USER EXPERIENCE WITH MOBILE SECURITY AND PRIVACY MECHANISMS

vorgelegt von
Dipl.-Ing.
Lydia Kraus
geb. in Memmingen

von der Fakultät IV - Elektrotechnik und Informatik
der Technischen Universität Berlin
zur Erlangung des akademischen Grades

Doktorin der Ingenieurwissenschaften
– Dr.-Ing. –

genehmigte Dissertation

Promotionsausschuss:

Vorsitzender: Prof. Dr. Jean-Pierre Seifert
Gutachter: Prof. Dr.-Ing. Sebastian Möller
Gutachterin: Prof. Dr.-Ing. Delphine Reinhardt
Gutachter: Prof. Dr. Markus Dürmuth

Tag der wissenschaftlichen Aussprache: 4. Juli 2017

Berlin 2017

Lydia Kraus: *User experience with mobile security and privacy mechanisms*

ABSTRACT

Smartphones have become indispensable in the life of many people. They are constant companions, connections to the world, information sources, and substitutes for other devices and tools that had to be carried individually in the past. While smartphones offer a variety of sources for positive user experience, their downside is their vulnerability to security attacks and the potential they offer to harm a users' privacy. However, due to their known vulnerabilities, smartphones also encompass a number of mechanisms to protect a user's security and privacy. This thesis focuses especially on security and privacy mechanisms which are visible to the end-user and which involve actions by the end-user, such as app permissions and screen locks with authentication.

Research on the human factors related to mobile security and privacy mechanisms often follows the usable security and privacy paradigm. Thereby, usability forms the basis of understanding and improving the interaction between humans and security systems. An extension of the usability paradigm is the user experience (UX) paradigm which considers interaction factors beyond usability such as motivation, affect and emotion, and joy of use.

The present thesis extends the body of knowledge on human factors and mobile security and privacy mechanisms by taking a user experience approach to the topic. It first investigates users' experiences with and motivations to use mobile security and privacy in several qualitative, explorative studies. The findings thereof suggest that users not only suffer from limited usability of mobile security and privacy mechanisms, but that such mechanisms also need to address non-functional product qualities (e.g. hedonic quality) and the fulfillment of psychological needs. Those needs do not necessarily have to be related to the psychological need of Security only, but can also encompass aspects such as Autonomy and Stimulation.

By the help of two use cases – app permissions and screen locks with authentication – several quantitative studies evaluate the potential of these mechanisms to shape the user experience in general and in particular with respect to hedonic quality. The results of the quantitative studies suggest that usability is an important factor for a good user experience with mobile security and privacy mechanisms. Furthermore, the results indicate that also these kinds of mechanisms can be manipulated in their potential to address aspects such as hedonic quality and need fulfillment. This suggests an extended design space for mobile security and privacy mechanisms which provides system designers with new possibilities to design secure systems that enable

positive experiences. Based on these findings, directions for future research are discussed.

ZUSAMMENFASSUNG

Smartphones sind im Leben vieler Menschen unabkömmlich geworden – sie sind ständige Begleiter, Verbindung in die Welt, Informationsquellen und zu guter Letzt ein Ersatz für viele Geräte oder Werkzeuge, die man in der Vergangenheit einzeln mit sich tragen musste. Obwohl Smartphones eine Vielzahl an positiven Erlebnissen bieten können, leiden sie unter der Einschränkung, dass sie verwundbar gegenüber Angriffen auf die Sicherheit und Privatsphäre der Nutzer sind. Aus diesem Grund beinhalten Smartphones jedoch eine Reihe von Mechanismen zum Schutz gegen selbige. Die vorliegende Dissertation beschäftigt sich mit der Anwendung solcher Mechanismen und dabei speziell mit den Mechanismen, die vom Endnutzer wahrgenommen und eingesetzt werden können, wie zum Bespiel App-Berechtigungen und Bildschirmsperren mit Authentifizierung.

Die Erforschung menschlicher Einflussfaktoren in Bezug auf die Nutzung mobiler Sicherheits- und Privatsphäremechanismen folgt oft dem Paradigma der "Usable Security and Privacy". In diesem Paradigma ist die Gebrauchstauglichkeit der Kernfaktor um Interaktionen mit mobilen Sicherheits- und Privatsphäremechanismen zu verstehen und zu verbessern. Eine Erweiterung des Gebrauchstauglichkeitsparadigmas ist das Nutzererlebnisparadigma (*engl.* User Experience (UX)), das Interaktionsaspekte berücksichtigt, die über die Gebrauchstauglichkeit hinausgehen, wie z.B. Motivation, Affekt und Emotion, oder auch Spaß bei der Nutzung.

Die vorliegende Dissertation erweitert den Kenntnisstand zu menschlichen Einflussfaktoren bei der Interaktion mit mobilen Sicherheits- und Privatsphäremechanismen, indem sie einen Nutzererlebnis-basierten Ansatz zur Erforschung des Themengebiets aufgreift. Dabei werden zuerst Nutzererlebnisse mit und Motivatoren für die Nutzung mobiler Sicherheits- und Privatsphäremechanismen in qualitativen Studien erforscht. Die Ergebisse dieser Studien deuten darauf hin, dass Nutzer nicht nur unter der eingeschränkten Gebrauchstauglichkeit solcher Systeme leiden, sondern, dass auch Bedarf besteht, nicht-funktionale Produktqualitäten (wie z.B. hedonische Qualität) und die Erfüllung von psychologischen Bedürfnissen mit solchen Mechanismen anzusprechen. Diese Bedürfnisse müssen sich nicht allein am psychologischen Bedürfnis nach Sicherheit ausrichten, sondern können auch andere Bedürfnisse wie zum Beispiel das Bedürfnis nach Autonomie und Stimulation einschließen.

Anhand zweier Fallbeispiele – App-Berechtigungen und Bildschirmsperren mit Authentifizierung – wird in mehreren quantitativen Stu-

dien das Potenzial dieser Mechanismen, das Benutzererlebnis im Allgemein und im Besonderen in Bezug auf hedonische Qualitäten zu formen, evaluiert. Die Ergebnisse der quantitativen Studien lassen darauf schließen, dass Gebrauchstauglichkeit ein wichtiger Faktor für das Benutzererlebnis mit solchen Mechanismen ist. Darüber hinaus zeigen die Ergebnisse, dass auch solche Arten von Mechanismen in ihrem Potenzial, Aspekte wie hedonische Qualität und Bedürfniserfüllung anzusprechen, manipuliert werden können. Dies eröffnet einen erweiterten Gestaltungsraum für mobile Sicherheits- und Privatsphäremechanismen, der Systemdesignern neue Möglichkeiten bietet sichere Systeme, deren Benutzung ein positives Benutzererlebnis hervorruft, zu gestalten. Basierend auf diesen Ergebnissen werden Richtungen für zukünftige Forschung aufgezeigt.

PUBLICATIONS

Parts of this thesis have been previously published in the following papers or articles. An asterisk (*) at the end of a paper indicates that I received support from students in conducting the studies and/or analyzing the data. In that case, the students provided support according to my instructions or under my guidance.

Peer-reviewed workshop, conference, and journal publications:

"Using Statistical Information to Communicate Android Permission Risks to Users." Lydia Kraus, Ina Wechsung, and Sebastian Möller. *Proceedings of the 4th Workshop on Socio-Technical Aspects in Security and Trust. Co-located with the 27th IEEE Computer Security Foundations Symposium.* IEEE. 2014, pp. 48 -– 55. `http://dx.doi.org/10.1109/STAST.2014.15` *

While searching Google Play for a new app, I noticed that many apps of similar functionality greatly differ in the number and kinds of permissions they request. Consequently, I came up with the concept of using statistical information about permissions of apps with similar functionality to support users in estimating the privacy intrusiveness of an app. I designed and conducted the user study, analyzed the data, and wrote the manuscript. Ina Wechsung supported me with the study design and the data analysis. Furthermore, she provided feedback on the manuscript. Sebastian Möller provided feedback for the study design and on the manuscript.

"Analyzing end-users' knowledge and feelings surrounding smartphone security and privacy." Lydia Kraus, Tobias Fiebig, Viktor Miruchna, Sebastian Möller, and Asaf Shabtai. *Proceedings of the Workshop on Mobile Security Technologies (MoST). Co-located with the IEEE Symposium on Security & Privacy.* 2015. 11 pages.*

This paper is based upon my idea to understand threat models of mobile security and privacy from a user's perspective. I designed and conducted the focus group study, analyzed the data and wrote the manuscript. Tobias Fiebig supported me with his knowledge of IT security during the course of the research and greatly contributed to the abstract, the introduction and the background section of the manuscript. Furthermore, he supported me in finalizing the discussion section. Viktor Miruchna was a great support in data analysis. Asaf Shabtai provided feedback during the preparation of the study

and for the manuscript, and Sebastian Möller provided feedback for finalizing the paper.

"Exploring Psychological Need Fulfillment for Security and Privacy Actions on Smartphones." Lydia Kraus, Ina Wechsung, and Sebastian Möller. *Proceedings of the 1st European Workshop on Usable Security (EuroUSEC)*. Internet Society. 2016. 12 pages. http://dx.doi.org/10.14722/eurousec.2016.23009 *

This paper is based on my idea to understand users' motivations to use mobile security and privacy mechanisms from an experiential point of view, by applying Hassenzahl's user experience framework. While I came up with the concept, designed and conducted the interview study, Ina Wechsung contributed to data analysis and the discussions with Ina Wechsung supported me in making sense of the data. I then wrote the manuscript for which Ina Wechsung and Sebastian Möller provided feedback.

"Psychological Needs as Motivators for Security and Privacy Actions on Smartphones." Lydia Kraus, Ina Wechsung, and Sebastian Möller. *Journal of Information Security and Applications (JISA)*. Volume 34, Part 1. Elsevier. 2017. pp. 34–45. https://doi.org/10.1016/j.jisa.2016.10.002 *

This article is an extended version of a previously published paper ("Exploring Psychological Need Fulfillment for Security and Privacy Actions on Smartphones.", see above). Together with Ina Wechsung, I conducted an additional online study to investigate psychological need fulfillment when using mobile security and privacy mechanisms. Ina Wechsung provided support for the study design and the data analysis and gave feedback on the manuscript which was written by myself. Sebastian Möller also provided feedback on the manuscript.

"User Experience in Authentication Research: A survey." Lydia Kraus, Jan-Niklas Antons, Felix Kaiser, and Sebastian Möller. *Proceedings 5th ISCA/DEGA Workshop on Perceptual Quality of Systems*. ISCA/DEGA. 2016. pp. 54 – 58. http://dx.doi.org/10.21437/PQS.2016

This paper is based on my idea to understand to which extent the concept of user experience has been taken up in works on usable authentication. I contributed the concept and analyzed the data together with Felix Kaiser. The discussions with Jan-Niklas Antons and Sebastian Möller helped me to clarify the dimensions and influencing factors of user experience. The manuscript was written by myself; all co-authors provided feedback on the manuscript.

"Implications of the Use of Emojis in Mobile Authentication." Lydia Kraus, Robert Schmidt, Marcel Walch, Florian Schaub, Christopher Krügelstein, and Sebastian Möller. *Who are you? Adventures in Authentication; Workshop at the Symposium on Usable Privacy and Security (SOUPS)*. 2016. 2 pages.*

This short position paper results from an ongoing collaboration between myself (together with colleagues and students from the Quality and Usability Lab), Marcel Walch and Florian Schaub. It presents the EmojiAuth prototype and shortly summarizes the results of a lab study on Emoji-based mobile authentication. The paper was written by myself with support of Marcel Walch and Florian Schaub. Detailed results of the collaboration on EmojiAuth are presented in the paper "On the Use of Emojis in Mobile Authentication" (see subsequent paper).

"On the Use of Emojis in Mobile Authentication." Lydia Kraus, Robert Schmidt, Marcel Walch, Florian Schaub, and Sebastian Möller. *32nd International Conference on ICT Systems Security and Privacy Protection (IFIP SEC)*. IFIP Advances in Information and Communication Technology, vol 502. Springer. 2017. pp. 265-280. `http://dx.doi.org/10.1007/978-3-319-58469-0_18` *

This paper is based on my idea to investigate the influence of Emoji-based authentication on user experience and behavior. While I conducted the studies and analyzed the data, Florian Schaub's and Marcel Walch's experience from earlier studies on graphical authentication and their advice regarding the design of the lab and the field study have been invaluable for the study designs. Furthermore, Marcel Walch contributed with his knowledge on mobile and graphical authentication to the related work section of the paper. Robert Schmidt implemented the EmojiAuth app according to my ideas and provided valuable feedback on issues of implementation. I wrote the initial manuscript and iteratively improved it with support from Florian Schaub and Marcel Walch. Sebastian Möller provided feedback during the course of the research and on the manuscript.

The following paper was under submission to a peer-reviewed workshop when this thesis was submitted for review:

"Comparing the Influence of Different App Permission User Interfaces on User Experience and Behavior." Lydia Kraus, Domenic Reuschel, Maija Poikela and Sebastian Möller. *Unpublished*. 2017. 6 pages.

This paper is based on my idea to compare the influence of different permission user interfaces on user experience and behavior. While I came up with the concept and advertised a student thesis accordingly, Domenic Reuschel designed the online study under my guidance and also used the obtained data for his Bachelor's thesis. As Domenic's research questions differed in some parts from my research questions, I independently analyzed the data for this paper. Maija Poikela provided input on the user interface design of the permission dialogs. The manuscript was written by myself. All co-authors provided feedback on the manuscript.

"The purpose of life is to live it, to taste experience to the utmost, to reach out eagerly and without fear for newer and richer experience."

— Eleanor Roosevelt

ACKNOWLEDGMENTS

At this point, I want to thank all people who have accompanied me during the last years and provided support, especially during the time that I was working on this thesis.

Special thanks go to my supervisor and mentor, Prof. Dr.-Ing. Sebastian Möller, for supporting me with my research and giving me the freedom to find my own way and research interests. Furthermore, I am very grateful to Prof. Dr.-Ing. Delphine Reinhardt and Prof. Dr. Markus Dürmuth who agreed to serve on my doctoral committee. I am indebted to Dr.-Ing. Ina Wechsung who helped me to acquire the knowledge needed to conduct psychological studies. She was also the one who called my attention to the fact that, besides usable security and privacy, user experience is also an extremely interesting research topic. Thank you for the many collaborations and for being my mentor the last four years!

