PhD-FSTM-2022-038
The Faculty of Science, Technology and Medicine

# DISSERTATION

Presented on 26/04/2022 in Esch-sur-Alzette

to obtain the degree of

## DOCTEUR DE L'UNIVERSITÉ DU LUXEMBOURG EN INFORMATIQUE

by

Borče STOJKOVSKI
Born on 25 December 1985 in Virovitica (Croatia)

# USER EXPERIENCE DESIGN FOR CYBERSECURITY & PRIVACY: ADDRESSING USER MISPERCEPTIONS OF SYSTEM SECURITY AND PRIVACY

## Dissertation defence committee

Dr Gabriele LENZINI, Dissertation Supervisor
*Professor, Université du Luxembourg, Luxembourg*

Dr Vincent KOENIG, Chairman
*Professor, Université du Luxembourg, Luxembourg*

Dr Peter Y. A. RYAN, Vice Chairman
*Professor, Université du Luxembourg, Luxembourg*

Dr Melanie VOLKAMER. Member
*Professor, Karlsruhe Institute of Technology, Germany*

Dr Robert BIDDLE, Member
*Professor, Carleton University, Canada*

# User Experience Design *for* Cybersecurity & Privacy

*addressing user misperceptions of system security and privacy*

# Thesis Abstract

The increasing magnitude and sophistication of malicious cyber activities by various threat actors poses major risks to our increasingly digitized and inter-connected societies. However, threats can also come from non-malicious users who are being assigned too complex security or privacy-related tasks, who are not motivated to comply with security policies, or who lack the capability to make good security decisions. Neglecting the importance of user experience (UX) and the absence of a human-centered design approach, can not only lead to a system that fails to meet user needs and requirements, but can also induce user misperceptions about the security and privacy aspects of a system. This can have a direct impact on the effective and secure application of those systems as well as on users' decisions to adopt a specific security or privacy-enhancing technology. This thesis posits that UX design methods and practices are necessary to complement security and privacy engineering practices in order to (1) identify and address user misperceptions of system security and privacy; and (2) inform the design of secure systems that are useful and appealing from end-users' perspective.

The first research objective in this thesis is to provide new empirical accounts of interaction and UX aspects in three distinct contexts that encompass security and privacy considerations, namely: cyber threat intelligence, secure and private communication, and digital health technology. The second objective is to empirically contribute to the growing research domain of mental models in security and privacy by investigating user perceptions and misperceptions in the afore-mentioned contexts. Our third objective is to explore and propose methodological approaches to incorporating users' perceptions and misperceptions in the socio-technical security analyses of systems. To reach these objectives, we employed a case study approach driven by the following core research questions:

**RQ1:** *How do people experience the use and/or anticipated use of the security or privacy-critical systems under investigation in these three contexts?*

**RQ2:** *What perceptions and misperceptions do users have about the security and privacy aspects of the systems under investigation?*

**RQ3:** *Which methods can be used to incorporate users' perceptions and misperceptions in the socio-technical security analyses of security and privacy-critical systems?*

Qualitative and quantitative user research methods with experts as well as end users of the applications and systems under investigation were used to achieve the first two objectives. To achieve the third objective, we also employed simulation and computational methods.

Following the introduction (Chapter 1) we outline the necessary background knowledge which focuses on user experience design and evaluation, mental models, and user misperceptions of security and privacy, followed by an overview of the state of the art in three specific cybersecurity and digital privacy contexts (Chapter 2). The rest of the dissertation adopts the following structure:

**CYBER THREAT INTELLIGENCE: CTI sharing platforms**

**Chapter 3.** CTI sharing platforms are becoming indispensable tools for cooperative and collaborative cybersecurity. This thesis offers a unique contribution towards understanding the constraining and enabling factors of security information sharing within one of the leading CTI sharing platforms, called MISP. We report on a number of user studies conducted over a period of two years and shed light on the strengths and weaknesses of MISP from an end-users' perspective. Finally, we discuss the role usability and UX (could) play in effective CTI sharing.

**Chapter 4.** We propose a conceptual workflow and toolchain that would seek to detect user (mis)perceptions of key tasks in the context of CTI sharing, such as verifying whether users have an accurate comprehension of how far information travels when shared in a CTI sharing platform. We contextualize our concept within MISP as a use case, and discuss the benefits of our socio-technical approach as a potential security analysis tool, simulation tool, or educational / training support tool.

**SECURE & PRIVATE COMMUNICATION: Secure Email**

**Chapter 5.** Email related threats continue to be a prime vector for cyber attacks. We propose and describe *multi-layered user journeys*. This conceptual framework serves to capture the interaction of a user with a system as she performs certain goals along with the associated user beliefs and perceptions about specific security or privacy-related aspects of that system. We instantiate the framework within a use case, a recently introduced secure email system called $\mathsf{p} \equiv \mathsf{p}$, and demonstrate how the approach can be used to detect misperceptions of security and privacy by comparing user opinions and behavior against system values and objective technical guarantees offered by the system.

**Chapter 6.** We perform an initial validation of the findings obtained by the socio-technical security analysis of $\mathsf{p} \equiv \mathsf{p}$ in Chapter 5. We present two sets of user studies focusing on the usability and effectiveness of $\mathsf{p} \equiv \mathsf{p}$'s security and privacy indicators and their traffic-light inspired metaphor to represent different privacy states and guarantees. We conclude with a discussion on the potential implications on the perceived security and use of such systems.

**DIGITAL HEALTH TECHNOLOGY: Contact Tracing Apps**

**Chapter 7.** Considering human factors when exploring the adoption as well as the security and privacy aspects of COVID-19 contact tracing apps is a timely societal challenge as the effectiveness and utility of these apps highly depend on their widespread adoption by the general population. We present the findings of eight focus groups on the factors that impact people's decisions to adopt, or not to adopt, a contact tracing app, conducted with participants living in France and Germany. We report how our participants perceived the benefits, drawbacks, and threat model of the contact tracing apps in their respective countries, and discuss the similarities and differences between and within the study groups.

In Chapter 8, we consolidate the findings from these studies and discuss future challenges and directions for UX design methods and practices in cybersecurity and digital privacy.

# Acknowledgments

I would like to start by expressing my heartfelt gratitude to my supervisor, Prof. Gabriele Lenzini. I am deeply thankful for having been given the opportunity to embark on this challenging journey under his exceptional mentorship and guidance. I am greatly appreciative of the trust Prof. Lenzini placed in me and the academic freedom he afforded me while pursuing my research. His compassionate support, wise counsel, and openness for knowledge exchange, complemented by culinarily delights and social moments spent beyond the realm of formal workdays have enriched my experience as a PhD student, allowing me to learn and grow tremendously as a researcher and a person.

My deep gratitude goes to Prof. Vincent Koenig, who closely followed my journey from the very beginning and whose knowledge, experience, and kind support greatly helped me steer my path. Our discussions and collaboration allowed me to reflect on and refine my work and to become better at realizing my objectives, both academically and professionally.

I would also like to sincerely thank Prof. Peter Y. A. Ryan for his guidance and support of my work and learning aspirations. I enjoyed our conversations, and I appreciate the opportunities presented to expose and challenge myself to new perspectives and knowledge.

My profound gratitude goes to Prof. Melanie Volkamer, Prof. Robert Biddle, and Prof. Konrad Wrona for accepting to be part of my dissertation defense committee, for their time, and for their thought-provoking and valuable questions and comments.

I would like to thank my co-authors Ruba Abu-Salma, Vincent Koenig, Gabriele Lenzini, Salvador Rivas, Karen Triquet, and Itzel Vazquez Sandoval for their collaboration, trust and patience. I thank all the participants involved in the research studies presented in this dissertation as well as the project partners $\mathsf{p} \equiv \mathsf{p}$ foundation | security and the Computer Incident Response Center Luxembourg. My research was only possible thanks to funding by the Luxembourg National Research Fund through grant PRIDE15/10621687/SPsquared.

The idea of embarking on a PhD journey was born during my master program. I would therefore like to thank my prior mentors Prof. Wendy Mackay, Prof. Michel Beaudouin-Lafon, Prof. Dirk Heylen, Prof. Mariët Theune, and Prof. Dennis Reidsma for sparking an interest that eventually set me on course to consider studies and research at a doctoral level.

A special thanks goes to all my colleagues at the University of Luxembourg with whom I shared the ups and downs of this journey. In particular, I would like to acknowledge current and former members of the IRiSC research group at SnT who provided me with much needed feedback, inspiration, encouragement, and support throughout the years. During my doctoral studies, I was fortunate to be closely linked to two additional and enriching re-

search units, APSIA and the HCI research group, as well as the SP2 doctoral training unit. I am immensely grateful for the opportunities to discuss, socialize as well as to learn from and together with so many talented researchers. Moreover, I am honored to count many of them as my friends.

Outside of the University, I am particularly thankful to a great deal of friends, relatives and extended family who wholeheartedly supported me along my journey, who were considerate of my needs and availability, and who made sure I stayed in touch with the world outside of my doctoral bubble.

I will be forever indebted to my parents, Katica and Ljupče, whose love and support knows no limits. For their eternal positive outlook and determination that never ceases to inspire me, and their values and principles that guide me, I am thankful! Exceptional gratitude goes to my sister Jovana, brother-in-law Trajče, niece Sofi and nephew Mateo, for their heart-warming love and care as well as inexhaustible imagination and motivation.

Finally, I would like to acknowledge the tremendous inspiration, support, and encouragement from my partner Karen. I can hardly imagine reaching this milestone if it wasn't for her softhearted understanding, her exceptional strength, and her remarkable wit. A destination has been reached, but our journey continues.

In closing, I would like to make a slightly more distant, but ever pervasive recognition of the creators and creatives behind the musical notes, the stills and the motion pictures that carried me through this journey. A special thank you to the Worldwide FM roster of artists and presenters for the auditory joy, motivation, and good vibrations that accompanied me throughout the years, in particular during lonesome lockdown periods.

# Contents

*Progress imposes not only new possibilities for the future but new restrictions.*

Norbert Wiener

# 1 Introduction

It is widely accepted that rapid advancements in Information and Communication Technologies (ICT) have been key drivers of economical, technological and social change of unprecedented scale and speed. As digital technologies and services continue to evolve and permeate virtually every aspect of our lives, so are we exposed to intensifying forces of digitalization, transforming the ways we learn, work, socialize, access services, and so on.

An inherent characteristic of this continuing shift is that the interactions that people have with, by means of, or in the presence of interconnected computers, mobile phones, wearables, and other digital mediums, are becoming more and more critical from a security and/or privacy perspective. Yet the far-reaching implications of this corollary are oftentimes neglected, underestimated, or perplexing for developers, end users, regulators, and other stakeholders at the technical, socio-technical, and governance layers of this complex environment called cyber space.

Over the past years, we have witnessed a great deal of scandalous data breaches by criminal groups and foreign adversaries, unethical and unlawful data-enabled practices by various corporations as well as revelations about mass surveillance capabilities and actions by some governments and agencies. These have brought to the fore the significance and urgency of protecting critical infrastructures, businesses, and above all the security and safety of citizens as well as core values and fundamental rights in the digital age.

A positive development in this direction is the growing to nearly universal acknowledgement that addressing the security and privacy challenges of today and tomorrow requires a holistic perspective and multi-disciplinary discourse and collaboration. Be that as it may, protecting the different interdependent layers of cyber space and driving the adoption of security technologies is a Herculean task.

The ever-increasing magnitude and sophistication of malicious cyber activities by various threat actors indubitably poses distressing risks to our increasingly digitized and interconnected societies. However, as highlighted in literature, threats to security and privacy can also come from non-malicious users of digital products, services, and systems who are being assigned too complex security or privacy-related tasks, who are not motivated to comply with security policies, or who lack the capability to make good security decisions [78]. Furthermore, neglecting the importance of user experience and the absence of a human-centered design approach during the different stages of a system's lifecycle, can not only lead to a system that fails to meet user needs and requirements, but this can also induce or reinforce user misperceptions about the security and privacy aspects or guarantees of a particular system or technology. This can have a direct impact on the effective and secure application of those systems as well as on users' decisions whether to adopt and use a specific security or privacy-enhancing technology, or not.

## 1.1 Motivation

The current state of affairs regarding user-facing cybersecurity and digital privacy challenges motivates the need to further embrace interdisciplinary approaches not only in declaration, but also in practice. Hereupon, this doctoral dissertation is motivated by further opportunities that exist at the fertile intersection of the computer security and human-computer interaction (HCI) disciplines applied within the context of real-world systems. Through the lens of user experience design more concretely, this thesis aspires to examine known and emerging user-related conundrums in different systems that aim to address specific security and privacy problems or respond to matters of pressing societal concern.

Blending the knowledge base, processes, and methods of science, engineering, and design, the work presented in this thesis is grounded in a research and design challenge that guides the identification of questions and opportunities in the contexts and systems under investigation. It reads as follows:

---

*How can user experience (UX) design methods and techniques complement security and privacy engineering practices in different cybersecurity and digital privacy contexts in order to (1) identify and address user misperceptions of system security and privacy; and (2) inform the design of secure systems that are useful and appealing from end-users' perspective?*

---

The above formulation refers to a number of concepts and sub-topics which should be briefly highlighted so that the motives behind the chosen research path may be understood.

### The quest for secrecy and information protection

Protecting information and communicating secretly has been a human activity since ancient times [190]. Next to the development of the methods and artifacts to encipher and hide messages over the centuries, the parallel art and science of analyzing and breaking the different cryptographic security systems has been of utmost importance, having a profound influence on the course of history leading to the world of today. To illustrate, there is nowadays widespread recognition of how cracking the code of the Enigma cipher machines helped turn the tide during World War II [190].

Modern day cryptography has gone a long way from its military beginnings. Finding many applications beyond the warfare and espionage domain, cryptography underpins the security protocols that enable the ongoing digital transformation of our societies. The legacy of building cryptographic security systems by military and secret government organizations for a long time, however, has left many everyday users bewildered by the complexity of current security mechanisms and their policies in new application contexts that do not necessarily require military-grade protection nor exhibit such organizational characteristics. As an example, take the still ubiquitous mandates to frequently change our passwords in adherence to stringent rules and criteria*.

The converse scenarios of insufficient protection are unfortunately also common. Sensitive data of and about individuals, governments, and organizations gets eavesdropped, exfiltrated, deleted, locked, or sold. Critical infrastructures and essential services get sabotaged. Misinformation, hate speech, and discrimination get amplified online. There are certainly many factors at play here, but to a large extent, it is due to poorly deployed protection mechanisms, flawed processes, or insufficient motivation and capabilities of those tasked with building, protecting, and maintaining secure and privacy-preserving digital systems. Thus, a key challenge that hardly any system designer can overlook in today's interconnected world revolves around understanding what needs protecting and how best to achieve that.

*One could also note here that these are often based on outdated and fallacious password security guidelines [66, 234, 392].

### Engineering security and privacy

Over the course of time, *security engineering* has emerged as a distinct discipline dealing with the tools, processes, and methods which are needed to build systems that "remain dependable in the face of malice, error, or mischance" [15, p. 3]. This description implies that particular focus in the design, implementation, and testing of systems needs to be placed on the possible adversaries: who they might be, why they would attack the system, and how they could or would do that. It also suggests that the system could be sabotaged from inside as people employing the system could be an attack vector, could have malicious intentions or could inadvertently disrupt the system or introduce vulnerabilities. These threats are inherently related to the assessment of risk in the given contexts and what mechanisms (social and technical) could be put in place as an appropriate mitigation response. According to Anderson, the dependability of systems relies on four concepts and their interaction, namely, policy, mechanisms, assurance, and incentives [15]. Security engineering, consequently, requires not only computer security and cryptography expertise, but also cross-disciplinary insights from software and systems engineering, human factors and applied psychology, organizational studies, economics, law, etc. [15].

While seen as a branch of security engineering by some, and as a distinct complementary discipline by others, *privacy engineering* is an emerging field of research and practice. According to Gürses and del Alamo, it focuses on "designing, implementing, adapting, and evaluating theories, methods, techniques, and tools to systematically capture and address privacy issues in the development of socio-technical systems" [156, p. 40]. In similar fashion to security engineering, it is inherently interdisciplinary. Utilizing tools, techniques, and insights from other computer science subdisciplines and liaising closely with other topics that inform privacy, in particular law, ethics, and norms [156], privacy engineering aims to turn privacy laws and user expectations into meaningful information systems [256].

A key theme transcending security and privacy engineering is the necessity to consider the multitude of factors at interplay in the environment in which the engineered artifacts exist. One such facet deals with the topic of human factors[†]. This thesis focuses on human-centered security and privacy as an overarching umbrella of different user-centric aspects that are of prime importance when engineering security and privacy i.e., in the deliberate attempts to design, develop, and deploy dependable, secure and privacy-preserving systems.

[†]While the phrase *human factors* is ubiquitously used in the computer security and privacy domain, in the Human-Computer Interaction literature it can have connotations to the field of Human Factors/Ergonomics which traditionally had narrow and limited views of *users* in computer systems and the settings in which they work, often reducing the human to merely another system component characterized by certain constraints such as limited attention span, etc. [29]

The aspects under closer scrutiny relate to the perceptions and misperceptions that users have regarding the security and privacy guarantees offered by systems in different contexts as well as users' impressions of their experience interacting with such systems. We elaborate on these aspects and discuss their relevance next.

### The need to investigate user (mis)perceptions of system security and privacy

The necessity to build secure systems that users can understand and correctly deploy within their context of use is no modern desideratum. In 1883 Kerckhoffs enunciated six design principles for military ciphers, some of which are still critically important to the present day [197]. Of particular relevance to our topic is the sixth principle which states that given the circumstances in which it is to be used "*the system should be easy, neither requiring knowledge of a long list of rules nor involving mental strain*" [190, p. 235]. Almost a century later, in their seminal work on the protection of information in computer systems, Saltzer and Schroeder put forward eight principles that can guide the design of protection mechanisms and contribute to their implementation without security flaws [292]. One of them is the concept of psychological acceptability, which they described as follows: "*It is essential that the human interface be designed for ease of use, so that users routinely and automatically apply the protection mechanisms correctly. Also, to the extent that the user's mental image of his protection goals matches the mechanisms he must use, mistakes will be minimized. If he must translate his image of his protection needs into a radically different specification language, he will make errors*" [292, p. 1283].

The arguments above clearly indicate the significance of designing ciphers and protection mechanisms around the needs and capabilities of their users. Yet, despite such early acknowledgments of the fundamental role users play in achieving the goals of security and privacy when interacting with protection mechanisms as well as the recognition of potential risks that might arise should the design fail to take this into account, security solutions became ever more complex and intrusive over time [170]. Historically, the design of security solutions took primarily highly trained technical users into consideration [195]. However, with the proliferation of computers and communication networks into the enterprise and eventually the home, the user base of security solutions and protection mechanisms broadened to include different roles and skill sets. This revealed limitations and deficiencies in existing approaches to securing systems and illuminated new threats and challenges:

- On the one hand, the defenses were often not working because the security was not protecting against what attackers were ultimately exploiting. Think of easily-guessable passwords and their reuse across systems, spear-phishing or any other social engi-

neering avenue attackers would tend to prefer before taking the more costly path of attacking the technical components of a system [301].

- On the other hand, proposed security solutions were unusable. Not only by "unmotivated" and less technically apt *Janes* [274] and *Johnnys* [372] who did not have extensive threat and attacker models, but also by experts [28]. Consequently, protection mechanisms were underutilized, if adopted at all, and more often than not, they were circumvented by users who did not agree with or understand the reasoning behind the security technologies, procedures, and policies they were confronted with while trying to do their job [8, 201, 252].

While much effort and progress has been made towards improving our defenses and resilience on different levels, such socio-technical problems are still prevalent as evidenced, for example, by the prominence of user-related and non-malicious threats in the ENISA Threat Landscape 2021 report [110]. To move the needle in a positive direction, the design of systems in general, and of the protection mechanisms in particular, needs to be grounded in real human behavior and accompanied by coherent and comprehensible conceptual models so that users could better understand the necessity for protection as well as evaluate the efforts required to deploy the mechanisms that enforce security and privacy [252]. To this end, it is of paramount importance to investigate which threats and risks users perceive in connection with the different digital products, services, and systems that they interact with or might encounter in the future. Understanding user perceptions and misperceptions of the security and privacy guarantees offered by those systems could additionally help avoid situations where users have a false sense of security or insecurity, both of which can have dire consequences. As research on user mental models[‡] of security and privacy has shown, perceptions of the efficacy of security practices impact the adoption of security technologies [351]. Therefore, system designers cannot afford to overlook the implications of these aspects in a world where every user interaction is becoming increasingly sensitive from a security or privacy perspective.

**The design of secure and privacy-enhancing systems should also focus on *usefulness* and *appeal* from end-users' perspective**

USEFULNESS. Nielsen describes *usefulness* as "the issue of whether the system can be used to achieve some desired goal" [248, p. 24]. It may well be the case that for certain users, or for specific applications, the sole provision of security and privacy guarantees (against a par-

[‡]Mental models are sets of assumptions or beliefs about how a (security or privacy-critical) system works.

ticular threat) sufficiently responds to identified user needs and requirements. For instance, a system administrator resorting to a software tool that generates and securely stores strong passwords. Providing adequate security and privacy is becoming a common user expectation and key trust factor for more and more systems. That being said, the security and/or privacy aspect is generally only one of the factors at play, especially for interactive systems. Security for most users is often a secondary task, meaning that people primarily employ digital products and services for purposes other than security [262, 385]. So, what makes a secure system useful? Stated differently, what makes a system useful in general, if for a moment we disregard the fact that the system at hand also provides adequate security and privacy guarantees that the user may or may not be aware of or even interested in?

According to Grudin [152], *usefulness* is comprised of two parts, *utility* and *usability*. In short, *utility* denotes whether a system provides the functionality users really need; *usability* refers to how well users are able to make use of that functionality [248]. For example, a Health app on a smartphone can serve to help manage, store, and keep track of health related information about an individual, thereby offering a clear utilitarian value for certain population segments. The usability of this app could be found, for instance, in the *ease of use* when adding new health data, when reading personal health metric trends, or when sharing data with a healthcare team.

While there exist differences in the HCI literature with respect to the definitions, relationship, and superiority of these factors [150, 220], both notions are considered to be important quality attributes that should be equally in the focus when designing or evaluating interactive systems [185]. Taking into account both aspects together has not always been the case, however. Different system development contexts, geographical differences, and a number of other reasons, have led to the emergence of distinct communities that historically focused on software function and on software form separately, frequently giving rise to (i) potentially useful systems that were unusable or to (ii) usable systems that were not serving a recognizable purpose [152].

This siloed design approach has been typical also in the case of secure-sensitive systems. On one end of the spectrum i.e., when looking at systems that primarily have a security focus, the human factor has oftentimes been largely neglected when designing, developing or rolling out security technologies, creating conditions for pernicious interpretations that people are the "weakest link" in the security chain [296]. On the other end of the spectrum, security has been wrongly perceived as a feature that can be simply added to a nearly complete system or bolted onto an existing one, rather than regarded as a system-wide property that requires careful planning and design [358]. To make things worse, aligning different system quality properties such as security and usability has been a notorious challenge, fos-

tering the fallacy that there exists an unresolvable trade-off between achieving security and making systems easy to use [385]. Fortunately, a great deal of interdisciplinary research on the human factor in security over the past two decades has significantly contributed towards narrowing the chasm between these "competing" design goals. While much focus here has been placed on *usable security*, some researchers have accentuated that the emphasis should be put on usefulness more broadly and that we need to go beyond the design of usable security technologies towards the design of useful secure applications [313].

APPEAL. Usefulness is not always enough to make a particular product, service, or system appealing for the end user, however. The question of appeal is closely related to the issue of differentiation i.e., why a particular user would choose one alternative over another if they have the same perceived utilitarian and usability value in her eye. In fact, some products or systems may be more preferred even though they have lower utilitarian or usability qualities, in particular in specific contexts. Take the preference of listening to music on vinyl records over any of the latest digital offerings, or driving a car with a manual transmission over an automatic one, for instance. The physical world is abundant with such examples, but we do not have to think too hard to find the same in the digital one. What is more concerning for our discussion is that it is not uncommon for people to choose systems that could lead to negative security and privacy outcomes over more secure and privacy-preserving alternatives which offer the same functionality and comparatively have similar usability properties. This calls for an expanded view and understanding of the factors that influence people's judgments of appeal and decisions to adopt a (security-sensitive) system.

This is certainly a non-trivial topic capturing the interest of diverse disciplines, looking into factors that play a role or developing theories that model how users come to accept and use a technology. In the HCI field, the broader question of appeal started getting more attention at the turn of the new millennium as exemplified by the work of Hassenzahl et al. [167]. Against the backdrop of an expanded notion of the user experience, which encompasses both subjectively perceived *pragmatic* and *hedonic* quality dimensions, the authors proposed a model to reason about software and system appeal, arguing that both aspects play an almost equal role in people's judgments [164, 167].

To briefly illuminate this expanded notion of the user experience and highlight its significance, we need to take a retrospective look. During a period often referred to as the third wave in HCI, the focus of computing shifted from the workplace towards new use contexts and applications, like the new spheres of the home, leisure and the arts [49]. The human-computer interactions were consequently transformed and enriched with new elements such as culture, identity, values, emotions, and experience [48]. In contrast to the

existing views of interaction which focused on *pragmatic* quality aspects only, third wave perspectives put emphasis also on *hedonic* dimensions that fulfill general human needs [90]. While the *pragmatic* group refers to instrumental or task-related aspects related to traditional usability (such as effectiveness and efficiency), the *hedonic* group is not related to the user task, but rather refers to aspects such as visual aesthetics and beauty, joy of use, stimulation, surprise, personal growth, and so on [30].

### The added value of User Experience Research

While, from the perspective of a security or privacy engineer, the afore-mentioned pragmatic and hedonic aspects may be bundled under the umbrella term of *human factors*, many of those engineers would probably agree that they do not deal with such aspects directly, nor that their core domain of expertise lies there. As security "cannot be seen in isolation from time, place, emotions, experiences, purpose of the interaction or other actors" [225, p. 2327], security and privacy engineering needs to turn to adequate methods and practices that can capture, reason about, and integrate those factors which would otherwise be overlooked.

The grand design challenge, thus, lies in building secure and privacy-enhancing systems that empower users to be effective in their primary tasks and offer a seamless user experience, while keeping any inherent costs within reasonable limits [252]. This thesis posits that user experience design methods and practices are well-positioned to contribute significantly towards this goal. Not only by shedding light on many missing pieces of a challenging socio-technical puzzle, but also by reshuffling the strategy of completing the picture. By placing human actors (be it end users, system administrators, developers, or any other target population of interest) at the forefront of the design activities that amount to building, deploying, and maintaining secure and privacy-enhancing systems, we can more-readily ensure that the security tasks fit to the human, rather than the other way round.

This change of perspective has been a long held mission by the usable security community. For instance, two decades ago, in line with ISO 9241-11:1998 [179], Sasse and colleagues enunciated four key components that need to be aligned in order to make the security task usable and fit to the human: (i) the capabilities and limitations of the users; (ii) their goals as well as the fundamental and enabling tasks that they carry out in order to accomplish the goals; (iii) context i.e., the physical and social factors that need to be considered and accommodated; and (iv) the capabilities and limitations of the technical artifacts on which the security mechanisms are deployed [295]. By adopting a UX-led approach, system designers can go a step further and take a more holistic view of the intrinsically-connected *sensual*, *emotional*, *compositional*, and *spatio-temporal* aspects that have an impact on the

relationship between people and (security and privacy-enhancing) technology [230].

Just as the UX movement at its onset searched for new approaches to the design of interactive products by going beyond the purely cognitive and task-oriented aspects of interaction [30], so can our motivation in this thesis be summarized as a quest to transpose the UX research lens to new cybersecurity and digital privacy contexts. What lies at the core is the aim to improve the quality of security and privacy-sensitive digital products, services, and systems by incorporating experiential qualities of technology use.

## 1.2 Objectives, Research Questions and Approach

### 1.2.1 Objective 1

The first research objective of this thesis is to provide new empirical accounts of interaction and user experience aspects in three distinct contexts that encompass security and privacy considerations, namely: cyber threat intelligence, secure and private communication, and digital health technology. To attain this objective, we ask the following overarching research question, and constituent sub-questions:

**RQ1** How do people experience the use and/or anticipated use of the security or privacy-critical systems under investigation in these three contexts?

- *What motivates people to employ the systems and which factors facilitate or impede their use and adoption?*
- *What are users' goals, tasks, and actions within the studied systems?*
- *What experiences emerge with respect to the use or anticipated use of these systems and how does the user experience develop over time?*

### 1.2.2 Objective 2

The second objective of this thesis is to empirically contribute to the growing research domain of mental models in security and privacy by investigating user perceptions and misperceptions of security and privacy in the afore-mentioned contexts. To reach the objective, we ask the following research question and sub-questions:

**RQ2** What perceptions and misperceptions do users have about the security and privacy aspects of the systems under investigation?

- *What is the role of the system image, in particular security and privacy indicators, on users' perceptions and misperceptions of security and privacy?*

- *What are the security and privacy implications associated with the identified misperceptions as well as the implications on the adoption of the studied systems?*
- *How can we address the identified misperceptions?*

### 1.2.3 Objective 3

The third research objective of this thesis is to explore and propose methodological approaches to incorporating users' perceptions and misperceptions in the socio-technical security analyses of systems. To reach this objective, we ask the following question and corresponding sub-questions:

**RQ3** Which methods can be used to incorporate users' perceptions and misperceptions in the socio-technical security analyses of security and privacy-critical systems?

- *How can we automate the identification of misalignments between the objective security and privacy guarantees offered by a system and the subjective guarantees as perceived by users?*
- *How can we incorporate interaction behavior and user experience aspects that could lead to negative security and privacy outcomes?*
- *What insightful discoveries about a system's socio-technical security or insecurity can be obtained via such analyses?*

### 1.2.4 Approach

To improve our understanding of user experience aspects as well as misperceptions in specific cybersecurity and digital privacy contexts, we took a case study approach which is suitable for the exploratory nature of our research. Case studies can be defined as "analyses of persons, events, decisions, periods, projects, policies, institutions, or other systems that are studied holistically by one or more methods" [339, p. 513].

To achieve the first and second objective, we used qualitative and quantitative user research methods with experts as well as actual and prospective end users of applications and systems in the contexts introduced next. To achieve the third objective, we additionally employed simulation and computational methods. As illustrated in the structure overview of this thesis, Section 1.4, we conducted a number of user studies wherein we instantiated the above-formulated research questions. More details on the methodological approach and deployed methods in each study are provided in the corresponding chapters of this thesis.

## 1.3 Contexts, Challenges and Contributions

Historically, there have been a few major themes in usable security and privacy research, such as user authentication; email security and PKI; anti-phishing efforts; web, mobile, and social media privacy, etc. [133]. While keeping such longer-term strategic trends in sight, this thesis addresses current needs, focusing on specific security and privacy problems of the day and responding to matters of pressing societal concern. The following three cybersecurity and digital privacy contexts serve as the locus of our research activities.

### 1.3.1 Cyber Threat Intelligence

The ever-increasing scale and complexity of cyber attacks and cyber-criminal activities necessitate secure and effective sharing of cyber threat intelligence (CTI) among a diverse set of stakeholders and communities. CTI sharing platforms are becoming indispensable tools for cooperative and collaborative cybersecurity. Nevertheless, despite the growing research in this area, the emphasis is often placed on the technical aspects, incentives, or implications associated with CTI sharing, as opposed to investigating challenges encountered by users of such platforms. To date, user experience (UX) aspects remain largely unexplored.

This thesis offers a unique contribution towards understanding the constraining and enabling factors of security information sharing within one of the leading cyber threat intelligence (CTI) sharing platforms. Through the use case of MISP [240], an open source CTI sharing platform used by more than 6,000 organizations worldwide, we establish the first UX benchmark in this context and uncover what users value about the studied platform and why. This investigation not only provides actionable inputs to the developers of MISP, but equally serves to highlight key findings and UX recommendations of relevance to CTI sharing platforms more generally. Besides advancing our understanding of human factors and interaction aspects within the CTI sharing context, this report also draws attention to the possible negative outcomes in terms of CTI sharing effectiveness or (inadvertent) disclosure of sensitive information due to usability issues or overall poor UX. To investigate this further, this thesis puts forward a workflow and toolchain for analyzing users' perceptions in CTI sharing platforms, in particular regarding users' understanding of how far the information that is shared in a CTI platform travels and whom it reaches.

#### Related Publications

**Chapter 3:** Borce Stojkovski, Gabriele Lenzini, Vincent Koenig, and Salvador Rivas. 2021. What's in a Cyber Threat Intelligence Sharing Platform? A Mixed-Methods User Experience Investigation of MISP. In *Annual Computer Security Applications Conference*

(Virtual Event, USA) *(ACSAC)*. Association for Computing Machinery, New York, NY, USA, 385–398. https://doi.org/10.1145/3485832.3488030. [327]

**Chapter 4:** Borce Stojkovski and Gabriele Lenzini. 2021. A workflow and toolchain proposal for analyzing users' perceptions in cyber threat intelligence sharing platforms. In *2021 IEEE International Conference on Cyber Security and Resilience (CSR)*. 324–330. https://doi.org/10.1109/CSR51186.2021.9527903. [323]

### 1.3.2 Secure and Private Communication

Email use has been continuously growing, with the total number of emails sent and received *per day* forecast to exceed 376 billion by the end of 2025 [337]. At the same time, email related threats continue to be a prime vector for cyber attacks exploiting the human element [110]. Researchers and practitioners have highlighted major challenges and difficulties associated with attaining protocols that are able to satisfy security properties, especially when people are key elements in the achievement of security goals. The impressions that a user has about distinct aspects of a system depend on the experience perceived before, while, and after interacting with it. Considering the effects of these interactions in a security analysis gives rise to a new class of security properties that can be defined in terms of misalignments between the system's technical guarantees and the user's perceptions of them. This motivates us to propose a new framework to detect and reason about misaligned conceptual models, and demonstrate the framework within an email use-case. In this context, we present a model (which combines elements related to system-user interaction) for reasoning about the security of systems from a socio-technical perspective. This refers to and builds on the concept of security ceremonies, but relies on UX notions and on security analysis techniques to put together the information needed to verify misalignment properties about users' perceptions and system's security guarantees. We comment on a formal model that can be used with existing model checkers for an automatic analysis of misalignments.

Improving the usability and adoption of secure email systems has been a notorious challenge for over two decades. One of the open questions concerns the amount and format of information that secure email systems should communicate to users to inform them of the security and privacy properties pertaining to different messages and correspondents. This thesis sheds light on users' evaluation of traffic light-inspired indicators, as a metaphor to represent different privacy states and guarantees, provided by a new secure email system called $\mathsf{p} \equiv \mathsf{p}$. Over two system (re)design iterations, we highlight the pros and cons of the traffic light semantic in $\mathsf{p} \equiv \mathsf{p}$ 's context and beyond, and discuss the potential implications on the perceived security and use of such systems.

RELATED PUBLICATIONS

**Chapter 5:** Borce Stojkovski, Itzel Vazquez Sandoval, and Gabriele Lenzini. 2019. 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)*. 172–181. https://doi.org/10.1109/EuroSPW.2019.00026. [328]

**Chapter 6:** Borce Stojkovski and Gabriele Lenzini. 2020. Evaluating ambiguity of privacy indicators in a secure email app. In *Proceedings of the Fourth Italian Conference on Cyber Security, Ancona, Italy, February 4th to 7th, 2020 (CEUR Workshop Proceedings,Vol. 2597)*, Michele Loreti and Luca Spalazzi (Eds.). CEUR-WS.org, 223–234. [322]

**Chapter 6:** Borce Stojkovski, Gabriele Lenzini, and Vincent Koenig. 2021. "I Personally Relate It to the Traffic Light": A User Study on Security & Privacy Indicators in a Secure Email System Committed to Privacy by Default. In *Proceedings of the 36th Annual ACM Symposium on Applied Computing* (Virtual Event, Republic of Korea) *(SAC '21)*. Association for Computing Machinery, New York, NY, USA, 1235–1246. https://doi.org/10.1145/3412841.3441998. [325]

### 1.3.3 DIGITAL HEALTH TECHNOLOGY

The Coronavirus (COVID-19) pandemic has led numerous governments, health agencies, and technology companies to develop solutions to control the spread of this infectious disease. Digital contact tracing (or proximity tracing) has been proposed to help break the chain of COVID-19 infections, complement manual tracing, and relax lockdown restrictions. Considering human factors when exploring the adoption as well as the security and privacy aspects of COVID-19 contact tracing apps is a timely societal challenge as the effectiveness and utility of these apps – whether centralized (like the French TousAntiCovid app [143]) or decentralized (like the German Corona-Warn-App [279]) – highly depend on their widespread adoption by the general population.

By conducting focus groups with participants living in two of Europe's most populous countries that have developed contact tracing apps based on different architectural choices i.e., France and Germany, this thesis provides greater granularity and understanding of the factors that influence people's decisions to adopt, or not to adopt, a certain contact tracing app as well as how they perceive the benefits, drawbacks, and threat models of contact tracing apps. Our findings complement ongoing efforts from a socio-technical lens, given the

complex and interdisciplinary needs required to overcome this shared reality, and serve to highlight future recommendations for practice and policy.

### Related Publications

**Chapter 7:** Borce Stojkovski, Ruba Abu-Salma, Karen Triquet, and Gabriele Lenzini. 2021. "Unless one does the research, it may seem as just a useless battery-consuming app" - Field Notes on COVID-19 Contact Tracing Applications. *Digital Threats: Research and Practice* (August 2021). https://doi.org/10.1145/3480466. [321]

Other Publications. The peer-reviewed publications listed above serve as the basis for the primary chapters in this dissertation. In addition, parts of this thesis build upon material that has been accepted for presentation or publication at the following symposia:

- Itzel Vazquez Sandoval, Borce Stojkovski, and Gabriele Lenzini. 2018. A Protocol to Strengthen Password-Based Authentication. In *Emerging Technologies for Authorization and Authentication*, Andrea Saracino and Paolo Mori (Eds.). Springer International Publishing, Cham, 38–46. https://doi.org/10.1007/978-3-030-04372-8_4. [357]
- Borce Stojkovski and Gabriele Lenzini. 2019. A preliminary user experience evaluation of MISP (Work in Progress). In *5th Workshop on Security Information Workers (WSIW 2019)*, affiliated with SOUPS 2019. Usenix Security 19. Santa Clara, CA, USA.
- Borce Stojkovski and Gabriele Lenzini. 2019. How Users Understand Privacy Indicators in a Secure Email App (Work in Progress). In *International Workshop on Human-centered cybersecurity*, affiliated with CHITALY 2019. Padova, Italy.
- Borce Stojkovski, Gabriele Lenzini, Vincent Koenig, and Salvador Rivas. 2021. Methodological Challenges In Investigating the User Experience of Cyber Threat Intelligence Data Sharing Platforms. In *Learning from Authoritative Security Experiment Results Workshop (LASER)*, affiliated with ACSAC 2021. Virtual Event. USA.

## 1.4 Organization of the Thesis

The rest of the thesis is structured as follows:

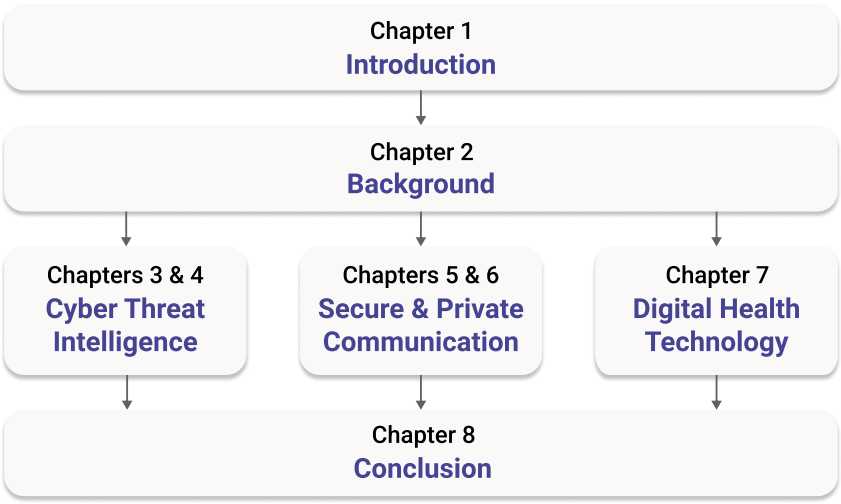



**Figure 1.1:** Overview of the thesis structure

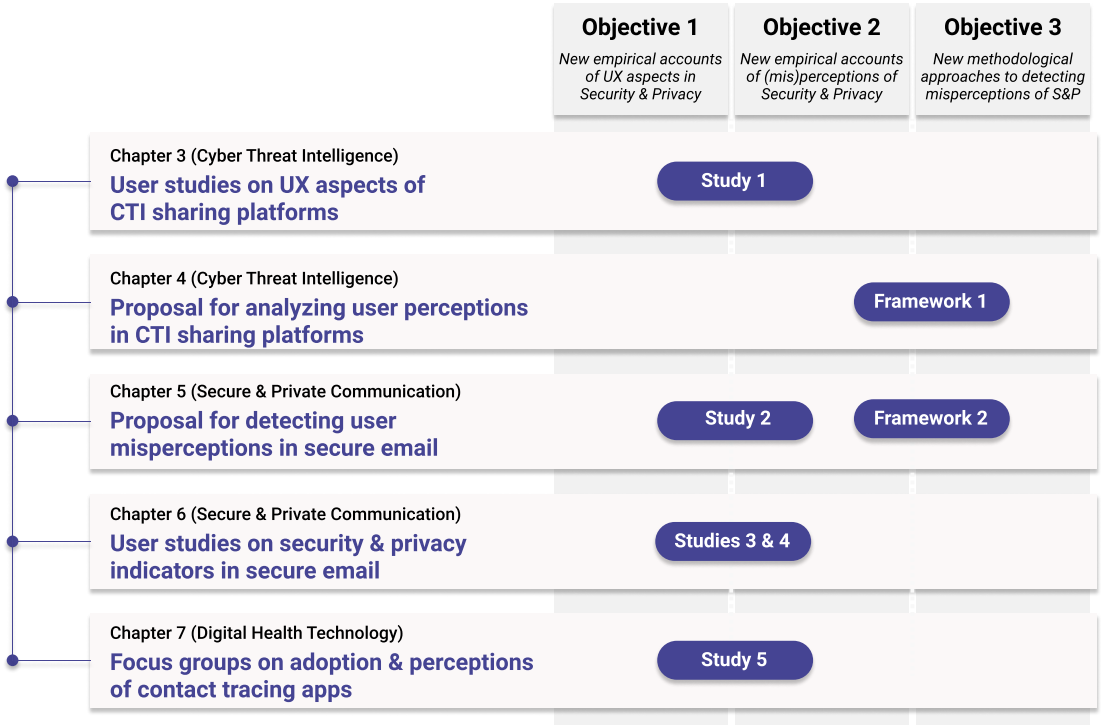



**Figure 1.2:** Breakdown of the research activities per cybersecurity and digital privacy context

**Chapter 2** We present an overview of the necessary background knowledge by focusing on three key areas: (i) user experience design and evaluation, (ii) mental models and user misperceptions of security and privacy, and (iii) state of the art in the specific contexts of cyber threat intelligence sharing, secure email communication, and COVID-19 contact tracing applications. Work related to our investigations within these three contexts is provided in the individual chapters under the corresponding cybersecurity and digital privacy context.

**Chapter 3** Using a mixed methods approach, we investigate how security information workers perceive the user experience of a leading CTI sharing platform called MISP. We report on a number of user studies conducted over a period of two years and shed light on the strengths and weaknesses of MISP from an end-users' perspective. Finally, we discuss the role usability and user experience (could) play in effective CTI sharing.

**Chapter 4** We propose a conceptual workflow and toolchain that would seek to detect user (mis)perceptions of key tasks in the context of CTI sharing, such as verifying whether users have an accurate comprehension of how far information travels when shared in a CTI sharing platform. We contextualize our concept within MISP as a use case, and discuss the benefits of our socio-technical approach as a potential security analysis tool, simulation tool, or educational / training support tool.

**Chapter 5** We propose and describe *multi-layered user journeys*. This extended conceptual framework serves to capture the interaction of a user with a system as she performs certain goals along with the associated user beliefs and perceptions about specific security or privacy-related aspects of that system. We instantiate the framework within a use case, a new secure email system called $\mathsf{p} \equiv \mathsf{p}$, and demonstrate how it can be used to detect user misperceptions of system security and privacy by combining it with system values and objective technical guarantees offered by the system.

**Chapter 6** We perform an initial validation of the findings obtained by the socio-technical security analysis of $\mathsf{p} \equiv \mathsf{p}$ in Chapter 5. We present two sets of user studies focusing on the usability and effectiveness of $\mathsf{p} \equiv \mathsf{p}$'s security and privacy indicators and their traffic-light inspired metaphor to represent different privacy states and guarantees. We conclude with a discussion on the potential implications on the perceived security and use of such systems.

**Chapter 7** We present the findings of eight focus groups on the factors that impact people's decisions to adopt, or not to adopt, a contact tracing app, conducted with participants living in France and Germany. We report how our participants perceived the benefits, drawbacks, and threat model of the contact tracing apps in their respective countries, and discuss the similarities and differences between and within the study groups.

**Chapter 8** We summarize the work presented in the thesis and discuss future research challenges and directions.

*Thoughts without content are empty,*
*intuitions without concepts are blind.*

Immanuel Kant

# 2 Background

## 2.1 From Human-Computer Interaction to User Experience

### 2.1.1 Multidisciplinarity

Rooted in formal disciplines such as logic, mathematics, and linguistics, computer science has always borrowed from other fields, in particular, the humanities and social sciences since we came to understand that in addition to making computers work we need to understand how computers are used [334]. Needless to say, the field of Human-Computer Interaction (HCI) emerged as a new area of research and practice dealing with the design and use of computer technology. HCI is inherently multidisciplinary, informed not only by the social and natural sciences which are concerned with human and naturally occurring phenomena, respectively, but also by the design and engineering disciplines which deal with the processes that lead to the emergence and creation of innovative technology in support of human activity [36]. In literature, there has been a proclivity for viewing the relationship between humans and computers as one-sided, wherein humans realize their intentions through a computer [172]. However, *interaction* lies at the core of HCI and it "concerns two entities that *determine* each other's behavior over time" [172, p. 5049]. In other words, the interaction between people and information technology is a phenomenon marked by co-adaptation, where people both adapt to the technology, but also re-interpret and adapt it for their own purposes in novel ways [221].

The question of what users and computers can or should do within a specific interaction has profound design implications. According to Kuutti (2001, as cited in McCarthy et Wright [230, p. 6]), the dominant view regarding the user in the relationship between people and computers has transitioned from the "user as a cog in a rational machine" in the 1970s, to

the "user as a source of error" in the 1980s, to "users as partners in social interaction" in 1990s, to "users as consumers" in the 2000s. While the focus in this thesis is on the *user* of today, it can be useful to revisit the historical context, and some of the key ideas that guided the design of interactive computer systems in the past or that remained influential to the present day [153].

### 2.1.2 What is Interaction

Per Hornbæk and Oulasvirta's review of key interaction concepts in HCI literature [172], interaction can be seen as:

- *Dialogue:* users and computers engage in a cycle of communication acts, manifested via perception/action loops on the user side, and input/output cycles on the computer's side. Norman's seven stage model [253], which we further elaborate below, is representative of this interaction concept.
- *Transmission of information:* based on Shannon's theory of communication [308], interaction is seen as transmission of information between computers and users. Good interaction according to this view is characterized by the maximum throughput of information over a noisy channel.
- *Tool use:* a prominent view of interaction that places emphasis on usefulness and utility as key evaluation criteria of good interaction. This view is also associated with the important notion of the mediating role of technology i.e., the aims for using a tool go beyond the tool itself (see *Generative principles of instrumental interaction* [36]) .
- *Optimal behavior*: interaction is seen as a joint behavior between the user and computer, whereby a user purses a specific goal under the constraints of the user interface, the environment or the task at hand. Examples include *adaptive interaction* [202] and *economic models of interaction* [24].
- *Embodied action*: refers to concepts such as *embodiment* [1] and situatedness [330] of technology use. In contrast to purposeful action derived from well specified goals, situated action refers to ad hoc responses to the actions of others or the contingencies of specific situations. This perspective insists that all action is richly contextualized and coupled with multiple contexts.
- *Experience*: this view of interaction is concerned with experiential qualities of technology use, aesthetics, emotions, fulfillment of psychological needs, as well as surprise and stimulation. We expand on this view further below.

- *Control*: this perspective supports simulations of complex interactive behavior by viewing a human-computer interaction as a system of goals, signals, feedback and feedforward mechanisms as well as system states in which a goal-directed user controls the system as it tries to reach a specific reference state.

As a representative example of the *interaction as dialogue* concept, we mention Norman's Action theory [253], which has been influential in the field of interaction design, inspiring several concepts and frameworks for evaluating and constructing interaction [172].

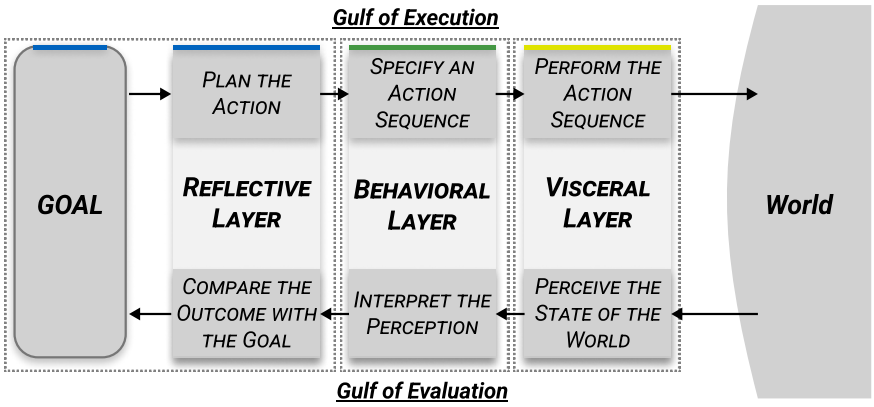



**Figure 2.1:** Norman's Seven Stages of Action and Three Levels of Processing, adapted from [253]

According to Norman [253], the goal of the user drives the planning of an action, the specification of an action sequence and the actual performance of the actions. These stages of *execution* are followed by three stages of *evaluation*. The user first perceives the changes in the system, the environment, or as Norman puts it, the state of the world. She then interprets the perception and finally compares the outcomes with the goal. A direct link can be made between these stages of action and three levels of cognitive and emotional processing, namely, visceral, behavioral, and reflective. According to Norman, the user's cognitive and emotional state is determined by all three levels of processing working together, thus designing with consideration of all three levels is paramount for an optimal user experience.

### 2.1.3 What is User Experience

As touched upon in the Motivation of this thesis (Section 1.1), the third wave in HCI broadened our perspectives regarding the nature of the interaction between people and technology and also put emphasis on new aspects that went beyond the traditional, instrumental view that had predominantly focused on the achievement of behavioral goals in work settings [48]. The third wave embraced *experience* and *meaning-making* [49].

*User experience*, or UX, quickly permeated the HCI field, prompting efforts to try define and scope the concept, as it was vaguely defined and poorly understood by many [215]. In 2010, a Dagstuhl seminar* dedicated to demarcating user experience took place. As stated in the resulting User Experience White Paper—a written account of the discussions of leading UX researchers and practitioners at the seminar—there is no one single definition of user experience that suits all perspectives [283].

The ISO 9241-11:2018 standard defines user experience as "*user's perceptions and responses that result from the use and/or anticipated use of a system, product or service*" [180, definition 3.2.3]. Two notes associated with this definition further indicate that the users' perceptions and responses include the "*users' emotions, beliefs, preferences, perceptions, comfort, behaviours, and accomplishments that occur before, during and after use*", and that the user experience is a consequence that "*also results from the user's internal and physical state resulting from prior experiences, attitudes, skills, abilities and personality; and from the context of use*" [180].

In this section, we attempt to unpack this definition by providing a brief elucidation of the core concepts and frameworks that relate to UX as reported in literature and discourse.

### Perception and Understanding of the World

The Oxford English Dictionary defines *perception*† in the following ways: (1) the process of becoming aware or conscious of a thing or things in general; the state of being aware; consciousness; (2) the process of becoming aware of physical objects, phenomena, etc., through the senses; an instance of this; (3) the faculty of perceiving; the ability or power to perceive; (4) the mental product or result of perceiving something; (5) the action of the mind by which it refers sensations to external objects, phenomena, etc., as their cause.

As such, perception is often discussed in philosophical contexts, but it has important practical implications in the area of user experience because it is essential for our understanding and experience of the things we use. In this regard, it is Heidegger's phenomenology of perception that can offer some relevant insights for system designers since Heidegger holds that our understanding of things (or beings, in general, as he refers to them) is achieved through the so-called "comportment towards beings" [169]. Put simply, we understand the world and ourselves within this world through our involvement and interactions with it, i.e., through action and behavior. Consequently, we experience and understand things through using and utilizing them for specific purposes and within specific contexts,

*https://www.dagstuhl.de/10373, Accessed February 10, 2022.

†"perception, n." OED Online, Oxford University Press, December 2021, www.oed.com/view/Entry/140560. Accessed February 10, 2022.

and not by merely observing them. This is why a set of qualities that a certain system possesses can only make sense for the user if she gets involved with these qualities.

In the context of experience, the works of the philosophers Dewey and Bakhtin have also been largely influential underpinning McCarthy et Wright's framework [230] for looking at technology as experience, described next.

### Technology as experience

McCarthy et Wright explicated how technology can be seen in terms of experience with technological artifacts and introduced a framework consisting of four intertwined threads of experience and six sense-making processes [230]. The first thread of experience is *sensual*. This refers to people's "sensory engagement with a situation, which orients us to the concrete, palpable, and visceral character of experience" [230, p. 80]. Examples include the look-and-feel of a particular product or the warmth and comfort one might experience in a social setting [231]. The second thread is *emotional* which refers to value judgements we attribute to other people and things with respect to our goals, needs, and desires. According to McCarthy et Wright, what makes one experience different from others are the associated emotions that hold all aspects of that particular experience together [230, p. 83]. The third thread is *compositional* which relates to the "relationship between the parts and the whole of an experience" [230, p. 87]. This refers to e.g., action possibilities, consequences, and explanations of actions, and is inherently linked to how people *frame an experience* i.e., bring structure and meaning to it. The fourth thread is *spatio-temporal* which is constructed through interaction and draws attention to the effects that space and time have on people's experience [231].

McCarthy et Wright described six inter-related, non-liner processes for making sense *in* and *of* experience [230]. *Anticipating* refers to expectations, possibilities and sense-making associated prior to an experience. *Connecting* relates to the "immediate, pro-conceptual and pre-linguistic sense of a situation encountered" [230, p. 125], meaning judgements are made instantly and intuitively. *Interpreting* refers to the sense-making process during which we try to figure out what is happening and what our feelings and reactions towards it are like. *Reflecting* refers to the process during which we make judgements about the unfolding experience. Examining and evaluating events and relating them to our motivation and sense of fulfillment [230, p. 126]. *Appropriating* refers to the process of making an experience part of oneself, by relating it to one's sense of self, the personal history or anticipated future. Finally, *recounting* refers to telling about the experience to others and oneself, considering it in the context of other experiences and finding new possibilities and meanings in it [230].

### Crucial elements of experience and underpinning constructs

We continue the discussion by looking at some of the underpinning psychological constructs and elements of user experience. Hassenzahl et Tractinsky highlighted three important facets of user experience: the first is concerned with addressing human needs, the second focuses on the affective and emotional dimensions of interaction, the third pertains to the nature of experience [168]. As emotion is the centerpiece of experience, inextricably intertwined with cognition, motivation, and action [165], we briefly touch upon these concepts.

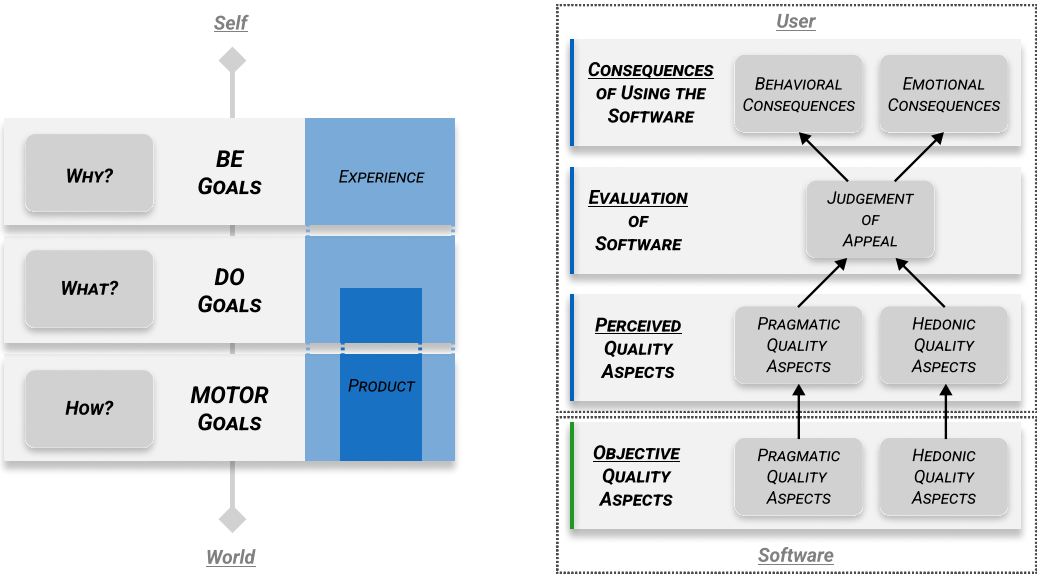
One of the most frequently used theories in HCI research that deals with the factors that promote motivation, informing user experience and experience design, is Ryan et Deci's self-determination theory (SDT) [289]. SDT distinguishes between extrinsic and intrinsic motivation, depending on the origin of the factors that drive a person towards a certain goal or accomplishment [289]. Extrinsic factors can be in the form of values, beliefs, and regulations originating from external sources, while intrinsic factors are internal to the person concerned, and can be in the form of personal needs, desires, values, beliefs, etc. [289]. Extrinsic and intrinsic motivations play a decisive role in influencing a certain attitude, which is a construct that can be defined as a "learned, global evaluation of an object (person, place, or issue) that influences thought and action" [261, p 87]. Attitudes are complex, they involve affect and emotions, and they can be expressed through thoughts, feelings, and behavior [261]. Like motivations, they are both implicit and explicit and can be inconsistent and contradictory [272]. Emotions are reactions to "events deemed relevant to the needs, goals, or concerns of an individual" and encompass "physiological, affective, behavioral, and cognitive components" [56, p. 78]. Emotion and motivation are related in two ways. Emotions are a type of motive that, like other motives, energize, direct and sustain behavior [272]. Emotions also indicate one's ongoing motivational states and personal adaptation, or metaphorically said, positive emotions during motivated action provide a *green light* for continuing to pursue the goal or need satisfaction, while negative emotions can be seen as a *red light* for stopping the pursuit of that goal or need satisfaction [272].

STD posits three basic psychological needs whose satisfaction fuels intrinsic motivation, namely *competence*, *autonomy*, and *relatedness* [289]. Drawing from the STD as well as other needs theories, Sheldon et al. identified and validated 10 candidate psychological needs in an attempt to determine which of them are truly most fundamental for humans [309]. The 10 candidate needs are: *autonomy*, *competence*, *relatedness*, *self-actualization-meaning*, *physical thriving*, *pleasure-stimulation*, *money-luxury*, *security*, *self-esteem*, and *popularity-influence* [309, p. 328]. Their findings established a clear link between positive experience

and need fulfillment, inspiring further work, such as Hassenzahl et al.[‡] who investigated and confirmed a relationship between need fulfillment and hedonic quality perceptions of interactive products and technologies [166].

### The pragmatic, hedonic, and eudaemonic dimension of user experience

When discussing about the relation between technology and experience, Hassenzahl makes a distinction between three types of goals with respect to action mediated by interactive technology [165]. As depicted in Figure 2.2a, *do-goals* are at the middle of the hierarchy and refer to specific outcomes we wish to achieve using technology, e.g., to send an encrypted email. How that action is carried out is in the domain of subgoals and *motor-goals* which are close to the world i.e., the technology through which we interact and the context. Sitting at the top of the hierarchy are self-referential *be-goals* which are related to motivation and meaning. They explain why one would want to send an encrypted email, e.g., to *be competent*, to *be close to others* who communicate via encrypted email, to *be admired* by others, etc.




**(a)** Hierarchy of goals, adapted from [165]

**(b)** Product appealingness framework, adapted from [167]

**Figure 2.2:** Hassenzahl's UX framework.

The primary focus of HCI for a long time was on *do-goal* achievement, closely related to the utility and usability of interactive products. However, an experiential approach to designing and evaluating interaction needs to be holistic i.e., also consider *be-goals* [165].

[‡]In their investigation, Hassenzahl et al. selected 7 out of the 10 candidate needs, which according to them were appropriate and promising in the context of interactive technologies [166].

The relationship between product qualities and *do-goals* and *be-goals* can be seen through the product appealingness framework by Hassenzahl et al. [167, p. 202], [164, p. 484]. In essence, the qualities of a specific interactive technology, according to this model, can be divided into two groups, *pragmatic* and *hedonic* quality aspects, as depicted in Figure 2.2b. The *pragmatic dimension*, also known as *ergonomic* or *instrumental*, is concerned with behavioral (*do*) goals and focuses predominantly on task-related efficiency and effectiveness [167, 168]. The *hedonic dimension* is not related to the task, but refers to non-instrumental aspects such as visual aesthetics, beauty, joy of use, stimulation, surprise, etc., that relate to fulfillment of general human needs and which are subjectively perceived [30]. Both play an almost equal role as to how a particular system is perceived and evaluated by users, ultimately leading to various behavioral outcomes (e.g., increased usage frequency) as well as emotional consequences (e.g., feelings of fun, frustration, etc.) [164]. Research suggests that instrumental and non-instrumental goals tend to be interwoven and inseparable [30].

Recently, a third, *eudaimonic*, dimension has been gaining prominence in the UX discourse and relates to the experience of *meaning* [236]. According to Aristotle, hedonic happiness as a life goal was a "vulgar" ideal; instead, "true happiness" was to be found "in the expression of human excellence and virtue–that is, in the doing well of what is worth doing" [289, p. 240]. Beyond philosophical differences between *hedonia* and *eudaimonia* and their respective relationship to well-being [200, 289], it has been argued that *hedonia* may not cover all possible positive experiences involving interactive technology [235]. The notion of *eudaimonia* as a complementary dimension to the hedonic aspect is a matter of ongoing research in HCI.

#### Temporality and time spans of user experience

Karapanos et al. studied how the quality of users' experience develops over time [194]. They found that product qualities that initially gave rise to positive experiences were not as consequential for motivating prolonged use, which was in fact more linked to aspects that reflected how meaningful a product became in one's life. Based on their findings, the authors proposed a temporality framework, describing how expectations start forming during the act of *anticipating* an experience and how the experience shifts through the phases of *orientation*, *incorporation*, and *identification*. What motivates the transition through these phases are three corresponding forces, namely increasing *familiarity*, *functional dependency*, and *emotional attachment*.

The different time spans of user experience are also enunciated in the UX Whitepaper [283], which makes a distinction between *anticipated*, *momentary*, *episodic*, and *cumula-*

*tive* UX. Within these time spans, a number of corresponding processes take place, namely *imagining an experience*, *experiencing*, *reflecting on an experience*, and *recollecting multiple periods of use*, respectively.

### Scoping user experience

As mentioned earlier, different views exist when talking about user experience. For instance, UX can be seen as a phenomenon, as a field of study, or as practice [283]. UX is informed by different disciplines, thus some approaches take the user perspective, some look at how UX relates to product qualities, and some take an interaction-centered view [127]. Bargas-Avila et Hornbæk [30] highlighted the following key tenets associated with UX in literature:

- a holistic view of users' interactions with technology;
- a focus on positive aspects of users' interaction with interactive products;
- an emphasis on the situational and dynamic aspects of using interactive technology as well as the importance of the context;
- a multidimensional perspective on quality;
- a need for new methods and approaches for designing and evaluating experience.

While user experience remains a concept without a clear definition [209], there is consensus that the *user*, the *system*, and the *context*, are all important factors that shape it.

### User Experience Design

We conclude the discussion on the subject of user experience with a reference to the system design and development approach that pays special attention to people's experience of technology i.e., User Experience Design (UXD). Notwithstanding the debate and criticism around the use of the terms *experience design* and *experience designer*—as to design a user experience would suggest "a return to the simplicity of a technologically determinist position on what experience is" [231, p. 10]—UXD is increasingly considered as part of Human-Centered Design (HCD) [209]. Norman describes HCD as "the process that ensures that the designs match the needs and capabilities of the people for whom they are intended" and sees Experience Design as one of the focus areas of HCD [253, p. 9].

## 2.2 From Mental Models to User Misperceptions of Security and Privacy

### 2.2.1 What are Mental Models

Despite HCI research embracing new perspectives well beyond the dominant cognitive stance at its onset (as discussed in the previous sections), the assumption that cognition, and especially mental models, still have a role to play in how people use and interact with technology is prevalent [347]. To appreciate the relevance of mental models for HCI in general, and security and privacy in particular, one first needs to consider what constitutes a mental model and how mental models affect the way in which a user sees and utilizes a particular (security and privacy-sensitive) product or system.

As mental models have been a topic of interest for a variety of subdisciplines that had adopted the concept and developed their own terminology and methodology, there is no universal agreement on what mental models are, how they function or what they consist of [284]. It needs to be pointed out, however, that mental models can be discussed from two different aspects, i.e., by focusing on the structure of the mind (mental architecture) or on the contents of the mind (mental content). For our discussion, we focus on the latter, which in HCI literature has been associated with a variety of aspects related to users' knowledge about the systems they use [259]. According to Payne, even a simple construct that a mental model refers to users' knowledge as well as beliefs about the systems they use is already useful because the "*contents* of people's knowledge, including their theories and beliefs, can be an important explanatory concept for understanding users' behavior in relation to systems" [259, p. 64]. As discussed, understanding users' behavior is important as it can help system designers in their efforts to design technology which is aligned with users' needs, perceptions and expectations. Further, technology has a greater chance of being adopted if system designers are aware of how users conceive the functioning of a certain system, and how their interactions with the system are shaped by the things they know or believe.

Rouse et Morris defined mental models as the "mechanisms whereby humans are able to generate descriptions of system purpose and form, explanations of system functioning and observed system states, and predictions of future system states" [284, p. 351]. In other words, the purpose of mental models is to help us *describe* why a particular system exists and what it looks like, *explain* how it operates and what it is doing as well as *predict* what it is going to do. As referenced in Jonassen et Cho [187], mental models are seen as "structural analogues of the world as perceived and conceptualized, which enable people to make inferences and predictions", they are "formed on the basis of previous experience and current observation", they are dynamic, often created ad hoc in response to "demands of specific problem-solving situations" and they "dictate the level of task performance" [187, p. 145-146].

### Mental Models and Conceptual Models

In the discussion of mental models, Norman points out that we need to make a distinction between four things: (i) the *target system*, which is the system a person is using or learning to use; (ii) the *conceptual model* of that target system, which refers to models invented by designers, engineers, instructors etc. with the aim of appropriately representing the target system; (iii) the *mental model* of the user, which refers to the naturally evolving model formulated as people interact with a target system; (iv) *scientist's conceptualization* of the user's mental model, which is a model of a model that serves to understand how a person interacts with a target system [251]. The target system, along with all accompanying information, documentation, training, advertising materials, etc. forms what Norman calls the *system image*. The importance of making a distinction between these elements becomes evident when looking at the frequent disconnect that exists between the conceptual model that guided the designers and developers of a (security or privacy-critical) system, the resulting system image, and the mental model of the user [253].

