sole objective. Instead, we want to redirect their actions to a more secure path, making insecure behaviors harder or less comfortable, and making the encouraged behavior easier to adopt and more comfortable in comparison.

While the option to engage in the insecure behavior remains available, the secure behavior is relatively easier to choose.

Another example of friction in the physical world is **rumble strips on highways**. When a driver starts to leave their lane, thus attempting to engage in unsafe behavior, these strips introduce physical friction. Instead of encouraging drivers to slow down, they direct them back to the safe course of action and encourage them to stay in their lane.

Friction is frequently used to improve safety in contexts beyond driving. Firearms include safety mechanisms to prevent accidental firing, child-proof medication bottles use a push-and-turn mechanism to make access more difficult for children. In contexts where security and safety are of highest importance, two persons with separate sets of credentials can be required to perform a high-risk action, from accessing data to launching missiles.

These examples of friction in the physical world demonstrate how friction can encourage certain behaviors over others. Similar approaches are used in the digital sphere. According to this definition, fear appeals [3, 30, 48], for instance, are attempts to design for friction with short spikes of fear in order to make users behave more securely. However, taking up the notion of friction from a UX perspective, there are several more dimensions we can consider with respect to a negative experience. These call for a better understanding of the interplay between momentary friction, subjective user perceptions, emotions and, eventually, behavioral change for better security. To incorporate these dimensions, we introduce a new concept, which we call "security-enhancing friction".

7.8. Introducing security-enhancing friction

Based on the theoretical foundations presented in Section 7.7, we define security-enhancing friction as follows:

Security-enhancing friction is friction that is designed to mitigate the risk of a certain attack by lowering the occurrence of risk-taking behavior without affecting overall episodic UX. Security-enhancing friction can encourage a defined, more secure behavior. Security-enhancing friction may have a momentary negative effect on a user’s UX, but overall UX remains within acceptable levels to avoid disuse.

As described in this definition, and as shown in Figure 4, security-enhancing friction causes a short spike in negative UX, which then recovers to an acceptable level to avoid disuse.

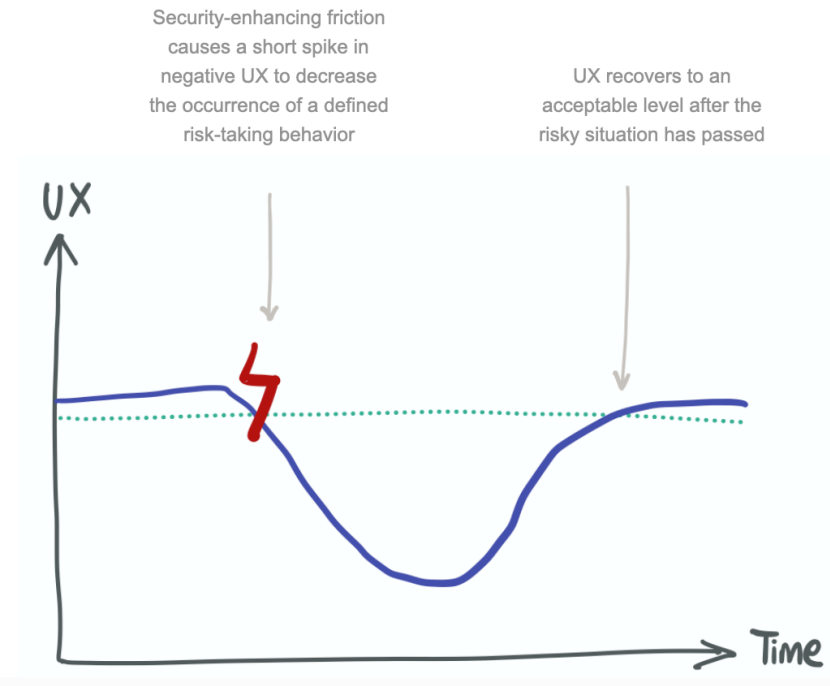


Figure 4: The impact of security-enhancing friction on UX. After the risky situation has passed, UX recovers to an acceptable level.

The definition suggests that we can assess whether a perturbation qualifies as friction by applying UX methods. In order to decide whether a friction is "security-enhancing", however, we need to compare it to a solution without friction or with another type of friction so that we can observe its effect on the occurrence of a defined risky behavior. By measuring the occurrence of secure/insecure behavior and UX in combination, we can avoid security interventions that lead to bad UX, and in the worst case, disuse.

What is the advantage of introducing the concept of security-enhancing friction?

Security-enhancing friction, as a concept:

- Helps design interactions that encourage users to avoid risk-taking behaviors while keeping overall UX at an acceptable level, thus contributing to bridging UX theory and usable privacy and security with a useful framework that systematically considers both security concerns and UX concerns. Security-enhancing friction can help avoid interactions that are perceived as "too annoying" or disruptive, and thus avoid disuse of secure technologies.
- Provides a new perspective for understanding security-enhancing interventions through the lens of friction.

- Encourages the use of methods from the fields of psychology and UX to gain a better understanding of the psychological reasons why people engage in certain behaviors. It attempts to facilitate the transfer to practice by providing a set of methods that can be combined to measure the effect of the intervention on security-relevant behavior and on a given user's experience (both momentary and overall).

We can use the insights from negative experience design described in the previous section to suggest examples of security-enhancing friction.

7.8.1. Examples of security-enhancing friction

In the digital realm, there are various ways friction can be used to improve security behaviors in design interventions. We will discuss three examples that can improve security behaviors while also providing acceptable UX: password meters, anti-phishing interventions, and SSL/TSL warnings. Note that these examples, and the impact of the described friction design on UX, still need to be backed up by empirical data (as described in Section 7.10.). We use them here to illustrate the concept of security-enhancing friction.

7.8.1.1. Password meters

Password meters indicate whether a user's password is strong or weak (for an example, see Figure 5). They can employ a variety of interaction attributes, including the strategic use of colors, a comparison to other people's passwords [17], size of the password meter, presence of suggestions for improvement, or the presence of a visual indicator vs. text only [58]. Overall, they have a positive impact on the security of chosen passwords [17, 58].

- Insecure behavior that should be avoided: Use of “insecure” passwords.
- Intended behavior: Set password that is harder to crack.
- Interaction attributes used to induce friction: Colors, comparison to others' passwords, size of password meter, presence of suggestions for improvement.
- UX is acceptable because: Users can easily evaluate the progress they have made in coming up with a more secure password.

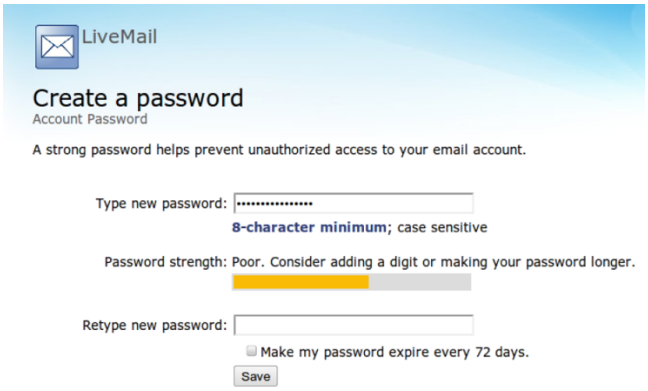


Figure 5: Example of the password meters studied by Ur et al. [58]. Appearance and scoring changed depending on the condition.

7.8.1.2. Anti-phishing intervention

The second example builds on ideas from Bravo-Lillo and colleagues [8, 9], who successfully tested interventions similar to Figure 6 in the context of plugin installation dialogues. Turning to the context of phishing attempts, we can imagine a system that recognizes suspicious elements in an email, such as a button whose text (e.g., "Go to Amazon") does not match the associated URL (e.g., "amaz0n.com"). By asking the user to re-type the security-relevant information (the URL), security-enhancing friction could help re-direct the user's attention and encourage the safer behavior. It is crucial, of course, that such warnings do not appear every time users want to click on a link in an email. Instead, such pop-ups should be a rare exception whenever suspicious elements are discovered in an email.

- Insecure behavior that should be avoided: Clicking mindlessly on a link in an email that seems to be a phishing attempt.
- Intended behavior: Verify certain properties of the email (e.g., sender address, contextual cues, does the URL correspond to what the button says).
- Interaction attributes used to induce friction: Color, contrast, de-activated button, re-typing security-relevant information.
- UX is acceptable because: the threat is clear, the interruption is short.

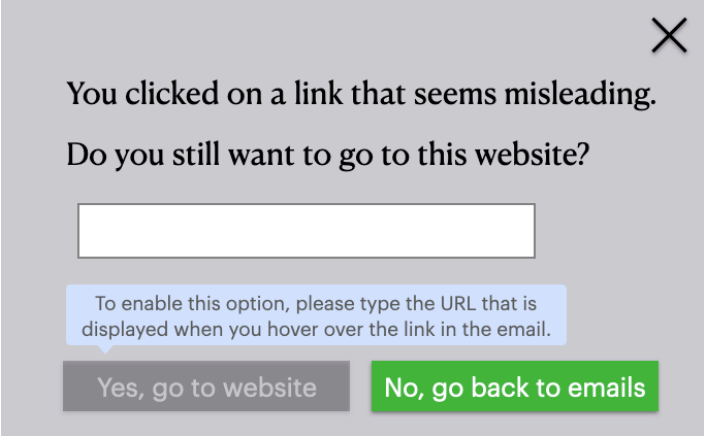


Figure 6: To protect against phishing attempts, security-enhancing friction can be used when a link is recognized as suspicious (e.g., button text and link destination do not match) in order to draw the user's attention to the URL they intend to visit.

7.8.1.3. SSL/TSL warnings

Web browsers use SSL/TSL warnings to inform users that the privacy of their connection could be at risk [19]. Their objective is to allow informed decision-making, or at least guide the user to safety. Felt et al. [19] tested different variants of warnings and found that a modified button placement and design was able to promote the safe choice and demote the unsafe choice (see Figure 7). While not all certificate errors indicate an insecure website, the authors were still able to increase the default secure behavior and lead users back to the previous website. Note that their warning design did not improve user understanding, but nevertheless increased secure behavior.