During the time at the Quality and Usability Lab, I further had the pleasure to work with many dear colleagues: Dr.-Ing. Jan-Niklas Voigt-Antons and Dr. Benjamin Weiss who were always ready to listen and to provide advise when I needed a second opinion on scientific questions or organizational issues, Alexander Bajic, Maija Poikela, and Tobias Hirsch, with whom I worked together in the "Usable Security and Privacy" research group, Prof. Michael Wagner and Laura Fernandez-Gallardo, Ph.D., who were great collaborators in the Biometrics Seminar, and Dr.-Ing. Tilo Westermann and Dr.-Ing. Stefan Hillmann who were great room mates and proof-read parts of this thesis. I am also grateful to Irene Hube-Achter and Yasmin Hillebrenner for providing administrative support.

Special thanks go to my long-time student workers Robert Schmidt and Felix Kaiser who were a great support for my research!

During the work on this thesis, I also had the opportunity to collaborate with several awesome researchers of whom some even turned into friends: Tobias Fiebig who shared his deep knowledge on IT security with me, Dr. Florian Schaub who shared his deep understanding of usable security and privacy with me, as well as the art of writing papers that are interesting to read, and Marcel Walch, who shared his knowledge on graphical authentication and LaTeX with me. I also enjoyed very much the scientific discussions with Dr. Asaf Shabtai and Dr. habil. Florian Kammüller.

During the work on my thesis, I also had the opportunity to supervise some great students in study projects and in writing their thesis.

My deepest thanks go to my family and friends. Working on this thesis was an exciting, but sometimes also exhausting time and I am grateful that I have a great family and great friends who often cheered me up. My deepest gratitude goes to you, Arne, the love of my life, for showing me the adventures that life and the world have to offer. With your never-ending love and support you made the last four years much easier to bear up. I am also grateful to my parents, Anne and Willi († 2015), and my sisters, Julia and Antonia, for their love and support. Deepest thanks also go to my friends Iris, Kaca, Slavica, Jakob, and Ari. Thanks for your friendship and support! I am further grateful to my former boss, Prof. Sanja Vranes, who provided great support during my time in Belgrade and who showed me how much fulfillment research can bring to one's life.

CONTENTS

LIST OF FIGURES

LIST OF TABLES

ACRONYMS

ATT	Attractiveness
AUT	Autonomy
BOD	Physical/Bodily
COMP	Competence
FG	Focus Group
HCI	Human-Computer Interaction
HQ	Hedonic Quality
KTM	Keeping the meaningful
MON	Money/Luxury
PIN	Personal Identification Number
POP	Popularity
PQ	Pragmatic Quality
REL	Relatedness

SE Self-Esteem

SEC Security

SEL Self-actualization

STIM Stimulation

UI User Interface

USP Usable Security and Privacy

UX User Experience

Part I

INTRODUCTION

1 INTRODUCTION

1.1 MOTIVATION

1.1.1 *Smartphones: opportunities and threats*

Since the early 2000's, smartphones have experienced an immense growth in popularity[1]. As of 2016, more than half of Germany's population is using a smartphone [181]. Being hybrids of computers and mobile phones, smartphones offer vast functionality on a small size. Modern smartphones have a relatively high processing power and are equipped with a variety of sensors for connectivity and activity tracking such as WiFi, bluetooth, GPS, and accelerometer. At the same time, smartphones feature a relatively high storage volume.

The mentioned characteristics allow users to pursue a variety of smartphone-related activities. Third party and native applications (apps) for all kind of purposes such as information gathering, gaming, efficiency tools, and the like are available. Users can communicate over a variety of channels such as instant messaging, SMS, and calling. Furthermore, smartphones provide functionality for which additional tools such as cameras and alarm clocks were necessary in past.

As a consequence smartphones offer vast opportunities for positive experiences. However, there is also a lot of sensitive data gathered with the phone, processed, and finally stored on the phone or remotely. This makes smartphone users vulnerable to security and privacy related threats.

But what do the terms *security* and *privacy* mean? This thesis adopts the ISO/IEC 2382-8 definition of security, and the privacy definition by Westin, according to Garfinkel and Lipfort who also use these definitions in their book on the history of usable security [69]. In ISO/IEC 2382-8, security is defined as "the protection of data and resources from accidental or malicious acts, usually by taking appropriate actions" [95]. ISO/IEC 2382-8 further defines security threats, i.e. "accidental and malicious acts" as "modification, destruction, access, disclosure, or acquisition if not authorized". Schneier notes that security is a process which enables the effective use of security products [172]. The process thereby consists of prevention, detection, and response. Similar to Schneier, Bishop notes in the organizational context that a security system consists of requirements, policies, mecha-

1 Text fragments of the present chapter have been previously published in Kraus, Antons, Kaiser, and Möller (2016) [124] and Kraus, Wechsung, and Möller (2016) [121].

nisms, and assurance [18]. Mechanisms thereby serve to enforce security policies and may be either of technical or procedural nature [18]. The end-user is usually involved in the security process through the interaction with security mechanisms. As the present thesis is settled in the context of end-user security, its focus is on users' interaction with security and privacy mechanisms.

In the remainder of this thesis, privacy is defined according to Westin's definition. This definition states that privacy is the "right of an individual to control the accuracy, use, and distribution of digital information about themselves" [200]. A privacy mechanism is thus a technological or procedural mean that enables a user to control the accuracy, use, and distribution of digital information about themselves.

Related work indicates that users are concerned about security related threats and about their privacy on smartphones [32, 59, 100, 123, 150]. In a survey on mobile internet usage among German smartphone users, 70% of the respondents either strongly agreed or agreed with the statement that "mobile internet usage carries the risk that somebody gains illegal access to my data" [100].

To mitigate security and privacy related risks there is a variety of mechanisms users can apply [93]. The downside of such mechanisms is, however, that their deployment and usage takes additional time, adds complexity to the interactions, and keeps the users from pursuing their primary task. As a consequence, users may start circumventing those mechanisms.

1.1.2 *From security and privacy to usability*

There are several examples of how users circumvent security and privacy mechanisms in the mobile context. For example, a user may not pay attention to app permissions and grant them without reading [61]. Or, users may choose easy-to-guess passwords or PINs to restrict access to their smartphone [22].

In the past, users used to be blamed for acting in an insecure manner and for decreasing system security [1]. However, around the mid 90's the research field of Usable Security and Privacy (USP) emerged [69]. USP is an interdisciplinary field of study bringing together methods from Human-Computer Interaction (HCI) research, and thereby specifically usability engineering, and security and privacy research (when writing about usability in this thesis, I refer to the ISO 9241-11 definition of usability: "The extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use" [178]).

USP research started to promote another view on security: instead of blaming the users for security failures, the goal of USP is to ensure that the design of security mechanisms is usable and follows a user-centered design approach [1]. Dourish and Anderson identify

three main areas in USP research: empirical studies on security practice, empirical studies on the usability of security, and design of new security and privacy mechanisms for end-users [50]. While there is consensus that security and privacy mechanisms need usability and user-centered design, there is no "official" guideline that would tell security and privacy mechanisms designers how this can be achieved.

Usable security and privacy is different from usability studies of consumer or work-related products as security and privacy mechanisms need to be evaluated under a threat model [69]. Furthermore, usable security and privacy is complex, as the three factors interact in complex ways and improving one of them does not necessarily lead to the improvement of the other factors [69]. Several works have approached the issue of what usability in the security and privacy context means. Some of those works are summarized in the book "Usability and Security", edited by Cranor and Garfinkel [40]: for example, Adams and Sasse emphasize the importance of feedback to the user on the security of the system [1]. They further note raising awareness about threats, user guidance, and the compatibility of security mechanisms and work procedures as crucial factors of user-centered design. Whitten and Tygar also emphasize the importance of threat awareness and the ability of users to "figure out how to successfully perform" security tasks [202]. Furthermore, they note the prevention of dangerous errors made by users and that users need to be "sufficiently comfortable with the interface to continue using it".

In their book on the history of usable security of 2014, Garfinkel and Lipfort summarize several lessons that have been learned during two decades of research regarding the user-centered design of usable security and privacy mechanisms [69, pp. 87]: the number of decisions a user has to make needs to be reduced; defaults need to be "safe and secure"; users need to be provided with "better information, not more information"; users need a "clear context" to "make good decisions"; the presentation of information to users is "critical"; and, user "education works" to a certain point, "but has limits".

The above mentioned recommendations are important milestones and address typical aspects of usability in the context of security and privacy research. They emphasize the functional aspects of the interaction: Users should be educated in order to be able to achieve security tasks. Furthermore, the system should be designed for usability by providing guidance, feedback, preventing dangerous errors, avoiding too many user decisions, providing usable information presentation and a clear context for decision making.

1.1.3 *From usability to user experience*

Around the beginning of the new millennium, a new research area emerged within the field of HCI: whereas until this time, the focus

of determining system qualities has been rather on functional aspects related to usability, researchers got more and more interested in viewing interactions with products holistically [9]. This holistic view on user interactions with systems and products - conceptualized in the term "User Experience (UX)" - focuses on users' experiences with a product or system, for instance in terms of affect and emotion, non-instrumental product qualities, and situatedness of interaction [87].

In the present thesis, I deploy the definition of user experience given in the UX White Paper which has been elaborated by Roto et al. as a result of a Dagstuhl seminar on Demarcating User Experience [165].

> "Experience in general covers everything personally encountered, undergone, or lived through. User experience differs from 'experiences in a general sense', in that it explicitly refers to the experience(s) derived from encountering systems." — Roto et al. [165, p.6]

In his book on user experience, Hassenzahl provides three main reasons why it is important to take experience design into account in HCI: experiences help users to identify themselves with a product, experiences are able to evoke positive feelings, and experiences can serve as motivators for future actions [83]. McCarthy and Wright argue that "it is only by seeing technology as participating in felt experience that we understand the fullness of its potential" [145, preface]. User experience research emphasizes not only a holistic perspective on interaction with technology, it also includes aspects such as affect, emotion and motivation in the context of human-computer interaction (cf. e.g. [9, 83]). Moreover, UX may change depending on the context and is considered to be time-dependent, i.e. it may change over time and is not constant [9, 87, 133, 145]. From a product perspective, user experience encompasses not only usability-related product characteristics, but also a capability of a product to address positive aspects of interaction reflected in attributes such as hedonic quality [82] (cf. Section 2.1.2). In several studies, positive experiences with products have been shown to positively influence long-term customer relationships [33, 70], cited according to [128].

The necessity to include principles from user experience research into the design of security and privacy technologies in order to gain a rich understanding of people's experiences and practices with security and privacy mechanisms, has been recognized in earlier works [21, 51]. UX approaches foster the ability to unify the three USP research areas as defined by Dourish and Anderson [50] (cf. Section 1.1.2). Investigating security practice and usability from an experiential point of view has the potential to unfold new ideas regarding the design of new security and privacy mechanisms for end-users. Addressing aspects of positive experience in the interaction with security and pri-

vacy mechanisms may furthermore positively influence the adoption of such mechanisms.

However, the use of UX-centered approaches is not yet common in USP research. Dunphy et al. note in their work on experience-centered security and privacy that the UX-centered approach has been only slowly taken up in USP research [51]. Furthermore, Kraus et al. found in a literature survey on user experience and usable authentication that while several of the considered works (19%) contained UX topics, only a minority of those papers explicitly mentioned in their abstract or title the word "experience" or "user experience" [124]. Thus, UX seems not yet to be recognized as an own field of study in USP research [124].

1.2 RESEARCH QUESTIONS AND CONTRIBUTIONS

The present thesis aims at advancing the state of knowledge about UX-centered mobile security and privacy. While aspects of usability and actual security/privacy are crucial for the analysis of security and privacy mechanisms, this thesis investigates aspects beyond the functional towards an experiential view of such mechanisms. This means that – besides usability and security/privacy evaluations – experiential aspects such as users' feelings and motivations are investigated. Furthermore, it is investigated how such aspects contribute to the interactions with mobile security and privacy mechanisms. Thereby, the thesis first explores the experiences that smartphone users have with security and privacy mechanisms. Thereafter, it explores the motivators for using such mechanisms from an experiential perspective. Based on these two explorations it reflects on the principles that should be used in the experiential design of mobile security and privacy mechanisms.

The insights gained from the explorative studies address the following research questions:

- **RQ1:** What experiences do users have with security and privacy on their smartphones?
- **RQ2:** What motivates users to employ security and privacy actions on their smartphones?
- **RQ3:** Which principles should the experiential design of mobile security and privacy mechanisms follow?

By learning from the answers of **RQ1**, **RQ2**, and **RQ3**, prototypes of and user interfaces for mobile security and privacy mechanisms were developed. Those prototypes and user interfaces were evaluated regarding their potential to shape user experience and security and privacy related behavior, leading to the following research questions:

- **RQ4:** How do specific implementations of mobile security and privacy mechanisms perform in terms of usability, user experience, security and/or privacy?
- **RQ5:** Is it possible to manipulate the hedonic quality of security and privacy mechanisms on smartphones?
- **RQ6:** How does the user experience with a mobile security mechanism develop over time?

By answering the above mentioned research questions, this thesis contributes (1) a collection of security and privacy related experiences that users may encounter when using their smartphones and (2) a collection of the most salient intrinsic motivational factors in terms of psychological needs for using mobile security and privacy mechanisms (3) three prototypes that were designed to address experiential aspects of mobile security and privacy (4) an evaluation of the prototypes in terms of usability, user experience, security, and/or privacy (5) and insights on the temporal development of user experience on a mobile security mechanism.

1.3 STRUCTURE OF THE THESIS

In Part II of the thesis, the field of user experience and its dimensions are discussed (cf. Chapter 2). Thereafter, related work on threats and risk mitigation for smartphones is detailed, as well as related work on the usability and adoption of mobile security and privacy mechanisms (Chapter 3).