### Observations on Mental Models

Viewing mental models as analog representations that approximate the structure of what they represent (e.g., in the way a scale model incorporates and maintains relationships between its different aspects) gives rise to the notion of *mental simulation* [259]. However, people are limited in their abilities to *run* their models i.e., to predict future states or consequences of actions by *running* the model forward or provide explanations for the lead-up to a state by running it backwards [251]. Functionality comes before accuracy i.e., mental models are often fragmentary, incomplete, and unstable [251, 259]. They are not easily known to others, moreover not always fully grasped by the knower [187]. Research shows that mental models of laypeople and experts differ in knowledge content and organization, with the understanding of laypeople being more concrete, whereas expert understanding being more abstract, suggesting that both biology and learning play a part in mental model formation [188]. Problem solving, verbal report, drawing, categorization, and conceptual pattern representation are methods researchers have used extensively to identify mental models [187]. However, they are difficult for researchers to capture, and attempts to do so may induce a change in the mental model, which calls for special care not to affect them when they are being measured [362]. Finally, shared, collective and cultural mental models all refer to a degree of understanding among a group of people, which is an important notion given the growing recognition that cognition has a social component and that decision making takes place at a range of scales, from an individual to a group to a societal level [188].

### 2.2.2 Mental Models *of* and *in* Security and Privacy

#### Folk Models

Continuing our discussion from the perspective of shared mental models among similar members of a culture, a topic that has received a notable attention in the security and privacy discourse is the one of *folk models*. They refer to oftentimes inaccurate mental models of how security and privacy systems work or what the associated threats and risks are, potentially leading to erroneous decision making [367]. Folk models are typically associated with non-expert, non-technical or untrained users of various computer systems, within an organizational as well as in home settings. For instance, Wash identified eight such models among home computer users: four of them were concerned with viruses and other malware, while the other four were related to hackers breaking into computers, highlighting that there was a serious gap between untrained users' capabilities to protect themselves and the level of sophistication and quantity of security risks they were faced with. [367]. Wash noted how people applied their folk models to determine for themselves whether a certain piece of security advice was considered important and necessary to follow, whether it was considered helpful, too costly in terms of efforts and money, or extremely important that it should never be ignored, even if it was inconvenient, costly, or difficult to follow [367]. While confirming the presence of the eight folk models presented by Wash, a subsequent replication study in Germany by Kauer et al. [196] introduced three new ones, highlighting that different cultural backgrounds might play a role in the folk models exhibited. The authors suggested that accurate reporting in the media could help improve folk models of computer security and privacy as well as promote appropriate countermeasures [196].

#### Risk Communication

Mental models in cybersecurity have been approached from two angles, namely as an approach to understanding users' models of security and privacy (like the afore-mentioned investigations of folk models) as well as a mechanism for effectively communicating with users [47]. The rationale for the latter application is rooted in analogical reasoning i.e., transferring knowledge from a source domain that is well-understood to a target domain that is less-understood via mapping [316]. Among the first studies along these lines, Jean Camp proposed a number of mental models that could be used for communicating complex security risks: a *physical security*, a *medical*, a *criminal*, a *warfare*, and a *market* model [59]. These were validated in a subsequent investigation [20], however, it was noted that none of the models on their own offered a solution to the security problem as a whole, but instead ad-

dressed different facets, implying that multiple metaphors or extra-domain schemas would need to be used to address the different security and privacy-related dimensions.

### Differences between expert and non-expert users

Increased awareness of security risks and threats among non-technical users has made them invest efforts into increasing their levels of protection against such risks or threats. However, prior research has shown that security experts and non-experts differ between themselves when it comes to their respective mental models of security risks (e.g., [20, 181, 320, 338]). For instance, non-technical end users in most cases do not regard security as their primary goal as far as their interactions with technology are concerned [8, 385]. Their knowledge about security is insufficient and they demonstrate low levels of self-efficacy when taking action aimed at security [159, 320]. Security experts, on the other hand, demonstrate rather different views and practices when it comes to security [181, 338]. One example of such differences is that experts mostly keep their systems up-to-date, and use two-factor authentication when interacting online, while non-experts express their reliance on antivirus software and use of strong passwords [181]. Another example is the issue of proactivity. While non-experts rarely demonstrate proactive attitude and therefore depend on the supposed protection and security provided by others, e.g. websites or online entities, experts are typically proactive by taking additional action and making their own plans and scenarios to protect themselves from potential risks and threats [338]. Non-technical end users' mental models can lead to some misconceptions related to various security aspects. For example, it has been found that non-technical end users happen to disregard SSL warnings on banking websites since they assume banks to be safe, or they might believe that opening a file is safer than storing it on their local device [57]. They may also be unaware that their data sent over public wifi unencrypted might be intercepted by other users on the network [203].

These findings should come as no surprise if we take into account the differences between experts and non-experts concerning their background, technical knowledge and experience in the area of cybersecurity. What is important to note here are the consequences of such differences for the design of and communication about security systems by experts. In this regard, it has been reported that risk communication is predominantly based on the experts' mental models. Instead, it is proposed that it should be designed by taking into account the end users' perspective [20]. Distinguishing between experts and laypeople may not be enough, however, as individual participant accounts point to a broad spectrum of perceptions and heterogeneous argumentation patterns, which calls for improving security interventions through individualization [32].

### 2.2.3 User (Mis)perceptions of Security and Privacy

Researchers use a range of terms when referring to internal constructs of the world, such as analogy, metaphor, perception, theme, theory, internal concept, and reasoning [362]. Furthermore, (mis)conceptions, (mis)perceptions, and (mis)alignments are also frequently found in usable security literature when referring to manifestations of (erroneous) user understandings and attitudes that may be based on their mental models. As described in the subsequent section, in this thesis we mostly use the terms perceptions and misperceptions of security and privacy to denote and discuss such manifestations, which have been reported extensively in various security and privacy contexts.

For instance, password security is an area abundant with examples ranging from misperceptions about password strength and the use of letters, digits, and keyboard patterns when setting up passwords [352] to overreliance on password-strength meters, whose estimates are not always accurate or informative enough [82, 98, 352, 354]. A systematic literature review of password misconceptions identified 23 such types, which the authors grouped in four broader categories, namely: misconceptions regarding password *composition*, *handling* (e.g., password reuse across accounts), *attacks* (e.g., attackers and their strategies), and a *miscellaneous* category that refers to general issues applicable to passwords as well [227].

Recent investigations have looked into misconceptions in domains ranging from biometric authentication, data breaches, and smart home security to malware, E2E encryption, and e-voting, to name a few. On the subject of biometric authentication, for example, users mistakenly thought that biometrics were being sent over the network and stored in service providers' databases [42, 211], that biometrics were being accessed and used by third parties [379], or that sharing a device with another user would no longer be possible once a biometric authentication feature was activated [83].

When it comes to misconceptions about data breaches, it has been reported that end users commonly felt personally responsible for preventing data breaches, and if cases of breaches happened, they attributed blame to themselves for not being cautious enough or not taking sufficient measures to prevent data breaches. They commonly failed to realize that their institutions/organizations, where the data breach occurred, are responsible for data security and therefore accountable in this respect to the regulatory authorities [163, 228]. Risk perceptions in the context of smart homes have been related e.g., to concerns about security due to a lack of trust in the smart home security technology manufacturer [389], or reversely to overreliance on the security and protection assumed as inherent in the trusted manufacturer's smart devices [381, 393].

It has been noted that users often see privacy policies as giving them automatically assurances with respect to privacy, serving as so-called "trust-marks" even when users do not consult them at all and are unaware whether such protection is actually assured or not [184]. Private browsing mode is mistakenly perceived by users as protecting them from tracking by service providers, advertising companies or government agencies and bodies [383]. Some users even believe that private browsing mode can protect them from viruses or malware [132]. As regards malware, non-technical users tend to think about malware as something completely negative, and regular software as something completely positive, failing to realize that even helpful software may contain undesirable features and pose hidden security and privacy risks [317]. Some non-expert users do not trust the capabilities of protective mechanisms and security systems because they overestimate the strength of their potential attackers, which makes them feel that any protective measures are useless. Others, on the other hand, doubt that any potential attacker would target them because they feel there is nothing about them that would attract attackers [85]. Users mistake the security protection offered by different tools and services e.g., it has been reported that some users believe that SMS or landline phones offer more security than E2EE communication [3, 85].

In the context of e-voting, voting schemes are developed to be end-to-end verifiable, however, it has been reported that trust issues may arise due to the lack of understanding of the verification phase following a vote cast, ultimately leading participants to question the integrity of the elections and the purpose of the verification phase, which is a concept that does not feature in users's mental models of voting [395, 396].

As can be seen by the above-reference to some illustrative related work, there is a broad stream of literature investigating mental models and user (mis)perceptions of security and privacy in various domains. In the next sections, we introduce the contexts within which we situate our investigations and research.

### Further Reading

We refer interested readers to Volkamer et Renaud's review of mental models and their applications in human-centered security [362] for further information. User perceptions and misperceptions related to the three cybersecurity and digital privacy contexts of this thesis, i.e., those referring to CTI sharing platforms, secure and private communication via email, and COVID-19 contact tracing applications are provided later in the respective chapters.

## 2.3 Terminological Clarifications

Throughout this work, when referring to the issues affecting users' secure use of ICT technology, we have mainly used the term *misperceptions*. In various contexts, we have also talked about *misconceptions*, *misalignments*, and in some cases about *mistakes* and *errors*. We have also mentioned that *misperceptions* and *misconceptions* can be based on certain *assumptions* and *beliefs*. As much as our use of terminology is consistent with the common practice applied by academics, researchers and experts working in the area of cybersecurity, there is some terminological ambiguity in this area since sometimes the same term is used for several aspects of certain phenomena.

To clarify the potential ambiguities, it is worth discussing our use of terminology in more detail. If we consider *misperception*, for instance, from the semantic point of view, this term can refer to any of the following meanings: (1) a wrong or incorrect understanding or interpretation[§]; (2) wrong or incorrect perception; an instance of this[¶]; (3) a belief or opinion about something that is wrong or not accurate[‖]. Seen in relation to the term *perception*, and the action of *perceiving*, *misperceptions* can be analyzed from two different viewpoints: (1) from the aspect of sensory perception (in the sense of what is perceptible, i.e., detectable by our senses); and (2) from the aspect of cognition (in the sense of what is perceivable, i.e., able to be perceived by the mind; intelligible, comprehensible). Impaired sensory perception can seriously affect the risk communication between the system designer and the user, e.g., when the user is confronted with security warnings or symbols that involve qualities such as shape and color, and the user is unable to see or notice some of these qualities (e.g., people with color vision deficiency might be unable to distinguish between colors). On the other hand, even if the user has no difficulties in identifying and distinguishing between visual qualities of a security symbol, there is no guarantee that what is seen will be understood or interpreted as the system designer intended or expected.

While both the sensory perception aspect and the cognitive aspect have been taken into account in our use cases and discussions herein, it should be noted that it is the cognitive aspect that prevails, which means that by *misperceptions* in this regard we mainly mean insufficient, inadequate or incorrect understanding or interpretation of how something works. Nevertheless, there is another important meaning of the term *misperception* which is present

[§]Google's English dictionary provided by Oxford Languages. Retrieved February 15, 2022 from www.google.com/search?as_q=misperception.

[¶]Oxford English Dictionary Online. Available from www.oed.com/view/Entry/119850. Accessed February 15, 2022.

[‖]Cambridge Advanced Learner's Dictionary & Thesaurus. Retrieved February 15, 2022 from https://dictionary.cambridge.org/dictionary/english/misperception.

within this work. Namely, when we talk about a user who has insufficient or inadequate understanding of how a system works or who misinterprets some of the system's features, we normally refer to a situation in which the user has some experience with the system and fails to benefit from its full potential because of the lack of understanding of its functioning. However, there are situations in which a user has some preconceived opinions or beliefs about a system even before she has actually used it. In the relevant literature, and within our discussions here, such preconceptions are also sometimes referred to as misperceptions.

## 2.4 State of the Art

The following three sections describe the state of the art and refer to work related to the specific contexts of cyber threat intelligence sharing, secure email communication, and COVID-19 contact tracing applications.

## 2.5 Cyber Threat Intelligence (CTI) Sharing

Intelligence sharing is by no means a recent practice, in particular between nation-states, which have been utilizing shared intelligence as a means to provide decision-makers with fresh perspectives on the problems they face or with information on the effects of their decision-making and policies taken [366].

With the rapid proliferation of ICT technology, many capabilities are no longer reserved to nation-states, diffusing the power across the private sector and individual actors [74]. Thus, increasingly interconnected, different participants engage in the collection, processing, analysis, and exchange of information relevant to the protection of the physical, logical or social layers of cyber space.

Threat intelligence (TI), or in this context, Cyber Threat Intelligence (CTI) refers to evidence-based knowledge about an existing or potential threat, that can aid decision-makers in preventing an attack or accelerating the detection of compromised assets [342]. TI can come from a variety of internal and external sources in structured or unstructured formats, such as indicators of compromise (IoCs), tactics, techniques, and procedures (TTPs), security alerts, threat intelligence reports, tool configurations, etc. [186].

The factual insights based on the analysis of the TI can add value and support a number of different activities inside an organization, e.g., security operations and incident response, vulnerability and risk management, brand protection, etc. [226]. Thus, depending on the information source, the form of analysis that is used to produce it as well as the intended audience, CTI can be categorized as strategic, operational, tactical and technical [342].

### 2.5.1 Benefits and Incentives for CTI sharing

According to the National Institute of Standards and Technology (NIST) of the U.S. Department of Commerce, organizations that engage in CTI exchange benefit from the shared situational awareness of the sharing community, enabling them to improve their security posture and achieve greater defensive agility [186]. Many other benefits have been reported in literature, classified along an operational, organizational, economic or policy dimension [394]. To a large extent these benefits overlap with the incentives as to why organizations participate in sharing activities. The European Union Agency for Cybersecurity (ENISA) outlined 12 incentives to information sharing [106]. Two of those, namely, economic incentives stemming from cost savings, and incentives stemming from the quality, value and use of information shared, were considered to be of high importance.

### 2.5.2 Risks and Obstacles to CTI Sharing

Establishing (mutual) trust has been identified as a key driving factor for reliable and effective information exchange [109, 366]. Trust issues have thus been widely reported as key impediments to information sharing. Research suggests that trust is established over time and in face-to-face meetings [364], but can be undermined in a number of ways, for instance, when information sharing is not reciprocal [107]. These situations pave way for free riding, which is considered to be an undesirable selfish behavior by certain participants in CTI exchange [244].

Contrary to common views that establishing and maintaining trust is hard and that free-riding is a problem, in a more recent survey of attitudes towards the benefits and barriers to CTI sharing, the majority of respondents did not consider trust establishment to be difficult to achieve, nor did they consider free riding to be a significant impediment [394].

Reluctance to CTI sharing is also driven by the fear of exposing the protective or detective capabilities of an organization, which can disrupt ongoing investigations or response actions as well as jeopardize information for future legal proceedings [186]. Fearing negative publicity and the risk of reputation damage, the perception that an incident is not worth sharing as well as the natural instinct not to share are other examples mentioned in literature [342].

Another significant obstacle is liability with respect to laws that regulate organizations' operations and privacy-related legislation [306]. Several studies have delved into the privacy implications of (automated) information sharing with the government, across organizations or in the context of (international) business-to-business CTI sharing [43, 123, 171, 304, 331]. For example, Schwartz et al. offered suggestions for how organizations can best ensure li-

ability protection pursuant to the Cybersecurity Information Sharing Act [304], while Sullivan et Burger argued that under the EU General Data Protection Regulation business-to-business sharing of CTI can be justified as being in the public interest [331]. Interested readers can refer to [303] and [305] for further literature on legal implications of information sharing.

In addition to the above-mentioned organizational, economic and policy barriers to CTI sharing, operational challenges such as the lack of standardization and the necessity to achieve interoperability and automation have perhaps received the most attention. We briefly mention them in Section 3.2.1.

### 2.5.3 Human, Cultural, and Organizational Aspects

There is a broad stream of literature that examines the nature of the job, the organizational setting, the tools and workflows of IT security professionals and operators [9, 54, 273, 318, 359]. Much of the work here is in the context of security management, security operation centers (SOCs), or incident response, where the importance of collaboration and automation has been highlighted [318, 332]. For instance, security practitioners rely on each other to see the "big picture"[53] and may resort to developing their own tools, e.g., customizable scripts, to carry out specific tasks, capture and share tacit knowledge or improve the usability of a tool [368]. Security managers and analysts in SOCs tend to agree that any cutting-edge technology at their disposal would be underutilized if it suffers from poor usability or if it is hard to learn, thereby also shifting their focus towards the tools and away from the incidents [204].

Investigating collaborative work practices in the context of CTI, Ahrend et al. found that practitioners engage in formal and informal collaborative activities, however, awareness about existing threat and defense knowledge (TDK), its availability, and correlation is impacted by the largely tacit nature of TDK, which is lost due to employee turnover or memory loss [10]. Further, the lack of formal documentation or access restrictions also played a role. A number of system circumvention activities were also reported, e.g., analysts storing TDK artifacts on local machines instead of uploading them to collaborative in-house systems due to perceived usability gains as well as perceptions that "their work is rather individualistic and not directly relevant to other analysts" [10]. When CTI is shared across borders, cultural and language barriers may also arise, thus parties engaged in CTI exchange should define a sharing language as well as understand and respect cultural differences [364].

Safa et Von Solms investigated the impact of extrinsic and intrinsic motivation on employees' attitudes toward the intention of sharing information security knowledge [290]. They

found that earning a reputation, gaining promotion, and satisfying curiosity, all had positive effects on employees' attitudes, which in turn affected CTI sharing behavior. Expanding on earlier work taking economic perspectives on information security sharing [130, 140], Mermoud et al. proposed a behavioral framework theorizing how and why human behavior and sharing of security information may be associated [238]. They highlighted that human behavior may be at the core of the problem why CTI is underutilized despite being beneficial, yet cautioned not to infer that CTI sharing should be mandated as that could achieve the adverse effects of inducing compliance by sharing threat information that may not be relevant, accurate, or timely [238].

The development and improvement of security professionals' skill-set is considered a key aspect of human capital management, however, recruiting and retaining security staff have been reported as major challenges [359]. Furthermore, there are high turnover rates among security analysts due to burnout, which not only leads to increased spending on frequent hiring and training of new analysts, but also impacts the team spirit and collective incident response [65]. Researchers found that operator fatigue and frustration increased significantly over the course of tactical cyber operations [95], while procedurally distinct network analysis tasks elicited differentiable effects on the cognitive stress and workload of operators [147]. As research in security practitioners and human aspects in cyber is still immature [95], the researchers encouraged further work regarding the specific needs and challenges associated with different tasks in the cyber domain, as well as the nature of the human-computer interaction and the effects of these interactions on the operators' mental states and performance capabilities [147].

### Further Reading

Additional references pertaining to CTI sharing standards and platforms as well as user experience aspects of CTI sharing platforms are provided in Chapter 3.

## 2.6 Secure and Private Communication via Email

Email continues to be one of the largest messaging systems on the internet and a key enabler of various online services. Over the 50 years since its inception, a number of enhancements have been proposed and deployed in response to the security and privacy shortcomings that are inherent to email by design [288]. While examples such as *link encryption* (i.e., securing email during its transit from one mail server to another or between a mail server and a client), *domain authentication* (i.e., ensuring that an email originated from a specific domain), or *spam mitigation techniques* (e.g., machine learning algorithms for filtering phish-

ing email [131]) are much-needed steps in the right direction, research shows that email still remains largely insecure [94, 176, 229]. According to the ENISA Threat Landscape 2021 Report, email related threats such as phishing, spear-phishing, business email compromise (BEC) and spam, continue to rank among the prime threats affecting organizations and individuals [110]. Moreover, phishing remains one of the two most common infection vectors for ransomware, and as of recently, plays a key role in disinformation attacks [110].

In Chapters 5 and 6 we focus on systems for *secure email* i.e., those that offer end-to-end encryption, which is the highest level of protection possible. In addition to the issues of unsecured links and message forgeries, end-to-end encryption also addresses the problem of untrusted servers [288]. Secure email, thus, provides the guarantees of *confidentiality*, *integrity*, *authenticity*, and *non-repudiation* [214]. From an end-user's perspective, this means:

- there are mechanisms in place that protect the email content from being read by entities other than the intended recipients;
- the contents of the message are received just as they were sent;
- a recipient can verify whether a message was sent by a party who is in possession of a specific (private) key;
- a recipient of a message can convince others that the message was sent by a party in possession of a specific (private) key i.e., the sender cannot successfully deny that she sent the message.

While a myriad of secure emailing tools exist as standalone desktop or mobile apps, plug-ins, browser extensions or websites, wide user adoption figures and continued use of secure email systems cannot be asserted even in the case of user groups that may communicate sensitive information over email, such as journalists [232].

Despite the lack of widespread adoption (as elaborated next), we believe that research in this topic is not only relevant for improving security, but it is of paramount significance for individuals, marginalized communities or disadvantaged groups that rely on these technologies to protect their privacy. Furthermore, secure email systems can be of utmost importance to professionals and businesses that strive to meet legal requirements with respect to data protection, such as the General Data Protection Regulation (GDPR) [113].

### 2.6.1 Usability and Adoption of Secure Email

Unlike secure instant messaging applications, end-to-end email encryption has failed to achieve widespread adoption even though solutions based on two of the most popular encryption standards, OpenPGP [22, 58] and S/MIME [100, 101], have been around for more

than two decades. Given the centralized trust model in S/MIME and the inherent reliance on Certificate Authorities (or delegated subordinate local agencies), proponents of full decentralization and zero trust advocate the use of PGP instead. However, a recent ethnographic study of PGP's decentralized trust model found that in practice both decentralized trust relationships as well as centralized assurance structures are used to construct PGP's *web of trust (WoT)* [224]. In the latest NIST recommendations and guidelines for enhancing trust in email, S/MIME has been highlighted as the recommended protocol for email end-to-end authentication and confidentiality, despite its usage not being common [281].

A recent study by Stransky et al. measured the use of PGP and S/MIME among 37,089 users at a large university over the period of 27 years [329]. While S/MIME was found to be more widely used than PGP for both encrypting and signing messages, the researchers found that only 5.46% of the users ever used PGP or S/MIME [329]. Furthermore, out of the 81,612,595 analyzed emails, only 0.06% were encrypted and 2.8% were signed [329]. The study confirmed a number of common beliefs and previous findings stemming from years of research in this field, in particular, that PGP and S/MIME are considered niche tools predominantly used by a small number of security and privacy conscious users [329]. We provide a brief overview of the main related work next.

Highlighting the importance of taking a user-centered approach to security, in the mid-1990s Zurko and Simon were among the first to indicate potential usability problems with PGP, in particular the complexity of managing keys and trust [397]. The seminal work by Whitten and Tygar [372] showed significant problems with the existing PGP client at the time, where only 4 out of 12 study participants were able to successfully encrypt a message, and only one participant successfully completed all secure email tasks. This research helped shape the new field of usable security and inspired subsequent investigations. While a study using an updated version of PGP by Sheng and colleagues showed similar results [310], the work by Garfinkel and Miller [134], which combined the idea of Key Continuity Management (KCM) with S/MIME, suggested that automatic key generation and management was more usable than the manual key management in the original study.

Usable security research in secure email suggests a strong user preference for encryption tools that offer a tight and seamless integration with users' existing email systems over standalone encryption software [23, 285, 287]. Studies on the implications of automatic vs manual encryption on usability and trust is mixed. Ruoti et al. initially found that trust in the system is reduced when it is hidden from users how a secure system provides security [285, 287]. In contrast to these findings, Atwater et al. indicated that user trust was not impacted by the transparency of encryption tools [23] .

Lerner et al. showed that despite lawyers and journalists having an equal motivation

for protecting their communications, the two user groups can have sufficiently different requirements that they may require entirely different tools for email encryption [216]. Furthermore, encrypted email may be unhelpful or worse, if it leads to a false sense of security among certain user groups which have specific requirements, e.g., journalists that need to protect metadata on communication patterns [216]. Designers should, thus, explain the security properties that encryption tools offer [26], whereby inline, context-sensitive tutorials and streamlined onboarding appear to be essential [286].

In addition to poor interface design choices, key management difficulties and mistaken mental models, researchers have identified social and cultural norms as factors that contribute towards non-adoption of email encryption too [134, 136, 274]. Similarly, usability might not necessarily be the primary obstacle to adoption of secure communication tools, but rather fragmented user bases, lack of interoperability and low quality of service [4]. The findings of Abu-Salma and colleagues, that many users adopt end-to-end encryption along with other features, rather than specifically for security reasons [3, 4], were also recently confirmed by Stransky et al. [329]. They suggested that future work of secure email systems should place emphasis on offering more value to users on top of security and privacy.

### Further Reading

Additional information and references pertaining to $\mathsf{p} \equiv \mathsf{p}$, the secure email system employed in our use case investigations, can be found in Chapters 5 and 6.

## 2.7 Digital Health Technology: COVID-19 Contact Tracing Applications

The World Health Organization (WHO) defines digital health as the "the field of knowledge and practice associated with the development and use of digital technologies to improve health" [373, p. 11]. The concept encompasses digital consumers along with a range of smart and connected devices as well as uses of digital technologies, such as Internet of Things, big data analytics, artificial intelligence, etc. Given the nature and sensitivity of health data, digital health technologies call for adherence to high safety and security standards as well as consideration of different issues related to cybersecurity, trust building, accountability, governance, and ethics, to name a few [373].

It goes without saying that people's perspectives and behavior regarding technology and health (care) are changing. For instance, reported figures suggest that there are over 100k smartphone health apps available worldwide, with over 500m users using them in order to keep track of their everyday activities (as referenced in [360]). However, questions have been raised about the usefulness and efficacy of such apps, with research showing that

there is often unavailable or questionable evidence supporting the claims made by health apps [246]. In terms of security and privacy, for instance, sensitive health information about a user can be revealed by the simple fact that a particular app is installed on a user's phone, which is even more problematic considering that the practice of collecting information about installed apps is widespread [263]. Thus, there is growing concern that digital health technologies often reach consumers directly without passing through the rigorous scientific and regulatory processes typical of many other medical products and services [75]. Such concerns are only exacerbated in extraordinary circumstances, wherein national health agencies and regulatory bodies look to digital technology for innovative solutions that can support public health efforts within existing and emerging threats, such as the COVID-19 pandemic, which swept across the world at the beginning of 2020.

### 2.7.1 Contact Tracing Application Origins

Contact tracing is a process in which public health workers interview or survey people who have been diagnosed with an infectious disease in an attempt to prevent onward transmission by identifying their recent contacts and isolating those who are at risk [242, 247, 254]. With the continuation of the COVID-19 pandemic, and the prevalence of increasingly contagious strains, a wide range of contact tracing solutions have been proposed from manual to semi automated to fully automated track and trace systems. At their core, all the approaches serve one objective, which is to allow for quick detection of infected individuals and prevention of further transmission of SARSCoV-2 through isolation and quarantine.

In the search for scale and speed of deployment and detection [199], smartphone apps have been developed to control, contain, and help mitigate the spread of the virus [241] and to supplement manual contact tracing efforts. By the end of March 2020 and the beginning of April 2020, many countries started to deploy contact tracing apps to combat the spread of the pandemic. These apps differed on several levels, such as their technological architecture, the functionalities they offered to their users as well as the very different realities and governance settings underpinning their implementation across countries [52, 67]. Nonetheless, the overarching and communicated purpose of all these digital contact tracing apps (CTAs) was a shared one: to identify and notify people of their potential exposure to COVID-19 in an effort to keep infection rates low, while also allowing greater freedom of movement.

### 2.7.2 Digital Contact Tracing Applications: Technologies and Design

National and local preferences have differed across countries in terms of the application design, functionalities and features, architecture as well as their development approach (i.e., involvement of research institutes and technology companies in the app design and deployment) [99]. Some apps have been designed by a small number of researchers and coders, while others jointly by states, medics, and tech companies like Google and Apple [19]. This has resulted in some important differences in how apps were actually rolled out and used in practice across different countries.

A number of papers, reports, and online resources have elaborated on the technological differences and architectural choices with respect to digital contact tracing (e.g., [241, 266, 356]). Apart from the crucial distinction between voluntary and non-voluntary approaches to digital contact tracing, for our discussion, it is important to highlight a distinction between two technological and two architectural differences. The first refers to the technology deployed for detecting exposures to a person infected with COVID-19, namely location-based tracking via GPS on the one hand, and proximity-based tracking via Bluetooth, on the other. The second distinction refers to where the contact tracing data is stored and processed. In a centralized architecture, the storing and processing takes place on a central server, typically run by a national health authority. In a decentralized architecture, this takes place on the mobile devices of the users.

Several European countries, including Belgium and Germany, decided to deploy contact tracing apps using Bluetooth technology and following a decentralized approach, whereas other countries like Singapore and France choose a more centralized approach [241]. In some other countries, public health authorities released apps using Apple and Google's Exposure Notification API [241]. Each choice has been debated in view of the associated implications on users' privacy and, conversely, the management of the pandemic [346, 356, 371].

### 2.7.3 Inclusion and Access

Another factor regarding the roll-out of contact tracing apps was linked to the potential limits of smartphone penetration, the capacities for user uptake and the implications thereof.

While smartphones were among some of the leading tools available following the COVID-19 onset, various wearable complements and solutions have emerged since. These wearables serve in some instances as a way to ensure greater capacity for uptake across the population, inclusive of potentially more socio-economically vulnerable groups or temporary visitors, such as the case for Singapore's Bluetooth-based TraceTogether Tokens which are compatible with tracing apps and have an extended battery life [146]. In other instances,

these have been employed to further control and enforce quarantine requirements such as the case of Hong Kong's complementary wristband [145], in which the usage would imply greater enforcement of governmental control. Nevertheless, apprehensions of users to these wearables and other alternatives, with respect to their collecting and processing of "unnecessary" data when it comes to the pandemic, stress that the price to access may ultimately be higher for those individuals and groups who do not have a phone or cannot download the app, thus concerns for adoption may consequently remain equally prevalent [199].

Focusing on inclusivity in order to ensure effective user adoption, however, has not only relied on the technical infrastructure, but also on the application designs themselves. Blacklow et al. [45] focused on evaluating the usability of 26 covid contact tracing apps in the United States. The study was particularly focused on the access to contact tracing apps by individuals with low digital literacy skills and those who displayed communication barriers. The study highlighted poor considerations to users who did not speak English, emphasizing the high reading capacities that were required, and suggested that the reach of the apps as public health tools may thereby be limited. Furthermore, only 12% of the apps were complemented with inclusive illustrations representative of the population they aimed to serve, and the majority demanded extra effort (additional clicks) to reach testing and public health support. Similar limitations on inclusiveness in apps were also noted in a study conducted in the Netherlands by Bente et al. [41], which is discussed in greater detail in Chapter 7.

### 2.7.4 Contact Tracing Application Adoption

Research to date on the motives for users' willingness, undecidedness or hesitation to adopt contact tracing apps has been studied across and within a range of settings. Studies have employed different methods in their investigations of the user experience and perceptions of security and privacy aspects of such applications. These studies, in most part, have taken the form of surveys, or have leveraged existing public health datasets to answer app effectiveness and uptake reasonings. That being said, many findings to date have been based on the evaluation of hypothetical application scenarios and demonstrated a tendency towards quantitative methods.

More recently, a shift in focus towards rolled out contact tracing apps and new studies conducted with think-aloud protocols, focus groups, longitudinal approaches, as well as other qualitative and quantitative methods have provided new findings on the range of technological, user, societal and cross-cultural factors that impact the intentions and decisions to adopt and use contact tracing apps. The aforementioned and overarching points on user adoption are described and discussed in greater detail in Section 7.2, followed by

an overview of the empirical studies, findings and gaps in the context of France and Germany more concretely, which forms our third cybersecurity and digital privacy context under study in this thesis.

### 2.7.5 Effectiveness/Efficacy of Digital Contact Tracing Applications

The MIT's Pandemic Technology Project [241] whose objective is to monitor the developments, roll-outs and usage of contact tracing and notification apps globally in its last update (March, 2021) listed a total of 49 international applications not counting the different states in the US. The Knowledge Hub [218] lists 22 European apps, of which 19 decentralized, 3 centralized, all Bluetooth-based except for one, Bulgaria's ViruSafe, which it notes as employing GPS. In their review and taxonomy of existing health apps aimed at combatting the COVID-19 pandemic, Almalki and Giannichi [12], in screening Google Play and the Apple Store between April and September 2020, found 298 apps, of which 115 were further analyzed as they met their inclusion criteria. The authors documented 29 technical features, which they then translated to five driving purposes underpinning the apps. 67% of the applications were nationally developed (government national authority) with the aims of promoting individuals to monitor their health. Other design aims focused on awareness raising on mitigating the pandemic (27%), exposure management (20%), health monitoring by health care professionals (17%) and research (3.5%). The study highlighted the participatory approach of current apps given that emphasis of apps were largely driven by self-tracking and assessing of health.

Despite this influx of contact tracing apps, very little remains known about their societal impact: how many people will download and use these apps? What will make people continue using them? How widely used do the apps have to be in order to succeed? How do people perceive the benefits and drawbacks of such apps? Are there any cross-cultural differences in people's perceptions, expectations, and privacy concerns with regard to these contact tracing apps?

At the onset of the pandemic, the introduction of COVID-19 contact tracing apps was initially touted as a possible solution solving the burdensome challenges of manual contact tracing needs. Countries saw the applications as a potential low-cost and scalable solution able to support timely testing and isolation [55]. Nevertheless, marred by a number of challenges (technological sensitivity, privacy concerns, user experience, actual adoption, etc.), the initial hype was met with a variety of disappointments from setbacks on application roll-outs to poor adoption rates across population groups, disruptive large scale isolations such as the UK *pingdemic* and potentials for false positives [365].

With the increasing penetration of contact tracing apps, the substantial investments dedicated to developing, communicating and maintaining them, as well as the supportive promise that they brought to struggling health departments in the aims of containing the COVID-19 pandemic, researchers have aimed at gaining a better understanding as to what user preferences drive as well as hinder uptake in order to enable broad adoption.

Conducting one of the first systematic reviews on the effectiveness of contact tracing apps in October of 2020, Jenniskens et al. [183] searched across databases for model-based and empirical studies on the efficacy of contact tracing to retrieve a total of 2,140 studies. Their findings, based on a further refined and eligibility criteria adhering 17 studies, highlighted that, in general, the studies they investigated demonstrated contributory effects of the adoption of contact tracing apps on total infection numbers, R and mortality rates when rates of adoption were 20% or higher. Nonetheless they also pointed out that effect sizes were variable based on parameters employed across different study models (i.e., delays in testing, asymptomatic cases), and the methods of resulting interventions following contact tracing app notification. This serves to highlight the importance of further understanding the effects of contact tracing applications through comparative, empirical and methodologically sound studies.

Shahroz et al. [307] in their study reviewing post deployment merits of contact tracing solutions, shared similar findings in questioning the effectiveness of apps, underscoring the lack of comparative evaluations of different contact tracing apps to date. Furthermore, the study raised the need for an additional dimension in efficacy assessment stating that "from a global perspective, digital contact tracing may be suitable for developed countries. However, in developing and underdeveloped countries, digital contact tracing frameworks may not achieve their full potential" [307, p 5]. These statements and the implications on fairness, social justice and inclusion of COVID-mitigating efforts, are in line with aforementioned movements in the creation of wearable alternatives. Nevertheless, they also serve to draw light on people in more vulnerable and economically precarious conditions with respects to scalability of the solutions for effective deployment, on the one hand, as well as capacity and willingness to adopt, on the other. Coupled with findings such as those from the French Health Literacy Survey administered to 1,003 people in France in 2019 during the pandemic onset, which demonstrated the importance of ensuring equal opportunities, literacy and connectivity in the development of effective applications [343]. The survey which asked perceptions on institutional trust, health literacy, COVID-19 prevention and the acceptability of mobile contact tracing, alongside sociodemographic data grouped users into three different willingness profiles: App-supporting, App-willing (19.2%) and a majority group App-reluctant (50.3%). More concretely in its investigation of associated factors to

willingness and rejection, the study concluded that "the most economically precarious people, who are more at risk of SARS-CoV-2, are also the most reluctant to use a contact tracing app" [343, p 2] stressing the need for "a reduction in inequalities by acting on structural determinants" [343, p 2].

More recently, Vogt et al. [361] put forward that future applications should include effectiveness evaluations so as to be able to better justify investing in them. In the study, the authors sought to evaluate the usefulness of CovidSafe, Australia's national contact tracing app, more specifically on New South Wales, using data across the new South Wales Management System, Case interviews and the National COVID Safe database, documenting individuals in the state above 12 years old who confirmed cases locally from May-Nov 2020. The app ultimately was shown to have identified (<0·1%) added close contacts who had not initially been identified by conventional contact tracing. The study also conducted 6 semi-structured interviews with staff to understand the perceived usefulness. Staff findings highlighted that "COVIDSafe generated a substantial additional perceived workload for public health staff and was not considered useful" [361, p 1]. The authors further put forward the need to reconsider investments, as well as the necessity to consider the human load that apps entail in the uptake so as to enable the provision of more supportive and meaningful contributions to users.

However, despite their efficacy remaining a contested issue and findings diverging significantly across countries and studies [148], there is some consensus that contact tracing apps are not inconsequential, but instead have become part of the pandemic-fighting toolbox (alongside maintaining general hygiene, masks, ventilation, regular testing, health policies, vaccinations, covid passports and health certificates).

Several recent studies have highlighted the efficacy of diverse apps [291] and provided greater insights into necessary conditions for their usage as complementary tools to the health crisis. Wymant et al. [384], investigating the deployment of apps in Wales and England through modeling and statistical comparisons, claimed that the use of digital contact tracing allowed for a larger reach in contacts being traced and notified in a timely manner as opposed to contact tracing. They further elaborated that this was believed to hold especially beneficial for the identification of contacts beyond individual's homes. Rodriguez et al. [280] conducted a study that consisted of 4 simulated outbreaks and user behavior tracking across the 10,000 inhabitants in the Canary Islands to test the Spanish Radar Covid app's efficacy. The authors concluded that the controlled experiment provided demonstrable positive evidence of the technologies complementarity to manual contact tracing efforts, given that campaigning for uptake was clear and appropriate to ensure penetration and user compliance. Elmokashfi et al. [105] in investigating Norway's centralized Smittestopp app,

albeit criticized for its privacy invasive nature and stopped given its invasive tracking practices, do provide us with some unique data gathering and efficacy insights. In their study the authors claimed that an approximate of 11% of the contacts identified via the contact tracing app would have otherwise gone unidentified in manual contact tracing.

Efficacy and effectiveness as well as privacy discourse has also centered around the ongoing debate of centralized versus decentralized systems. White et Basshuysen [371] in comparing the risks associated with each approach, through a safety engineering lens demonstrated the vulnerability to privacy breaches across both. Furthermore, the authors posit that the binary trade-off arguments between respecting user privacy and promoting public health are not so clear cut, with the authors arguing instead that the differing systems instead present users and adopters with the threat of being prone to different types of breaches.

Download thresholds (%'s of the population) and app uptake with respects to potential efficacy have also been featured in several studies. Despite the initial views that contact tracing apps need at least 60% adoption to be effective, studies have since displayed the added value of contact tracing and early notification systems as potential complements in the fight against COVID-19 even if the rate of adoption is under 60% [5]. These debates nonetheless serve as an important reminder that contact tracing apps are not a standalone solution, but a complementary measure in support of curtailing the pandemic.

### Chapter Conclusion

Having introduced the necessary background and preliminaries relating to our thesis, we are next going to dive deeper into the three cybersecurity and digital privacy contexts of *(i)* CTI sharing platforms, *(ii)* secure and private communication via email, and *(iii)* COVID-19 contact tracing apps.

Context I

# Cyber Threat Intelligence

*A little learning is a dang'rous thing;*
*Drink deep, or taste not the Pierian spring:*
*There shallow draughts intoxicate the brain,*
*And drinking largely sobers us again.*

Alexander Pope

# 3

# What's in a cyber threat intelligence sharing platform?

CHAPTER ORGANIZATION. This chapter is organized in 7 sections. First, we provide more information regarding our research context and related work. Then, we introduce our use case investigation, research methodology and study design. Subsequently, we present and discuss the results of our study. Finally, we put forward avenues we believe are worth investigating further within the context of our use case and beyond.

## 3.1 INTRODUCTION

Even before the onset of COVID-19, the scale and sophistication of malicious cyber activities by various threat actors highlighted the distressing risks posed to our increasingly digitized and interconnected societies. The pandemic only further demonstrated how cyber criminals and other actors have adapted their practices to fit the COVID-19 narrative and exploit the crisis [118]. The Colonial Pipeline [72] and SolarWinds [71] cyber attacks further illustrate the palpable disruption to business continuity of critical infrastructure and potential threats to national and global cybersecurity. The consequences of cyber attacks are manifold, with attacked organizations often experiencing not only different kinds of out-of-pocket costs, such as investigation and remediation expenses, legal and regulatory fines, etc., but also reputation costs which can economically be much larger [192]. Furthermore, there are spillover effects where industry competitors of attacked organizations do not benefit from such cyber attacks, but in turn also experience shareholder wealth losses [192]. Thus, in order to mitigate the likelihood or impact of future incidents, organizations tend to engage in cooperative relationships with other third parties [198].

The timely and efficient gathering, analysis and, in particular, exchange of cyber threat intelligence (CTI) is therefore seen as a promising approach to countering these new generation threats. Parties that belong to a CTI sharing community can leverage the collective knowledge, experience, and capabilities to create an extensive situational awareness picture of the threats their organization may face [186]. It has been shown that CTI sharing can be effective in the mitigation of ongoing and the prevention of potential attacks, in the faster identification and detection of threats, threat actors, and their tactics, techniques and procedures (TTPs) [341]. Furthermore, CTI sharing can be a cost-effective tool and reduce the likelihood of cascading effects across entire systems, sectors or industries [341]. Thus, there is a wide consensus on the benefits of CTI sharing in different contexts, such as financially-driven cyber criminal activities, cyberwar, hacktivism and terrorism [312]. That being said, CTI exchange depends on a number of dimensions and is complicated by challenges that entail technical, organizational, legal, economical, and social aspects [106, 109, 130, 394]. These include efficient cooperation and coordination, legal and regulatory compliance, standardization, regional and international implementation, and technology integration [312].

The acknowledgement of the multi-faceted complexity of CTI exchange, motivates for a multi-disciplinary and multi-stakeholder discourse as well as mobilization of diverse expertise in the collective pursuit of defending our societies from malicious cyber activities. In recent years there has been significant progress in overcoming technical hurdles in establishing the formats and platforms for CTI exchange. Further, some attention has been devoted to uncovering and addressing challenges around organizational modalities, incentives, and implications associated with CTI sharing. For instance, in light of the persistent and increasingly sophisticated cyber attacks, a recently signed Executive Order on Improving the Nation's Cybersecurity [350] made a specific reference to removing (contractual) barriers to threat information sharing. Many questions still remain open, however. In particular, those concerning the user experience and unique challenges faced by security professionals and other participants in CTI exchange that make use of threat intelligence sharing platforms, which have become indispensable tools for cooperative and collaborative cybersecurity.

Despite early views that security and usability are at odds with each other [77], the security world has become acutely conscious of the importance human aspects play in the overall security, use, and adoption of systems that are critical from a security and privacy perspective. This is recognized also in the CTI context, where human motivation and UX design have been highlighted as critical success factors for threat intelligence sharing platforms [293]. Yet, empirical evidence on how UX impacts the use and adoption of such platforms, and by extension the cyber incident prevention and response efforts, is largely missing.

**Contributions**

Motivated by this research gap, in a first study of its kind, we establish a UX benchmark for a leading open source CTI sharing platform, called MISP, which is used by over 6,000 organizations [240]. Further, applying a blend of quantitative and qualitative methods in a delicate user research context, we uncover what users value about the studied platform and why, as well as, what they think could be improved in order to overcome the voiced limitations and pain points.

As the core concepts of CTI exchange are incorporated in many CTI sharing platforms, our study not only provides actionable inputs to the developers of MISP, but equally serves to highlight key findings and UX recommendations of relevance to CTI sharing platforms more generally. Besides advancing our understanding of human factors and interaction aspects within the CTI sharing context, this report also draws attention to the possible negative outcomes in terms of CTI sharing effectiveness or disclosure of sensitive information due to usability issues or overall poor UX.

It is worth mentioning that our study insights may be limited due to the challenging participant recruitment circumstances. Nevertheless, we believe that our research has an empirical and a methodological contribution. The former informs the improvement of cybersecurity in real-world systems, the latter demonstrates the utility and necessity of UX research methods applied in a new context, which is in dire need of further interdisciplinary scrutiny.

## 3.2 Background and Related work

### 3.2.1 CTI sharing standards and platforms

From the very beginning, organizations engaged in CTI exchange have been faced with a number of technical and operational hurdles, e.g., CTI exchange can demand a great deal of manual effort as threat information can come from a variety of sources [364]; organizations use their own terminology and data standards, which do not directly correspond to those of other organizations [306]; the utilization of meaningful threat intelligence depends on the relevance, timeliness, accuracy, and other quality aspects of CTI artifacts [300], etc.

Thus, questions such as how to automate, harmonize and standardize CTI, while keeping human judgment and control involved in sharing [31], have led to the establishment of a number of standards for structuring and sharing data as well as to the emergence of sharing platforms in an attempt to facilitate sharing and address the problems of collecting and storing threat intelligence. In recent years, a number of papers investigated the CTI

sharing landscape, providing comparative analyses of the different platforms, standards, exchange formats and languages as well as the publicly available sources of threat feeds [33, 84, 270, 297].

For instance, Sauerwien et al. [297] found that most CTI sharing platforms rely on standards such as OpenIOC, STIX, and IODEF, arguing that STIX [31] can be considered as the de-facto standard for describing threat intel as it is the one most commonly used. Ramsdale et al. highlighted, however, that despite having industry and community support, the use of STIX is not that widespread, it often suffers from poor implementation, and that recent trends indicate the use of APIs or platform-specific formats (e.g., MISP and custom JSON formats) as a better fit for the given use cases [270].

In a recent investigation, De Melo e Silva et al. established evaluation criteria for the different CTI sharing standards and platforms based on the selection of the most relevant candidates [84]. They reported that due to the different goals that CTI sharing platforms have, at the moment there is not one fully complete platform that attends to all CTI processes. Nevertheless, MISP and OpenCTI were highlighted as platforms with the most holistic approach, and applicable in a great deal of scenarios. Furthermore, MISP was ranked highest in terms of popularity and considering the compatibility with different formats it could be considered as the most flexible.

### 3.2.2 User Experience of CTI sharing platforms

The fact that human-centered design and UX aspects are of paramount importance in the CTI sharing context can also be attested by the inclusion of *usability* as a key evaluation criterion in the recently proposed frameworks for comparing CTI platforms [84]. Nevertheless, despite this recognition, the question of usability and UX remains largely unexplored in this context.

To the best of our knowledge, the only study that explicitly is motivated and investigates UX aspects is the work by Sander and Hailpern [293]. Conducting a series of interviews and ethnographic observations of security analysts and domain experts, the authors proposed a number of *personas* i.e., narrative descriptions of user archetypes reflective of the most important users of a CTI sharing platform. Furthermore, they proposed a number of design requirements, and reflected on three high level insights, grounded in their user research. These refer to: (i) the oftentimes differing personal and corporate motivations and incentives to CTI sharing; (ii) the fact that there is no one typical user, but that there are significant differences as to the type and amount of information that is consumed and contributed across the different personas; and (iii) that younger users expect CTI sharing

platforms to offer a sophisticated UX. Finally, they expressed an interest in collaborating with existing solutions in an effort to try and integrate the various design requirements that they put forward, and highlighted the importance of validating them in formal user studies.

Apart from an informal inquiry into the impressions of the usability of a new decentralized CTI platform prototype [237], we are not aware of any study that has performed a formal usability or UX evaluation of an established CTI platform.

The gap in our understanding of the constraining and enabling factors of CTI sharing platforms from a UX lens poses significant challenges in terms of ensuring that our designs match the needs and capabilities of the people we are designing for in such a highly-complex cooperative environment. Furthermore, we believe that it also prevents us from identifying and addressing user misperceptions of system security and privacy, which can have adverse effects on CTI sharing effectiveness. To this end, as far as we know, we are conducting the first such UX evaluation, within the context of the MISP sharing platform.

## 3.3 MISP

Conceived within military circles as a malware information sharing platform a decade ago, MISP has in the meantime matured into a community-driven project for gathering, sharing and correlating diverse types of threats, such as indicators of compromise (IoCs), financial fraud information, counter-terrorism information, etc. [240, 363]. As previously mentioned, MISP is regarded as one of the leading OSINT platforms, used by thousands of organizations active in different domains, ranging from NATO agencies and ministries of defense, CSIRT communities, private sector actors etc. [240].

Organizations wishing to engage in CTI exchange via MISP, either need to approach i.e., be invited to an established sharing community, or initiate their own MISP instance given that the source code underpinning the platform is publicly and freely available on the MISP GitHub project page [138]. MISP can also be easily retrofitted for specific communities or objectives, such as the recent COVID-19 MISP instance dedicated to sharing medical information, cyber threats and disinformation related to COVID-19 [239].

### Technical details

We invite interested readers to consult available MISP resources (e.g., [138, 240, 363]) in case they would like to better familiarize themselves with the technical details and implementation. Here, we briefly outline some main points.

A MISP instance can be considered as an independent centralized server that facilitates the consumption and contribution of CTI among a defined set of participating organiza-

tions. MISP instances can be standalone or they can connect to and exchange information with other instances via different synchronization mechanisms, pursuant to the sharing rules or negotiated terms. Connecting or syncing MISP instances allows for shared CTI to traverse between them in one or both directions, as per user-defined distribution settings. Thus, interconnecting multiple instances creates a de facto decentralized network which is able to send and receive data entries, called *events*, described with different levels of granularity of information as per the user's wish. In terms of the interface used to access MISP, a key distinction can be made between UI users (those using the web portal) and API users (those using ReST API).

**Features and functionalities**

In terms of supported features and functionalities, MISP seems to account for a large number of the design requirements highlighted by Sander et Hailpern [293], e.g., automatic correlations to find relationships between attributes and indicators from malware or attack campaigns, historical info for indicators and pivoting capability, non-attribution, etc.

A number of actors in the MISP user community regularly organize training sessions and community meetups in order to address training needs as well as discuss the future development of the platform. Furthermore, lots of resources, such as training materials, virtual environments and online repositories, are available to help (prospective) users experiment and test the latest updates, builds and features under development [70].

### 3.3.1 Study motivation

MISP is a technically-advanced system. If it aims to cater for a diverse set of users involved in CTI exchange, it needs to account for their distinct needs and objectives as well as their capabilities to engage in CTI sharing activities of various complexity. To date, there appears to be no empirical evidence on UX evaluations of MISP by the different user groups, nor investigations of usability issues or challenges faced by users. Given the wide adoption and large user base of MISP, we were motivated to shed light on UX aspects of CTI sharing platforms by taking MISP as a representative use case in this relevant cybersecurity context.

To this end, we formulated the following research questions:

1. How do different security information workers evaluate the user experience of MISP?
2. What do users value about MISP and what do they think could be improved?
3. Which user needs are addressed and accounted for by MISP, and which are neglected?

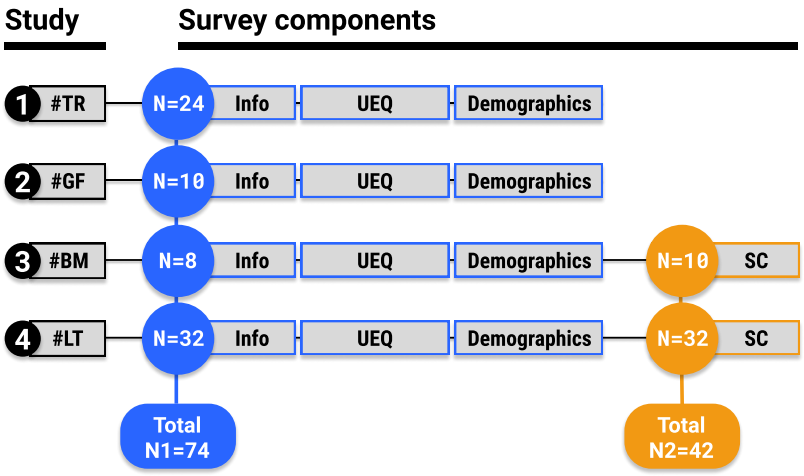



**Figure 3.1:** Overview of the studies conducted in Chapter 3

In line with lessons learned and taking into account the voiced difficulties getting access to participants for cybersecurity research [54, 95, 255, 258] we chose to conduct several smaller studies that had a low impact on the environment.

*Recruitment.* Over the course of two years, we took part in a number of events organized within the MISP user community that were facilitated by the Computer Incident Response Center Luxembourg [69], which is an organization that co-finances and resource-wise supports the development of MISP.

These events represented in Figure 3.1 – Study overview, refer to: two in-person training sessions, indicated as Study 1 and Study 4; an annual summit of the MISP user community, indicated as Study 2; and one regional community event, indicated as Study 3.

*Survey.* Data collection for Studies 1, 3 and 4 took place in person, whereas for Study 2 via an online form.

*Ethics.* The study was approved by our organization's ethics review panel, and consent was obtained through voluntary participation, which was not financially compensated.

### 3.4.1 STUDY COMPONENTS AND METHODS

INFORMATION AND CONSENT. At the beginning of the studies, the participants were informed that the survey is part of an investigation that aims to assess the user experience of the MISP Open Source Threat Intelligence Sharing Platform and learn more about the needs of its users. They were informed that participation was voluntary and anonymous as well as

that they can withdraw their consent to participate at any time without giving reasons and without negative consequences.

UEQ – User Experience Questionnaire. The UEQ is a validated instrument for measuring UX [213] and it is the most widely used standardized UX questionnaire in recent years [96]. It contains 6 scales with a total of 26 items in the form of semantic differentials: (i) *attractiveness* measures users' overall impression of a system or technology; (ii) *perspicuity* measures the degree of ease of learning how to use a system; (iii) *efficiency* measures whether users have to put unnecessary effort into solving a task; (iv) *dependability* measures whether users feel they can rely on the system; (v) *stimulation* measures the level of excitement or motivation to use the system; (vi) *novelty* measures how innovative or creative do users perceive the system to be i.e., whether it triggers their interest [302]. Through the *perspicuity*, *efficiency*, and *dependability* scales, the UEQ investigates the pragmatic, goal-directed, quality aspects. The *stimulation* and *novelty* scales investigate the hedonic aspects, which are not goal-directed, but appeal to sensations. The *attractiveness* scale is considered as a pure valence dimension [302].

Demographics. After the UEQ, there was a demographics section where we sought to learn more about our participants, their education, technical background as well as prior experience and engagement with MISP. This was the last section in Studies 1 & 2.

SC – Sentence Completion. SC is a semi-structured projective technique that can be deployed to understand user needs and values, as well as evaluate user experience, by providing only a sentence stimulus to research participants who are free to interpret it and respond to it from their own frame of reference [207]. Complementing UX questionnaires, sentence completion is a practical method for obtaining qualitative inputs and a quick overall understanding of how users interpret their experiences with a system, in a structured way and in a fraction of the time in comparison to interviews [207]. For our investigation, we tailored the stems used by Kujala et al. [207] to our context, represented in Table 3.6. SC was the final section of the survey in Studies 3 and 4.

## 3.5 Results and Analysis

### 3.5.1 Participants

Out of the 74 participants, 70 (95%) were male. 66 participants (89%) had an engineering or computer science background. 63 of them (85%) had a Bachelor's degree or higher.

| N | Demographic | Count | Percent |
|---|---|---|---|
| 74 | Gender | | |
| | • *Female* | 2 | 2.7 % |
| | • *Male* | 70 | 94.6 % |
| 74 | Age group | | |
| | • *18–25* | 11 | 14.9 % |
| | • *26–35* | 32 | 43.2 % |
| | • *36–45* | 27 | 36.5 % |
| | • *46–55* | 4 | 5.4 % |
| 73 | Education | | |
| | • *Less than a Bachelor's degree* | 10 | 13.7 % |
| | • *Bachelor's degree* | 32 | 43.8 % |
| | • *Master's degree* | 28 | 38.4 % |
| | • *Doctoral degree* | 3 | 4.1 % |
| 74 | Engineering or Tech Background | 66 | 89.2 % |
| 74 | Role (multiple possible) | | |
| | • *Security Analyst* | 53 | 71.6 % |
| | • *Intelligence Analyst* | 25 | 33.8 % |
| | • *Malware Researcher* | 14 | 18.9 % |
| | • *Risk Analyst* | 13 | 17.6 % |
| | • *Law Enforcement* | 3 | 4.1 % |
| | • *Academic Researcher* | 3 | 4.1 % |
| | • *Fraud Analyst* | 2 | 2.7 % |
| | • *Other* | 5 | 6.7 % |
| 74 | Industry (multiple possible) | | |
| | • *ICT Consulting/Advisory* | 20 | 27.0 % |
| | • *National or Governmental CSIRT* | 12 | 16.2 % |
| | • *Telecommunications* | 9 | 12.2 % |
| | • *Bank* | 8 | 10.8 % |
| | • *Software company* | 7 | 9.5 % |
| | • *Public Health* | 6 | 8.1 % |
| | • *Military* | 3 | 4.1 % |
| | • *Other* | 12 | 16.2 % |
| 74 | Prior experience with MISP | | |
| | • *I have never used MISP before* | 18 | 24.3 % |
| | • *Less than 1 month* | 11 | 14.9 % |
| | • *1 – 6 months* | 18 | 24.3 % |
| | • *6 – 12 months* | 10 | 13.5 % |
| | • *1 – 2 years* | 6 | 8.1 % |
| | • *More than 2 years* | 11 | 14.9 % |

| N | Demographic | Count | Percent |
|---|---|---|---|
| 52 | MISP usage frequency | | |
| | • *Less than once a week* | 11 | 21.2 % |
| | • *Between 1 and 3 times per week* | 19 | 36.5 % |
| | • *Between 3 times per week & every day* | 11 | 21.2 % |
| | • *Every day* | 11 | 21.2 % |
| 74 | Previously attended a MISP training | 13 | 17.6 % |
| 74 | Previously used MISP training materials | 33 | 44.6 % |
| 74 | Previously used MISP virtual machines | 33 | 44.6 % |
| 50 | Previously used PyMISP | 15 | 30.0 % |
| 50 | Previously cloned a MISP repository | 21 | 42.0 % |
| 50 | Previously contributed to a repository | 9 | 18.0 % |

**Table 3.1:** Participant demographics

There were 32 participants (43%) in the age span of 26 – 35 years, and the second largest age group consisted of 27 participants (37%) in the range 36 – 45. In terms of prior experience with MISP, the largest subgroups consisted of those that had never used MISP before their training session and those that had used MISP between 1 – 6 months, which in both cases was 24%. Less than 25% of the participants had used MISP for more than 12 months.

28 participants (38%) saw themselves as having more than one role, with *Security Analyst* being the most frequent role indicated by 53 participants (72%). The most represented group in terms of industry was *ICT Consulting/Advisory* with 20 participants (27%).

It was the first training session for 61 attendees (82%), and 45% of our participants indicated that they had used the training materials and MISP virtual machine before. 30% indicated that they had used the PyMISP API before, 42% had cloned a MISP repository, whereas 18% had contributed to any of the MISP repositories.

### 3.5.2 Quantitative section (UEQ)

All responses were collected for preparatory coding and analysis using the UEQ data analysis tool (ver. 8) [348] and with the statistical software SPSS. Inconsistent responses were identified and removed whenever more than 3 subscales contained inconsistent response patterns, leading to 74 responses available for further analysis.

Data grouping. To investigate the possibility of grouping our responses from the four studies into a single data set, we performed tests of homogeneity of variance, and an ANOVA

with post hoc tests using bootstrapping of 1,000 samples to determine any statistically significant differences between the means of the 6 UEQ scales from our four studies. This led to the exclusion of the 10 responses from Study 2. No statistically significant differences were obtained for Studies 1, 3 and 4, which we grouped for subsequent analyses.

### UEQ Results

The following subsection provides the main results of the combined UEQ analysis for Studies 1 (#TR), 3 (#BM) and 4 (#LT).

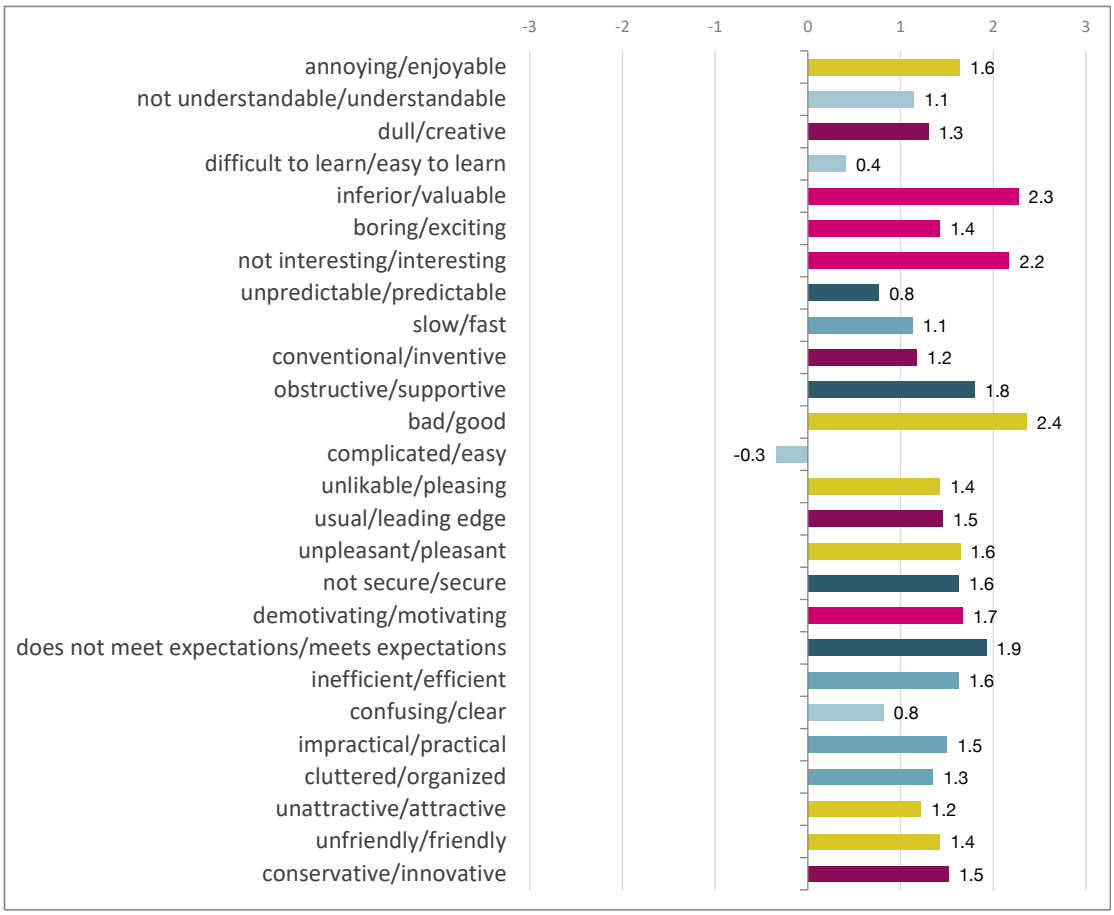
Table 3.2 and Figure 3.2a show the mean values per individual UEQ item.

| Item | Mean | Var | STD | No. | Left | Right | Scale |
|---|---|---|---|---|---|---|---|
| 1 | 1.6 | 1.2 | 1.1 | 63 | annoying | enjoyable | Attractiveness |
| 2 | 1.1 | 1.6 | 1.3 | 63 | not understandable | understandable | Perspicuity |
| 3 | 1.3 | 1.7 | 1.3 | 64 | creative | dull | Novelty |
| 4 | 0.4 | 2.1 | 1.4 | 64 | easy to learn | difficult to learn | Perspicuity |
| 5 | 2.3 | 0.9 | 1.0 | 63 | valuable | inferior | Stimulation |
| 6 | 1.4 | 1.2 | 1.1 | 64 | boring | exciting | Stimulation |
| 7 | 2.2 | 0.7 | 0.9 | 64 | not interesting | interesting | Stimulation |
| 8 | 0.8 | 1.2 | 1.1 | 64 | unpredictable | predictable | Dependability |
| 9 | 1.1 | 1.4 | 1.2 | 64 | fast | slow | Efficiency |
| 10 | 1.2 | 1.0 | 1.0 | 64 | inventive | conventional | Novelty |
| 11 | 1.8 | 0.7 | 0.8 | 64 | obstructive | supportive | Dependability |
| 12 | 2.4 | 0.7 | 0.9 | 64 | good | bad | Attractiveness |
| 13 | -0.3 | 1.9 | 1.4 | 64 | complicated | easy | Perspicuity |
| 14 | 1.4 | 0.8 | 0.9 | 64 | unlikable | pleasing | Attractiveness |
| 15 | 1.5 | 1.1 | 1.1 | 64 | usual | leading edge | Novelty |
| 16 | 1.6 | 0.9 | 0.9 | 64 | unpleasant | pleasant | Attractiveness |
| 17 | 1.6 | 1.0 | 1.0 | 64 | secure | not secure | Dependability |
| 18 | 1.7 | 0.9 | 1.0 | 63 | motivating | demotivating | Stimulation |
| 19 | 1.9 | 0.6 | 0.7 | 63 | meets expectations | does not meet expectations | Dependability |
| 20 | 1.6 | 1.1 | 1.0 | 64 | inefficient | efficient | Efficiency |
| 21 | 0.8 | 2.1 | 1.4 | 64 | clear | confusing | Perspicuity |
| 22 | 1.5 | 1.4 | 1.2 | 64 | impractical | practical | Efficiency |
| 23 | 1.3 | 2.1 | 1.4 | 63 | organized | cluttered | Efficiency |
| 24 | 1.2 | 2.6 | 1.6 | 64 | attractive | unattractive | Attractiveness |
| 25 | 1.4 | 2.1 | 1.4 | 64 | friendly | unfriendly | Attractiveness |
| 26 | 1.5 | 1.3 | 1.2 | 64 | conservative | innovative | Novelty |

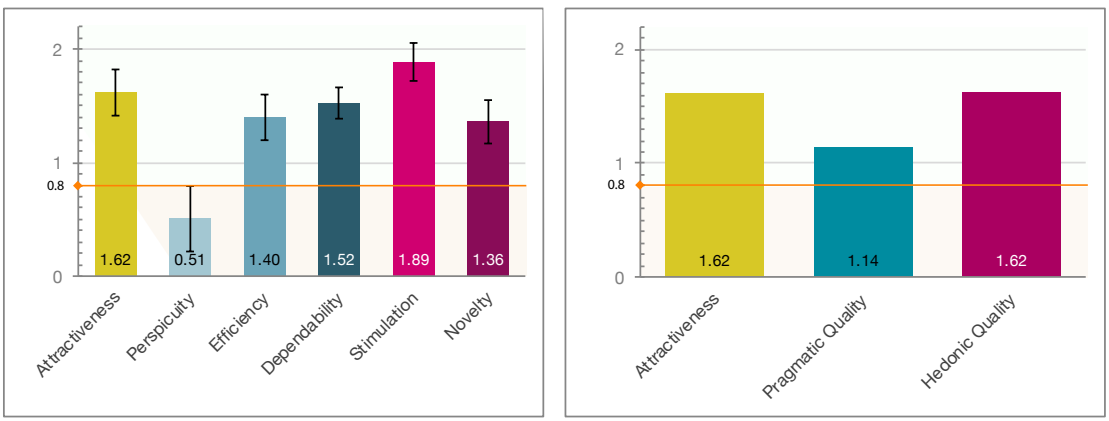
**Table 3.2:** Overview of the UEQ evaluation of MISP, mean values per scale item

The mean values per UEQ scale can be found in Figure 3.2b & Table 3.3.