- Insecure behavior that should be avoided: Visiting a website without a valid SSL/TSL certificate.
- Intended behavior: Go back to the previous website.
- Interaction attributes used to induce friction: Color (red for danger), placement (button hard to find). Users are often forced to leave their navigation path, leading to strong friction.
- UX is acceptable because: Users can still go to the insecure website if they really want to; disruption stays within acceptable bounds.

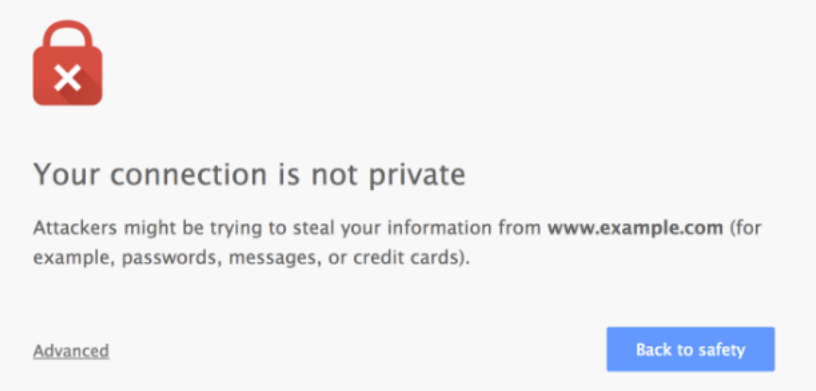


Figure 7: Felt et al. [17] designed a warning for SSL/TSL certificate errors and improved adherence to secure behavior by promoting the secure choice and demoting the insecure choice.

7.8.2. Example of a failed attempt at security-enhancing friction

To demonstrate which types of security interventions may lead to disuse of technology, imagine attempting to sign up for an online newspaper subscription. To encourage new subscribers to choose more secure passwords, the website reacts to each attempt to type in an insecure password by changing the placement of the sign-up button and decreasing its contrast, making it harder to see. Thus, after each attempt to sign up with an insecure password, it becomes harder to sign up, but the user does not get detailed feedback on why the process is so difficult. The UX curve of such a sign-up process would likely look similar to Figure 4, where UX drops at the security-enhancing friction (button changes contrast and placement), but does **not** recover after the intervention. We can consider this a failed attempt to create security-enhancing friction, since UX does not recover, and such a scenario would likely lead users to switch to another website providing similar services.

- Insecure behavior that should be avoided: Use of “insecure” passwords.
- Intended behavior: Set password that is harder to crack.
- Interaction attributes used to induce friction: Placement of sign-up button, contrast.
- UX is **not** acceptable because: Friction is too high and user does not get sufficient feedback explaining the difficulties.

Note that this is an imaginary use case intended to illustrate the possibility of introducing friction that is too strong and leads to a persistent drop in overall UX. To confirm whether this example is really a failed attempt, the impact of the described design interventions would need to be measured empirically (see Section 7.10.). This example also illustrates

how business interests and security interests can impact each other. Secure passwords improve the user's resilience to attacks, but strong friction as described above will lead to disuse and lack of sign-ups to the service. This exemplifies the importance of empirical user research when implementing security measures that impact a users' experience with a product or service.

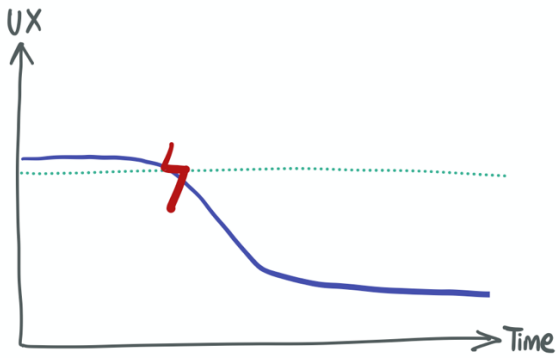


Figure 8: When UX does not recover to an acceptable level after the risky situation has passed, friction can lead to disuse, and thus does not fulfill the requirements of security-enhancing friction.

7.9. How to induce security-enhancing friction

The examples in the previous section demonstrate a wide variety of ways design can be used to induce friction. Color, contrast, step-wise advancement, placement of buttons, sound and more can be used. We refer to these ways of **how** to induce friction as interaction attributes, similar to the interaction attributes used in UX design when defining interaction aesthetics [38].

Table 2 shows examples of interaction attributes that can be used by designers to induce security-enhancing friction.

Category	Induces less friction	Induces more friction
Speed	Fast	Slow
Steps	One step	Several steps
Color	Muted	Flashy
Contrast	High contrast	Low contrast
Typography	More legible	Less legible
Conventions	Follows design conventions	Does not follow design conventions

Placement	Directly visible	Needs scrolling
Input	No manual input, one click	Needs manual inputs
Complexity	Straight-forward	Complex
Sound	Silent	Loud
Movement	Static	Moving
Physical vibration	Slight	Strong

Table 2: Examples of interaction attributes that can be used to induce security-enhancing friction. These attributes represent a continuum. The attributes can influence each other, and combining multiple attributes can lead to higher friction.

Designers may worry that introducing security-enhancing friction could lead to disuse of their product or service. Disuse would be the result of friction that creates overly negative UX (i.e., UX that does not recover to acceptable levels). To avoid such negative user experience, it is important to consider which interaction attributes are appropriate for the users of a specific interaction. For instance, when users of a website are typically pressed for time (e.g., when attempting to buy a product that sells out quickly), introducing friction that slows them down would not be a wise choice and UX would likely not recover if they were not able to buy the product in time. Instead, a designer of friction would need to align use of other interaction attributes (Table 2) with the objectives and motivations a user has for an interaction. For example, changing colour, contrast, typography, or even using physical vibration could be more appropriate for users who are typically under time pressure. A rich understanding of typical user objectives and motivations can be achieved through user research.

Second, it is imperative that designers carefully measure the impact of any friction they introduce with a representative sample of users, through empirical measures of momentary, episodic and long-term UX of an interaction that includes security-enhancing friction. Note that any friction will impact certain qualities of UX more strongly than others. For instance, slowing down an interaction by asking a user to re-type an URL (as displayed in Figure 6) could impact the pragmatic quality (achievement of "do-goals") of an experience, but at the same time could improve hedonic quality of the experience (achievement of "be-goals", see Section 7.6.) by fulfilling the psychological need for security and control. When deciding which UX dimensions to retain when designing for

friction and which ones to momentarily compromise, both the objectives and motivations of the user, as well as security, need to be carefully balanced.

In the next section, we describe how designers can obtain such detailed and nuanced measures of UX in order to understand the impact of friction, fine-tune friction design and avoid disuse.

7.10. How to measure the success of security-enhancing friction

In this section, we suggest a framework for systematically measuring the effects of security-enhancing friction in a nuanced way based on UX theory.

By "systematic measurement", we mean nuanced measurements that can be applied across studies and take the temporal aspect of UX into consideration.

In order to transfer the concept of security-enhancing friction to practice, we suggest applying a range of experience evaluation methods to security- and privacy-relevant contexts to systematically integrate both experience-based and behavioral measures. Table 2 describes how researchers and designers can measure the temporal dynamics of UX throughout a privacy/security-relevant interaction in order to achieve the intended security-enhancing friction experience at each step. In addition, security-enhancing friction needs to lower the likelihood of a defined risk-taking behavior, thereby reducing the likelihood of a successful attack (while keeping overall UX at an acceptable level).

The combination of empirical methods (Table 3) also enables researchers and designers to understand the impact of various types and combinations of security interventions have on their user experience and behavior.

What is measured	At what stage	Evaluation methods	Intended experience
Experience-based			
Momentary UX	While using technology	When assessing the effects of security-enhancing friction, participants will likely be asked to interact with a prototype or finished product – for instance, through a user test. In this context, the **think-aloud method** [39] can be applied to assess momentary UX. This method consists of asking people to think aloud while solving a problem or during an interaction. The think-aloud method allows researchers to understand	Momentary UX should be lowered so that the user has an appropriate perception of their current risk (see Figure 4).

		whether the security-enhancing friction created the intended short spike of negative UX and whether UX recovers afterwards. If used in pre-tests, the think-aloud method should also be used to verify that the spike of momentary UX is not too strong. Psychophysiological measurements are another option to understand momentary experience. **Eye tracking** [47] can give insights into privacy and security perceptions, as used for instance by [43] to compare Facebook interfaces tailored for privacy support by analyzing differences in gaze patterns and areas of interest between the interfaces. **Facial Action Coding** (FACS) [18] is another promising method used to catego- rize facial movements and match them with categories of emotional expressions. **fMRI scans** are a way of understanding brain responses to stimuli, which have been used to understand habituation to warnings in the past [5, 60]. Most psychophysiological measurements work best when triangulated with other methods for richer experiential insights.	
Episodic UX	After using a technology	To evaluate experience after use, qualitative tools such as **focus groups** or **interviews** can give rich insights into participants' experience with a security- enhancing friction; examples include [15, 53]. Standardized **questionnaires** can help gain comparable insights based on theory. Good candidates for measuring overall UX include the UEQ questionnaire [36], AttrakDiff [28], and Psychological Needs Questionnaire [55]. The Geneva Emotions Wheel can help evaluate overall emotions after use [54].	After an interaction, the user should have an acceptable UX overall; the momentary drop in UX should not have overly impeded their experience.
Long-term/ cumulative UX	After multiple uses	When conducting an asynchronous study on security-enhancing friction, researchers can also use the **diary method** [6] and ask participants to write down certain elements or take pictures of moments where they felt a short spike of negative UX in security- and privacy-related situations. The diary method has been used by [29, 42] to study privacy/security topics.	After multiple uses, the user should continue to have an acceptable UX overall and have adopted the technology.