Empirical studies on the user experience with mobile security and privacy mechanisms are presented in Part III and Part IV of this thesis. Part III presents research that explores in a mostly qualitative manner the experiences that users have with security and privacy on their smartphones (Chapter 5) and the psychological needs that motivate users to voluntarily use such mechanisms (Chapter 6). Furthermore, implications of the findings of those two chapters are drawn. Consequently, Part III addresses RQ1, RQ2, and RQ3. Part IV introduces the use cases of app permissions and mobile authentication to showcase how the design of such mechanisms influences user experience and related security and privacy behavior: in Chapter 8-10, different prototypes of app permissions and mobile authentication are introduced that build upon the findings of Part III (Chaper 5 and 6), and dedicated literature. Those prototypes are then quantitatively evaluated regarding the user experience they provide and the related security and privacy behavior they evoke. Furthermore, the development of user experience over time is evaluated for the mobile authentication prototype. Consequently, Part IV addresses RQ4, RQ5, and RQ6. Part V of the thesis finally draws conclusions, and reflects on future work (Chapter 11).

Part II

THEORETICAL BACKGROUND AND RELATED WORK

2 USER EXPERIENCE

User Experience (UX) is not just "old wine in new bottles". It is a truly extended and distinct perspective on the quality of interactive technology: away from products and problems to humans and the drivers of positive experience.

— Marc Hassenzahl [82, p.11]

In the Introduction, the motivation for investigating the user experience with security and privacy mechanisms was presented. The reader has heard that UX is a new concept with a holistic view on users' interactions with a system. Furthermore, the reader has heard that UX has been – so far – little considered in USP research. However, which aspects does UX encompass? How can it be measured? The present chapter will shed light to these questions[1].

2.1 WHAT IS USER EXPERIENCE?

When discussing the concept of UX, one needs to distinguish between an *experience* and *experiencing*. Experiencing occurs in every moment, whereas an experience is a judgment of past events [83]. Experiencing – in the context of user experience – is a "stream of perceptions, interpretations of those perceptions, and resulting emotions during an encounter with a system" [165, p.7]. Those perceptions, interpretations, and emotions are subjective [83, 133]. They are seen through the eye of an individual observer and vary between observers, but they also vary within observers [83]. For example, a user who is rather unfamiliar with digital technologies and who wants to use a smartphone for the first time, may be confused by the variety of icons and options presented on the user interface (UI). However, once gotten familiar with the device, the user may be enchanted by the new features and possibilities that smartphones offer compared to traditional feature phones. Thus, an experience is unique, is likely to change over time, and cannot be replicated [83, 145]. Referring back to the example of the novice smartphone user, this user will never encounter again the experience of using a smartphone for the first time.

A lot of research and discussion in the UX research and practitioner community has taken place to come to a unified definition of what UX is (cf. e.g. [9, 87, 133, 165]). A survey among UX researchers and practitioners, conducted in 2008 by Law et al. [133], revealed that even

1 Text fragments of this chapter have been previously published in Kraus, Wechsung and Möller, 2016 [121].

within the community there is dissent about the interrelation and importance of different UX aspects. The community agreed, however, that user experience is subjective, dynamic, and context-dependent [133]. Another source of dissent among academics is whether UX can and should be measured [132]. Whereas one part of researchers argues for a "qualitative design-based" approach, another part argues for a "quantitative model-based" approach [132, p.1].

In the following, two UX frameworks from related work, the framework by McCarthy and Wright [145] which can be considered as qualitative design-based, and the framework by Hassenzahl [83] which can be considered as quantitative model-based, are presented. After discussing and comparing the two frameworks, the UX dimensions used in this thesis will be defined.

2.1.1 *McCarthy and Wright's experience framework*

The framework suggested by McCarthy and Wright in their book "Technology as Experience" [145] mainly builds upon works of the philosophers Dewey and Bhaktin. McCarthy's and Wright's framework emphasizes the importance of a holistic view on experience without being reductionistic [206]: it aims at understanding the complex interactions between different threads of experience and at recognizing sense-making as the "central process of experiencing" [206, p. 44] (cf. Figure 1). They suggest four threads to describe experiences and six processes of making sense of an experience. The four threads include the *sensual*, the *emotional*, the *spatio-temporal* and the *compositional* thread.

The sensual thread refers to the "sense or meaning immediately available in a situation" [145, p. 87]. As such it describes gut feelings or intuitions. A question to pose when investigating the sensual thread could be, for example, how a situation is/was perceived at the first look. In contrast to the sensual thread, which is, as described above, rather based on intuitive feelings, the emotional thread describes the emotional response to an experience. The concepts of emotions will be discussed in detail later on in this chapter (cf. Section 2.2.1). The spatio-temporal thread encompasses the context and situation in which an experience takes place. Furthermore, it describes the temporal development of an experience as well as the perceived temporal aspects. McCarthy and Wright provide the following example: "An intense emotional engagement can make our sense of time change. A frustrating experience can leave us perceiving space as confined and closeting." [145, p. 91]. The compositional thread describes how different parts of an experience contribute to the experience as a whole [145].

The six processes of sense-making help to describe how an individual subjectively makes sense of an experience. They encompass *antic-*

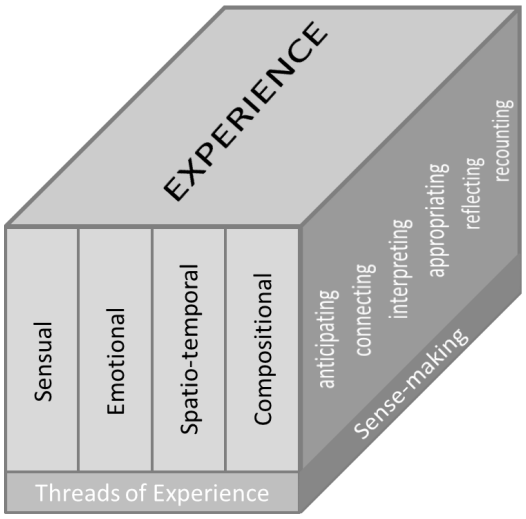


Figure 1: Illustration of McCarthy and Wright's UX framework.

ipating, *connecting*, *interpreting*, *reflecting*, *appropriating*, and *recounting* [145]. McCarthy and Wright emphasize that there is no particular order of the processes and no implication of causality between the processes [145].

In summary, McCarthy and Wright stress the importance of experience as a subjective, holistic, and dynamic construct. The four threads of experiences help to describe the parts of an experience in terms of feelings, emotions, context or space, and time, as well as the interaction between the parts of an experience. The six processes of sense-making help to reflect on individual sense-making of an experience.

2.1.2 *Hassenzahl's user experience framework*

Whereas McCarthy and Wright provide a framework to describe experiences, experiencing, and making sense of an experience, Hassenzahl emphasizes the importance of a (technological) artifact that accounts for the experience. In his book "Experience Design - Technology for all the right reasons" [83], Hassenzahl describes different properties of experience and how they relate to the interaction with an artifact.

According to Hassenzahl, experiences are subjective, holistic, situated, and dynamic, but nevertheless manipulable ("shapeable") by technology [83]. To describe the relation between technology and experience, Hassenzahl suggests a three-tier hierarchical model of user experience (cf. Figure 2). This model is based upon the self-regulation theory by Carver and Scheier [30] and activity theory (cf. e.g. [20]). The three tiers consist of be-goals, do-goals, and motor goals. Be-goals are related to motives, do-goals are related to actions, and motor-

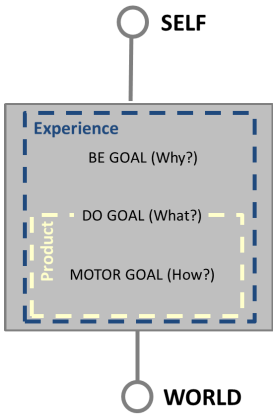


Figure 2: Hassenzahl's UX framework. Graphic based on [83].

goals to specific conditions [83]. Thus, be-goals describe *why* something is done, do-goals describe *what* is done, and motor-goals describe *how* it is done. For example, a user who feels bored could download a game on the smartphone. Escaping the feeling of boredom and experiencing instead an interesting game that makes time fly by would be the be-goal then (i.e. being entertained). Downloading and playing a game would be the do-goal and playing the particular implementation of the game the motor-goal. Whereas much work in human-computer interaction (HCI) mainly considered designing for do- and motor-goals, Hassenzahl's model aims at taking a holistic perspective by also considering aspects of personal relevance of the user (i.e. the be-goals) [83].

To deploy the model to the design of experience-centered products, Hassenzahl suggests to use classes of be-goals that correspond to classes of experiences. Although an experience cannot be replicated, products can be designed to address classes of experience [83]. For example, (smartphone) games likely all have in common that they entertain users and enable them to escape boredom (and other experiences). Reading a book could provide a similar experience. Although very different products, both could be described as belonging to the class of products that offer the potential for entertaining experiences. The particular experience itself is however, as described above subjective, dynamic, and situated. One person may prefer reading a book over playing a smartphone game; another person might have played a game so many times that it is not interesting anymore; yet another person might not be in the right situation to enjoy playing the game and might thus have a negative experience or no experience at all.

Consequently, emotional responses to an experience can be positive or negative. Whereas work with a focus on do-goals and motor-goals is rather engaged with avoiding negative experiences by making products usable, Hassenzahl stresses that user experience design

should strive for designing positive experiences or at least experiences that are worthwile [83].

The question is now what makes an experience positive. In the beginning of the 2000's, Sheldon et al. investigated the question of what makes satisfying life events satisfying [175]. Thereby, they investigated the role of basic psychological needs from well-known theories of psychological need fulfillment (such as Deci and Ryan's self-determination theory [46], Epstein's cognitive-experiential self-theory [57]) as a basis for making events satisfying. They found that the fulfillment of psychological needs is related to positive feelings ("affect", as it is called in the psychology literature) [175]. Based on Sheldon et al.'s work on psychological needs and satisfying life events [175], Hassenzahl suggests using psychological needs as classes of be-goals and thus classes of positive experiences [83]. In a study on positive experiences with interactive products, Hassenzahl et al. also showed a relation between positive affect and psychological need fulfillment in this context [85]. More detail about the theory of psychological needs and their relation to positive user experiences will be given later on in this chapter (cf. Section 2.2.1).

In the preceding paragraphs, it has been detailed how Hassenzahl's UX framework describes the emergence of user experience with interactive products from the interaction of be-, do-, and motor-goals. But how do particular product qualities contribute to the user experience? Hassenzahl provides an additional framework to describe the relation between be- and do-goals and product quality. According to this framework, product qualities can be divided into pragmatic and hedonic quality aspects [81, 83]. Pragmatic Quality (PQ) relates to the capability of a product to achieve the task for which the product was designed for [81]. Pragmatic quality is thus related to do-goals [83]. Hedonic Quality (HQ) relates to the capability of a product to address aspects of *personal relevance* [81, p. 38] and is thus related to the fulfillment of be-goals [83]. Both constructs can be measured with the AttrakDiff questionnaire [84] and will be detailed later on in this chapter (cf. Section 2.2.2).

In summary, Hassenzahl provides a framework which describes different properties of experiences such as being subjective, dynamic, holistic, and situated. Moreover, Hassenzahl provides a three-tier model of user experience that connects experiences as an outcome of the interaction between be-, do-, and motor-goals. To enable positive experiences, products should address psychological need fulfillment. The pragmatic/hedonic model describes product quality in terms of the capability of a product to fulfill do- and be-goals.

2.2 USER EXPERIENCE DIMENSIONS

Both user experience frameworks introduced in Section 2.1.1 and Section 2.1.2, have some aspects in common, but differ in other aspects. Whereas McCarthy and Wright argue that it should be avoided to reduce experiences to certain aspects, Hassenzahl's framework suggests the deployment of classes of experiences in order to design products accordingly [83]. For the present thesis, which is concerned with the design of smartphone security and privacy mechanisms, I apply portions of both frameworks, with a focus on Hassenzahl's framework due to its connection between the design of products and the user experience.

In both of the introduced frameworks, the central role of emotions in UX is stressed. Also, already in early work on psychology, dating back to 1890, James suggests that emotions color experiences [114]. Thus, emotions will be considered as an aspect in this thesis that contributes to UX. To account for McCarthy and Wright's sensual thread, I will further take into account feelings (a distinction between the concepts will be provided later on). Furthermore, psychological needs as sources of positive experiences will be taken into account.

Hassenzahl's model of hedonic and pragmatic product quality will be deployed as it describes the system dimension of experience. It is described in detail in Section 2.2.2.

Both frameworks and other earlier works agree on UX being dynamic, subjective, and context dependent (or situated) (cf. e.g. [83, 133, 145, 165]). Consequently, situatedness and time are also included as sub-dimensions of user experience.

Roto et al. define three factors that affect UX: the user, the system, and the context [165]. I will use these three factors as main dimensions according to which the related sub-dimensions that emerged from McCarthy and Wright's and Hassenzahl's UX framework are structured: affect, emotion, feelings and psychological needs relate to the *user* dimension of UX; hedonic and pragmatic product quality to the *system* dimension of UX; and time and situatedness to the *context* dimension of UX.

2.2.1 *User: affect, emotion, and psychological needs*

The *user* dimension encompasses the sub-dimensions that are inherent to the user from a psychological perspective: affect, emotion, and feelings, as well as psychological needs.

Affect, Emotion, and Feelings

As described above, emotions and feelings play a central role in UX. Emotion itself has been subject to discussion among researchers and a final definition of the concept has not yet been established [114][103].

Several works agree that emotions can be measured in terms of behavior, physiology, and conscious-experience (cf. e.g. Mauss and Robinson [144] as referenced by Keltner et al. [114] or Lang [130] as referenced by Bradley and Lang [25]). In his work "Core Affect and the Psychological Construction of Emotion", Russel provides a framework for the description of prototype emotions which will be discussed in the following [166].