According to the standard interpretation of the UEQ, values for the scale means that are $<$ -0.8 represent a negative evaluation, values in the range -0.8 to 0.8 represent a neutral




**(a)** Mean values per scale item




**(b)** Mean values per scale (left) and quality (right)

**Figure 3.2:** Main results of the UEQ evaluation of MISP.

| Scale | Evaluation | Mean | Std. Dev. | MoE | 5% CI |
|---|---|---|---|---|---|
| Attractiveness | Positive | 1.62 | 0.83 | 0.203 | [1.41, 1.82] |
| Perspicuity | Neutral | 0.51 | 1.18 | 0.288 | [0.21, 0.79] |
| Efficiency | Positive | 1.40 | 0.82 | 0.201 | [1.20, 1.60] |
| Dependability | Positive | 1.52 | 0.56 | 0.138 | [1.39, 1.66] |
| Stimulation | Positive | 1.89 | 0.68 | 0.167 | [1.72, 2.05] |
| Novelty | Positive | 1.36 | 0.78 | 0.191 | [1.17, 1.55] |

**Table 3.3:** Main UEQ results. Mean values per scale. N = 64.

evaluation, and values $> 0.8$ represent a positive evaluation. Our results denote an overall *positive* evaluation of MISP across all scales, except for *Perspicuity* where the scale mean belongs to the range -0.8 to 0.8, thus evaluated as *neutral*.

BENCHMARK COMPARISON. As this is the first study of its kind, there is no baseline to qualify the observed measurements within the CTI sharing context. However, these results can be compared to other studies that deploy the UEQ.

Setting the measured scale means from Table 3.3 in relation to a benchmark dataset that contains evaluations from 20,190 persons across 452 studies (as per version 8 of the UEQ handbook and data analysis tools [302]), we can estimate the relative UX quality of MISP compared to other systems. Table 3.4 & Figure 3.3a provide a comparison to the general benchmark consisting of the whole data set, whereas Table 3.5 & Figure 3.3b show the comparison against a specialized benchmark of 85 product evaluations of websites and web services.

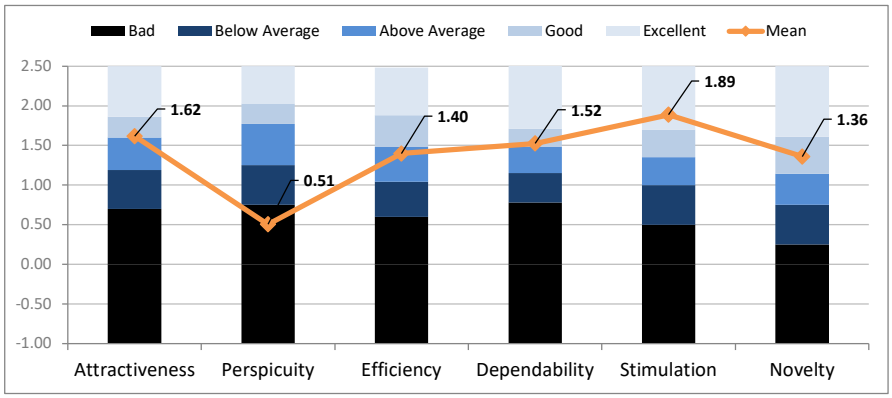
| Scale | Mean | Comparison to a general benchmark | Interpretation |
|---|---|---|---|
| Attractiveness | 1.62 | Good | 10% of results better, 75% of results worse |
| Perspicuity | 0.51 | Bad | In the range of the 25% worst results |
| Efficiency | 1.40 | Above average | 25% of results better, 50% of results worse |
| Dependability | 1.52 | Good | 10% of results better, 75% of results worse |
| Stimulation | 1.89 | Excellent | In the range of the 10% best results |
| Novelty | 1.36 | Good | 10% of results better, 75% of results worse |

**Table 3.4:** Comparison of the MISP results to a general UEQ benchmark (452 product evaluations)

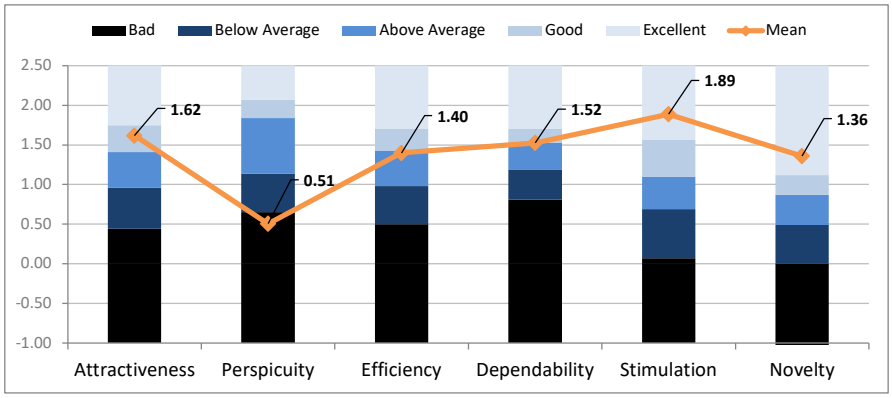
In both cases, MISP's *perspicuity* is categorized as *bad* i.e., among the 25% worst results. This is in contrast to the other scales, which are categorized at least as *above average*. In

| Scale | Mean | Comparison to a specialized benchmark | Interpretation |
|---|---|---|---|
| Attractiveness | 1.62 | Good | 10% of results better, 75% of results worse |
| Perspicuity | 0.51 | Bad | In the range of the 25% worst results |
| Efficiency | 1.40 | Above average | 25% of results better, 50% of results worse |
| Dependability | 1.52 | Above average | 25% of results better, 50% of results worse |
| Stimulation | 1.89 | Excellent | In the range of the 10% best results |
| Novelty | 1.36 | Excellent | In the range of the 10% best results |

**Table 3.5:** Comparison of the MISP results to a UEQ benchmark of websites and web services (85 product evaluations)




**(a)** Comparison to a general benchmark.




**(b)** Comparison to a specialized benchmark of websites and web services.

**Figure 3.3:** Comparison to benchmark values from UEQ evaluations of other systems.

both comparisons, the hedonic aspects are evaluated higher than in 75% of the investigated products, with *stimulation* categorized as *excellent* i.e., in the range of the 10% best results.

DEMOGRAPHIC DIFFERENCES. In order to investigate differences in the evaluation of MISP based on distinct participant profiles and characteristics, we performed a number of group comparisons, splitting our sample along the following dimensions: *age*, *education*, *role*, *industry*, *experience*, *frequency of use of MISP*, *use of training materials*, *use of MISP virtual machines*, *use of PyMISP*, and *cloning a MISP repo*. The statistical tests and results are reported next, which we discuss further in Section 3.6.

**Role.** A statistically significant difference in the UEQ evaluation of MISP was observed in the *Dependability* and *Stimulation* scales between users that reported multiple roles and users that reported a single role in terms of how they (intend to) use MISP.

Dependability: $(M_{mul} - M_{sin}) = 1.80 - 1.40 = 0.40$, 95% CI [0.11, 0.69], $d = 0.75$, 95% CI [0.20, 1.29]; $t(62) = 2.78$, $p = .007$.

Stimulation: $(M_{mul} - M_{sin}) = 2.19 - 1.75 = 0.44$, 95% CI [0.08, 0.79], $d = 0.67$, 95% CI [0.12, 1.21]; $t(62) = 2.47$, $p = .016$.

**Industry.** Participants who indicated working for an ICT consulting/advisory company, expressed significantly lower UEQ scores regarding the platform's *Attractiveness*, *Perspicuity*, and *Efficiency* in comparison to those working in other industries.

Attractiveness: $(M_{cons} - M_{oth}) = 1.20 - 1.77 = -0.57$, 95% CI [-1.02, -0.12], $d = -0.72$, 95% CI [-1.29, -0.15]; $t(62) = -2.54$, $p = .013$.

Perspicuity: $(M_{cons} - M_{oth}) = -0.13 - 0.74 = -0.87$, 95% CI [-1.50, -0.23], $d = -0.78$, 95% CI [-1.34, -0.20]; $t(62) = -2.74$, $p = .008$.

Efficiency: $(M_{cons} - M_{oth}) = 0.853 - 1.596 = -0.74$, 95% CI [-1.17, -0.31], $d = -0.98$, 95% CI [-1.56, -0.40]; $t(62) = -3.47$, $p = .001$.

**Experience.** The planned contrast between study participants that had used MISP for less than one year (*novice* users) and those that had used MISP for more than one year (*experienced* users) suggests that the latter group finds MISP more *stimulating*.

$(M_{exp} - M_{nov}) = 2.3 - 1.81 = 0.49$, 95% CI [0.02, 0.96], $d = 0.73$, 95% CI [0.35, 1.42]; $t(58) = 2.105$, $p = .04$.

**Use of Training materials.** The platform's *dependability* and *stimulation* were the two UX aspects evaluated significantly higher among participants that had used the MISP training materials before in comparison to those that had never used them.

Dependability: $(M_{yes} - M_{no}) = 1.78 - 1.37 = 0.41$, 95% CI [0.14, 0.68], $d = 0.78$, 95% CI [0.25, 1.30]; $t(62) = 3.001$, $p = .004$.

Stimulation: $(M_{yes} - M_{no}) = 2.21 - 1.69 = 0.51$, 95% CI [0.18, 0.84], $d = 0.80$, 95% CI [0.28, 1.33]; $t(62) = 3.114$, $p = .003$.

**Use of PyMISP.** The planned contrast between study participants that had used the PyMISP API and those that had not, revealed a statistically significant difference regard-

ing three UX aspects. The results denote that participants with PyMISP experience gave lower scores across all three aspects, namely:

Attractiveness: $(M_{yes} - M_{no}) = 1.09 - 1.77 = -0.68$, 95% CI [-1.31, -0.05], $d = -0.83$, 95% CI [-1.6, -0.06]; $t(38) = -2.191$, $p = .035$.

Efficiency: $(M_{yes} - M_{no}) = 0.86 - 1.52 = 0.66$, 95% CI [-1.21, -0.10], $d = -0.90$, 95% CI [-1.67, -0.13]; $t(38) = -2.384$, $p = .022$.

Novelty: $(M_{yes} - M_{no}) = 0.72 - 1.48 = -0.75$, 95% CI [-1.30, -0.21], $d = -1.07$, 95% CI [-1.84, -0.28]; $t(38) = -2.816$, $p = .008$.

**Cloning a MISP repo.** The planned contrast between study participants that had cloned a MISP repository and those that had not, revealed a statistically significant difference in the evaluation of the platform's *dependability*.

Dependability: $(M_{yes} - M_{no}) = 1.73 - 1.37 = 0.36$, 95% CI [0.01, 0.70], $d = 0.71$, 95% CI [0.26, 1.39]; $t(38) = 2.107$, $p = .042$.

No statistically significant differences were observed following planned contrasts between participants split according to the following characteristics: age, education, frequency of use of MISP, and use of the MISP virtual machines.

### 3.5.3 Qualitative section (SC)

| **Sentence stems** | **Responses** | **No answer** |
|---|---|---|
| S1: *When I use MISP, I feel ...* | 29 (69%) | 13 (31%) |
| S2: *MISP is best for ...* | 29 (69%) | 13 (31%) |
| S3: *MISP is not suitable for ...* | 19 (45%) | 23 (55%) |
| S4: *I think the appearance of MISP is ...* | 31 (74%) | 11 (26%) |
| S5: *I am happy with MISP because ...* | 32 (76%) | 10 (24%) |
| S6: *The problem with MISP is ...* | 27 (64%) | 15 (36%) |
| S7: *People who use MISP are typically ...* | 20 (48%) | 22 (52%) |
| S8: *Compared to other threat information sharing platforms, MISP is ...* | 24 (57%) | 18 (43%) |
| **Total:** | **211 (63%)** | **125 (37%)** |

**Table 3.6:** Overview of Sentence completion stems and corresponding response rates *(N=42)*.

As visible in Table 3.6, across the two sessions where the sentence completion activity was administered, 42 participants completed 211 out of possible 336 sentence stems (63%). In our analysis, we used a theoretically-driven inductive approach [335], in which, the coding system was generated inductively, but we drew from the theoretical perspectives of psy-

| **Themes** | **Theme frequency per sentence stem** | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | S1 | S2 | S3 | S4 | S5 | S6 | S7 | S8 | T |
| **User-related aspects** | | | | | | | | | |
| Needs and values | 9 | 0 | 0 | 0 | 11 | 2 | 4 | 6 | **32** |
| Emotion evocation | 34 | 2 | 0 | 4 | 1 | 3 | 0 | 0 | **44** |
| - *Positive emotions* | *22* | *2* | *0* | *0* | *0* | *2* | *0* | *0* | *26* |
| - *Negative emotions* | *12* | *0* | *0* | *4* | *1* | *1* | *0* | *0* | *18* |
| User characteristics | 0 | 1 | 7 | 1 | 0 | 6 | 13 | 0 | **28** |
| **System-related aspects** | | | | | | | | | |
| MISP characteristics | 1 | 0 | 0 | 0 | 12 | 6 | 1 | 7 | **27** |
| UX qualities | 16 | 34 | 12 | 39 | 31 | 25 | 2 | 21 | **180** |
| - *Attractiveness* | *0* | *0* | *0* | *16* | *0* | *0* | *0* | *6* | *22* |
| - *Lack of attractiveness* | *0* | *0* | *0* | *5* | *0* | *2* | *0* | *0* | *7* |
| - *Pragmatic qualities* | *3* | *34* | *0* | *7* | *29* | *0* | *2* | *10* | *85* |
| - *Lack of pragmatic qualities* | *10* | *0* | *12* | *7* | *0* | *23* | *0* | *0* | *52* |
| - *Hedonic qualities* | *3* | *0* | *0* | *0* | *2* | *0* | *0* | *5* | *10* |
| - *Lack of hedonic qualities* | *0* | *0* | *0* | *4* | *0* | *0* | *0* | *0* | *4* |

**Table 3.7:** Overview of the most frequent themes emerging from the data during the qualitative analysis.

chological needs [309], positive and negative emotions [264], as well as UX [166], when identifying and naming themes.

The thematically-driven stems were used as a guide for the creation of first level codes (user-related and system-related aspects) by which to assign all participant input. Inductive coding was then used to produce second level codes and to draw further insights on the guiding research questions. Preliminary coding from one session was undertaken by the lead researcher. This was then independently verified by a second researcher, so as to ensure consensus across the identified coding categories, and to drive discussion and further refining where coding disagreements arose. The rest was then coded by the lead researcher, in consultation where necessary. Table 3.7 outlines the main themes identified per SC stem.

#### USER-RELATED ASPECTS

NEEDS AND VALUES. As a major source of positive UX, the following themes were voiced as dominant psychological needs and values accounted for by MISP: *competence*, *control*, *autonomy*, and in particular, *relatedness*.

As exemplified by the following verbatims, users feel capable and effective in their work, they value that MISP supports their routines and habits, as well as their control over options.

**S1** "*When I use MISP, I feel confident about my ability to find bad guys*" (BM11)

**S5** "*... its flexibility allows me to solve my problems and I do not have to change my way of working*" (BM18)

The support in fulfilling the psychological need of *relatedness / belongingness* was raised most often, suggesting that MISP is perceived particularly well along its core objective of connecting parties interested in CTI sharing.

**S1** "*... I feel I'm part of a community*" (LT19)

**S5** "*I am happy with MISP because I'm a part of a community, I can help people like me*" (BM9)

**S5** "*... its aim is to promote sharing (cyber information); it includes a lot of users/contributors*" (LT28)

**S5** "*... it is a community-based sharing platform*" (BM10)

EVOCATION OF EMOTIONS. Besides need-related aspects, participants also expressed their emotional experiences with MISP.

Overall, positive emotions dominated, with *satisfaction*, *confidence*, *pride*, and *courage* being most reported.

**S1** "*When I use MISP, I feel like a genius*" (LT16)

**S2** "*MISP is best for people who aren't afraid of digging through Github issues as a suppliment [sic] to the documentation*" (BM14)

On the other hand, *confusion* was denoted as the most prominent negative emotion evoked, as hinted by these verbatims.

**S1** "*When I use MISP, I feel overwhelmed with the amount and type of data*" (BM12)

**S4** "*I think the appearance of MISP is causing confusion*" (BM10)

**S6** "*The problem with MISP is its integration, this is confusing for me*" (LT27)

Some participants highlighted *boredom* as well as *frustration*.

**S1** "*When I use MISP, I feel a bit lost, need to search a lot to find what I need*" (BM7)

USER CHARACTERISTICS. Another significant portion of user-related codes focused on the profile and characteristics of users, in particular the role of technical expertise and experience with MISP and CTI sharing in general.

**S7** "*People who use MISP are typically experts on security*" (LT11)

**S3** "*MISP is not suitable for non techies*" (BM11)

**S3** "*... not suitable for quick ad-hoc analysis by non IT professionals*" (LT25)

**S3** "*... not suitable for inactive organizations/users*" (LT22)

The opportunity to address an unmet user need of *relatedness* can be identified through the following statement.

**S6** "*The problem with MISP is lack of a public community that new users can join when starting out*" (LT3)

#### SYSTEM-RELATED ASPECTS

MISP CHARACTERISTICS. A number of SC stems triggered participants to express what system characteristics they value. Participants had a particularly high opinion of MISP's *freeness* and *openness*.

**S5** "*I am happy with MISP because it is open (source)*" (LT30)

**S5** "*... has potential to integrate with other tools and is open-source*" (LT16)

**S8** "*Compared to other TI sharing platforms, MISP is free, open-source and not managed by big companies*" (BM20)

**S8** "*... far more open*" (LT19)

MISP's *adaptation* properties were also much appreciated.

**S5** "*I am happy with MISP because it just works 95% of the time and it's enormously flexible as a tool*" (BM14)

**S5** "*... can be used in different ways*" (LT31)

UX QUALITIES. The largest proportion of user inputs described UX qualities (or lack thereof) grouped along three main dimensions.

I) ATTRACTIVENESS. Our participants did not provide a homogeneous response regarding the *attractiveness* of MISP, in particular the *aesthetics* of the platform, as evident by these opposing verbatims.

**S4** "*I think the appearance of MISP is quite pleasing*" (BM7)

**S4** "*I think the appearance of MISP is very good*" (LT27)

**S4** "*the appearance of MISP [is] has room for improvement*" (BM18)

**S6** "*The problem with MISP is [its] look and feel*" (LT19)

II) PRAGMATIC ASPECTS. The ability for MISP to support the effective and efficient achievement of CTI tasks i.e., the *instrumental* quality of the platform was the most frequent theme in our data. MISP was perceived as useful along both utility and usability dimensions.

**S5** "*... it has a lot of features*" (LT6)

**S8** "*...well-maintained and good feature set*" (LT16)

**S8** "*...complete, simple and free*" (LT16)

Participant statements reveal how MISP supports them in *searching*, *organizing*, *correlating* and *contextualizing* indicators of compromise (IoCs) and other CTI data.

**S5** "*... the API allows easy access to filter the data needed*" (BM12)

**S2** "*MISP is best for analysing and validating security incidents*" (LT7)

**S2** "*MISP is best for identifying events, their sources, and their attributes*" (LT7)

The core functionality of *collaboration* and *sharing* (technical) threat intelligence was particularly emphasized.

**S5** "*I am happy with MISP because it allows actionable information sharing*" (LT12)

**S2** "*MISP is best for exchanging IOC*" (LT13)

**S2** "*MISP is best for documenting malware and incidents and sharing that information*" (LT12)

**S2** "*MISP is best for having a centralized place to store and collaborate on data*" (LT8)

Participants did, however, also raise a number of pragmatic issues. On the utilitarian side, these ranged from the lack of applicability in certain sectors to the lack of suitability for specific CTI workflows.

**S6** "*The problem with MISP is it is too IOC-centered / IOC-oriented*" (BM2)

**S3** "*MISP is not suitable for long term analysis or assessment*" (LT3)

**S3** "*... not suitable for use out of the box (complex, needs deep integration into workflow)*" (LT30)

**S3** "*... not suitable for full IR management process*" (LT8)

As regards usability, which was much more commented, participants emphasized the *lack of clarity and efficiency* as well as the *complexity*, or more generally the *lack of perspicuity*, of MISP.

**S4** "*I think the appearance of MISP is chaotic at times*" (BM6)

**S6** "*The problem with MISP is it that it requires too much time*" (LT13)

**S6** "*The problem with MISP is finding the balance between good enough information and time invested*" (LT12)

**S6** "*The problem [...] is many tools/features (good problem)*" (LT9)

The *lack of learnability* and difficulty to cut through the complexity of MISP was a major concern:

**S6** "*...that is huge and kind of hard to start with* " (LT11)

**S6** "*...it has a steep learning curve*" (LT16)

**S4** "*...needs to be explained to be more used*" (LT28)

**S6** "*...it is hard to get started adding events if you never saw an example*" (LT6)

III) HEDONIC ASPECTS. While less frequent, users also mentioned hedonic aspects related to their experience with MISP, in particular, *novelty* and *stimulation*, or lack thereof.

**S4** "*... good, but a little old fashioned*" (BM9)

**S8** "*Compared to other threat information sharing platforms, MISP is a breath of fresh air*" (BM14)

**S5** "*I am happy with MISP because it is an awesome tool*" (LT27)

### Summary of key findings

The UEQ scores from Section 3.5.2 show an overall positive UX evaluation across the three main system quality aspects i.e., *attractiveness*, *pragmatic* and *hedonic* qualities. This finding is arguably not unexpected, as it would be challenging for MISP to achieve such widespread utilization if its UX was largely perceived as negative. At the same time, we cannot exclude the possibility that the obtained results are skewed towards more positive as the majority of our study participants were recruited around training events, which might imply active interest in the platform. Further, their level of experience both with the tool and in the industry may not fully reflect the body of actual users of MISP, potentially narrowing the scope of our findings.

Nevertheless, taking into account the shortage of security specialists [129], the high turnover rates among security analysts and their needs for adequate training [65], and the increased interest in CTI sharing beyond the security community, we can assume that the number of users who experience the system for the first time or are still novice is not insignificant. Understanding their UX needs and challenges is crucial to fully onboarding them as adopters who are confidently participating in CTI exchange. In this regard our research brings greater granularity and clarity regarding the different aspects that impact the experience.

The lower mean value for the *pragmatic* quality (1.14) is mainly due to the low *perspicuity* evaluation of MISP (0.51). One should not directly conclude, however, that MISP has a low utilitarian value. The qualitative insights obtained using the SC method (Section 3.5.3), provide further understandings behind the quantitative ratings of the UEQ. Furthermore, investigating the UX more holistically, rather than solely through a usability-focused prism (as discussed later), allowed us to capture user needs more comprehensively.

The results presented earlier point to the complex relationship many users have with MISP. On the one hand, the platform is praised for being useful, valuable, and empowering, on the other hand, it is also perceived as overwhelming. As regards the threat intelligence aspect of the system, users value the flexibility and adaptation offered by MISP. Nonetheless, they express concerns about the difficulty to learn the system and its complexity. Our results also highlight the importance of the user community, which in the case of MISP strongly values the openness, open-source nature of the platform and contributors. However, our findings also suggest that there might be a gap to be bridged among novice users until they feel onboarded. Furthermore, the SC responses indicate that the platform is very much technology-oriented, which might be a negative association for certain beginners or non-technical users that MISP attempts to onboard in different verticals or areas of interest (e.g.,

COVID research, misinformation etc.).

Our findings are of relevance beyond MISP. As reported in literature, many approaches to user-centered design rely on measures of the quality of interactive systems, such as benchmarking against usability measured for competitors' systems [173]. In this respect, similar investigations of other CTI platforms could estimate how those systems fare against MISP along the different UX dimensions. Further, many of the positive and negative accounts that our study participants reported transcend MISP as a system and relate to user needs that were either fulfilled or neglected. Thus, much can be learnt as to what users find important in this context and why, which can be of use to designers of other CTI sharing platforms as well as researchers of socio-technical security in general.

### Implications

The user concerns highlighted above, such as the complexity of the platform, the steep learning curve as well as the perceived lack of support or community for novice users, open potential problems both in terms of errors, as well as under-utilization i.e., adoption problems. Thus, designers of CTI sharing platforms should also take into account many of the base findings and assumptions coming from the field of computer-supported cooperative work (CSCW) [6], to narrow the gap between the social requirements and the technical feasibility in CTI exchange.

For instance, access control systems should accommodate the nuanced behavior that people have with respect to how and with whom they share information, their concerns about sharing specific pieces of information at a particular time, or the effects of information disclosure [6]. Awareness about who else is present in a "shared space" and allowing for low-level monitoring of others' activities as well as making information exchange visible is important both for guiding people's work and actions [112] as well as enabling learning and greater efficiencies [178]. However, making people's work visible may also open them to scrutiny or criticism, which can impact their willingness to share information [6].

Both of the afore-mentioned aspects are very important in particular for non-expert users. In this respect, MISP offers plenty of distribution options, meaning different pieces of information can reach different entities within the same and/or connected MISP instances. Furthermore, a *delegation* feature allows users to entrust another party on the MISP instance to share a CTI event and remove the binding between the information shared and the reporting organization. However, not knowing about these options due to the cognitive overload new users are faced with as they get started with MISP, or having a misperception about the core functioning of such a security system due to a poor UX, can have serious consequences.

To illustrate, even if a shared CTI event refers to indicators of compromise (IoCs) only, certain organizations might perceive the information as sensitive because its (premature) disclosure could impede a successful response to a cyber attack. Or it could be sensitive as the shared information might imply that the organization disclosing the event is a potential victim of a specific attack, which in itself can have negative reputation consequences. Thus, performing this core activity without knowing or disregarding who the (intended) recipients of the shared information are, can lead to both *oversharing* i.e., accidental leakage of sensitive information to parties beyond what was initially planned, as well as to *undersharing* i.e., to lower preparedness levels of the sharing community as vital pieces of information would not be reaching the other members. Both can play a role in the perception of the platform's efficiency, usefulness, and added value, ultimately impacting the future use and adoption, where no adoption equals to lower overall cyber preparedness and security.

#### Beyond usability

We can also pose the question: Why would someone start or continue using a certain CTI sharing platform even though it is hard to learn? Just as traditional models of rational choice disregard the numerous factors that impact actual privacy and security decision-making [7], so are narrow usability investigations unable to provide much insights in this direction. A typical usability study would normally focus on task-related efficiency and effectiveness, which would omit other equally important aspects that impact the overall impression, appeal and intention to use a system [167, 208, 391]. Our study shows that the psychological need of *relatedness / belongingness* [289] can play a key role here.

This is not to say that investigating pure functionality aspects is less important, especially in such an expert domain where *fun* is not the main design objective of the system. However, disregarding factors such as people's affective reactions before, during or after using a specific system, the emotional relationships they build with specific technology, or the fulfillment of psychological needs that can be mediated via technology, can pose major shortcomings during the design as well as evaluation stages of a system's lifecycle. Far too often, core security and privacy research takes an overly simplistic approach to investigating the human role or how to make systems usable. We hope that our study brings to the fore the importance of approaching UX in a holistic manner and that the deployed methods and approach taken can serve as a blueprint to the wider security community when investigating not only other CTI sharing platforms, but security tools and systems in general.

### Future Work

While we do not have compelling evidence of the relationship between the evaluation of MISP and the expertise level of the users, the results from Section 3.5.2 prod us to investigate whether users that, in one way or another, are more involved with the platform, are able to recognize more the different UX qualities in MISP. For instance, those that had used MISP in multiple roles, those that had used the system for more than one year, or those that had used the training materials, found MISP more *stimulating* to use. These assumptions and the other findings stemming from this baseline UX evaluation, would require further validation. To this end, replication studies are strongly encouraged.

More research in this field is needed not only to establish UX as a standard evaluation criteria when assessing different CTI sharing platforms, but also in terms of how UX design can help users cut through the complexity as they learn or use the system for different CTI activities. In light of the afore-mentioned adoption and security implications, future research questions could explore: *(i)* whether users have a correct understanding of how far CTI information travels when it is shared in a sharing platform like MISP; *(ii)* how users are supported in this core activity e.g., are there user interface mechanisms, supporting documentation, or is training required; *(iii)* how end-user feedback loops back to the designers of a CTI sharing platform and whose responsibility is the UX in open-source, community-driven projects like MISP.

Eliciting and incorporating representative views that reflect the different user groups of the platforms under investigation is of paramount importance. To this end, future work could also experiment with different user research methods and recruitment strategies as well as propose and explore how integrated avenues within the CTI sharing platforms themselves could seek to solicit UX feedback that could potentially reach a wider and more diverse user segment.

### Limitations

Our work comes with certain limitations that should be considered when interpreting the results and analysis of our study. Despite our best efforts to collect inputs from a larger sample of MISP users, we also experienced difficulties recruiting and getting access to larger numbers of participants from our target population. Thus, the given sample size, the profile of the participants, and the recruitment circumstances limit the generalizability of the different UX evaluations. Further, our sample was skewed towards novice users, who were mostly male and with a technical background. Thus, we risk omitting important underrepresented views.

As our study was conducted over a period of two years, different users were not working with exactly the same version of MISP, as it is a system that is in continuous development. Nevertheless, no radical changes were introduced to the system with respect to activities covered during the MISP training sessions.

Lastly, while we deployed standardized and validated methods for evaluating the UX, every context is specific and the methods are not a perfect fit for every situation [210]. For instance, we do not make a distinction between different components of MISP and consequently we do not know which aspect of the user interaction or experience was reported by the participants or dominated their evaluation. Similarly, it is hard to discern whether certain evaluations (e.g., stimulation) are restricted to MISP as a system or to the activity of CTI exchange via MISP more broadly.

## 3.7 Chapter Conclusion

The exchange of CTI is a crucial element in the fight against the increasing number and complexity of cyber attacks. To date, research in this field has mainly overlooked UX aspects, which are essential for the successful deployment and utilization of CTI sharing platforms. Through the use case of MISP, we highlighted what novice users perceive to be the strengths and weaknesses of a leading system of this kind. Furthermore, by specifying appropriate metrics and performing a benchmark UX evaluation of MISP, we not only aspired to contribute to the improvement in the quality of cybersecurity in real-world systems, but also to enrich the discourse on CTI sharing with new UX perspectives. These contributions provide much needed insights into an understudied facet of the CTI sharing problematic. Our study also demonstrated that many user and system-related needs can remain hidden unless we take an expanded notion of the UX and go beyond usability studies which look at task-related aspects only. This has implications beyond CTI, and should be taken into account in the investigations of security tools and systems in general.

We hope that the reported findings also help the designers and developers of other CTI platforms, who can take into account what users value about MISP and why, as well as how they could aim to overcome identified shortcomings from an aesthetic, pragmatic, or hedonic perspective. Through the presented methods and our accounts of conducting user research in this context, we also aim to inspire further studies, investigating both CTI sharing systems as well as different user groups. Further work is needed to incorporate additional views which we were unable to account for in this study, and to uncover a plethora of user related challenges and opportunities in the service of securing organizations and communities.

## 3.8 Chapter Appendix

The surveys and datasets with raw participant responses from the studies can be downloaded from the following link: https://doi.org/10.5281/zenodo.5531990 [326].

Supporting documents from this chapter are also provided in Appendix A.

*Prior to any perception there has to be*
*an openness for perceiving something.*

Dag Svanæs

# 4

# Analyzing user perceptions in CTI sharing platforms

CHAPTER ORGANIZATION. This chapter is organized in 6 sections. As a continuation of one future work direction outlined in Section 3.6, we first introduce the research challenge and questions addressed in this chapter. Next, we contextualize the problem within MISP and provide a brief description of how event representation and sharing is manifested in our use case CTI sharing platform. Then, we introduce our workflow and toolchain proposal for analyzing users' perceptions and discuss the potential benefits of our socio-technical approach as a tool for security analysis, simulation, or education/training support in the context of CTI exchange. We conclude with a brief outline of future work that would seek to evaluate and validate the proposed model.

## 4.1 INTRODUCTION

As elucidated in the previous chapter, cyber threat intelligence (CTI) sharing platforms are valuable tools in cybersecurity. Yet, despite the fact that effective CTI exchange highly depends on human aspects, cyber behavior in CTI sharing platforms has been notably less investigated by the security research community. In Chapter 3, we sought to gather insights on the overall UX, the enabling and constraining factors of security information sharing as well as how much effective CTI sharing could be impacted by usability problems or UX challenges. The focal point in this chapter is the extant knowledge gap regarding users' perceptions of key tasks pertaining to the consumption and use of cyber threat intel indicators, their organization and storing as well as their production and publishing.

While we find a number of questions around indicator prioritization such as the relative importance, perceived value, and actionability, worth exploring in this direction, in this chapter we focus on the related problem of understanding users' perceptions of the extent of information sharing in CTI sharing platforms. In other words, users' understanding of *how far* information (that is shared in a CTI platform) travels and whom does it reach.

#### Study Motivation

Having an accurate understanding of how far shared intel travels in a platform can help towards ensuring that the agreements and rules of the CTI sharing community are not violated. It can facilitate the prioritization of threat intel, and support the establishment of trust among the sharing community members. In particular, this is important to:

- avoid accidental leakage of sensitive information to entities beyond the intended recipients within a sharing community;
- avoid under-sharing i.e., to maximize the reach of shareable information with desired entities so that the members of the community can build a better situation awareness picture of the possible threats;

While not having accurate or even any knowledge about the underlying sharing mechanisms within a CTI sharing platform does not necessarily impede users to share threat intel per se, it can be problematic. Consequently, this chapter is motivated by the following research question:

RQ Do users of a CTI sharing platform have an accurate understanding of the extent of information sharing i.e., how far information travels when it is shared in a CTI sharing platform?

### Contributions

While we do not perform and report a user study, in this chapter we present a conceptual model of a workflow and toolchain, consisting of several *technical* and *social* components, that could be deployed to answer this question. An evaluation and validation of the proposed blueprint within a full-fledged user study is left for future work as discussed in Chapter 8. Nevertheless, we believe that the potential of this socio-technical approach can already be recognized as a useful complement to analysis, simulation, or education/training efforts in the CTI sharing domain.

The conceptual framework presented here and the one in Chapter 5 share the same inspiration. Both seek to detect misalignments between system states (or properties) and user perceptions. The intention could be, for instance, to identify situations where users might have a *false sense of security* or *a false sense of insecurity* which potentially impacts the secure use and UX of the deployed security or privacy-critical system.

In both the secure email setting (Chapter 5) and in the current CTI sharing context, the fundamental building blocks are the same. We need insights about both the technical aspects of a system and the users' perceptions, opinions or behavior, that we take in for a joint analysis with respect to a specific question.

Thus, in order to answer the above-stated research question, we need to obtain and compare *(i)* users' perceptions of how far information travels when shared in a CTI sharing platform, with *(ii)* the ground truth i.e., how far information travels in a CTI sharing platform in reality. This necessitates breaking down our motivating research question into the following two parts:

Q2 How can we obtain users' perception (i.e., understanding) about how far information travels when it is shared in a CTI sharing platform?

Q3 How can we obtain the ground truth i.e., how far information that is shared in a CTI sharing platform travels in reality?

In order to ground our theoretical concept within a practical CTI sharing setting, we demonstrate how the workflow and toolchain could look like within the same use case from Chapter 3 i.e., the leading CTI sharing platform MISP [363].

#### MISP Sharing and Event Representation

In Section 3.3, we introduced some of the core concepts behind the purpose and functioning of the MISP sharing platform. Next, we briefly restate and explain the main points related to CTI event representation and sharing in MISP.

The core functionality of MISP is to enable consumption and/or contribution of (cyber threat) information within a specific community of users. Thus, a MISP *instance* can be considered as an independent server (administered by a host organization) that facilitates this process among a defined set of participating organizations.

As depicted in Figure 4.1, MISP instances can be standalone or interconnected between each other using different synchronization mechanisms, allowing for shared information to flow between instances in one or both directions.

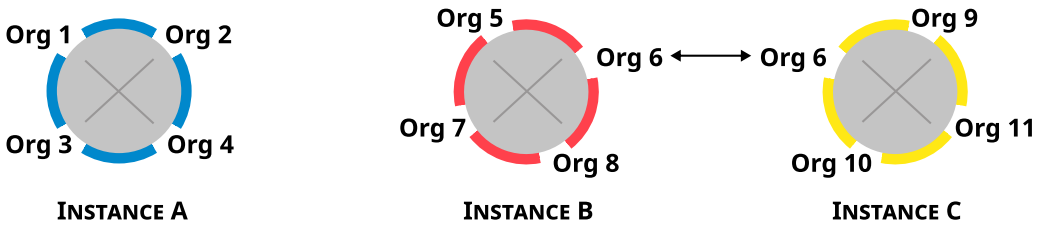



**Figure 4.1:** Abstract representation of information sharing in MISP: one standalone (A) and two connected MISP instances (B and C).

New data entries in MISP are called *event objects*, which can be described with different levels of granularity of information as per the user's wish [363]. Furthermore, the sharing model in MISP, which relies on voluntary action of its community to share information and indicators, allows those events to be shared under various scenarios [363]. More specifically, there are four sharing levels in MISP that dictate how shared CTI events will be distributed and displayed:

Organization only: the CTI event is displayed only to users that belong to the same organization on a MISP instance.

Community only: the CTI event is displayed only to users of organizations that are on the same MISP instance as well as organizations that run MISP instances which sync with the instance the event is shared from.

Connected communities: the CTI event is displayed to users of organizations that are on the same MISP instance as well as organizations on the instances which sync with the instance from which the event is shared. This also includes hosting organizations of instances that sync with connected instances.

All communities: the CTI event is displayed to all users of all organizations on directly and indirectly connected instances.

In addition, users can also choose to set the distribution setting to a *Sharing group*, which allows users to customize the list of organizations the event should reach or be visible to.

In terms of event representation in MISP, Figure 4.2 provides an abstract representation of an event and its optional sub-components. In the simplest form, we can think of an event as a construct that consists of core *data* and *metadata*, a *distribution* setting and a *published* status. It can also contain *attributes*, *objects*, and *attachments*, which in turn have *data*, *metadata*, and a *distribution* setting. Figure 4.3 shows how a hypothetical event might look like in MISP.

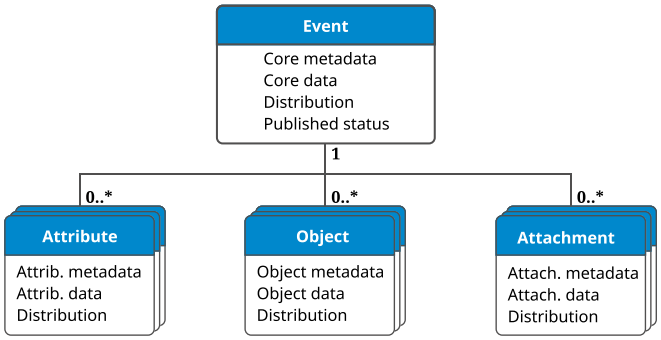



**Figure 4.2:** Abstract event representation in MISP.

| | | |
|---|---|---|
| **Event ID** | 82099038789 | |
| **UUID** | fkld933-930dk-2990392-928f39 | |
| **Creator org** | SnT | |
| **Creator user** | name.surname@uni.lu | |
| **Tags** | tlp:amber | Event core metadata |
| **Date** | 2021-01-28 | |
| **Analysis** | Initial | |
| **Threat level** | High | |
| **Info** | "Very important information" | Event core data |
| **Distribution** | This community only | Event distribution |
| **Published** | No | Event published status |
| | | |
| **#Attributes** | 1 (0 Objects) | |
| **Attribute date** | 2021-04-28 | |
| **Category** | External analysis | Attribute metadata |
| **Type** | attachment | |
| **Value** | file.txt | Attribute data |
| **Distribution** | All communities | Attribute distribution |

**Figure 4.3:** Hypothetical MISP event with only one attribute.

Depending on the published status and the different distribution settings provided for an event, its attributes, attachments, and/or objects, different pieces of information can reach (i.e., are visible to) different entities within the same and/or connected MISP instances. For instance, in Figure 4.4 one can see how that event distribution is restricted to the users belonging to the same organization only.

Some of the information in the event core, attachments, attributes, and/or objects may be sensitive, thus ensuring that it is not shared with specific entities, groups of entities or sharing communities is of paramount importance. To this end, we propose the conceptual framework depicted in Figure 4.5.

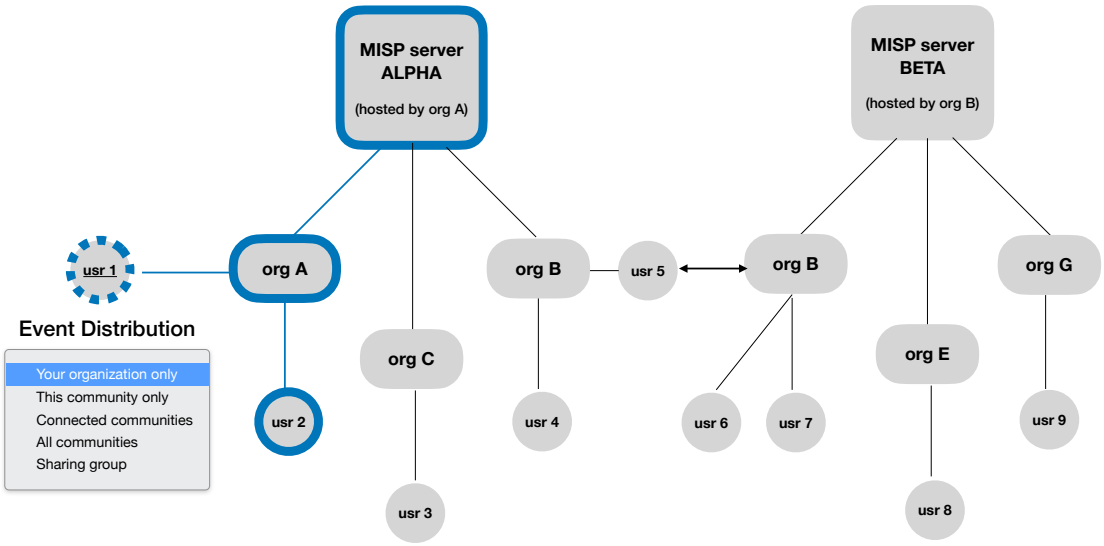



**Figure 4.4:** Event distribution example

## 4.3 Proposed Workflow and Toolchain

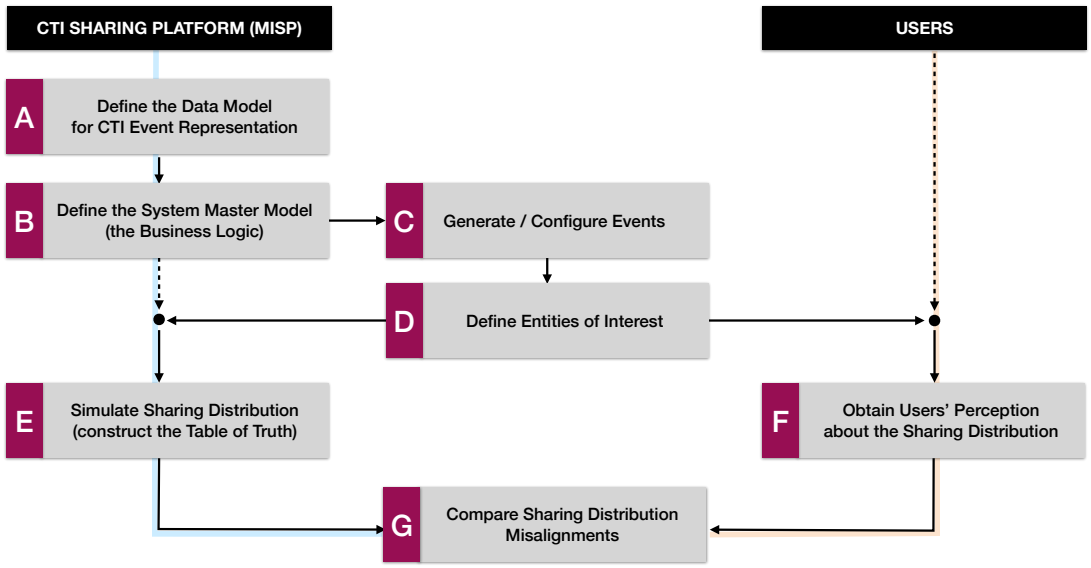



**Figure 4.5:** Workflow for analyzing users' perceptions in cyber threat intelligence sharing platforms

### 4.3.1 Definitions

The first step involves the definition or formalization of a data model for a simplified CTI event representation. Thus, events and their components, properties, and sharing in MISP, could be more formally expressed as follows.

### Distributions

$$D = \{d_1, ..., d_n\} \tag{4.1}$$

is a set of distribution options. For instance:

```
D = {All communities, This Community, Connected Communities,
    Sharing Group, Your organization, Inherit Event}
```

### Attributes

$$a = (data, metadata, distribution) \tag{4.2}$$

is an attribute that contains the *data* and related *metadata* that can be text, binaries, images, etc., and where *distribution* $\in D$.

$$A = \{a_1, ..., a_n\} \tag{4.3}$$

is a set of attributes, which can also be an empty set.

### Objects

$$o = (data, metadata, distribution) \tag{4.4}$$

is an object that contains the *data* and related *metadata* that can be text, binaries, images, etc., and where *distribution* $\in D$.

$$O = \{o_1, ..., o_n\} \tag{4.5}$$

is a set of objects, which can also be an empty set.

### Attachments

$$t = (data, metadata, distribution) \tag{4.6}$$

is an attachment that contains the *data* and related *metadata* that can be text, binaries, images, etc., and where *distribution* $\in D$.

$$T = \{t_1, ..., t_n\} \tag{4.7}$$

is a set of attachments, which can also be an empty set.

**Published status**

$$S = \{s_1, ..., s_n\} \tag{4.8}$$

is a set of statuses applicable for an event denoting whether an event has been published or not, and how. For example:

```
S = {Not published, Published, Published (no email)}
```

**Events**

$$e = (data, metadata, distribution, status, A, O, T) \tag{4.9}$$

is an event that consists of core information (i.e. the event *data* and *metadata* that can be text, binaries, images, etc.) with a *distribution* $\in D$, and a published *status* $\in S$. The event can containt zero or more *attributes* (each with individual distribution options), zero or more *objects* (each with individual distribution options), and zero or more *attachments* (each with individual distribution options).

$$E = \{e_1, ..., e_n\} \tag{4.10}$$

is a set of events, which can also be an empty set.

**Entities**

$$N = \{n_1, ..., n_n\} \tag{4.11}$$

is a set of entities i.e., organizations that are part of a sharing community.

**MISP instances**

$$m = \{admin, N, G, E, syncs\} \tag{4.12}$$

is an instance that consists of an *admin* organization that hosts and manages the instance, a set of *entities* N, a set of *sharing groups* G, a set of CTI *events* E, and a designated set of *synchronization users* that act as links with other instances.

$$M = \{m_1, ..., m_n\} \tag{4.13}$$

is a set of MISP instances.

### 4.3.2 System Master Model

While we could specify additional components depending on our research goals, the defined constructs above provide the underlying structure around which we can now build the rules, interaction and interdependency between the components. In other words, we can build the business logic of the CTI platform. Some examples of the business logic are:

- Every entity $n$ belongs to one MISP instance $m \in M$.
- There is a link between two entities $n_1$ and $n_2$ if and only if they belong to the same MISP instance $m$, or the MISP instance of $n_1$ e.g. $m_1$, is directly or indirectly connected to the MISP instance of $n_2$ e.g. $m_2$ via sync users.
- Data from entity $n_1$ can travel to entity $n_2$ if they are linked.
- Data from $n_1$ cannot travel to another entity if the event distribution setting is *This organization only*.

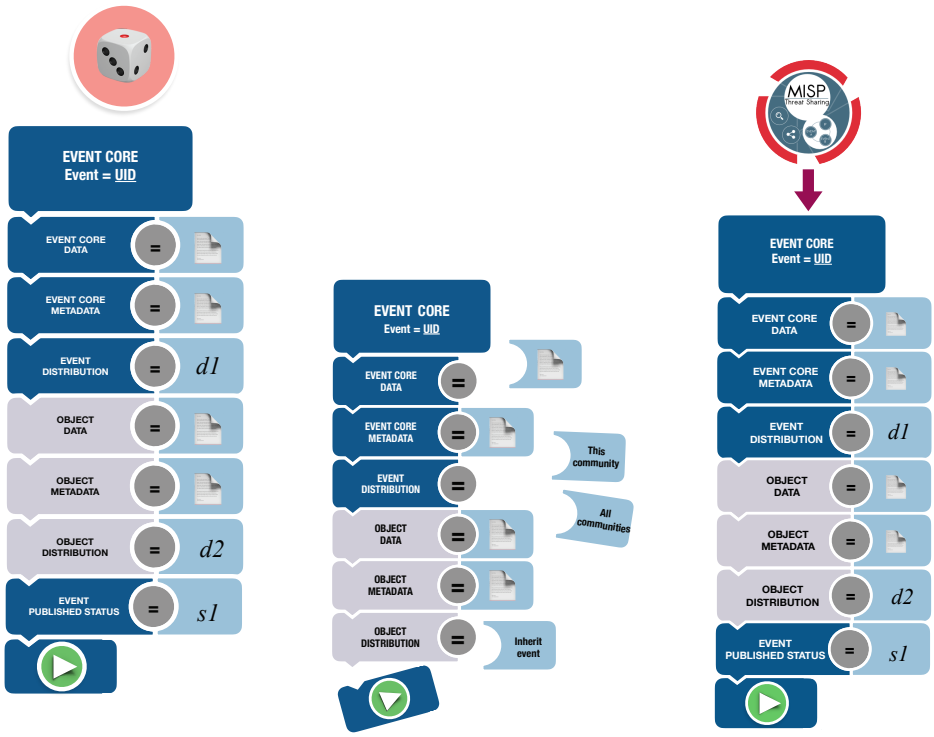
The above statements are only for illustration purposes as we do not provide an extensive specification nor a more formal representation here. Depending on the desired level of model replication of the CTI sharing platform, constructing the system master model can be a task of varying complexity and investment of resources. However, building the system master model is fundamentally related to Q3 i.e., once we have the necessary ingredients to construct the master model, we should know what happens to CTI information that is shared based on the business logic of the platform.

### 4.3.3 Event Generation and Configuration

Once the theoretical master model that defines how data is shared within and between MISP instances is complete, we can generate CTI events with different configurations in order to see the effects of the different distribution possibilities within the platform. We propose three modes of event generation i.e., configuration, as displayed in Figure 4.6.

#### Random Event Generator

"With a click of a button" the simulator generates a random event with a different number of attributes, objects, attachments, as well as settings e.g., a published status and different distributions. These are hypothetical, but valid combinations, representative of real MISP events.




**(a)** Random Event Generator

**(b)** Event Block Builder

**(c)** Replicator of existing events

**Figure 4.6:** Three proposed methods to generate or (re-)configure CTI events.

### Event Block Builder

Following the concept of drag-and-drop block programming we can construct a hypothetical event by combining the desired blocks, or simulating what-if scenarios by substituting targeted blocks which represent the different distribution and publishing settings. The detached example pieces in Figure 4.6b can be seen as interface components that allow for more controlled modifications to the event's configuration in comparison to the Random Event Generator.

### Replicator of existing CTI events

Existing events from MISP instances could be exported and automatically imported into the simulator in order to generate the *tables of truth* (described below) for real MISP events. Such events, could also be replicated manually using the Block Builder.

### 4.3.4 Entities of Interest

The next step involves the specification of entities relevant for our investigation. These can refer to the intended recipients of shared CTI information, or contrary, parties with which CTI should not be shared, thus the entities that might unintentionally have access to the shared data. For simplicity, we consider all data and metadata here to be sensitive or equally important and the overall purpose is to see who in the sharing community is able to see it i.e., who could it reach.

While one could aim to specify individual or very specific entities, the general application would be to analyze events against a bulk set of entities that share common characteristics e.g., organizations that are hosted on the same instance, organizations that are hosted on a connected instance, those in a specific sharing group, etc. These options should correspond to all valid distribution settings generated for the events and their subcomponents.

An investigation of specific entities, such as a particular organization, would require additional modeling or specification of the available entities and associations between them so that the system master model knows e.g., which organizations are hosted on the current MISP instance, which instances are connected to the current instance, etc.

### 4.3.5 Event Simulation

The next step is also linked to Q3 and involves the automatic generation of the *tables of truth* which represent the actual i.e., factual distribution of information from the technical perspective as defined by the business logic or system master model. Figure 4.7 displays an example table of truth generated for the hypothetical MISP event from Figure 4.3. It can be regarded as the output of a query sent to the system master model with the *generated event* and *entities of interest* as parameters to that query. The simulator output, thus, tells us how data is shared in MISP based on the distribution and publication settings defined for that event i.e., *which entities can see what information*?

The table of truth can be constructed either (i) *selectively*, focusing only on the set of entities $N$ that we are interested in, or alternatively, (ii) *exhaustively*, meaning all possible entities are considered, beyond the ones that we are interested in or that we had explicitely defined.

If we focus only on $N$, for each entity in the set, we can iteratively ask the simulator which data and metadata of $e$ and its components is it able to see. E.g.

- Can $n_k$ see $e.data$?
- Can $n_k$ see $e.metadata$?

- Can $n_k$ see $e.attribute1.data$?
- Can $n_k$ see $e.attribute1.metadata$?

We can similarly run queries for a bulk set of entities, e.g.:

- Can *other organizations on current instance* see $e.data$?

| | | | COMPONENT VISIBILITY BY ENTITY | | | |
|---|---|---|---|---|---|---|
| EVENT COMPONENTS | CTI Event | | Your organization on current MISP instance | Other organizations on current MISP instance | Other organizations on directly connected MISP instances | Other organizations on indirectly connected MISP instances |
| | Event Core Data | "Very important information" | ✔ | ✔ | ✗ | ✗ |
| | Event Core Metadata | ID, UUID, Creator org, Creator user, Tags, Date, | ✔ | ✔ | ✗ | ✗ |
| | Attribute Data | file.txt | ✔ | ✔ | ✗ | ✗ |
| | Attribute Metadata | Attribute date, Category, Type | ✔ | ✔ | ✗ | ✗ |

**Figure 4.7:** A *table of truth* indicates *which* entities can see *what* information. It is a summary of Y/N answers to queries about the CTI distribution specific to that event and entities of interest.

To illustrate, we can refer back to our hypothetical event from Figure 4.3. We can see that the distribution setting for the *event* is set to "This community only", while the distribution setting for its only *attribute* is set to "All communities". According to the MISP business logic, the most restrictive setting wins, thus the distribution of the event and its components is limited to "This community only". Furthermore, the event is not published which further limits propagation to directly connected instances via *pushing*. Even without an overview of specific entities and associations between them, the system master model is able to respond to the queries examplified earlier, and produce the appropriate *table of truth* in Figure 4.7.

Having obtained the *ground truth* i.e., the technical aspects necessary for our comparison, we can now focus on the second crucial component.

### 4.3.6 Obtaining users' perceptions

Numerous user research methods could be deployed to investigate Q2. Interviewing users, doing user observations or surveys could help us as a first step to understand how users learn about the sharing process in MISP. Is it via trial-and-error as they click through MISP or the numerous virtual machines made available for testing and training purposes? Do they read

the documentation? Do they use the visual aids and widget in the User Interface that is supposed to facilitate the understanding of sharing? Do they follow a training session?

Any insights gathered could be helpful in coming up with initial assumptions about users' perceptions that we would seek to validate in dedicated user studies. For instance, we could conduct a number of experiments wherein we could reuse the components from the previous steps. For a defined set of arbitrary events that have their unique components and distribution settings as well as a list of entities of interest relevant for the investigation, instead of running the simulator and queries, we could ask participants to tell us the extent of the data reach based on their understanding. Example prompt:

*"Please have a look at the following event, its components and distribution settings, and indicate which of the components can be seen by the entities listed in this table?"*

We can, thus, complete the table with user generated Y/N values similar to Figure 4.7 against which we are going to compare the values.

Depending on the study objective and format, such inquiries could take place in-situ while users are working on an actual MISP instance, or in an out of context investigation e.g., using a questionnaire administered online or paper-based.

### 4.3.7 Comparison

Having obtained both the table of user perceptions as well as the table of truth, we can perform an automatic check whether there are alignments or misalignments. This could be realized via direct comparisons of the outputs akin to software testing methods comparing expected vs observed values.

## 4.4 Discussion

### 4.4.1 Purpose

We see three main applications of such a socio-technical approach to comparing users' perceptions (the user generated table) of how far information travels when shared in MISP against what happens in reality (the table of truth).

**Security Analysis and Audit**

Our approach could assist organizations in the identification of specific misperceptions or misunderstandings among their staff members with respect to CTI sharing. For instance,

studies could show that users from Organization A predominantly share events with less entities than supposed to, whereas users from Organization B fail to realize that they are sharing beyond their community only. Once such misalignments are identified, a subsequent automated investigation could be performed to get an estimate of the exposure or extent of such already exchanged CTI. Under the assumption that we can easily feed into the Simulator specific MISP events of interest, an automated audit could quickly highlight all the *transactions* (i.e. exchanged events) where a misalignment regarding specific entities exists between how data was shared in reality and how we model the users' perception (even though we did not ask the users' input for that transaction specifically).

**Simulation**

As indicated earlier, such an approach could be a useful simulation tool for projecting and experimenting how CTI sharing could be impacted by tweaks to the numerous distribution options and settings on the event-level, object-level as well as attribute-level. While the security analysis/audit aspect of the tool is geared towards events that were already shared, the simulation aspect is geared towards minimizing the negative impact of sharing future CTI events with wrong or suboptimal distribution settings.

**Training**

In addition to simulating and generating the table of truth for a specific event & entities combination, a number of other tasks could be performed. For instance, the inverse. Participants could see a filled-out table of truth, and would be asked to (re)construct an event with a possible sharing configuration that will correspond/satisfy the table values. Furthermore, we could ask participants to construct an event and choose a sharing configuration where the objective would be, for instance, to allow the maximum reach of the data, while making sure that certain "sensitive data" is not shared beyond the instructions.

### 4.4.2 Other applications

We believe that in addition to the purposes of comparing users' perceptions to what happens in reality, as described above, the simulator could also be useful in the following scenarios:

- Verifying the correctness of the implementation in MISP i.e., checking whether information shared in MISP instances really matches the sharing specification of the theoretical model. Potential discrepancies could be investigated for implementation bugs and errors, adversarial manipulation, etc.

- Establishing the accuracy of the visual distribution graph / widget available in MISP that is supposed to facilitate users' understanding of the different distribution options when adding or editing events.

Figure 4.8 depicts the visual distribution graph for an event in MISP. Verifying the correctness would require additional experiments in a test-bed with connected MISP instances. Similarly, investigating the usability of the widget would be a separate user study.

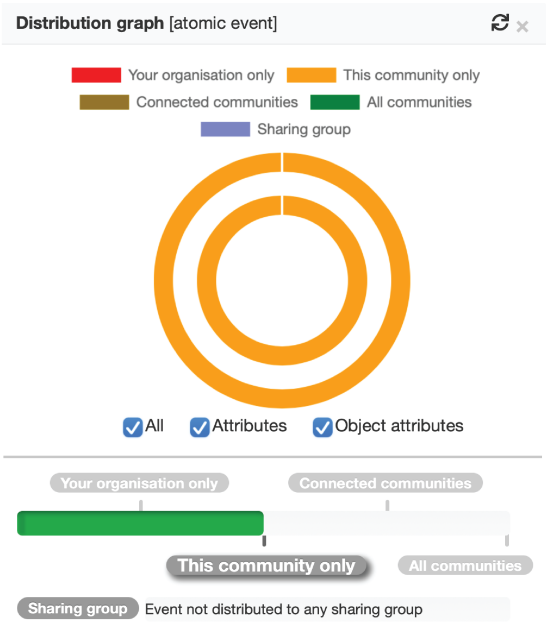



**Figure 4.8:** Visual distribution graph in MISP

## 4.5 Future Work

Despite being deeply rooted in a specific CTI information sharing platform, the applicability of the presented workflow and toolchain is limited by the theoretical nature of the work. The first steps towards instantiating the proposed model and obtaining the necessary social and technical components (Q2 and Q3) can be taken by means of:

- Looking at the available MISP user documentation, conducting experiments in the MISP VMs, and talking to lead developers from the MISP community, such as the Computer Incident Response Center Luxembourg. These efforts could serve to construct and validate a minimalistic theoretical master model that defines how data is shared within and between MISP instances.

- Conducting experimental user studies with existing MISP users, participants of MISP trainings, or with prospective MISP users. The last target group could be of particular interest when studying the applicability and suitability of MISP for new sharing communities that do not focus on technical threat intel and might not necessarily have highly-technical users, yet could benefit from information sharing, such as researchers of misinformation, dark patterns, etc.

As our focus is on investigating the distribution, less attention is paid here on the actual content of these CTI events. One can consider all data and metadata to be dummy values and the purpose of our investigation would be to see whether a certain entity could see the dummy values. Nevertheless, for the purpose of identifying inadvertent disclosure or undersharing, it is good to designate which dummy values should be considered as sensitive or important for the investigation. At the moment, this is left to the investigator to designate mentally or outside of the system which dummy values should be considered as such. The current approach is, thus, geared towards capturing the worst-case scenarios when a misalignment happens i.e., as if all data and metadata was sensitive, urgent, actionable, etc. In reality, not all data and metadata may be relevant and not all situations where a misalignments happen may be problematic. An extension of this work could be to designate inside the model which values are specifically important for the investigation at hand.

We believe that the master model of the system, along with additional modeling of the instances, entities, user perceptions, and other variables of interest, could be extended to a formal model. The application of model checking and formal methods could yield additional insights as well as helpful learning inputs to the participants as to where their understanding is wrong. What to consider and how to create such a formal model is left as an open question at this point.

## 4.6 Chapter Conclusion

Human aspects and behavior in CTI sharing platforms are vastly unexplored. In this chapter we proposed a theoretical concept of a workflow and toolchain that seeks to verify whether users have an accurate comprehension of how far information travels when shared in a CTI sharing platform. Our approach, presented in the context of MISP, argues to be helpful in the analysis, simulation and training efforts in CTI sharing. Validation of the proposed model would require performing additional technical and user research that we leave as future work. In the next chapter, we extend the introduced concept of socio-technical analysis of system properties and users' perceptions and explore ways to formalize and automate such analyses.

Context II

# Secure & Private Communication

*A very little key*
*will open a very heavy door.*

Charles Dickens

# 5

# Detecting misalignments between system security and user perceptions

CHAPTER ORGANIZATION. This chapter is organized in 7 sections. We start by introducing the research context, problem, and our research questions. We continue by framing our investigation within existing research and describe the methodology behind our proposal and models. We then exemplify our approach with a use case, an illustrative socio-technical security analysis of a recently developed E2E email encryption system. Next, we outline how the analysis pinpoints potentially problematic areas that could be investigated further by conducting appropriate user studies. Finally, we discuss how our approach could promote a more comprehensive understanding of socio-technical system security.

## 5.1 INTRODUCTION

From one philosophical viewpoint, technology is an "ongoing attempt to bring the world closer to the way one wishes it to be" [128]. Thus, the role of technology is to design techniques and instruments to respond to human needs. Central to the practice of technology is the design process during which the identified needs are translated into functional and non-functional requirements.

In security-critical systems, requirements can be expressed as desired security properties. These are then considered in the design of cryptographic protocols and the successive analysis where the properties are verified to hold in the presence of an adversary, i.e., a threat model. Researchers and practitioners, however, have highlighted major challenges and difficulties associated with attaining protocols able to meet the requirements—or, equivalently, to satisfy the security properties—especially when the protocols are meant to be used by peo-

ple or when people are key elements in the achievement of security goals [108, 223]. New threats to security can come from non-malicious users because of ill-designed user interfaces or unusable security policies. Security issues may also arise due to people being assigned too complex security-related tasks, them not being motivated to follow security policies, or due to them lacking the capability to make good security-related decisions [78].

Certain practices exacerbate the situation, e.g., not following a user-centered approach in the design of the product, service or system, examining the security of protocols in isolation, or referring to security models that are not conceived to capture the complexities of the real world. Therefore, it is essential to consider protocols in the context of their complex "human" environment, especially for systems whose security can be compromised in ways that cannot be captured by an analysis merely from a technical viewpoint. In this case, we are talking more precisely of *socio-technical systems*, where both human and technical components need to work together to achieve production tasks, as well as achieve the enabling task of securing that system effectively [124]. Thus, in order to study such systems we need a socio-technical mindset, which postulates that "people, machines and the context" [35] need to be considered as elements of the system and, therefore, as part of the security analysis, too [39].

Here we focus on a specific socio-technical aspect in the context of system security which has not been studied extensively in the domain of formal security verification, namely *misaligned conceptual models*. We are particularly interested in the potentially adverse *mismatch between the objective technical security guarantees provided by a system* and the *subjective security guarantees as perceived by users*. We believe that certain security issues can be defined in terms of such misalignments, then formally expressed as socio-technical security properties. In a system that has both technical and human components, users place trust in the technical system to support them in fulfilling their goal, but if there is a misalignment between what the user believes to have achieved and what the system has actually achieved—or if users cannot predict the effects of their actions or determine whether they have carried out their actions as intended—there might be security and privacy vulnerabilities on a socio-technical level which are not detectable via formal security testing or analysis. If such misaligned conceptual models are relevant for a system's socio-technical security, then there is the need of a new framework to detect and reason about them.

There are many illustrative examples why this is a relevant problem for socio-technical security. Let's take a look at the thriving cryptocurrency theft landscape, where it is estimated that $3.2 billion worth of coins were stolen in 2021 alone [276]. In 2018, IOTA cryptocurrency users lost $4 million by falling victim to an elaborate phishing site which collected a large number of seeds while appearing to be a legitimate IOTA seed generator. While the

IOTA developers justified that "the attackers correctly identified the 'human element' as the weak link"*, we can pose the question if this attack could have been avoided had the IOTA developers considered that the seed generation was a burdensome process for users and if they had offered a service with the same or better user experience than the one offered by the malicious seed generator. An alternative explanation is that users who fell for that trick must have had a misconception about the security of the fraudulent service. They might have also misjudged the level of security that the original secure service was capable of offering, which is not an uncommon misconception for users, as shown by Abu-Salma et al. in their investigation of mental models in E2E encrypted communication tools [3].

### Research Questions

The previous discussion leads to a few research questions:

- What models and what strategies can be used to investigate socio-technical misalignments of system security and user perceptions?
- How can such socio-technical security properties be defined and checked in the model?
- Can an analysis of misalignment lead to insightful discoveries about a system's socio-technical security or insecurity?

Despite security guarantees being embedded in most systems nowadays, users are not always aware of or even concerned about their existence. In our setting, nevertheless, we consider that the security and privacy goals are integrated as closely as possible with the workflow of the main user task and that the users understand, at least superficially, that achieving their goal in the system is relevant for the overall security and privacy. For example, a journalist may want to send an email containing sensitive information with utmost confidentiality. The goal of the journalist is then to send the email only to the intended recipient. Furthermore, the email should be readable only by that particular recipient. This corresponds directly to the system's security goals of authentication and encryption.

In an attempt to answer the questions above, which are aligned with our overarching thesis ***Objective 3*** (see Section 1.2), we present a two-stage strategy. First, we create a conceptual model that captures the interaction of a user with a system as they perform a certain goal, together with the associated beliefs of the user about specific security-related aspects of the system. Second, we additionally integrate the system behavior, i.e., specific system

*https://blog.iota.org/the-secret-to-security-is-secrecy-d32b5b7f25ef. Accessed: January 15, 2022

values at particular moments in time. This dual system-user representation allows for formalization that can be encoded as input to automated verification tools that allow reasoning about security aspects of the interaction when the user's beliefs and opinions are considered.