		Retrospective UX evaluation methods such as the **UX Curve** [33] can assist users in retrospectively reporting how their experience changed over time. The UX Curve is based on retrospective user reporting, where users themselves indicate their experience over time. For security-enhancing friction, the UX curve can help evaluate and visualize whether there was a momentary drop in UX, which then recovered to an acceptable level.	
Behavior-based			
Occurrence of risk-taking behavior	After exposure to the intervention	Risk-taking behavior can take many forms (e.g., continuously postponing updates to a later point, sending sensitive data over insecure channels). If possible, the occurrence of the risk-taking behavior should be measured through activity logs or observations. If direct measurement is not feasible, behavioral intention can be an easier-to-operationalise alternative.	The occurrence of risk-taking behavior should be lowered by the security-enhancing friction as compared to a control group.
Optional: Knowledge-based			
Understanding of security-relevant processes	After using a technology	Relevant knowledge questions can be used to understand whether a security-enhancing friction improved user understanding. The level of knowledge users should acquire through an interaction must be defined a priori. Most interactions will not aim at expert understanding of a technology. Refer to [19, 26] for an example in UPS.	Note that creating understanding of security issues is not the primary goal of friction, but understanding might be an intended effect in certain contexts.

Table 3: Methods to measure effects of security-enhancing interventions in a nuanced way, enabling the design of security-enhancing friction.

The described methods are meant as suggestions for how to evaluate users' experience with security-enhancing friction at various time points, which should be combined deliberately and with care. For instance, the think-aloud method is usually combined with another method, such as user tests. User tests usually also include an interview or questionnaires to obtain more complete observations of how participants interact. This remark holds true for all phases of the experience evaluation.

While, as described in Table 3, behavioral intention can be used as an approximation of behavior when behavioral data is not readily available, some measurement of behavior as

a ground truth would be advisable. Redmiles et al. [49], for instance, systematically compare real-world data to self-reported results with a focus on updating behavior. They show that self-reported data largely varies consistently and systematically with measured data in the context of software updates.

Note that creating understanding of security concepts is not the primary goal of security-enhancing friction, just like physical speed bumps or rumble strips do not attempt to help drivers understand specific safety issues. Instead, the goal is to make the insecure action less attractive through friction and make the secure course of action relatively more attractive, all while keeping UX at an acceptable level.

Table 3 includes knowledge-based measures of success, since the goal may be to improve understanding of security concepts in certain contexts. An example might be "private" browsing modes, which are often perceived as more secure by users than warranted [26]. In this context, improving understanding of the actual security properties of private browsing modes may be achieved through security-enhancing friction.

7.11. Discussion

7.11.1. Novelty

Table 1 shows that a number of security-enhancing interventions already exist, and Section 7.8.1. gives some examples of existing interventions that might be considered security-enhancing friction. Thus, one might question the novelty of our suggested approach. To the best of our knowledge, we are the first to compare security-enhancing interventions (e.g., nudges, warnings, fear appeals), which have to date been studied extensively but mostly separately. We compare and contrast them through the notion of friction, thus providing a means to reflect on the effect these interventions may have on the user experience.

Our original contribution is the introduction of the notion of security-enhancing friction enables the systematic, actionable and controlled migration, and subsequent integration, of UX concepts into usable privacy and security. Unlike previous concepts, security-enhancing friction encompasses both the objective of stimulating secure behavior and of maintaining an acceptable overall user experience. In this work, we strive to contribute to the further bridging of UX and security, which will be of mutual benefit to both fields: security can build on methods from UX and theories grounded in psychology, while UX

can be extended in include a security dimension, thus expanding the concept to the support of users' privacy and security.

7.11.2. Cumulative friction of security tasks and security-enhancing friction

One might question whether security-enhancing friction simply adds to the existing "friction" of having to complete certain security tasks, such as creating a new password. Note, however, that security-enhancing friction does not necessarily coincide with security tasks, instead it can support existing security tasks. As in the example of a password meter giving feedback to users, the form that requests us to choose a password, is already there. Security-enhancing friction attempts to improve the strength of the chosen password. The user could still fail the purpose of the security task, by choosing a guessable password. Actually, the "friction" of having to choose a new password and the security-enhancing friction of the password meters are not necessarily additive.

A security-enhancing friction can lighten the burden of having to choose a new password; the color of the bar can help the user's experience with the original security task of creating a new password by letting them succeed faster and with better quality of result, sparing them an otherwise long sequence of unsuccessful attempts, or the unpleasant surprise to have their password guessed by an intruder.

7.11.3. Habituation

Habituation might be a threat to the effectiveness of friction, as is the case for most security-enhancing interventions (e.g., warnings [2, 19, 23]). Longitudinal studies could reveal whether frictions are vulnerable to this threat. The concept and methods proposed in this article can help address habituation given that they allow us to understand temporal dynamics linked to friction, and this understanding can be used to periodically adapt the form of a friction element for which habituation is known to occur.

UX methods even have the advantage of detecting the effects of habituation on the experience level (e.g., decrease in perceived friction) before they have behavioral consequences. As such, they can also contribute to exploring the thresholds for "sufficient" friction to reliably expect an adequate behavioral response. Habituation might not occur in other contexts, such as systems that are only used for certain occasions (e.g., e-voting). Previous studies have reported on promising approaches that seem resistant to habituation, such as the use of polymorphic dialogues (dialogues that change the required form of user

input) [5, 60], opinionated design (visual design techniques to promote the safe choice as the preferred option) [19] or certain attractors (interface modifications that attempt to draw user's attention to important information, for instance by promoting interaction with salient information) [8].

7.11.4. Ethical challenges

There are two levels of ethical challenges that we find compelling.

First, on an experimental level, and in line with UPS experiments in general, research on friction design will inevitably run into the ethical challenge of exposing users to a certain level of risk, which can sometimes lead to the use of deception in user studies. Cranor and Buchler [13] point out that in the context of computer security warnings, it can be necessary to lead participants to believe that there is some actual risk involved. Such approaches make integrating ethical considerations at all stages of experiment design obligatory.

From another point of view, friction might seem unethical at first glance because it introduces a barrier to action, thus decreasing users' autonomy. However, given that security-enhancing friction is designed to keep UX constant, such friction is inherently positive for the user, since it aligns security and UX. We think that the concept of security-enhancing friction can help advance this discussion by providing a nuanced understanding of users' experience when using security-enhancing friction. For instance, Renaud and Zimmermann [51] outline ethical challenges linked to nudges, and suggest that there should be a reasonable plan for monitoring the effect of the intervention and for discontinuing it if unintended side effects are detected. Security-enhancing friction encourages such nuanced measurement of the effects of an intervention.

7.11.5. Similarities and differences to other concepts

Our definition of security-enhancing friction bears similarity to "soft paternalism" or nudges as defined by Acquisti et al., [1] in support of privacy and security decision-making. The difference is that security-enhancing friction encourages the use of UX methods for a nuanced measurement of momentary negative UX, while safeguarding an acceptable overall UX for users. The mere use of behavioral measurements does not allow researchers and designers to determine the success of security-enhancing friction.

One might also draw parallels to Kahneman's [31] dual processing theory, which differentiates between two modes of thought, system one (fast, instinctive and emotional) and system two (slower, deliberative, logical), and was previously applied to the context of security by Dennis and Minas [14]. These authors argue that security behaviors are mostly determined by system one cognition, which may issue an alert if it detects a surprise or anomaly. In this case, system two thinking can take over and potentially trigger a more deliberate response. The authors give some examples of how to trigger a switch from system one to system two thinking. For instance, an organization could apply aversion training by regularly sending out fake phishing emails and then lock individuals who click on them out of their account for 15 minutes. Another example is triggering a loud alarm whenever a person clicks on a phishing email. One could also change situational normality by prohibiting all organizational emails from containing a clickable link; any email containing a link would thus become suspicious. This has some parallels to our approach. Dennis and Minas' suggested interventions introduce friction into an experience in order to trigger deliberate system two thinking. However, extreme interventions can lead to strong negative emotions among an organization's employees (e.g., shame, frustration), potentially decreasing motivation and productivity.

These shortcomings make it unlikely, in our eyes, that such measures will be applied in organizations. In cases where users are free to switch away from a service that exposes them to such extreme interventions for security's sake, they might well choose to use another service provider. This makes it necessary to find a more balanced approach to trigger system two thinking.

Thus, while our approach has a similar objective, interventions that have a lasting deleterious effect on user experience cannot be considered security-enhancing friction according to our definition. Security-enhancing friction also requires the nuanced measurement of people's experiences during and after an interaction to ensure that lasting negative impressions or exceedingly strong negative emotions can reliably be avoided. The security-enhancing friction approach we describe in this paper could therefore enhance the dual processing framework by offering a controlled empirical approach to influencing switching between the two modes.

One might also relate our approach to dark patterns, which are part of a larger research agenda around persuasive design and nudges [44]. Dark patterns are defined as interface designs that try to guide end-users to desired behavior through malicious interaction flows

[24]. The difference is that security-enhancing friction, per definition, is designed in the interest of the user (on both a UX and a security level), while dark patterns are not designed with the user's best interest in mind. However, whenever design methods are applied with the objective of changing behaviors, the question arises as to for "whose good" nudges, and by extension security-enhancing frictions, are designed [51].

7.12. Conclusion

In this paper, we argue that in the security context, it can be desirable to use UX methods to design for moments of negative UX in security-critical situations. We compare and contrast existing security-enhancing interventions that are frequently studied separately (e.g., nudges, warnings, fear appeals) through the common lens of friction. Building on these insights, we introduce the novel framework of security-enhancing friction, which provides an actionable way to systematically integrate the concept of user experience into empirical UPS studies and ensure that both the objective of secure behavior and of an acceptable overall experience can be met. Through this work, we strive to further bridge the disciplines of user experience and privacy/security, and we hope that this article is the first of many investigating how to intentionally create temporary negative experiences through nuanced friction design when it is in the user's interest.

7.13. Acknowledgements

We acknowledge support from the National Research Fund (FNR) under Grant Number PRIDE15/10621687. We thank our shepherds Alisa Frik and Simon Parkin who provided valuable feedback on this paper. We also thank the anonymous reviewers and all NSPW participants for their thoughtful and constructive comments.