At the heart of emotion lies the *core affect*. Russel describes *core affect* as the "simply feeling of good or bad, energized or enervated" [166, p. 145]. *Core affect* can be described in terms of valence (pleasure – displeasure) and arousal (energized –enervated). For example, happiness is a rather energized affect with high positive valence (i.e. pleasure); jittery, is an affect which is described as highly energized and of rather negative valence (i.e. displeasure). According to Russel, emotion is constructed from *core affect*, *perception of affective quality*, *attribution to object*, *appraisal*, *instrumental action*, *emotional meta-experience*, and *emotion regulation* [166]. Each of these components contributes to what Russel calls "a prototype of a specific emotion". Thereby, the components influence each other but they are not in a particular causal order [166]. An emotional episode is triggered by an event which is perceived in terms of affect. *Attribution* is the degree to which the event is perceived as being responsible for the affect. By attributing an affect to an event, the event is becoming an object. *Appraisal* includes the cognitive processes starting to assess the object in terms of "its future prospects, its relevance to one's goals, its causal antecedents" [166, p. 150]. A prototypical emotion further encompasses an *action*, that is, for example, "approach versus withdrawal" from the object prepared by "physiological and expressive changes" such as "facial or vocal changes" [166, p. 150]. The emotion is furthermore consciously experienced.

As can be seen from the description above, emotions are complex constructs, their description and measurement is not straight forward. There exist, however, different questionnaires to measure affect such as the Positive Affect – Negative Affect Schedule (PANAS) [196] and the Self-Assessment Manikin (SAM) [25, 131].

Furthermore, I consider feelings in this thesis as part of UX. Thereby, feelings are defined as gut feelings or intuitions which may be parts of emotions but for which it is not possible to tell whether they include all components as defined in Russel's framework.

Psychological needs

The framework by Russel considers appraisal, i.e. the assessment of goal congruity with an object that has been attributed to an affect, as part of an emotion. The present sub-section describes basic goals that all humans have in common – that are – basic psychological needs.

Psychological needs have been suggested in several theories as an explanation for human behavior[2]: for instance, self-determination theory suggests basic psychological needs as the fundamental mechanism for self-motivation [167]. Furthermore, it has been shown that need fulfillment is related to satisfying events and positive affect [175].

In their work on satisfying life events, Sheldon et al. define psychological needs as "particular qualities of experience that all people require to thrive" [175, p. 325]. However, they also note that so far there is no consensus about what those needs are. As a consequence, they investigated ten psychological needs from well-known theories of psychological need fulfillment (such as Deci and Ryan's self-determination theory [46], Epstein's cognitive-experiential self-theory [57]) regarding their relationship to positive life events. They found that *Self-esteem*, *Autonomy*, *Relatedness* and *Competence* are the most salient needs in the context of satisfying life events. Their results were shown to be stable over time and across cultures.

As described before, Hassenzahl [83] took up the needs suggested by Sheldon et al. [175] and related them to a model of user experience. Thereby, psychological needs are used to describe classes of experiences [83]. This is done by considering different types of goals that underlie an action; *do-goals* and *be-goals* are differentiated [83]. Do-goals are derived from higher-level be-goals that are the fulfillment of an underlying need. A user, for instance, makes a phone call to experience the feeling of being close to others. Thus, the be-goal is feeling close to others (i.e. the fulfillment of the need *Relatedness*). The do-goal is the action of making the call (example taken from [83]). The fulfillment of psychological needs (the be-goal) leads to a positive user experience [85].

In the context of user experience research, Hassenzahl et al. [85] also showed that the main motivation to use an interactive technology is the fulfillment of psychological needs; a positive user experience is thus the result of need fulfillment [85].

While psychological needs serve to describe motivational aspects and thus allow for making interpretations of users' behavior, they can also serve as an inspiration for product design [68, 83]. Studies show that need fulfillment can be manipulated through product features leading to a positive change in user experience evaluations [68, 177]. Also, users' judgement of a system's hedonic quality, i.e. quality aspects beyond the functional, is positively influenced by need fulfillment [83]: the higher need fulfillment, the higher are hedonic quality

2 This subsection has been previously published in "Exploring Psychological Need Fulfillment for Security and Privacy Actions on Smartphones.", by Lydia Kraus, Ina Wechsung, and Sebastian Möller [121], which appeared in the Proceedings of EuroUSEC, Darmstadt, 18 July 2016. © Internet Society. http://dx.doi.org/10.14722/eurousec.2016.23009

ratings. However, this depends on the attribution, i.e. the degree to which users deem the product responsible for the experience [83].

Part of this thesis investigates the influence of psychological needs as motivators to use security and privacy mechanisms (cf. Chapter 6). Therefor, the psychological needs defined in Sheldon et al. are used [175]. The usefulness of this set of needs in the context of HCI has previously been shown by Hassenzahl et al. [85]. Fronemann and Peissner [68] also build upon a set of psychological needs defined by Sheldon et al. [175] and Reiss [163]. An additional need they define, which is not covered by the definitions of Sheldon et al. [175], is *Keeping the meaningful* [68]. This need was also included into the present studies. In the following, definitions of the psychological needs which were used in the present thesis are provided [175, p. 339]:

Autonomy (AUT): *"Feeling like you are the cause of your own actions rather than feeling that external forces or pressures are the cause of your actions."*
Competence (COMP): *"Feeling that you are very capable and effective in your actions rather than feeling incompetent or ineffective."*
Relatedness (REL): *"Feeling that you have regular intimate contact with people who care about you rather than feeling lonely and uncared for."*
Self-actualization (SEL): *"Feeling that you are developing your best potentials and making life meaningful rather than feeling stagnant and that life does not have much meaning."*
Security (SEC): *"Feeling safe and in control of your life rather than feeling uncertain and threatened by your circumstances."*
Popularity (POP): *"Feeling that you are liked, respected, and have influence over others rather than feeling like a person whose advice or opinions nobody is interested in."*
Money/Luxury (MON): *"Feeling that you have plenty of money to buy most of what you want rather than feeling like a poor person who has no nice possessions."*
Physical/Bodily (BOD): *"Feeling that your body is healthy and well-taken care of rather than feeling out of shape or unhealthy."*
Self-Esteem (SE): *"Feeling that you are a worthy person who is as good as anyone else rather than feeling like a 'loser'."*
Stimulation (STIM): *"Feeling that you get plenty of enjoyment and pleasure rather than feeling bored and understimulated by life."*
Keeping the meaningful (KTM): *"Collecting meaningful things"* [68]/ *"saving"* [163]

2.2.2 *System: pragmatic and hedonic quality*

In the preceding sections, user-related dimensions of UX were discussed. In the present section, system-related UX dimensions are detailed.

Usability and Pragmatic Quality

Since the early days of HCI research, the usability of systems and computers has been a main concern; ISO 9241-11 defines usability as "the extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use" [178]. Effectiveness and efficiency can be measured both with performance measures such as success rates and completion times of given tasks. However, both factors can be also measured with subjective measures such as questionnaires that determine the perceived usability (cf. e.g. to the System Usability Scale (SUS) by Brooke [27]). User satisfaction can only be measured with subjective measures.

In daily language use, usability is often confused with user experience [10, 82]. However, especially the academic UX research community stresses that usability contributes to UX, but that UX is more than usability (cf. e.g. [9, 10, 145, 165]). Thus, performance related usability measures are not good UX measures as they do not take into account the subjective nature of experience [165, 194, 197].

Hassenzahl differentiates between pragmatic and hedonic product qualities [81]. Pragmatic quality is related to usability and utility: a product with high pragmatic quality helps users in achieving *behavioral goals* [81, p. 35]. A behavioral goal could be, for instance, to type a message on a keyboard. If the keyboard enables users to easily type the message (i.e. to achieve their behavioral goal), it is likely to be perceived as highly pragmatic.

So far, the question of how pragmatic qualities (including usability) contribute to user experience remains open [48, 87]. It seems, at least, that a certain level of usability is necessary for positive user experience [132].

Hedonic quality

Hedonic quality is a concept which evolved from consumer research and which describes positive aspects of product perception [48]. It is related to aspects beyond the functional, i.e. product characteristics that address the fulfillment of be-goals [83].

In terms of emotional impact one could say that pragmatic quality rather relates to the capability of a product to achieve satisfaction (by fulfilling expectations), whereas hedonic quality rather relates to the capability of a product to achieve pleasure and psychological well-being (by exceeding expectations) [81].

A widely used and validated tool to measure pragmatic and hedonic quality is AttrakDiff2 [48]. In this thesis, the AttrakDiff2 mini questionnaire – a short version of AttrakDiff2 – was mainly used [86]. AttrakDiff2 mini measures product quality with 10 items on three dimensions: Pragmatic Quality, Hedonic Quality, and Attractiveness

(ATT). Thereby, attractiveness is related to the overall judgment of a product [47]. Each of the three dimensions is measured on a semantic-differential with 7 rating levels between differentials. Pragmatic quality is described by adjectives such as *structured–confusing*, *predictable–unpredictable*, whereas hedonic quality is described by adjectives such as *dull–captivating* or *tacky–stylish* [86]. In AttrakDiff2 mini, the hedonic quality scale is further divided into the subscales *Stimulation* and *Identity*. Stimulation refers to a products' capability to provide stimulating experiences (e.g. in terms of providing *new impressions, opportunities, insights*), whereas identity refers to a products' capability to communicate identity, thus to be seen by *relevant others in a specific way* [81, p. 35]. *Stimulation* is also reflected in the definitions of the psychological needs. *Identity* cannot directly be found in the definitions of psychological needs; however, the desire to be respected by others is covered in the need for *Popularity*.

According to Hassenzahl [81] and Diefenbach and Hassenzahl [47], a product is perceived as *desired* if it is of high pragmatic and high hedonic quality. On the contrary, a product which is of low pragmatic and low hedonic quality is perceived as *unwanted*. The question of how to address hedonic quality aspects in product design has been already raised a decade ago [87], but "insights on concrete strategies or design decisions to create hedonic quality are still limited" [48, p. 310]. Psychological needs have been suggested as enablers of positive experience [48, 82, 83, 85], but the need-based approach has also not yet been sufficiently elaborated in terms of design guidelines [48].

Consequently, the present thesis further investigates experiential perspectives on mobile security and privacy mechanisms and explores in several use cases whether it is possible to include aspects of hedonic quality in the user interface design of security and privacy mechanisms.

2.2.3 *Context: time and situatedness*

The third dimension of user experience concerns the context in which an interaction takes place. As mentioned before, UX researchers have often emphasized the dynamic and situated nature of UX (cf. e.g. [83, 87, 133, 145, 165, 194]). In the present thesis, I summarize temporal and situational aspects under the umbrella of "context".

Time

User experience is time-dependent. Within the introduced experience frameworks, this is reflected by the spatio-temporal thread in McCarthy and Wright's framework and the notion that an experience is dynamic in Hassenzahl's framework. For example, a mobile phone that is perceived as beautiful in the beginning may loose its capability to enchant as soon as the user has owned it for some time [83].

Thus, aspects of hedonic quality (stimulation) may deteriorate over time [109, 204]. In other cases, product attachment in terms of hedonic quality (identification) may increase over time [109]. Karapanos et al. [109] suggest three phases of temporal UX development: (I) *orientation*, (II) *incorporation*, and (III) *identification*: Phase I is determined by efforts to get familiar with a product, whereas in Phase II, the user starts to integrate a product and its functionality into daily life. Phase III finally describes the phase in which the user develops an emotional attachment to the product.

Roto et al. suggest to distinguish between four temporal categories of UX: *anticipated UX*, *momentary UX*, *episodic UX*, and *cumulative UX* [165]. Anticipated UX happens before usage; the user imagines how it would feel like to use the product. Momentary UX describes single experiential "snapshots" (e.g. seconds or minutes) during an interaction [194, p. 524]. Episodic UX connects pieces of momentary UX in retrospect, for example, a specific encounter with the product. Thereby, one should bear in mind that retrospective UX evaluations are influenced by biases of human cognition (cf. e.g. [83, 107]). Cumulative UX includes several interactions with the system over a longer time span (e.g. weeks or moths). Vermeeren et al. further distinguish between two kinds of episodic UX, i.e. single task-oriented episodes and "typical test sessions" including several tasks [194, p. 524].

As the majority of studies [9], the present thesis mostly evaluates UX during and/or after usage.

Situatedness

UX changes over time, but it also is dependent on situations. In one situation a user may walk while using a smartphone, whereas in another situation a user may sit during usage. This situatedness then influences the user experience, even though the same activity is pursued. For example, entering a long password with letters, numbers, and special characters while walking might be perceived as more annoying than entering it while sitting. Or, a lab study setting is different from a field study setting. While a lab study setting usually contains controlled tasks, a field study may allow for open usage situations [9]. Or, in one situation, a security-savvy user may click on a malicious link in a phishing e-mail because s/he is inattentive while in another situtation s/he would notice that there is something wrong with the e-mail.

2.2.4 *Methods for evaluating user experience*

There exist a variety of empirical qualitative and quantitative methods to investigate UX in general and its specific sub-dimensions. Whereas qualitative research is concerned with the "interpretation of

verbal material" [23, p. 296] or of other non-numerical symbolization, quantitative research quantifies the observed reality [23].

Examples of qualitative (data-collection) methods used in UX research are semi-structured or open interviews, participant/user observation, focus groups, and video recording [9]; quantitative methods in UX include, for instance, questionnaires or psychophysiological measures [9]. Data collection methods may have two goals: to inspire the design of new systems ("inspirational or generative methods") and/or to evaluate the user experience with existing systems [194, p. 522]. The latter is referred to as "evaluation methods". Besides the question of what needs to be evaluated, it also needs to be considered when UX is evaluated, as described in the preceding paragraphs: before, during, or after usage? Or accumulated over time?

In a survey, Vermeeren et al. found 96 distinct UX evaluation methods and analyzed their scope, weaknesses and strengths [194]. Four of those methods (plus additional methods) were deployed in the present thesis: these methods will be explained in the following.

Qualitative methods

In the present thesis, qualitative methods (interviews and focus groups) were used to explore UX-related aspects of interaction with security and privacy mechanisms.

Semi-structured interviews are a qualitative research method that allows for direct interaction with participants and the possibility for immediate follow up [143]. A weakness of the method is, however, that the interviewer may influence the data collection [2, 143] and the data is dependent on participants' cooperation and openess [143].

Focus groups allow to collect much data in a short time and immediate follow up and clarification [143]. Their drawback is however, that participants may influence each other.