**Contributions**

The main contributions of this thesis section include:

- *Multi-layered user journeys*: a new framework characterized by a visual approach to representing user goals, actions, and perceptions with respect to a certain security or privacy-critical system, based on the UX concept of user journeys;
- Proposal of a subsequent system-user alignment model that is open to formalization and automatic verification of any misalignments between system values pertaining to the technical level of security provided by a system and user perceptions thereof;
- Instantiation of the proposed framework within a use case investigation of $\mathsf{p} \equiv \mathsf{p}$, a new secure email system, and discussion of the innovative insights of this combined methodology that aims to expand our holistic understanding of system security.

## 5.2 Research Context

Our proposal builds upon previous research and concepts. We briefly introduce them next.

### 5.2.1 Ceremonies

The notion of security ceremonies extends the concept of security and network protocols by explicitly including humans and their interaction with other nodes or humans in the system [104, 269]. As introduced earlier, the motivation and necessity to extend the security analysis beyond the security protocol derives from the complex socio-technical nature of security systems and the numerous attacks and vulnerabilities that exist on different technical and social levels. By extending protocol analysis, previously undetected security flaws could potentially be found and solved [62]. Formal security analysis of ceremonies, however, has not been studied extensively [37, 314], their formal verification is not a straightforward process [62], and human behavior tends to be modeled arbitrarily rather than grounded in the context of use of the system under investigation. According to Ellison, to model the human nodes in ceremonies, we need to observe actual human behavior [104]. Bella et Coles-Kemp emphasized that a framework incorporating personas in the formal analysis of ceremonies is not available though strongly desirable [38].

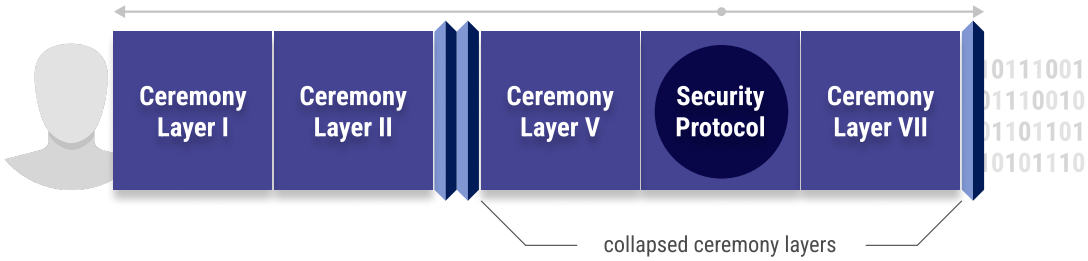



**Figure 5.1:** Abstract representation of a security ceremony, which extends the notion of a security protocol. The *ceremony concertina* can consist of multiple layers representing different socio-technical components.

One particular interpretation of this notion views a security ceremony as a multi-layered *concertina model* (see [38, 39]). According to this reference model, represented in Figure 5.1, a socio-technical system is broken down into its different information and communication layers. They include, from the one side, layers that extend towards the user, such as the interactions via the system's user interface and those pertaining to the persona, i.e., the behavior of the user or social interactions that humans have in society. From the other side, they extend inwards into the system's processes and protocols, including the elements with which the system interacts, which can also be remote, such as cloud services or other systems of communication peers. Depending on the questions and objectives of a security analysis, certain layers that are irrelevant for the investigation at hand or for which we assume that certain (security) properties hold, could be collapsed in order to allow the analyst to focus on the layers and the interconnections that matter most.

Despite being useful as a reference model, the notion of a layered security ceremony has to be instantiated if we want to use it for an analysis of a particular system's security. Here, one has to solve the problem of collecting the information necessary to detail the communication steps and the messages that realize the information and communication layers of a specific system's ceremony. As the intention in our approach is to highlight as elements of a security analysis the alignments and misalignments between the security guarantees of a certain system and users' understanding of them, we additionally need to collect such ancillary information relating to the users, and integrate it in the ceremony.

To extract the necessary information for the inward layers of a system and to uphold claims about the system's technical security qualities we resort to the more technical strategies of security analysis. As explained next, for the most outward layers of a system's ceremony we look into user experience methods, in particular, *user journeys* in order to collect the necessary information pertaining to user aspects, such as their perceptions of the security of the system. With personas being one of the core components of journey maps [137], our approach embraces well-established UX methods that are rooted in user insights.

### 5.2.2 User Experience (UX) Mapping Concepts

The necessity to harmonize security and usability as well as to maintain an agreement between a system's security state and the user's mental model has been highlighted by Yee [385]. We second Yee's position that conflicts between security and usability goals can be avoided by considering both aspects together throughout an iterative design process. Moreover, as already mentioned in previous chapters, we argue that the user experience needs to be looked at more holistically in order to consider different human needs that may be determining as to the way a user may interact or experience a particular system. In our investigations, we take an expanded approach to include topics such as pleasure, beauty, emotions, and experience, all of which the HCI research community has studied extensively over the past two decades [90].

In order to design useful secure applications from the user perspective, we need to direct our attention towards understanding users' goals, their motivations, rhythms and routines, the actions they take and the problems they face not only during, but also before and after they interact with a product or service. An approach often employed by companies that create remarkable customer experiences revolves around *user journeys* [233].

#### User Journeys

As a visual representation of the process that a person goes through in order to accomplish a goal, user journeys are rich in user thoughts and emotions, and are utilized to understand and address customer needs and pain points [250]. While there is not one single or standardized way of creating or representing user journeys, typical elements of a user journey map include: user/persona, scenario, goals and expectations, journey phases, touchpoints, actions, thoughts, and emotions [249].

The persona is the one experiencing the journey with respect to a specific scenario and goals. The journey can have multiple phases denoted by different touchpoints, which can start before the user interacts with the system and finish long after all the interaction takes place. The journey map, along with its supporting reports, is a compilation of insights about users' perceptions, the actions that they take at each stage, their motivations or hesitations, what they feel, what uncertainties they have and what barriers they face along the path.

Depending on the stage of the project, scenarios can be real or anticipated, journeys can be actual or expected, personas and actions can be rooted in data or fictional. In this regard, we can utilize a portfolio of multidisciplinary methods and tools, such as observations, interviews, probes, task and scenario analyses, walkthroughs, focus groups and usability studies, in order to understand and analyze the user, evaluate the system or generate new ideas.

Our approach, as explained in Section 5.3, takes inspiration from user journeys and related UX mapping methods, and depicts the interaction of a user with a security or privacy-critical system vis-à-vis the user goal. Similar to the human-in-the-loop security framework proposed by Cranor [78], our approach focuses on non-malicious users, i.e., those that do not intend to attack the system deliberately. To model their behavior, the cognitive and emotional processing—which determines the UX—as they perform their goal-driven action cycles or react to the system and external environment, we rely upon Norman's Action Theory [253] which is a simplified framework for understanding human action and processing at the descriptive level (see Figure 5.2 and Section 2.1.2).

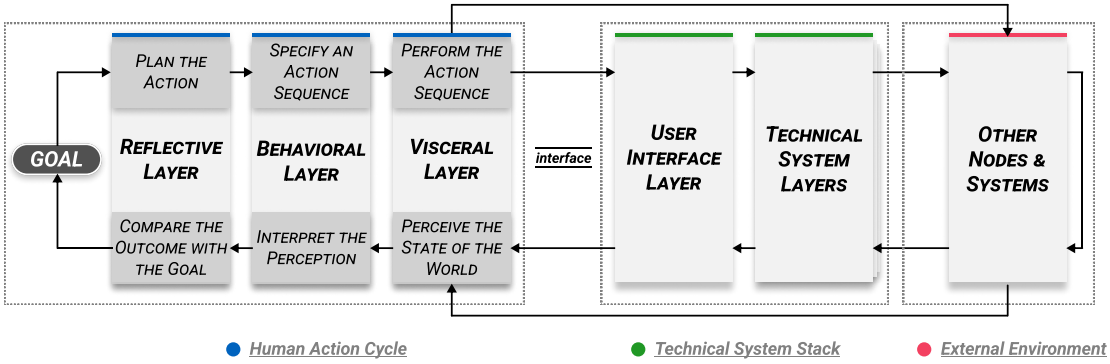



**Figure 5.2:** Abstract representation of the layers of our socio-technical security analysis proposal, called *multi-layered user journeys*.

## 5.3 Multi-layered User Journeys

We particularly focus on transcending the traditional, siloed approach of analyzing system security, thereby we marry the concept of security ceremonies with user journeys that cross-cut the different layers of a socio-technical system, i.e., the users with their perceptions and actions, the user interface, the other technical and back-end layers of the system as well as the external environment.

What distinguishes visually our mapping approach from traditional user journeys is the inclusion of the workflow that depicts the steps taken by a user to achieve a goal, which is spread out over a number of lanes. Thus, visually our maps resemble workflow diagrams, such as swimlane diagrams and service blueprints, which typically show the steps of an interaction between a user and different parts of a system or departments of an organization [191]. The separate lanes in our case correspond to different layers of a socio-technical system, portraying the interrelatedness of different activities, events and decision-making processes that take place sequentially or simultaneously.

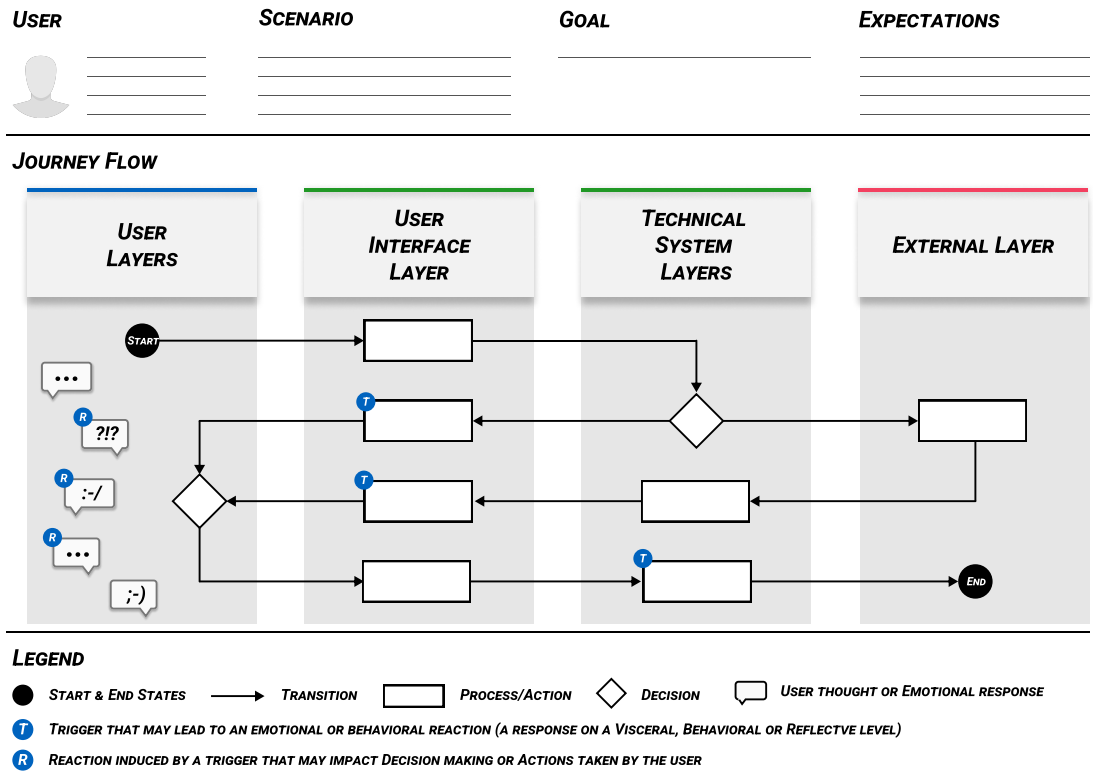



**Figure 5.3:** Deconstruction of a *multi-layered user journey* map.

Figure 5.3 depicts a deconstruction of a typical multi-layered user journey map where the breakdown and flow of the journey correspond to the processes and actions taken by the user, technical system and entities in the external environment during an interaction session. For instance, the planning, decision-making and cognitive evaluation processes can be represented in a sublayer of the *USER* layers set. These processes can be translated into specific actions that users typically perform via a user interface which are further propagated to the backend layers of the technical system. The sublayers in this *TECHNICAL SYSTEM* group can be collapsed or further expanded should we require a more fine-grained analysis of the processes that take place behind the scenes, such as the security protocol, cryptographic components, etc. *EXTERNAL ENVIRONMENT* is the last layer which covers external elements, nodes, and systems that are relevant for the socio-technical system or goal under investigation.

The user interface layer can contain perceivable indicators and signifiers to communicate system feedback or prompt the user for input. These can trigger an emotional or behavioral reaction that may impact decision-making or subsequent actions taken by the user. Ad-

ditional notes of interest, such as user mindsets or emotions can be added along the flow, referenced in a separate supporting document, or depending on the purpose of the analysis, mapped within the USER layer, like in our example.

It is important to restate that a multi-layered user journey represents how a particular user/persona experiences a particular security or privacy-critical system with respect to a specific goal. In this paper, we instantiate the framework and bound our analysis within the context of one secure email system, as explained in Section 5.5. Before we present our use case, we introduce how such journeys and the associated artifacts can be used to create follow-up models enabling a formal security analysis of the socio-technical system.

## 5.4 SYSTEM-USER ALIGNMENT MODEL AND SECURITY ANALYSIS

We now introduce the notion of formal verification and a formal model for the multi-layered user journey, along with a few interesting classes of security properties. Then, we describe how to use these concepts to execute an analysis for detecting and reasoning about misalignments between security related aspects implemented in a specific system and the perception that users have about those aspects when they interact with the system.

### 5.4.1 FORMAL VERIFICATION IN THE PRESENCE OF HUMAN INTERACTIONS

Formal verification is a technique to mathematically determine whether or not a system possesses a set of desirable properties. Systems are modeled through well-defined structures and properties are expressed by precise languages with formal syntax, semantics and decision rules. A formal analysis consists of interpreting the results of a formal verification in order to obtain insights about the behavior of the system in question. This technique has been particularly applied for technical analysis of hardware, software and security protocols. The literature on this topic is extensive, but one can refer to [79] for an introduction.

Existing research that has explored interaction between humans and systems using formal methods has largely focused on the formal analysis of Human-Automation Interaction (HAI). The purpose in that line of work has mostly been on the evaluation of safety and correctness of tasks that involve human operation in automated critical systems, such as flight controllers, infusion pumps, medical device interfaces, etc. (*e.g.,* [81, 86, 162]). In those studies, the aim is to detect errors in the design of human-machine interfaces that could potentially create confusion or decrease the system's usability, which could consequently prevent the human operator from successfully achieving a specific goal or lead to hazards. Such analyses have a technical perspective because, even if human interaction is

captured, the verified properties concern solely aspects of the system and/or its behavior, particularly the interface.

We are interested in defining properties to determine whether the perceptions of the user about the behavior of the system are consistent with the system's behavior, as per its implementation. In our approach the insights as to what the user perceives, believes or assumes and what the system guarantees, come from different investigations. Studying such properties can improve our understanding of the system's security by considering a more holistic, socio-technical perspective. For instance, one set of such properties, called *False Sense of Insecurity* (*False-SoI*) emerges when a secure and privacy-preserving system improperly transmits the degree of protection that it can actually provide. A second set of properties, which we call *False Sense of Security* (*False-SoS*), describes when insecure systems falsely inspire a sense of security, which is not justified by a technical analysis.

Our approach relies on three assumptions:

1. The implementation of the system meets the functional requirements of the technical specifications.
2. Standard cryptographic properties, such as authentication, confidentiality and integrity, have been proven in the implemented security protocols.
3. Any action performed by a user is valid in the ceremony.

These assumptions ensure that the misalignments that we may detect are neither due to a faulty implementation, nor a user intentionally subverting the system. It is worth noting that in our multi-layered user journey, it is possible to model a flawed system as well as a malicious user, however, the analysis that we aim at, focuses on detecting misalignments that emerge at the interaction level of a system and a non-malicious user.

### 5.4.2 Formalization of Multi-layered User Journeys

In order to perform a formal verification, we need a model and a set of properties of interest. Informally, our model captures all the possible states that a system can reach when a user performs any possible sequences of actions to achieve a specified goal. Thus, the *Journey flow*, represented in Figure 5.3, can be seen as a basis which the different states and transitions can be derived from. In each state of the model, we can store values that are pertinent to our investigation. In particular, values that refer to user perceptions of specific system *aspects* on the one hand, and on the other hand, values that refer to the actual status of

the system, its behavior or objective security and privacy guarantees. We call these values *evaluations* from the user side, and *evaluations* from the technical system side. The properties must be expressed in terms of unambiguous and measurable *aspects* of the system, as described in the next sections.

The formal analysis of the resulting model with respect to the predefined misaligned-security properties aims to detect situations where the evaluations from the user side differ from the system's assessment of the security features, and to examine the way in which they differ. Moreover, the identified situations are subject to further kinds of analysis, such as those targeted at finding and fixing the root causes of the confusion related to deficiencies in the interface design [86].

### The model

Such a model can be obtained through *labeled transition systems (LTSs)*, which are directed graphs used to model the evolution of systems where nodes distinguish states and edges represent transitions among states, triggered by actions labeling the edges [27].

Our socio-technical (s-t) transition system is a tuple $(S, Act, Prop, \rightarrow, I, A, evSys, evUsr)$[†] that consists of the following elements: a finite set of *states*, *actions*, atomic *propositions*, *transition relations*, *initial states*, *aspects*, and two *evaluation functions* that in each state assign to the *aspect* a *value* from a corresponding *domain*. With respect to formally representing a multi-layered user journey this means that the interaction between a user and a system in relation to a specific goal G is spread over a number of states, with a clear start and end state(s). The state transitions are triggered by user actions or by the system, subject to satisfaction of specific conditions (e.g., if the public key of a communication partner is available, the system will move to the next stage of encrypting a message using that key).

To study misalignments, we need to identify *aspects* of the system that are relevant for specifying security properties, and that are either directly or indirectly measurable by both users and the technical system itself. One such example could be the "trust level of a contact" in a messaging application or the "mode in which a message will be sent". The *domain* of possible values for the first *aspect* could be $D_{a_1} = \{trusted, unknown, mistrusted, \perp\}$, whereas for the second it could be $D_{a_2} = \{encrypted, plaintext, \perp\}$. The exact assignment of values regarding a specific aspect at a specific state is returned by the two *evaluation functions*, from the system and from the user side, respectively.

Another key aspect to consider is the system and user view regarding the achievement of the goal, i.e., the assessment reporting whether G has been reached, if it is still in progress

[†]The formalization specification can be found in Appendix B and in [328].

or if the conditions in a certain state prevent its future completion. Using this notion, we can also designate final states as those where the achievement of the goal is not *in progress*, from the system's point of view.

#### Misaligned-security properties

To express the misaligned-security properties we selected Computation Tree Logic (CTL) [73]. Its tree-like structure of time, means that at each state the future value of propositions is not yet determined, which is suitable for modeling the interaction in our case, as user's perceptions and *evaluations* of different aspects are built up or updated along the way.

The CTL operators **A** and **E** allow us to express properties over paths, while the operators **G, F** and **X** over states. In a nutshell, we can investigate if a certain CTL formula holds in all paths (A) of a formal model; if there exists (E) at least one path where the formula is true; if the formula can hold in all the states of a path (G), in the next state (X), or at least in a state reachable in the future (F).

This allows us to specify the following properties:

**Aligned-SoS** At every state of the ceremony, the *sense of security* that the user has about a specific aspect corresponds to the assignment from the technical side i.e., it corresponds to the system's evaluation of security.

**Lower-SoS** There is a state in the ceremony, where the user's *sense of security* about a specific aspect is lower than the system's evaluation of security.

**Higher-SoS** There exists a state during the ceremony where the user's *sense of security* about a specific aspect exceeds the system's evaluation of security.

**Misaligned-Goal** There exists a path where, even if the evaluation of all other aspects is aligned all the time, the understanding regarding the achievement of the goal differs from the user's and system's point of view.

The analysis certainly does not need to be constrained to the sole verification of the misaligned-security properties defined above. Analysts might as well choose to define properties specific to the socio-technical system under investigation.

### 5.4.3 An Approach for a Formal Verification of Misalignments

Misaligned-security properties can be automatically verified in socio-technical transition systems by *model checking* tools [73]. Such an automation allows us to efficiently explore

all the paths from each state in a model to determine if the specified property holds, which is especially advantageous for big models.

As stated earlier, to compare misalignments within our model we require *evaluations* regarding specific security aspects from the system side and from the user side. The system evaluations can be inferred from the design specification of the system or obtained by analyzing traces or logs recorded during the system's execution. The evaluations from the user side can be drawn from a multi-layered user journey depicting the interaction with respect to a certain goal. A verification based on hypotheses could be insightful as well. In such a case, selected values from the domain are assigned to the variables, depending on the hypothesis. A posteriori study with actual users could validate/invalidate the results obtained.

An analysis of the verification's results pinpoints the states in the system where certain security aspects are potentially misunderstood by users or where there is a discrepancy between what the user perceives and what the system communicates. Detecting such states opens the possibility for improvements to the system. An ideal application of the technique involves iterating the process [model-verify-analyze-improve] as many times as required, to obtain a desired alignment between user's perceptions and the reality, at least for the most critical steps of the user journey.

## 5.5 Case Study

In the next section we introduce the secure email system deployed for the demonstration of our proposal. Preliminaries on secure email communication as well as related work on the adoption and usability of end-to-end email encryption systems can be found in Section 2.6.

### 5.5.1 Pretty Easy Privacy (p≡p)

As a use case for our investigation, we employed p≡p[‡] whose underlying crypto relies on OpenPGP libraries (such as Sequoia-PGP[§]), and whose cryptographic protocols were investigated and found to be secure [294].

Based on opportunistic security [93], p≡p positions itself as technology for secure and private communication that has usability as a key motivation or goal [44]. Targeting primarily non-expert users, p≡p's approach is not to confront its users with technical jargon around cryptography. Thus, concepts such as *keys*, *certificates*, *fingerprints*, or even *encryption*, which are otherwise ubiquitous in tools for email end-to-end encryption, are deliberately concealed in p≡p.

[‡] https://pep.software, accessed on January 15, 2022
[§] https://sequoia-pgp.org, accessed on January 15, 2022

It automates the majority of user-related operations, e.g., key management, key discovery, private key handling etc., which as indicated in literature, have been seen as obstacles to the deployment and successful uptake of systems for secure end-to-end messaging. This means, p ≡ p automatically generates user keys, appends the public key to each outgoing message, and extracts and stores keys from incoming messages. Messages are automatically encrypted and decrypted.

The developers of p ≡ p argue that the system has been designed with functionality, security and privacy considerations in mind, such as interoperability, minimal configuration, and in particular, no trusted servers. It can be used for communication in both encrypted and plain text formats, with people that do or do not use p ≡ p or other encryption software. For compatibility reasons and the purpose of integration in organizational settings, p ≡ p supports S/MIME. However, according to the p ≡ p white paper, centralized cryptographic approaches do not provide sufficient protection and are considered an unreliable communication type from their perspective which advocates privacy without compromise [260]. The desktop distributions of p ≡ p integrate into Outlook and Thunderbird, whereas the iOS and Android distributions work as standalone clients.

#### Technical concept

The security goals that concern p ≡ p are confidentiality, integrity, and authentication of digital written communications. With prior work suggesting that automated key management is critical for usability by saving time and reducing confusion for participants (see Section 2.6.1), p ≡ p aims to achieve privacy by default whenever a technically secure communication channel between two p ≡ p users can be established. The system's *trust-on-first-use* (TOFU) approach means that once p ≡ p recognizes that it can protect the communication with the communication partner, it does so automatically.

Typically, the first message to a new communication partner is sent in the clear (i.e., unencrypted) with the public key of the sender attached. This allows the communication partner to respond already with an encrypted message utilizing the received public key. The public key of the communication partner being automatically appended in their reply completes the key exchange, which allows for subsequent messages to be encrypted and signed by both parties.

In order to avoid MITM (man-in-the-middle or machine-in-the-middle) attacks, p ≡ p further allows users to compare their *trustwords* by engaging in a p ≡ p handshake i.e., they can perform an out-of-bound authentication protocol with a communication partner, after which, a trust rating is assigned to that communication partner. A rating is also applied to

every sent and received message, depending on a number of technical security conditions such as the deployed crypto algorithms, key validity, etc. These ratings are then displayed in the user interface via a set of privacy indicators, which according to p≡p, should help users understand the level of protection applied and avoid accidental leakage of sensitive information.

p≡p differentiates between a number of protection levels and defines appropriate ratings:

***Unknown (N)*** the message has no recipient yet, hence, the privacy level cannot be determined.

***Unsecure (I)*** the communication partner does not use any secure email systems, hence, a ceremony to trust each other cannot be executed nor the message can be encrypted. The message is sent or has been received in plain text i.e., unencrypted.

***Secure (S)*** the user has the public key of the communication partner, thus the message is encrypted and signed. However, the identity of the communication partner has not been confirmed in a p≡p handshake.

***Secure and Trusted (S&T)*** the user has the public key of the communication partner and their identity has been confirmed in a p≡p handshake. The message is encrypted and signed.

***Mistrusted (M)*** if the verification of the identity of the communication partner did not succeed during the handshake i.e., it was designated to be mistrusted by the user, or if the communication is under a MITM attack, the channel is considered insecure and not private.

p≡p's privacy ratings and indicators are further elaborated and studied in Chapter 6.

### 5.5.2 p≡p Multi-layered User Journey

#### Our objectives

While the goal of this chapter is to put forward a new framework and methodological approaches to detecting user misperceptions of system security and privacy, the grounding of our demonstration within a representative use case allows us to gather inputs that are in line with our overarching thesis ***Objectives 1*** and ***2***. We were, thus, interested in understanding what experiences emerge with respect to the use or anticipated use of p≡p as well as what misperceptions users have or could potentially have regarding the security and privacy aspects of p≡p.

### Methodology

In order to obtain the necessary information and construct multi-layered user journeys for different aspects of p≡p, we resorted to the following methods:

COGNITIVE WALKTHROUGHS. Given that we conducted only a preliminary analysis of the desktop distribution of p ≡ p for Thunderbird (Enigmail/p ≡ p version 2.0.3) before any user studies took place, we were not able to ground user insights in actual observations. While that is certainly a limitation of this investigation, cognitive walkthroughs are well-established methods of inspection performed without any user involvement that allow reviewers to evaluate a proposed interface in the context of one or more specific user tasks [370]. With respect to a specific goal (as stated below), two reviewers examined each screen in the interface of p ≡ p taking into account all the possible actions and paths that can be taken via the interface.

CODE EXTRACTION. We analyzed the developer's publicly available technical documentation and code in order to extract the security protocol specifications [16–18]. This allowed us to understand and represent the entities and processes that take place in the technical layer of p≡p, i.e., the backend.

FOCUS GROUP. In order to get inputs on the experiences that might emerge and the possible emotion elicitation with respect to the use or anticipated use of p≡p, we conducted one focus group session with a total of 8 experts from the HCI research group of our university (5 female and 3 male). We gave them 24 hypothetical situations/steps that new, non-expert users could be faced with. These covered phases before and after interacting with a secure email system like p≡p. For instance:

- Searching online for secure e-mail 'solutions' and evaluating among the alternatives.
- Contacting the support team of the company that develops the secure e-mail system.

The focus, nevertheless, was on the interaction with the secure email system, as exemplified by the following situations/steps:

- Sending the first e-mail after installing the system.
- Receiving an email that is indicated by the system as being Secure.
- Changing the trust levels of people you authenticated.

For each step, we asked them to list the positive and negative emotions that could be elicited, drawing them from the Positive Emotional Granularity Cards [386] and Negative Emotion Typology [126]. All emotions listed by the experts were combined per situation and sorted according to the total count (raw frequency) of the emotion per situation. The top three per applicable situation were chosen to be modeled in the user journey, where they were classified as weak, mid or strong depending on the count.

### Components and Visualization of the Multi-Layered User Journey

Considering p≡p's principal functionality and target audience, we defined the components of the user journey as follows:

***USER*** *New and prospective users of* p ≡ p *who do not have a technical background or deep understanding of public-key cryptography, yet would like to communicate via email in a secure and private manner.*

***SCENARIO*** p≡p *for Thunderbird (Enigmail/*p≡p *version 2.0.3) is installed on the computer of a new or prospective user who wishes to send a confidential email. The user journey covers only the interaction aspects related to the goal.*

***GOAL*** *To send an e-mail in a confidential way exclusively to a specific person.*

***EXPECTATIONS*** *Despite their lack of experience, the user expects to achieve the goal. If they fail, at least they expect to know why they were not able to achieve the goal and what they should do differently.*

The *journey flow* is depicted in Figure 5.4 along a number of layers as explained next.

COGNITIVE EVALUATION & EXECUTION. The first user layer represents the emotions, thoughts, and decisions users go through as they perform the actions required to achieve the stated goal and as they perceive the state of p≡p and the environment.

USER ACTIONS. The execution of the specified action sequence is represented in this layer. This refers to actions that in practice the user effectuates solely through the user interface (UI) of p≡p. Other actions and behavior that the user may do within the *journey flow* that are not carried out via the UI, such as an out-of-bound phone call in order to check the correspondent's trustwords, in our case are represented in the external environment.

USER INTERFACE. This layer represents the signifiers, feedback, and input prompts communicated by the system to the user. This refers to different security and privacy indicators communicated by $\mathsf{p} \equiv \mathsf{p}$ to inform the user of the protection level applied to a message as well as any other dialog boxes.

$\mathsf{p} \equiv \mathsf{p}$ BACKEND. This layer can be regarded as a set of collapsed technical layers where a number of processes and activities take place, also in response to user action carried out via the user interface. These processes take place *behind the scenes* from the perspective of the user, but some of them may engage with the user via the interface.

EXTERNAL DOMAIN. This layer hosts all other nodes and processes that exist outside of the encryption software, such as the operating system, email servers, the internet, etc.

**Purpose and Use**

The visualization allows for easy tracing of the possible interaction paths between a user and $\mathsf{p} \equiv \mathsf{p}$ with respect to the stated goal. It serves to depict all privacy ratings that could be applied by $\mathsf{p} \equiv \mathsf{p}$ when sending emails. For example, even when a user wants to use $\mathsf{p} \equiv \mathsf{p}$ to protect the secrecy of emails, if the public key of the recipient is not in the key repository of the user ($\mathsf{p} \equiv \mathsf{p}$ backend), the message will be sent in plain text with a privacy rating *Unsecure*, unless the user decides to reformulate the goal and change the recipient of the message, in which case other privacy ratings could potentially be applied. Similarly, we can trail the steps that the user needs to perform to reach the maximum level of protection possible (i.e., *S&T*) which involves comparing the key fingerprint/trustwords with the recipient.

Such a visualization could be used for informal security analysis, workflow and experience optimization, and could potentially be beneficial in establishing a communication bridge between security experts, (UX) designers as well as other relevant stakeholders. In the next section, we discuss how it can also enrich formal security analyses.

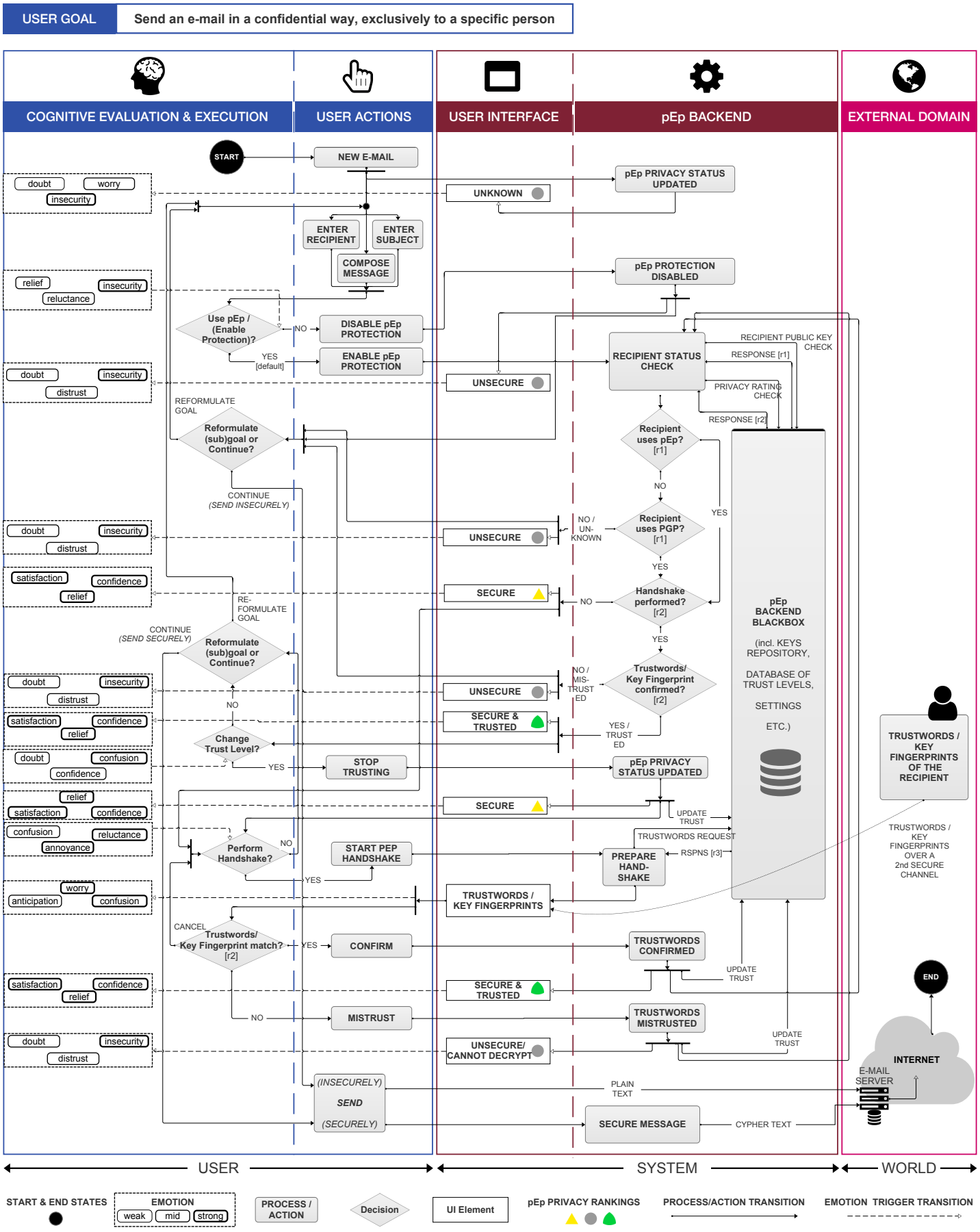



**Figure 5.4:** Multi-Layered User Journey depicting the process of performing specific goal-directed actions within p ≡ p

### 5.5.3 FORMALIZATION OF p≡p'S MULTI-LAYERED USER JOURNEY

Derived from the multi-layered user journey described above, we created the s-t transition system $\mathcal{M}_{\mathsf{p}\equiv\mathsf{p}}$ shown in Fig. 5.5 and specified as follows.

- $S$ and $\xrightarrow{x}$ denote the nodes and arrows in the diagram, where $s0$ is the initial state;
- Transition relations consist of user *actions*, labeled in green, and atomic *propositions*, labeled in blue;

The set of *propositions* consists of the following elements:

- *pepReceiver* = the communication partner is a user of p≡p;
- *handshake* = the authentication protocol (comparison of trustwords or key fingerprints) between the two communication partners has been performed;
- *trustwordsMatch* = the compared trustwords/fingerprints match in reality;
- *confirmedTrustwords* = the matching of the trustwords/fingerprints has been confirmed in the system;

We define two security and privacy-critical *aspects* of interest for our investigation:

- $A = \{privacy, goal\}$, where *privacy* represents the privacy protection level assigned to an email and *goal* captures the status of G as defined in Section 5.4.2.

The domain of privacy protection levels is defined by the set of p≡p's privacy ratings and corresponding security and privacy indicators:

- $D_{privacy} = \{I, S, S\&T, N, \perp\}$.

In the graph, we use *privacyS* and *privacyU* to model in a particular state the values of the system and user evaluation functions for the aspect *privacy*. For instance:

- $evSys(privacy, s_{10}) = S\&T$ is represented in the model with a label $privacyS = S\&T$ in the system state $s_{10}$.
- $evUsr(privacy, s_1) = N$ is represented in the model with a label $privacyU = N$ in the system state $s_1$.

Similarly, *goalS* and *goalU* capture the results of applying *evSys* and *evUsr* to the aspect *goal*, respectively.

$\mathsf{p} \equiv \mathsf{p}$ has been already verified for functional correctness, therefore, we obtained *privacyS* i.e., the output values of *evSys* directly from the diagram in Figure 5.4. However, the assignment for the output values of *evUsr* i.e., *privacyU*, is not straightforward in our use case. Due to the limitations of our preliminary investigation, we do not have direct user perceptions regarding the studied *aspects* which are grounded in actual user observations. Instead we had to perform a mapping based on (a subset of) the emotional responses featured in the COGNITIVE EVALUATION layer of Figure 5.4. We mapped the elicited emotions to a corresponding privacy level perception as follows[¶]:

- Not reported by user $\implies \perp$ *(undefined)*
- {doubt, confusion} $\implies$ *N (Unknown)*
- {insecurity, worry, distrust} $\implies$ *I (Insecure)*
- {security, reluctance, confidence} $\implies$ *S (Secure)*
- {trust, satisfaction} $\implies$ *S&T (Secure & Trusted)*

In an attempt to investigate whether there are any misalignments between the user's perceptions and how $\mathsf{p} \equiv \mathsf{p}$ applies the privacy protection levels during the interaction sequence of sending a confidential email out to a specific person, we analyzed the following misaligned-security properties:

**P1.** AG $(goal^{usr} \leq goal^{sys})$

**P2.** AG $(privacy^{usr} \leq privacy^{sys})$

**P3.** E $[(privacy^{usr} \leq privacy^{sys})$ U $(goal^{usr} \neq goal^{sys})]$

**P4.** AG $(\neg trustwordsMatch \rightarrow (\text{AG } privacy^{sys} \neq S\&T))$

P1, P2 and P3 are instances of the properties in Section 5.4.2. P4 is a property specifically of $\mathsf{p} \equiv \mathsf{p}$ and expresses that, whenever the trustwords to be compared are different, $\mathsf{p} \equiv \mathsf{p}$'s privacy level is never S&T in any of the future reachable states. This property can be customized to provide specific insights, for instance, to ensure that not only the system, but also the user never evaluates the privacy level with the highest rank if the trustwords do not match in reality.

[¶]The mapping would need to be validated by means of an actual user study.

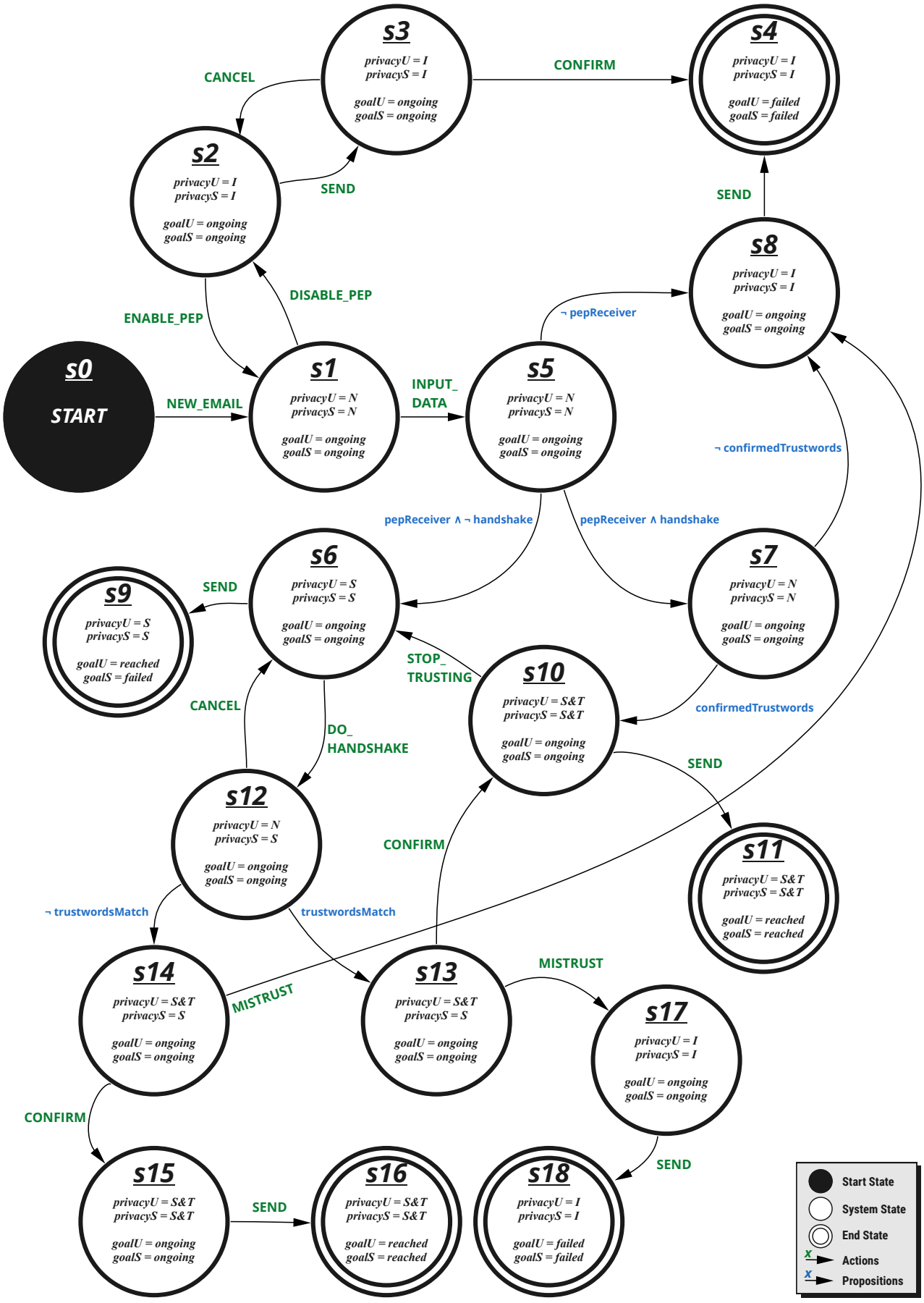



**Figure 5.5:** $\mathcal{M}_{\mathsf{p} \rightleftharpoons \mathsf{p}}$ – System User Alignment Model of the ceremony to confidentially send an email exclusively to a specific peer in $\mathsf{p} \equiv \mathsf{p}$.

### 5.5.4 Verification Results

We used the NuSMV model checker [68] to verify the misalignment properties in our model.

**P1** P1 does not hold when the user follows the trace $s0 \rightarrow s1 \rightarrow s5 \rightarrow s6 \rightarrow s9$. This reflects the case when the user wants to send an email to another user e.g., Bob, who is a $\mathsf{p} \equiv \mathsf{p}$ user too. However, the fact that Bob's email address corresponds to the real-life person has not been verified and confirmed in the system (the handshake can be initiated in state $s6$). $\mathsf{p} \equiv \mathsf{p}$ evaluates the privacy level with S as per the definition above, however, if the email is sent next ($s9$), the achievement of $\mathsf{G}$ fails because, even if the content is sent confidentially (encrypted), the system does not have enough information to guarantee that the email will be delivered to the intended person. On the contrary, the user's positive evaluation of *goal* can be justified in several ways; for instance they might be certain about the ownership of Bob's email (e.g., if they created the account for Bob); but it could also be the case that the user simply has blind trust in $\mathsf{p} \equiv \mathsf{p}$.

**P2** P2 is not satisfied either, when the user goes through $s0 \rightarrow s1 \rightarrow s5 \rightarrow s6 \rightarrow s12 \rightarrow s13$. The result is interpreted as follows: after the user selects to execute a handshake in $s6$, $\mathsf{p} \equiv \mathsf{p}$ shows a list of so-called *trustwords* supposed to belong to the intended receiver Bob ($s12$). Ideally, the user is expected to validate the displayed trustwords with Bob personally through a second channel, for instance via a phone call. $s13$ represents the moment when the peers determine that the trustwords match in reality; at that point the user trusts that the stated email addresses does indeed belong to Bob, but the system still does not elevate the privacy rating to the highest possible because the trustwords have not yet been confirmed in the UI of $\mathsf{p} \equiv \mathsf{p}$. This case is not a security problem if in the next step, the user submits the confirmation in the system ($s10$).

**P3** P3 holds. The explanation for P1 applies here too.

**P4** Finally, the satisfiability of P4 is falsified by the trace $s0 \rightarrow s1 \rightarrow s5 \rightarrow s6 \rightarrow s12 \rightarrow s14 \rightarrow s15$, i.e., when the trustwords do not match in reality ($s14$), yet the user confirms them in $\mathsf{p} \equiv \mathsf{p}$ ($s15$). Since the system is incapable of checking reality, it processes the user confirmation and assigns the corresponding privacy level, S&T. Furthermore, $\mathcal{M}$ reports that the user indeed evaluates $\mathsf{p} \equiv \mathsf{p}$ as S&T too, perhaps even knowing that the trustwords were different. Consequently, the system and user present an aligned assessment of the successful achievement of $\mathsf{G}$ ($s16$) which is, however, misaligned to reality.

The results of our illustrative security analysis of p≡p highlight problems of socio-technical nature that traditional technical analyses, such as symbolic verification of protocols would not detect given their inherent focus on the cryptographic methods of the technical system. Our approach confirms some known problems with the use of secure email identified by the usable security community. The use of formal verification for a socio-technical analysis, nonetheless, made it possible to define precise properties and extensively cover all scenarios that users could follow within an interaction driven by a specific goal.

The misalignments identified with P1, P2 and P3 give insights regarding the achievement of G and steps of the ceremony that may cause confusion in users. For example, in the case of P1, the fact that p≡p shows "Secure" as the privacy rating for a particular message might instill a false sense of security, as a non-expert user might not be aware of the potential security/privacy issues of not having the corresponding recipient authenticated. This is a valid concern as Lerner et al. showed that only a few of their participants worried about email content authenticity [216]. With the analysis of P4 we highlight a security weakness that is neither derived from an implementation problem nor from a misalignment, but from the user not having performed all the steps in the ceremony that offer the maximum privacy protection.

Even though our analysis is about the p ≡ p system, we might further pose the more general question whether the assessment of certain aspects of a system by a user is influenced by the observed evaluation of the system in a way that they rely more on the values projected by the system rather than on the real facts. For instance, if a user blindly confirms the trustwords without checking them in reality — and thereby assigns the Secure & Trusted rating — would subsequent and multiple exposures to the green privacy rating for that particular recipient make the user believe that the system will provide the maximum privacy protection (although in reality that is not possible given that trustwords have never been compared)? A user study for examining the understanding of the privacy indicators provided by p≡p and the perceptions of security that might be triggered by them would be a first step to investigate empirically.

Our preliminary analysis could potentially help in the hypothesis building by pre-selecting the candidate system states, i.e., critical points in the journey (where the formal validation fails) to test whether this is a real concern or a "false positive". In other words, in reality it suffices that an alignment is achieved before a critical action is taken by the user, and otherwise there could be states in the ceremony where a misalignment is harmless.

**Related Work**

In his dissertation, Houser [175] adapted Degani's human-automation interaction (HAI) [86] analysis concepts to a cybersecurity domain and extended the generic formal modeling framework with folk models of security [367]. The method was reported to be capable of detecting security vulnerabilities that are introduced by the user as a result of their mental model of system functionality being misaligned with the actual state of the world [175]. Despite similarities between Houser's and our concept, the approach of obtaining insights about user actions and user perceptions of security is different. He relies on a user mental model which is generic or corresponds to a set of pre-defined folk models, whereas in our case it is primarily informed by the multi-layered user journey.

### 5.6.1 Limitations

The modeling of user actions in our multi-layered user journey concept is based on Norman's model of 7 stages of action [253], which is a simplified and approximate cognitive model of action. It is particularly critiqued in relation to opportunistic aspects of everyday activity as the goals and intentions for many everyday tasks are not well specified i.e, they are not planned, but rather opportunistic [230, 253]. Nevertheless, if we assume that the user activity is planned, such as in our use case investigation, the model could be useful for understanding how users interact with a particular system.

Our methodology is still preliminary and needs to be validated, which can be done in several directions. One is horizontal, whereby we can attempt to apply our methodology to other use cases, within the secure communication domain or beyond. Another is vertical, by applying it more extensively in the analysis of the $\mathsf{p} \equiv \mathsf{p}$ system. Here, probably the most urgent validation task is to verify whether other kinds of investigations, for instance user studies, would confirm the same type of misalignment in the same specific points of the ceremony as our analysis has found. Note that this investigation would practically reduce to a validation of the methodology we are using to capture user's perceptions. Given that the system's guarantees (*e.g.,* that a message has been sent encrypted) are in fact technically determined—and therefore correctly represented in the model under our assumptions—and also our properties are defined without ambiguity, thanks to precise semantics of the formal model, a contradictory finding would mean that the only part that could be flawed is the wrong assignment of user's perceptions in our multi-layered journeys. For instance, the real user's perceptions could change in a way that we fail to capture, resulting in an erroneous analysis and, consequently, in an invalid conclusion.

In our preliminary investigation we have only looked at one user goal, thus we have not

performed an extensive analysis that covers different scenarios, nor different distributions of $p \equiv p$. As we have not performed any user studies, the emotions in our user journey are assumptions based on the input received during the focus group session, which might inherently lack accuracy and be biased. Therefore, we should bring more evidence that we can collect insights on the perceptions of actual users with different UX methods. Furthermore, the mapping that we are able to do between the elicited emotions and perceptions of security is not validated, and is modeled statically, rather than dynamically, hence it does not take into account how the emotions and perceptions might change over time or with experience. We also have to prove that we are able to define more and more realistic classes of properties, such as, for instance, expressing whether alignments happen only in particular moments of the ceremony. Despite these limitations, we believe that the methodology presented here to formalize user insights and detect issues on socio-technical levels opens interesting possibilities for further improvements also to this initial model.

For our proposal to make tangible contributions towards improving the security and privacy of real-world systems, the approach would need to integrate in modern iterative system development processes. UX practitioners have highlighted that the activity of journey mapping helps align stakeholders around a common vision and shared goals, facilitates collaboration between different groups and helps teams concentrate on users and design around their needs [249]. Hence, our multi-layered user journeys could help narrow down the disconnect between socio-technical design methods and technical engineering, and mitigate a fragmented understanding of the problem that is being solved. Some of the aspects that further empirical research should investigate in this regard include the: costs in terms of time and resources needed for conducting such investigations; complementarity to existing methods and tools employed by multi-disciplinary teams building security-critical systems; suitability of our approach in different development stages; effectiveness of the socio-technical user journeys as a communication medium for different involved stakeholders.

## 5.7 Conclusion and future work

We presented two models—that combine elements related to system-user interaction—for reasoning about the security of systems from a socio-technical perspective.

The multi-layered user journeys represent security ceremonies enriched with user insights obtained via a multitude of HCI and UX methods. The s-t transition system adds the formalization of user perceptions about aspects of interest, such as security or privacy related system values, onto standard transition systems. The inclusion of such concepts allows for reasoning about misalignments between the user's perception of security features imple-

mented in a system, and their actual implementation, thereby assisting a security analysis. We also introduced a class of security properties to express such misalignments which we tested in the context of a secure email use case. Based on the findings, we highlight the areas that could be investigated first via user studies in our use case system, which would also benefit the refinement of our model. More specifically, this refers to a user study examining the understanding of the privacy indicators provided by $p \equiv p$ and the perceptions of security that might be triggered by them.

The aim of the work presented in this Chapter was to detect security issues as a result of user misunderstandings or misperceptions of the security and privacy guarantees provided by a system during a specific interaction. Therefore, we did not consider external attackers or malfunction of the system. An analysis with specific adversary models is, however, a direction that we consider for future work.

## 5.8 Chapter Appendix

Supporting documents from this chapter are provided in Appendix B.

*Some painters transform the sun*
*into a yellow spot,*
*others transform a yellow spot*
*into the sun.*

Pablo Picasso

# 6

# Security & privacy indicators in secure email

CHAPTER ORGANIZATION. This chapter is organized in 9 sections. First, we introduce the topic and broader context of the research presented in this part of the dissertation. This is followed by an outline of related work. We then state our research objectives and present the methods, results, and analyses of two sets of user studies investigating the usability and effectiveness of user interface indicators for communicating security and privacy information to users in a secure email context. We conclude with a discussion and set forth future work directions.

## 6.1 INTRODUCTION

With the proliferation of information and communication technology, we have transferred many real-world concepts into the digital realm. While the degree of resemblance between the user interface representation and the real-world counterparts can vary among different systems (e.g., skeuomorphic design is one approach where the material look of everyday objects is borrowed in the digital representation [151, 374]), the basic idea is to enable users to interact with and via a system using concepts that they can recognize.

One such example is the notion of traffic lights. In the real world, they are universal signaling devices that control and regulate the flow of traffic, and whose mode of operation is something that we have learnt to interpret within a specific context (e.g. as drivers, pedestrians etc.). The digital counterparts, either derived directly or inspired by the traffic light semantic, can be found across various computer systems. For instance, a laptop or a smartphone battery that is fully or sufficiently charged on many systems is depicted using a *green* indicator, which changes into *amber* once the battery level is low, and ultimately into *red* if it becomes critically low. In fact, the corresponding traffic light rating system is something

we have repurposed in many different domains and in particular in systems that are security and privacy critical, where user interface representations of risks, alerts, and warnings often follow the *Red*/*Amber*/*Green* model.

While all those systems have the traffic light semantic in common, the represented concepts and their interpretation are often context-dependent and system-specific. The possibility to deploy the traffic light semantic within a specific context is fundamentally related to Ashby's "Law of Requisite Variety" [21], which here essentially means the following: a traffic light system has a finite number of states that it can represent. Consequently, a system that seeks to deploy the traffic light semantic when communicating security or privacy critical information to users needs to take into account the number of signals it can effectively send to its users.

In this regard, we were motivated to investigate whether the traffic light semantic can be effectively utilized in systems for end-to-end encryption of email. This naturally emanated from the desire to validate the preliminary findings obtained via our socio-technical security analysis of p≡p presented in Chapter 5. In order to evaluate whether the critical points in the user journey, where the formal validation failed, represent a real concern, we wanted to perform user studies which would investigate users' perceptions and potential misperceptions of traffic light-inspired indicators. Therefore, we framed our investigation within p≡p which argues to have the traffic-light semantic at its core as a "clear and easily understandable presentation" [222] of the different privacy states that messages and communication peers can have.

On the whole, our work contributes to the ongoing discussion on the usability and effectiveness of security and privacy indicators, which in the secure email context has received relatively less attention. Through two empirical studies involving 192 participants in total, we shed light on users' evaluation of traffic light-inspired indicators, used as a metaphor to represent the privacy states and guarantees that a secure email system can provide.

More concretely, our findings provide direct feedback to the developers of p ≡ p by *(i)* reporting on user research that probes p ≡ p's approach to utilizing traffic-light inspired indicators, and *(ii)* studying the adequacy of such indicators to represent desired privacy states, from a users' perspective. We also *(iii)* inform how user evaluation of an indicator differs when examined alone or as part of an indicator set, highlighting the complex relationship between different indicator cues and their interpretation with respect to security and privacy. This is relevant beyond our use case.

The next sections present the frame of our investigation, the methodology, results and analysis. We conclude with a discussion and future research directions.

## 6.2 Context and Related Work

Our focus remains on systems for *secure email*, as in the previous chapter, wherein we provided an overview of secure email preliminaries and related work. While the guarantees of *confidentiality*, *integrity*, *authenticity*, and *non-repudiation* are achieved through well-established crypto primitives, such as public-key cryptography and digital signatures, communicating in a secure and private fashion is a broader socio-technical challenge. For instance, digital signatures provide authenticity in the true sense, as long as the recipient is certain that the sender is really who they say they are (i.e., the recipient holds and trusts a public key that corresponds to the private key which signed the message). Thus, it quickly becomes evident that secure email systems need to discern many different *states* that correspond to security and privacy concepts being met or violated (e.g., is a message encrypted, is it signed, is the key trusted, mistrusted or unknown, etc.). How granular should this distinction be and how best to convey this to users?

Before we discuss related work on security indicators in the context of secure email more deeply, we provide an overview of the theoretical concepts underpinning security indicators, warnings and risk communication in computer security.

### 6.2.1 Human Factors and Warning Research

A security indicator can be understood as a medium through which security experts communicate the results of an analysis of a security-sensitive system to its users. Its role is, thus, to inform the users of the results of this security analysis with the implicit expectation that it helps users understand the implications of the result, as well as the actions that they should or should not take. In other words, its purpose is also to influence the behavior of the user. Finally, it also serves as a reminder to help a user — who may be knowledgeable of a potential threat, the associated consequences, or would otherwise exhibit the appropriate behavior — become aware of the security status of the system at a crucial point in time.

Given the numerous risks and hazards that are inherent in computer security and privacy systems, security indicators bear many of the same characteristics as warnings, which in addition to providing information, influencing behavior, and serving as a reminder, at the most general level have the purpose of making the world a safer place [212]. In the human factors and safety domain, warnings are the third line of defense in the *hazard control hierarchy* i.e., they are deployed as support tools when it is not possible or feasible to eliminate a hazard through an alternative design or prevent contact with the hazard through (procedural) safeguards [212].

Based on theoretical approaches from communication theory and human information-

processing theory, Wogalter, DeJoy, and Laughery [377] devised the C-HIP model that describes the sequence of stages through which warning information flows. In a nutshell, for a warning to be successful, it must not only capture attention and be understood, but also align with existing beliefs and attitudes and motivate users to comply [378]. As summarized by Laughery and Wogalter [212], there are a number of design and non-design factors that influence warning effectiveness, in particular regarding attention (i.e. noticing and encoding a warning) and compliance (i.e. costs-benefit trade-off decisions):

- Design factors that influence attention: size, location / placement, color / contrast, signal word, the presence of a pictorial, message length, interactivity.
- Design factors that influence compliance: the presence of a pictorial and explicitness of content (i.e., for people to make informed judgements and decisions, information needs to be presented at the right degree of specificity).
- Non-design factors that influence attention: sensory capabilities and limitations, cognitive competencies, perceived hazard, familiarity (i.e., experience with a particular or similar product or environment).
- Non-design factors that influence compliance: familiarity, modeling (social context and observing the behavior of others), and cost of compliance (money, time, effort, and convenience).

In contrast to early views which considered emotion and reason at odds with each other, research shows that cognition and emotion are closely intertwined and to a large extent cooperative [219]. Emotions, thus, have impact on attention, working memory, information processing and decision-making. Besides, there are individual as well as cultural differences in how people perceive, process, and behave toward affective stimuli [219].

There are significant methodological challenges associated with the evaluation of warning effectiveness. Nevertheless, testing by means of exposing the warning to a representative sample of the target audience and assessing specific properties (e.g. noticeability, readability, comprehension, behavioral intention and behavioral compliance), can be an effective approach that should be integrated into the warning design process [378].

### 6.2.2 Risk Communication in Computer Security

In the computer security setting, *explanations* are thought to bridge the gap between the *actual* and *perceived* security [265]. There exists, therefore, a clear need to provide appropriate feedback about security and communicate risks, so that users can make informed decisions

[40, 369]. To this end, visual feedback mechanisms have been proposed to help users operate security or defend themselves from the growing number and sophistication of attacks online.

However, research shows that computer warnings and security indicators have oftentimes been ineffective [57, 89, 206]. Users either ignore [97, 333] or do not even take notice of security indicators [299, 382], they do not understand them [92], or they underestimate the associated risks or are completely unaware of the risks [46, 92]. Users ignore warnings as they become desensitized by frequent exposure and false alarms [206]. Interruptions substantially impact alert disregard [182], while habituation (the diminishing of attention because of frequent exposure) seems to be largely obligatory as a result of how the brain processes familiar visual stimuli [14].

Mental models have been proposed as a method to improve communication to users about computer security risks [60], as well as an approach to getting insights into how users perceive and respond to computer alerts. Bravo-Lillo and colleagues highlighted that advanced and novice users observed different sets of cues, had a different interpretation of the underlying risks, and exhibited different responses [57]. As risk communication is mainly designed by computer scientists, it is often influenced by mental models of experts [46] which is problematic for many systems that rely on a "human in the loop" to perform security-critical functions [78].

Over the years, significant improvements to both warning adherence [11] and comprehension [122] have been reported in the context of web browsers, wherein much research was conducted. In contrast, the question of security indicators within systems for secure email has received relatively less attention.

### 6.2.3 Indicators in secure email

Indicators in the context of secure email are very much linked to metaphors, a number of which have been proposed in an effort to help users understand the underlying complexity of PKI [25, 282, 340]. Lausch, Wiese and Roth reviewed existing indicators used in secure email systems, and performed a comparative study to identify the ones best suited to represent the concept of email security [214]. The findings highlighted that postcards, mail envelopes, and a torn envelope emerged as promising candidates on par with the dominant padlock for signaling the encryption and integrity states.

Garfinkel and Miller investigated the effects of indicators in relation to security threats, such as social engineering and new-identity attacks [134]. They pointed out that users would need to occasionally face trust decisions, and they defined color-codes for security

indicators depending on different situations. A *yellow* indicator would appear if a digitally signed message is received from a particular address for the first time; a *green* one for subsequent messages with the same key; a *red* one if a different key is used for that address (with the possibility for users to override the code); and a *gray* one if the message is unsigned.

A similar traffic-light inspired approach can be found in p≡p, as described next.

## 6.3 p≡p

### p≡p Privacy States

As per p≡p's documentation [44, 222], and as summarized in Table 6.1, the system differentiates between 13 internal privacy rating states, which are assigned corresponding number codes, color codes and labels.

Captions and explanations are provided for a subset of the states that are visible in the user interface (UI), as shown in Table 6.2. For instance, a rating code of -3 ("Under Attack") would be assigned to incoming messages when the p≡p client would detect a man-in-the-middle (MITM) attack, communicating this to users in the UI using a red indicator.

Depending on several factors, each communication channel to different peers may have a different privacy status. For example, the system can independently and automatically categorize a particular message as *reliable* whenever it can be encrypted or decrypted with sufficient cryptographic parameters. However, certain privacy states i.e., *Mistrusted* and *Secure & Trusted*, can be reached only in combination with user interaction. To illustrate, a message would be mapped into the green color code and a green indicator would be displayed to the user provided she had at an earlier point successfully performed a verification of the correspondent's authenticity in the p≡p client. Peers can be verified to be authentic by a second-channel out-of-bound communication, e.g., a phone call where the peers verify a human-friendly version of their fingerprint. In p≡p this version is a sequence of easily readable words, called *trustwords*, taken from a dictionary according to an index that depends on the combination of the two peers' fingerprints. The implicit expectation is that users will seek to communicate in the *Secure & Trusted* state as it guarantees the highest protection possible.

### p≡p Security and Privacy Indicators

The mapping of the internal privacy states to the corresponding UI elements results in a set of indicators that follow the traffic light semantic. p≡p accounts for color-blindness in potential users by additionally providing a distinctive shape with each indicator.

| Rating Code | Rating Label | Color Code | Color Label | User Interface Label |
|---|---|---|---|---|
| -3 | under attack | -1 | red | Under Attack |
| -2 | broken | -1 | red | Broken |
| -1 | mistrust | -1 | red | Mistrusted |
| 0 | undefined | 0 | no color | Unknown |
| 1 | cannot decrypt | 0 | no color | Cannot Decrypt |
| 2 | have no key | 0 | no color | -/- |
| 3 | unencrypted | 0 | no color | Unsecure |
| 4 | unencrypted for some | 0 | no color | Unsecure for Some |
| 5 | unreliable | 0 | no color | Unreliable Security |
| 6 | reliable | 1 | yellow | Secure |
| 7 | trusted | 2 | green | Secure & Trusted |
| 8 | trusted and anonymized | 2 | green | -/- |
| 9 | fully anonymous | 2 | green | -/- |

**Table 6.1:** Overview of p≡p's internal privacy rating codes, color codes, color labels and UI labels

| User Interface Label | User Interface Explanation |
|---|---|
| Under Attack | This message is not secure and has been tampered with. |
| Broken | This message has broken encryption or formatting. |
| Mistrusted | This message has a communication partner that has previously been marked as mistrusted. |
| Unknown | This message does not contain enough information to determine if it is secure. |
| Cannot Decrypt | This message cannot be decrypted because the key is not available. |
| Unsecure | This message is unsecure. |
| Unsecure for Some | This message is unsecure for some communication partners. |
| Unreliable Security | This message has unreliable protection. |
| Secure | This message is secure but you still need to verify the identity of your communication partner. |
| Secure & Trusted | This message is secure and trusted. |

**Table 6.2:** Overview of the privacy ratings as displayed in the UI of p≡p for Thunderbird (Enigmail/p≡p version 2.0.12))

**Figure 6.1:** Default security and privacy indicators in p≡p (red, no color, yellow, green)

The default visual indicators, as implemented in p≡p for Outlook (ver. 1.1) and Thunderbird (Enigmail/p≡p ver. 2.0.12), can be seen in Fig. 6.4a. While p≡p promotes only three color codes i.e. a *red*, *yellow*, and *green* indicator, the one with color code 0 (no color) can effectively be seen as a fourth indicator in *gray* when implemented in the UI. As described in Section 6.5, the default visual indicators have in the meantime been updated/replaced with a new set of icons, partly in view of our findings presented next in Section 6.4.

#### User Studies

The following two sections (6.4 and 6.5) report on two sets of user studies conducted in line with our overarching thesis ***Objective 2*** (see Section 1.2), wherein a specific focus is placed on the role security and privacy indicators play in users' perceptions and misperceptions of system security and privacy. The findings from the first set of studies (Section 6.4) and the subsequent redesign iteration of p≡p's security and privacy indicators serve as basis for the follow-up set of studies presented in Section 6.5.

## 6.4 User Studies Set No. 1

### 6.4.1 Motivation and Objectives

The design choice for p ≡ p's security and privacy indicators was justified by arguments, but not by evidence. While discussing with the p ≡ p developers, we were told that the shapes were meant to be easily understood by color-blind persons, and were suggested after consultation with experts. The color choices were meant to reflect the universally-deployed traffic light semantic.

There are many interesting questions that could be investigated here, such as, how to draw user attention to these indicators; where to display those icons in the user interface; what privacy situations do such shapes suggest to users; are such shapes better than conventional icons used in the context of secure email (e.g., envelopes), etc. In the first place, however, we sought to conduct a preliminary inquiry into how prospective or first-time p≡p users would understand the p≡p privacy indicators at the most basic level.

Formally stated, we intended to shed light on the following research questions:

**Q1** Which of the 4 visual icons do users associate with the different p≡p privacy ratings?

**Q2** Which of the 4 visual icons do users associate with the different p ≡ p privacy rating explanations?

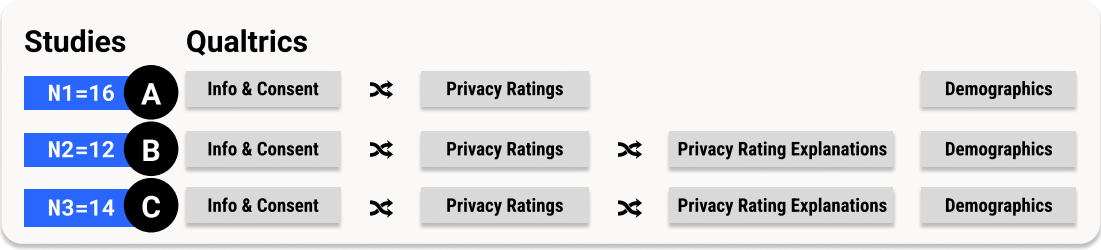



**Figure 6.2:** Conceptual overview of the User Studies Set No. 1

### 6.4.2 Methodology

In Q2 of 2019, we conducted three preliminary online studies to assess how people would interpret the various privacy rating indicators offered by the p≡p email encryption system. Figure 6.2 provides an overview of the user test sessions, the number of participants per session as well as the focus of investigation.