7.14. References

[1] Alessandro Acquisti, Manya Sleeper, Yang Wang, Shomir Wilson, Idris Adjerid, Rebecca Balebako, Laura Brandimarte, Lorrie Faith Cranor, Saranga Komanduri, Pedro Giovanni Leon, Norman Sadeh, and Florian Schaub. 2017. Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online. *Comput. Surveys* 50, 3 (Aug. 2017), 1–41. https://doi.org/10.1145/3054926

[2] Devdatta Akhawe and Adrienne Porter Felt. 2013. Alice in Warningland: A Large-Scale Field Study of Browser Security Warning Effectiveness. In *22nd USENIX Security*

Symposium (USENIX Security 13). USENIX Association, Washington, D.C., 257–272. https://www.usenix.org/conference/usenixsecurity13/technical-sessions/presentation/akhawe

[3] Yusuf Albayram, Mohammad Maifi Hasan Khan, Theodore Jensen, and Nhan Nguyen. 2017. "...better to use a lock screen than to worry about saving a few seconds of time": Effect of Fear Appeal in the Context of Smartphone Locking Behavior. In *Thirteenth Symposium on Usable Privacy and Security (SOUPS '17)*. USENIX Association, 49–63. https://www.usenix.org/conference/soups2017/ technical-sessions/presentation/albayram

[4] Hazim Almuhimedi, Florian Schaub, Norman Sadeh, Idris Adjerid, Alessandro Acquisti, Joshua Gluck, Lorrie Faith Cranor, and Yuvraj Agarwal. 2015. Your Location Has Been Shared 5,398 Times! A Field Study on Mobile App Privacy Nudging. In *Proceeding of the Annual Conference on Human Factors in Computing Systems (CHI '15)*. ACM, 787–796. https://doi.org/10.1145/2702123.2702210

[5] Bonnie Brinton Anderson, C. Brock Kirwan, Jeffrey L. Jenkins, David Eargle, Seth Howard, and Anthony Vance. 2015. How Polymorphic Warnings Reduce Habituation in the Brain: Insights from an fMRI Study. In *Proceedings of the Annual ACM Conference on Human Factors in Computing Systems (CHI '15)*. ACM, 2883–2892. https://doi.org/10.1145/2702123.2702322

[6] Ruth Bartlett and Christine Milligan. 2015. *What is diary method?* Bloomsbury Academic.

[7] Franklin J. Boster and Paul Mongeau. 1984. Fear-Arousing Persuasive Messages. *Annals of the International Communication Association* 8, 1 (Jan. 1984), 330–375. https://doi.org/10.1080/23808985.1984.11678581

[8] Cristian Bravo-Lillo, Lorrie Cranor, Saranga Komanduri, Stuart Schechter, and Manya Sleeper. 2014. Harder to Ignore? Revisiting Pop-Up Fatigue and Approaches to Prevent It. In *10th Symposium On Usable Privacy and Security (SOUPS '14)*. USENIX Association, 105–111. https://www.usenix.org/conference/ soups2014/proceedings/presentation/bravo-lillo

[9] Cristian Bravo-Lillo, Saranga Komanduri, Lorrie Faith Cranor, Robert W. Reeder, Manya Sleeper, Julie Downs, and Stuart Schechter. 2013. Your Attention Please: Designing Security-decision UIs to Make Genuine Risks Harder to Ignore. In *Proceedings*

of the Ninth Symposium on Usable Privacy and Security - SOUPS '13. Newcastle, United Kingdom, 1. https://doi.org/10.1145/2501604.2501610

[10] José Carlos Brustoloni and Ricardo Villamarín-Salomón. 2007. Improving Security Decisions with Polymorphic and Audited Dialogs. In *Proceedings of the 3rd Symposium on Usable Privacy and Security (SOUPS '07).* ACM Press, Pittsburgh, Pennsylvania, 76. https://doi.org/10.1145/1280680.1280691

[11] Anna L. Cox, Sandy J.J. Gould, Marta E. Cecchinato, Ioanna Iacovides, and Ian Ren- free. 2016. Design Frictions for Mindful Interactions: The Case for Microboundaries. In *Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems - CHI EA '16.* ACM Press, Santa Clara, California, USA, 1389–1397. https://doi.org/10.1145/2851581.2892410

[12] Lorrie Faith Cranor. 2008. A Framework for Reasoning about the Human in the Loop. In *Proceedings of the 1st Conference on Usability, Psychology, and Security.* USENIX Association, USA.

[13] Lorrie Faith Cranor and Norbou Buchler. 2014. Better Together: Usability and Security Go Hand in Hand. *IEEE Security & Privacy* 12, 6 (Nov. 2014), 89–93. https://doi.org/10.1109/MSP.2014.109

[14] Alan R. Dennis and Randall K. Minas. 2018. Security on Autopilot: Why Current Security Theories Hijack Our Thinking and Lead Us Astray. *SIGMIS Database* 49, SI (April 2018), 15–38. https://doi-org.proxy.bnl.lu/10.1145/3210530.3210533

[15] Verena Distler, Carine Lallemand, and Vincent Koenig. 2020. How Acceptable Is This? How User Experience Factors Can Broaden our Understanding of The Acceptance of Privacy Trade-offs. *Computers in Human Behavior* 106 (May 2020), 106227. https://doi.org/10.1016/j.chb.2019.106227

[16] Serge Egelman, Lorrie Faith Cranor, and Jason Hong. 2008. You've Been Warned: an Empirical Study of the Effectiveness of Web Browser Phishing Warnings. In *Proceedings of the Annual ACM Conference on Human Factors in Computing Systems (CHI '08).* ACM Press, Florence, Italy, 1065. https://doi.org/10.1145/ 1357054.1357219

[17] Serge Egelman, Andreas Sotirakopoulos, Ildar Muslukhov, Konstantin Beznosov, and Cormac Herley. 2013. Does my Password go up to Eleven?: the Impact of Password

Meters on Password Selection. In *Proceedings of the Annual ACM Conference on Human Factors in ComputingSystems (CHI '13).* ACM, Paris, France, 2379–2388.

[18] Rosenberg Ekman. 1997. *What the Face Reveals: Basic and Applied Studies of Spontaneous Expression Using the Facial Action Coding System (FACS).* Oxford University Press, USA.

[19] Adrienne Porter Felt, Alex Ainslie, Robert W. Reeder, Sunny Consolvo, Somas Thyagaraja, Alan Bettes, Helen Harris, and Jeff Grimes. 2015. Improving SSL Warnings: Comprehension and Adherence. In *Proceedings of the Annual ACM Conference on Human Factors in Computing Systems (CHI '15).* ACM, 2893–2902. https://doi.org/10.1145/2702123.2702442

[20] Steven Fokkinga and Pieter Desmet. 2012. Darker Shades of Joy: The Role of Negative Emotion in Rich Product Experiences. *Design Issues* 28, 4 (Oct. 2012), 42–56. https://doi.org/10.1162/DESI_a_00174

[21] Alisa Frik, Nathan Malkin, Marian Harbach, Eyal Peer, and Serge Egelman. 2019. A promise is a promise: The Effect of Commitment Devices on Computer Security Intentions. In *Proceeding of the Annual Conference on Human Factors in Computing Systems (CHI '19).* 1–12.

[22] Peter Leo Gorski, Yasemin Acar, Luigi Lo Iacono, and Sascha Fahl. 2020. Listen to Developers! A Participatory Design Study on Security Warnings for Cryp- tographic APIs. In *Proceeding of the Annual Conference on Human Factors in Computing Systems (CHI '20).* Association for Computing Machinery, Honolulu, HI, USA. https://doi-org.proxy.bnl.lu/10.1145/3313831.3376142

[23] Peter Leo Gorski, Luigi Lo Iacono, Dominik Wermke, Christian Stransky, Sebastian Möller, Yasemin Acar, and Sascha Fahl. 2018. Developers Deserve Security Warnings, Too: On the Effect of Integrated Security Advice on Cryptographic API Misuse. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS '18).* USENIX Association, 265–281. https://www.usenix.org/conference/soups2018/presentation/gorski

[24] Colin M. Gray, Yubo Kou, Bryan Battles, Joseph Hoggatt, and Austin L. Toombs. 2018. The Dark (Patterns) Side of UX Design. In *Proceeding of the Annual Conference on Human Factors in Computing Systems (CHI '18).* ACM Press, Montreal QC, Canada, 1–14. https://doi.org/10.1145/3173574.3174108

[25] Siddharth Gulati, Sonia Sousa, and David Lamas. 2017. Modelling Trust: An Empirical Assessment. In *Human-Computer Interaction – INTERACT 2017,* Regina Bernhaupt, Girish Dalvi, Anirudha Joshi, Devanuj K. Balkrishan, Jacki O'Neill, and Marco Winckler (Eds.). Vol. 10516. Springer International Publishing, Cham, 40–61. https://doi.org/10.1007/978-3-319-68059-0_3

[26] Hana Habib, Jessica Colnago, Vidya Gopalakrishnan, Sarah Pearman, Jeremy Thomas, Alessandro Acquisti, Nicolas Christin, and Lorrie Faith Cranor. 2018. Away From Prying Eyes: Analyzing Usage and Understanding of Private Browsing. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS '18).* USENIX Association, 159–175. https://www.usenix.org/conference/soups2018/presentation/habib-prying

[27] Marc Hassenzahl. 2008. User Experience (UX): Towards an Experiential Perspective on Product Quality. In *Proceedings of the 20th International Conference of the Association Francophone d'Interaction Homme-Machine (IHM '08).* ACM Press, Metz, France, 11. https://doi.org/10.1145/1512714.1512717

[28] Marc Hassenzahl, Michael Burmester, and Franz Koller. 2003. *AttrakDiff: Ein Fragebogen zur Messung Wahrgenommener Hedonischer und Pragmatischer Qualität.* Vieweg & Teubner Verlag, Wiesbaden, 187–196. https://doi.org/10.1007/978- 3-322-80058-9_19

[29] Qatrunnada Ismail, Tousif Ahmed, Apu Kapadia, and Michael K. Reiter. 2015. Crowdsourced exploration of security configurations. In *Proceedings of the Annual ACM Conference on Human Factors in Computing Systems (CHI '15).* 467–476.