Quantitative methods

As a measure for affect, a German translation [47, 126] of the Positive Affect – Negative Affect Schedule (PANAS), [196] was used in several studies. PANAS consists of 20 items on two scales (i.e. positive affect and negative affect), each encompassing a list of ten adjectives describing affective states (e.g. "enthusiastic", "excited", "active", "strong", "scared", "distressed", "guilty") [196]. Those adjectives are rated on a 5-point scale from 1 (= *not at all*) to 5 (= *extremely*). Valence ratings are determined by subtracting the mean of the negative affect scale from the mean of the positive affect scale.

As described in the *System* Section of this chapter (Section 2.2.2), AttrakDiff2 mini was used to evaluate pragmatic and hedonic quality of a mechanism, as well as its attractiveness. While the AttrakDiff

(and its successors AttrakDiff 2 and AttrakDiff 2 mini) is a widely used and validated questionnaire, it faces the limitation that hedonic quality can be determined only in terms of stimulation and identity [48]. To account for the limitations of the AttrakDiff2 mini, hedonic aspects are often complemented – in the studies that are presented in this thesis – with the psychological need fulfillment questionnaire.

As a measure for psychological need fulfillment, a German translation [47] of the questionnaire deployed in Sheldon et al. [175] is used. Ten psychological needs from well-known theories of psychological need fulfillment are included in the questionnaire. The questionnaire consists of 30 items (3 per need) introduced by the sentence "During this event I felt..." [175, p. 328]. Each item is answered on a scale from 1 (= not at all) to 5 (= very much). Furthermore, the items for *Keeping the meaningful* of the UNEEQ questionnaire were used [190], as described in the work by Fronemann and Peissner [68].

Mixed methods

A mixed empirical method that was deployed in this thesis is the time-triggered experience sampling method (ESM) [3, 90]. In this method, participants are prompted during a certain time of the day to report on their experiences. Reporting thereby can be done in a qualitative, quantitative, or mixed manner [3]. While an advantage of this method is that data can be collected during daily use, a drawback of experience sampling is that the reporting triggers may disturb participants or interrupt their experience [3, 128].

2.3 SUMMARY

This chapter has introduced the core idea of user experience by the help of two frameworks from the literature. Whereas McCarthy and Wright's framework focuses on the description of UX, Hassenzahl provides a framework for the experiential design of interactive products. The remainder of this thesis builds mainly upon Hassenzahl's framework due to its connection between experience and product.

UX emerges along three main dimensions: user, system, and context [165]. This thesis considers the user's point of view in terms of affect, emotion, and feelings, as well as psychological need fulfillment. The experiential qualities of a system will be determined in this thesis according to Hassenzahl's hedonic/pragmatic model [81]. According to this model, pragmatic aspects relate to usability and hedonic aspects relate to non-functional product qualities that address issues of personal relevance to the user.

UX is more than usability, but usability is a part of UX. Thus, pure usability evaluations (especially performance-related usability measures) are not suitable to determine UX as they do not reflect subjective experiences [165, 197].

So far, empirical studies on UX are rather focused on interactive products such as products related to art, mobile phones, TV, and websites in the context of leisure [9]. In the course of this thesis, I will consider mobile security and privacy mechanisms according to the dimensions from UX research to gain a deeper understanding of end-user matters with mobile security and privacy mechanisms.

Applying UX approaches to the domain of security and privacy is different from "traditional" UX research. Whereas "traditional" UX research puts the user as actor into the foreground, in security and privacy research two types of actors are involved: the user and the attacker [51]. This fact introduces complexity to the evaluation of security and privacy mechanisms, as such mechanisms need to be tested under a threat model [69]. A threat model can be considered as the context in which a security and privacy mechanisms has been tested. As a system cannot be secured against everything [69], a threat model can be considered as the context in which a security and privacy mechanism has been tested as it defines, for example, different threats and attack situations.

In the following chapter, I detail those mobile security and privacy mechanisms that a user is likely to encounter during smartphone usage, together with their threat models – in general and for two specific use cases (app permissions and screen unlocking).

3

MOBILE SECURITY AND PRIVACY MECHANISMS

In comparison to traditional mobile phones ("feature phones"), smartphones are full-fledged computers that offer a variety of features, among them the ability to place phone calls. The present thesis focuses especially on the user group of consumers which will be referred to as "users" in the remainder of this thesis. While the increase in functionality brought numerous advantages for users, it also increased the vulnerability to security and privacy attacks. Therefore, smartphone security and privacy mechanisms have received increased attention in the research community during the last decade.

The present chapter is introduced by an overview of security and privacy mechanisms a user may encounter during a typical usage session of the device (Section 3.1)[1]. Covering all available mechanisms of smartphone security and privacy, especially those that are rather on a technical level and not noticeable by users, is out of the scope of this thesis. Therefore, two mechanisms – screen locks and application (app) permissions – will serve as use cases later on in this thesis to investigate users' experiences with specific mechanisms.

The reasons for selecting these two use cases are manifold. First, both mechanisms are frequently encountered by users. Earlier studies showed that users unlock their phone about 50 times per day on average [78] which would result in 50 uses of authentication only for unlocking, given that those users use a screen lock with authentication. Another work estimated that users download on average five apps per month [35] which would result in five encounters with permission requests at install-time per month, and multiple times more for runtime permissions. As such, the above mentioned mechanisms are more frequently used than other mechanisms and they are characteristic of smartphone usage. For example, a device encryption password only needs to be entered when the device is booted. Other use cases such as the communication over the internet with the help of secure communication protocols are integrated into applications, in this case into the browser. Although users may be confronted in the latter scenario with browser certificate warnings, this use case is not unique to smartphones as the same issues occur with all kinds of devices that deploy browser-based internet communication. A detailed description of mechanisms that users may encounter during a typical usage session is provided in the following section.

1 Text fragments of the present chapter have been previously published in Kraus, Wechsung, and Möller (2016) [121], Kraus, Wechsung, and Möller (2014) [120], Kraus, Schmidt, Walch, Schaub and Möller (2017) [125], and Kraus, Antons, Kaiser, and Möller (2016) [124].

Second, both mechanisms address different kind of threats related to smartphone usage. Surveys show that the threats that motivate the usage of these two mechanisms are a pressing concern for users (cf. e.g. [24, 32, 59, 100]).

Third, both mechanisms require special attention by the user in order to be performed correctly. As such their effectiveness is influenced by user behavior. As a consequence, user behavior with this kind of mechanisms needs to be studied to determine their effectiveness. Both mechanisms also present obstacles that keep users from pursuing their primary task, that is, using their smartphones in general and using apps on their smartphones. As such they influence the overall user experience when using a smartphone. A detailed description of the two use cases is provided in Section 3.2 and 3.3, respectively.

3.1 SECURITY AND PRIVACY IN A TYPICAL USAGE SESSION

This section describes the security and privacy mechanisms of the major mobile platforms (Android and iOS) that a user may encounter during a typical usage session. As of the second quarter of 2016, the end-user market of smartphones is dominated by two operating systems (OSes): Android (86.2% market share) and iOS (12.9% market share) [179]. Android is an open-source OS for mobile platforms developed by Google Inc. iOS is a proprietary OS used in mobile platforms by Apple Inc.

3.1.1 *Device security*

A user who owns a smartphone may start a typical usage session by switching the device on. A bootloader starts the device hardware and subsequently the operating system [56]. Already during booting, a number of security operations can take place. For example, a "secure boot chain" (as it is called in iOS [97, p. 5]) or a "verified boot" process (as it is called in Android [56, p. 254]) can ensure that the device has not undergone unauthorized modifications. If the device encounters a security problem during the booting process, a notification may be shown to the user. For example, in iOS, the user is prompted to connect the device with iTunes [97], Apple's app distribution marketplace.

Device encryption is a mean to protect the device from unauthorized use and the data on the device from unauthorized access [93, 174]. If the device encryption is enabled, the user needs to enter a password or Personal Identification Number (PIN) during booting [158]. For iOS, device encryption is enabled by default and cannot be turned off by the user [97]. For Android 5.0 and above, device encryption is also automatically enabled [158]; for older versions of

Android, disk encryption had to be enabled by the user or a device policy [56].

Assuming that the device has booted without security problems and the password for decryption has been entered, the user can now access the User Interface (UI). The UI may be further secured against unauthorized access by employing a screen lock mechanism that requires authentication [93, 174]. Again, the loaded data may be further protected by data encryption as device/disk encryption protects the data on the device only when the device is turned off [56].

3.1.2 *App security*

An essential characteristic of smartphones is their ability to run apps. A user who accesses the UI of a smartphone for the first time, can already find a number of preinstalled apps. Those can include, for example, apps to place phone calls, to read and write SMS, calendar apps, and alarm clocks. While those functionalities could be also found on most feature phones, smartphones further allow users to install apps developed by third parties. It is thus crucial to provide app security and privacy features such as security and privacy mechanisms *on* the device and mechanisms that already prevent the distribution of malicious third party apps.

A smartphone is equipped with a variety of sensors such as camera, connectivity sensors (e.g. Wi-Fi or bluetooth), accelerometer, and gyroscope. Moreover, users may store sensitive data on their device such as photos, chat conversations, e-mails, notes, and the like. The sensors provide attack vectors which may be used for security attacks or privacy intrusions, e.g. by accessing sensitive user data or by collecting information about users' habits and behavior.

To restrict app access to sensitive services and data, applications are sandboxed. This means that each application is given its own data directory and can only access its own files [56, 97]. Moreover, each application runs in a separate process [56]. If an application wants to access other files or services on the device, it needs to ask for permission [56, 97]. The most sensitive permissions need to be granted by the user at runtime. Either every time (Android [186]; if not already granted) or the first time (iOS) an app accesses a sensitive system resource, the user is shown a permission dialog where the asked permission can be either granted or denied.

When it comes to third party app distribution, Android and iOS both have official marketplaces – Google Play for Android and iTunes for iOS. "Google Play is a collection of services that allow users to discover, install, and purchase applications from their Android device or the web" [159]. Google play provides security services such as automatic security scanning ("Bouncer") [71] and an expert review process [41]. Furthermore, for Android, apk files (the file format in

which apps are provided for installation) are signed by the developer in order to ensure that updates come from the same developer ("same origin policy") [56, p. 16]. Third party application for iOS undergo a review process before they are being published [97]. Also, it is ensured that each app comes from a known source as each app needs to be signed by an Apple-issued certificate [97]. iOS app developers need to be part of the developer program where their identity is checked before registration [97].

Although, both official marketplaces review apps, it might happen that malicious apps (i.e. apps that are unwanted and/or have the ability to harm the device and/or performs unwanted actions) enter the marketplace [49, 113]. Most malicious apps are developed to target Android devices [113]. Whereas the App Store is the only marketplace for iOS users, Android users can also download and install apps from other sources. Therefore, Android users need to be especially careful when installing apps from unknown sources [93]. Keeping the device up-to-date is another mitigation strategy against malware. However, in a case study on update installation behavior, many users of an Android app did not immediately install updates - a behavior which may result in security vulnerabilities [146].

3.1.3 *Network security*

Due to the inherent characteristic of smartphones of being a communication device, there are numerous usage and attack scenarios that include network communication. For example, data that is sent over the Internet might be intercepted or eavesdropped by attackers [174] or users may connect to malicious networks with spoofed network names [93]. To counteract the former, secure communication protocols should be implemented. Both, iOS and Android, provide standard secure communication protocols such as transport layer security (TLS) [56, 97]. Furthermore, both platforms support virtual private network (VPN) connections [56, 97]. Instant messaging apps have become a very popular mean for users to communicate. Thereby, communication surveillance attacks may be a concern. Full end-to-end encryption mitigates even surveillance attacks from a service provider [93, 174]. Only recently, Whatsapp, one of the most popular instant messaging services for Smartphones, has introduced end-to-end encryption which is activated by default [201]. However, the usage of instant messaging services is not only accompanied by the risk of being eavesdropped, but also by the risk of privacy intrusions by other users. The latter can be counteracted by appropriate privacy settings which should be provided within the app.

To mitigate the risk of connecting to a malicious network with spoofed network name, users should exercise caution on which network to connect and disable automatic connections [93]. Threats may

also arise from the device being unavailable due to involvement in denial of service attacks or exhausted battery power [174]. For counteracting the former, a resource management solution may be installed; these kind of applications are, however, difficult to implement [174].

3.1.4 *Security in case of theft or loss*

The last scenario which is considered in the present chapter – smartphone loss or theft – is not part of a typical usage situation; it may be rather part of a smartphone ownership lifecycle. Besides unauthorized access, another negative consequence of device loss or theft is data loss. Data loss can be easily mitigated by regular backups [93]. Backup services to the cloud may be provided for example by OS providers or by third party apps.

Furthermore, remote management solutions such as remote wipe or a device locator can support the users in finding the phone in case of loss or theft and they can ensure that the data is being made unavailable to attackers [93, 150, 174]. As of 2012, 41% of smartphone users in the US are estimated to back-up their data [24].

3.2 USE CASE I: SCREEN LOCKS WITH AUTHENTICATION

As soon as a smartphone is lost or stolen, the device is vulnerable to unauthorized access. Loss or theft are realistic scenarios which have a medium to high probability to occur: while Hogben and Dekker, based on a UK-based survey, estimated the risk of a device being lost or stolen as medium [93], a survey from 2012 among US smartphone users estimated that almost a third of smartphone users have had their smartphone lost or stolen [24].

Unauthorized access to the device is not only a problem when the device is lost or stolen. Users also show concern regarding unauthorized access attacks by so called "insiders", i.e. people they know such as friends or coworkers [149]. As of 2012, 12% of users report to have experienced privacy intrusions by someone else accessing the phone [24, 149]. However, the real number of unauthorized accesses is likely to be much higher, as there may be many cases in which users are not aware that someone accessed their device. For example, 31% of the participants in a large-scale online survey reported to have accessed the smartphone of someone else without the permission of the owner [142].

A smartphone can be protected from unauthorized access and subsequent privacy intrusions or security issues, by deploying a screen lock together with an authentication method. Ideally, the data on the smartphone is thereby encrypted [93].