#### Study structure

At the beginning of each session, participants were informed about the nature of the study before they could voluntarily choose to commence the study and continue to the questions. The first part of the study, called Privacy Ratings, contained a block of 10 questions which asked participants to choose an icon which according to them best corresponded to a given privacy statement i.e., rating. The upper part in Figure 6.3 shows an example of questions belonging to this block. The second part of the study, called Privacy Rating Explanations, similarly asked the participants to match an icon to a privacy rating explanation (see Figure 6.3 lower part). The last part of the study asked about demographics. The 10 privacy rating statements and explanations were drawn from the p≡p for Thunderbird distribution (Enigmail/p≡p version 2.0.12 (20190707-1417)). To minimize order bias, the sequence of all questions per block was randomized for each test participant. The order of all answer choices (icons) per question was also randomized. The studies were administered via Qualtrics*.

#### Participants

All participants were relatively tech-savvy, with at least a Bachelor's degree. The participants of Session A and B were based in Luxembourg and were recruited at the University of Luxembourg via an email invitation to participate in a pilot study (Session A) and during

*https://www.qualtrics.com, accessed on January 15, 2022

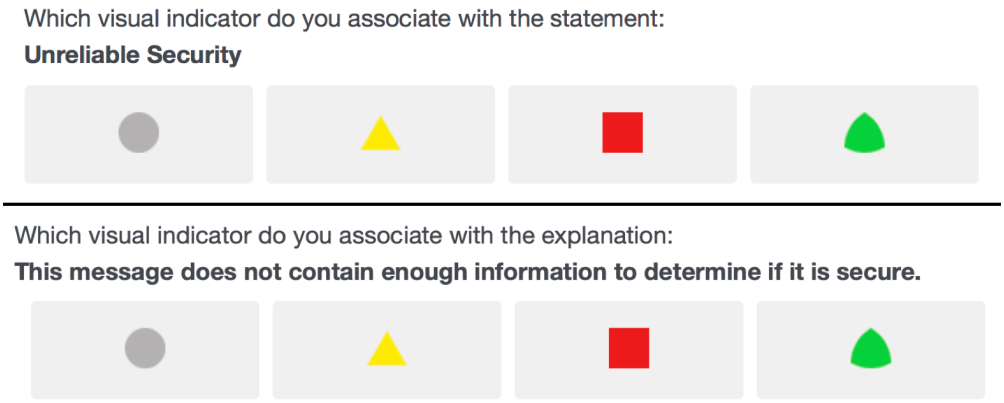



**Figure 6.3:** Sample questions asking participants to choose the icon which according to them best corresponds to a given privacy statement i.e., rating (*upper question*), and a privacy rating explanation (*lower question*).

a lecture on Security Engineering (Session B). No incentive was offered to the participants of Sessions A and B. The participants of Session C were based in different European countries and were recruited in Portugal during a workshop on User Experience in security and privacy-critical systems. As a compensation for their participation in the study, all participants of Session C were offered a commercial license of p≡p for continued use of their paid apps i.e., the Outlook and Android distributions.

### Analysis

We performed a comparative analysis to understand if our participants associated icons to the various privacy ratings and explanations in the same way as implemented by p≡p. If the icon chosen by the majority of participants was the same as the one chosen by p≡p, the alignment test for that rating or explanation equaled "MATCH", and otherwise "NO MATCH".

The *Match strength* refers to how many participants selected the same icon as p≡p. Hence, the higher the match, the narrower the gap between what the developers wanted to communicate via the system and what the users understood. Similarly, the lower the match, the higher the ambiguity of the intended privacy indicator.

## 6.4.3 Results

Table 6.3 summarizes the participant responses, detailing the distribution of votes per icon for each rating statement and explanation. The distribution under the most voted icon by the participants is formatted in bold letters. The number of people that had voted for the

| ITEM | | PRIVACY RATINGS (Statements & Explanations) | PARTICIPANTS' RESPONSES (%) | | | | | p≡p's CHOICE | MATCH STRENGTH | RESULT |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | 🟢 | ⚪ | 🟥 | 🔺 | Most voted | | | |
| 1 | Q1 | Under Attack | 0.0 | 2.4 | **76.2** | 21.4 | 🟥 | 🟥 | 76% | MATCH |
| 1 | Q2 | This message is not secure and has been tampered with. | 0.0 | 11.5 | **69.2** | 19.2 | 🟥 | 🟥 | 69% | MATCH |
| 2 | Q1 | Broken | 2.4 | 16.7 | **59.5** | 21.4 | 🟥 | 🟥 | 60% | MATCH |
| 2 | Q2 | This message has broken encryption or formatting. | 0.0 | 0.0 | 38.5 | **61.5** | 🔺 | 🟥 | 38% | NO MATCH |
| 3 | Q1 | Mistrusted | 2.4 | 14.3 | 40.5 | **42.9** | 🔺 | 🟥 | 40% | NO MATCH |
| 3 | Q2 | This message has a communication partner that has previously been marked as mistrusted. | 3.9 | 0.0 | 23.1 | **73.1** | 🔺 | 🟥 | 23% | NO MATCH |
| 4 | Q1 | Unknown | 0.0 | **78.6** | 2.4 | 19.1 | ⚪ | ⚪ | 79% | MATCH |
| 4 | Q2 | This message does not contain enough information to determine if it is secure. | 3.9 | 23.1 | 11.5 | **61.5** | 🔺 | ⚪ | 23% | NO MATCH |
| 5 | Q1 | Cannot Decrypt | 7.1 | 28.6 | **42.9** | 21.4 | 🟥 | ⚪ | 29% | NO MATCH |
| 5 | Q2 | This message cannot be decrypted because the key is not available. | 0.0 | 38.5 | 19.2 | **42.3** | 🔺 | ⚪ | 38% | NO MATCH |
| 6 | Q1 | Unsecure | 0.0 | 11.9 | **69.1** | 19.1 | 🟥 | ⚪ | 12% | NO MATCH |
| 6 | Q2 | This message is unsecure. | 0.0 | 7.7 | **61.5** | 30.8 | 🟥 | ⚪ | 8% | NO MATCH |
| 7 | Q1 | Unsecure for Some | 2.4 | 9.5 | 16.7 | **71.4** | 🔺 | ⚪ | 10% | NO MATCH |
| 7 | Q2 | This message is unsecure for some communication partners. | 0.0 | 11.5 | 19.2 | **69.2** | 🔺 | ⚪ | 12% | NO MATCH |
| 8 | Q1 | Unreliable Security | 2.4 | 14.3 | 26.2 | **57.1** | 🔺 | ⚪ | 14% | NO MATCH |
| 8 | Q2 | This message has unreliable protection. | 0.0 | 15.4 | 19.2 | **65.4** | 🔺 | ⚪ | 15% | NO MATCH |
| 9 | Q1 | Secure | **90.5** | 7.1 | 2.4 | 0.0 | 🟢 | 🔺 | 0% | NO MATCH |
| 9 | Q2 | This message is secure but you still need to verify the identity of your communication partner. | 0.0 | 19.2 | 7.7 | **73.1** | 🔺 | 🔺 | 73% | MATCH |
| 10 | Q1 | Secure & Trusted | **95.2** | 4.8 | 0.0 | 0.0 | 🟢 | 🟢 | 95% | MATCH |
| 10 | Q2 | This message is secure and trusted. | **100.0** | 0.0 | 0.0 | 0.0 | 🟢 | 🟢 | 100% | MATCH |

**Table 6.3:** Results of the preliminary investigation of alignment between participants' associations of p≡p privacy ratings, explanations and visual icons against the actual associations as implemented by default in several applications of p≡p at the time of the investigation. (For each item, the match strength refers to the percentage of participants that associated an icon to a statement or explanation in the same fashion as it was implemented by p≡p.)

same icon as implemented in p≡p at the time of the investigation is underlined. Hence, in case of a *match*, the distribution of the icon is formatted as bold and underlined.

These preliminary results highlighted profound differences in what p≡p tried to convey to users in terms of the security and privacy rating of messages and how prospective or first-time p≡p users would interpret those ratings. The icon displayed by p≡p matched the association made by the test participants in only 4 out of 10 cases. When it comes to rating explanations, there was a match only in 3 out of 10 cases. There was additionally the internal inconsistency in the case of Items 2, 4 and 9 where either the statement or the corresponding explanation matched the icon choice of the study participants, but not both. When looking at the ratings and explanations combined, there was a match in 7 out of 20 cases.

While we can notice a strong alignment between the choice made by p≡p and the study participants in the case of a fully secure rating (Item 10 i.e., "Secure & Trusted" and its corresponding explanation), the alignment is less strong on the other end of the spectrum (Items 1 and 2). In all other cases (except for Item 4) the associations people made were different from the intentions of the designers. This is even more worrying given the fact such indicators would very likely be shown before the ones on the extremes of the rating spectrum (e.g., existing email messages or those received/sent unencrypted after installing p≡p would have the privacy rating "Unsecure").

The match strength was the lowest (=0%) in the case of Item 9-Q1. The results suggested that if p≡p displayed a yellow triangle as a visual indicator of a privacy rating for a message, no prospective or first-time user would associate it with a "Secure" status, which is contrary to what p≡p tried to communicate. This is probably not too surprising given our constant pattern recognition efforts [120] in combination with the ubiquity of the triangle in hazard alerting or warning symbols [315]. Unfortunately, without a deeper understanding of how secure email works or any additional context, such as an explanation (Item 9-Q2), it is hard for users to foresee why p≡p would be trying to denote that the message is "Secure", yet cautiously.

### 6.4.4 Discussion

Understanding why there was a dichotomy between what the developers wanted to convey with the different privacy indicators in p≡p and how prospective users would interpret them, or which privacy indicators could be better in narrowing this chasm, was not in the scope of the investigation. Nevertheless, we hypothesize that the following elements potentially play a role:

- the shapes of the indicators;
- the colors of the indicators;
- the choice of words in the statements and explanations;
- the perception of risk associated with the shapes, colors, metaphor and wordings of the indicators;
- the clustering of risks;
- the understandability of the indicators;
- the awareness and concern about different scenarios and privacy ratings.

It is often the case that visual input tends to dominate other modalities when it comes to our perceptual and memorial judgements [267]. Color is one of the characteristics of human visual perception that can carry important meaning and can have an important impact on people's affect, cognition, and behavior [103]. According to Elliot & Maier's color-in-context theory [102], some color meanings and effects are biologically-based, while others are posited to stem from the repeated pairing of color and particular concepts, messages, and experiences. The authors state that observing color-meaning associations over time and cultures can contribute to reinforcing and extending the applicability of those links to objects in the broader environment, such as signs and signals. We did not have the opportunity to perform this investigation with existing p≡p users. We would be interested in comparing such results with the current findings and looking at the role of experience with the system on the interpretation of the privacy ratings and indicators.

Disregarding some regional variations, traffic signs and traffic lights are now found all over the world, and their meaning is internationally recognizable. The corresponding traffic light rating system (*red, amber, green*) is something we have repurposed in many different domains, from nutrition labels for pre-packed products [349] to energy consumption labeling [114] and project management status reporting [111], to name a few. In that respect, the provision of the traffic light color codes can serve to communicate more accurate, relevant, and comparable information to users, as well as to transmit certain levels of risk or allow for a quick recognition of potential hazards. Nevertheless, while signs and pictograms have been standardized in specific areas, in many different contexts harmonized communication or a shared understanding of the risk communicated by signs, symbols, or colors cannot be taken for granted [315]. The reasons can range from cross-cultural differences [177] to varying levels of technical expertise within a specific domain. As mentioned earlier, the number of different situations that arise in secure email is not so small. Deciding which ones and how many to represent graphically, as well as, which metaphor to use, is not an easy choice.

Furthermore, there are differing views about how transparent should systems for secure email be [23, 285]. In the case of Item 9, it is evident that p≡p attempted to find the balance between these two approaches: on the one hand the system would like to instill a sense of security provided by the automatic end-to-end encryption akin to other secure messaging and emailing systems, but on the other hand, the system would still like to warn users of potential threats such as a man-in-the-middle attack that they could be susceptible to if they do not verify the corresponding party via a second secure channel (e.g., by comparing the trustwords in person or over the phone).

While over time, we might be able to recognize more consistency in the symbols used by security and privacy-critical systems, including secure email, in the immediate term, developers of such systems should devote an equal amount of attention and resources to understanding their (target) users and the different dimensions and requirements of their socio-technical proposition. Fine-grained inspiration could perhaps be drawn from the vast body of work on browser security indicators and warnings (e.g., [11, 122, 271]), in particular, the incremental user-centered approach where proposed designs and changes were validated with thousands of users. Caplin's book [61] could potentially be a useful reference to some developers in the specific context of icons in computer interface design, however, as pointed out by Felt et al. "Millions of Internet users have recently come online via smartphones without learning 'standard' iconography from desktop browsers" [122], thus it is important to acknowledge that the expectations of users in terms of interfaces are not necessarily associated with desktop computing and, in many cases, obsolete metaphors.

### 6.4.5 Summary and Next Steps

We reported on a 42-participant study of users' perceptions of email privacy ratings in the context of p ≡ p. Although our preliminary study had an evident limitation mainly due to the limited sample size, the outcome suggested that prospective or first-time p≡p users would have a difficulty understanding the privacy information communicated by p≡p though its security and privacy indicators.

The findings called for a broader and deeper investigation that would seek to assert which design choices in terms of the privacy rating statement, explanation and visual icon (shape, colour, metaphor etc.) would need to be reconsidered if p≡p would like to accurately communicate the degree of protection that it offers to its users as they send and receive email through its system bearing in mind their experience, awareness and concerns. We are of the opinion that despite looking trivial, this interaction experience should not be in the way of users adopting systems for end-to-end email encryption, let alone a source of confusion or

frustration that could result in unsecure behavior or unwanted leakage of confidential information. This is particularly relevant within an organizational setting, where policy and culture may also contribute towards the way users go about employing end-to-end email encryption systems.

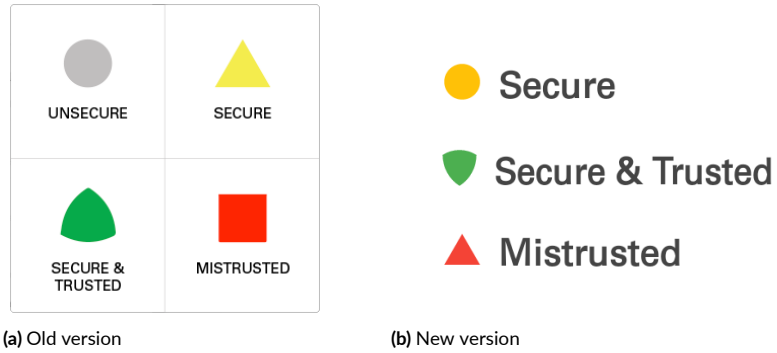
We believe that communicating the results of our preliminary findings helped trigger a deeper discussion at p≡p on the existing icon design choices. As explained next, p≡p subsequently overhauled the security and privacy indicators in their different app distributions which we used as basis for further investigations of the traffic-light inspired metaphor.

## 6.5 User Studies Set No. 2

### 6.5.1 Motivation and Objectives

#### p≡p Indicators – Revisited

Interacting with updated versions of p≡p and contacting the developers, we learned that p≡p updated the indicator shapes, while keeping the color codes and traffic light metaphor. In the new version, shown in Figure 6.4b, *Mistrusted* is represented with a red triangle, *Secure* with a yellow/amber circle, and *Secure & Trusted* with a green shield pointing downwards. As per the Android onboarding tutorial (ver. 1.1.008), there is no *gray* indicator, and it appears to be left out in the UI.




**(a)** Old version **(b)** New version

**Figure 6.4:** Security and Privacy indicators in p≡p

Aspiring to highlight the importance of early user research in the development process of privacy-enhancing tools, in this study we were driven by the following questions:

- How do we compare different design alternatives that try to convey specific information via the traffic light semantic?

- Which of the proposed indicators do end-users find appropriate for the designated privacy states?
- Does the perception about a traffic light indicator change when it is considered as part of an indicator set, rather than individually?

To this end, we formulated the following hypotheses:

**H1 — H3:** The majority of participants would select the new versions of the icons over the old versions for each of the three privacy states *Mistrusted*, *Secure*, and *Secure & Trusted*.

**H4:** The majority of participants would express agreement that the new version of the icon (red triangle) is a good representation of the text *Mistrusted*.

**H5:** The majority of participants would *not* express agreement that the new version of the icon (yellow circle) is a good representation of the text *Secure*.

**H6:** The majority of participants would express agreement that the new version of the icon (green shield pointing downwards) is a good representation of the text *Secure & Trusted*.

**H7:** Onboarding has a positive effect i.e. participants exposed to a priming screen displaying the whole indicator set, express higher agreement scores versus non-primed participants across all three states.

## 6.6 Methodology

In order to test our hypotheses we conducted three independent, within-subject experiments, Study D, E and F, as described below. Each was organized according to a within-subject design as visible in the conceptual overview in Fig. 6.5.

**Recruitment.** The study participants were recruited via the platform Prolific[†]. Given that the icons in the investigation had different colors, we restricted the participation to those that could see color normally. In total, 152 participants were recruited, thereof 150 were eligible and taken into consideration (50 per study). To ensure independence of the experiments and exclude any accidental participant overlap, the studies were conducted sequentially and all participants were "blocked" for further recruitment.

**Survey.** The experiments were conducted online. We administered one survey per study via Qualtrics.

[†] https://www.prolific.co/, accessed on January 15, 2022

**Ethics.** Our study was approved by our organization's ethics review panel, and we obtained informed consent from all subjects.

**Compensation.** The participants were informed that it would take them about 3 minutes to complete the survey. They were compensated £0.25 for their participation, which corresponded to Prolific's fair rewarding practice of at least £5.00 ($6.50) per hour.

### 6.6.1 Experiment protocol

**Information and Consent.** At the beginning of all studies, the participants were prompted that the survey is part of an investigation that aims to research and improve the UX of products and systems for secure messaging, in particular secure email. We informed them that we are interested in understanding how icons can be used for communicating different levels of privacy for messages exchanged in such systems. After consenting to take part in the study and confirming that they see color normally, depending on which study the participants were part of, they were shown three consecutive questions, as described below.

**Study D (H1 — H3).** First we wanted to investigate how participants would evaluate or score the two sets of icons with respect to the privacy states that they are supposed to represent. The purpose was to understand among prospective p ≡ p users, the preference between the old and new versions of the icons designated to represent three different privacy states i.e. *Mistrusted*, *Secure*, and *Secure & Trusted*. Preference, here, refered to the selection of one icon alternative over the other, based on the perceived fitness of the icon with the corresponding privacy state, labeled under each icon.

Fig. 6.6 features the question set shown to each participant, each shown on a separate page. To counterbalance possible biases, the order of the questions and answer options was randomized.

**Study E (H4 — H6).** Next we wanted to find out how strong is the presumed fitness be-

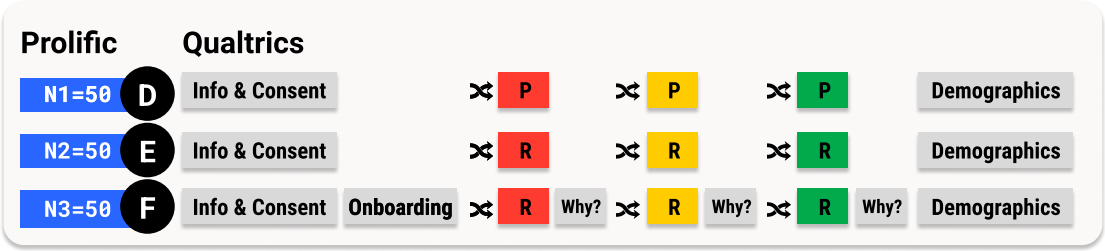



**Figure 6.5:** Conceptual overview of our investigation. *P* refers to the 3 preference questions asked in Study D (Fig. 6.6); *R* to the 3 rating questions in Study E and F (Fig. 6.7); *Why?* to the optional *Why do you think so?* question in Study F; the red, amber and green colors refer to the states *Mistrusted*, *Secure*, and *Secure & Trusted*, respectively, shown to each participant in a randomized fashion.

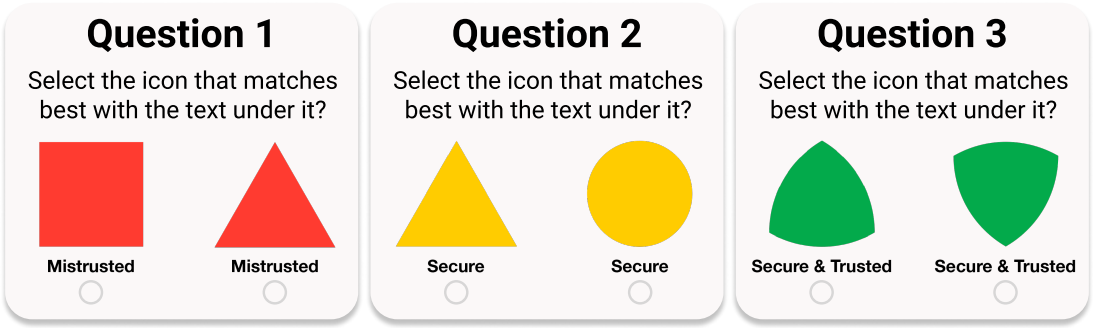



**Figure 6.6:** The three preference questions shown in Study D

tween the proposed icon and the corresponding label. In other words, while a new version of an icon might be better than its predecessor, it does not mean that it is a good representation for the privacy concept that it is supposed to convey. As exemplified in Figure 6.7, each Study E participant was shown, in a randomized fashion, a set of three questions, asking her to state on a 7-point rating scale how much she agreed or disagreed with the statement that the displayed icon was a good representation of the text under it. Only the new versions for each of the three privacy states were displayed.

**Study F (H4 — H7).** Finally, we conducted a follow-up investigation almost identical to Study E, whereby the traffic light semantic was made more explicit. This was done to see if there was an effect of the onboarding on the evaluation of the individual fitness of the indicators. Thus, the crucial difference was the inclusion of an onboarding screen, where all three icons were displayed all-together on a page, before the Likert item questions were randomly shown to participants, as in Study E (Fig. 6.7). Another minor change was that along with each rating question, a non-mandatory free-entry question *"Why do you think so?"* was also shown. This was done in order to gather additional input and try to understand, whenever possible, what reasoning backed the fitness scores that the participants gave.

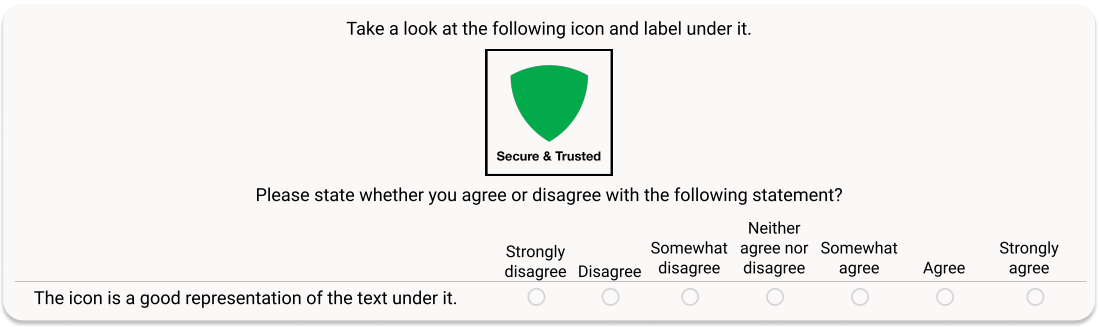



**Figure 6.7:** One of the three main rating questions (one per privacy state) shown to each participant in Study E and in Study F.

**Demographics.** At the end of all experiments, there was a demographics section where we inquired if our participants had a computer science / technical background and whether they had ever used systems for end-to-end encryption (E2EE) of email. Those that affirmed, were further asked to name the systems that they use or had used in the past. We asked this to establish any skewness of our sample towards privacy-aware and tech-savvy users.

## 6.7 Results and Analysis

### 6.7.1 Participants

Table 6.4 provides an overview of the main participant demographics. Our sample consisted of participants that had different technical skills and experience with systems for secure email. PGP and Protonmail were mentioned most frequently as tools/systems that they used or had used in the past. No participant mentioned $\mathsf{p} \equiv \mathsf{p}$.

| **Demographics** | **Study D** | **Study E** | **Study F** |
|---|---|---|---|
| Female | 28 (56%) | 22 (44%) | 18 (36%) |
| Male | 19 (38%) | 28 (56%) | 32 (64%) |
| No attribution | 3 (6%) | 0 | 0 |
| Average age | 28 | 32 | 29 |
| Age range | [18 – 46] | [18 – 63] | [18 – 69] |
| English as first language | 28 (56%) | 21 (42%) | 13 (26%) |
| Student status | 19 (38%) | 19 (38%) | 13 (26%) |
| Computer Science / tech background | 16 (32%) | 22 (44%) | 14 (28%) |
| Use of E2EE systems | 13 (26%) | 14 (28%) | 10 (20%) |

**Table 6.4:** Participant demographics. N=50 for each study.

### 6.7.2 Quantitative analysis

**Study D**

The proportions of icon preference were estimated using exact binomial tests. The results, displayed in Table 6.5 and Fig. 6.8, confirmed H1 — H3 that, for each state, the majority of participants would select the new versions of the icons over the old ones.

The new version was selected as the one that better matches with the text under it in 40/50 times in the case of the *Mistrusted* and *Secure* privacy states. For *Secure & Trusted*, it was 47/50 times. The confidence intervals for the new versions are way above chance performance of $\Pi_0 = .5$ ( $p < .001$), confirming H1, H2 and H3.

| State | Version | # | Count | % | Proportion | | 95% CI* | Mean | SD | Var |
|---|---|---|---|---|---|---|---|---|---|---|
| M | Old | 1 | 10 | 20% | $P_{M\text{-}1}$ | 0.2 | [.1124, .3304] | 1.80 | .404 | .163 |
| | New | 2 | 40 | 80% | $P_{M\text{-}2}$ | 0.8 | [.6696, .8876] | | | |
| | Total: | | 50 | 100% | | 1 | | | | |
| S | Old | 1 | 10 | 20% | $P_{S\text{-}1}$ | 0.2 | [.1124, .3304] | 1.80 | .404 | .163 |
| | New | 2 | 40 | 80% | $P_{S\text{-}2}$ | 0.8 | [.6696, .8876] | | | |
| | Total: | | 50 | 100% | | 1 | | | | |
| S&T | Old | 1 | 3 | 6% | $P_{ST\text{-}1}$ | 0.06 | [.0206, .1622] | 1.94 | .240 | .058 |
| | New | 2 | 47 | 94% | $P_{ST\text{-}2}$ | 0.94 | [.8378, .9794] | | | |
| | Total: | | 50 | 100% | | 1 | | | | |

*CI method: Wilson Score interval

**Table 6.5:** Study D - Statistics and Frequency Table

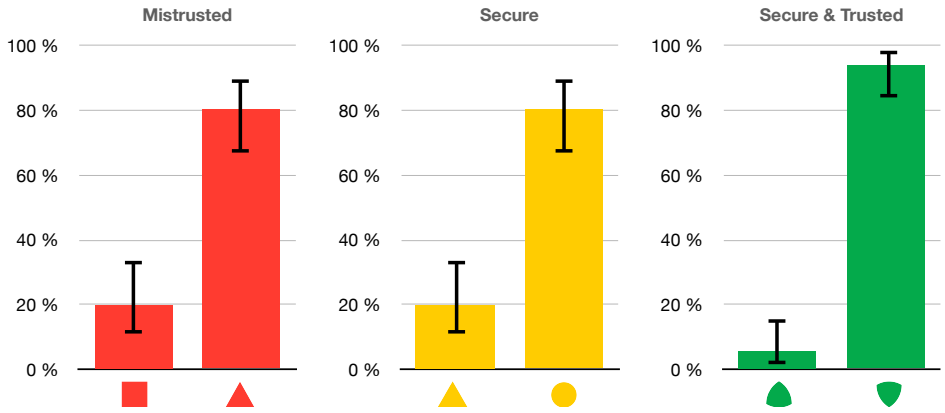



**Figure 6.8:** Study D - Proportions of frequencies of the two icon versions per privacy state (old *vs* new)

### Study E and Study F

Figures 6.9 and 6.10 show the distributions of the responses to the three rating questions from Study E and F. As visible in the figures and summarized in Table 6.6, the majority of participants expressed agreements that the icon is a good match for the text for the *Mistrusted* and *Secure & Trusted* privacy states in both studies. These high agreement scores were in contrast to the ones expressed for the privacy state *Secure*.

**Mistrusted:** The combined (Study E and Study F) agreement score denotes that the percentage of participants that either *Strongly agree*, *Agree* or *Somewhat agree* that the red triangle is a good representation for *Mistrusted* is **81% [72.22, 87.49]**. This is way above the benchmark of 50% of participants, thus confirming Hypothesis 4. Onboarding appears to be associated with an increase of the aggregated agreement score of 18 percentage points,

| State | Strongly disagree | Disagree | Somewhat disagree | Neither agree nor disagree | Somewhat agree | Agree | Strongly agree | Total |
|---|---|---|---|---|---|---|---|---|
| ▲ | 4 | 2 | 4 | 4 | 15 | 16 | 5 | 50 |
| M | 8 % | 4 % | 8 % | 8 % | 30 % | 32 % | 10 % | 100 % |
| ● | 3 | 17 | 17 | 9 | 2 | 2 | 0 | 50 |
| S | 6 % | 34 % | 34 % | 18 % | 4 % | 4 % | 0 % | 100 % |
| ♥ | 1 | 1 | 2 | 1 | 6 | 19 | 20 | 50 |
| S&T | 2 % | 2 % | 4 % | 2 % | 12 % | 38 % | 40 % | 100 % |

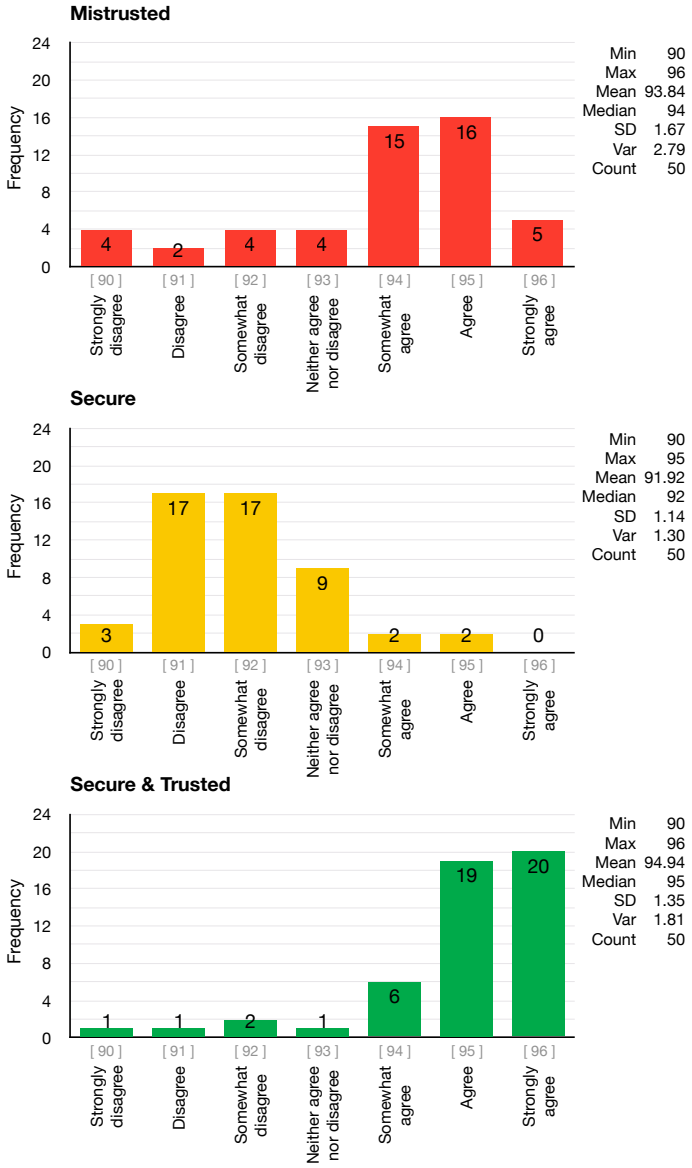



**Figure 6.9:** Frequency histograms for participant responses to the three main rating questions in Study E (i.e. without onboarding). The 7 response categories are ordered and assigned numerical codes [90 to 96] on the x-axis.

| State | Strongly disagree | Disagree | Somewhat disagree | Neither agree nor disagree | Somewhat agree | Agree | Strongly agree | Total |
|---|---|---|---|---|---|---|---|---|
| ▲ | 2 | 1 | 1 | 1 | 9 | 21 | 15 | 50 |
| M | 4 % | 2 % | 2 % | 2 % | 18 % | 42 % | 30 % | 100 % |
| ● | 4 | 10 | 11 | 5 | 11 | 8 | 1 | 50 |
| S | 8 % | 20 % | 22 % | 10 % | 22 % | 16 % | 2 % | 100 % |
| ♥ | 0 | 0 | 0 | 0 | 2 | 24 | 24 | 50 |
| S&T | 0 % | 0 % | 0 % | 0 % | 4 % | 48 % | 48 % | 100 % |

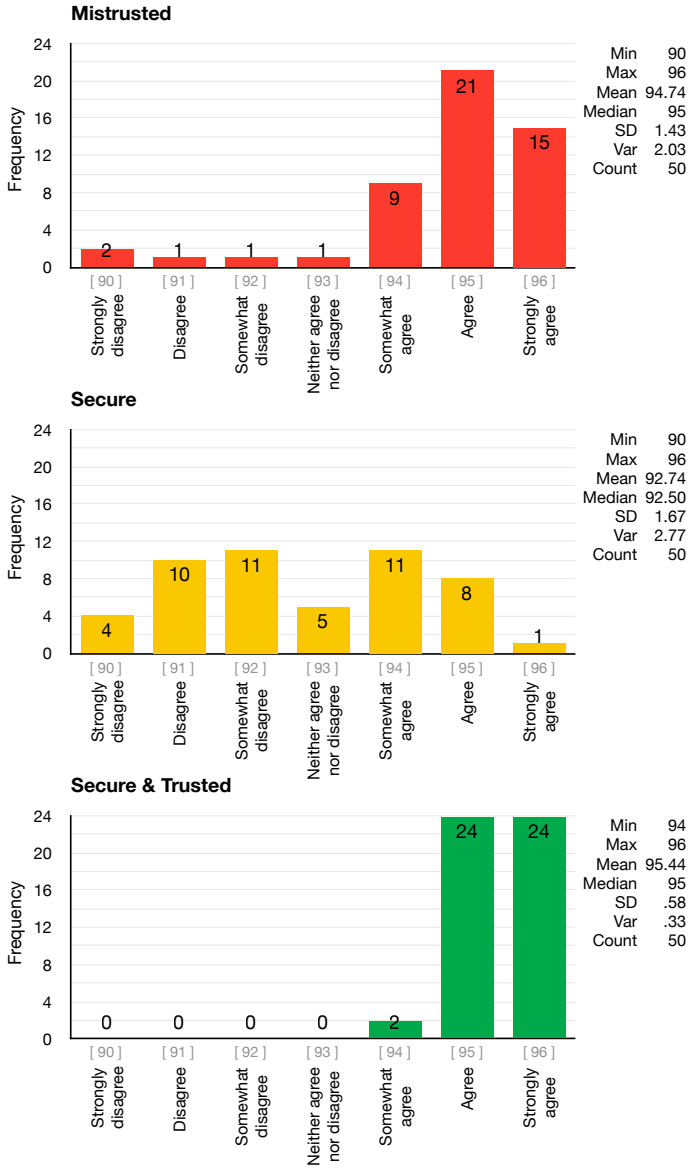



**Figure 6.10:** Frequency histograms for participant responses to the three main rating questions in Study F (i.e. with onboarding). The 7 response categories are ordered and assigned numerical codes [90 to 96] on the x-axis.

| Study | State | Agreement | 95% CI |
|---|---|---|---|
| E | Mistrusted | 72% | [58.33, 82.53] |
| F | Mistrusted | 90% | [76,84, 95.65] |
| Combined | Mistrusted | 81% | [72.22, 87.49] |
| E | Secure | 8% | [3.15, 18.84] |
| F | Secure | 40% | [27.61, 53.82] |
| Combined | Secure | 24% | [16.69, 33.23] |
| E | Secure & Trusted | 90% | [78.64, 95.65] |
| F | Secure & Trusted | 100% | [92.87, 100] |
| Combined | Secure & Trusted | 95% | [88.82, 97.85] |

**Table 6.6:** Aggregated percentage of participants that *Somewhat agree*, *Agree* or *Strongly agree*. (*CI method: Wilson score*)

from 72% in Study E (no onboarding screen) to 90% in Study F (with onboarding).

**Secure:** The percentage of participants in Study E that express agreement that the yellow circle is a good representation for the text *Secure* is 8% [3.15, 18.84]. Providing an onboarding screen is associated with an increase of the aggregated agreement score of 32 percentage points to 40%. Nevertheless, the 95% confidence interval around the percentage of primed participants who would express agreement is between 27.61% and 53.82%, denoting that we do not have convincing evidence that the majority of participants would be in agreement. The combined (Study E and Study F) agreement score for the *Secure* privacy state is **24% [16.69, 33.23]**, way below the benchmark of 50%, thus confirming Hypothesis 5.

**Secure & Trusted:** The highest agreement scores were expressed for the green shield icon and the *Secure & Trusted* label. The combined (Study E and Study F) agreement score is **95% [88.82, 97.85]**, thus confirming Hypothesis 6. Onboarding is associated with an increase of 10 percentage points, from an already high 90% to 100%.

The agreement scores and associated confidence intervals are above the benchmark of 50% even if we take a more conservative approach by excluding the *Somewhat agree* category from our aggregated agreement frequency count. In this case, the percentage of those that *Agree* or *Strongly agree* is 78% [64.76, 87.25] for Study E, 96% [86.54, 98.9] for Study F, and 87% [79.02, 92.24] combined for Study E and F.

### Differences in agreement scores across different categories of onboarding (between-subject)

Mann-Whitney U tests were run to determine if there were differences in the agreement score between study participants that were exposed to an onboarding screen (primed) and

not i.e. Study C *versus* Study B.

*Mistrusted*: Distributions of the agreement scores for both groups were similar, as assessed by visual inspection. Median agreement score was statistically significantly higher for primed participants (95) than for non-primed ones (94), $U = 1712$, $z = 3.308$, $p = .001$.

*Secure*: Distributions of the agreement scores for primed and non-primed participants were not similar, as assessed by visual inspection. Agreement scores for non-primed participants (mean rank = 43.48) were statistically significantly lower than for primed participants (mean rank = 57.52), $U = 1601$, $z = 2.480$, $p = .013$.

*Secure & Trusted*: Distributions of the agreement scores were similar, as assessed by visual inspection. Median agreement score was not statistically significantly different between primed and non-primed participants, $U = 1468$, $z = 1.645$, $p = .100$.

While participants in Study F expressed higher agreement scores than those in Study E, the Mann-Whitney U tests above indicate that this difference was statistically significant only for the *Mistrusted* and *Secure* privacy states, thus Hypothesis 7 is only partially confirmed. It is important to note, however, that the agreement score in Study E was already high at 90%.

#### Differences in agreement scores based on technical background (between-subject)

Further Mann-Whitney U tests were run to determine differences among participants with and without a technical / computer science background. The agreement scores were not statistically significantly different.

- *Mistrusted*: $U = 1249.5$, $z = .727$, $p = .467$.
- *Secure*: $U = 1252.5$, $z = .740$, $p = .460$.
- *Secure & Trusted*: $U = 1179$, $z = .212$, $p = .832$.

### 6.7.3 Qualitative analysis

Input to the optional *"Why do you think so?"* question in Study F, was provided by 33 participants for the *Mistrusted*, 37 participants for the *Secure*, and 32 participants for the *Secure & Trusted* state. Based on this data, we performed inductive category formation. Table 6.7 provides an overview of the main themes identified per privacy state.

#### Mistrusted

As summarized in Table 6.7, column (M), and as visible from the following verbatims, participants tended to agree that the color of the *Mistrusted* indicator is appropriate, but they

| Themes | Theme frequency per state | | | |
|---|---|---|---|---|
| | M | S | S&T | **Total** |
| **Indicator characterization** | | | | |
| - The color is adequate | 24 | 4 | 24 | **52** |
| - The color is not adequate | 2 | 18 | 0 | **20** |
| - The shape is adequate | 8 | 2 | 20 | **30** |
| - The shape is not adequate | 7 | 9 | 2 | **18** |
| - The indicator is confusing | 0 | 9 | 0 | **9** |
| **Indicator interpretation** | | | | |
| - Traffic light semantic | 2 | 5 | 7 | **14** |
| **Evocation of feelings** | | | | |
| - Sense of security | 0 | 3 | 22 | **25** |
| - Sense of reassurance | 1 | 1 | 14 | **16** |
| - Sense of caution | 10 | 12 | 0 | **22** |
| - Sense of danger | 15 | 1 | 0 | **16** |

**Table 6.7:** Overview of the most frequent themes emerging from the data during the qualitative analysis.

were divided when it comes to the shape of the indicator.

- *"the triangle does not make me think mistrusted or problematic. Red is a good choice tho."* (P107)
- *"It is bold and makes you stop and think. Red is a good representation of danger."* (P111)
- *"the red colour is a good warning sign, the colour is powerful so would catch your attention."* (P112)
- *"Colour is adequate, geometrical form could be better"* (P115)

As hinted in the verbatims above, the indicator was mostly associated with *danger* and *caution*.

### Secure

The most frequent themes under the (S) column in Table 6.7 and the representative verbatims below provide first insights as to why the indicator received a poor overall score in the 7-point rating question. In most cases, the color choice for the indicator was criticized for not being representative of the concept of *Security*:

- *"secure is usually in a green symbol."* (P102)
- *"the yellow represents a colour which is not secure nor unsecure, in my opinion."* (P105)

- *"color doesn't seem to scream safe to me."* (P108)
- *"the yellow color doesn't seems to be so secure at all."* (P144)

These were accompanied by comments of *doubt* and *confusion*:

- *"not so sure that this indicates security."* (P114)
- *"to some, the color could be misleading."* (P139)

Participants also voiced the inadequacy of the circle:

- *"The shape is not good. I'd like prefer yellow shield."* (P119)
- *"'Secure' usually indicates a shield icon should be used."* (P124)
- *"circle isn't a particularly distinctive symbol."* (127)
- *"it should be shield image, it looks safe, not circle."* (P140)

In fact, the large number of low agreement scores provided in the rating question can also be explained by the participant association of the indicator with a *Sense of caution* rather than a *Sense of security*:

- *"I associate it with the yellow light in traffic, that in my country means proceed with caution."* (P117)
- *"Yellow signals warning for me so I would not feel it is secure."* (P128)
- *"Shape isn't anything special, additionally yellow colour associate, as if something dangerous."* (P143)

In contrast, there was also a small number of participants who associated the indicator with *caution*, yet expressed positive agreement scores for the corresponding rating question:

- *"As yellow is like amber use with caution."* (P106)
- *"Yellow generally means caution."* (P116)
- *"I personally relate it to the traffic light, it is not dangerous but it does not tell me that I am sure."* (P120)

While we hypothesize that $p \equiv p$ envisions users to interpret the *Secure* indicator as in the above three verbatims, our results suggest that this feeling of *"self-reflective security"* (which we discuss in Section 6.8) is evoked only in a minor proportion of the users.

**Secure & Trusted**

Given that the agreement scores for this state were only positive (see Figure 6.10), most comments, were confirmations of the adequacy of the color and shape of the indicator. Participants mentioned positive associations, such as *Sense of security* (22 times), and *reassurance* (14 times). A reference to a *Traffic Light Semantic* was observed 7 times. Representative verbatims include:

- *"I feel like green is colour of safety and that shape looks kind of shield. All of it makes me feel really secure and trusted."* (P143)
- *"The shield shape and the green colour are a trustworthy and appear regularly on computer programs."* (127)
- *"The color and shape make me feel at ease. I am used to green meaning go from driving so perhaps that has something to do with it as well."* (P111)

Nevertheless, the challenge of representing *trust* and the insufficiency of the shield icon to represent both the concepts of *security* and of *trust* was highlighted too:

- *"With a shield look to it, it looks like things should be okay to proceed. but I think it needs something else for the 'Trusted' part like a little start on it or a banner badge."* (P124)
- *"good representation for secure, but I think a different icon should be used for Secure & Trusted."* (P196)

### 6.7.4 Summary of key results

**The new indicators are better.** In comparison to the old version, participants found that p ≡ p's new visual indicators better correspond to the names for all three privacy states.

**Better does not always mean good enough.** Irrespective of their tech background, participants did not find p ≡ p's new indicator to be a good representation for the state *Secure*.

**Onboarding has a positive effect.** Exposing users to a priming screen with the whole indicator set impacted how users evaluated the individual indicators.

**Onboarding is not a silver bullet.** While users exposed to onboarding did find the indicator for the state *Secure* to be more fitting than those that were not exposed, the majority of them, nevertheless, disagreed that it is a good representation.

**"Something is Rotten in the State of" *Secure*.** Participant feedback clearly pointed to the color and shape of the indicator as not being adequate for the *Secure* state. Furthermore, the indicator evoked feelings of caution, rather than security.

**Indicator shapes should not be downplayed.** While overall the red indicator was evaluated as fitting, participant feedback hints at potential issues with the designated shape to represent the *Mistrusted* state. In the case of *Secure & Trusted*, it is not clear whether the green shield reflects both the concepts of *Security* and of *Trust*.

## 6.8 Discussion

Coming up with effective indicators in systems for secure email is closely tied to these two user-related challenges: understanding and controlling secure email. The first deals with users' ability to recognize the security status for a particular message or correspondent that a system tries to communicate through a concept familiar to the user. The second deals with the amount of control that the user exerts over the system or is expected to contribute for the interaction to take place with the desired security outcome.

In view of the afore-mentioned complexities intrinsic to secure email, two options are available to systems that attempt to deploy traffic lights as means to communicate security information to their users: either reduce the variety in the environment (i.e. choose to communicate only a subset of the possible states); or increase the variety in the system (i.e. resort to additional "mechanisms" to communicate the desired states). While the number and relative ordering between the three states in $\mathsf{p} \equiv \mathsf{p}$ allows for a direct mapping onto the indicators found in traffic lights, this is not as straightforward from a user's perspective, as our study shows.

**What is the role of the yellow indicator?** The key question boils down to: "What does $\mathsf{p} \equiv \mathsf{p}$ want to communicate with the *Secure* privacy state"? A sense of security, a sense of caution, or both in order to accommodate for a range of threat models at the same time? We term this *self-reflective security*. As our investigation highlights, combining both is a daunting task. For experts and security-savvy users, it is immediately clear that in the *reliable* security state, users could be susceptible to a man-in-the-middle attack. Thus, $\mathsf{p} \equiv \mathsf{p}$ attempts to signal this potential problem by suggesting a cautious approach using the yellow indicator. The name of the state in the UI, however, for the majority of users instills a sense of security, in contradiction to the visual indicator.

Our data suggests two avenues that could be explored to resolve the current discrepancy:

- Remove the secure association from the indicator, and communicate cautiousness more. This is a design choice i.e. if the *reliable* state is not secure, it should not be called *Secure*.
- Alternatively, if it is "secure enough" for non-expert users that do not have extensive threat models and already use other systems that offer the same or lower levels of protection (e.g. centralized E2EE instant messaging), then change the indicator to represent the concept of security (rather than caution). The system could still provide a hint on the indicator's position relative to other indicators in the set in order to denote that there might be a higher protection level, yet without unnecessarily sending mixed signals.

**IMPLICATIONS ON THE PERCEIVED SECURITY.** While discussing the preliminary analysis of this investigation with the p≡p developers, we realized that the reasoning behind the secure, yet cautious indicator can be traced back to their founding mission. p≡p is rooted in privacy activism, thus one of their core ideas is to "nudge" users to be more privacy-conscious. As research suggests, however, "greater familiarity, assuming no negative experiences in the past, may result in lower levels of perceived hazard and, in turn, less motivation to seek warning information" [212]. Meaning, users can be easily habituated if all goes well in the *Secure* state, and as verifying key fingerprints (or trustwords in p≡p's case) is neither a primary task, nor done frequently [336], users would be less likely to move to the next state with higher security guarantees i.e., *Secure & Trusted*.

This is problematic, because, on the one hand, users might have a false sense of security while still being susceptible to MITM attacks. On the other, for non-expert users without special security or privacy requirements, the perceived hazard is probably low, making the interaction with a system that sends mixed signals confusing, potentially impacting the usability and adoption.

**BEYOND THE COLORS OF TRAFFIC LIGHT INDICATORS.** Inclusive design aims to meet the needs of non-disabled and disabled users alike [189], which is of concern in the context of indicator and warning design too [378]. The introduction of shapes to improve the accessibility can come with side-effects, however, such as communicating additional information that may be in contradiction to the other cues.

Apart from colors and shapes, constitutive components of indicators are also the associated text labels. While substituting PKI jargon with non-technical terms is the right way forward for systems targeting non-expert users, one needs to bear in mind that such labels

might carry connotations subjective to each user. In p≡p's case, do novice users understand what *Mistrusted* and *Trusted* refer to? Could it be the public key of the correspondent, the actual person or the contents of the message that they sent? In other words, misinformation, malicious links or malware attachments might also come via advanced E2EE systems, intentionally or unintentionally, even from people that we trust.

Exposing users to an indicator set, e.g. via "onboarding tutorials", can support them in positioning individual indicators with respect to the others in the set. This can potentially help users understand the ordinal location and by extension, any associated risks or security connotations, the system is trying to communicate to users, as long as they have a "correct" understanding of the extremes of the indicator spectrum. As such, traffic-light inspired indicators could be fit for purpose provided the intermediary state is neutral i.e. logically equidistant to the indicator spectrum ends.

### Limitations

Our work is by no means exhaustive and comes with certain limitations that should be considered when interpreting the results and analysis of our study.

We conducted an investigation with hypothetical, prospective users out of context. While this removes prior bias that actual p≡p users might have had, it omits the context of use and situated interaction. Our approach can, nevertheless, be a useful first test of indicator recognition and information-scent.

We cannot exclude the possibility that the score deviations in Study B and C can be confounded by the possible extra differences of the participants, which is inherent to between-subject studies.

To investigate user opinion for each state, we used only one question. Nevertheless, given the importance of the number of steps for single-item measurements, we used a 7-step question as suggested by literature [298].

The study was grounded in one particular system. We argue, however, that the methods and insights are easily transferable to other privacy-enhancing systems that aim to or already employ the traffic light metaphor as a visual feedback mechanism.

## 6.9 Chapter Conclusion

User interfaces inspired by the traffic light semantic are omnipresent in computer systems. In this chapter, we studied the adequacy of this metaphor in the context of a secure email system. Participant input suggests that representing certain privacy states, such as those concerning confidentiality and entity authentication, can be challenging and potentially

problematic as a result of indicator misinterpretation. The simultaneous yet contradictory signals that can be communicated by an indicator, such as *security* and *cautiousness* in our use case, can impact the perceived security, or potentially the adoption of a system. While displaying an indicator set (e.g. via onboarding screens) could serve as a cue to engage users' familiarity with a specific concept and potentially prime users towards a specific goal, its effectiveness can be overshadowed by one or more contradictory indicators that constitute that set.

In addition to scrutinizing the use of the traffic light metaphor in other systems, future work could also examine more deeply how users infer the "implications" that the indicator may aim to communicate, and in turn whether or not they adapt their behavior accordingly. While further investigations within the studied context of use would be needed to validate the results, our findings highlight a larger problem. This goes beyond the simple design of an indicator, and more importantly it concerns the amount of security information that system designers try to communicate to users via an indicator. Making difficult design choices with respect to user-facing challenges such as entity authentication are widespread across security and privacy critical systems, thus, investigating those with representatives of the target population is a practice we strongly encourage as early as possible in the design process of privacy-enhancing technologies.

## 6.10 Chapter Appendix

The surveys and datasets with raw participant responses from the second set of user studies can be downloaded from the following link: http://doi.org/10.5281/zenodo.4322893 [324].

Supporting documents from this chapter are also provided in Appendix C.

Context III

# Digital Health Technology

*A fundamental concern for others in our individual and community lives would go a long way in making the world the better place we so passionately dreamt of.*

Nelson Mandela

# 7

# Field Notes on COVID-19 Contact Tracing Apps

CHAPTER ORGANIZATION. This Chapter is organized in 7 sections. First, we provide a short background on contact tracing apps and present related work in this domain. This is followed by an overview of the epidemiological situation in France and Germany in the second half of 2020 to better understand the context within which our study was conducted. We then describe our study design and present our findings. We conclude with a discussion and provide a set of recommendations and future work directions.

## 7.1 INTRODUCTION

The coronavirus (COVID-19) pandemic has led governments, health agencies, and technology companies to develop solutions to control the spread of this infectious disease. Digital contact tracing (or proximity tracing) has been proposed to help break the chain of COVID-19 infections, complement manual tracing [64], and relax lockdown restrictions. Many countries around the globe have launched national contact tracing apps that individuals can voluntarily download on their smartphones (notifying users if they have been in close proximity to someone who has tested positive for COVID-19 [243]). However, the effectiveness (or utility) of these apps – whether centralized (like the French TousAntiCovid [143] based on ROBERT [63]) or decentralized (like the German Corona-Warn-App [279] based on DP-3T [345]) – highly depends on their widespread adoption by the general population.

Several user studies—mainly surveys (e.g., [13, 193, 217, 311])—have quantitatively explored how users perceive the use and features of contact tracing apps. In this chapter, we present our study, conducted in November 2020, consisting of eight focus groups with participants living in France and Germany. The aim of the study, founded on the identified empirical and methodological gaps in the provision of insights for actual app adoption, was

to understand: (1) the factors that influence people's decision to adopt and use a contact tracing app; (2) people's perceived benefits and drawbacks of such an app; and (3) people's perceived threat/adversarial model of a contact tracing app.

## 7.2 Background and Related Work

**Online surveys.** Prior work has examined public opinion of contact tracing smartphone apps. Zhang et al. conducted one of the earliest survey studies (2,612 participants) between March 30 and April 1, 2020, to explore Americans' perceptions of privacy and surveillance during the COVID-19 pandemic [390]. Preliminary results showed that Americans preferred the use of manual tracing and traditional health screenings over contact tracing smartphone apps. Abeler et al. conducted a survey of 1,055 respondents residing in the UK in March 2020 (just before the first lockdown was imposed in the UK and before any contact tracing app was deployed) [2]. About three-quarters of respondents said they would definitely or probably download and use a contact tracing app – though some respondents cited the following as barriers to adoption: risk of government surveillance and fear of user's phone being compromised. These motives and additional factors underlying hesitance to adoption have also been found in studies conducted in Germany, UK as well as France. Several cross-cultural investigations have further elaborated in greater depth how perceived benefits and drawbacks of smartphone-based contact tracing applications have been seen to influence adoption.

Altmann et al. conducted a survey of 5,995 respondents recruited from five countries (France, Germany, Italy, the UK, and the US) between March 2020 and April 2020, to measure public support for contact tracing apps [13]. Although none of the respondents had used a contact tracing app in the past, German and US respondents were less supportive of contact tracing apps compared to respondents from other countries – citing security and privacy concerns. Using a study similar to that of Altmann et al., Kostka and Habich-Sobiegalla studied public acceptance of contact tracing apps in China, Germany, and the US in June 2020; they also found that respondents recruited from Germany and the US were much less accepting of using a contact tracing app than those recruited from China [205].

Other similar survey studies have been conducted [160, 193, 217, 344, 353]. Trang et al., for instance, collected data from 518 participants in Germany between April 20 and 24, 2020 investigating how the intention to install contact tracing apps is influenced by different app specifications, focusing on three dimensions: benefit appeal, privacy design, and convenience design [344]. They suggested that in order to achieve mass acceptance, policy makers should categorize a country's population into three major groups: critics, undecided,

and advocates. Depending on where the majority falls, policy makers should employ corresponding strategies; for example, communicating societal-benefit appeals and ensuring minimal privacy risks are paramount for *critics*; for the *undecided* group, "convenience in app usage" is more important than highlighting privacy risks, while societal-benefit appeals should be stressed even more.

Similar findings with respect to users' differences in adoption were also found by Utz et al. [353]. In evaluating user adoption and acceptance through an online hypothetical app study with over 1,000 participants in Germany, the US and China respectively, the study revealed significant differences between all three countries in willingness to use contact tracing apps. In alignment with the afore-mentioned study, acceptance for the apps in China was higher than Germany and the US. Chinese participants also had significantly higher "perceived normative pressure" within their social circles to adopt the app as well as positive views on the apps' usefulness in pandemic mitigation. Furthermore, the study highlighted distinct concerns between users, with skepticism for governmentally provided apps resulting in 15-21% of participants in the US and Germany not wanting to adopt the app as well as preferring anonymity (privacy concerns) over personalization. Conversely, findings for Chinese users raised concerns about the potential for heightened stress as a result of continued awareness that would result from app use and a preference for more personalized data collection approach. A consensus across countries was visible however on the preference for tracing over the blanket enforcement of quarantine (positive association for user acceptance) and the negative effects on adoption of technical defects. When non-adoption was concerned, reasons cross-countries highlighted current lack of app and/or suitability of app as well as the deemed necessity. Uniquely, Chinese participants also voiced the lack of need for a standalone offer due to existing plugins inherent in systems such as WeChat and AliPay.

Häring et al. [161] investigated the intentions and misconceptions of adoption within a sample of 744 Germans, prior to the roll out of the German Corona-Warn-App. With emphasis placed on understanding what was already known about the actual app among the population, as well as gauging people's views on potential app functionalities and willingness to adopt it, the study highlighted the complexity that is often found between users' trust in governments and public communication on adoption willingness. Positive influences on user's willingness to adopt the Corona-warn-app were found when users held favorable views of the government, when they demonstrated being attentive to their health and when the adoption would be a means by which to return to some form of normality in users' everyday lives. Privacy conscious and concerned individuals were less likely to adopt the app. Furthermore, when the application properties were seen to have societal or individual benefits, these had a significant positive effect on users' intent to install. Conversely, when the

advantage to the individual user proved to be less clear, this had a negative influence on app installation. The study served to highlight the prevalence and diversity of false beliefs among potential non/users with the highlighted misconceptions ranging from a false sense of security and protection through app usage (i.e,. real-time awareness of infected individuals nearby), to misconceptions about the type of data collected and connectivity requirements, trust and level of data shared (i.e., governments watching you every minute). Ultimately the study also pointed to the challenges that the overload of conflicting information could have in negatively impacting user adoption.

Through the conducting of focus groups in the UK, Williams et al. [375] equally found that the self-protective misconception associated with contact tracing apps (i.e., a warning of infected individuals in the vicinity) was one of the most common among participants. Across the 6 online focus groups conducted in May 2020 during the lockdown, Williams et al, reported mixed views as to the potential for app uptake among the 27 participants. Generally, all participants (in the *decided*, *undecided* and *unwilling* groups) "either expressed a lack of knowledge of contact tracing and contact tracing apps or appeared to have misconceptions over what the official UK government-proposed app entails"[375, p 380]. In accordance with other survey studies, voiced willingness for uptake was seen to align with views on acting for the greater good. Also reinforcing previous results from survey studies [161, 353], was the observation that privacy concerns were more prominent among those who intended not to adopt contact tracing apps. For willing users, privacy proved to be outweighed by shared public health objectives and the promise of increased freedom of movement. Stigma, or the concern for individual identification, potential discrimination and harm was also voiced by undecided and non-adopters. Cultural distinctions (i.e., UK deemed as less collectivist and favorable towards state interventionism as compared to Singapore and China), also formed the basis of unwilling participants' arguments for belief in the apps reach, uptake and resulting efficacy. This was stated alongside the re-occurring view on limitations to uptake for vulnerable groups.

In France, the importance of trust was also noted by Guillon et Kergall [155], who while studying quarantine compliance, also sought to investigate the potential and acceptability for a contact tracing app. They surveyed online a sample of 1,909 individuals' beliefs through items on user perceived susceptibility, severity, benefits and barriers, from April-May 2020. Their findings highlighted that greater trust in the government correlated with the use and acceptability of contact tracing apps. Additionally, the individual impacts on health, as observed also in other studies [161], as well as characteristics towards future orientation (i.e., being less impulsive) were positively correlated with uptake willingness. These findings reiterate that "public communications should focus on restoring trust among the

population as trust is of prominent importance in the willingness to use the contact-tracing application"[155, p 30]. A final recommendation suggests promoting short-term benefits of the French COVID app, which could be useful to promote its adoption.

**Longitudinal studies.** Garrett et al. examined public opinion over time in several countries (including Australia, Germany, and the UK). They periodically recruited and surveyed respondents from these countries "in waves". Garrett et al. found that despite the widespread acceptance of contact tracing apps in Australia, download rates were lower than what was predicted [135]. Simko et al. deployed a sequence of online surveys (100 respondents recruited from various countries around the world per survey) as part of a longitudinal study [311]. They found that a significant minority of the respondents had reservations about downloading and using a contact tracing app even in the best possible privacy scenario (i.e., when a contact tracing app would provide "perfect data protection").

**Real app use cases.** Most user studies conducted to explore people's privacy perceptions of and attitudes toward contact tracing smartphone apps have been quantitative in nature (mainly through online surveys and/or existing databases) as well as larger overarching comparative reports on adoption. Furthermore, past studies have often captured intentions to install or adopt a contact tracing app through a variety of hypothetical settings which in themselves serve as a proxy for actual behavior. Propelled by greater calls for the advancement and rigor in the evaluation of contact tracing [76], more recently emerging studies have started to investigate reasoning for adoption and non-adoption of deployed apps. Several of these online surveys, focus groups and longitudinal studies are briefly expanded on below and serve to consolidate several initial findings across hypothetical scenarios as well as provide greater insights on perceptions and extracted behavior towards smartphone application use, discontinuity and non-use.

In their study Horstmann et al. [174] surveyed 1,972 adults in Germany after the app was rolled out, with the aims of better understanding reasons behind use and non-use of the Corona-Warn-App through an existing dataset. Participants were provided with possible drop down reasonings specific to their usage and with open questions. The study echoed findings regarding demographic gender dispositions to adoption [353] , with female users making up a larger majority of non-users. However, distinct to prior studies, likelihood for adoption decreased as age increased. In reinforcement of coinciding studies, non-users also voiced concerns over privacy, questioned the effectiveness of the app and voiced the lack of technical equipment to use the app. This latter point aligns with a finding raised in the French health literacy survey conducted at the onset of the pandemic [343] as well as with the review of Shahroz et al. [307] highlighting the distinct efficacy concerns for app usage of individuals in more precarious circumstances. The majority of users, on the other hand,

seemingly saw no reason not to adopt the application (71.7%), with many voicing beliefs in efficacy (66.5%) and benefits outweighing risks (65%). Conversely, curiosity (i.e., trying something new) and a *sense of obligation* were seen as minimal motives for uptake. This latter point aligns to findings from Utz et al. [353] on the limited sense of peer pressure among German users. Ultimately, the authors' findings highlight important similarities with pre-app deployment concerns and underline the importance of future public health campaigns that could target different target groups consisting of non-users in an effort to encourage behavior change regarding COVID-19.

Similarly, in studying the usability of the Dutch contract tracing app CoronaMelder through a convenience sample of 21 adults and 23 young people in Twente, Bente et al [41] asked whether the contact tracing app is "user-friendly, understandable, reliable and credible, and inclusive". Incorporating the Dutch User Experience Questionnaire, the app's usability testing was conducted through a mixed methods approach leveraging scenarios for think-aloud tests complemented by interviews and the wearing of eye trackers by some participants. The study demonstrated consensus in its findings with respect to underlining the importance of trust in the app, and communication iterating that "the perceived lack of clarity led to misconceptions about the app, mostly regarding its usefulness and privacy-preserving mechanisms" [41, p 1]. Congruent with other studies [155], the authors recommended the need for the provision of targeted and multi-channel information as to the app's actual purpose and functionalities. Furthermore, their findings also suggest considerations are needed towards greater inclusion with respect to the app's delivery of content, as well as the need for health workers (i.e., the public health authorities who contact potentially infected persons), to be trained to interact with users in an empathetic way.

In studying the Corona Alert App in Belgium, Walvare et al. [365] focused on 1,850 users who "did not install the app, those who downloaded but did not activate the app, and those who uninstalled the app". The study highlighted distinct attitudes between the groups. In their findings non-users shared similar concerns with those documented by Horstmann et al. [174], with the lack of perceived gains for downloading the application and privacy surfacing as the key disablers. Technical limitation (i.e., not having a smartphone) were present too, albeit lesser in extent. The researchers reported that adopters were more convinced of the app's utility and more open to new features than non-adopters. However, distinctions in preferences as to how the app would be extended were noted for users, with greater pandemic informative functionalities and entailed practicalities (i.e., testing appointments) taking precedence over less favorable certifications and elements of control and access (i.e., digital certifications, event 'green' passes).

Post-deployment longitudinal studies which have since surfaced are also worth mention-

ing briefly. Consisting of 4,960 participants, the study conducted by Grill et al. [149] aimed to understand user fidelity and prevalence of barriers across diverse sociodemographic groups in Germany. The findings highlighted a divide across a number of dimensions, ultimately impacting the willingness to adopt Corona-Warn-App. In particular, non-adopters were more likely to be younger, had attained lower educational levels, had lower income, and were seen to voice less cooperative motives (such as, disclosing tests and quarantining). Furthermore, alongside perceived trust in the data compliance of the apps, which for older adults and those with higher income was significantly higher, the digital divide was also seen to separate the users from non-users, as was mother tongue (other than German), and minority group belonging. The study stressed the necessity of equal societal access based also on the infection risks that current profiles of non-adopters raised (i.e., smaller living spaces at home and work, public transport etc.). This is a recurring trend also seen in aforementioned studies [41, 174] as is the missed communication opportunity to inform about the usefulness and effectiveness of the contact tracing app.

Our investigation builds upon the prior work presented above by providing qualitative insights into why people decided to use, or not to use, the official contact tracing app in their country of residence, how they viewed the benefits and drawbacks of the app, and what security and privacy concerns they had. Our study is also a cross-cultural one (Germany and France) conducted in a focus group setting, allowing participants to discuss and examine any similarities and differences in their perceptions and expectations.

## 7.3 Contextual information

### 7.3.1 Epidemiological situation in France and Germany

Following a decline in the number of confirmed cases and the associated morbidity and mortality rates, which in most European countries peaked in April and early May of 2020, the summer months of 2020 saw a relaxation of the stringent lockdowns and restrictions imposed during the first wave of the pandemic [115]. The second wave, however, emerged as much more disastrous with the number of deaths mounting even in Germany [277], which was largely perceived as a country that was successfully tackling the pandemic at its onset [91]. By late October 2020, a dramatic increase in the number of confirmed infections (as illustrated in Figure 7.1) as well as hospital and emergency unit admissions could be observed, leading to a renewed imposition of tighter control measures in various European countries [115].