[30] Jurjen Jansen and Paul van Schaik. 2017. Persuading End Users to Act Cautiously Online: Initial Findings of a Fear Appeals Study on Phishing. In *Proceedings of the Eleventh International Symposium on Human Aspects of Information Security & Assurance (HAISA 2017).*

[31] Daniel Kahneman. 2011. *Thinking, Fast and Slow.* Farrar, Straus and Giroux.

[32] Farzaneh Karegar, John Sören Pettersson, and Simone Fischer-Hübner. 2020. The Dilemma of User Engagement in Privacy Notices: Effects of Interaction Modes and Habituation on User Attention. *ACM Transactions on Privacy and Security* 23, 1 (Feb. 2020), 1–38. https://doi.org/10.1145/3372296

[33] Sari Kujala, Virpi Roto, Kaisa Väänänen-Vainio-Mattila, Evangelos Karapanos, and Arto Sinnelä. 2011. UX Curve: A Method for Evaluating Long-term User Experience. *Interacting with Computers* 23, 5 (Sept. 2011), 473–483. https://doi.org/10.1016/j.intcom.2011.06.005

[34] Matthias Laschke, Sarah Diefenbach, and Marc Hassenzahl. 2015. "Annoying, but in a nice way": An Inquiry into the Experience of Frictional Feedback. *International Journal of Design* 9, 2 (2015), 129–140.

[35] Matthias Laschke, Marc Hassenzahl, Jan Brechmann, Eva Lenz, and Marion Digel. 2013. Overcoming Procrastination with ReMind. In *Proceedings of the 6th International Conference on Designing Pleasurable Products and Interfaces - DPPI '13.* ACM Press, Newcastle upon Tyne, United Kingdom, 77–85. https://doi.org/10.1145/2513506.2513515

[36] Bettina Laugwitz, Theo Held, and Martin Schrepp. 2008. Construction and Evaluation of a User Experience Questionnaire. In *HCI and Usability for Education and Work, Andreas Holzinger (Ed.).* Vol. 5298. Springer Berlin Heidelberg, Berlin, Heidelberg, 63–76. https://doi.org/10.1007/978-3-540-89350-9_6

[37] Effie Lai-Chong Law, Arnold P. O. S. Vermeeren, Marc Hassenzahl, and Mark Blythe. 2007. Towards a UX Manifesto. In *Proceedings of the 21st British HCI Group Annual Conference on People and Computers: HCI...But Not As We Know It - Volume 2* (BCS-HCI '07). BCS Learning & Development Ltd., Lancaster, UK, 205–206. http://dl.acm.org/citation.cfm?id=1531407.1531468

[38] Eva Lenz, Sarah Diefenbach, and Marc Hassenzahl. 2014. Aesthetics of Interaction: a Literature Synthesis. In *Proceedings of the 8th Nordic Conference on Human- Computer Interaction (NordiCHI '14).* ACM Press, Helsinki, Finland, 628–637. https://doi.org/10.1145/2639189.2639198

[39] Jacobijn A.C. Sandberg Maarten W. van Someren, Yvonne F. Barnard. 1994. *The Think Aloud Method: A Practical Guide to Modelling Cognitive Processes.* Academic Press.

[40] Sascha Mahlke. 2005. Understanding Users' Experience of Interaction. In *Proceedings of the 2005 Annual Conference on European Association of Cognitive Ergonomics.* 251–254.

[41] Sascha Mahlke. 2008. *User Experience of Interaction with Technical systems.* Doc- toral Dissertation.

[42] Shrirang Mare, Mary Baker, and Jeremy Gummeson. 2016. A Study of Authentication in Daily Life. In *Twelfth Symposium on Usable Privacy and Security (SOUPS '16).* USENIX Association, 189–206. https://www.usenix.org/conference/soups2016/technical-sessions/presentation/mare

[43] Moses Namara and Curtis John Laurence. 2019. What Do You See? An Eye-tracking study of a Tailored Facebook Interface for Improved Privacy Support. *ACM Symposium on Eye Tracking Research Applications (ETRA)* (2019), 7.

[44] Midas Nouwens, Ilaria Liccardi, Michael Veale, David Karger, and Lalana Kagal. 2020. Dark Patterns after the GDPR: Scraping Consent Pop-Ups and Demonstrating Their Influence. In *Proceeding of the Annual Conference on Human Factors in Computing Systems (CHI '20) (Honolulu, HI, USA) (CHI '20).* Association for Computing Machinery, New York, NY, USA, 1–13. https://doi.org/10.1145/3313831.3376321

[45] Eyal Peer, Serge Egelman, Marian Harbach, Nathan Malkin, Arunesh Mathur, and Alisa Frik. 2020. Nudge me Right: Personalizing Online Security Nudges to People's Decision-making Styles. *Computers in Human Behavior (2020),* 106347.

[46] Justin Petelka, Yixin Zou, and Florian Schaub. 2019. Put Your Warning Where Your Link Is: Improving and Evaluating Email Phishing Warnings. In *Proceedings of the Annual ACM Conference on Human Factors in Computing Systems (CHI '19).* ACM Press, Glasgow, Scotland Uk, 1–15. https://doi.org/10.1145/3290605.3300748

[47] Alex Poole and Linden J. Ball. 2006. Eye tracking in HCI and Usability Research. In *Encyclopedia of Human-Computer Interaction.* IGI Global, 211–219.

[48] Elham Al Qahtani, Mohamed Shehab, and Abrar Aljohani. 2018. The Effectiveness of Fear Appeals in Increasing Smartphone Locking Behavior among Saudi Arabians. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS '18).* USENIX Association, 31–46. https://www.usenix.org/conference/soups2018/presentation/qahtani

[49] Elissa M Redmiles, Ziyun Zhu, Sean Kross, Dhruv Kuchhal, Tudor Dumitras, and Michelle L Mazurek. 2018. Asking for a Friend: Evaluating Response Biases in Security

User Studies. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security.* 1238–1255.

[50] Karen Renaud and Marc Dupuis. 2019. Cyber Security Fear Appeals: Unexpectedly Complicated. In *Proceedings of the New Security Paradigms Workshop (NSPW).* ACM, San Carlos Costa Rica, 42–56. https://doi.org/10.1145/3368860.3368864

[51] Karen Renaud and Verena Zimmermann. 2018. Ethical guidelines for nudging in information security & privacy. *International Journal of Human-Computer Studies 120 (Dec. 2018),* 22–35. https://doi.org/10.1016/j.ijhcs.2018.05.011

[52] Virpi Roto, Effie Law, Arnold Vermeeren, and Jettie Hoonhout. 2011. User Experience White Paper. In *Result from Dagstuhl Seminar on Demarcating User Experience*, September 15-18, 2010. 12.

[53] Nithya Sambasivan, Garen Checkley, Amna Batool, Nova Ahmed, David Nemer, Laura Sanely Gaytán-Lugo, Tara Matthews, Sunny Consolvo, and Elizabeth Churchill. 2018. "Privacy is not for me, it's for those rich women": Performative Privacy Practices on Mobile Phones by Women in South Asia. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS '18).* USENIX Association, 127–142. https://www.usenix.org/conference/soups2018/presentation/sambasivan

[54] Klaus R. Scherer. 2005. What are Emotions? And how can they be Measured? *Social Science Information* 44, 4 (Dec. 2005). https://doi.org/10.1177/0539018405058216

[55] Kennon M. Sheldon, Andrew J. Elliot, Youngmee Kim, and Tim Kasser. 2001. What is Satisfying about Satisfying Events? Testing 10 Candidate Psychological Needs. *Journal of Personality and Social Psychology* 80, 2 (2001), 325.

[56] Richard H. Thaler and Cass R. Sunstein. 2008. *Nudge: Improving Decisions about Health, Wealth, and Happiness.* New Haven, CT, US.

[57] James Turland, Lynne Coventry, Debora Jeske, Pam Briggs, and Aad van Moorsel. 2015. Nudging Towards Security: Developing an Application for Wireless Network Selection for Android Phones. In *Proceedings of the 2015 British HCI conference*. 193–201.

[58] Blase Ur, Patrick Gage Kelley, Saranga Komanduri, Joel Lee, Michael Maass, Michelle L. Mazurek, Timothy Passaro, Richard Shay, Timothy Vidas, Lujo Bauer,

Nicolas Christin, and Lorrie Faith Cranor. 2012. How Does Your Password Measure Up? The Effect of Strength Meters on Password Creation. In *USENIX Security Symposium (USENIX Security '12).* USENIX, Bellevue, WA, 65–80.

[59] Christine Utz, Martin Degeling, Sascha Fahl, Florian Schaub, and Thorsten Holz. 2019. (Un) informed Consent: Studying GDPR Consent Notices in the Field. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security.* London, United Kingdom, 973–990.

[60] Anthony Vance, Brock Kirwan, Daniel Bjornn, Jeffrey Jenkins, and Bonnie Brinton Anderson. 2017. What do we Really Know About how Habituation to Warnings Occurs Over Time?: A Longitudinal fMRI Study of Habituation and Polymorphic Warnings. In *Proceeding of the Annual Conference on Human Factors in Computing Systems (CHI '17).* 2215–2227.

[61] Yang Wang, Pedro Giovanni Leon, Alessandro Acquisti, Lorrie Faith Cranor, Alain Forget, and Norman Sadeh. 2014. A Field Trial of Privacy Nudges for Facebook. In *Proceeding of the Annual Conference on Human Factors in Computing Systems (CHI '14).* 2367–2376.

[62] Yang Wang, Pedro Giovanni Leon, Kevin Scott, Xiaoxuan Chen, Alessandro Acquisti, and Lorrie Faith Cranor. 2013. Privacy Nudges for Social Media: an Exploratory Facebook Study. In *Proceedings of the 22nd International Conference on World Wide Web.* 763–770.