There are three kinds of authentication: knowledge-based, object-based, and ID-authentication (also sometimes referred to as knowledge-

based, token-based, and biometric authentication) [153]. Knowledge-based authentication is based on something a user knows, e.g. a password or a secret [153]. Passwords may contain letters, numbers, or special characters (alphanumerical passwords), numbers only (PINs), or images and drawings (graphical passwords). Object-based authentication is based on something a user has, e.g. a token such as a (physical) key [153]. Biometric authentication relies on something a user "is", i.e. something that is unique to a user [153]. Biometric authentication methods on smartphones have recently emerged as a viable alternative to knowledge-based authentication methods. Examples of biometric methods include fingerprint recognition such as Touch ID on iOS [97] or face recognition such as face unlock on Android devices [56].

3.2.1 *Knowledge-based authentication*

Usability

The usability of knowledge-based authentication methods can be determined by the efficiency and effectiveness with which the password can be entered, as well as the memorability of the password [171]. Efficiency and effectiveness can be determined with performance measures: entry time and success rates, respectively.

Security

The security of knowledge-based authentication methods depends on two factors: the susceptibility of the system to guessing attacks and to capture attacks [17]. Thereby, guessing attacks refer to attacks where an attacker tries to "guess" a password. This can be done, for example, by conducting an exhaustive search through the entire password space ("brute-force") or by deploying a dictionary with popular passwords [17].

Guessing attacks can be further divided into online or offline attacks [65]: In an online attack, the attacker uses the login screen to enter the password guesses. Rate-limiting can be used on smartphones, to defend against online brute-force attacks [56]. Thereby, each login attempt that occurs after a certain number of incorrect login attempts is delayed by a certain time interval. For example, if a password is entered incorrectly five times in a row, the next login trial could be delayed by 30 seconds [56]. This increases the attacker's cost in terms of time to obtain the password. Fore example, in iOS, the rate limit is designed in such a way, that an attacker would need more than 5 years to try all possible password combinations for a six-character alphanumeric password [97].

The susceptibility to guessing attacks depends on the theoretical and practical password space. The theoretical password space is the

number of all passwords which can be theoretically generated from the password alphabet [171]. Thereby, all passwords are assumed to have the same probability to occur. For example, the theoretical password spaces of a four- and six-digit PINs are $10^4 = 10,000$ and $10^6 = 1,000,000$, respectively, whereas the theoretical password space of a purely text-based four-character password is $26^4 = 456,976$. As can be seen from these calculations, four-digit PINs have a rather small theoretical password space.

The practical password space is a subset of the theoretical password space. It refers to the password space resulting from the actual probability distribution of all possible passwords which is – due to predictable user choice - not equally distributed [171][42].

Capture attacks refer to attacks where a password is obtained, for example by observing the user when entering the password or by intercepting the password when it is entered to the system [17]. Passwords can be captured for example by directly observing the password entry ("shoulder surfing"), by deceiving the user in order to bring him or her to reveal the password (e.g. by phishing), or by malware which may be installed on the device [17].

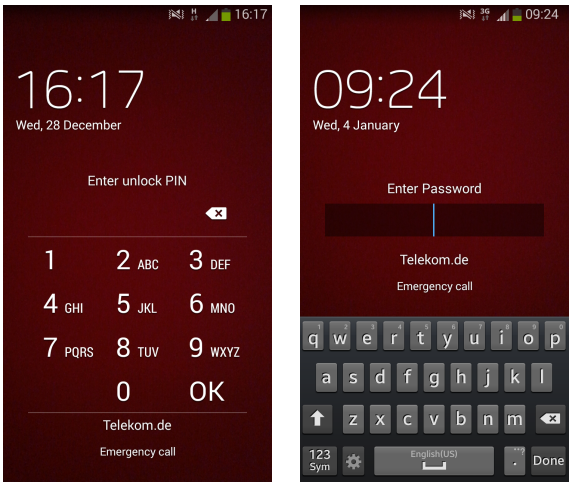
To defend against an attacker who succeeds in obtaining the *stored* password, the password should be stored in encrypted form. This could be done by applying a hash function together with a random generated bit sequence ("salt") [56].

This defense causes additional costs for the attacker as s/he needs to mount another guessing attack to decrypt the password ("offline guessing attack") [65]. In contrast to online guessing attacks, in an offline attack, the attacker has access to the hashed and salted password. However, only if the attacker has access to the cryptographic algorithms that generated the hash and to the salt value, s/he can start to calculate salted hash values for the passwords in the theoretical password space and compare them to the obtained, salted and hashed, password.

3.2.2 *Example 1: Passwords and PINs*

The most common options for knowledge-based authentication on smartphones are PINs and passwords, as well as graphical passwords (the only graphical method that is widely adopted is the Android unlock pattern). All three methods have been widely studied and are detailed in the following sections.

Users have a variety of reasons to use PIN unlocks. Egelmann et al. found privacy considerations, the intention to prevent strangers from accessing the device, bad experiences in the past, and social influence as reasons to use a screen lock with authentication [54]. Furthermore, default smartphone setup procedures such as the prompting towards a screen lock during setup may encourage users to deploy such a



(a) (b)

Figure 3: Screenshot of a PIN screen lock (left) and a password screen lock (right), both on Android.

mechanism [54]. Harbach et al. found that an important reason which keeps users from using a locking mechanism is inconvenience [80].

A PIN or password UI usually consists of two elements: the entry field and the keyboard. The keyboard usually contains the allowed characters, a backspace button to correct errors or slips, and an enter button to confirm the password (cf. Figure 3). The backspace button may be also placed next to the entry field. An advantage of passwords and PINs is their easy deployability and portability between different platforms, as well as the fact that most users are already familiar with the concept [17].

Usability

PIN locks have a short entry time which depends on the PIN length [171], e.g. around 1.5 sec [195] to 4.7 sec [78] in the field. The entry time depends also on the measuring method which may either start when the PIN screen is shown to the user or when the first digit is entered, and finished when the whole PIN is entered correctly. Success rates for PIN entry are usually high, both, in the lab [171] and in the field [195].

The entry time of passwords also depends on the password length and the available keyboard [170], as well as on the measuring method of the entry time. Password entry time for virtual keyboards is rather high – around 20 sec for seven- to nine-digit passwords [170].

Regarding memorability, passwords and PINs face the problem that random passwords are more secure but harder to remember [207]. PINs generated under a security policy are more secure, but also harder to remember than freely-chosen PINs [115].

Security

PIN and passwords are both susceptible to online guessing attacks. As described above, four-digit PINs have a rather small theoretical password space ($10^4 = 10.000$) compared to alphanumerical passwords for which the password alphabet is much higher (at least 36 characters if letters and numbers are included). The practical password space of PINs is even smaller, as users tend to weaken the security of PINs by choosing combinations like birth dates which are easy to remember, but also easy to guess by an attacker [22]. The practical password space of alphanumerical passwords is also smaller than the theoretical password space, as many users also prefer common words or predictable sequences as passwords [65].

Regarding the susceptibility to offline guessing attacks, Elenkov notes in his book on Android security that for PINs, "generating a targeted hash table for a particular device (assuming the salt value is also available) is still relatively cheap" [56, p. 275].

For casual attackers, the shoulder surfing susceptibility of PIN and password UIs on smartphones depends on the PIN/password length and different UI design features such as the keyboard design [170]. For example, the Symbian-T9 keyboard has been found to be less susceptible to shoulder surfing than the Android-Sense and the Android-Swype keyboards [170]. Regarding password entry, the magnification of keyboard buttons when being pressed was linked to higher shoulder-surfing susceptibility and attackers who focused on the entry field had a higher success rate [170].

In another study, Schaub et al. found that the susceptibility to shoulder surfing of short PINs (14 bit theoretical password space) is rather low, whereas for long PINs (42 bit theoretical password space) it is rather high [171].

Theoretically, the shoulder surfing susceptibility of short PINs seems to be rather low. Thus, one could assume that shoulder surfing presents a non-neglible risk for smartphone users. However, in a field study on smartphone unlocking, Harbach et al. found that 83% of the participants did not perceive shoulder surfing as a threat; furthermore, participants rated shoulder surfing only in a minority of usage situations (<1%) as being possible and possibly leading to severe or very severe consequences [78]. They also found that in usage situations where shoulder surfing was possible, threats arose rather from known people than from unknown people [78].

User experience

There is not much related work on the user experience (in terms of subjective measures) with passwords and PINs on smartphones. One example is the work by von Zezschwitz et al. [195] who found in a field study on PIN and pattern usage that 75% of the participants felt

good using a PIN and 83% of the participants reported to like the PIN UI. Another field study by Harbach et al. yields similar results with most of the participants indicating being happy with their unlocking method (either PIN, pattern, or unlock without authentication), without a difference in the annoyance ratings between the methods [78]. A general drawback of knowledge-based authentication methods on smartphones is, however, that, accumulated over days and months, their deployment consumes much time [78].

While little is known about the user experience with passwords and PINs on smartphones, several studies have evaluated user experiences with passwords in general. Dunphy et al. [52] provide an illustrative example of how self-reported user experiences can enable researchers to gain broad insights into complex password handling practices: through the qualitative analysis of password experiences expressed in micro blogs (tweets), they find, for example, that passwords can serve as "social currency" with which people define relationships and their degree of closeness to others [52]. Other papers used qualitative studies and diary studies to investigate users' coping strategies for managing a high number of passwords (e.g. [182]), password use in the wild and in daily life (e.g. [88, 99]), password policy handling (e.g. [98]), and password sharing between users (e.g. [111]).

In terms of subjective measures, researchers also showed to be interested in the feelings during password creation such as comfort [77] and sentiment in terms of annoyance and difficulty [118].

Another experiential perspective on passwords is the use of experiences to generate passwords that are easy to remember and personally meaningful: for example, Woo et al. suggest supporting password creation by asking users to assemble passwords from meaningful life experiences [205]; or, Hang et al. suggest that fallback authentication may use security questions about locations which are related to meaningful experiences (such as the location of "one's longest travel so far") [76]. In terms of security, authentication methods that rely on meaningful experiences may suffer from vulnerabilities. For instance, when including personal experiences into knowledge-based authentication, it needs to be considered that this knowledge might be also known to "attackers" from a users' social circle. The location-based questions suggested by Hang et al. [76] which are related to meaningful events showed, however, a good potential to be easy to answer and recall by a legitimate user and hard to guess by an attacker according to their study results.

3.2.3 *Graphical authentication*

Since the late 90's, another research field of knowledge-based authentication received increased attention: graphical authentication which

relies on a graphical password or secret, for example a sequence of images or a drawing [17].

The idea of using graphical information for authentication builds upon the dual coding theory: images are encoded twice in the memory (visually and verbally) rather than only verbally like alphanumeric passwords [155]. Thus, graphics are easier to remember than passwords [17].

Biddle et al. classify graphical authentication systems according to the underlying memory mechanism: recall, recognition, and cued-recall [17]: in **recall-based systems**, the user needs to memorize the components of the password as well as their order. An example for recall-based graphical systems are drawmetric systems, where the password consists of a sketch which is drawn by the user. Password-based systems also belong to the category of recall-based systems. In **recognition-based schemes** users need to recognize their password images among decoy images during the authentication challenge [17]. **Cued-recall-based schemes** support the user with visual cues to memorize the password [17].

As for PINs and passwords, major security issues of graphical passwords arise from the susceptibility to capture and guessing attacks [17]: for instance, image-based cued-recall schemes are prone to hotspots, i.e. image regions users are likely to select. This preference for image regions limits the practical password space. Graphical passwords can also take longer to enter [171, 195]. Another security limitation of graphical passwords is the necessity of some graphical authentication systems to store their passwords or parts thereof in unencrypted form [17]. This makes these systems more vulnerable to offline guessing attacks. Recognition-based and cued-recall schemes have been shown on smartphones to better balance the trade-offs between usability and security [171].

3.2.4 *Example 2: Image-based password schemes*

Research on graphical authentication has suggested the use of images [42, 89, 189] or icons [15, 16] for password creation. An example for an image-based system is Use-Your-Illusion (UYI) [89]. In this scheme, users have to recognize a blurred version of their password images among decoy images in several authentication rounds (challenges) where password images are placed on random positions. Another example is PassFaces where users are assigned a password of face images [38]. Both schemes have been shown to leverage reasonable success rates and memorability [17]. However, the login time of both schemes is much higher than for PINs [17, 171] and PassFaces are also vulnerable to user choice [42].

Another class of graphical authentication schemes which are of interest for this thesis are icon-based systems. They are a sub-class

of recognition-based systems and constitute an interesting approach for authentication. Depending on the system design, they may leverage the advantages of recognition-based graphical authentication (i.e. good trade-off between usability and security [171]) together with a short entry time [171].

Two hybrid, icon-based schemes are "Story" [42] and GPI (Graphical Passwords with Icons)/ GPIS (Graphical Passwords with Icons suggested by the system) [15]. Both schemes are hybrid as the users have to recognize their password icons first among decoy images and then recall the order of icons in their password. Bicakci et al. proposed GPI and GPIS as two icon- and click-based schemes for computer use in which users either select a password from a panel of icons (GPI) or are assigned a password randomly chosen from the panel (GPIS) [15]. The user interface for password entry showed 150 icons, which represented 15 different categories. Drawing the available icons from different categories was supposed to reduce the hotspot problem (i.e. the issue that some areas of images may be favored over others) [15]. Nevertheless, study participants still favored some icons over others making the system susceptible to guessing attacks.

In the "Story" scheme by Davis et al., users have to select a sequence of 4 images from a panel of 9 images whereas the panel images are selected from different categories such as cars and landscapes [42]. Users were furthermore asked to create a story from their images to support memorability of the password. However, many participants did not follow the recommendation to create a story for better memorability. This might be a reason that the "Story" scheme password resulted in limited success rates (only about 75% of password entries were correct) [42]. However, while memorability seems to be limited in this scheme, the probability distribution of the passwords created in the study seemed not to be skewed [42]. Both systems, Story and GPI/ GPIS, were conceived for desktop computers and not tested on smartphones, thus usability considerations beyond memorability are not discussed at this point. Furthermore, their resistance to shoulder surfing was also not tested. As a consequence, the security issues mentioned above only refer to the susceptibility to guessing attacks.