In an effort to tackle the new surge of COVID-19 in France, a second nationwide lockdown began on October 30, 2020 [142]. While it was characterized by a higher number of ex-

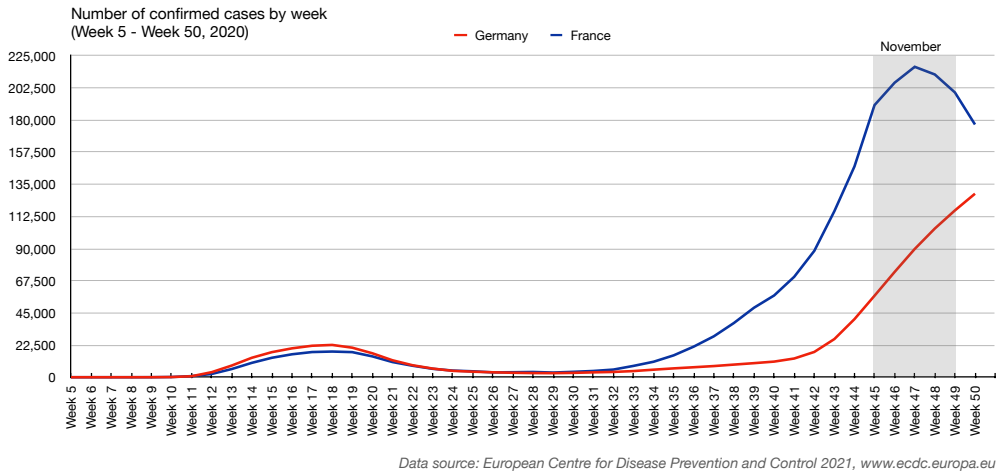



**Figure 7.1:** Overview of the epidemiological situation in France and Germany in 2020.

ceptions in comparison to the first lockdown, such as schools and certain sectors remaining open, all non-essential stores and activities were again closed, working from home was requested whenever possible, and restrictions on movement were reimposed. Consequently, any activity requiring people to leave their homes, such as accessing essential services, food shopping, or outdoor exercising had to be declared in a specific form called *Certificate of Travel Restriction Waiver* (*Attestation de déplacement dérogatoire*) that had to be carried at all times [144]. 38% of the people polled by YouGov in November 2020 thought that France handled the pandemic very or somewhat well [387].

In response to the spiraling coronavirus crisis in Germany, a partial lockdown was imposed on November 2, 2020 [121]. While being a softer version of the restrictions imposed during the first wave, the partial lockdown, nevertheless, entailed closure of most non-essential premises, restrictions on meeting in public spaces, and limits on the number of people allowed to visit someone else's home. Unnecessary travel was strongly discouraged, while working from home was expected to be the norm. Regarding people's perceptions of the German government's handling of the pandemic, in mid-November 2020, 55% of the people polled by YouGov thought that it was handled very or somewhat well [388].

### 7.3.2 Contact tracing apps in France and Germany

France. Built upon the centralized ROBERT (ROBust and privacy-presERving proximity Tracing) protocol [63], the official French contact tracing app was initially called StopCovid when it was launched on June 2, 2020. In an effort to address certain limitations and make progress with respect to the initial low adoption figures of StopCovid among the French

population, the government relaunched the app based on the same technical principles, under the name TousAntiCovid on October 22, 2020, effectively replacing the previous version [268]. According to the open dataset published by the Ministry of Solidarity and Health of France [141], by November 20, 2020, the StopCovid/TousAntiCovid app was downloaded 9.26m times in total (roughly by 14% of the population*). 48,959 people had confirmed their infection with COVID-19 using the app, while 12,901 people were notified by the app about exposure to COVID-19 [141].

GERMANY. Abandoning the initial plans of developing a contact tracing app based on a centralized software architecture akin to the one in France [87], the official German contact tracing app, called Corona-Warn-App, was launched on June 16, 2020 based on the DP-3T (Decentralized Privacy-Preserving Proximity Tracing) protocol [345]. As per the published facts and figures on November 20, 2020 by the federal government agency responsible for disease control and prevention [278], the app was downloaded 22.8m times in total (roughly by 27% of the population†). More than 3.9m test results (both positive and negative) were communicated to users via the app, and 56% of the positive results were further shared by the users in order to alert others and break the chain of infections [278]. Corona-Warn-App was among the first three contact tracing apps in Europe to link to the EU interoperability gateway system, allowing for a seamless exchange of information between apps (and across borders) based on a decentralized architecture [117].

## 7.4 METHODOLOGY

To answer our research questions, we conducted eight focus group sessions with 24 participants in total (12 per country) during the second half of November 2020.

PARTICIPANTS. Study recruitment was conducted via Prolific, an online crowdsourcing platform‡. Several control measures were set as pre-screening filters, such as current country of residence (France or Germany), desktop access, and willingness to participate in video interviews. To encourage greater representation and inclusion, eligible candidates were then provided with potential dates, so that they could register for a focus group session. Upon selecting a suitable time slot, participants were sent a link to the online session that they would take part in. Online sessions were hosted on the Webex video conferencing sys-

*As of 2020, population of France: 67.3m [119]
†As of 2020, population of Germany: 83.2m [119]
‡https://www.prolific.co, retrieved August 16, 2021

tem and facilitated by the Miro collaborative platform[§]. This resulted in a total of eight focus groups (four French and four German), lasting for approximately one hour each. Sessions took place during the day and in the evening to meet participants' schedules.

ETHICS. Our study was approved by our institution's ethics review panel, and informed consent was obtained from all participants. Participants' names and personal details were kept anonymous. Participants were also given the option to use a pseudonym when participating in the online session hosted on Webex and facilitated by Miro. All 62 participants that took part in the short pre-screening survey were compensated £0.09, corresponding to Prolific's fair rewarding practice of at least £5.00 ($6.50) per hour. 24 of these participants were subsequently compensated at an hourly rate of £10 for their participation in the focus group sessions, as per Prolific's recommendations.

FOCUS GROUPS. The focus groups, which ranged in size from two to four participants, adopted a semi-structured approach based on the guide available in Appendix D. After briefly introducing contact tracing apps – supported by excerpts from the World Health Organization (WHO)[¶] – and making sure that participants understood key terminology, we asked a series of questions.

Participants were asked to take part in a number of individual and group activities (as prompted by each question) using Miro. As depicted in Figure 7.2, Miro is a collaborative platform where individual projects, by default consisting of a blank canvas, can be created and shared with (anonymous) guests who can view or edit the canvas using a series of tools. For each focus group, a separate project consisting of several boards was created. Each board was dedicated to one question from our focus group guide. For each question, which was written on the top of the board, participants were asked to share and document their thoughts using color-coded notes that they attached to the board, to achieve breadth of knowledge and collect as many individual experiences as possible. This was followed by short plenary group discussions (before jumping to the next question), to glean insights into and explore individual experiences in depth through group discourse. Each participant was given the chance to address and build on the comments of other participants in the group. When necessary, the moderator asked individual participants direct questions to ensure all views were considered.

[§] https://www.miro.com, retrieved August 16, 2021

[¶] https://www.who.int/publications/i/item/WHO-2019-nCoV-Contact_Tracing-Tools_Annex-2020.1, retrieved August 16, 2021

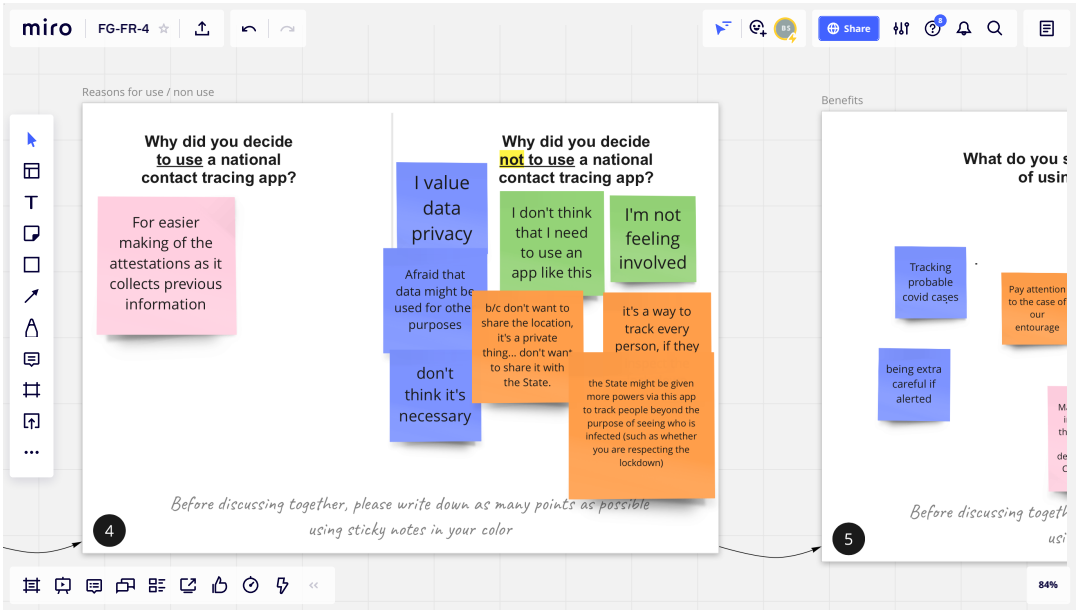



**Figure 7.2:** The Miro online collaborative platform used in the focus group sessions

DATA ANALYSIS. The data collected and analyzed for the purpose of this study included individually written participant answers (color-coded notes on the Miro platform) and group discussions (transcripts of Webex recordings). Session recordings were transcribed, and individual notes were exported to MAXQDA, to allow for subsequent thematic analysis. Tags denoting the French and German groups were included for all notes. The thematically-driven questions on the Miro boards were used as a guide for the creation of first-level codes (e.g., adoption/non adoption factors, benefits/drawbacks, etc.), which we used to analyze the focus group data (i.e., individual answers and discussion points). Inductive coding was then used to produce second-level codes, which we used to analyze the data in depth and formulate insights.

Preliminary coding of the data collected from one focus group session was undertaken by the lead researcher. The coding was then independently verified by a second researcher, to refine the codebook, resolve disagreements, and reach consensus about the identified coding categories. The data collected from the other three focus group sessions was then coded by the lead researcher, in consultation with the second researcher when necessary. Our qualitative codebook can be found in Appendix D.

**Table 7.1:** Participant demographics. N=12 per country.

| **Demographics** | **France** | **Germany** |
|---|---|---|
| Female | 4 (33%) | 7 (58%) |
| Male | 8 (67%) | 5 (42%) |
| Median age | 30 | 31 |
| Age range | [20 – 62] | [26 – 54] |
| National residents | 5 (42%) | 10 (83%) |
| Foreign residents | 7 (58%) | 2 (17%) |
| Employed (full-time or part-time) | 8 (67%) | 10 (83%) |
| Student status | 4 (33%) | 2 (17%) |
| Currently use a national contact tracing app | 2 (17%) | 8 (67%) |
| Used a national contact tracing app in the past, but stopped using it | 3 (25%) | 1 (8%) |
| Have not used a national contact tracing app | 7 (58%) | 3 (25%) |

## 7.5 Findings

Table 7.1 provides an overview of our participant demographics.

### 7.5.1 Reasons for adoption

The following themes were identified as dominant reasons for installing and using contact tracing apps by focus group participants. Participants included those that at the time of the study used or had previously used a contact tracing app.

#### Desire to act responsibly and exercise civic responsibility

Participants from both countries (France and Germany) viewed the adoption of contact tracing apps as a means to contribute to a greater societal cause and to help prevent the spread of coronavirus. This is depicted more clearly by the following statements:

- "*to limit the propagation of the virus as efficiently as possible – a civic duty, I guess* " (FR, p7)
- "*helping scientists do their job* " (DE, p22)
- "*supporting the society* " (DE, p23)

One participant viewed the adoption and use of a contact tracing app as a self-imposed duty to (positively) influence others' beliefs and behaviors in this regard: "*To be a role model ... to encourage friends, colleagues to use that by themselves. Show to my kids that I want to do everything [that] I can do*" (DE, p23).

### Personal safety

Another recurring theme and key motivator for adoption was the desire to protect oneself and others, especially family members, friends, elderlies, and vulnerable people (at-risk groups):

- "*because I want to know if I have been in contact with an infected person*" (DE, p19)
- "*to know if I am under risk*" (DE, p17)
- "*take precautions like self isolation if appropriate* " (DE, p15)
- "*to stay safe and take care of family and friends* " (DE, p20)
- "*protecting the parent generation* " (DE, p23)

### Security, privacy, and trust

Feeling in (partial) control of the data collected, taking an informed approach regarding the type and use of data handled, and having trust in the government and/or app developers handling the data were voiced as motivating factors that increase adoption of contact tracing apps and/or minimize users' privacy concerns.

- "*A lot of warnings and options to respect the privacy of every user - seemed like a safe choice to use it*" (FR, p7)
- "*because they're safe when it comes to my data*" (DE, p19)

### Other reasons

Being curious about trying out a 'new technology', evolving social dynamics (e.g., increased social interactions and the desire to avoid lockdowns), and requests to install a contact tracing app by an employer or when traveling abroad were all mentioned as reasons why participants installed and/or considered using contact tracing apps. Moreover, several participants indicated that although they preferred to voluntarily install an app, they would still install an app even if it were mandatory to do so. In contrast, others demonstrated a preference for a more mandated approach. One participant specifically voiced refusing to install a contact tracing app, precisely because it was voluntary to do so, questioning the app's reliability and placing greater trust in a more mandated approach. We describe reasons for non-adoption next.

### 7.5.2 Reasons for non-adoption

**Lack of utility**

A significant number of participants believed that there was no added benefit or value of existing contact tracing apps, as illustrated by these verbatims:

- "*don't think it's necessary*" (FR, p10)
- "*I don't think that I need to use an app like this*" (FR, p12)

Moreover, the second (partial) lockdown which overlapped with our focus group sessions, seemed to have impelled participants to further question the usefulness of the apps in light of remote working and more general self-isolation measures, as the following expressions highlight:

- "*I do not need them because of home office*" (DE, p13)
- "*I have never been in the situation to use one, I'm mostly at home*" (DE, p18)

This lack of perceived utility or perceived benefit was both driven by and in turn reinforced low adoption rates. Participants considered the number of current users of a contact tracing app (and how in turn they perceived its value) when making their own decisions to adopt or not adopt the app.

- "*Even [if] smartphone was activated, wouldn't have done it because no one seemed to be doing it. The consensus was that it was not very efficient.*" (FR, p4)
- "*It's still like a trial at the moment, I feel like it needs to be out... so basically, I don't*" (DE, p18)

**Lack of trust**

A number of factors and entities were brought up in the context of trust. Participants mentioned that they did not necessarily trust their government, the developers of the contact tracing app, nor the technology itself.

- "*the results of those apps with the underlying technology do not work as intended, especially the distance cannot be determined precisely*" (DE, p13)
- "*Not accurate enough due to the Bluetooth used as a technology*" (FR, p5)
- "*I do not trust the companies which developed the app*" (DE, p13)

- "*Not enough information about the editor [developer]*" (FR, p3)
- "*the State might be given more powers via this app to track people beyond the purpose of seeing who is infected (such as whether you are respecting the lockdown)*" (FR, p9)

**Lack of clarity and communication**

Poor public communication, in terms of clarity and outreach, and lack of public engagement were issues that emerged from our focus groups and were especially discussed by French participants.

- "*...[it] wasn't really explained, they said you can download it, it would be a good idea, but had no idea of what the use of this would be*" (FR, p4)
- "*You don't know where and who owns the data in the end. When the government told about that application, they told it was a private company and we use Bluetooth, but we do not keep the tracing data. So it's a little bit difficult to tell.*" (FR, p1)

Participants also stressed the additional effort being placed on them to understand the purpose of a contact tracing app.

- "*The benefits of using it are not clearly explained by the State. Unless one does the research, it may seem as just a useless battery-consuming app*" (FR, p7)

The government's approach to persuading the population to start using a contact tracing app was perceived as paternalistic by some participants, which resulted in unwillingness to participate in the collective action.

- "*they treat us as children so I acted as a child*" (FR, p1)

In this context, participants also expressed lack of role models promoting app adoption. Some participants believed that public figures and government officials did not install contact tracing apps.

**Poor usability**

In addition to lack of utility, some participants mentioned that contact tracing apps drained their phone's battery, while others found using and interacting with the apps complicated, resulting in them not using the apps (any longer).

- "*Not user friendly, they need to create something easy to understand to make it popular*" (FR, p6)

**The ostrich effect**

Psychological and practical discomforts resulting from the apps' potential exposure notifications were mentioned by participants as reasons for not adopting contact tracing apps.

- "*I'm afraid of what will happen if it counts me as an infected person - I prefer not knowing!*"
  (FR, p7 quoting a friend)

Other participants explained that they did not find the current privacy-preserving mechanisms in contact tracing apps flexible or reliable enough to meet the needs of citizens who were willing to share more private data in return for more contextual information.

- "*If I would use the app, I think I would have, to be frank, a psychological problem. If I get an alarm I would like to know where I put myself at risk, as I am extremely careful. I'm not carrying a normal mask, I'm wearing a gas mask, with highly-effective filters, I wear highly-effective protection glasses, I always carry gloves and I only go shopping when it is absolutely necessary. If I would get an alarm, I would be really concerned what I have done wrong and where I put myself at risk*" (DE, p21)

### 7.5.3 Benefits and Drawbacks

The benefits highlighted by participants in the focus groups corresponded to and echoed the reasons why participants decided to adopt a contact tracing app. Reasons included helping identify and break chains and clusters of infection, identifying potential risks, and informatively deciding and planning next steps.

- "*Ability to trace the possible infections scenarios objectively - when getting tested as "positive" a person often forgets to warn every single person he/she contacted*" (FR, p7)
- "*knowing the risk level for myself, feel rather comfortable because others will be notified if I am infected and I can't reach the people I contacted by myself*" (DE, p17)
- "*Knowing whether or not you should stay home/get things delivered or go out instead*" (FR, p11)

Recent improvements and additions of features in the French app, demonstrating contextual sensitivities to user needs (i.e., administrative mobility considerations during lockdown), albeit not directly linked to the act of digital contact tracing, were appreciated by participants who used the app. These voiced benefits could potentially mobilize people to adopt contact tracing apps.

- "*While the former functions were just "nice to have" (just global security, but no everyday "usefulness"), the attestations management was a really nice feature for everyday use*" (FR, p7)
- "*[decided to use TousAntiCovid] for easier making of the attestations as it collects previous information*" (FR, p11)

While making a link between perceived benefits and reasons for adoption is straightforward, and arguably the voiced themes in this section could be analyzed in conjunction with Section 7.5.1, here we are interested in developing a better understanding of the benefits highlighted by participants who had not used a contact tracing app before.

Unsurprisingly, even participants who had not used contact tracing apps agreed to a great extent with the potential benefits of these apps.

- "*To know if you have got the virus or if you're exposed to*" (FR, p3)
- "*help scientists get enough data about the pandemic and the spreading behavior of the virus*" (DE, p24)
- "*I discovered that we can complete attestations faster, [I could] globally gain some time*" (FR, p12)

Nevertheless, there were some participants, albeit a very small number, that did not see any benefits of these apps personally or whatsoever.

- "*for really frightend people this could help to ease their minds or to give them the feeling of security* " (DE, p13)
- "*I will not have the app to tell me, my friend or family if they have covid will just tell me*" (FR, p9)
- "*searching for the benefits... but I couldn't figure it*" (FR, p6)

As for drawbacks, participants who used the French and German apps highlighted a number of shortcomings with regard to what and how apps communicated information to users as well as the general app design. Most participants touched upon the fact that current apps provided insufficient procedural information and did not offer personalized and useful information (e.g., personal risk levels).

- "*People don't know what to do with certain warning levels*" (DE, p14)

- "*somehow quantify my personal risk better, but result is poor, no personal gain, only confusion (by usage, by information about risks)*" (DE, p23)

Further, contact tracing apps were perceived as lacking interactivity. In this regard, participants offered their input and suggested the design of features that would address some of their unmet needs.

- "*Feature request: to receive the latest updates about the pandemic and specific to my area*" (DE, p18)
- "*It would be nice to have a list of places where you can go and get a test, news about new developments on the pandemic situation, list of special places that are crowded and not to be visited etc.*" (DE, p17)

Our participants also mentioned costs and expenses, such as the usage of own mobile data plans, device data storage, and battery drainage as drawbacks they were concerned about.

Another issue mentioned by participants revolved around the poor implementation of a Test-Trace-Isolate strategy, which in some cases could render contact tracing apps useless.

- "*problem is also the accuracy, who did really have it... maybe i'm positive but i never tested, because there is not enough hospital staff to do it nor test itself is accurate enough*" (FR, p6)
- "*the data is a few days old, so if you're infected, you could already have been a risk for others*" (DE, p19)

Finally, some of the drawbacks mentioned referred to the security and privacy aspects of contact tracing apps.

- "*in theory it could be tracked where I have been, probably through the contacts but I think that is unlikely*" (DE, p15)
- "*I can see why there would be privacy concerns (because it asks for your location), but since I was in other countries that utilize COVID19 applications, it didn't bother me anymore (due to priming).*" (FR, p11)

### 7.5.4 Privacy Concerns and Threats

One of the most prominent privacy concerns particularly raised by participants residing in France was *location tracking*. This was mentioned among other concerns with regard to the power that governments and involved parties could exert by gathering large amounts of data through the app.

- "*I think they ask for too much information*" (FR, p2)
- "*the government can track the people and abuse the data*" (FR, p5)
- "*it invades my privacy and I don't want the state to know where I am and who I am with*" (FR, p7 quoting a friend)
- "*the government institutions could learn my activities, my habits, maybe even commercial vendors, difficult to know...*" (FR, p5)

Yet, some participants did not express any privacy concerns in this specific context.

- "*Not really concerned about "privacy" of my geolocation and interaction data, especially for a state-backed app*" (FR, p7)
- "*not really... the government can find a lot of things about me or anybody already, they don't need this sort of app for that info, so not concerned*" (FR, p4)

As for adversaries, our participants mostly mentioned their government followed by app developers, referring to companies behind app development and not individual programmers. In this regard, participants were mostly concerned about either not having sufficient levels of trust to start with, hindering adoption by default, or experiencing negative outcomes as a result of erosion of trust which was placed in the collective response to the pandemic.

- "*I don't want anyone to know about my location history. I am willing to share this in the app only to protect myself and others but without the individual details. If the government, or app developers, any company, any third party could possibly know about this for any reason other than covid-tracing I would be very uncomfortable.*" (DE, p17)

### 7.5.5 Security and Privacy Misperceptions

We observed a number of misperceptions among adopters and non-adopters of contact tracing apps in both France and Germany, with the most prominent one being *location tracking*. As expressed in the verbatims below as well as in Section 7.5.4, this was manifested along a number of dimensions, such as: concerns that the government, contact tracing app developers or commercial entities could have insights into where and with whom app users were present, either in real-time or at a particular point in the past; concerns that their home address as well as their activities, habits, and political beliefs may be revealed; concerns that the location data may be stolen from the health authorities or entities operating the app and

further resold. These concerns are tightly linked to misperceptions regarding the *capabilities* of different stakeholders involved in digital contact tracing, in particular, the ability to (re)identify users.

- "*they are going to follow everyone who are using the application... they will use data about movements, how much time they spent, etc.*" (FR, p6)
- "*don't think location at every moment is something I want to put out there*" (FR, p10)
- "*people who run the app, probably governments, but also IT support behind it... [can learn] location data, durations of stays, who I am in contact with, to a certain extent my political belief/ideology*" (DE, p15)

These are valid concerns taking into consideration the many unknowns and ongoing efforts to find and fix vulnerabilities in this domain of security and privacy research [34, 158, 355, 356]. Nevertheless, participant discussions shed light on potential misunderstandings of the technicalities of contact tracing (i.e., exhibiting examples of folk models). We also speculate that participant discussions about geophysical location tracking might as well be due to specific (mis)understandings of how the official contact tracing apps in France and Germany work. While TousAntiCovid and Corona-warn-app are Bluetooth-based apps that do not use positioning, on Android 10 and earlier systems users need to enable the geolocation service in order to use Bluetooth Low Energy [139]. We hypothesize that this further contributed to confusion among Android users.

In contrast, some participants erroneously thought that location and other related metadata can be used to see the most risky areas in terms of infections so that they can avoid those places. While such misperceptions were rectified among some users as they started interacting with the app, the realignment to what the app can actually do in turn resulted in disappointment in terms of the app's expected utility.

- "*I am completely unhappy with the app... I expected more out of the app, I hoped more if I would get a timestamp or something like this, I could say it must have been in the park...*" (DE, p2)

As a proxy for the desired functionality of getting insights into which of their activities were more risky in terms of contracting the virus, some users reported paying special attention to the number of encounters their contact tracing apps showed after doing different activities in specific locations.

- "*The app shows me daily how many encounters I have been with. So I know my activities, where I go to, restaurants, parks, etc. So I know that in certain activities that number increases up to 7 or 8 with encounters with low risk, it's probably people sit next to me in restaurant or metro... but going for a run... it's either 1 or none. So it helps me to understand, what [activity] is really making these encounters more or less.*" (DE, p17)

While we did not observe that as a result of installing a contact tracing app users lowered their guard when it comes to protecting themselves from COVID-19, assessing which activities are more or less "risky" based on solely the number of encounters reported by the app could potentially lead to a false sense of security as well as insecurity.

## 7.6 Discussion

### 7.6.1 Summary of results

Our findings suggest that, quite often, participants demonstrated a sense of civic responsibility and willingness to adopt contact tracing apps. However, our findings also show that miscommunicating the purpose and benefits of contact tracing apps, insufficient user inclusion (in the app design process), and lack of transparency (with regard to app functionality and data collection and processing) are factors that hinder the adoption of contact tracing apps.

The investigation into perceived benefits and drawbacks of contact tracing apps echoed and served to further reinforce why participants might have chosen to adopt/not adopt their country's official contact tracing app. The intent to contribute to a more societal mission (i.e., identifying risks and exposure) was most prominent in the discourse. Instances of participants finding personal value and/or daily relevance of the app (e.g., easing the attestation process) were seen as beneficial. In contrast, lack of personalization in current apps, poor interactivity, and lack of communication were expressed as drawbacks impacting perceived relevance and usefulness.

Ultimately, participants did voice concerns regarding the possible risks of location tracking as well as the placement of trust in enabling the collection and creation of rich individual data profiles that could potentially be misused. Nevertheless, these privacy concerns and perceived threats seemed to be mostly overshadowed by other needs across the focus groups. This raises the question as to whether the perceived benefits and usefulness of contact tracing apps are on par with, if not even more important than, privacy-preserving features when it comes to adoption.

### 7.6.2 Similarities and differences between and within study groups

In an effort to better understand and represent the different perspectives that were expressed during the sessions as well as to position similar views in relative proximity to each other, we divided our study participants into four groups (A, B, C, and D), as depicted in Figure 7.3.

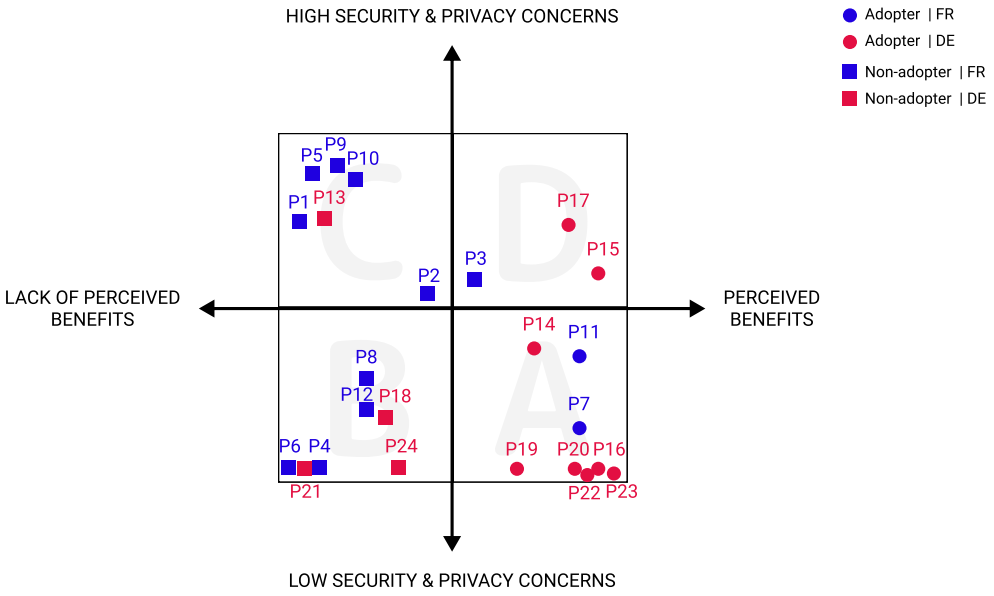



**Figure 7.3:** Affinity mapping of focus group participants based on their responses

French participants that used a contact tracing app are represented using a blue circle next to their ID. German adopters are represented using a red circle. Those that had not adopted an app are represented using a square next to their ID, in blue and red, to denote French and German non-adopters, respectively. The two axes divide the space along the dimensions of *(x)* the perception of benefits and *(y)* security & privacy concerns.

**Group A** The bottom-right quadrant consists solely of adopters of contact tracing apps that have low security and privacy concerns, and for whom the perceived benefits of contact tracing apps outweigh any drawbacks by far.

**Group B** The bottom-left region gathers non-adopters who, despite having low or moderate security and privacy concerns, decided not to adopt a contact tracing app because they do not perceive the benefits or added values of the available contact tracing app in their country or in general.

**Group C** The upper-left quadrant gathers those participants that have moderate to high concerns about security and privacy associated with the usage of contact tracing apps. Furthermore, they either do not see the benefits of using such apps, or for them the drawbacks outweigh any benefits.

**Group D** The upper-right quadrant consists of both adopters and non-adopters. Both groups share moderate security and privacy concerns; however, for the first group, the perceived benefits associated with using a contact tracing app outweigh any drawbacks or concerns. For the latter, the perceived benefits are not there yet for them to decide to adopt or continue using a contact tracing app.

Looking at the distribution of our small sample of French and German participants across the four groups, we can observe that German study participants mostly fall in Group A; i.e., they clearly saw the benefits of using contact tracing apps and they expressed low to moderate security and privacy concerns. In contrast, the lack of perceived benefits was overwhelming among the French study participants, who are divided into two equal sets based on the level of concern with respect to security and privacy.

Contextualizing the adoption trend observed in our focus groups using the official adoption figures of the German and French contact tracing apps reported in November 2020 (see Section 7.3.2), we can see that our findings are in line with the higher adoption figures in Germany compared to France at the time of the study. Interestingly, this contrasts with the cross-cultural investigations of Altmann et al. [13] who reported that intentions to use contact tracing apps among Germans would be lower due to security and privacy concerns.

While this is certainly a question worthy of further exploration, we speculate that the following factors could have contributed to the higher adoption rate among Germans:

- A public debate on the benefits and drawbacks of centralized and decentralized approaches to contact tracing, contributing to the decentralized architecture of the Corona-Warn-App and the discourse surrounding it. For instance, German participants reported that it was common knowledge that in Germany a lot of emphasis is placed on data protection. Thus, while the majority of our German participants did not express security and privacy concerns, this should not be interpreted as if they had no concerns in general, but rather that they did not have these concerns with regard to Corona-Warn-App.

- The higher levels of trust in the government and positive perceptions of the government's handling of the crisis. According to Kostka and Habich-Sobiegalla, whether or

not people have trust in the government has a powerful impact on the acceptance of contact tracing apps in Germany [205].

- The perception of a streamlined and clear public communication of the app's role and benefits as part of the collective response to the pandemic, including deep integration in the country's TTI strategy.

Looking at Group B, we can observe that for a number of French and German participants, security and privacy concerns are not the (primary) obstacle to adoption. To make these participants become adopters, both countries would need to work on the value proposition relevant to this potential user group. While some citizens may benefit from clear, targeted, and streamlined communication of the benefits and ways to get onboarded, others may be motivated to join only after a significant proportion of the population is already using a contact tracing app, which could potentially ease some of their doubts about effectiveness and accuracy. In this regard, additional useful features, such as the travel restriction waiver certificate (attestation) in France or local and personalized information could potentially further increase adoption.

While citizens that fall in Group C appear to be most resistant to adoption of contact tracing apps, some might decide to adopt, provided that the benefits outweigh their perceived drawbacks, and their concerns with regard to security and privacy are addressed or alleviated. To this end, the app's usefulness and effectiveness need to be evident, and trust needs to be established and nurtured. If we assume that this group corresponds to what Trang et al. have categorized as *critics* [344], emphasis should particularly be placed on the societal benefits of contact tracing apps. Nevertheless, as highlighted by Utz et al., we should expect that a certain number of people would be unwilling to adopt the app [353].

The question of trust is particularly important also for adopters in Group D, who are likely to discontinue using a contact tracing app should the trust they placed be eroded. To ensure that this does not happen, all stakeholders involved in the development, maintenance, and operation of the contact tracing app need to apply appropriate cybersecurity measures and practice the highest ethical standards at all times.

LIMITATIONS. Our study has limitations that can be broadly attributed to the collection of self-report data, which does not necessarily reflect actual behavior and the fast-tracked nature of the research conducted to inform the current and future design of contact tracing apps. That said, we aimed – by conducting our focus groups – to elicit diverse views and opinions, by offering flexible interview schedules and minimizing the use of Prolific's prescreening filters to recruit participants. However, our focus groups were conducted in

English, which might have impacted how participants expressed themselves (if English was not their first language). Further, as opposed to Prolific, in-situ and multi-channel targeted recruitment approaches could have allowed us to reach out to a diverse sample of participants, based on age, profession, and digital literacy, ensuring that different user profiles and risk groups were explicitly accounted for.

Due to the COVID-19 pandemic, we are aware that our study design and online participant recruitment approach inevitably excluded a large portion of participants and made our findings less generalizable. Further, participating in sessions in a hybrid fashion via Webex and using Miro to share thoughts, in contrast with a traditional in-situ focus group discussion, might have required extra effort from participants who lacked prior experience with those communication and collaboration platforms. While many welcomed this novel participatory approach, on a few occasions we had to assist participants in attaching their notes or navigating Miro. In some cases, this might have got in the way of gleaning additional insights into our investigation.

While we cannot exclude the possibility of social desirability bias toward the moderator and other focus group participants, we believe that the wide range of responses and preferences expressed by our participants indicate that heterogeneity of views was acquired. Furthermore, we did not observe tendencies of participants to take over the discussion or devalue the opinions of others, and we ensured to offer every participant a chance to express their views.

FUTURE WORK. Future large-scale quantitative studies would enable greater generalizability of our findings. Future work should also consider investigating the potential differences with respect to people's opinions of centralized and decentralized approaches. In this regard, our focus groups aimed to account for a balanced view (centralized and decentralized) to answer our research questions. Furthermore, the unique socio-technical differences that different countries may have to deal with to understand societal uptake are worth noting. Several differences were visible in our focus groups among French and German participants, but those would require more systematic analysis for app deployment and uptake.

## 7.7 CHAPTER CONCLUSION

Considering human factors when exploring the adoption as well as the security and privacy aspects of COVID-19 contact tracing apps is a timely societal challenge. Our work aims to provide greater granularity and understanding of the current more abstract quantitative

investigations of contact tracing app adoption and use. Our findings complement ongoing efforts from a socio-technical lens, given the complex and interdisciplinary needs required to overcome this shared reality.

Our field notes also serve to highlight future recommendations for practice and policy. There is a broad spectrum of user needs that contact tracing apps should take into consideration, in order to enhance uptake. Therefore, we believe that it would be useful to explore and define "archetypes" reflecting the diverse decisions that people make to adopt and use contact tracing apps. These in turn could be responsively leveraged to provide targeted, clear, and dedicated communication pathways within and beyond the app (policy and practice action), as well as integrated functionalities and design features (practice action).

## 7.8 Chapter Appendix

Supporting materials from this chapter can be found in Appendix D.

*Each new hour holds new chances*
*For a new beginning.*
...
*The horizon leans forward,*
*Offering you space to place new steps of change.*

Maya Angelou

# 8 Conclusion

## 8.1 Thesis Summary

Designing, developing, and deploying secure and privacy-preserving digital products, services, and systems is a complex multi-disciplinary endeavor. In this thesis, we sought to investigate how user experience design methods and techniques can contribute towards these efforts in order to help (1) identify and address user misperceptions of system security and privacy; and (2) inform the design of secure systems that are useful and appealing from end-users's perspective.

We began by introducing the two key themes that feature throughout our research efforts in this thesis. The first is concerned with the necessity to investigate and address user misperceptions of system security and privacy, while the second deals with the proposition that in the design of secure and privacy-enhancing systems equal emphasis should be placed on the end user experience. Along these lines, central prominence in this dissertation was given to user experience research and its potentiality to add value to security and privacy discourse and practice.

With aspirations to improve the quality of real-world systems, we took the approach of scrutinizing representative use cases in three specific cybersecurity and digital privacy contexts whereby we were guided by three overarching research objectives:

**Objective 1** Contribute new findings on user experience aspects in security and privacy

**Objective 2** Contribute new findings on user misperceptions of security and privacy

**Objective 3** Contribute new methodological approaches to detecting user misperceptions of security and privacy

The following sections serve to provide a brief summary of the main insights and contributions along these three objectives in each of our studied cybersecurity and digital privacy contexts.

### 8.1.1 UX Aspects in Security and Privacy

**1. Cyber Threat Intelligence – CTI Sharing Platforms**

We first discussed our mixed-methods user experience evaluation of MISP, a leading open source cyber threat intelligence (CTI) sharing platform (Chapter 3). Driven by the higher-level questions of why MISP users decide to adopt this highly-technical system, what their goals, tasks, and actions are as well as what experiences emerge or how they evolve, we performed a set of quantitative (N=74) and qualitative (N=42) investigations over the course of two years. Applying UX methods in a particularly sensitive context, we managed to uncover many user and system-related aspects that help explain what works and does not work well in such a leading CTI sharing platform, and why.

According to our findings, MISP was perceived as *attractive*, *stimulating* and *novel*. Furthermore, users found it *dependable* and *efficient*. However, many novice users found the system difficult to learn and overly complex. We concluded that MISP was overall positively evaluated across all three system quality aspects, namely *attractiveness*, *pragmatic* and *hedonic* qualities. Nevertheless, we highlighted how the complexity of the platform, the steep learning curve and the perceived lack of support or community for novice users could impact system adoption as well as induce errors that can have negative security and privacy outcomes. In particular, if novice users would encounter too many learning difficulties and would be overwhelmed with feelings of confusion and frustration—so much that they overshadow initial positive impressions and feelings of excitement—users would struggle to transition from the *orientation* phase to the *incorporation* phase in terms of system adoption*. This would prevent them from appropriating MISP and forming a more long-term impression of the usability and, more generally, usefulness of the system.

Our findings highlighted how MISP accounts for a number of psychological needs and supports users in the effective and efficient achievement of CTI tasks. We saw how increased incorporation led to emotional attachments and a clear transition to a phase of *identification*. Users particularly valued the flexibility of MISP and the possibility to adapt the system according to their needs. Finally, our findings highlighted a strong sense of community and shared values and goals among the users.

*As introduced in Section 2.1.3, the *temporality of experience* model distinguishes between three product adoption phases: *orientation*, *incorporation*, and *identification* [194].

A key takeaway from this chapter is the necessity to look at the user experience holistically and go beyond traditional usability studies when investigating security tools and systems in general. Combining quantitative and qualitative research methods—which we acknowledge can be challenging due to the nature of the research context—can help researchers find missing pieces of a complex socio-technical puzzle and understandings of their relationships.

### 2. SECURE & PRIVATE COMMUNICATION – Secure Email

Moving onto our second research context, in this thesis we focused on secure and private communication via email (Chapters 5 and 6). We started by motivating the need for new tools and techniques for detecting user misperceptions of system security and privacy, which rely on technical as well as user-related aspects that are taken in for a joint socio-technical analysis of a given system. In an effort to demonstrate how our proposal for detecting user misperceptions in the context of email works in practice, we performed a preliminary investigation of UX aspects related to the activity of communicating via a new secure email system called p≡p.

As a proxy for a user study, we conducted a focus group investigation with HCI experts (N=8) in order to glean insights into the elicitation of possible emotions or the experiences that might emerge with respect to the use or anticipated use of p≡p. We obtained an indication of the positive and negative emotions that could be elicited among new, non-expert users through 24 hypothetical situations, covering different interaction scenarios as well as phases before and after interacting with a secure email system like p≡p. These were then fed into our proposed model for detecting misalignments (as summarized in Section 8.1.3). The preliminary results from Chapter 5 brought p≡p's security and privacy indicators into our focus. This prodded us to conduct further user studies in Chapter 6 which focused on the usability and effectiveness of p≡p's security and privacy indicators and their traffic-light inspired metaphor to represent different privacy states and guarantees.

The indicators consisted of a visual icon, a corresponding rating label and textual explanation. The first set of studies (N=42) pointed out huge discrepancies between how prospective p≡p users, on the one hand, and how the designers and developers of p≡p, on the other hand, made the associations between different visual icons and the corresponding privacy ratings and explanations. Communicating these results to p≡p potentially helped trigger a deeper discussion on their end regarding the indicator design choices, which they subsequently redesigned. In a new set of user studies (N=150) scrutinizing the new indicator set,

we observed the following results: while prospective $\mathsf{p} \equiv \mathsf{p}$ users found the new indicators as better fitting to represent the privacy states in comparison to the previous version, the indicator designated to represent the privacy state *Secure* was not perceived as adequate. Participants pointed to the yellow color and shape of the indicator as not being representative of *security*, and that contrary to the name/label of the state, the indicator mostly evoked feelings of caution. We also observed that exposing participants to an *onboarding* screen that contained the whole indicator set impacted how they evaluated the adequateness of individual indicators, however, this did not have the desired effect in the case of the indicator for the state *Secure*.

One key insight from this use case investigation is that while color plays a central role in the traffic light-inspired indicators, the associated shapes, labels, explanations, etc. are all elements that users take into account when evaluating how adequate those indicators are with respect to representing the designated privacy states and guarantees. They should not be downplayed as contradictory signals sent by these various cues can result in user confusion, potentially leading to insecure use and operation or to system non-adoption.

### 3. Digital Health Technology – COVID-19 Contact Tracing Applications

In the final research context studied in this thesis we delved into: the factors that influence people's decisions to adopt and use a contact tracing app; the perceived benefits and drawbacks of such apps; and the potential threats that they perceive in connection with the use of these apps. We took the national French and German apps as representative examples of centralized and decentralized architectural choices to digital contact tracing, respectively. Our eight focus groups consisted of participants living in France and Germany (N=24, 12 per country), who either had never used a contact tracing app in the past; had used a national contact tracing app, but stopped using it; or were using a national contact tracing app at the time of our study.

We found that key drivers of adoption, irrespective of the country or app, were altruistic and collective-oriented motives to contribute to a greater societal cause and to help prevent the spread of the coronavirus. This suggests that the experience of *meaning* [200] and the fulfillment of the psychological need of *relatedness / belongingness* [289] have a more prominent role in the context of contact tracing apps, as opposed to hedonic experience aspects such as the need for stimulation, pleasure, etc.

Other significant reasons for adoption included the desire to protect oneself (and others) as well as to maintain the autonomy and independence in face of rising infection numbers and possible lockdowns. This is tightly connected with the perceived usefulness of contact

tracing apps. A significant number of our participants did not believe in the added value of such apps at all, while others found the utility and usability of their national contact tracing app to be unsatisfactory. This was problematic as the lack of perceived utility and benefit was both driven by and in turn reinforced low adoption rates, given that participants took into consideration the number of (active) users when making their own decisions to adopt the app or not. Poor public communication, lack of clarity and outreach, was found to be a missed opportunity to increase user trust and demystify the security and privacy concerns among citizens or to onboard those that were not deterred by any particular threats or "threat actors" associated with the use of contact tracing apps.

A key insight from our qualitative investigation is that while some participants did raise security, privacy and trust concerns, these were not the only and primary reasons for non-adoption of contact tracing apps. In most cases, the lack of perceived benefits and usefulness of such apps was a prominent inhibitor along a number of other socio-technical factors that go beyond the architectural choice of centralized or decentralized digital contact tracing, which was a highly debated topic among the security community at the onset of the pandemic.

Both TousAntiCovid and Corona-warn-app have been in continuous development and expanded in features and functionality since we conducted our focus group studies in the second half of November 2020. For instance, at the moment of writing (i.e., February 2022) both apps offer users the functionality of storing their EU Digital COVID vaccination certificates, which have become mandated proofs of protection against the virus in many parts of Europe. The number of cumulative downloads of Corona-warn-app has almost doubled in the meantime. By the end of January 2022, this figure stood at 41.8m (in comparison to 22.8m when we did the study)[†]. In the case of TousAntiCovid, this figure has more than quadrupled to 42.5m (in comparison to 9.26m)[‡]. What the future holds for contact tracing apps is all but certain. Two full years since the start of the pandemic, the world is still battling the coronavirus as new variants, such as Omicron, are causing record infections throughout the world, including Europe [116]. Whether a plausible endgame for the pandemic is in sight [380] or we should brace for renewed resurgence in infections remains to be seen. Contact tracing apps perhaps did not live up to the expectations and excitement that were created around them at the onset of the pandemic, nevertheless, for now they keep running on millions of mobile devices, which, in our view, makes them a research context worthy of further multidisciplinary scrutiny.

[†]Source: https://www.coronawarn.app/en/analysis/, retrieved February 1, 2022.

[‡]Source: https://www.data.gouv.fr/en/datasets/metriques-dutilisation-de-lapplication-tousanticovid/, retrieved February 1, 2022.

### 8.1.2 User Misperceptions of Security and Privacy

**1. Cyber Threat Intelligence – CTI Sharing Platforms**

Turning our attention to user misperceptions that can lead to negative security and privacy outcomes, in the CTI sharing context we discussed about two prominent types which are associated with the distribution of threat intel (Chapters 3 and 4). The first misperception relates to *CTI oversharing*, and the second to *CTI undersharing*. Both can give rise to a *false sense of security* as well as a *false sense of goal achievement*.

In addition to inadvertent leakage of privacy-sensitive data, which can carry a myriad of consequences, *CTI oversharing* can also be associated with a host of security-related implications, such as self-exposing exploitable vulnerabilities or impeding a successful response to a cyber attack as the premature disclosure of CTI can alert the attacker in different ways. In similar fashion, *CTI undersharing* can result in threat intel not reaching the intended parties, inducing a misalignment between what happens in reality and the perception as to whom the shared CTI reaches. One direct consequence is that the sharing community can fail to increase their preparedness levels by accidentally confining vital CTI. Both *over-* and *undersharing* can in turn potentially contribute to misconceptions as to how a specific CTI sharing platform works as well impact its perceived usefulness and appeal, and ultimately its adoption.

In Chapter 4 we brought to the fore this question of user misperceptions of the extent of information sharing i.e., whether users of a CTI sharing platform have an accurate understanding as to how far information travels when shared in a CTI sharing platform and whom it reaches. We laid out the social and technical components we deemed necessary in order to investigate and detect such misperceptions, however, conducting user studies that would provide the needed insights and inputs on behalf of CTI sharing platform users is beyond the scope of this thesis and is recommended as a future research direction.

**2. Secure & Private Communication – Secure Email**

In our second research context, misperceptions about the security and privacy guarantees offered by the studied email system related to misinterpretations of its traffic-light inspired indicators and their constituent elements (icon shapes, privacy rating labels, explanations).

Our preliminary analysis of $\mathsf{p} \equiv \mathsf{p}$ (Chapter 5) highlighted that the system's security and privacy indicators could potentially induce a *false sense of security* as well as a *false sense of insecurity* among people as they interact with the system. Motivated to better understand how users perceive the indicators, we conducted the afore-mentioned series of studies with

prospective p ≡ p users (Chapter 6). The results of the first batch of studies, which investigated the default version of the indicators, suggested profound misinterpretations that could easily result in people not being able to determine the protection applied to incoming and outgoing email messages in different communication scanarios. A follow up investigation of the new set of redesigned indicators, showed more promising results. Nevertheless, the indicator representing the privacy state *Secure* remained problematic as it was perceived as confusing due to the contradictory cues of its privacy rating label on the one hand, and the indicator's color and shape, on the other hand. Non-expert users who are unaware of the technicalities of public-key infrastructure and the ceremonies that are necessary to ensure that communication partners are not subjected to a man-in-the-middle attack, might be overly confident in the security and privacy guarantees provided in the *Secure state*. At the same time, for other users the indicator might induce a *sense of insecurity* even though the guarantees provided in this state are on par if not higher than in many end-to-end instant messaging systems that the user may otherwise adopt and use without hesitation (either as a conscious decision or due to a lack of an extensive threat and attacker model). To address such conundrums, (difficult) design choices need to be made. They might not be perfect, but probably better than the status quo which could negatively impact both secure use as well as adoption. UX design methods can play a key role here to iteratively improve the product, service, or system based on insights by the users we are designing for.

One key insight from this investigation relates to the suitability of the traffic-light metaphor for use in the cybersecurity and digital privacy context. When attempting to deploy the traffic light semantic within security and privacy indicators, the key question to ask is how much security and privacy information do we actually want to communicate to users and can this be done effectively, given the finite number of states that traffic light systems can support.

### 3. Digital Health Technology – COVID-19 Contact Tracing Applications

When it comes to user perceptions of security and privacy in the context of COVID-19 digital contact tracing, we observed a number of misconceptions with respect to the national contact tracing apps of France and Germany. As presented in Section 7.5.5, these related to capabilities of the government and/or contact tracing app developers to collect different types of personal information and re-identify users. The most voiced misperceptions revolved around *location tracking*. While they were mostly expressed as security and privacy concerns that inhibited adoption, location related misperceptions were also mentioned by contact tracing app adopters who believed or expected the app to offer additional function-

ality based on location data and related metadata. These findings are in line with other research conducted in Germany [161] where the study participants wrongly thought that Corona-warn-app would inform them if infected people were nearby or the app would enable the government to track them, detect violations of quarantine, access their phone contacts, etc. Misperceptions around geo-location as well as the collection and sharing of personal data were also reported in France, where they were manifested as privacy concerns that had impact[§] on the willingness to adopt and use the app [245].

Among other measures, a great deal of research on adoption of COVID-19 contact tracing apps, including ours, has called for clearer and more targeted public communication by the authorities in an effort to motivate app uptake among the population by promoting the societal benefits as well as demystifying the privacy implications associated with digital contact tracing [154, 155, 161, 245, 343, 344]. However, should it be a surprise at all that so many citizens failed to grasp the actual privacy threats and implications associated with contact tracing apps when consensus was not reached even among the security and privacy community [356], especially at the early stages of the pandemic? Distrust in digital contact tracing and concerns of surveillance can only be exacerbated when authorities try to use available digital contact tracing data for purposes other than contact tracing, such as criminal investigations [275]. One such recent attempt in January 2022 in Germany [88] revolved around the digital presence tracing system called Luca-app [80], which transmits contact data to health authorities as part of contact tracking requirements when visitors attend an event or check in at an establishment[¶]. While this case was not linked to Corona-warn-app, such instances of data misuse by authorities (even if done for understandable reasons) can only undermine public trust and contribute towards users' misunderstandings of how contact tracing apps work, what is being collected, and what the authorities and others are able to do with the exchanged digital contact tracing data.

A takeaway from our investigation is that clear and transparent communication is necessary to alleviate different security and privacy concerns and clarify misunderstandings around digital contact tracing. However, to a large degree the voiced concerns go beyond the contact tracing apps themselves and require a more holistic perspective to understand the different country-specific and contextual factors that impact trust and adoption.

[§]Just like in our case, such concerns played a significant role, but the main reason for non-adoption was attributed to the potential lack of effectiveness of the StopCovid/TousAntiCovid app [245].

[¶]A preliminary security analysis of the Luca tracing system, reported in 2021, highlighted a number of potential harms to individuals, venues, and communities [319].

### 8.1.3 Methodological Approaches to Detecting User Misperceptions of Security & Privacy

In this thesis, we presented two conceptual frameworks for socio-technical security analysis of systems (Chapter 4 and 5). The two approaches share the same fundamental principle that both technical and user aspects need to be taken in together for a joint analysis of certain properties pertaining to the security and privacy of the system under investigation. By comparing the *objective* security and privacy guarantees provided by the system and the *subjective* guarantees as perceived by users, the goal of the frameworks is to detect user misperceptions of security and privacy or identify critical points in the interaction that could lead to negative security and privacy outcomes.

In Chapter 4, we presented our theoretical model of a workflow and toolchain that seeks to detect cases of information *oversharing* and *undersharing* in the context of a CTI platform, like MISP. We described what social and technical components would be necessary to achieve this goal and how such a framework could be used for *(i)* conducting a security analysis / audit of exchanged CTI events; *(ii)* experimenting with different distribution options and simulating what impact in terms of over or undersharing that could entail; *(iii)* training purposes in the CTI sharing context. The proposed framework, however, is only at the conceptual level and future work, involving technical and user research, would be required to validate the proposed model and its potential benefits.

In Chapter 5, we introduced *multi-layered user journeys*, our second framework which is characterized by a visual approach to representing user goals, actions, and perceptions with respect to a certain security or privacy-critical system. We instantiated the framework within the context of the secure email system $\mathsf{p} \equiv \mathsf{p}$, and described a subsequent system-user alignment model that is open to formalization and automatic verification of security and privacy properties. We showed how our approach can be deployed in a goal-directed interaction to identify instances where a user could experience a *false sense* of security, insecurity, goal achievement as well as goal inachievement, and what the security and/or adoption implications of those misperceptions are. The preliminary findings from this investigation pointed to $\mathsf{p} \equiv \mathsf{p}$'s security and privacy indicators as potential triggers of user misperceptions, which directed our subsequent research efforts in that direction (Chapter 6).

A key takeaway regarding both afore-mentioned frameworks is that they are not intended to represent generic models of how humans interact with a specific security protocol or ceremony. Instead they need to be instantiated within a specific context if we want to use them for an analysis of a particular system's security.

## 8.2 Consolidated Contributions

The thesis makes a number of contributions outlined below. They are grouped under the corresponding research contribution type as inspired by the classification of Wobbrock et Kientz [376].

### Empirical Contributions

Cyber Threat Intelligence – CTI Sharing Platforms:

- First mixed-methods UX investigation of a sharing platform in the CTI context;
- Establishment of a UX benchmark that subsequent investigations of MISP or other CTI sharing platforms can compare against;
- Actionable inputs and discussion of key UX findings that CTI sharing platforms should take into account from an aesthetic, pragmatic, and hedonic perspective.

Secure and Private Communication – Secure Email:

- Insights into experiential aspects relating to the use/anticipated use of a secure email system;
- Emotion elicitations and user interpretations of security and privacy indicators inspired by the ubiquitous metaphor of traffic lights;
- Discussion on the role of different indicator cues and of onboarding tutorials in users' evaluations of security and privacy indicator adequacy.

Digital Health Technology – COVID-19 contact tracing applications:

- Greater granularity and understanding of contact tracing app adoption and non-adoption factors at the early stages of contact tracing app development and deployment;
- Discussion of the perceived benefits, drawbacks and threat models among adopters and non-adopters of contact tracing apps in France and Germany;
- Insights into security and privacy misperceptions of contact tracing apps;
- Evidence-informed recommendations for practice and policy regarding experiential aspects of contact tracing apps.

**Methodological Contributions**

- New methodological framework for user experience mapping across security ceremonies i.e., *multi-layered user journey*;
- New methodological framework open to formalization and automatic verification of misalignments between system and user values i.e., *system-user alignment model*.

**Theoretical/Conceptual Contributions**

- New conceptual framework for analyzing user (mis)perceptions in CTI sharing platforms, with a focus on CTI *oversharing* and *undersharing*;
- Definition and formal specification of new socio-technical security properties, applied within the context of a system-user alignment model.

**Dataset Contributions**

- User study datasets and supplementary materials published to open science repositories and/or provided as appendix.

## 8.3 Limitations and Future Work Directions

Throughout Chapters 3–7, which present the core of our research efforts in this thesis, we provided respective Limitations and Future Work sections. We reflected on the different factors that potentially limited our findings and discussed how future research could address those limitations. Moving from the individual chapters to the thesis as a whole, we find the following points worth highlighting.

Framework Evaluation. In line with the third objective in this thesis, we explored and proposed methodological approaches to incorporating users' (mis)perceptions in the socio-technical security analysis of systems. A natural extension of this work is to perform an evaluation of the proposed frameworks. This would be beneficial not only within the same cybersecurity and digital privacy contexts presented in this thesis, but also in new contexts. In an ideal setting, the frameworks could be deployed within an iterative design approach to building security or privacy-critical systems throughout different stages of the system design lifecycle. This could give system designers the opportunity to incorporate any possible findings yielded by these frameworks into subsequent design iterations.

EVOLVING USER EXPERIENCE. As UX is dynamic, highly-contextual and subjective, it is important to keep in mind how it evolves over time from the perspective of different (types of) users. In our proposed frameworks the user aspects represent snapshots of particular dimensions of the UX at particular moments in time. This imposes certain requirements upon the design of the system-user interactions and the mapping of the security and privacy perceptions in our models. In particular, this means that new instances of the multi-layered user journeys and system-user alignment models need to be created whenever we want to incorporate changes to the system design or when the experience of the user evolves. A future work direction could explore the possibilities of augmenting the proposed frameworks with dynamic aspects of the UX (user, system and context-level changes).

ATTACKER. The attacker was knowingly out of scope in our investigations and conceptual proposals. This was a conscious decision as the focus of our work was on the interaction between systems and non-malicious users, investigating different socio-technical aspects that could negatively impact security and privacy outcomes even without the presence of adversaries. Nevertheless, we believe that incorporating the attacker in the discussion of the overall security of a system is of prime importance. Thus, one future work direction could look into the role of the attacker in our proposed frameworks and contexts of investigation.

## 8.4 LOOKING AHEAD

In an increasingly connected world where the potential for malicious security and privacy attacks as well as inadvertent mistakes will be amplified by the ubiquity of digitalization, the speed at which secure systems will need to be deployed and adopted is going to be of prime importance. This means that in addition to providing higher levels of security and privacy as opposed to their competing alternatives, systems that strive to succeed in terms of end user adoption and continued use will also need to be superior in terms of their user experience. To up their user experience propositions, such systems would need to take advantage of the opportunities presented to them.

Opportunities arise as users become more conscious of the numerous security and privacy issues associated with the use of digital products, services, and systems, and in particular, when people look for alternatives which are more in line with their security and privacy expectations. Furthermore, as new user needs emerge and constantly evolve as their practice, experience, and context change over time [51], designers and developers of secure and privacy-preserving systems can capitalize on this state of flux by pioneering new ideas and artifacts that support rich interactions and meaningful experiences. To meet this aspira-

tion, this thesis promotes the view that user experience design needs to be fundamentally reprioritized and repositioned at the forefront of the design and development efforts of next generation products, services, and systems, which otherwise take pride in their security and privacy guarantees. While being conscious of the constraints imposed by the security and privacy context, the argument that is raised, nevertheless, attempts to stress the necessity to put UX considerations on par with the security and privacy aspects. This is important not only in view of the crucial role humans play in ensuring the overall security of a socio-technical system [125], but also their motivation and goal-orientation with respect to a system, its use, adaptation, etc. [50]. This view goes beyond applying lessons learned and adopting best practices from the academic and practitioner fields that are concerned with UX and socio-technical issues. It calls for setting new trends and reimagining the interaction with new digital products, services, and systems more broadly, with the added benefit that they would strive to be secure and privacy-respecting by design and by default. Thus, the security and privacy aspects could be an added point taken favorably by the informed and security/privacy conscious user, yet the superior UX would be the key selling point that would drive the adoption of those new digital offerings more generally.

For this vision to materialize, a number of shifts would need to be promoted. According to one recent study, missing knowledge of user-centered methods and lack of awareness about usable security and privacy are keeping the mythical trade-off between security and usability very much alive in some professional software development teams [157]. The responsibility cannot fall solely on the security and privacy engineers, however, but these challenging circumstances need to be a concern for everyone in the broader *ecosystem*. If HCI research is about solving problems related to human use of computing [257], we need to become better at raising awareness about the numerous challenges and opportunities in cybersecurity among the current and next generation of HCI/UX researchers and designers. In particular, a key gap can be filled by motivated HCI researchers and UX designers who are proactive about applying their methods, practices and skills within new contexts that are inherently associated with new design constraints. This shift starts with more interdisciplinary education and practice all the way to systemic structures that promote and reward holistic solutions that are mindful of the latest security and privacy threats, user expectations, and regulatory requirements.

To this end, our work in this thesis can serve as a demonstration that there are UX methods and practices that can be borrowed and successfully applied in the cybersecurity and digital privacy context. We hope that by motivating our reasons for deploying such methods, and our accounts of using them, raises awareness among researchers and practitioners in the security and privacy domain, promoting their adoption and further refinement.

# References


[1] 2001. *Where the Action is: The Foundations of Embodied Interaction*. MIT Press, Cambridge, MA, USA.

[2] Johannes Abeler, Sam Altmann, Luke Milsom, Séverine Toussaert, and Hannah Zillessen. 2020. Support in the UK for app-based contact tracing of COVID-19. (March 26, 2020). https://osf.io/huqtr/

[3] Ruba Abu-Salma, Elissa M Redmiles, Blase Ur, and Miranda Wei. 2018. Exploring User Mental Models of End-to-End Encrypted Communication Tools. *8th USENIX Workshop on Free and Open Communications on the Internet (FOCI)* (2018).

[4] Ruba Abu-Salma, Martina Angela Sasse, Joseph Bonneau, Anastasia Danilova, Alena Naiakshina, and Matthew Smith. 2017. Obstacles to the Adoption of Secure Communication Tools. In *2017 IEEE Symposium on Security and Privacy (SP)*. 137–153. https://doi.org/10.1109/SP.2017.65

[5] Matthew Abueg, Robert Hinch, Neo Wu, Luyang Liu, William Probert, Austin Wu, Paul Eastham, Yusef Shafi, Matt Rosencrantz, Michael Dikovsky, Zhao Cheng, Anel Nurtay, Lucie Abeler-Dörner, David Bonsall, Michael V. McConnell, Shawn O'Banion, and Christophe Fraser. 2020. Modeling the combined effect of digital exposure notification and non-pharmaceutical interventions on the COVID-19 epidemic in Washington state. *medRxiv* (2020). https://doi.org/10.1101/2020.08.29.20184135

[6] Mark S. Ackerman. 2000. The Intellectual Challenge of CSCW: The Gap between Social Requirements and Technical Feasibility. *Hum.-Comput. Interact.* 15, 2 (Sept. 2000), 179–203. https://doi.org/10.1207/S15327051HCI1523_5

[7] Alessandro Acquisti, Idris Adjerid, Rebecca Balebako, Laura Brandimarte, Lorrie Faith Cranor, Saranga Komanduri, Pedro Giovanni Leon, Norman Sadeh, Florian Schaub, Manya Sleeper, Yang Wang, and Shomir Wilson. 2017. Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online. *ACM Comput. Surv.* 50, 3, Article 44 (Aug. 2017), 41 pages. https://doi.org/10.1145/3054926

[8] Anne Adams and Martina Angela Sasse. 1999. Users Are Not the Enemy. *Commun. ACM* 42, 12 (dec 1999), 40–46. https://doi.org/10.1145/322796.322806

[9] Enoch Agyepong, Yulia Cherdantseva, Philipp Reinecke, and Pete Burnap. 2020. Challenges and performance metrics for security operations center analysts: a systematic review. *Journal of Cyber Security Technology* 4, 3 (July 2020), 125–152. https://doi.org/10.1080/23742917.2019.1698178

[10] Jan M. Ahrend, Marina Jirotka, and Kevin Jones. 2016. On the collaborative practices of cyber threat intelligence analysts to develop and utilize tacit Threat and Defence

Knowledge. *2016 International Conference on Cyber Situational Awareness, Data Analytics and Assessment, CyberSA 2016* (2016). https://doi.org/10.1109/CyberSA.2016.7503279

[11] Alex Ainslie, Adrienne Porter Felt, Robert W. Reeder, Somas Thyagaraja, Helen Harris, Alan Bettes, Jeff Grimes, and Sunny Consolvo. 2015. Improving SSL Warnings. (2015), 2893–2902.

[12] Manal Almalki and Anna Giannicchi. 2021. Health Apps for Combating COVID-19: Descriptive Review and Taxonomy. *JMIR Mhealth Uhealth* 9, 3 (2 Mar 2021). https://doi.org/10.2196/24322

[13] Samuel Altmann, Luke Milsom, Hannah Zillessen, Raffaele Blasone, Frederic Gerdon, Ruben Bach, Frauke Kreuter, Daniele Nosenzo, Séverine Toussaert, and Johannes Abeler. 2020. Acceptability of App-Based Contact Tracing for COVID-19: Cross-Country Survey Study. *JMIR Mhealth Uhealth* 8, 8 (28 Aug 2020), e19857. https://doi.org/10.2196/19857

[14] 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. *Conference on Human Factors in Computing Systems - Proceedings* 2015-April (2015), 2883–2892.

[15] Ross Anderson. 2008. *Security engineering : a guide to building dependable distributed systems* (2nd ed.). Wiley, Indianapolis.

[16] p ≡ p foundation. 2022. p ≡ p Foundation Developer Documentation. Retrieved January 15, 2022 from https://dev.pep.foundation

[17] p ≡ p foundation. 2022. p ≡ p software. Retrieved January 15, 2022 from https://pep.foundation/pep-software/index.html

[18] p ≡ p security. 2022. Welcome to p ≡ p Documentation. Retrieved January 15, 2022 from https://www.pep.security/docs/en/index.html

[19] Apple Inc. and Google Inc. 2020. Privacy-Preserving Contact Tracing. (April 10, 2020). Retrieved August 16, 2021 from https://covid19.apple.com/contacttracing.

[20] Farzaneh Asgharpour, Debin Liu, and L. Jean Camp. 2007. Mental Models of Computer Security Risks. In *Workshop on the Economics of Information Security, Pittsburgh, PA (USA)*.

[21] W. Ross Ashby. 1956. *An Introduction to Cybernetics*. Chapman & Hall, London. http://pcp.vub.ac.be/books/IntroCyb.pdf

[22] Derek Atkins, William Stallings, and Philip Zimmermann. 1996. *PGP Message Exchange Formats*. RFC 1991. RFC Editor. https://doi.org/10.17487/RFC1991

[23] Erinn Atwater, Cecylia Bocovich, Urs Hengartner, Ed Lank, and Ian Goldberg. 2015. Leading Johnny to Water: Designing for Usability and Trust. In *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*. USENIX Association, Ottawa, 69–88. https://www.usenix.org/conference/soups2015/proceedings/presentation/atwater

[24] Leif Azzopardi and Guido Zuccon. 2019. Building Economic Models of Human Computer Interaction. In *Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems (CHI EA '19)*. Association for Computing Machinery, New York, NY, USA, 1–4. https://doi.org/10.1145/3290607.3298809

[25] Wei Bai, Doowon Kim, Moses Namara, Yichen Qian, Patrick Gage Kelley, and Michelle L Mazurek. 2016. An Inconvenient Trust: User Attitudes Toward Security and Usability Tradeoffs for Key-Directory Encryption Systems. *Symposium On Usable Privacy and Security (SOUPS)* Soups (2016), 113–130.

[26] W Bai, D Kim, M Namara, Y Qian, P G Kelley, and M L Mazurek. 2017. Balancing Security and Usability in Encrypted Email. *IEEE Internet Computing* 21, 3 (2017), 30–38.

[27] Christel Baier and Joost-Pieter Katoen. 2008. *Principles of model checking*. MIT Press.

[28] Dirk Balfanz, Glenn Durfee, Rebecca E. Grinter, Diana K. Smetters, and Paul Stewart. 2004. Network-in-a-Box: How to Set Up a Secure Wireless Network in Under a Minute. In *13th USENIX Security Symposium (USENIX Security 04)*. USENIX Association, San Diego, CA. https://www.usenix.org/conference/13th-usenix-security-symposium/network-box-how-set-secure-wireless-network-under-minute

[29] Liam J Bannon. 1995. From human factors to human actors: The role of psychology and human-computer interaction studies in system design. In *Readings in human–computer interaction*. Elsevier, 205–214.