[63] Bo Zhang, Mu Wu, Hyunjin Kang, Eun Go, and S. Shyam Sundar. 2014. Effects of Security Warnings and Instant Gratification Cues on Attitudes Toward Mobile Websites. In *Proceeding of the Annual Conference on Human Factors in Computing Systems (CHI '14).* ACM, 111–114. https://doi.org/10.1145/2556288.2557347

[64] Bo Zhang and Heng Xu. 2016. Privacy Nudges for Mobile Applications: Effects on the Creepiness Emotion and Privacy Attitudes. In *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing (CSCW '16).* ACM Press, San Francisco, California, USA, 1674–1688. https://doi.org/10.1145/2818048.2820073

Chapter 8: Concluding Remarks

In this chapter, I take a broader perspective and synthesize the key findings as well as the interdependencies between the studies making up this dissertation (Section 8.1). I then describe the contributions of this PhD thesis (Section 8.2), as well as limitations and implications for future work (Section 8.3). Afterwards, I hypothesize how the field might move forward with the subjective experience of security in human-computer interactions (HCI) (Section 8.4), before providing a final conclusion (Section 8.5).

8.1. Synthesis of results

The objective of this doctoral dissertation is to contribute to a better understanding of the factors that induce a perception of security and privacy risks and how user-centered methods can contribute to designing these factors. This question was investigated from four angles: how UPS researchers induce a perception of risks in their research participants; the factors that contribute to people accepting certain risks; the design and evaluation of visible instances of security mechanisms; and how we might conceptually link security and privacy perceptions to behaviors. I will now synthesize the results.

8.1.1. How UPS researchers induce a perception of security and privacy risks in their research participants

The first objective of this PhD thesis was to analyze how UPS researchers induce a perception of security and privacy risk in their research participants (Chapter 2). In this study, we analyzed a large body of research in usable privacy and security. We investigated the tension researchers in the field face between exposing research participants to realistic risk and ethical, legal and practical considerations. We found that researchers creatively combine a large variety of methods and "tools" to induce a perception of risk (including scenarios, prototypes, security and privacy tasks, deception). When measuring response to risk, researchers frequently used self-reported measures alone or in combination with observed measures. The studies in our sample that exclusively used self-reported measures focused on subjective perceptions, for which self-reported measures seem most suitable and least intrusive (e.g., in Ahmed et al., 2015; Angulo & Ortlieb, 2015). Co-creation and participatory design methods were relatively rarely used (exceptions included Adams et al., 2018; Egelman et al., 2015). We discussed

participant recruitment and risk representation, finding that many studies rely on convenience samples and crowdworkers, and that certain user groups were underrepresented in the empirical studies in the sample, including children and teenagers, older adults, and people with disabilities. We also discussed ethics-related topics, such as the use of deception in the studied papers and find that definitions of deception differ. We also found that attackers were sometimes used as research "participants" without obtaining informed consent. We provided a framework for reporting user study methods in UPS as a means of encouraging better replicability and understanding of research methods and results.

8.1.2. Exploring the factors that contribute to the acceptance of privacy and security risks

The second objective of this dissertation was to explore the factors that contribute to the acceptance of privacy and security risks in situations in which people need to weigh the potential advantages of a technology against the associated privacy and security risks. To do so, in Chapter 3, we used one of the tools described in Chapter 2, scenarios, to describe potential privacy trade-offs (Rainie & Duggan, 2015). In this way, we encouraged participants to consider ambiguous situations that may lead their privacy to be compromised, both in scenarios that currently exist, and hypothetical ones. In focus groups, we found that people's rationalizations of why they accept or reject certain compromises to their privacy are varied. Often, we found that people's reasoning was based on perceived usefulness, a dimension in technology acceptance models (Davis, 1985; Venkatesh et al., 2003, 2012), in addition to non-instrumental aspects of UX, such as autonomy (i.e., being able to decide freely whether they wish to accept or reject a privacy trade-off). The need for autonomy is accounted for in certain technology acceptance models, for example through the dimension of voluntariness of use in the UTAUT model (Venkatesh et al., 2003). In addition to being able to choose freely to use or avoid using a technology, participants expressed a desire to have control over their data in the scenarios. The need for control is considered a psychological need in need theories and is often conceptualized together with the need for security (Diefenbach & Hassenzahl, 2011; Hassenzahl et al., 2010; Sheldon et al., 2001). The fulfilment of psychological needs is considered relevant for technology acceptance (Hornbæk & Hertzum, 2017).

8.1.3. Designing and evaluating visible instances of security to understand how they influence security perceptions

The third objective was to design and evaluate visible instances of security mechanisms, focusing on encryption during data transmission. Previous work has argued that visible security mechanisms can help users develop a more accurate understanding of what the system is doing (Rader & Slaker, 2017; Spero & Biddle, 2020). It has thus been argued that security mechanisms should be visible and available for inspection (Dourish et al., 2004). Chapters 4 to 6 of this dissertation investigate this argument empirically and study the effects of visible instances of security on perceptions of security in a series of user studies. We applied a mixed-methods approach combining both qualitative, in-person studies (Chapter 4), and more quantitative approaches (Chapter 5). In one study, we also combined qualitative expert co-creation and a novel survey experiment (Chapter 6).

The user study in Chapter 4 simulated an e-voting context to research participants in a lab setting. The results give some qualitative indication that displaying encryption to users might impact their perceived understanding of the e-voting process. However, the study did not measure how well the participants understood encryption. Qualitative analysis showed that the version that did not display encryption may be perceived as too simple and quick, thus not reassuring users with respect to the application's security. We also evaluated the effects of a second visual security mechanism in this study, vote verification, which is a required component of e-voting schemes (Olembo & Volkamer, 2013). In our study, the verification phase used a tracking number that allowed participants to verify that their vote had been taken into account once the simulated elections had ended (Ryan et al., 2016). The verification phase had a negative effect on UX, and our interviews showed that it was not aligned with the users' goal at that point, as they were not expecting to double-check their vote had been counted. Similarly, previous research had also found that verification is sometimes considered an "unnatural" concept for users, since it has no real-life equivalent they could use to understand how it works (Winckler et al., 2009). This example suggests that visible security mechanisms should be aligned with users' goals at a specific point in an interaction. Note that in Chapter 4, we selected only one visual representation of encryption and vote verification due to the qualitative lab setting.

Chapter 5 then addresses some of the open questions from the previous chapter and attempts to find security-inducing ways of describing encryption through text. We found that mentioning possible threats during data transmission led participants to worry about

security more than they would have without this information. This is aligned with the literature on warnings, which finds that a higher level of full and precise information ("explicit" information) can lead to a higher perception of risk (Laughery & Smith, 2006). Chapter 6 addressed multiple aspects that were not focused on in Chapter 5 – for example, the fact that participants were primed to think about security after the first question. The text in Chapter 5 was also presented in isolation, making it impossible to make any statements about the effects of possible combinations of text and visual representations. The textual descriptions of encryption in Chapter 5 were also kept relatively simple, and the study did not measure how accurately they were understood by participants.

Chapter 6 addressed these points by combining an extended iterative co-creation phase with both security and HCI experts and a large-scale vignette experiment spanning two use contexts with 2400 non-experts. The visual and textual representations were designed by security experts with the aim of creating technically accurate representations of encryption to be presented to non-experts. The vignette experiment tested the effect of these textual and visual indicators both alone and in combination, enabling us to understand causal relationships between the indicators and the outcomes of interest (UX, perceived security and understanding of encryption). The chapter further underlines the significant impact interface design elements can have on perceptions of security and understanding, particularly for textual indicators, less so for visual representation. These results corroborate and extend previous work showing that text can help users' understanding (Cranor, 2021; Wiedenbeck, 1999).

This group of empirical studies on the effects of visual instances on perceptions of security provides a number of findings that can be discussed in combination with one another, and with regard to the overarching research objectives. Both in Chapters 4 and 6, participants mentioned that interactions without any visible security display seemed too fast or easy, especially when the context was perceived as security-critical (online banking, e-voting). This opens up a design space we can use to communicate security properties to the user in which interactions are deliberately designed for a positive experience, perceived security and understanding of security properties. Our results show the relevance of measuring the effects of user interface elements such as visual and textual indicators on facets of experience such as perceived security, UX and understanding. This series of studies provides empirical underpinnings for design choices that include security indicators. Of course, malicious designers could apply these insights to deliberately imply security

properties that are not consistent with the system state, for example to make scam websites seem more trustworthy. Despite this potential for misuse, we hope that these studies provide insights for benevolent actors to better understand how their users perceive the security of an interaction and how to ensure that no erroneous perceptions are created through the design of an interaction.

8.1.4. Applying moments of negative UX to help people behave more securely through security-enhancing friction

Chapter 7 of this dissertation addressed the fourth research objective, namely, how designing for moments of negative UX in security-critical situations may help users behave more securely. Based on the experience-related insights from Chapters 3 to 6, we explored the idea of using the aforementioned design space to create friction that encourages certain, security-enhancing actions over other, more insecure actions. We proposed integrating the concept of UX into usable privacy- and security studies that attempt to change behaviors by applying friction. We introduced the novel concept of security-enhancing friction, friction that effectively reduces the occurrence of risk-taking while ensuring that overall UX (after use) is not compromised. By considering the objective to reduce risk-taking behaviors while simultaneously continuing to provide acceptable UX in order to avoid having people stop using the product or service, security-enhancing friction represents an actionable way to achieve better security while maintaining acceptable UX.

8.2. Contributions

This dissertation makes a number of contributions that can be categorized into the conceptual/theoretical, methodological and empirical levels.

On a **conceptual/theoretical** level, we provide a systematic review of the methods employed in UPS papers from 2014 to 2018 to induce a perception of privacy and security risks and identify methods, topics and user groups that are under-represented in the UPS research literature, suggesting potential directions for future UPS research to advance the field (Chapter 2). This is, to the best of our knowledge, the first review of methods used in UPS studies, and the contributions are thus relevant for the UPS research community as well as anyone wishing to gain a broad understanding of the field.