An interesting direction for positive interaction in mobile authentication is the use of Emojis as password characters. Emojis are small icons, e.g., smileys or objects, that are often used in digital communication to express emotions [154]. Emojis are largely used in positive contexts [152] and are popular among users. Thus, providing potential for offering positive user experiences. Emoji-based passwords have recently been introduced by a commercial application [101]. Golla et al. found user-chosen Emoji-based 4-digit passwords which were generated on an Emoji keyboard with 20 Emojis to be harder to guess than 4-digit user-chosen PINs [72]. While a first quantification of the

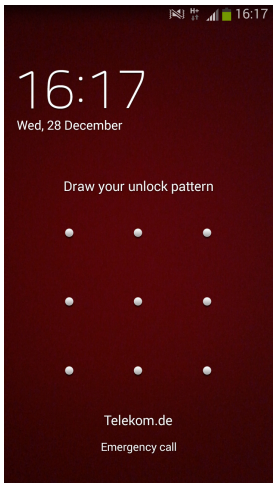


Figure 4: Screenshot of an Android unlock pattern.

guessing resistance of Emoji-based passwords has been provided by Golla et al. [72], it has not been studied how Emoji-passwords affect user experience and the degree to which an Emoji-based authentication scheme is resistant to capture attacks.

3.2.5 *Example 3: Android unlock pattern*

The Android unlock pattern is the only graphical authentication system which is currently widely deployed on smartphones. The Android unlock pattern is an example of recall-based system, based upon the idea of the DAS (draw-a-secret) system [195] [105]. The Android unlock pattern UI consists of nine dots which are place on a 3x3 grid (cf. Figure 4). Users can select a password by connecting the dots with strokes.

After choosing a starting point, the user proceeds to further points in the grid. This procedure leads to a graphical pattern presenting the password. The process of choosing points in the grid is subject to a number of rules: once a point has been visited it cannot be visited again [56] [191], single points on a straight line cannot be omitted [191], and the password has to consist of at least four points [191].

Usability

Regarding usability, Android unlock patterns showed to have a rather long entry time (approximately twice as much as PIN) in a field study [195]; in the same study, Android unlock patterns furthermore showed to have lower success rates and to be more prone to errors compared to PINs; nevertheless, they were perceived similar to PINs regarding usability and likeability by the study participants [195]. In another field study, patterns showed a shorter entry times than PINs, around 3 s [78]. Note that again, the different entry times may be

influenced by different measurement methods and the length of the pattern.

Security

When it comes to security, unlock patterns face the same issues as all knowledge-based authentication methods, i.e. the susceptibility to guessing and capture attacks. Due to their limited theoretical password space (389,112 for all possible patterns [191] or 32,768 for five-stroke patterns [195]), their susceptibility to (online) guessing attacks is higher compared to PINs selected from a nine-digit alphabet [56]. Furthermore, patterns were also found to be susceptible to user choice: for example, users prefer patterns that contain the upper left corner, and straight lines consisting of three points [191]. Letters from the Latin alphabet have been furthermore found as popular parts of patterns [140]. Demographic factors may also serve as indicators for the choice of specific patterns [140]. As patterns are stored hashed but not salted [56], they are also vulnerable to offline guessing attacks

As for PINs and alphanumeric passwords, shoulder surfing attacks are a threat to the security of patterns. Another vulnerability of patterns, is their susceptibility to smudge attacks [7] [56]. As patterns are entered on touch screen, the fingers usually leave an oily residue on areas which are often touched – those residues may be used to infer the pattern [7]. As a result of the above mentioned vulnerabilities, pattern security is considered to be rather low [56].

3.2.6 *Biometric authentication*

In comparison to knowledge-based authentication, biometric methods have the advantage that the authentication is not based on secrets that need to be memorized by users. Instead, biometric authentication is based on pattern recognition and machine learning. Examples of biometric systems that are currently featured on smartphones are fingerprint recognition [5, 74] and face recognition [73]. Also, other schemes such as touch recognition [43, 117] or gesture-based authentication have been suggested in related works [116].

Even before biometric authentication was widely available on smartphones, users expected fingerprint recognition to be both, secure and usable [176]. On contrary, methods such as iris recognition and face recognition were rather rated low in terms of willingness to adopt such methods [176]. Ideally, biometric authentication should work seamlessly without being perceived by the user. That this is not the case has been shown in a study by Bhagavatula et al. [14]. For example, facial recognition on smartphones has the limitation that it works poorly in dark lighting conditions and fingerprint recognition may not work with wet fingers [14]. Moreover, biometric authentication methods rely on knowledge-based authentication as a fallback

mechanism. From a security point of view, they further face the vulnerability of not being revocable, i.e. once a biometric feature has been compromised, it is "insecure" [153].

There exist several papers that investigate affect, emotion and felt experience during biometric authentication. Regarding currently available biometric authentication methods on smartphones, De Luca et al. [44] find that (besides good usability) also positive emotional outcomes such as fun and joy play an important role as motivators for the adoption of fingerprint-based authentication. They further find that negative emotional outcomes such as annoyance is related to the abandonment of face-recognition-based authentication on smartphones [44].

Aumi and Kratz [6] suggest a new authentication method for mobile devices based on in-air hand gestures. To authenticate, users perform gestures with their hand in front of a tablet PC which uses a short-range depth camera as input sensor. In a lab study, their authentication system has shown to be able to evoke positive emotions during interaction even for complicated, i.e. more secure, gestures [6]. Thus, they suggest that security and user experience do not necessarily need to contradict each other.

3.2.7 *Summary*

Despite their usability and security shortcomings, knowledge-based security mechanisms are unlikely to be substituted in the near future: they are still needed as fallback mechanisms for biometric methods, they are easy and cheap to deploy [17][65], and they are well-known to users [65].

Graphical authentication methods are not (yet) widely deployed on smartphones. The only graphical scheme that is provided by default on Android devices – the unlock pattern – seems to provide good usability and easy error recoverability [195], but suffers from severe security limitations [56, 191]. User-chosen PINs seem to provide a good usability and are not perceived as too annoying by users [78, 195]. An issue that remains to be solved, is however, the limited security of PINs caused by a limited theoretical password space and predictable user choices [22]. Furthermore, it would be desirable to create an attractive authentication alternative for users who refuse to use passwords or PINs. The recognition-based graphical authentication system Story shows some promise in addressing the problem of predictable user choice for passwords, though there is space for improvement regarding the memorability of these kinds of passwords [42]. Emoji-based methods would be also an option for knowledge-based mobile authentication as they may provide a positive user experience. Furthermore, user-chosen Emoji-based passwords seem to be less sus-

ceptible to guessing attacks compared to user-chosen PINs of same length [72].

Already in 2011, despite the known usability issues of screen locks, users reported being interested in applying further authentication mechanisms [12]. As of 2014, many users are using a PIN or password to protect their device: 66% of users in Germany use a screen lock with a password [100].

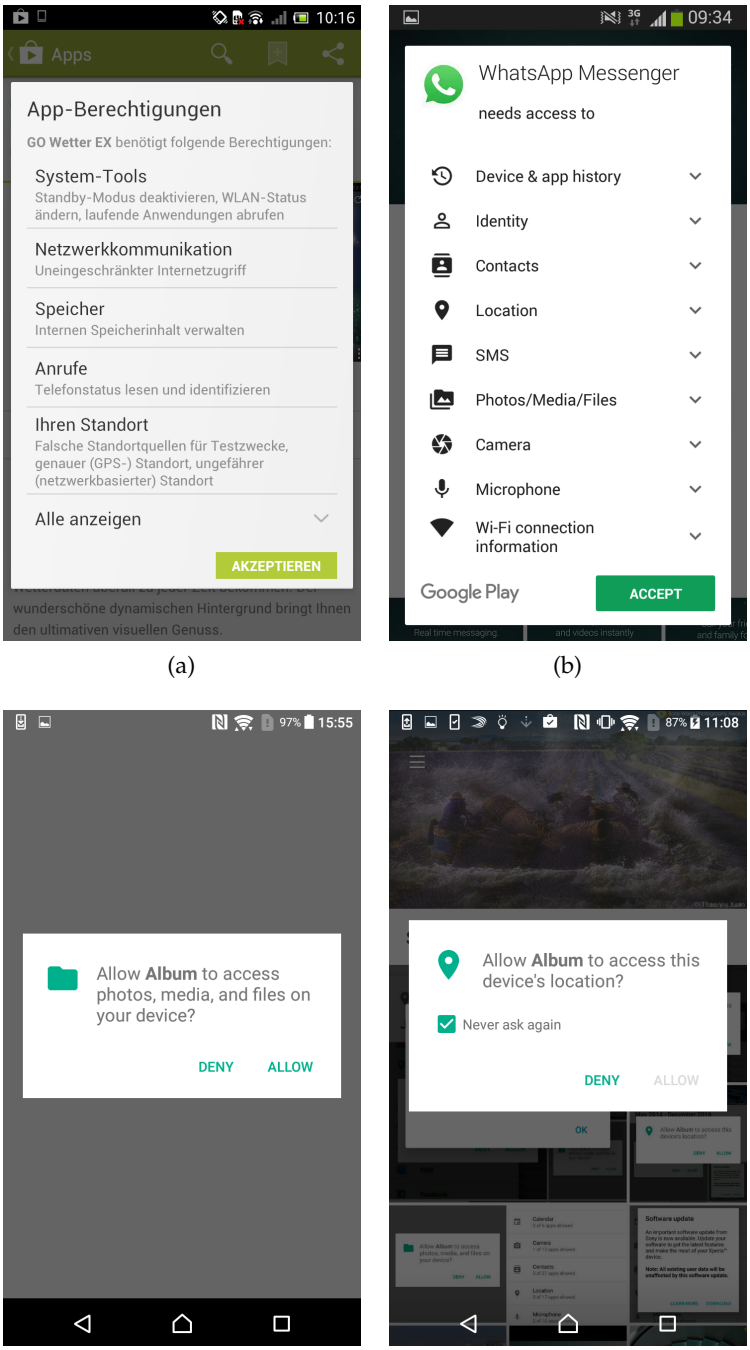
3.3 USE CASE II: APP PERMISSIONS

As described in Section 3.1.2, modern smartphone platforms rely on sandboxing to ensure application security and privacy. However, there may be apps which ask for more permissions than would be necessary to ensure their functionality [60]. Thereby, excessive usage of permissions does not necessarily mean that an app is intentionally collecting data – it can also be a consequence of a programmer's lack of understanding on how to use the different permissions [60]. In some cases it might be even easier for developers to request plenty of permissions for their apps to make sure they work correctly [11]. The risk of permission abuse and data collection is difficult to determine for users and is subject to a high degree of uncertainty.

Felt et al. surveyed more than 3,000 US-based smartphone users regarding their concerns related to 100 risks associated with permission abuse [59]. They found that users are most concerned regarding malware, especially about apps that would permanently break the phone or that would abuse permissions to enable premium calls or send premium text messages without the user's knowledge. However, also privacy related risks rank among the top 10 concerns of users, for instance the concern that apps would abuse permissions to publicly share users' e-mails or text messages. Furthermore, users are more concerned about privacy issues on their phone compared to their desktop computer [32].

Different surveys also show that users are concerned regarding the misuse of personal information by app providers. In a survey on mobile protection behavior among 154 German smartphone users, Kraus et al. found over 60% of the users to report that they have refrained from installing an app due to a high number of permissions [119]. Also, more than 70% of participants reported in this survey that they have refrained from installing an app due to unusual permissions. In a survey of among US smartphone users, more than half of the users reported that they have uninstalled an app due to privacy concerns [24].

Users can mitigate the risk of disclosing too much personal information to third party providers and subsequent privacy intrusions by scrutinizing app permissions and only granting them if they consider them to be necessary.



(a) (b)

(c) (d)

Figure 5: Android: (a) "basic permission dialog" (in German, 2013), (b) "advanced permission dialog" (2016), (c) runtime permission dialog (2016), and (d) runtime permission dialog with "never ask again" option (2016).

Felt et al. discuss the different possibilities that developers have to ask users for permission [62]. Thereby, the authors apply two guiding principles: First, they emphasize that developers need to conserve users' attention. As a consequence developers should only ask users

for permissions concerning actions that result in severe consequences [61]. Second, they emphasize that permissions should try avoiding to interrupt the users' "workflow". The second principle, is a problem which is often faced in usable security and privacy: users usually pursue a primary task (e.g. they download an app because they want to use the functionality of the app). This primary task is interrupted by security or privacy "calls for action" which are only a secondary task for users [69].

Felt et al. [62] recommend that if (1) a user's action can be undone and if (2) the consequence of granting the permission would – in the worst case – constitute only an annoyance to users, the permission should be granted automatically. If those two aspects ((1) and (2)) are not the case, developers should further ask themselves if (3) the user initiated the action and if (4) the action can be altered by the user. If either of those two alternatives ((3) and (4)) is the case, a "Trusted UI " should be deployed. Trusted UIs are embedded in an app's workflow which makes them part of the primary task [62]. Only if permissions cannot be granted automatically, and if they cannot be represented in a Trusted UI, they should be visible to the users in an disruptive dialog: this dialog can be either shown at runtime or at install-time [62], whereas both types have their pros and cons which will be discussed in the following subsections.

3.3.1 *App permissions: history and current state*

In the past, the implementation of the permission dialogs differed between different smartphone OSes: Whereas iOS users have always been shown runtime permission requests, Android users were shown an install-time permission requests prompting them to accept a list of all permissions before an app could be installed.

Android: From install-time to runtime permissions

The permission-granting process for Android users was roughly as described in the following: Whenever users viewed an app in Google Play, they were provided with information about the app including screenshots of an app, a textual description of the app, star ratings, the number of downloads, and reviews of other users. This information was prominently placed on the top of the user interface together with an "install" button. The permissions of an app were only visible in a pop-up window after the "install" button was pressed (cf. Figure 5a). The permission dialog included headings for different categories of permissions, a short description of each permission, and a drop down button which showed, when being pressed, the less severe permissions. This version of the permission dialog was approximately shown to users until the course of 2014. In the remainder of this work, this permission dialog is referred to as the "basic permission dialog".