[30] Javier A. Bargas-Avila and Kasper Hornbæk. 2011. Old Wine in New Bottles or Novel Challenges: A Critical Analysis of Empirical Studies of User Experience. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '11)*. Association for Computing Machinery, New York, NY, USA, 2689–2698. https://doi.org/10.1145/1978942.1979336

[31] Sean Barnum. 2012. Standardizing cyber threat intelligence information with the structured threat information expression (stix). *Mitre Corporation* 11 (2012), 1–22.

[32] Steffen Bartsch and Melanie Volkamer. 2013. Effectively communicate risks for diverse users: A mental-models approach for individualized security interventions. In *INFORMATIK 2013 – Informatik angepasst an Mensch, Organisation und Umwelt*, Matthias Horbach (Ed.). Gesellschaft für Informatik e.V., Bonn, 1971–1984.

[33] Sara Bauer, Daniel Fischer, Clemens Sauerwein, Simon Latzel, Dirk Stelzer, and Ruth Breu. 2020. Towards an Evaluation Framework for Threat Intelligence Sharing

Platforms. In *53rd Hawaii International Conference on System Sciences, HICSS 2020, Maui, Hawaii, USA, January 7-10, 2020*. ScholarSpace, 1–10. http://hdl.handle.net/10125/63978

[34] Lars Baumgärtner, Alexandra Dmitrienko, Bernd Freisleben, Alexander Gruler, Jonas Höchst, Joshua Kühlberg, Mira Mezini, Richard Mitev, Markus Miettinen, Anel Muhamedagic, Thien Duc Nguyen, Alvar Penning, Dermot Frederik Pustelnik, Filipp Roos, Ahmad-Reza Sadeghi, Michael Schwarz, and Christian Uhl. 2020. Mind the GAP: Security & Privacy Risks of Contact Tracing Apps. arXiv:cs.CR/2006.05914

[35] Gordon Baxter and Ian Sommerville. 2011. Socio-technical systems: From design methods to systems engineering. *Interacting with Computers* 23, 1 (jan 2011), 4–17.

[36] Michel Beaudouin-Lafon, Susanne Bødker, and Wendy E. Mackay. 2021. Generative Theories of Interaction. *ACM Trans. Comput.-Hum. Interact.* 28, 6, Article 45 (nov 2021), 54 pages. https://doi.org/10.1145/3468505

[37] Bernhard Beckert and Gerd Beuster. 2006. A Method for Formalizing, Analyzing, and Verifying Secure User Interfaces BT - Formal Methods and Software Engineering, Zhiming Liu and Jifeng He (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 55–73.

[38] Giampaolo Bella and Lizzie Coles-Kemp. 2012. Layered Analysis of Security Ceremonies. In *Information Security and Privacy Research*, Dimitris Gritzalis, Steven Furnell, and Marianthi Theoharidou (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 273–286.

[39] Giampaolo Bella, Paul Curzon, and Gabriele Lenzini. 2015. Service security and privacy as a socio-technical problem. *Journal of Computer Security* 23, 5 (2015), 563–585. Issue Security and High Performance Computing Systems. https://doi.org/10.3233/JCS-150536

[40] Victoria Bellotti and Abigail Sellen. 1993. Design for Privacy in Ubiquitous Computing Environments. In *Proceedings of the Third Conference on European Conference on Computer-Supported Cooperative Work (ECSCW'93)*. Kluwer Academic Publishers, USA, 77–92.

[41] Britt Elise Bente, Jan Willem Jaap Roderick van 't Klooster, Maud Annemarie Schreijer, Lea Berkemeier, Joris Elmar van Gend, Peter Jan Hendrik Slijkhuis, Saskia Marion Kelders, and Julia Elisabeth Wilhelmina Cornelia van Gemert-Pijnen. 2021. The Dutch COVID-19 Contact Tracing App (the CoronaMelder): Usability Study. *JMIR Form Res* 5, 3 (26 Mar 2021). https://doi.org/10.2196/27882

[42] Rasekhar Bhagavatula, Blase Ur, Kevin Iacovino, Su Mon Kywe, Lorrie Faith Cranor, and Marios Savvides. 2015. Biometric authentication on iPhone and Android: Usability, perceptions, and influences on adoption. (2015).

[43] Jaspreet Bhatia, Travis D. Breaux, Liora Friedberg, Hanan Hibshi, and Daniel Smullen. 2016. Privacy risk in cybersecurity data sharing. *WISCS 2016 - Proceedings of the 2016 ACM Workshop on Information Sharing and Collaborative Security, co-located with CCS 2016* (2016), 57–64. https://doi.org/10.1145/2994539.2994541

[44] Volker Birk, Hernâni Marques, and Bernie Hoeneisen. 2020. *pretty Easy privacy (pEp): Privacy by Default*. Internet-Draft draft-birk-pep-06. Internet Engineering Task Force. https://datatracker.ietf.org/doc/html/draft-birk-pep-06 Work in Progress.

[45] Serena O Blacklow, Sarah Lisker, Madelena Y Ng, Urmimala Sarkar, and Courtney Lyles. 2021. Usability, inclusivity, and content evaluation of COVID-19 contact tracing apps in the United States. *Journal of the American Medical Informatics Association* 28, 9 (06 2021), 1982–1989. https://doi.org/10.1093/jamia/ocab093

[46] Jim Blythe, Jean Camp, and Vaibhav Garg. 2011. Targeted risk communication for computer security. *International Conference on Intelligent User Interfaces, Proceedings IUI* (2011), 295–298.

[47] Jim Blythe and L. Jean Camp. 2012. Implementing Mental Models. In *2012 IEEE Symposium on Security and Privacy Workshops*. 86–90. https://doi.org/10.1109/SPW.2012.31

[48] Susanne Bødker. 2006. When Second Wave HCI Meets Third Wave Challenges. In *Proceedings of the 4th Nordic Conference on Human-Computer Interaction: Changing Roles (NordiCHI '06)*. Association for Computing Machinery, New York, NY, USA, 1–8. https://doi.org/10.1145/1182475.1182476

[49] Susanne Bødker. 2015. Third-Wave HCI, 10 Years Later—Participation and Sharing. *Interactions* 22, 5 (Aug. 2015), 24–31. https://doi.org/10.1145/2804405

[50] Susanne Bødker and Clemens Nylandsted Klokmose. 2011. The Human–Artifact Model: An Activity Theoretical Approach to Artifact Ecologies. *Human–Computer Interaction* 26, 4 (2011), 315–371. https://doi.org/10.1080/07370024.2011.626709 arXiv:https://doi.org/10.1080/07370024.2011.626709

[51] Susanne Bødker and Clemens Nylandsted Klokmose. 2012. Dynamics in Artifact Ecologies. In *Proceedings of the 7th Nordic Conference on Human-Computer Interaction: Making Sense Through Design (NordiCHI '12)*. Association for Computing Machinery, New York, NY, USA, 448–457. https://doi.org/10.1145/2399016.2399085

[52] Philipp Boeing and Yihan Wang. 2021. Decoding China's COVID-19 'virus exceptionalism': Community-based digital contact tracing in Wuhan. *R&D Management* 51, 4 (2021), 339–351. https://doi.org/10.1111/radm.12464 arXiv:https://onlinelibrary.wiley.com/doi/pdf/10.1111/radm.12464

[53] David Botta, Kasia Muldner, Kirstie Hawkey, and Konstantin Beznosov. 2011. Toward understanding distributed cognition in IT security management: The role of cues and

norms. *Cognition, Technology and Work* 13, 2 (2011), 121–134. https://doi.org/10.1007/s10111-010-0159-y

[54] David Botta, Rodrigo Werlinger, André Gagné, Konstantin Beznosov, Lee Iverson, Sidney Fels, and Brian Fisher. 2007. Towards understanding IT security professionals and their tools. *ACM International Conference Proceeding Series* 229 (2007), 100–111. https://doi.org/10.1145/1280680.1280693

[55] Isobel Braithwaite, Thomas Callender, Miriam Bullock, and Robert W Aldridge. 2020. Automated and partly automated contact tracing: a systematic review to inform the control of COVID-19. *The Lancet Digital Health* 2, 11 (nov 2020). https://doi.org/10.1016/S2589-7500(20)30184-9

[56] Scott Brave and Clifford Nass. 2007. Emotion in Human-Computer Interaction. In *The Human-Computer Interaction Handbook: Fundamentals, Evolving Technologies, and Emerging Applications* (2nd ed.), Andrew Sears and Julie A. Jacko (Eds.). L. Erlbaum Associates Inc., Boca Raton, USA, 77–92.

[57] Cristian Bravo-Lillo, Lorrie Faith Cranor, Saranga Komanduri, Julie Downs, and Saranga Komanduri. 2011. Bridging the Gap in Computer Security Warnings: A Mental Model Approach. *IEEE Security and Privacy* 9, 2 (mar 2011), 18–26.

[58] Jon Callas, Lutz Donnerhacke, Hal Finney, David Shaw, and Rodney Thayer. 2007. *OpenPGP Message Format*. RFC 4880. RFC Editor. https://doi.org/10.17487/RFC4880

[59] L. Jean Camp. 2009. Mental models of privacy and security. *IEEE Technology and Society Magazine* 28, 3 (2009), 37–46. https://doi.org/10.1109/MTS.2009.934142

[60] L. Jean Camp. 2011. Mental Models of Privacy and Security. *SSRN Electronic Journal* (2011).

[61] Steve Caplin. 2001. *ICON Design: Graphic Icons in Computer Interface Design*. Watson-Guptill Publications, Inc., USA.

[62] Marcelo Carlomagno Carlos, Jean Everson Martina, Geraint Price, and Ricardo Felipe Custódio. 2013. An updated threat model for security ceremonies. (2013), 1836. https://doi.org/10.1145/2480362.2480705

[63] Claude Castelluccia, Nataliia Bielova, Antoine Boutet, Mathieu Cunche, Cédric Lauradoux, Daniel Le Métayer, and Vincent Roca. 2020. ROBERT: ROBust and privacy-presERving proximity Tracing. (May 2020). https://hal.inria.fr/hal-02611265

[64] Justin Chan, Landon P. Cox, Dean P. Foster, Shyam Gollakota, Eric Horvitz, Joseph Jaeger, Sham M. Kakade, Tadayoshi Kohno, John Langford, Jonathan Larson, Puneet Sharma, Sudheesh Singanamalla, Jacob E. Sunshine, and Stefano Tessaro. 2020. PACT: Privacy-Sensitive Protocols And Mechanisms for Mobile Contact Tracing.

*IEEE Data Eng. Bull.* 43, 2 (2020), 15–35. http://sites.computer.org/debull/A20june/p15.pdf

[65] Sathya Chandran, Xinming Ou, Alexandru G. Bardas, Jacob Case, Michael Wesch, John McHugh, and S. Raj Rajagopalan. 2019. A human capital model for mitigating security analyst burnout. *SOUPS 2015 - Proceedings of the 11th Symposium on Usable Privacy and Security* (2019), 347–359.

[66] Sonia Chiasson and Paul C. van Oorschot. 2015. Quantifying the security advantage of password expiration policies. *Designs, Codes and Cryptography* 77, 2 (2015), 401–408. https://doi.org/10.1007/s10623-015-0071-9

[67] Fabio Chiusi, Sarah Fischer, Matthias Spielkamp, Rosamunde van Brakel, Brigitte Alfter, Maris Männiste, Tuukka Lehtiniemi, Minna Ruckenstein, Nicolas Kayser-Bril, Louisa Well, et al. 2020. Automated Decision-Making Systems in the COVID-19 Pandemic: A European Perspective. (2020).

[68] A. Cimatti, E.M. Clarke, F. Giunchiglia, and M. Roveri. 1999. NuSMV: a new Symbolic Model Verifier. In *Proceedings Eleventh Conference on Computer-Aided Verification (CAV'99) (Lecture Notes in Computer Science)*, N. Halbwachs and D. Peled (Eds.). Springer, Trento, Italy, 495–499.

[69] CIRCL. 2021. CIRCL – Computer Incident Response Center Luxembourg. Retrieved May 15, 2021 from https://www.circl.lu Last accessed on May 15, 2021.

[70] CIRCL. 2021. MISP - Malware Information Sharing Platform and Threat Sharing - Training Materials. Retrieved May 15, 2021 from https://www.circl.lu/services/misp-training-materials/ Last accessed on May 15, 2021.

[71] CISA. 2020. Alert (AA20-352A) Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations. https://us-cert.cisa.gov/ncas/alerts/aa20-352a, Last accessed on May 15, 2021.

[72] CISA. 2021. Alert (AA21-131A) DarkSide Ransomware: Best Practices for Preventing Business Disruption from Ransomware Attacks. Retrieved May 15, 2021 from https://us-cert.cisa.gov/ncas/alerts/aa21-131a Last accessed on May 15, 2021.

[73] Edmund M. Clarke and E. Allen Emerson. 1982. Design and Synthesis of Synchronization Skeletons Using Branching-Time Temporal Logic. In *Logic of Programs, Workshop*. Springer-Verlag, 52–71.

[74] Dave Clemente. 2013. Cybersecurity. In *Routledge Companion to Intelligence Studies*. Routledge, Chapter chapter26. https://doi.org/10.4324/9780203762721.ch26

[75] Adam B Cohen, Simon C Mathews, E Ray Dorsey, David W Bates, and Kyan Safavi. 2020. Direct-to-consumer digital health. *The Lancet Digital Health* 2, 4 (2020), e163–e165. https://doi.org/10.1016/S2589-7500(20)30057-1

[76] Vittoria Colizza, Eva Grill, Rafael Mikolajczyk, Ciro Cattuto, Adam Kucharski, Steven Riley, Michelle Kendall, Katrina Lythgoe, David Bonsall, Chris Wymant, Lucie Abeler-Dörner, Luca Ferretti, and Christophe Fraser. 2021. Time to evaluate COVID-19 contact-tracing apps. *Nature Medicine* 27, 3 (2021), 361–362. https://doi.org/10.1038/s41591-021-01236-6

[77] Lorrie Cranor and Simson Garfinkel. 2005. *Security and Usability: Designing Secure Systems that People Can Use*. O'Reilly Media, Inc.

[78] Lorrie Faith Cranor. 2008. A framework for reasoning about the human in the loop. *Proceedings of the 1st Conference on Usability, Psychology, and Security (UPSEC'08)* (2008), 1–15. https://doi.org/10.1109/MSP.2010.198

[79] Cas Cremers and Sjouke Mauw. 2012. *Operational semantics and verification of security protocols* (1st reprint. ed.). Springer, Berlin New York.

[80] culture4life. 2022. luca App - verschlüsselte Kontaktdatenübermittlung. Retrieved February 10, 2022 from https://www.luca-app.de

[81] Paul Curzon, Rimvydas Rukšėnas, and Ann Blandford. 2007. An approach to formal verification of human–computer interaction. *Formal Aspects of Computing* 19, 4 (01 Nov 2007), 513–550.

[82] Xavier de Carné de Carnavalet and Mohammad Mannan. 2014. From very weak to very strong: Analyzing password-strength meters. In *Network and Distributed System Security Symposium (NDSS 2014)*. Internet Society.

[83] Alexander De Luca, Alina Hang, Emanuel von Zezschwitz, and Heinrich Hussmann. 2015. I Feel Like I'm Taking Selfies All Day! Towards Understanding Biometric Authentication on Smartphones. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (CHI '15)*. Association for Computing Machinery, New York, NY, USA, 1411–1414. https://doi.org/10.1145/2702123.2702141

[84] Alessandra de Melo e Silva, João José Costa Gondim, Robson de Oliveira Albuquerque, and Luis Javier García Villalba. 2020. A methodology to evaluate standards and platforms within cyber threat intelligence. *Future Internet* 12, 6 (2020), 1–23. https://doi.org/10.3390/fi12060108

[85] Sergej Dechand, Alena Naiakshina, Anastasia Danilova, and Matthew Smith. 2019. 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)*. 401–415. https://doi.org/10.1109/EuroSP.2019.00037

[86] Asaf Degani and Michael Heymann. 2002. Formal Verification of Human-Automation Interaction. *Human Factors* 44, 1 (2002), 28–43. https://doi.org/10.1518/0018720024494838

[87] Deutsche Welle. 2020. In U-turn, Germany backs Google and Apple on virus app. (April 26, 2020). Retrieved August 16, 2021 from https://p.dw.com/p/3bRKp.

[88] Deutsche Welle. 2022. German police under fire for misuse of COVID contact tracing app. (January 11, 2022). Retrieved February 10, 2022 from https://p.dw.com/p/45P8H.

[89] Rachna Dhamija, J. D. Tygar, and Marti Hearst. 2006. Why Phishing Works. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '06)*. ACM, New York, NY, USA, 581–590.

[90] Sarah Diefenbach, Nina Kolb, and Marc Hassenzahl. 2014. The 'Hedonic' in Human-Computer Interaction – History, Contributions, and Future Research Directions. *Proc. DIS 2014* (2014), 305–314. https://doi.org/10.1145/2598510.2598549

[91] Heribert Dieter. 2020. Germany in the COVID-19 crisis: Poster child or just lucky? *The Journal of Australian Political Economy* 85 (2020), 101–107. https://search.informit.org/doi/10.3316/ielapa.213086677935227

[92] Julie S. Downs, Mandy B. Holbrook, and Lorrie Faith Cranor. 2006. Decision strategies and susceptibility to phishing. *ACM International Conference Proceeding Series* 149 (2006), 79–90.

[93] V Dukhovni. 2014. *Opportunistic Security: Some Protection Most of the Time*. RFC 7435. RFC Editor. https://www.rfc-editor.org/info/rfc7435

[94] Zakir Durumeric, David Adrian, Ariana Mirian, James Kasten, Elie Bursztein, Nicolas Lidzborski, Kurt Thomas, Vijay Eranti, Michael Bailey, and J. Alex Halderman. 2015. Neither Snow Nor Rain Nor MITM...: An Empirical Analysis of Email Delivery Security. In *Proceedings of the 2015 Internet Measurement Conference (IMC '15)*. Association for Computing Machinery, New York, NY, USA, 27–39.

[95] Josiah Dykstra and Celeste Lyn Paul. 2018. Cyber Operations Stress Survey (COSS): Studying fatigue, frustration, and cognitive workload in cybersecurity operations. *11th USENIX Workshop on Cyber Security Experimentation and Test, CSET 2018, co-located with USENIX Security 2018* (2018).

[96] Ignacio Díaz-Oreiro, Gustavo López, Luis Quesada, and Luis A. Guerrero. 2019. Standardized Questionnaires for User Experience Evaluation: A Systematic Literature Review. *Proceedings* 31, 1 (2019). https://doi.org/10.3390/proceedings2019031014

[97] 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 SIGCHI Conference on Human Factors in Computing Systems (CHI '08)*. ACM, New York, NY, USA, 1065–1074.

[98] 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 SIGCHI Conference on Human Factors in Computing Systems (CHI '13)*. Association for Computing Machinery, New York, NY, USA, 2379–2388. https://doi.org/10.1145/2470654.2481329

[99] Mahmoud Elkhodr, Omar Mubin, Zainab Iftikhar, Maleeha Masood, Belal Alsinglawi, Suleman Shahid, and Fady Alnajjar. 2021. Technology, Privacy, and User Opinions of COVID-19 Mobile Apps for Contact Tracing: Systematic Search and Content Analysis. *J Med Internet Res* 23, 2 (9 Feb 2021). https://doi.org/10.2196/23467

[100] Michael Elkins. 1996. *MIME Security with Pretty Good Privacy (PGP)*. RFC 2015. RFC Editor. https://doi.org/10.17487/RFC2015

[101] Michael Elkins, Dave Del Torto, Raph Levien, and Thomas Roessler. 2001. *MIME Security with OpenPGP*. RFC 3156. RFC Editor. https://doi.org/10.17487/RFC3156

[102] Andrew J Elliot and Markus A Maier. 2012. Chapter two - Color-in-Context Theory. Advances in Experimental Social Psychology, Vol. 45. Academic Press, 61–125.

[103] Andrew J Elliot and Markus A Maier. 2014. Color Psychology: Effects of Perceiving Color on Psychological Functioning in Humans. *Annual Review of Psychology* 65, 1 (jan 2014), 95–120.

[104] Carl Ellison. 2007. Ceremony Design and Analysis. *Citeseer* 399 (2007), 1–17. http://eprint.iacr.org/2007/399

[105] Ahmed Elmokashfi, Joakim Sundnes, Amund Kvalbein, Valeriya Naumova, Sven-Arne Reinemo, Per Magne Florvaag, Håkon Kvale Stensland, and Olav Lysne. 2021. Nationwide rollout reveals efficacy of epidemic control through digital contact tracing. *medRxiv* (2021). https://doi.org/10.1101/2021.02.27.21252577

[106] ENISA. 2010. *Incentives and Challenges for Information Sharing in the Context of Network and Information Security*. Technical Report. European Union Agency for Network and Information Security, Heraklion.

[107] ENISA. 2013. *Detect, SHARE, Protect: Solutions for Improving Threat Data Exchange among CERTs*. Technical Report. European Union Agency for Network and Information Security, Heraklion.

[108] ENISA. 2014. *Study on cryptographic protocols*. Technical Report. European Union Agency for Network and Information Security, Heraklion. https://doi.org/10.2824/3739

[109] ENISA. 2015. *Cyber Security Information Sharing: An Overview of Regulatory and Non-regulatory Approaches*. Technical Report December. European Union Agency for Network and Information Security, Heraklion. 1–64 pages.

[110] ENISA. 2021. *ENISA Threat Landscape 2021*. Technical Report. European Union Agency for Network and Information Security, Heraklion. https://doi.org/10.2824/324797

[111] C. N. Enoch and L. Labuschagne. 2012. Project portfolio management: using fuzzy logic to determine the contribution of portfolio components to organizational objectives. Paper presented at PMI® Research and Education Conference, Limerick, Munster, Ireland. Project Management Institute, Newtown Square, PA.

[112] Thomas Erickson, David N. Smith, Wendy A. Kellogg, Mark Laff, John T. Richards, and Erin Bradner. 1999. Socially Translucent Systems: Social Proxies, Persistent Conversation, and the Design of "Babble". In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '99)*. Association for Computing Machinery, New York, NY, USA, 72–79. https://doi.org/10.1145/302979.302997

[113] EU. 2016. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). *Official Journal of the European Union* L119 (may 2016), 1–88. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L:2016:119:TOC

[114] EU. 2017. Regulation (EU) 2017/1369 of the European Parliament and of the Council of 4 July 2017 setting a framework for energy labelling and repealing Directive 2010/30/EU (Text with EEA relevance. ). *Official Journal of the European Union* L198 (2017), 1–23.

[115] European Centre for Disease Prevention and Control. 2020. *Updated projections of COVID-19 in the EU/EEA and the UK. (November 23, 2020)*. Technical Report. ECDC, Stockholm.

[116] European Centre for Disease Prevention and Control. 2022. COVID-19 situation update worldwide, as of week 4, updated 3 February 2022. Retrieved February 3, 2022. from https://www.ecdc.europa.eu/en/geographical-distribution-2019-ncov-cases

[117] European Commission. 2020. Coronavirus: EU interoperability gateway goes live, first contact tracing and warning apps linked to the system. (October 19, 2020). [Press release], Retrieved August 16, 2021 from https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1904.

[118] Europol. 2020. *Internet Organised Crime Threat Assessment (IOCTA) 2020*. Technical Report. European Union Agency for Law Enforcement Cooperation. 64 pages.

[119] Eurostat. 2021. Population on 1 January [TPS00001]. Retrieved August 7, 2021 from https://ec.europa.eu/eurostat/databrowser/bookmark/6ef61f16-dadc-42b1-a6ce-3ddfda4727e8?lang=en.

[120] Michael W Eysenck. 2015. Cognitive psychology : a student's handbook.

[121] Federal Government of Germany. 2020. Videokonferenz der Bundeskanzlerin mit den Regierungschefinnen und Regierungschefs der Länder. (October 28, 2020). [Press

release 381], Retrieved August 16, 2021 from https://www.bundesregierung.de/breg-de/suche/videokonferenz-der-bundeskanzlerin-mit-den-regierungschefinnen-und-regierungschefs-der-laender-am-28-oktober-2020-1805248.

[122] Adrienne Porter Felt, Robert W Reeder, Alex Ainslie, Helen Harris, Max Walker, Christopher Thompson, Mustafa Emre Acer, Elisabeth Morant, Sunny Consolvo, and U C Berkeley. 2016. Rethinking Connection Security Indicators. *the Symposium On Usable Privacy and Security (SOUPS)* Soups (2016), 1–14.

[123] Gina Fisk, Calvin Ardi, Neale Pickett, John Heidemann, Mike Fisk, and Christos Papadopoulos. 2015. Privacy principles for sharing cyber security data. *Proceedings - 2015 IEEE Security and Privacy Workshops, SPW 2015* (2015), 193–197. https://doi.org/10.1109/SPW.2015.23

[124] Ivan Flechais, Jens Riegelsberger, and M Angela Sasse. 2005. Divide and Conquer: The Role of Trust and Assurance in the Design of Secure Socio-technical Systems. In *Proceedings of the 2005 Workshop on New Security Paradigms*. ACM, New York, NY, USA, 33–41. https://doi.org/10.1145/1146269.1146280

[125] Ivan Flechais, Jens Riegelsberger, and Martina Angela Sasse. 2005. Divide and Conquer: The Role of Trust and Assurance in the Design of Secure Socio-technical Systems. In *Proceedings of the 2005 Workshop on New Security Paradigms (NSPW '05)*. ACM, New York, NY, USA, 33–41. https://doi.org/10.1145/1146269.1146280

[126] Steven Fokkinga. 2022. Negative emotion typology. Retrieved January 15, 2022 from https://emotiontypology.com/

[127] Jodi Forlizzi and Katja Battarbee. 2004. Understanding Experience in Interactive Systems. In *Proceedings of the 5th Conference on Designing Interactive Systems: Processes, Practices, Methods, and Techniques (DIS '04)*. Association for Computing Machinery, New York, NY, USA, 261–268. https://doi.org/10.1145/1013115.1013152

[128] Maarten Franssen, Gert-Jan Lokhorst, and Ibo van de Poel. 2018. Philosophy of Technology. In *The Stanford Encyclopedia of Philosophy* (Fall 2018 ed.), Edward N. Zalta (Ed.). Metaphysics Research Lab, Stanford University.

[129] Steven Furnell, Pete Fischer, and Amanda Finch. 2017. Can't get the staff? The growing need for cyber-security skills. *Computer Fraud & Security* 2017, 2 (2017), 5–10. https://doi.org/10.1016/S1361-3723(17)30013-1

[130] Esther Gal-Or and Anindya Chose. 2005. The economic incentives for sharing security information. *Information Systems Research* 16, 2 (2005), 186–208. https://doi.org/10.1287/isre.1050.0053

[131] Tushaar Gangavarapu, C D Jaidhar, and Bhabesh Chanduka. 2020. Applicability of machine learning in spam and phishing email filtering: review and approaches. *Artificial Intelligence Review* (2020).

[132] Xianyi Gao, Yulong Yang, Huiqing Fu, Janne Lindqvist, and Yang Wang. 2014. Private Browsing: An Inquiry on Usability and Privacy Protection. In *Proceedings of the 13th Workshop on Privacy in the Electronic Society (WPES '14)*. Association for Computing Machinery, New York, NY, USA, 97–106. https://doi.org/10.1145/2665943.2665953

[133] Simson Garfinkel and Heather Richter Lipford. 2014. *Usable Security: History, Themes, and Challenges*. Morgan & Claypool. 124 pages.

[134] Simson L Garfinkel and Robert C Miller. 2005. Johnny 2: a user test of key continuity management with S/MIME and Outlook Express. *Proceedings of the 2005 symposium on Usable privacy and security* 6 (2005), 13–24.

[135] Paul M Garrett, Joshua P White, Stephan Lewandowsky, Yoshihisa Kashima, Andrew Perfors, Daniel R Little, Nic Geard, Lewis Mitchell, Martin Tomko, and Simon Dennis. 2021. The acceptability and uptake of smartphone tracking for COVID-19 in Australia. *Plos one* 16, 1 (2021), e0244827.

[136] Shirley Gaw, Edward W. Felten, and Patricia Fernandez-Kelly. 2006. Secrecy, flagging, and paranoia. (2006), 591.

[137] Sarah Gibbons. 2018 (accessed 2019-04-19). Journey Mapping 101. https://www.nngroup.com/articles/journey-mapping-101/

[138] GitHub. 2021. GitHub - MISP/MISP/ MISP (core software) - Open Source Threat Intelligence and Sharing Platform. Retrieved May 15, 2021 from https://github.com/MISP/MISP Last accessed on May 15, 2021.

[139] Google. 2022. About the Exposure Notifications System and Android location settings. Retrieved February 10, 2022 from https://support.google.com/android/answer/9930236

[140] Lawrence Gordon, Martin Loeb, and William Lucyshyn. 2003. Sharing information on computer systems security: An economic analysis. *Journal of Accounting and Public Policy* 22, 6 (2003), 461–485.

[141] Government of France. 2020. Métriques d'utilisation de l'application TousAntiCovid. [Data set], Retrieved August 16, 2021 from https://www.data.gouv.fr/en/datasets/metriques-dutilisation-de-lapplication-tousanticovid/.

[142] Government of France. 2020. Présentation du Premier ministre sur les mesures contre la Covid-19. (October 29, 2020). Retrieved February 10, 2022 from https://www.gouvernement.fr/partage/11839-presentation-du-premier-ministre-sur-l-application-des-mesures-pour-lutter-contre-la-covid-19

[143] Government of France. 2020. TousAntiCovid. Retrieved December 15, 2021 from https://bonjour.tousanticovid.gouv.fr.

[144] Government of France. 2021. Attestations de déplacement. Retrieved August 16, 2021 from https://www.interieur.gouv.fr/Actualites/L-actu-du-Ministere/Attestations-de-deplacement.

[145] Government of Hong Kong. 2021. "StayHomeSafe" Mobile App User Guide. (September 15, 2021). Retrieved February 10, 2022 from https://www.coronavirus.gov.hk/eng/stay-home-safe.html

[146] Government of Singapore. 2021. TraceTogether Token. (March 11, 2021). Retrieved February 10, 2022 from https://www.tracetogether.gov.sg/common/token/index.html

[147] Eric T. Greenlee, Gregory J. Funke, Joel S. Warm, Ben D. Sawyer, Victor S. Finomore, Vince F. Mancuso, Matthew E. Funke, and Gerald Matthews. 2016. Stress and workload profiles of network analysis: Not all tasks are created equal. *Advances in Intelligent Systems and Computing* 501 (2016), 153–166. https://doi.org/10.1007/978-3-319-41932-9_13

[148] George Grekousis and Ye Liu. 2021. Digital contact tracing, community uptake, and proximity awareness technology to fight COVID-19: a systematic review. *Sustainable Cities and Society* 71 (2021), 102995. https://doi.org/10.1016/j.scs.2021.102995

[149] Eva Grill, Sarah Eitze, Freia De Bock, Nico Dragano, Lena Huebl, Patrick Schmich, Lothar H. Wieler, and Cornelia Betsch. 2021. Sociodemographic characteristics determine download and use of a Corona contact tracing app in Germany—Results of the COSMO surveys. *PLOS ONE* 16, 9 (09 2021), 1–12. https://doi.org/10.1371/journal.pone.0256660

[150] Georges Grinstein, Alfred Kobsa, Catherine Plaisant, and John T. Stasko. 2003. Which comes first, usability or utility?. In *IEEE Visualization, 2003. VIS 2003.* 605–606. https://doi.org/10.1109/VISUAL.2003.1250426

[151] Shad Gross, Jeffrey Bardzell, and Shaowen Bardzell. 2014. Skeu the evolution: Skeuomorphs, style, and the material of tangible interactions. *TEI 2014 - 8th International Conference on Tangible, Embedded and Embodied Interaction, Proceedings* (2014), 53–60.

[152] Jonathan Grudin. 1992. Utility and usability: research issues and development contexts. *Interacting with Computers* 4, 2 (1992), 209–217. https://doi.org/10.1016/0953-5438(92)90005-Z

[153] Jonathan Grudin. 2012. *A Moving Target "The Evolution of Human-Computer Interaction"* (human-computer interaction handbook: fundamentals, evolving technologies, and emerging applications. (3rd edition). ed.). Taylor & Francis Group. https://www.microsoft.com/en-us/research/publication/moving-target-evolution-human-computer-interaction/

[154] Marlene Guillon. 2021. Digital contact-tracing in France: uptake by COVID-19 risk factor and by exposure risk. *Journal of Public Health* (09 2021).

[155] Marlene Guillon and Pauline Kergall. 2020. Attitudes and opinions on quarantine and support for a contact-tracing application in France during the COVID-19 outbreak. *Public Health* 188 (2020), 21–31. https://doi.org/10.1016/j.puhe.2020.08.026

[156] Seda Gürses and Jose M. Del Alamo. 2016. Privacy Engineering: Shaping an Emerging Field of Research and Practice. *IEEE Security and Privacy* 14, 2 (2016), 40–46. https://doi.org/10.1109/MSP.2016.37

[157] Marco Gutfleisch, Jan H. Klemmer, Niklas Busch, Yasemin Acar, M. Angela Sasse, and Sascha Fahl. 2022. How Does Usable Security (Not) End Up in Software Products? Results From a Qualitative Interview Study. In *43rd IEEE Symposium on Security and Privacy, IEEE S&P 2022, May 22-26, 2022*. IEEE Computer Society.

[158] Yaron Gvili. 2020. Security Analysis of the COVID-19 Contact Tracing Specifications by Apple Inc. and Google Inc. Cryptology ePrint Archive, Report 2020/428. https://ia.cr/2020/428.

[159] Julie Haney, Yasemin Acar, and Susanne Furman. 2021. "It's the Company, the Government, You and I": User Perceptions of Responsibility for Smart Home Privacy and Security. In *30th USENIX Security Symposium (USENIX Security 21)*. USENIX Association, 411–428. https://www.usenix.org/conference/usenixsecurity21/presentation/haney

[160] Eszter Hargittai, Elissa M. Redmiles, Jessica Vitak, and Michael Zimmer. 2020. Americans' willingness to adopt a COVID-19 tracking app. *First Monday* 25, 11 (Oct. 2020). https://doi.org/10.5210/fm.v25i11.11095

[161] Maximilian Häring, Eva Gerlitz, Christian Tiefenau, Matthew Smith, Dominik Wermke, Sascha Fahl, and Yasemin Acar. 2021. Never ever or no matter what: Investigating Adoption Intentions and Misconceptions about the Corona-Warn-App in Germany. In *Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021)*. USENIX Association, 77–98. https://www.usenix.org/conference/soups2021/presentation/acar

[162] Michael D. Harrison, Paolo Masci, José Creissac Campos, and Paul Curzon. 2017. Verification of User Interface Software: The Example of Use-Related Safety Requirements and Programmable Medical Devices. *IEEE Trans. Human-Machine Systems* 47, 6 (2017), 834–846.

[163] Zahra Hassanzadeh, Robert Biddle, and Sky Marsen. 2021. User Perception of Data Breaches. *IEEE Transactions on Professional Communication* 64, 4 (2021), 374–389. https://doi.org/10.1109/TPC.2021.3110545

[164] Marc Hassenzahl. 2001. The Effect of Perceived Hedonic Quality on Product Appealingness. *International Journal of Human–Computer Interaction* 13, 4 (2001), 481–499. https://doi.org/10.1207/S15327590IJHC1304_07 arXiv:https://doi.org/10.1207/S15327590IJHC1304_07

[165] Marc Hassenzahl. 2010. Experience design: Technology for all the right reasons. *Synthesis lectures on human-centered informatics* 3, 1 (2010), 1–95.

[166] Marc Hassenzahl, Sarah Diefenbach, and Anja Göritz. 2010. Needs, affect, and interactive products – Facets of user experience. *Interacting with Computers* 22, 5 (September 2010), 353–362. https://doi.org/10.1016/j.intcom.2010.04.002

[167] Marc Hassenzahl, Axel Platz, Michael Burmester, and Katrin Lehner. 2000. Hedonic and ergonomic quality aspects determine a software's appeal. *Conference on Human Factors in Computing Systems - Proceedings* 2, 1 (2000), 201–208. https://doi.org/10.1145/332040.332432

[168] Marc Hassenzahl and Noam Tractinsky. 2006. User experience - a research agenda. *Behaviour & Information Technology* 25, 2 (2006), 91–97. https://doi.org/10.1080/01449290500330331

[169] Martin Heidegger. 1988. *The basic problems of phenomenology*. Vol. 478. Indiana University Press.

[170] Cormac Herley. 2014. More Is Not the Answer. *IEEE Security & Privacy* 12, 1 (2014), 14–19. https://doi.org/10.1109/MSP.2013.134

[171] Martin Horák, Václav Stupka, and Martin Husák. 2019. GDPR compliance in cybersecurity software: A case study of DPIA in information sharing platform. *ACM International Conference Proceeding Series* (2019). https://doi.org/10.1145/3339252.3340516

[172] Kasper Hornbæk and Antti Oulasvirta. 2017. What Is Interaction?. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems (CHI '17)*. Association for Computing Machinery, New York, NY, USA, 5040–5052. https://doi.org/10.1145/3025453.3025765

[173] Kasper Hornbæk. 2006. Current practice in measuring usability: Challenges to usability studies and research. *International Journal of Human-Computer Studies* 64, 2 (2006), 79–102. https://doi.org/10.1016/j.ijhcs.2005.06.002

[174] Kai T Horstmann, Susanne Buecker, Julia Krasko, Sarah Kritzler, and Sophia Terwiel. 2020. Who does or does not use the 'Corona-Warn-App' and why? *European Journal of Public Health* 31, 1 (12 2020), 49–51. https://doi.org/10.1093/eurpub/ckaa239

[175] Adam Michael Houser. 2018. *Mental models for cybersecurity: a formal methods approach*. Ph.D. Dissertation. State University of New York at Buffalo.

[176] Hang Hu and Grang Wang. 2018. End-to-End Measurements of Email Spoofing Attacks. *Usenix Security Symposium* (2018), 1095–1112.

[177] Ralph B Hupka, Zbigniew Zaleski, Jurgen Otto, Lucy Reidl, and Nadia V Tarabrina. 1997. The Colors of Anger, Envy, Fear, and Jealousy: A Cross-Cultural Study. *Journal of Cross-Cultural Psychology* 28, 2 (1997), 156–171.

[178] Edwin Hutchins. 1995. (1995b). How a cockpit remembers its speeds. Cognitive Science, 19, 265-288. (1995).

[179] International Organization for Standardization (ISO). 1998. *ISO 9241-11:1998(en), Ergonomic requirements for office work with visual display terminals (VDTs) — Part 11: Guidance on usability*. Technical Report. International Organization for Standardization, Geneva, CH.

[180] International Organization for Standardization (ISO). 2018. *ISO 9241-11:2018(en), Ergonomics of human-system interaction — Part 11: Usability: Definitions and concepts*. Technical Report. International Organization for Standardization, Geneva, CH.

[181] Iulia Ion, Rob Reeder, and Sunny Consolvo. 2015. "...No one Can Hack My Mind": Comparing Expert and Non-Expert Security Practices. In *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*. USENIX Association, Ottawa, 327–346. https://www.usenix.org/conference/soups2015/proceedings/presentation/ion

[182] Jeffrey L. Jenkins, Bonnie Brinton Anderson, Anthony Vance, C. Brock Kirwan, and David Eargle. 2016. More harm than good? How messages that interrupt can make us vulnerable. *Information Systems Research* 27, 4 (2016), 880–896.

[183] Kevin Jenniskens, Martin C J Bootsma, Johanna A A G Damen, Michiel S Oerbekke, Robin W M Vernooij, René Spijker, Karel G M Moons, Mirjam E E Kretzschmar, and Lotty Hooft. 2021. Effectiveness of contact tracing apps for SARS-CoV-2: a rapid systematic review. *BMJ Open* 11, 7 (2021). https://doi.org/10.1136/bmjopen-2021-050519

[184] Carlos Jensen, Colin Potts, and Christian S. Jensen. 2005. Privacy practices of Internet users: Self-reports versus observed behavior. *Int. J. Hum. Comput. Stud.* 63, 1-2 (2005), 203–227. https://doi.org/10.1016/j.ijhcs.2005.04.019

[185] Guðrún Hulda Jónsdóttir Johannessen and Kasper Hornbæk. 2014. Must evaluation methods be about usability? Devising and assessing the utility inspection method. *Behaviour & Information Technology* 33, 2 (2014), 195–206. https://doi.org/10.1080/0144929X.2012.751708 arXiv:https://doi.org/10.1080/0144929X.2012.751708

[186] Christopher S. Johnson, Mark Lee Badger, David A. Waltermire, Julie Snyder, and Clem Skorupka. 2016. *Guide to Cyber Threat Information Sharing*. Technical Report NIST Special Publication (SP) 800-150, October, 2016. National Institute of Standards and Technology, Gaithersburg, MD. https://doi.org/10.6028/NIST.SP.800-150

[187] David Jonassen and Young Hoan Cho. 2008. *Externalizing Mental Models with Mindtools*. Springer US, Boston, MA, 145–159. https://doi.org/10.1007/978-0-387-76898-4_7

[188] Natalie A Jones, Helen Ross, Timothy Lynam, Pascal Perez, and Anne Leitch. 2011. Mental Models: An Interdisciplinary Synthesis of Theory and Methods. *Ecology and society* 16, 1 (2011), 46.

[189] Patrick W. Jordan. 2000. Inclusive design: An holistic approach. *Proceedings of the XIVth Triennial Congress of the International Ergonomics Association and 44th Annual Meeting of the Human Factors and Ergonomics Association, 'Ergonomics for the New Millennium'* (2000), 917–920.

[190] David Kahn. 1996. *The codebreakers : the story of secret writing* (rev. and updated ed.). Scribner, New York.

[191] James Kalbach. 2016. *Mapping experiences : a guide to creating value through journeys, blueprints and diagrams*. O'Reilly Media Inc.

[192] Shinichi Kamiya, Jun-Koo Kang, Jungmin Kim, Andreas Milidonis, and René M Stulz. 2021. Risk management, firm reputation, and the impact of successful cyberattacks on target firms. *Journal of Financial Economics* 139, 3 (2021), 719–749. https://doi.org/10.1016/j.jfineco.2019.05.019

[193] Gabriel Kaptchuk, Daniel G. Goldstein, Eszter Hargittai, Jake M. Hofman, and Elissa M. Redmiles. 2020. How good is good enough for COVID19 apps? The influence of benefits, accuracy, and privacy on willingness to adopt. *CoRR* abs/2005.04343 (2020). arXiv:2005.04343 https://arxiv.org/abs/2005.04343

[194] Evangelos Karapanos, John Zimmerman, Jodi Forlizzi, and Jean-Bernard Martens. 2009. User Experience over Time: An Initial Framework. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '09)*. Association for Computing Machinery, New York, NY, USA, 729–738. https://doi.org/10.1145/1518701.1518814

[195] John Karat, Clare-Marie Karat, and Carolyn Brodie. 2007. Human-computer interaction viewed from the intersection of privacy, security, and trust. In *The Human-Computer Interaction Handbook: Fundamentals, Evolving Technologies, and Emerging Applications (Human Factors and Ergonomics Series)* (2nd ed.), Andrew Sears and Julie A. Jacko (Eds.). L. Erlbaum Associates Inc., Boca Raton, USA, 639 – 658.

[196] Michaela Kauer, Sebastian Günther, Daniel Storck, and Melanie Volkamer. 2013. A Comparison of American and German Folk Models of Home Computer Security. In *Human Aspects of Information Security, Privacy, and Trust - First International Conference, HAS 2013, Held as Part of HCI International 2013 (Lecture Notes in Computer Science)*, Louis Marinos and Ioannis Askoxylakis (Eds.), Vol. 8030. Springer, 100–109. http://tubiblio.ulb.tu-darmstadt.de/63066/ Event Title: First International Conference, HAS 2013, Held as Part of HCI International 2013.

[197] Auguste Kerckhoffs. 1883. La Cryptographie Militaire. *Journal des Sciences militaires* 9 (January 1883), 5–38.

[198] Mazaher Kianpour, Harald Øverby, Stewart James Kowalski, and Christopher Frantz. 2019. Social Preferences in Decision Making Under Cybersecurity Risks and Uncertainties. In *HCI for Cybersecurity, Privacy and Trust*, Abbas Moallem (Ed.). Springer International Publishing, Cham, 149–163.

[199] Philipp H. Kindt, Trinad Chakraborty, and Samarjit Chakraborty. 2021. How Reliable is Smartphone-Based Electronic Contact Tracing for COVID-19? *Commun. ACM* 65, 1 (dec 2021), 56–67. https://doi.org/10.1145/3471933

[200] Laura A King, Joshua A Hicks, Jennifer L Krull, and Amber K. Del Gaiso. 2006. Positive Affect and the Experience of Meaning in Life. *Journal of personality and social psychology* 90, 1 (2006), 179–196.

[201] Iacovos Kirlappos, Simon Parkin, and M Angela Sasse. 2014. Learning from "Shadow Security": Why understanding non-compliant behaviors provides the basis for effective security. *Usec '14* February (2014), 1–10. https://doi.org/10.14722/usec.2014.23<007>

[202] Alex Kirlik. 2006. *Adaptive Perspectives on Human-Technology Interaction: Methods and Models for Cognitive Engineering and Human-Computer Interaction (Human-Technology Interaction)*. Oxford University Press, Inc., USA.

[203] Predrag Klasnja, Sunny Consolvo, Jaeyeon Jung, Benjamin M. Greenstein, Louis LeGrand, Pauline Powledge, and David Wetherall. 2009. "When I Am on Wi-Fi, I Am Fearless": Privacy Concerns & Practices in Everyday Wi-Fi Use. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '09)*. Association for Computing Machinery, New York, NY, USA, 1993–2002. https://doi.org/10.1145/1518701.1519004

[204] Faris Bugra Kokulu, Yan Shoshitaishvili, Ananta Soneji, Ziming Zhao, Gail Joon Ahn, Tiffany Bao, and Adam Doupé. 2019. Matched and mismatched SOCs: A qualitative study on security operations center issues. *Proceedings of the ACM Conference on Computer and Communications Security* (2019), 1955–1970. https://doi.org/10.1145/3319535.3354239

[205] Genia Kostka and Sabrina Habich-Sobiegalla. 2020. In Times of Crisis: Public Perceptions Towards COVID-19 Contact Tracing Apps in China, Germany and the US. *SSRN (September 16, 2020)* (2020). https://doi.org/10.2139/ssrn.3693783

[206] Kat Krol, Matthew Moroz, and Martina Angela Sasse. 2012. Don't work. Can't work? Why it's time to rethink security warnings. *7th International Conference on Risks and Security of Internet and Systems, CRiSIS 2012* (2012), 1–8.

[207] Sari Kujala, Tanja Walsh, Piia Nurkka, and Marian Crisan. 2014. Sentence completion for understanding users and evaluating user experience. *Interacting with Computers* 26, 3 (2014), 238–255. https://doi.org/10.1093/iwc/iwt036

[208] Mike Kuniavsky. 2007. User Experience and HCI. In *The Human-Computer Interaction Handbook: Fundamentals, Evolving Technologies, and Emerging Applications* (2nd ed.), Andrew Sears and Julie A. Jacko (Eds.). L. Erlbaum Associates Inc., Boca Raton, USA, 897–916.

[209] Carine Lallemand, Guillaume Gronier, and Vincent Koenig. 2015. User experience: A concept without consensus? Exploring practitioners' perspectives through an international survey. *Computers in Human Behavior* 43 (2015), 35–48. https://doi.org/10.1016/j.chb.2014.10.048

[210] Carine Lallemand and Vincent Koenig. 2017. How Could an Intranet Be Like a Friend to Me? Why Standardized UX Scales Don't Always Fit. In *Proceedings of the European Conference on Cognitive Ergonomics 2017 (ECCE 2017)*. Association for Computing Machinery, New York, NY, USA, 9–16. https://doi.org/10.1145/3121283.3121288

[211] Leona Lassak, Annika Hildebrandt, Maximilian Golla, and Blase Ur. 2021. "It's Stored, Hopefully, on an Encrypted Server": Mitigating Users' Misconceptions About FIDO2 Biometric WebAuthn. In *30th USENIX Security Symposium (USENIX Security 21)*. USENIX Association, 91–108. https://www.usenix.org/conference/usenixsecurity21/presentation/lassak

[212] Kenneth R. Laughery and Michael S. Wogalter. 2006. Designing Effective Warnings. *Reviews of Human Factors and Ergonomics* 2, 1 (2006), 241–271.

[213] 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.). Springer Berlin Heidelberg, Berlin, Heidelberg, 63–76.

[214] Joscha Lausch, Oliver Wiese, and Volker Roth. 2017. What is a Secure Email? *EuroUSEC 2017* (2017).

[215] Effie Lai-Chong Law, Virpi Roto, Marc Hassenzahl, Arnold P.O.S. Vermeeren, and Joke Kort. 2009. Understanding, Scoping and Defining User Experience: A Survey Approach. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '09)*. Association for Computing Machinery, New York, NY, USA, 719–728. https://doi.org/10.1145/1518701.1518813

[216] A Lerner, E Zeng, and F Roesner. 2017. Confidante: Usable Encrypted Email: A Case Study with Lawyers and Journalists. In *2017 IEEE European Symposium on Security and Privacy (EuroS&P)*. 385–400.

[217] Tianshi Li, Jackie Yang, Cori Faklaris, Jennifer King, Yuvraj Agarwal, Laura Dabbish, and Jason I. Hong. 2020. Decentralized is not risk-free: Understanding public perceptions of privacy-utility trade-offs in COVID-19 contact-tracing apps. *CoRR* abs/2005.11957 (2020). arXiv:2005.11957 https://arxiv.org/abs/2005.11957

[218] LibertiesEU. 2021. COVID-19 Contact Tracing Apps in the EU. (June 2, 2021). Retrieved February 10, 2022 from https://www.liberties.eu/en/stories/trackerhub1-mainpage/43437

[219] Danielle Lottridge, Mark Chignell, and Aleksandra Jovicic. 2011. Affective Interaction: Understanding, Evaluating, and Designing for Human Emotion. *Reviews of Human Factors and Ergonomics* 7, 1 (2011), 197–217.

[220] Craig M. MacDonald and Michael E. Atwood. 2014. What Does It Mean for a System to Be Useful? An Exploratory Study of Usefulness. In *Proceedings of the 2014 Conference on Designing Interactive Systems (DIS '14)*. Association for Computing Machinery, New York, NY, USA, 885–894. https://doi.org/10.1145/2598510.2598600

[221] Wendy Mackay. 2000. Responding to cognitive overload : Co-adaptation between users and technology. *Intellectica. Revue de l'Association pour la Recherche Cognitive* 30, 1 (2000), 177–193. https://doi.org/10.3406/intel.2000.1597

[222] Hernâni Marques and Bernie Hoeneisen. 2020. *pretty Easy privacy (pEp): Mapping of Privacy Rating*. Internet-Draft draft-marques-pep-rating-03. Internet Engineering Task Force. https://datatracker.ietf.org/doc/html/draft-marques-pep-rating-03 Work in Progress.

[223] Keith M Martin. 2012. Everyday cryptography: fundamental principles and applications.

[224] Ashwin Mathew. (in press). Can Security be Decentralised? The Case of the PGP Web of Trust. In *Socio-Technical Aspects in Security and Trust*, Luca Viganò and Simon Parkin (Eds.). Springer International Publishing, Cham. Retrieved January 15, 2022 from https://sanmathi.org/ashwin/wp-content/uploads/sites/2/2021/10/Trust-PGP-preconference.pdf Preprint.

[225] Niels Raabjerg Mathiasen and Susanne Bødker. 2011. Experiencing Security in Interaction Design. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '11)*. Association for Computing Machinery, New York, NY, USA, 2325–2334. https://doi.org/10.1145/1978942.1979283

[226] Jeff May. 2020. *The Security Intelligence Handbook: How to disrupt adversaries and reduce risk with security intelligence*. CyberEdge Group, LLC.

[227] Peter Mayer and Melanie Volkamer. 2018. Addressing Misconceptions about Password Security Effectively. In *Proceedings of the 7th Workshop on Socio-Technical Aspects in Security and Trust (STAST '17)*. Association for Computing Machinery, New York, NY, USA, 16–27. https://doi.org/10.1145/3167996.3167998

[228] Peter Mayer, Yixin Zou, Florian Schaub, and Adam J. Aviv. 2021. "Now I'm a bit angry:" Individuals' Awareness, Perception, and Responses to Data Breaches that Affected Them. In *30th USENIX Security Symposium (USENIX Security 21)*. USENIX Association, 393–410. https://www.usenix.org/conference/usenixsecurity21/presentation/mayer

[229] Wilfried Mayer, Aaron Zauner, Martin Schmiedecker, and Markus Huber. 2016. No need for black chambers: Testing TLS in the E-mail ecosystem at large. *Proceedings - 2016 11th International Conference on Availability, Reliability and Security, ARES 2016* (2016), 10–20. arXiv:1510.08646

[230] John McCarthy and Peter Wright. 2004. Technology as experience.

[231] John McCarthy and Peter Wright. 2004. Technology as Experience. *Interactions* 11, 5 (sep 2004), 42–43. https://doi.org/10.1145/1015530.1015549

[232] Susan E Mcgregor, Polina Charters, Tobin Holliday, and Susan E Mcgregor. 2015. 2015. Survey. Investigating the Computer Security Practices and Needs of Journalists. This Paper Is Included in the Proceedings of the Investigating the Computer Security Practices and Needs of Journalists. *24th USENIX Security Symposium (USENIX Security 15)* (2015).

[233] McKinsey & Company. 2017. *Customer experience: New capabilities, new audiences, new opportunities*. Technical Report 2.

[234] Robert McMillan. 2017. The man who wrote those password rules has a new tip: N3v$r M1-d. *The Wall Street Journal* (2017).

[235] Elisa D. Mekler and Kasper Hornbæk. 2016. Momentary Pleasure or Lasting Meaning? Distinguishing Eudaimonic and Hedonic User Experiences. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems (CHI '16)*. Association for Computing Machinery, New York, NY, USA, 4509–4520. https://doi.org/10.1145/2858036.2858225

[236] Elisa D. Mekler and Kasper Hornbæk. 2019. A Framework for the Experience of Meaning in Human-Computer Interaction. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems (CHI '19)*. Association for Computing Machinery, New York, NY, USA, 1–15. https://doi.org/10.1145/3290605.3300455

[237] Florian Menges, Benedikt Putz, and Günther Pernul. 2020. DEALER: decentralized incentives for threat intelligence reporting and exchange. *International Journal of Information Security* (2020). https://doi.org/10.1007/s10207-020-00528-1

[238] Alain Mermoud, Marcus Matthias Keupp, Kévin Huguenin, Maximilian Palmié, and Dimitri Percia David. 2019. To share or not to share: A behavioral perspective on human participation in security information sharing. *Journal of Cybersecurity* 5, 1 (2019), 1–13. https://doi.org/10.1093/cybsec/tyz006

[239] MISP. 2021. COVID-19 MISP Information Sharing Community. Retrieved May 15, 2021 from https://www.misp-project.org/covid-19-misp/ Last accessed on May 15, 2021.

[240] MISP. 2021. MISP - Open Source Threat Intelligence Platform & Open Standards For Threat Information Sharing. Retrieved May 15, 2021 from https://www.misp-project.org/ Last accessed on May 15, 2021.

[241] MIT Technology Review. 2020. A flood of coronavirus apps are tracking us. Now it's time to keep track of them. (May 7, 2020). Retrieved February 10, 2022 from https://www.technologyreview.com/2020/05/07/1000961/launching-mittr-covid-tracing-tracker

[242] MIT Technology Review. 2020. Five things we need to do to make contact tracing really work. (April 28, 2020). Retrieved August 16, 2021 from https://www.technologyreview.com/2020/04/28/1000714/five-things-to-make-contact-tracing-work-covid-pandemic-apple-google/.

[243] MIT Technology Review. 2020. Some prominent exposure apps are slowly rolling back freedoms. (November 23, 2020). Retrieved August 16, 2021 from https://www.technologyreview.com/2020/11/23/1012491/contact-tracing-mandatory-singapore-covid-pandemic.

[244] Aziz Mohaisen, Omar Al-Ibrahim, Charles Kamhoua, Kevin Kwiat, and Laurent Njilla. 2017. Rethinking Information Sharing for Threat Intelligence. In *Proceedings of the Fifth ACM/IEEE Workshop on Hot Topics in Web Systems and Technologies (HotWeb '17)*. Association for Computing Machinery, New York, NY, USA, Article 6, 7 pages. https://doi.org/10.1145/3132465.3132468

[245] Ilaria Montagni, Nicolas Roussel, Rodolphe Thiébaut, and Christophe Tzourio. 2020. The French Covid-19 contact tracing app: knowledge, attitudes, beliefs and practices of students in the health domain. *medRxiv* (2020). https://doi.org/10.1101/2020.10.23.20218214

[246] Jessica Morley, John Powell, and Luciano Floridi. 2021. What's the Evidence that Health Apps Work? A Scoping Study of Evidence of Effectiveness for Direct-to-Consumer Apps on the App Store. *A Scoping Study of Evidence of Effectiveness for Direct-to-Consumer Apps on the App Store (May 22, 2021)* (2021). https://doi.org/10.2139/ssrn.3851242

[247] National Geographic. 2020. The magnitude of America's contact tracing crisis is hard to overstate. (September 1, 2020). Retrieved August 16, 2021 from https://www.nationalgeographic.com/science/article/contact-tracing-crisis-magnitude-hot-mess-america-fixes-coronavirus-cvd.

[248] Jakob Nielsen. 1994. *Usability Engineering* (1st edition. ed.).

[249] Nielsen Norman Group. 2016. Journey Mapping in Real Life: A Survey of UX Practitioners (October 16, 2016). Retrieved January 15, 2022 from http://www.nngroup.com/articles/journey-mapping-ux-practitioners/.

[250] Nielsen Norman Group. 2016. When and How to Create Customer Journey Maps (July 31, 2016). Retrieved January 15, 2022 from https://www.nngroup.com/articles/customer-journey-mapping/.

[251] Donald A. Norman. 1983. Mental Models in Human-Computer Interaction. In *Mental Models* (1 ed.), Dedre Gentner and Albert L. Stevens (Eds.). Psychology Press, New York, USA, 7–14.

[252] Donald A. Norman. 2009. When Security Gets in the Way. *Interactions* 16, 6 (nov 2009), 60–63. https://doi.org/10.1145/1620693.1620708

[253] Donald A Norman. 2013. *The design of everyday things* (rev. and expanded ed.). Basic Books, New York, New York.

[254] NPR. 2020. COVID-19 Contact Tracing Workforce Barely 'Inching Up' As Cases Surge. (October 14, 2020). Retrieved August 16, 2021 from https://www.npr.org/sections/health-shots/2020/10/14/923468159/covid-19-contact-tracing-workforce-barely-inching-up-as-cases-surge.

[255] Sean Oesch, Robert Bridges, Jared Smith, Justin Beaver, John Goodall, Kelly Huffer, Craig Miles, and Dan Scofield. 2020. An Assessment of the Usability of Machine Learning Based Tools for the Security Operations Center. *Proceedings - IEEE Congress on Cybermatics: 2020 IEEE International Conferences on Internet of Things, iThings 2020, IEEE Green Computing and Communications, GreenCom 2020, IEEE Cyber, Physical and Social Computing, CPSCom 2020 and IEEE Smart Data, SmartData 2020* (2020), 634–641. https://doi.org/10.1109/iThings-GreenCom-CPSCom-SmartData-Cybermatics50389.2020.00111

[256] Ian Oliver. 2014. *Privacy Engineering: A Dataflow and Ontological Approach* (1st ed.). CreateSpace Independent Publishing Platform, North Charleston, SC, USA.

[257] Antti Oulasvirta and Kasper Hornbæk. 2016. HCI Research as Problem-Solving. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems (CHI '16)*. Association for Computing Machinery, New York, NY, USA, 4956–4967. https://doi.org/10.1145/2858036.2858283

[258] Celeste Lyn Paul. 2014. Human-centered study of a network operations center: Experience report and lessons learned. *Proceedings of the ACM Conference on Computer and Communications Security* 2014-November, November (2014), 39–42. https://doi.org/10.1145/2663887.2663899

[259] Stephen J. Payne. 2007. Mental Models in Human-Computer Interaction. In *The Human-Computer Interaction Handbook: Fundamentals, Evolving Technologies, and Emerging Applications* (2nd ed.), Andrew Sears and Julie A. Jacko (Eds.). L. Erlbaum Associates Inc., Boca Raton, USA, 63–76.

[260] pep Foundation. 2016. Privacy By Default [White Paper]. Retrieved January 15, 2022 from https://pep.foundation/docs/pEp-whitepaper.pdf

[261] Richard M Perloff. 2017. The dynamics of persuasion : communication and attitudes in the 21st century.

[262] Shari Lawrence Pfleeger, Martina Angela Sasse, and Adrian Furnham. 2014. From Weakest Link to Security Hero: Transforming Staff Security Behavior. (2014).

[263] Anh Pham, Italo Dacosta, Eleonora Losiouk, John Stephan, Kevin Huguenin, and Jean-Pierre Hubaux. 2019. HideMyApp: Hiding the Presence of Sensitive Apps on Android. In *28th USENIX Security Symposium (USENIX Security 19)*. USENIX Association, Santa Clara, CA, 711–728. https://www.usenix.org/conference/usenixsecurity19/presentation/pham

[264] Desmet Pieter and Hekkert Paul. 2007. Framework of Product Experience. *International Journal of Design* 1, 1 (2007), 57–66. http://www.ijdesign.org/ojs/index.php/IJDesign/article/viewFile/66/7

[265] Wolter Pieters. 2011. Explanation and trust: What to tell the user in security and AI? *Ethics and Information Technology* 13, 1 (2011), 53–64.

[266] Elise Poillot, Giorgio Resta, Vincenzo Zeno-Zencovich, and Gabriele Lenzini. 2021. Technical and legal frameworks of tracing applications. *Data Protection in the Context of Covid-19. A short (hi)story of tracing applications* (November 2021), 5–22.

[267] Michael I. Posner, Mary J. Nissen, and Raymond M. Klein. 1976. Visual dominance: An information-processing account of its origins and significance. *Psychological Review* 83, 2 (1976), 157–171.

[268] Radio France Internationale. 2020. France rolls out new Covid tracking app 'TousAntiCovid'. (October 22, 2020). Retrieved August 16, 2021 from https://www.rfi.fr/en/france/20201022-france-rolls-out-new-covid-19-mobile-tracking-app-tous-anti-covid-stopcovid.

[269] Kenneth J. Radke. 2013. *Security ceremonies : including humans in cryptographic protocols*. Ph.D. Dissertation. Queensland University of Technology. https://eprints.qut.edu.au/63704/

[270] Andrew Ramsdale, Stavros Shiaeles, and Nicholas Kolokotronis. 2020. A comparative analysis of cyber-threat intelligence sources, formats and languages. *Electronics (Switzerland)* 9, 5 (2020). https://doi.org/10.3390/electronics9050824

[271] Robert W. Reeder, Adrienne Porter Felt, Sunny Consolvo, Nathan Malkin, Christopher Thompson, and Serge Egelman. 2018. *An Experience Sampling Study of User Reactions to Browser Warnings in the Field*. Association for Computing Machinery, New York, NY, USA, 1–13. https://doi.org/10.1145/3173574.3174086

[272] Johnmarshall Reeve. 2015. Understanding motivation and emotion.

[273] Lena Reinfelder, Robert Landwirth, and Zinaida Benenson. 2019. Security managers are not the enemy either. *Conference on Human Factors in Computing Systems - Proceedings* (2019), 1–7. https://doi.org/10.1145/3290605.3300663

[274] Karen Renaud, Melanie Volkamer, and Arne Renkema-Padmos. 2014. Why Doesn't Jane Protect Her Privacy?. In *Privacy Enhancing Technologies*, Emiliano De Cristofaro and Steven J Murdoch (Eds.). Springer International Publishing, Cham, 244–262.

[275] Reuters. 2021. Singapore COVID-19 contact-tracing data accessible to police. (January 4, 2021). Retrieved February 10, 2022 from https://www.reuters.com/business/healthcare-pharmaceuticals/singapore-covid-19-contact-tracing-data-accessible-police-2021-01-04/.

[276] Reuters. 2022. Crypto crime hit record $14 billion in 2021, research shows. (January 6, 2022). Retrieved January 6, 2022 from https://www.reuters.com/markets/us/crypto-crime-hit-record-14-billion-2021-research-shows-2022-01-06/.

[277] Robert Koch Institut. 2020. Coronavirus Disease 2019 (COVID-19) Daily Situation Report of the Robert Koch Institute. (November 15, 2020). Retrieved August 16, 2021 from https://www.rki.de/DE/Content/InfAZ/N/Neuartiges_Coronavirus/Situationsberichte/Nov_2020/2020-11-15-en.pdf.

[278] Robert Koch Institut. 2020. Kennzahlen zur Corona-Warn-App. (November 20, 2020). Retrieved August 16, 2021 from https://www.coronawarn.app/assets/documents/2020-11-20-cwa-daten-fakten.pdf.

[279] Robert Koch Institut. 2020. Open-Source Project Corona-Warn-App. Retrieved December 15, 2021 from https://www.coronawarn.app.

[280] Pablo Rodríguez, Santiago Graña, Eva Elisa Alvarez-León, Manuela Battaglini, Francisco Javier Darias, Miguel A Hernán, Raquel López, Paloma Llaneza, Maria Cristina Martín, Oriana Ramirez-Rubio, Adriana Romaní, Berta Suárez-Rodríguez, Javier Sánchez-Monedero, Alex Arenas, Lucas Lacasa, and RadarCovidPilot Group. 2021. A population-based controlled experiment assessing the epidemiological impact of digital contact tracing. *Nature Communications* 12, 1 (2021), 587. https://doi.org/10.1038/s41467-020-20817-6

[281] Scott Rose, J. Stephen Nightingale, Simson L. Garfinkel, and Ramaswamy Chandramouli. 2019. *Trustworthy Email*. Technical Report NIST Special Publication (SP) 800-177, February, 2019. National Institute of Standards and Technology, Gaithersburg, MD. https://doi.org/10.6028/NIST.SP.800-177r1

[282] Volker Roth, Tobias Straub, and Kai Richter. 2005. Security and usability engineering with particular attention to electronic mail. *Int. J. Hum. Comput. Stud.* 63, 1-2 (2005), 51–73. https://doi.org/10.1016/j.ijhcs.2005.04.015

[283] Virpi Roto, Effie Law, Arnold Vermeeren, and Jettie Hoonhout. 2011. *User experience white paper: Bringing clarity to the concept of user experience*.

[284] William B Rouse and Nancy M Morris. 1986. On looking into the black box: Prospects and limits in the search for mental models. *Psychological Bulletin* 100, 3 (1986), 349–363.

[285] Scott Ruoti, Jeff Andersen, Scott Heidbrink, Mark O'Neill, Elham Vaziripour, Justin Wu, Daniel Zappala, and Kent Seamons. 2016. "We'Re on the Same Page": A Usability Study of Secure Email Using Pairs of Novice Users *(CHI '16)*. ACM, 4298–4308.

[286] Scott Ruoti, Jeff Andersen, Travis Hendershot, Daniel Zappala, and Kent Seamons. 2016. Private Webmail 2.0: Simple and easy-to-use secure email. *UIST 2016 - Proceedings of the 29th Annual Symposium on User Interface Software and Technology* (2016), 461–472. arXiv:1510.08435

[287] Scott Ruoti, Nathan Kim, Ben Burgon, Timothy van der Horst, and Kent Seamons. 2013. Confused Johnny: When Automatic Encryption Leads to Confusion and Mistakes *(SOUPS '13)*. ACM, 5:1–5:12.