Our research adds knowledge on factors influencing the acceptability of privacy risks and gives insights into the non-instrumental aspects affecting the acceptance of privacy-relevant technology, including autonomy, control and context, encouraging the creation of acceptance models that take into account privacy and security concerns (Chapter 3). This contribution is relevant to both the research community and practitioners interested in the acceptance of privacy trade-offs who may want to adapt existing theoretical models to be more applicable to privacy and security-relevant technologies.

The dissertation conceptualizes security-enhancing friction, which can help users avoid risky behaviors while keeping overall UX at an acceptable level. Thereby, the results of the present work contribute to further bridging the disciplines of UPS and UX (Chapter 7). This contribution is of interest to researchers in both UPS and UX, but also practitioners who create products and services for end users that need to deliver a positive experience to users, but also respect their privacy and security.

On a **methodological** level, this dissertation applies a wide range of qualitative and quantitative methods that contribute to a better understanding of security perceptions in HCI and UPS. With studies ranging from 32 participants (Chapter 3) to 2400 participants (Chapter 6) and using methods such as focus groups (in-person and remote), expert co-creation, survey experiments and in-person user tests, we make several methodological contributions. In Chapter 2, we provide a framework for systematically analyzing methods in UPS studies and how they address perceptions of security and privacy risks. Publication venues that publish UPS work could use these guidelines to encourage better reporting, thus improving the quality of user studies and encouraging replicability and ethical approaches. Students could also consider these guidelines when writing research papers.

Chapter 6 applies an original methodological combination of an iterative co-creation process with security and HCI experts followed by a quantitative vignette experiment to investigate the best way of combining textual and visual indicators of security to describe encryption to non-experts. This is one of the few applications of vignette experiment methodologies to the interface design of security and privacy technologies. For instance, Naeini et al. (2017) applied a vignette experiment to explore user privacy expectations and preferences regarding Internet of Things technologies. In contrast, we did not explore preferences; instead, our results directly inform interface design. This chapter also demonstrated the applicability of vignette experiments to the context of user-centered interfaces. The method has proven highly relevant to understand the effects of visual and

textual elements on our variables of interest. Working with experts in the initial co-creation phase had the additional advantage of not requiring us to initially frame the security concept of encryption, since the experts already had an understanding of it. In this way, we were able to avoid one of the disadvantages of co-design methods with non-expert users, who can be strongly influenced by the initial framing of the threat (Fassl et al., 2021). This methodological contribution is relevant for researchers wanting to transmit and evaluate expert knowledge with participants who are not experts in security and privacy topics.

Chapter 7, with the concept of security-enhancing friction, also provides practical guidelines for the use of UX methods to gain a better understanding of the reasons underlying security and privacy behaviors, thus weaving together methods and objectives from both UX and UPS. This can be beneficial for researchers and practitioners who wish to improve users' security and privacy behaviors without compromising UX in a way that could lead to disuse.

Another contribution of this dissertation is of an **empirical** nature. In Chapters 3-6, we investigate the factors that induce a perception of risk in research participants, transitioning from the reasons why they accept trade-offs to their privacy (Chapter 2) to their perception of visible security mechanisms in the context of e-voting and other realistic use contexts (online banking and online pharmacies) (Chapter 4-6). These insights also lead to empirically sound recommendations for UX and UPS practitioners and researchers who wish to communicate security properties such as encryption or vote verification to non-expert users. The empirical studies thus contribute to work discussing the important question of whether security should be visible to end users, or hidden out of sight (Dourish et al., 2004; Spero & Biddle, 2020). We find that visible instances of security can be beneficial for user experience if designed in a user-centered way (Chapter 4). We also find that textual representations of encryption seem to have a positive effect on understanding of encryption and perceived security. This does not seem to be the case for novel visual representations of encryption, which did not have a statistically significant effect on perceived security, UX or understanding. These practical contributions are of relevance for researchers and practitioners in the field who can use these insights when designing technologies where security perceptions play a role.

Overall, this dissertation contributes to the field of HCI by improving the field's understanding of how researchers induce a perception of security and privacy risks and of

factors influencing people's security perceptions on a conceptual/theoretical, methodological, and empirical level.

8.3. Limitations and future work

Each chapter of this dissertation carefully outlines its respective limitations. Thus, in this section, we focus on the limitations relevant to this work at an overall level.

8.3.1. Risk representation

The analysis framework described in Chapter 2 lends itself to evaluating this dissertation in terms of risk representation and measurement methods. Within the studies making up this dissertation, we apply a variety of risk representation methods, including simulated risk through scenarios (e.g., Chapter 4) and a combination of naturally occurring and simulated risks (e.g., Chapter 3), with no studies using no representation of risk. In terms of how risk is measured, the studies in this dissertation mostly rely on self-reported data or a combination of observed and self-reported data (e.g., Chapter 4, where participants interacted with an e-voting application in a lab environment and we examined both observational data on usability issues and self-report responses). Limitations related to self-reported data can include a lack of accuracy compared to data measuring behaviors (Wash et al., 2017). Since the focus of this dissertation was to gain a better understanding of subjective experiences, not to improve security and privacy behaviors, the combination of methods applied was carefully chosen to provide rich insights into user perceptions rather than information about behaviors. To draw conclusions about behaviors, future studies should study how our results translate into security- and privacy-relevant behaviors.

8.3.2. Generalizability of results

The empirical user study results may be of limited generalizability, as none used participants' own data and we asked participants to situate themselves in scenarios for the purpose of our studies. These factors can influence security and privacy risk perceptions. For instance, Schechter et al. (2007) found that participants engaged in role-plays behaved less securely than participants using their own data in the same experiment. For our purposes, this trade-off was carefully considered: by using fictitious scenarios, we were able to recruit larger samples and thus achieve higher statistical power (e.g., in Chapter 6) than if participants would have had to download a smartphone application, which some

users might not have been willing to do. In all cases, the use of fictitious use scenarios and fictitious data protected participants' privacy, and the researchers facilitating the study were not able to see or access any personal data. Furthermore, the studied use contexts (online banking, e-voting) do not lend themselves very well to using participants' own data, as they are security- and privacy-critical and using participants' real data would have been invasive. To improve the applicability of our results to real-life circumstances, we used a number of scenarios with the intention of helping participants situate themselves in a realistic use context in both the in-person studies and during online data collection. All studies were carefully pre-tested to address any difficulties participants may have had with the scenarios.

Another limitation to the generalizability of our findings are our research participants. The studies in this dissertation did not use representative sampling methods, meaning that certain demographics are underrepresented, including older adults, children and teenagers, and people with disabilities, who can have different privacy and security needs (Ahmed et al., 2015; Dosono et al., 2015; Dosso & Chevalier, 2021; Lastdrager et al., 2017; McReynolds et al., 2017). Nevertheless, the dissertation contributed to demonstrate the related research gaps in the systematic literature review. Investigating the perceptions of security and privacy risks differences among underrepresented populations is a promising way forward to advance the understanding of security and privacy risk perceptions in HCI.

8.4. Moving forward with the subjective experience of security in human-computer interactions

It is challenging to study how users of digital systems perceive privacy and security risks, and researchers need to continuously balance realistic risk representation with ethical and legal concerns. Overall, we found that researchers creatively combine a variety of methods to study security and privacy perceptions (Chapter 2). Our review of the methods applied in UPS studies promotes transparency and improves our understanding of the practices that have been adopted. We provide a checklist and guidelines for the methodological information we recommend be included in all empirical UPS studies. Thereby, we contribute to an ongoing discussion regarding methods for risk representation within the UPS community. Moving forwards, we hope that the results of this dissertation contribute to negotiating a common understanding of valid, ethical and replicable science.

We also aimed to link privacy perceptions, technology acceptance models and user experience, and found that certain UX factors can help complement acceptance models (Chapter 3). In particular, aspects related to the psychological needs for autonomy and control were found to be important when considering privacy trade-offs, corroborating previous work (Hornbæk & Hertzum, 2017). The perceived usefulness (present in both technology acceptance and UX models) of a technology with privacy implications was crucial when judging its acceptability. Past experience was also found to be important when evaluating acceptability. Here, it seems relevant to point out the underrepresentation of negative emotions and experiences in work assessing technology acceptance and user experience (Hornbæk & Hertzum, 2017). Nevertheless, negative experiences could play a role in the acceptance of compromises to privacy trade-offs, as addressed for instance in a paper on how people were impacted by a large data breach (Zou et al., 2018). Including negative experiences would be relevant for UX to be more applicable to security and privacy contexts. In addition, momentary negative experience should be evaluated more closely, as it may help introduce a notion of security-enhancing friction, as we argue in Chapter 7. Other researchers have likewise argued that momentary negative emotion might contribute to meaningful experiences (Fokkinga & Desmet, 2012; Fokkinga, 2015).

Throughout this dissertation, user experience was a concept we found helpful for examining subjective perceptions of security and privacy. However, in order to enhance its applicability to privacy and security contexts, we suggest broadening the lens of UX to go beyond what is typically assessed with the concept. It is not precisely clear how traditional conceptualizations of UX (e.g., Mahlke, 2008, 2005) would take into account perceived security. While psychological needs include the need for security, it is measured through question items that are relatively general and do not seem as applicable to online interactions: “During this event, I felt that my life was structured and predictable”, “During this event, I felt glad that I have a comfortable set of routines and habits”, “During this event, I felt safe from threats and uncertainties.” (Sheldon et al., 2001). In this dissertation, we used the need for security in Chapter 3 when classifying qualitative answers and applied the aforementioned measurement items in Chapter 4. However, we found that this measurement is quite general and not always easily applicable to technology-related security contexts. Participants perceived the questions as rather general for assessing the perceived security in a specific interaction. In subsequent studies, we thus decided to use a one-item measurement of perceived security (“How secure or insecure did this

experience feel to you?") on a scale from 1 (very insecure) to 10 (very secure). In further developing research into security perceptions, scholars might address the question of how to best standardize the measurement of perceived security beyond such self-constructed measures.

While there are multiple examples of how user-centered design can lead to more secure behaviors (some of which I describe in Chapter 1.1.2), there is little theorizing on how perceptions of security can be linked to behavior conceptually. It would be relevant to see more theorizing on how perceptions of security can be conceptually linked to UX and how subjective perceptions of the interaction and its security may be linked to security-relevant behaviors. An early attempt is presented in Chapter 7 and the associated publication at the New Security Paradigms Workshop (Distler et al., 2020), another example relates theory on mental models to security-relevant behaviors (Spero & Biddle, 2020).

8.5. Conclusion

This dissertation's overarching research aim was to advance our understanding of individual's security perceptions when engaging with technology. In interactions that do not include technology, most people understand risks to their security and privacy and how to mitigate against them. When humans interact with technology, it can be much harder to accurately evaluate how secure or insecure an interaction is, especially without the technical knowledge of the underlying processes. The way human-technology interactions are designed can thus lead users to over- or underestimating the security provided. Consequently, user behaviors can be overly cautious or, conversely, people may adopt behaviors that do not account for the risks associated with the interaction. An in-depth understanding of the factors that play into these subjective perceptions of security is key to purposefully design for or against perceived security. In this dissertation, we explored the methods researchers use to induce a perception of risk in their empirical studies. The present work also provides empirical insights into the factors that play into subjective perceptions of security, both on a more general level in people's lives (as demonstrated in the focus groups exploring privacy trade-offs), as well as experimentally by varying interface elements and measuring people's response in terms of perceived security and overall experience. Finally, we explored implications for behavior by introducing the concept of security-enhancing friction, which attempts to combine the objectives of more secure behavior and acceptable user experience.

The presence of technologies in many areas of people's lives inevitably introduces risks to their security and privacy. It is important for those who design technologies to understand how people perceive and understand the security of technologies to avoid having their designs contribute to any erroneous perceptions. This dissertation gives some empirical indication that solely considering instrumental aspects in security-critical interactions may contribute to erroneous user perceptions of security and privacy risks, and by keeping security mechanisms hidden without exploring alternative visible representations, designs can contribute to a lack of understanding and mistaken perceptions of security. There is thus space to design for security-related interactions that optimize user experience, perceived security and understanding of security properties. This dissertation hopes to contribute to answering the question of *how* to best achieve such user-centered communication within security-relevant interactions.

8.6. References

Adams, D., Bah, A., Barwulor, C., Musaby, N., Pitkin, K., & Redmiles, E. M. (2018). Ethics Emerging: The Story of Privacy and Security Perceptions in Virtual Reality. *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*, 427–442. https://www.usenix.org/conference/soups2018/presentation/adams

Ahmed, T., Hoyle, R., Connelly, K., Crandall, D., & Kapadia, A. (2015). Privacy concerns and behaviors of people with visual impairments. *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, 3523–3532.

Angulo, J., & Ortlieb, M. (2015). "WTH..!?!" Experiences, Reactions, and Expectations Related to Online Privacy Panic Situations. *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*, 19–38. https://www.usenix.org/conference/soups2015/proceedings/presentation/angulo

Cranor, L. F. (2021). Informing California privacy regulations with evidence from research. *Communications of the ACM*, *64*(3), 29–32. https://doi.org/10.1145/3447253

Davis, F. D. (1985). *A technology acceptance model for empirically testing new end-user information systems: Theory and results* [PhD Thesis]. Massachusetts Institute of Technology.

Diefenbach, S., & Hassenzahl, M. (2011). The dilemma of the hedonic – Appreciated, but hard to justify. *Interacting with Computers*, *23*(5), 461–472. https://doi.org/10.1016/j.intcom.2011.07.002

Distler, V., Lenzini, G., Lallemand, C., & Koenig, V. (2020). The Framework of Security-Enhancing Friction: How UX Can Help Users Behave More Securely. *New Security Paradigms Workshop 2020*, 45–58. https://doi.org/10.1145/3442167.3442173

Dosono, B., Hayes, J., & Wang, Y. (2015). "I'm Stuck!": A Contextual Inquiry of People with Visual Impairments in Authentication. *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*, 151–168. https://www.usenix.org/conference/soups2015/proceedings/presentation/dosono

Dosso, C., & Chevalier, A. (2021). How do older adults process icons during a navigation task? Effects of aging, semantic distance, and text label. *Educational Gerontology*, *47*(3), 132–147. https://doi.org/10.1080/03601277.2021.1886634

Dourish, P., Grinter, R. E., de la Flor, J. D., & Joseph., M. (2004). Security in the Wild: User Strategies for Managing Security as an Everyday, Practical Problem. *Personal and Ubiquitous Computing*, *8*.

Egelman, S., Kannavara, R., & Chow, R. (2015). Is This Thing On?: Crowdsourcing Privacy Indicators for Ubiquitous Sensing Platforms. *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, 1669–1678. https://doi.org/10.1145/2702123.2702251

Fassl, M., Gröber, L., & Krombholz, K. (2021). Exploring User-Centered Security Design for Usable Authentication Ceremonies. *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, 15.

Fokkinga, S. (2015). *Design-|+ Negative emotions for positive experiences*.

Fokkinga, S., & Desmet, P. (2012). Darker Shades of Joy: The Role of Negative Emotion in Rich Product Experiences. *Design Issues*, *28*(4), 42–56. https://doi.org/10.1162/DESI_a_00174

Hassenzahl, M., Diefenbach, S., & Göritz, A. (2010). Needs, affect, and interactive products – Facets of user experience. *Interacting with Computers*, *22*(5), 353–362. https://doi.org/10.1016/j.intcom.2010.04.002

Hornbæk, K., & Hertzum, M. (2017). Technology Acceptance and User Experience: A Review of the Experiential Component in HCI. *ACM Transactions on Computer-Human Interaction*, *24*(5), 1–30. https://doi.org/10.1145/3127358

Lallemand, C. (2015). *Towards consolidated methods for the design and evaluation of user experience*. University of Luxembourg, Luxembourg.

Lastdrager, E., Gallardo, I. C., Hartel, P., & Junger, M. (2017). How Effective is Anti-Phishing Training for Children? *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*, 229–239. https://www.usenix.org/conference/soups2017/technical-sessions/presentation/lastdrager

Laughery, K. R., & Smith, D. P. (2006). Explicit information in warnings. In M. Wogalter (Ed.), *Handbook of Warnings* (pp. 605–615). CRC Press. https://doi.org/10.1201/9781482289688

Mahlke, S. (2008). *User experience of interaction with technical systems* [Doctoral dissertation.].

Mahlke, S. (2005). Understanding users' experience of interaction. *Proceedings of the 2005 Annual Conference on European Association of Cognitive Ergonomics*, 251–254.

McReynolds, E., Hubbard, S., Lau, T., Saraf, A., Cakmak, M., & Roesner, F. (2017). Toys That Listen: A Study of Parents, Children, and Internet-Connected Toys. *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, 5197–5207. https://doi.org/10.1145/3025453.3025735

Naeini, P. E., Bhagavatula, S., Habib, H., Degeling, M., Bauer, L., Cranor, L. F., & Sadeh, N. (2017). Privacy Expectations and Preferences in an IoT World. *Thirteenth Symposium on Usable Privacy and Security ({SOUPS} 2017)*, 399–412. https://www.usenix.org/conference/soups2017/technical-sessions/presentation/naeini

Olembo, M., & Volkamer, M. (Eds.). (2013). *Human-Centered System Design for Electronic Governance: Lessons for Interface Design, User Studies, and Usability Criteria*. IGI Global. https://doi.org/10.4018/978-1-4666-3640-8

Rader, E., & Slaker, J. (2017). The importance of visibility for folk theories of sensor data. *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*, 257–270. https://www.usenix.org/conference/soups2017/technical-sessions/presentation/rader

Rainie, L., & Duggan, M. (2015). *Privacy and Information Sharing*. Pew Research Center.

Ryan, P. Y., Rønne, P. B., & Iovino, V. (2016). Selene: Voting with transparent verifiability and coercion-mitigation. *International Conference on Financial Cryptography and Data Security*, 176–192.

Schechter, S. E., Dhamija, R., Ozment, A., & Fischer, I. (2007). *The Emperor's New Security Indicators*. 51–65. https://doi.org/10.1109/SP.2007.35

Sheldon, K. M., Elliot, A. J., Kim, Y., & Kasser, T. (2001). What is satisfying about satisfying events? Testing 10 candidate psychological needs. *Journal of Personality and Social Psychology*, *80*(2), 325.

Spero, E., & Biddle, R. (2020). Out of Sight, Out of Mind: UI Design and the Inhibition of Mental Models of Security. *New Security Paradigms Workshop 2020*, 127–143. https://doi.org/10.1145/3442167.3442174

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User Acceptance of Information Technology: Toward a Unified View. *MIS Quarterly*, *27*(3), 425–478. https://doi.org/10.2307/30036540

Venkatesh, V., Thong, J., & Xu, X. (2012). Consumer Acceptance and Use of Information Technology: Extending the Unified Theory of Acceptance and Use of Technology. *MIS Quarterly 36(1):157-178*, 22.

Wash, R., Rader, E., & Fennell, C. (2017). Can People Self-Report Security Accurately?: Agreement Between Self-Report and Behavioral Measures. *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, 2228–2232. https://doi.org/10.1145/3025453.3025911

Wiedenbeck, S. (1999). The use of icons and labels in an end user application program: An empirical study of learning and retention. *Behaviour & Information Technology*, *18*(2), 68–82. https://doi.org/10.1080/014492999119129

Winckler, M., Bernhaupt, R., Palanque, P., Lundin, D., Leach, K., Ryan, P., Alberdi, E., & Strigini, L. (2009). Assessing the usability of open verifiable e-voting systems: A trial with the system Prêt à Voter. *Proceedings of ICE-GOV*. https://www.irit.fr/page-perso/Marco.Winckler/publications/2009-ICEGOV.pdf

Zou, Y., Mhaidli, A. H., McCall, A., & Schaub, F. (2018). "I've Got Nothing to Lose": Consumers' Risk Perceptions and Protective Actions after the Equifax Data Breach.

Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018), 197–216. https://www.usenix.org/conference/soups2018/presentation/zou