[288] Scott Ruoti and Kent Seamons. 2019. Johnny's Journey Toward Usable Secure Email. *IEEE Security and Privacy* 17, 6 (2019), 72–76.

[289] Richard M Ryan and Edward L Deci. 2000. Self-Determination Theory and the Facilitation of Intrinsic Motivation, Social Development, and Well-Being. *The American psychologist* 55, 1 (2000), 68–78.

[290] Nader Sohrabi Safa and Rossouw Von Solms. 2016. An information security knowledge sharing model in organizations. *Computers in Human Behavior* 57 (2016), 442–451. https://doi.org/10.1016/j.chb.2015.12.037

[291] Marcel Salathé, Christian L Althaus, Nanina Anderegg, Daniele Antonioli, Tala Ballouz, Edouard Bugnion, Srdjan Capkun, Dennis Jackson, Sang-Il Kim, James R Larus, et al. 2020. Early evidence of effectiveness of digital contact tracing for SARS-CoV-2 in Switzerland. *Swiss medical weekly* 150 (2020), w20457.

[292] J.H Saltzer and M.D Schroeder. 1975. The protection of information in computer systems. *Proc. IEEE* 63, 9 (1975), 1278–1308.

[293] Tomas Sander and Joshua Hailpern. 2015. UX Aspects of Threat Information Sharing Platforms: An Examination and Lessons Learned Using Personas. In *Proceedings of the 2Nd ACM Workshop on Information Sharing and Collaborative Security (WISCS '15)*. ACM, New York, NY, USA, 51–59. https://doi.org/10.1145/2808128.2808136 http://doi.acm.org/10.1145/2808128.2808136.

[294] Itzel Vázquez Sandoval and Gabriele Lenzini. 2019. A Formal Security Analysis of the pep Authentication Protocol for Decentralized Key Distribution and End-to-End Encrypted Email. In *2nd International Workshop on Emerging Technologies for Authorization and Authentication, ESORICS International Workshops*.

[295] Martina Angela Sasse, Sacha Brostoff, and Dirk Weirich. 2001. Transforming the 'weakest link' - A human/computer interaction approach to usable and effective security. *BT Technology Journal* 19, 3 (2001), 122–131. https://doi.org/10.1023/A:1011902718709

[296] Martina Angela Sasse and Ivan Flechais. 2005. Usable Security: Why Do We Need It? How Do We Get It? O'Reilly Media, Inc.

[297] Clemens Sauerwein, Christian Sillaber, Andrea Mussmann, and Ruth Breu. 2017. Threat intelligence sharing platforms: An exploratory study of software vendors and research perspectives. *The 13th International Conference on Wirtschaftsinformatik* (2017), 837–851.

[298] Jeff Sauro and James R. Lewis. 2016. *Quantifying the User Experience, Second Edition: Practical Statistics for User Research* (2nd ed.). Morgan Kaufmann Publishers Inc., San Francisco, CA, USA.

[299] Stuart E. Schechter, Rachna Dhamija, Andy Ozment, and Ian Fischer. 2007. The Emperor's New Security Indicators. In *2007 IEEE Symposium on Security and Privacy (SP '07)*. 51–65.

[300] Daniel Schlette, Fabian Böhm, Marco Caselli, and Günther Pernul. 2021. Measuring and visualizing cyber threat intelligence quality. *International Journal of Information Security* 20, 1 (2021), 21–38. https://doi.org/10.1007/s10207-020-00490-y

[301] Bruce Schneier. 2004. *Secrets and lies : digital security in a networked world*. Wiley, Indianapolis.

[302] Martin Schrepp. 2019. User Experience Questionnaire Handbook. Version 8 (31.12.2019).

[303] Jessica Schroers and Damian Clifford. 2017. Legal Implications of Information Sharing. In *Collaborative Cyber Threat Intelligence : Detecting and Responding to Advanced Cyber Attacks at the National Level*, Florian Skopik (Ed.). Auerbach Publishers, Incorporated.

[304] Ari Schwartz, Sejal C Shah, Matthew H MacKenzie, Sheena Thomas, Tara Sugiyama Potashnik, and Bri Law. 2016. Automatic threat sharing: how companies can best ensure liability protection when sharing cyber threat information with other companies or organizations. *U. Mich. JL Reform* 50 (2016), 887.

[305] Erich Schweighofer, Vinzenz Heussler, and Walter Hötzendorfer. 2017. Implementation Issues and Obstacles from a Legal Perspective. In *Collaborative Cyber Threat Intelligence : Detecting and Responding to Advanced Cyber Attacks at the National Level*, Florian Skopik (Ed.). Auerbach Publishers, Incorporated.

[306] Oscar Serrano, Luc Dandurand, and Sarah Brown. 2014. On the Design of a Cyber Security Data Sharing System. In *Proceedings of the 2014 ACM Workshop on Information Sharing & Collaborative Security (WISCS '14)*. Association for Computing Machinery, New York, NY, USA, 61–69. https://doi.org/10.1145/2663876.2663882

[307] Muhammad Shahroz, Farooq Ahmad, Muhammad Shahzad Younis, Nadeem Ahmad, Maged N. Kamel Boulos, Ricardo Vinuesa, and Junaid Qadir. 2021. COVID-19 digital contact tracing applications and techniques: A review post initial deployments. *Transportation Engineering* 5 (2021), 100072. https://doi.org/10.1016/j.treng.2021.100072

[308] C. E. Shannon. 1948. A mathematical theory of communication. *The Bell System Technical Journal* 27, 3 (1948), 379–423. https://doi.org/10.1002/j.1538-7305.1948.tb01338.x

[309] 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), 325–339.

[310] Steve Sheng, Levi Broderick, Jeremy J Hyland, and Colleen Alison Koranda. 2006. Why Johnny still can't encrypt: evaluating the usability of email encryption software. *Symposium On Usable Privacy and Security* (2006), 3–4.

[311] Lucy Simko, Ryan Calo, Franziska Roesner, and Tadayoshi Kohno. 2020. COVID-19 Contact Tracing and Privacy: Studying Opinion and Preferences. *CoRR* abs/2005.06056 (2020). arXiv:2005.06056 https://arxiv.org/abs/2005.06056

[312] Florian Skopik, Giuseppe Settanni, and Roman Fiedler. 2017. The Importance of Information Sharing and Its Numerous Dimensions to Circumvent Incidents and Mitigate Cyber Threats. In *Collaborative Cyber Threat Intelligence : Detecting and Responding to Advanced Cyber Attacks at the National Level*, Florian Skopik (Ed.). Auerbach Publishers, Incorporated.

[313] Diana K. Smetters and Rebecca E. Grinter. 2002. Moving from the Design of Usable Security Technologies to the Design of Useful Secure Applications. In *Proceedings of the 2002 Workshop on New Security Paradigms (NSPW '02)*. ACM, New York, NY, USA, 82–89.

[314] S W Smith. 2003. Humans in the Loop: Human-Computer Interaction and Security. *IEEE Security and Privacy* 1, 3 (2003), 75–79. https://doi.org/10.1109/MSECP.2003.1203228

[315] Tonya L Smith-Jackson and Michael S Wogalter. 2000. Users' Hazard Perceptions of Warning Components: An Examination of Colors and Symbols. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* 44, 32 (2000), 6–55–6–58.

[316] Eric Spero and Robert Biddle. 2020. Out of Sight, Out of Mind: UI Design and the Inhibition of Mental Models of Security. In *New Security Paradigms Workshop 2020 (NSPW '20)*. Association for Computing Machinery, New York, NY, USA, 127–143. https://doi.org/10.1145/3442167.3442174

[317] Eric Spero, Milica Stojmenović, Zahra Hassanzadeh, Sonia Chiasson, and Robert Biddle. 2019. Mixed Pictures: Mental Models of Malware. In *2019 17th International Conference on Privacy, Security and Trust (PST)*. 1–3. https://doi.org/10.1109/PST47121.2019.8949030

[318] Jessica Staddon and Noelle Easterday. 2019. 'It's a generally exhausting field' A Large-Scale Study of Security Incident Management Workflows and Pain Points. *2019 17th International Conference on Privacy, Security and Trust, PST 2019 - Proceedings* (2019). https://doi.org/10.1109/PST47121.2019.8949012

[319] Theresa Stadler, Wouter Lueks, Katharina Kohls, and Carmela Troncoso. 2021. Preliminary Analysis of Potential Harms in the Luca Tracing System. arXiv:cs.CR/2103.11958

[320] Brian Stanton, Mary F. Theofanos, Sandra Spickard Prettyman, and Susanne Furman. 2016. Security Fatigue. *IT Professional* 18, 5 (2016), 26–32. https://doi.org/10.1109/MITP.2016.84

[321] Borce Stojkovski, Ruba Abu-Salma, Karen Triquet, and Gabriele Lenzini. 2021. "Unless One Does the Research, It May Seem as Just a Useless Battery-Consuming App" - Field Notes on COVID-19 Contact Tracing Applications. *Digital Threats: Research and Practice* (aug 2021). https://doi.org/10.1145/3480466

[322] Borce Stojkovski and Gabriele Lenzini. 2020. Evaluating ambiguity of privacy indicators in a secure email app. In *Proceedings of the Fourth Italian Conference on Cyber Security, Ancona, Italy, February 4th to 7th, 2020 (CEUR Workshop Proceedings)*, Michele Loreti and Luca Spalazzi (Eds.), Vol. 2597. CEUR-WS.org, 223–234.

[323] Borce Stojkovski and Gabriele Lenzini. 2021. A workflow and toolchain proposal for analyzing users' perceptions in cyber threat intelligence sharing platforms. In *2021 IEEE International Conference on Cyber Security and Resilience (CSR)*. 324–330. https://doi.org/10.1109/CSR51186.2021.9527903

[324] Borce Stojkovski, Gabriele Lenzini, and Vincent Koenig. 2020. "I personally relate it to the traffic light" - Appendix [Data set]. https://doi.org/10.5281/zenodo.4322893

[325] Borce Stojkovski, Gabriele Lenzini, and Vincent Koenig. 2021. "I Personally Relate It to the Traffic Light": A User Study on Security & Privacy Indicators in a Secure Email System Committed to Privacy by Default. In *Proceedings of the 36th Annual ACM Symposium on Applied Computing (SAC '21)*. Association for Computing Machinery, New York, NY, USA, 1235–1246. https://doi.org/10.1145/3412841.3441998

[326] Borce Stojkovski, Gabriele Lenzini, Vincent Koenig, and Salvador Rivas. 2021. What's in a Cyber Threat Intelligence sharing platform? - Appendix [Data set]. https://doi.org/10.5281/zenodo.5531990

[327] Borce Stojkovski, Gabriele Lenzini, Vincent Koenig, and Salvador Rivas. 2021. What's in a Cyber Threat Intelligence Sharing Platform? A Mixed-Methods User Experience Investigation of MISP. In *Annual Computer Security Applications Conference (ACSAC)*. Association for Computing Machinery, New York, NY, USA, 385–398. https://doi.org/10.1145/3485832.3488030

[328] Borce Stojkovski, Itzel Vazquez Sandoval, and Gabriele Lenzini. 2019. Detecting Misalignments between System Security and User Perceptions: A Preliminary Sociotechnical Analysis of an E2E email Encryption System. In *2019 IEEE European Symposium on Security and Privacy Workshops (EuroS PW)*. 172–181. https://doi.org/10.1109/EuroSPW.2019.00026

[329] Christian Stransky, Oliver Wiese, Volker Roth, Yasemin Acar, and Sascha Fahl. 2022. 27 Years and 81 Million Opportunities Later: Investigating the Use of Email Encryption for an Entire University. In *43rd IEEE Symposium on Security and Privacy, IEEE S&P 2022, May 22-26, 2022*. IEEE Computer Society. Advance online publication. https://publications.teamusec.de/2022-oakland-email/pdf/2022_oakland_email_stransky_preprint.pdf Last accessed on January 15, 2022.

[330] Lucy A Suchman. 1987. *Plans and situated actions: The problem of human-machine communication*. Cambridge university press.

[331] Clare Sullivan and Eric Burger. 2017. "In the public interest": The privacy implications of international business-to-business sharing of cyber-threat intelligence. *Computer Law and Security Review* 33, 1 (2017), 14–29. https://doi.org/10.1016/j.clsr.2016.11.015

[332] Sathya Chandran Sundaramurthy, John McHugh, Xinming Ou, Michael Wesch, Alexandru G. Bardas, and S. Raj Rajagopalan. 2016. Turning Contradictions into Innovations or: How We Learned to Stop Whining and Improve Security Operations. (June 2016), 237–251. https://www.usenix.org/conference/soups2016/technical-sessions/presentation/sundaramurthy

[333] Joshua Sunshine, Serge Egelman, Hazim Almuhimedi, Neha Atri, and Lorrie Faith Cranor. 2009. Crying Wolf: An Empirical Study of SSL Warning Effectivenes. *18th USENIX Security Symposium* (2009), 399–432.

[334] Dag Svanæs. 2000. *Understanding interactivity: steps to a phenomenology of human-computer interaction.* Norges teknisk-naturvitenskapelige universitet.

[335] Moin Syed and Sarah C. Nelson. 2015. Guidelines for Establishing Reliability When Coding Narrative Data. *Emerging Adulthood* 3, 6 (2015), 375–387. https://doi.org/10.1177/2167696815587648

[336] Joshua Tan, Lujo Bauer, Joseph Bonneau, Lorrie Faith Cranor, Jeremy Thomas, and Blase Ur. 2017. Can Unicorns Help Users Compare Crypto Key Fingerprints?. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems (CHI '17)*. Association for Computing Machinery, New York, NY, USA, 3787–3798.

[337] The Radicati Group. 2021. *Email Statistics Report, 2021-2025*. Technical Report. The Radicati Group, Inc., Palo Alto, CA.

[338] Mary Theofanos, Brian Stanton, Susanne Furman, Sandra Spickard Prettyman, and Simson Garfinkel. 2017. Be prepared: How US government experts think about cybersecurity. In *Workshop on Usable Security (USec). Internet Society*.

[339] Gary Thomas. 2011. A Typology for the Case Study in Social Science Following a Review of Definition, Discourse, and Structure. *Qualitative Inquiry* 17, 6 (2011), 511–521. https://doi.org/10.1177/1077800411409884

[340] W. Tong, Gold S., S. Gichohi, M. Roman, and J. Frankle. 2014. Why King George III Can Encrypt. https://www.cs.princeton.edu/~arvindn/teaching/spring-2014-privacy-technologies/king-george-iii-encrypt.pdf

[341] Wiem Tounsi. 2019. What is Cyber Threat Intelligence and How is it Evolving? In *Cyber-Vigilance and Digital Trust*. John Wiley & Sons, Ltd, Chapter 1, 1–49. https://doi.org/10.1002/9781119618393.ch1

[342] Wiem Tounsi and Helmi Rais. 2018. A survey on technical threat intelligence in the age of sophisticated cyber attacks. *Computers and Security* 72 (2018), 212–233. https://doi.org/10.1016/j.cose.2017.09.001

[343] Rajae Touzani, Emilien Schultz, Seth M Holmes, Stéphanie Vandentorren, Pierre Arwidson, Francis Guillemin, Dominique Rey, Alexandra Rouquette, Anne-Déborah Bouhnik, and Julien Mancini. 2021. Early Acceptability of a Mobile App for Contact Tracing During the COVID-19 Pandemic in France: National Web-Based Survey. *JMIR Mhealth Uhealth* 9, 7 (19 Jul 2021). https://doi.org/10.2196/27768

[344] Simon Trang, Manuel Trenz, Welf H Weiger, Monideepa Tarafdar, and Christy MK Cheung. 2020. One app to trace them all? Examining app specifications for mass acceptance of contact-tracing apps. *European Journal of Information Systems* 29, 4 (2020), 415–428. https://doi.org/10.1080/0960085X.2020.1784046

[345] Carmela Troncoso, Mathias Payer, Jean-Pierre Hubaux, Marcel Salathé, James Larus, Edouard Bugnion, Wouter Lueks, Theresa Stadler, Apostolos Pyrgelis, and Daniele Antonioli. 2020. DP-3T: Decentralized Privacy-Preserving Proximity Tracing. Retrieved August 16, 2021 from https://github.com/DP-3T/documents.

[346] Carmela Troncoso, Mathias Payer, Jean-Pierre Hubaux, Marcel Salathé, James Larus, Edouard Bugnion, Wouter Lueks, Theresa Stadler, Apostolos Pyrgelis, Daniele Antonioli, Ludovic Barman, Sylvain Chatel, Kenneth Paterson, Srdjan Čapkun, David

Basin, Jan Beutel, Dennis Jackson, Marc Roeschlin, Patrick Leu, Bart Preneel, Nigel Smart, Aysajan Abidin, Seda Gürses, Michael Veale, Cas Cremers, Michael Backes, Nils Ole Tippenhauer, Reuben Binns, Ciro Cattuto, Alain Barrat, Dario Fiore, Manuel Barbosa, Rui Oliveira, and José Pereira. 2020. Decentralized Privacy-Preserving Proximity Tracing. https://doi.org/10.48550/arXiv.2005.12273 arXiv:cs.CR/2005.12273

[347] Phil Turner and Emilia Sobolewska. 2009. Mental models, magical thinking, and individual differences. *Human Technology: An Interdisciplinary Journal on Humans in ICT Environments* (2009).

[348] UEQ. 2021. User Experience Questionnaire. Retrieved May 15, 2021 from https://www.ueq-online.org/ Last accessed on May 15, 2021.

[349] UK Department of Health and Social Care. 2013. Guide to creating a front of pack (FoP) nutrition label for pre-packed products sold through retail outlets.

[350] United States, Executive Office of the President [Joseph R. Biden Jr.]. 2021. Executive Order No. 14,028 of May 12, 2021, 86 FR 26633. , 26633–26647 pages. https://www.federalregister.gov/executive-order/14028

[351] Blase Ur, Jonathan Bees, Sean M. Segreti, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. 2016. Do Users' Perceptions of Password Security Match Reality?. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems (CHI '16)*. Association for Computing Machinery, New York, NY, USA, 3748–3760. https://doi.org/10.1145/2858036.2858546

[352] 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 *21st USENIX Security Symposium (USENIX Security 12)*. USENIX Association, Bellevue, WA, 65–80. https://www.usenix.org/conference/usenixsecurity12/technical-sessions/presentation/ur

[353] Christine Utz, Steffen Becker, Theodor Schnitzler, Florian M. Farke, Franziska Herbert, Leonie Schaewitz, Martin Degeling, and Markus Dürmuth. 2021. Apps Against the Spread: Privacy Implications and User Acceptance of COVID-19-Related Smartphone Apps on Three Continents. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems (CHI '21)*. Association for Computing Machinery, New York, NY, USA, Article 70, 22 pages. https://doi.org/10.1145/3411764.3445517

[354] Steven Van Acker, Daniel Hausknecht, Wouter Joosen, and Andrei Sabelfeld. 2015. Password Meters and Generators on the Web: From Large-Scale Empirical Study to Getting It Right. In *Proceedings of the 5th ACM Conference on Data and Application Security and Privacy (CODASPY '15)*. Association for Computing Machinery, New York, NY, USA, 253–262. https://doi.org/10.1145/2699026.2699118

[355] Serge Vaudenay. 2020. Analysis of DP3T. Cryptology ePrint Archive, Report 2020/399. https://ia.cr/2020/399.

[356] Serge Vaudenay. 2020. Centralized or Decentralized? The Contact Tracing Dilemma. Cryptology ePrint Archive, Report 2020/531. https://ia.cr/2020/531.

[357] Itzel Vazquez Sandoval, Borce Stojkovski, and Gabriele Lenzini. 2018. A Protocol to Strengthen Password-Based Authentication. In *Emerging Technologies for Authorization and Authentication*, Andrea Saracino and Paolo Mori (Eds.). Springer International Publishing, Cham, 38–46. https://doi.org/10.1007/978-3-030-04372-8_4

[358] John Viega and Gary R McGraw. 2001. *Building Secure Software: How to Avoid Security Problems the Right Way* (1st ed.). Pearson Education.

[359] Manfred Vielberth, Fabian Bohm, Ines Fichtinger, and Gunther Pernul. 2020. Security Operations Center: A Systematic Study and Open Challenges. *IEEE Access* (2020), 1–25. https://doi.org/10.1109/ACCESS.2020.3045514

[360] Gabriela Villalobos-Zúñiga, Iyubanit Rodríguez, Anton Fedosov, and Mauro Cherubini. 2021. *Informed Choices, Progress Monitoring and Comparison with Peers: Features to Support the Autonomy, Competence and Relatedness Needs, as Suggested by the Self-Determination Theory*. Association for Computing Machinery, New York, NY, USA. https://doi.org/10.1145/3447526.3472039

[361] Florian Vogt, Bridget Haire, Linda Selvey, Anthea L Katelaris, and John Kaldor. 2022. Effectiveness evaluation of digital contact tracing for COVID-19 in New South Wales, Australia. *The Lancet Public Health* (feb 2022). https://doi.org/10.1016/S2468-2667(22)00010-X

[362] Melanie Volkamer and Karen Renaud. 2013. *Mental Models – General Introduction and Review of Their Application to Human-Centred Security*. Springer Berlin Heidelberg, Berlin, Heidelberg, 255–280. https://doi.org/10.1007/978-3-642-42001-6_18

[363] Cynthia Wagner, Alexandre Dulaunoy, Gérard Wagener, and Andras Iklody. 2016. MISP: The Design and Implementation of a Collaborative Threat Intelligence Sharing Platform. *Workshop on Information Sharing and Collaborative Security (WISCS)* (2016), 49–56. https://doi.org/10.1145/2994539.2994542 http://dl.acm.org/citation.cfm?doid=2994539.2994542.

[364] Thomas D. Wagner, Khaled Mahbub, Esther Palomar, and Ali E. Abdallah. 2019. Cyber threat intelligence sharing: Survey and research directions. *Computers & Security* 87 (2019), 101589. https://doi.org/10.1016/j.cose.2019.101589

[365] Michel Walrave, Cato Waeterloos, and Koen Ponnet. 2022. Reasons for Nonuse, Discontinuation of Use, and Acceptance of Additional Functionalities of a COVID-19 Contact Tracing App: Cross-sectional Survey Study. *JMIR Public Health Surveill* 8, 1 (14 Jan 2022). https://doi.org/10.2196/22113

[366] James Igoe Walsh. 2013. Intelligence Sharing. In *Routledge Companion to Intelligence Studies*. Routledge, Chapter chapter30. https://doi.org/10.4324/9780203762721.ch30

[367] Rick Wash. 2010. Folk Models of Home Computer Security. In *Proceedings of the Sixth Symposium on Usable Privacy and Security (SOUPS '10)*. Association for Computing Machinery, New York, NY, USA, Article 11, 16 pages. https://doi.org/10.1145/1837110.1837125

[368] Rodrigo Werlinger, Kasia Muldner, Kirstie Hawkey, and Konstantin Beznosov. 2010. Preparation, detection, and analysis: The diagnostic work of IT security incident response. *Information Management and Computer Security* 18, 1 (2010), 26–42. https://doi.org/10.1108/09685221011035241

[369] Tara Whalen and Kori M. Inkpen. 2005. Gathering evidence: Use of visual security cues in web browsers. *Proceedings - Graphics Interface* (2005), 137–144.

[370] Cathleen Wharton, John Rieman, Clayton Lewis, and Peter Polson. 1994. The Cognitive Walkthrough Method: A Practitioner's Guide. In *Usability Inspection Methods*, Jakob Nielsen and Robert L Mack (Eds.). John Wiley & Sons, Inc., New York, NY, USA, 105–140.

[371] Lucie White and Philippe van Basshuysen. 2021. Privacy versus Public Health? A Reassessment of Centralised and Decentralised Digital Contact Tracing. *Science and Engineering Ethics* 27, 2 (2021), 23. https://doi.org/10.1007/s11948-021-00301-0

[372] Alma Whitten and J. Doug Tygar. 1999. Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0. In *8th USENIX Security Symposium (USENIX Security 99)*. USENIX Association, Washington, D.C., 169–184. https://www.usenix.org/conference/8th-usenix-security-symposium/why-johnny-cant-encrypt-usability-evaluation-pgp-50

[373] WHO. 2021. *Global strategy on digital health 2020-2025*. Technical Report. World Health Organization.

[374] Mikael Wiberg. 2014. Methodology for materiality: interaction design research through a material lens.(Report). *Personal and Ubiquitous Computing* 18, 3 (2014).

[375] Simon N. Williams, Christopher J. Armitage, Tova Tampe, and Kimberly Dienes. 2021. Public attitudes towards COVID-19 contact tracing apps: A UK-based focus group study. *Health Expectations* 24, 2 (2021), 377–385. https://doi.org/10.1111/hex.13179

[376] Jacob O. Wobbrock and Julie A. Kientz. 2016. Research Contributions in Human-Computer Interaction. *Interactions* 23, 3 (apr 2016), 38–44. https://doi.org/10.1145/2907069

[377] Michael S Wogalter, David M DeJoy, and Kenneth R Laughery. 1999. Warnings and risk communication.

[378] Michael S. Wogalter and Kenneth R. Laughery. 1996. Warning! Sign and label effectiveness. *Current Directions in Psychological Science* 5, 2 (1996), 33–37.

[379] Flynn Wolf, Ravi Kuber, and Adam J. Aviv. 2019. "Pretty Close to a Must-Have": Balancing Usability Desire and Security Concern in Biometric Adoption. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems (CHI '19)*. Association for Computing Machinery, New York, NY, USA, 1–12. https://doi.org/10.1145/3290605.3300381

[380] World Health Organization. 2022. Statement – Cancer services disrupted by up to 50% in all countries reporting: a deadly impact of COVID-19 (February 3, 2022). Retrieved February 3, 2022. from https://www.euro.who.int/en/media-centre/sections/statements/2022/statement-cancer-services-disrupted-by-up-to-50-in-all-countries-reporting-a-deadly-impact-of-covid-19

[381] Peter Worthy, Ben Matthews, and Stephen Viller. 2016. Trust Me: Doubts and Concerns Living with the Internet of Things. In *Proceedings of the 2016 ACM Conference on Designing Interactive Systems (DIS '16)*. Association for Computing Machinery, New York, NY, USA, 427–434. https://doi.org/10.1145/2901790.2901890

[382] Min Wu, Robert C. Miller, and Simson L. Garfinkel. 2006. Do security toolbars actually prevent phishing attacks? *Conference on Human Factors in Computing Systems - Proceedings* 1 (2006), 601–610.

[383] Yuxi Wu, Panya Gupta, Miranda Wei, Yasemin Acar, Sascha Fahl, and Blase Ur. 2018. Your Secrets Are Safe: How Browsers' Explanations Impact Misconceptions About Private Browsing Mode. In *Proceedings of the 2018 World Wide Web Conference (WWW '18)*. International World Wide Web Conferences Steering Committee, Republic and Canton of Geneva, CHE, 217–226. https://doi.org/10.1145/3178876.3186088

[384] Chris Wymant, Luca Ferretti, Daphne Tsallis, Marcos Charalambides, Lucie Abeler-Dörner, David Bonsall, Robert Hinch, Michelle Kendall, Luke Milsom, Matthew Ayres, Chris Holmes, Mark Briers, and Christophe Fraser. 2021. The epidemiological impact of the NHS COVID-19 app. *Nature* 594, 7863 (2021), 408–412. https://doi.org/10.1038/s41586-021-03606-z

[385] Ka-Ping Yee. 2004. Aligning security and usability. *IEEE Security & Privacy* 2, 5 (2004), 48–55. https://doi.org/10.1109/MSP.2004.64

[386] J. Yoon, A.E. Pohlmeyer, and P.M.A. Desmet. 2015. *Positive Emotional Granularity Cards*. Delft University of Technology, Delft.

[387] YouGov. 2020. YouGov COVID-19 tracker: government handling, France. (November 24, 2020). Retrieved August 16, 2021 from https://yougov.co.uk/topics/international/articles-reports/2020/03/17/perception-government-handling-covid-19.

[388] YouGov. 2020. YouGov COVID-19 tracker: government handling, Germany. (November 18, 2020). https://yougov.co.uk/topics/international/articles-reports/2020/03/17/perception-government-handling-covid-19. Retrieved August 16, 2021 from.

[389] Eric Zeng, Shrirang Mare, and Franziska Roesner. 2017. End User Security and Privacy Concerns with Smart Homes. In *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*. USENIX Association, Santa Clara, CA, 65–80. https://www.usenix.org/conference/soups2017/technical-sessions/presentation/zeng

[390] Baobao Zhang, Sarah Kreps, Nina McMurry, and R. Miles McCain. 2020. Americans' perceptions of privacy and surveillance in the COVID-19 pandemic. *Plos one* 15, 12 (2020), e0242652.

[391] Ping Zhang and Na Li. 2005. The Importance of Affective Quality. *Commun. ACM* 48, 9 (Sept. 2005), 105–108. https://doi.org/10.1145/1081992.1081997

[392] Yinqian Zhang, Fabian Monrose, and Michael K. Reiter. 2010. The Security of Modern Password Expiration: An Algorithmic Framework and Empirical Analysis. In *Proceedings of the 17th ACM Conference on Computer and Communications Security (CCS '10)*. Association for Computing Machinery, New York, NY, USA, 176–186. https://doi.org/10.1145/1866307.1866328

[393] Serena Zheng, Noah Apthorpe, Marshini Chetty, and Nick Feamster. 2018. User Perceptions of Smart Home IoT Privacy. *Proc. ACM Hum.-Comput. Interact.* 2, CSCW, Article 200 (nov 2018), 20 pages. https://doi.org/10.1145/3274469

[394] Adam Zibak and Andrew Simpson. 2019. Cyber threat information sharing: Perceived benefits and barriers. *ACM International Conference Proceeding Series* (2019). https://doi.org/10.1145/3339252.3340528

[395] Marie-Laure Zollinger, Verena Distler, Peter Roenne, Peter Ryan, Carine Lallemand, and Vincent Koenig. 2019. User Experience Design for E-Voting: How mental models align with security mechanisms.

[396] Marie-Laure Zollinger, Ehsan Estaji, Peter Y. A. Ryan, and Karola Marky. 2021. "Just for the Sake of Transparency": Exploring Voter Mental Models of Verifiability. In *Electronic Voting*, Robert Krimmer, Melanie Volkamer, David Duenas-Cid, Oksana Kulyk, Peter Rønne, Mihkel Solvak, and Micha Germann (Eds.). Springer International Publishing, Cham, 155–170.

[397] Mary Ellen Zurko and Richard T. Simon. 1996. User-centered security. *Proceedings New Security Paradigms Workshop* Part F1294 (1996), 27–33.

# A

This section contains the supporting documents and materials from Chapter 3:

- UEQ Questionnaire
- Demographics Questionnaire
- Sentence Completion Questionnaire
- Qualitative codes table from the analysis of the Sentence Completion section


# User Experience Questionnaire

For the assessment of the MISP platform, please fill out the following questionnaire, which consists of pairs of contrasting attributes that may apply to the platform. You can express your agreement with the attributes by ticking the circle that most closely reflects your impression.

Example:

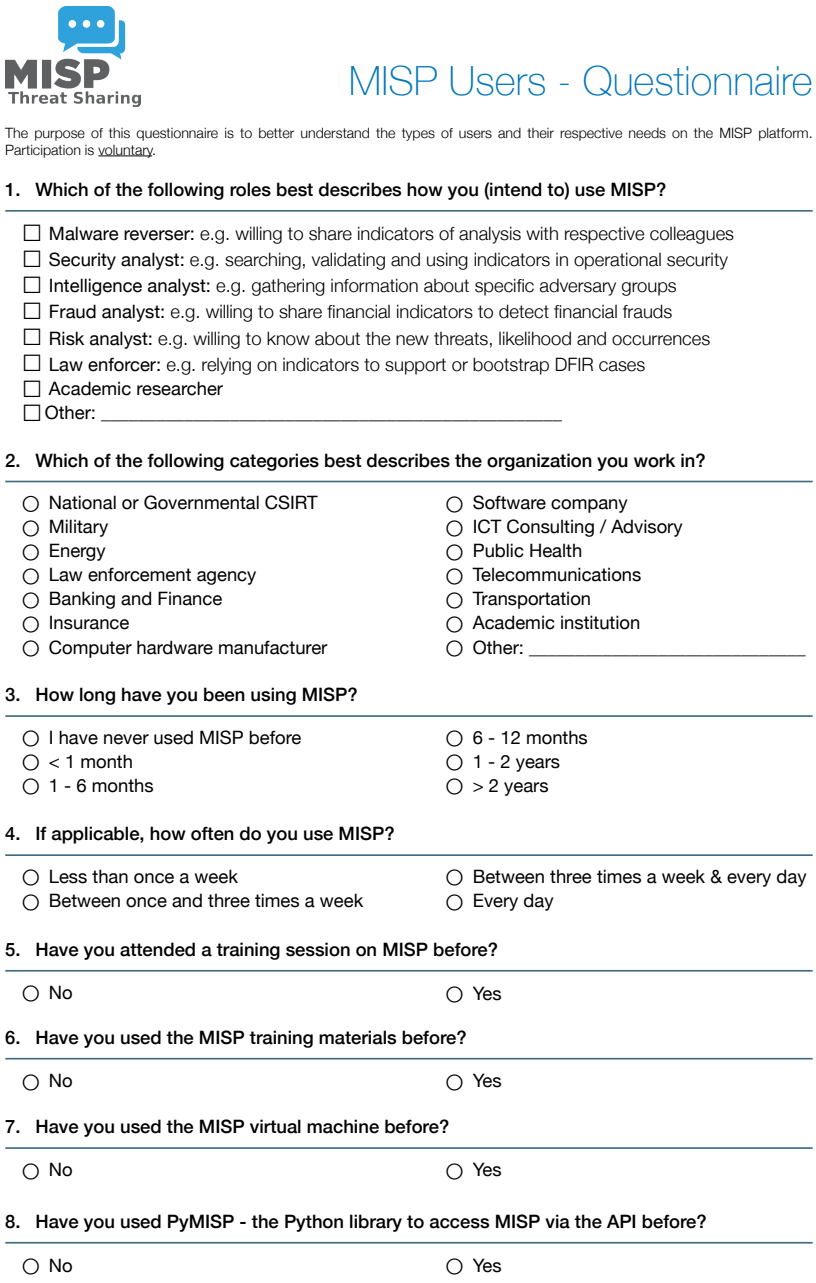
| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| attractive | ○ | ⊗ | ○ | ○ | ○ | ○ | ○ | unattractive |

This response would mean that you rate the application as more attractive than unattractive.

Please decide spontaneously. Don't think too long about your decision to make sure that you convey your original impression. Sometimes you may not be completely sure about your agreement with a particular attribute or you may find that the attribute does not apply completely to the platform. Nevertheless, please tick a circle in every line. It is your personal opinion that counts. Please remember: there is no wrong or right answer!

| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | | |
|---|---|---|---|---|---|---|---|---|---|
| annoying | ○ | ○ | ○ | ○ | ○ | ○ | ○ | enjoyable | 1 |
| not understandable | ○ | ○ | ○ | ○ | ○ | ○ | ○ | understandable | 2 |
| creative | ○ | ○ | ○ | ○ | ○ | ○ | ○ | dull | 3 |
| easy to learn | ○ | ○ | ○ | ○ | ○ | ○ | ○ | difficult to learn | 4 |
| valuable | ○ | ○ | ○ | ○ | ○ | ○ | ○ | inferior | 5 |
| boring | ○ | ○ | ○ | ○ | ○ | ○ | ○ | exciting | 6 |
| not interesting | ○ | ○ | ○ | ○ | ○ | ○ | ○ | interesting | 7 |
| unpredictable | ○ | ○ | ○ | ○ | ○ | ○ | ○ | predictable | 8 |
| fast | ○ | ○ | ○ | ○ | ○ | ○ | ○ | slow | 9 |
| inventive | ○ | ○ | ○ | ○ | ○ | ○ | ○ | conventional | 10 |
| obstructive | ○ | ○ | ○ | ○ | ○ | ○ | ○ | supportive | 11 |
| good | ○ | ○ | ○ | ○ | ○ | ○ | ○ | bad | 12 |
| complicated | ○ | ○ | ○ | ○ | ○ | ○ | ○ | easy | 13 |
| unlikable | ○ | ○ | ○ | ○ | ○ | ○ | ○ | pleasing | 14 |
| usual | ○ | ○ | ○ | ○ | ○ | ○ | ○ | leading edge | 15 |
| unpleasant | ○ | ○ | ○ | ○ | ○ | ○ | ○ | pleasant | 16 |
| secure | ○ | ○ | ○ | ○ | ○ | ○ | ○ | not secure | 17 |
| motivating | ○ | ○ | ○ | ○ | ○ | ○ | ○ | demotivating | 18 |
| meets expectations | ○ | ○ | ○ | ○ | ○ | ○ | ○ | does not meet expectations | 19 |
| inefficient | ○ | ○ | ○ | ○ | ○ | ○ | ○ | efficient | 20 |
| clear | ○ | ○ | ○ | ○ | ○ | ○ | ○ | confusing | 21 |
| impractical | ○ | ○ | ○ | ○ | ○ | ○ | ○ | practical | 22 |
| organized | ○ | ○ | ○ | ○ | ○ | ○ | ○ | cluttered | 23 |
| attractive | ○ | ○ | ○ | ○ | ○ | ○ | ○ | unattractive | 24 |
| friendly | ○ | ○ | ○ | ○ | ○ | ○ | ○ | unfriendly | 25 |
| conservative | ○ | ○ | ○ | ○ | ○ | ○ | ○ | innovative | 26 |

**Figure A.1:** UEQ Questionnaire



MISP Threat Sharing

# MISP Users - Questionnaire

The purpose of this questionnaire is to better understand the types of users and their respective needs on the MISP platform. Participation is voluntary.

**1. Which of the following roles best describes how you (intend to) use MISP?**

- ☐ **Malware reverser:** e.g. willing to share indicators of analysis with respective colleagues
- ☐ **Security analyst:** e.g. searching, validating and using indicators in operational security
- ☐ **Intelligence analyst:** e.g. gathering information about specific adversary groups
- ☐ **Fraud analyst:** e.g. willing to share financial indicators to detect financial frauds
- ☐ **Risk analyst:** e.g. willing to know about the new threats, likelihood and occurrences
- ☐ **Law enforcer:** e.g. relying on indicators to support or bootstrap DFIR cases
- ☐ Academic researcher
- ☐ Other: _____

**2. Which of the following categories best describes the organization you work in?**

- ○ National or Governmental CSIRT
- ○ Military
- ○ Energy
- ○ Law enforcement agency
- ○ Banking and Finance
- ○ Insurance
- ○ Computer hardware manufacturer
- ○ Software company
- ○ ICT Consulting / Advisory
- ○ Public Health
- ○ Telecommunications
- ○ Transportation
- ○ Academic institution
- ○ Other: _____

**3. How long have you been using MISP?**

- ○ I have never used MISP before
- ○ < 1 month
- ○ 1 - 6 months
- ○ 6 - 12 months
- ○ 1 - 2 years
- ○ > 2 years

**4. If applicable, how often do you use MISP?**

- ○ Less than once a week
- ○ Between once and three times a week
- ○ Between three times a week & every day
- ○ Every day

**5. Have you attended a training session on MISP before?**

- ○ No
- ○ Yes

**6. Have you used the MISP training materials before?**

- ○ No
- ○ Yes

**7. Have you used the MISP virtual machine before?**

- ○ No
- ○ Yes

**8. Have you used PyMISP - the Python library to access MISP via the API before?**

- ○ No
- ○ Yes

**Figure A.2:** Demographics Questionnaire 1/2

9. Have you cloned a MISP repository before?

○ No ○ Yes

10. Have you contributed to any of the MISP repositories before?

○ No ○ Yes

11. Do you have an engineering or computer science background?

○ No ○ Yes

12. What is the highest level of school you have completed / degree you have received?

○ Less than high school degree
○ High school diploma or equivalent
○ Associate degree in college (2-year)
○ Bachelor's degree
○ Master's degree
○ Doctoral degree
○ Professional degree (JD, MD)
○ Other: _____

13. What is your age group?

○ 17 and under
○ 18-25
○ 26-35
○ 36-45
○ 46-55
○ 56-65
○ 66+
○ Prefer not to submit

14. To which gender identity do you most identify?

○ Prefer not to say
○ Female
○ Male
○ Prefer to self-describe

15. Do you have any additional comments that you would like to share?

**Thank you for your participation!**

**Figure A.3:** Demographics Questionnaire 2/2


# Sentence Completion

Please complete the sentences below. There are no wrong replies, respond rather quickly without thinking too long. You can leave a sentence without an answer if you feel that it is not suitable for your situation.

When I use MISP, I feel …

_____

MISP is best for …

_____

MISP is not suitable for …

_____

I think the appearance of MISP is …

_____

I am happy with MISP because …

_____

The problem with MISP is …

_____

People who use MISP are typically …

_____

Compared to other threat information sharing platforms, MISP is …

_____

**Figure A.4:** Sentence Completion Questionnaire

| Code System | Frequency |
|---|---|
| Code System | 322 |
| USER-RELATED | 106 |
| Psychological Needs | 0 |
| Control | 0 |
| Structure | 1 |
| Routines and Habits | 3 |
| Autonomy | 2 |
| Personalization | 6 |
| Competence | 0 |
| Self-efficacy | 3 |
| Relatedness | 17 |
| User profiles | 28 |
| Users that do not share | 1 |
| Inactive users | 1 |
| Non-experts | 0 |
| Beginners / No technical expertise | 11 |
| Experts | 2 |
| Technical expertise | 13 |
| Beliefs and Attitudes | 2 |
| Emotional Responses | 0 |
| Negative | 0 |
| Agitation | 0 |
| Frustration | 1 |
| Overwhelm | 0 |
| Confusion | 14 |
| Uncertainty of action | 0 |
| Insecurity | 1 |
| Unmotivation | 0 |
| Boredom | 2 |
| Positive | 0 |
| Gratification | 0 |
| Satisfaction | 6 |
| Relief | 1 |
| Interest | 0 |
| Fascination | 1 |
| Inspiration | 1 |
| Assurance | 0 |
| Courage | 3 |
| Pride | 3 |
| Confidence | 4 |
| Animation | 0 |
| Energetic | 2 |
| Optimism | 0 |
| Enjoyment | 0 |
| Joy | 2 |
| Amusement | 1 |
| Empathy | 0 |
| Respect | 1 |
| Kindness | 1 |

**Figure A.5:** Qualitative codes table 1/3

| Code System | Frequency |
|---|---|
| SYSTEM-RELATED | 207 |
| MISP characteristics | 0 |
| Openess | 8 |
| Adaptation | 10 |
| Features | 0 |
| Integration | 1 |
| Feature-Request | 1 |
| API | 1 |
| User-Role Hierarchy | 1 |
| Marketing aspects | 5 |
| Cost-Benefit | 0 |
| Benefit | 4 |
| Brand recognition | 1 |
| Usefulness and UX Qualities | 0 |
| Attractiveness | 6 |
| Aesthetics | 16 |
| Lack of Attractiveness | 7 |
| Pragmatic Qualities | 0 |
| Usability | 2 |
| Perspicuity | 3 |
| Dependability | 12 |
| Support | 7 |
| Efficiency | 5 |
| Organized | 1 |
| Utility | 11 |
| Organizing data | 6 |
| Searching data | 1 |
| Analyzing data | 2 |
| Correlating | 2 |
| Contextualizing | 7 |
| TI Sharing and Collaborating | 19 |
| Technical Threat Intelligence (TTI) | 7 |
| Lack of Pragmatic Qualities | 0 |
| Lack of usability | 0 |
| Lack of dependability | 1 |
| Lack of perspicuity | 6 |
| Complexity | 25 |
| Lack of efficiency | 2 |
| Lack of clarity | 5 |
| Lack of utility | 2 |
| Analyzing data | 1 |
| Searching data | 1 |
| TI Sharing and Collaborating | 2 |
| Workflows | 6 |
| Sectors | 1 |
| Hedonic Qualities | 0 |
| Novelty | 3 |
| Stimulation | 4 |
| Exciting | 1 |
| Interesting | 1 |
| Motivating | 1 |

**Figure A.6:** Qualitative codes table 2/3

| Code System | Frequency |
|---|---|
| Lack of Hedonic Qualities | 0 |
| Lack of Novelty | 2 |
| Lack of Stimulation | 2 |
| TRAINING-RELATED | 1 |
| Useful | 1 |
| FLAG | 4 |
| N/A | 4 |

**Figure A.7:** Qualitative codes table 3/3

# B

This section contains the supporting documents and materials from Chapter 5:

- Formalization of an s-t transition system
- Focus Group Materials

### Formalization of an S-T transition system

An *s-t transition system* $\mathcal{M}$ is a tuple $(S, Act, Prop, \rightarrow, I, \mathcal{A}, evSys, evUsr)$ where

- $S = \{s_1, ..., s_k\}$ is a finite set of states
- $Act$ is a finite set of action names
- $Prop$ is a finite set of atomic propositions
- $\xrightarrow{x} \subseteq S \times (Act \cup Prop) \times S$ is a transition relation
- $I \subseteq S$ is a set of initial states
- $\mathcal{A} = \{a_1, \ldots, a_n\}$ is a finite set of variable names. Each $a_i \in \mathcal{A}$ has a corresponding domain $D_{a_i}$ with a partial order defined. The value *undefined* ($\perp$) is in every $D_{a_i}$
- $evSys, evUsr : \mathcal{A} \times S \rightarrow \bigcup_{i=1}^{n} D_{a_i}$ are evaluation functions that, in each $s_j \in S$, assign to each $a_i \in \mathcal{A}$ a value from its predefined domain $D_{a_i}$

### Formalization of socio-technical security properties

**Aligned-SoS** At every state of the ceremony, the *sense of security* that the user has about a specific aspect corresponds to the assignment from the technical side i.e., it corresponds to the system's evaluation of security. **AG** $a_i^{usr} = a_i^{sys}$

**Lower-SoS** There is a state in the ceremony, where the user's *sense of security* about a specific aspect is lower than the system's evaluation of security. **EF** $a_i^{usr} < a_i^{sys}$

**Higher-SoS** There exists a state during the ceremony where the user's *sense of security* about a specific aspect exceeds the system's evaluation of security. **EF** $a_i^{usr} > a_i^{sys}$

**Misaligned-Goal** There exists a path where, even if the evaluation of all other aspects is aligned all the time, the understanding regarding the achievement of the goal differs from the user's and system's point of view. **E** $\left(\left(a_1^{usr} = a_1^{sys} \wedge \cdots \wedge a_n^{usr} = a_n^{sys}\right)\ \mathbf{U}\ \left(goal^{usr} \neq goal^{sys}\right)\right)$

Further details can be found in [328].

### Focus Group Materials

Focus Group participant template for eliciting positive and negative emotions along 24 user journey steps, and the supplementary p≡p documentation.

Name: _____

Please write down the first three positive and negative emotions (if possible) that come to your mind at each step of the User Journey. You can also add additional comments if you like.

| STEP / SITUATION | Positive Emotions | Negative Emotions | Optional comments |
|---|---|---|---|
| **Recognising the problem / need to use secure e-mail (encryption, decryption etc.)** | | | |
| **Searching online for secure e-mail 'solutions' and evaluating among the alternatives.** | | | |
| **Having made a choice and purchased one of the 'solutions'.** | | | |
| **Installing and setting up the purchased secure e-mail 'solution' system.** | | | |
| **Having installed and set up the system.** | | | |
| **Sending the first e-mail after installing the system.** | | | |
| **Receiving the first e-mail after installing the system.** | | | |
| **Reading the Documentation / FAQ of the system.** | | | |
| **Receiving an e-mail you are unable to read as it is full of random characters.** | | | |
| **Receiving an email from your correspondent complaining that he/she is unable to read the email you sent, as it is full of random characters.** | | | |
| **Temporarily disabling the secure e-mail system in order to send a message to a colleague that at the moment doesn't use such a system.** | | | |
| **Sending a confidential e-mail using the system to a wrong recipient.** | | | |
| **Receiving an email whose Privacy status is indicated by the system as being Unknown.** | | | |
| **Receiving an email that is indicated by the system as being Unsecure.** | | | |
| **Receiving an email that is indicated by the system as being Secure.** | | | |
| **Receiving an email that is indicated by the system as being Secure & Trusted.** | | | |
| **Realising that even though you exchanged an e-mail securely with your correspondent, you can only fully trust it's him/her if you authenticate each other.** | | | |
| **Authenticating yourself with your correspondent.** | | | |
| **Exchanging e-mails with a correspondent you have authenticated and who you have designated to trust.** | | | |
| **Receiving an email indicated by the system as Unsecure, even though it comes from a person that you authenticated and designated to trust.** | | | |
| **Realising a confidential piece of information you shared via e-mail with a correspondent you authenticated and who you designated to trust gets leaked online.** | | | |
| **Changing the trust levels of people you authenticated.** | | | |
| **Changing the default settings of the secure e-mail system.** | | | |
| **Contacting the support team of the company that develops the secure e-mail system.** | | | |

**Figure B.1:** Focus Group Materials

Name: _____

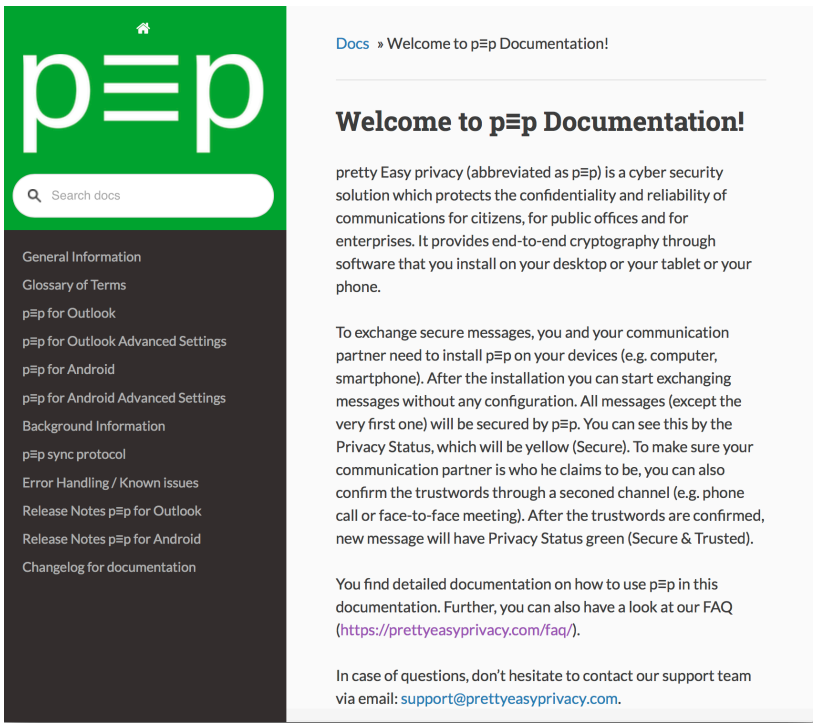
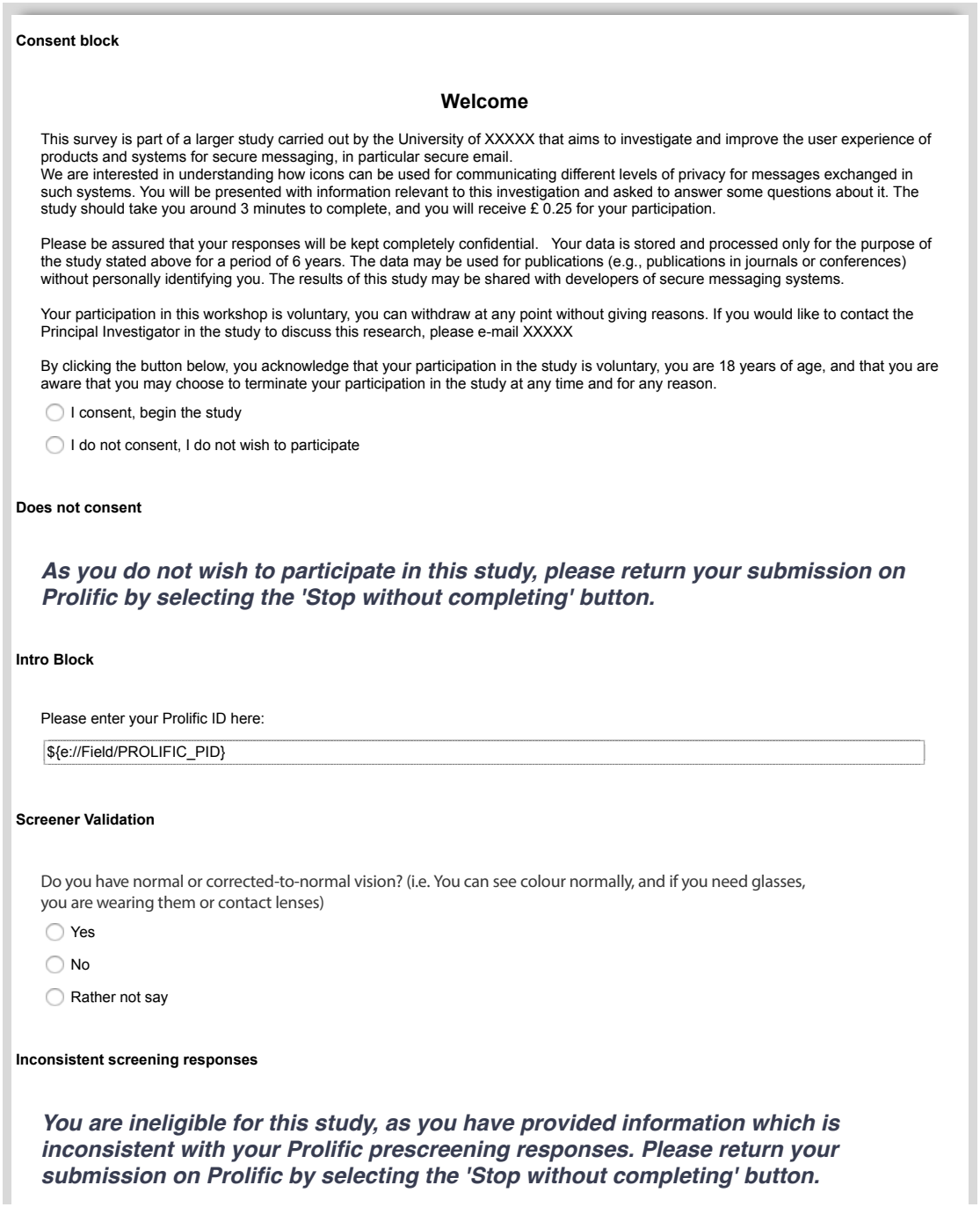



**Figure B.2:** Focus Group Materials

# C

This section contains the supporting documents and materials from Chapter 6:

- Survey Information and Consent Form
- Study B and C Survey
- Study D Survey
- Study E Survey
- Study F Survey



**Consent block**

**Welcome**

This survey is part of a larger study carried out by the University of XXXXX that aims to investigate and improve the user experience of products and systems for secure messaging, in particular secure email.
We are interested in understanding how icons can be used for communicating different levels of privacy for messages exchanged in such systems. You will be presented with information relevant to this investigation and asked to answer some questions about it. The study should take you around 3 minutes to complete, and you will receive £ 0.25 for your participation.

Please be assured that your responses will be kept completely confidential. Your data is stored and processed only for the purpose of the study stated above for a period of 6 years. The data may be used for publications (e.g., publications in journals or conferences) without personally identifying you. The results of this study may be shared with developers of secure messaging systems.

Your participation in this workshop is voluntary, you can withdraw at any point without giving reasons. If you would like to contact the Principal Investigator in the study to discuss this research, please e-mail XXXXX

By clicking the button below, you acknowledge that your participation in the study is voluntary, you are 18 years of age, and that you are aware that you may choose to terminate your participation in the study at any time and for any reason.

- ◯ I consent, begin the study
- ◯ I do not consent, I do not wish to participate

**Does not consent**

***As you do not wish to participate in this study, please return your submission on Prolific by selecting the 'Stop without completing' button.***

**Intro Block**

Please enter your Prolific ID here:

${e://Field/PROLIFIC_PID}

**Screener Validation**

Do you have normal or corrected-to-normal vision? (i.e. You can see colour normally, and if you need glasses, you are wearing them or contact lenses)

- ◯ Yes
- ◯ No
- ◯ Rather not say

**Inconsistent screening responses**

***You are ineligible for this study, as you have provided information which is inconsistent with your Prolific prescreening responses. Please return your submission on Prolific by selecting the 'Stop without completing' button.***

**Figure C.1:** Survey Information and Consent Form (Study D - F)

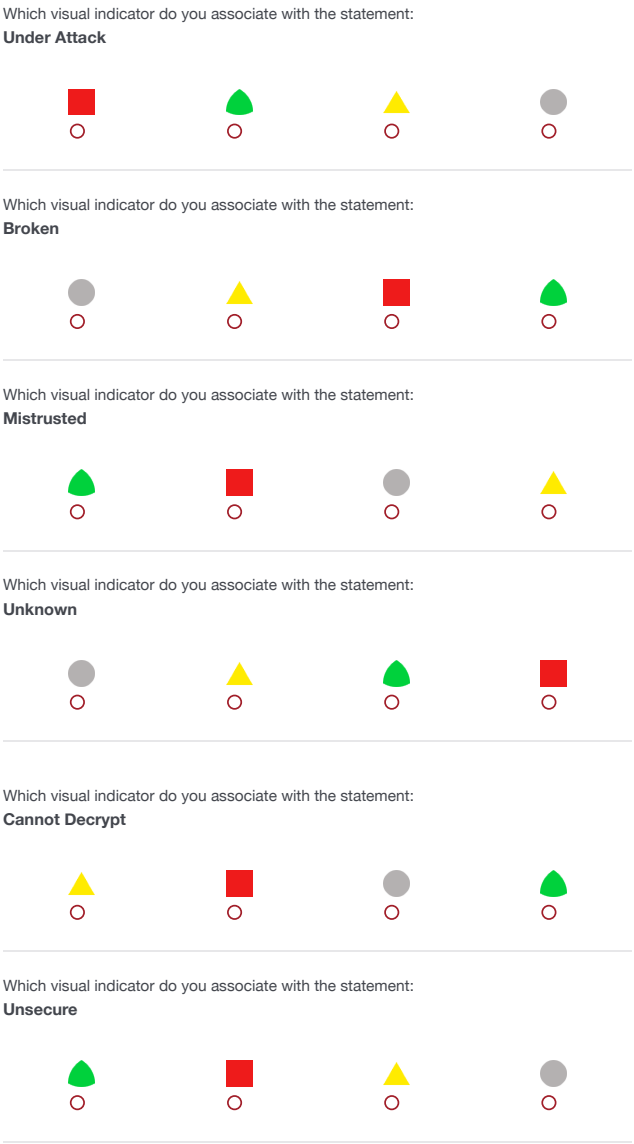



**Figure C.2:** Study B and C - Survey (p. 1)

Which visual indicator do you associate with the statement:
**Unsecure for Some**

Which visual indicator do you associate with the statement:
**Unreliable Security**

Which visual indicator do you associate with the statement:
**Secure**

Which visual indicator do you associate with the statement:
**Secure & Trusted**

**Indicators Explanations Block**

Which visual indicator do you associate with the explanation:
**This message is not secure and has been tampered with.**

Which visual indicator do you associate with the explanation:
**This message has broken encryption or formatting.**

Which visual indicator do you associate with the explanation:
**This message has a communication partner that has previously been marked as mistrusted.**

Which visual indicator do you associate with the explanation:
**This message does not contain enough information to determine if it is secure.**

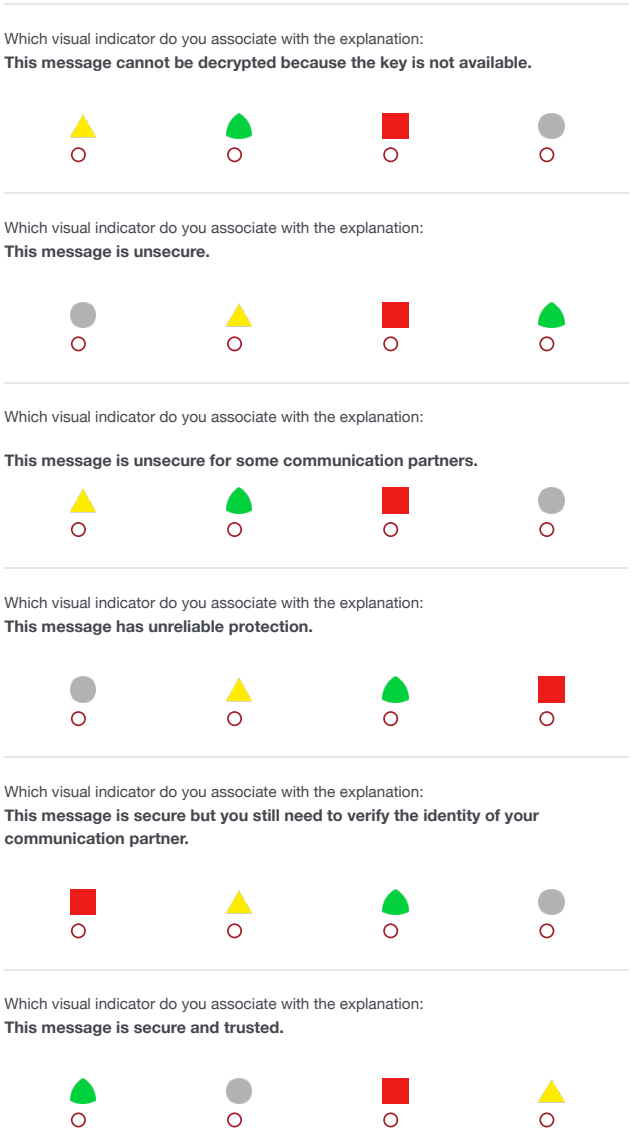



**Figure C.3:** Study B and C - Survey (p. 3)

**Select the icon that matches best with the text under it?**

Mistrusted

Mistrusted

**Select the icon that matches best with the text under it?**

Secure & Trusted

Secure & Trusted

**Select the icon that matches best with the text under it?**

Secure

Secure

**Demographics**

Do you have a computer science or technical background?

- Yes
- No

Have you ever used tools/systems for end-to-end e-mail encryption?

- Yes
- No
- I don't know

Please enter which tools/systems for end-to-end e-mail encryption you use or have used in the past?

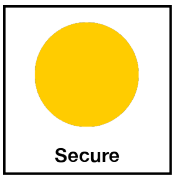
**Figure C.4:** Study D - Survey

Take a look at the following icon and label under it.


Please state whether you agree or disagree with the following statement?

| | Strongly disagree | Disagree | Somewhat disagree | Neither agree nor disagree | Somewhat agree | Agree | Strongly agree |
|---|---|---|---|---|---|---|---|
| The icon is a good representation of the text under it. | ○ | ○ | ○ | ○ | ○ | ○ | ○ |

Take a look at the following icon and label under it.




Please state whether you agree or disagree with the following statement?

| | Strongly disagree | Disagree | Somewhat disagree | Neither agree nor disagree | Somewhat agree | Agree | Strongly agree |
|---|---|---|---|---|---|---|---|
| The icon is a good representation of the text under it. | ○ | ○ | ○ | ○ | ○ | ○ | ○ |

Take a look at the following icon and label under it.


Please state whether you agree or disagree with the following statement?

| | Strongly disagree | Disagree | Somewhat disagree | Neither agree nor disagree | Somewhat agree | Agree | Strongly agree |
|---|---|---|---|---|---|---|---|
| The icon is a good representation of the text under it. | ○ | ○ | ○ | ○ | ○ | ○ | ○ |

**Demographics**

Do you have a computer science or technical background?

- ○ Yes
- ○ No

Have you ever used tools/systems for end-to-end e-mail encryption?

- ○ Yes
- ○ No
- ○ I don't know

Please enter which tools/systems for end-to-end e-mail encryption you use or have used in the past?

**Figure C.5:** Study E - Survey

**Onboarding**

To distinguish between three different levels of privacy, one system for secure emailing uses the following visual indicators:


We will now ask you a few questions about these indicators.

**ST-Block**

Take a look at the following icon and label under it.


Please state whether you agree or disagree with the following statement?

| | Strongly disagree | Disagree | Somewhat disagree | Neither agree nor disagree | Somewhat agree | Agree | Strongly agree |
|---|---|---|---|---|---|---|---|
| The icon is a good representation of the text under it. | ○ | ○ | ○ | ○ | ○ | ○ | ○ |

Why do you think so?

**Secure Block**

Take a look at the following icon and label under it.


Please state whether you agree or disagree with the following statement?

| | Strongly disagree | Disagree | Somewhat disagree | Neither agree nor disagree | Somewhat agree | Agree | Strongly agree |
|---|---|---|---|---|---|---|---|
| The icon is a good representation of the text under it. | ○ | ○ | ○ | ○ | ○ | ○ | ○ |

Why do you think so?

**Mistrusted Block**

Take a look at the following icon and label under it.


Please state whether you agree or disagree with the following statement?

| | Strongly disagree | Disagree | Somewhat disagree | Neither agree nor disagree | Somewhat agree | Agree | Strongly agree |
|---|---|---|---|---|---|---|---|
| The icon is a good representation of the text under it. | ○ | ○ | ○ | ○ | ○ | ○ | ○ |

Why do you think so?

**Demographics**

Do you have a computer science or technical background?

- ○ Yes
- ○ No

Have you ever used tools/systems for end-to-end e-mail encryption?

- ○ Yes
- ○ No
- ○ I don't know

Please enter which tools/systems for end-to-end e-mail encryption you use or have used in the past?

**Figure C.6:** Study F - Survey

# D

This section contains the supporting materials from Chapter 7:

- Semi-structured Focus Group Guide
- Qualitative Codebook

## Semi-structured Focus Group Guide

- Informed Consent
- Welcome
- WHO excerpt
- Q1: Have you ever used an official contact tracing app nationally approved by a health authority or the government?
- Q2: Why did you decide to [use | not use] a national contact tracing app?
- Q3: What do you see as the major benefits (if any) of using a contact tracing app?
- Q4: What do you see as the major drawbacks (if any) of using a contact tracing app?
- Q5: What features of the contact tracing app [do you | did you] use? What [do you | did you] value most about the app?
- Q6: When travelling abroad, would you be willing to install a contact tracing app approved by the public health authorities or government of the country where you are travelling to?
- Q7: Should a contact tracing app from your country be able to detect and share proximity contacts with other users of contact tracing apps, regardless of the app or its country of origin?
- Q8: Are there any privacy concerns that you have with respect to the use of national contact tracing apps?
- Debrief

## Qualitative Codebook

We present our codebook with the first- and second-level codes as well as their respective counts below.

• **adoption (48)**: *active social context (1), avoiding misinformation (1), curiosity (2), personal safety (7), influence (1), request / mandate (1), security, privacy & trust (10), society (21), technical capability (1), usefulness (3)*; • **non-adoption (64)**: *herd mentality (3), lack of efficiency (4), lack of interoperability (1), lack of promotion (1), lack of role models (2), lack of technical capability (1), distrust in the government (6), distrust in the developers (2), distrust in the technology (4), lack of usability (8), lack of utility (12), limited / lack of social interactions (4), privacy concerns (11), psychological discomfort (4), voluntary approach (1)*; • **benefits (56)**: *self-determination (16), useful features (1), efficiency (2), staying informed (4), identification of potential risks (11), mental and emotional comfort (4), help in modelling the spread (3), identification of infections (15)*; • **drawbacks (47)**: *potential repercussions (1), interoperability (1), costs and expenses (9), lack of usability (3), lack of functionality (1), lack of perceived effectiveness (13), privacy invasion (6), lack of clear information / communication (6), lack of perceived benefits (7)*; • **features (7)**: *requests (7)*;

This thesis was typeset using LaTeX, originally developed by Leslie Lamport and based on Donald Knuth's TeX.
It uses the Dissertate template by Jordan Suchow.