Note that there was and is also an option to view the permissions in the Google Play before pressing the installation button. This can be done by scrolling down to the bottom of the app overview and by clicking on another button ("permission details").

In the basic permission dialog, Android permissions showed to be difficult to understand for users and only few users paid attention to the permission dialog during installation [61]. Besides these usability issues, another problem of the Android permission system was the high amount of defined permissions (approximately 134 in Android 2.2 [61]).

In 2014, the Android permissions were grouped and their presentation was modified to include icons for each group (cf. Figure 5b). Users could now view the requested permission groups together with an icon for each group during the time of installation. For each permission group there further is a drop down button that shows, when being pressed, the requested permission of this group. In the remainder of this work, this permission dialog is referred to as the "advanced permission dialog". While this modification of the permission dialog improved information presentation, security concerns remained [188]: users were now asked to accept groups of permissions. Once a permission group has been accepted, users were not asked again during updates of an app when permissions within an group had been modified [188]: This situation could enable developers to add permissions without users' consent.

Since Android version 6.0, users have the possibility to grant or deny single permissions for each app [186]. Users are asked at runtime for each permission whether they would grant the permission or not [186] (cf. Figure 5c). Furthermore, they can change the status of single permissions (enabled or disabled) within the settings. If a permission has been denied in Android, the app will ask again, when the app tries to access the related functionality [186]. However, when users are asked for the second time, they have the possibility to select the "never ask again" option (cf. Figure 5d).

In iOS, developers have the possibility to add a short explanation ("purpose string") to the runtime permission request which states the purpose for which the data is being used [184]. This option is offered in Android, too. However, in Android, developers need to show the explanation *before* the runtime permission is being asked. Adding an explanation dialog before the permission dialog may be annoying or confusing for users, as they may have the impression to agree twice to the permission [157]. Another option for Android developers is to measure whether a user continues trying to access a functionality although the related permission has been denied before [186]. In this case, also an additional explanation could be shown to explain why the permission is needed.

As of March 2016, Android 6.0 still has a negligible market share (2.3%) in Germany. Those users who own a smartphone running Android 5.x or below, still face the advanced permission dialog at install-time without the option of granting individual permissions for each app.

Types of permissions

At the time of writing, Android defines two types of permissions: normal and dangerous permissions [160]. Normal permissions can be granted without asking the user for confirmation, whereas dangerous permissions require user consent. Dangerous permissions encompass the following permission groups [160]: Calendar (read and write), Camera (access to the camera), Contacts (read and write contacts, get accounts), Location (access to fine and coarse location), Microphone (possibility for audio recording), Phone (read phone state, call, read and write call logs, add voicemail, use SIP, and process outgoing calls), Sensors (access body sensors), SMS (send and receive SMS, read SMS, receive wap push, and receive MMS), and Storage (read and write to external storage).

iOS 10 defines the following permissions [96][97]: Location, Contacts, Calendars, Reminders, Photos, Bluetooth Sharing, Microphone, Camera, Health (access to data from health and fitness apps), HomeKit (home automation), Media Library, Motion and Fitness, Twitter, and Facebook.

Usability and privacy

Regarding the usability of permission dialogs (in terms of effectiveness), users' understanding of and attention to permissions plays an important role [61]. Furthermore, the time a user needs to make a decision regarding permission requests determines their usability. For runtime permission systems, the degree of privacy that results from a permission request UI is usually described with the percentage of permission grants per app (cf. e.g. [184]). In studies on install-time permissions, users are usually provided with two apps of similar functionality which differ in the number of permissions they require. The degree of privacy that results from a permission request UI is then determined by measuring the percentage of users who decided for the app with the higher number of permissions (cf. e.g. [112]).

3.3.2 *Install-time permissions*

Users' coping with install-time permission in the basic permission dialog for Android has been a subject of several studies. Thereby, users' understanding of and attention to permissions [61] was investigated, as well as new interface designs to improve both [13, 53, 79, 91, 112].

In an online study Felt et al. found that only a minority of users (17.5%) paid attention to the basic permission dialog, and even less users understood all given permissions (2.6%) [61]. The authors concluded that the basic permission dialog cannot be used in the way it is supposed to be used, as users can only make correct decisions if they understand what is being asked.

Other researchers focused on optimizing the basic permission dialog and including the permissions in the decision-making process in order to facilitate the users' understanding of the permissions. Kelley et al. [112] provided users with additional information about permissions in the app market (before the decision is made) in the form of a privacy facts check list (a clustering of permissions in categories based on the kind of privacy sensitive information needed). They found the privacy check list to lead to decreased installation rates of high-requesting apps, whereas only providing the list of permissions within the app store did not show significant effects on users' decision making behavior.

Benton et al. [13] found that providing an additional explanatory text about the permission use did not significantly influence users' installation behavior or regret of having installed a high-requesting app. On the contrary, adding visual cues to the provided inforation had a significant effect on users' installation behavior for some experimental conditions.

Egelmann et al. [53] used a choice architecture to present apps of similar functionality and their requested permissions side-by-side, where low-requesting apps have a higher pricing than high-requesting apps. In a user study they found that when users were presented with a choice architecture, 25% of users were willing to pay a premium for privacy and to put more weight on privacy as a decision factor.

Hettig et al. [91] introduced another method for including permissions in the decision-making process by visualizing the accompanying risks with worst case examples. For example, users were presented with a satellite view of their current location, when the permission to access the fine-grained location is requested. However, worst case examples are overestimated risks which might lead to a loss of user attention as consequently all apps are considered dangerous [61]. In a later version of the prototype described by Hettig et al. [91], Harbach et al. [79] redefined the worst case examples to personal examples. Again, permissions were shown together with actual examples from the user's smartphone resource. For example, when the permission for modifying the content of SD card of the smartphone was requested, a photo from the user's gallery which is stored on the SD card is shown together with the permission. Harbach et al. [79] conducted a lab study and an online study to compare the personal examples dialog with the basic permission dialog. In the lab and in the online study, those participants who viewed the permis-

sion dialog with personal examples opted more often to not install any of the provided apps [79]. Comments gathered with the thinking aloud method during the lab study further revealed that the user interface arose negative affect for some of the participants. Furthermore, significantly more participants in the personal examples conditions reported in the online study that they were afraid that personal information would be lost.

3.3.3 *Runtime permissions*

The all-or-nothing approach of install-time permissions has been criticized in several works [69, 137, 203]. For example, Lin et al. found in a large-scale online study that users had different app privacy preferences which were related to the purpose for which the data was being used [137]. Runtime permissions address the issue of diverging privacy preferences as users are shown permission-wise requests. Furthermore, they provide users with a context for decision-making. For example, if a public transport app asks the user to share his/her location as soon as the user wants to see information about nearby bus stations, the user can use the temporal context in which the request was sent to make sense of the permission request. Andriotis et al. conducted a field study on the adoption of the permission request system in Android 6.0 [4]. They found that users actively use the feature for selective permission granting and that users seem to be satisfied with the new permission granting approach.

Moreover, runtime permissions appear to be more effective. An online and a lab study by Balebako et al. revealed that when privacy notices were shown before, during, or after app use, participants were more likely to recall information about the notice compared to when the notice was shown in the app store [8].

As for install-time permissions, if shown too often and without varying content, runtime permissions may be also subject to habituation [62]. Therefore, developers could add individual explanations why they need a certain permission. Another issue that developer-defined explanations address is the question of the purpose of data use. As mentioned above, users seem to be sensitive to which kind of permissions they grant depending on the purpose of data use.

In Android, developers are advised to provide an explanation before the permission is requested or when a permission has been declined several times by the user, but the user continues trying to access the related functionality [186]. In iOS, developers can add a purpose string to the permission request providing the user with an explanation why the permission is needed [184]. Tan et al. conducted an online study to compare user behavior and satisfaction when being confronted with runtime permission requests with and without purpose strings [184]. In a benign (i.e. non-malicious) permission re-

quest scenario, the results of their study showed significantly more permission approvals when a purpose was stated. Furthermore, there was a difference in the user satisfaction between the user interfaces: participants were more satisfied with the interface that provided a purpose string. However, purpose strings did not have an effect on users' understanding of the requested permission.

3.3.4 *Summary*

Whereas iOS always featured a runtime permission model, the Android permission system has changed from install-time permissions to run-time permissions during the last years. Both approaches have their advantages and shortcomings, with runtime permissions likely to perform better in terms of memorability of the information and the capability to address diverse privacy preferences.

The above described studies on install-time permissions provide examples on how to increase users' attention to the permission dialog and how to influence users' decision making behavior when selecting an app towards more privacy-friendly decisions. All of these studies addressed the basic permission dialog, whereas – to the best of the author's knowledge –the advanced permission dialog has not been investigated in user studies. Although Android users can now grant permissions at install-time, the undertaken research on install-time permissions provides valuable insights into the kinds of information that could be provided to users in order to make privacy-friendly decisions. Furthermore, the suggestions for information presentation could be also applied to runtime permission dialogs to further support users' understanding and resulting consequences permission granting.

Most of the above presented studies evaluated the permission granting with different UIs in terms of usability and privacy behavior (e.g. decision making). A single dimension of user experience was only addressed in one work – that was 'affect' in Harbach et al. [79]. While the other works have used subjective measures to determine users' satisfaction with the interfaces, subjective evaluations of user experience such as felt experience and hedonic quality have not been applied. Furthermore, the comparison of UX and user behavior related to different kinds of newly suggested permission UIs has been little considered, as newly suggested UIs have been mostly evaluated against the established baseline only (cf. e.g. [78, 112, 184]).

3.4 SUMMARY

A user may encounter different security and privacy mechanisms during a typical smartphone usage session. Those include, for example, secure booting, device encryption, screen locks with authentication,

app permission requests, and mechanisms for secure communication. In some cases, the user only interacts with the mechanisms or with notifications send by the mechanisms if a security issue has been detected (e.g. secure booting, browser certificate warnings). In other cases, the user always interacts with those mechanisms if s/he wants to perform a certain action, e.g. using the device (screen lock with authentication), installing an app (app permission requests at install-time). Thereby, the latter two mechanisms, i.e. screen locks and app permissions, are likely to be encountered more frequently and will therefore be considered as application examples for studying user experience, usability, and security/privacy with specific mobile security and privacy mechanisms.

Several methods are available for screen locks with authentication. Thereby, knowledge-based methods such as PINs, passwords, or graphical authentication schemes and biometric methods such as fingerprint-based authentication are currently widely deployed. Biometric methods also rely on knowledge-based fallback authentication and the latter is unlikely to disappear due to several reasons discussed above. A commonly deployed knowledge-based authentication method – PIN – has the drawback that especially short, 4-digit user-chosen PINs are rather vulnerable to guessing attacks [72]. The Android unlock pattern has a smaller theoretical password space than PIN and is furthermore also susceptible to user choice [191]. Emoji-based authentication schemes may constitute an alternative to PINs and unlock patterns: an earlier study shows that user-chosen 4-digit Emoji-passwords are less susceptible to guessing than user-chosen 4-digit PINs [72]. Furthermore, the use of Emojis may enable a positive authentication experience.

When it comes to app permission requests, most users will face runtime permission requests in the future. While iOS always used runtime permissions, Android's permission model has changed from install-time permissions to runtime permissions in 2015. The "basic permission dialog" for Android install-time permissions has been criticized as it was hard to understand for users [61] and shown at an unfavorable point in the decision making [112]. Several solutions have been suggested to increase users understanding and attention to the "basic permission dialog" (cf. e.g. [78, 112]). Although the former install-time permission dialog had several drawbacks, install-time permissions are not per se a bad thing, if implemented in a usable way. Also, while usability and behavioral aspects of interactions with permission requests have been intensively studied, little work has been conducted to investigate different UX dimensions of those interactions. Furthermore, as the Android runtime dialog is relatively new, future studies should investigate the effectiveness of and user experiences with this dialog.

4

CONCLUSIONS FROM THEORETICAL BACKGROUND AND RELATED WORK

So far, empirical studies on UX have been mostly conducted in the context of interactive products (cf. Chapter 2). The goal of this thesis is to gain a deeper understanding of user-related matters with mobile security and privacy mechanisms by considering different UX dimensions and by using methods from UX research. Therefore, the first empirical part of this thesis (Part III) applies mainly qualitative methods to explore users' experiences with mobile security and privacy and motivational factors (in terms of psychological need fulfillment) for voluntarily deploying related mechanisms.

While the explorative studies in Part III of this thesis serve to gain a deeper understanding of experience-related issues with mobile security and privacy in general, the second empirical part of this thesis (Part IV) applies the insights of the explorative studies in the design and evaluation of specific mobile security and privacy mechanisms, i.e. permission request dialogs and screen locks with authentication. Those two mechanisms are frequently encountered in typical usage sessions and are thus highly relevant from an experiential point of view.

Furthermore Part IV considers the research gaps that were identified in related work on mobile security and privacy mechanisms (cf. Chapter 3). For example, as Android install-time permissions, and thereby especially the "basic permission dialog", have been shown to be little effective, there is a need to provide users with additional information to help them determine the privacy intrusiveness of an app. Thereby, it also needs to be evaluated how providing such information impacts user experience and related behavior when selecting an app. During the work on this thesis, the Android permission model has changed from install-time permissions to runtime permissions. Therefore, the impact of the new runtime permission dialogs on user experience and related behavior needs also to be evaluated. Moreover, for both kind of permission dialogs, UX dimensions have been insufficiently studied.

Screen locks with authentications constitute another mechanism with which users frequently interact – dozens of times per day [78]. Thus, mobile authentication is part of the overall user experience with smartphones. User-chosen PINs and unlock patterns seem to provide a good usability [78, 195], but they suffer from security limitations resulting from a biased user-choice [22, 191] Emoji-based authentication constitutes an interesting, alternative use case for mobile authentica-

tion as user-chosen passwords seem to be harder to guess [72] and the authentication with Emojis may provide a positive user experience. Moreover, while concurrent work has evaluated the resistance of Emoji passwords against guessing attacks, user experience and resistance against capture attacks has not yet been studied.

Part III

QUALITATIVE, EXPLORATIVE STUDIES

5

EXPERIENCES WITH MOBILE SECURITY AND PRIVACY

5.1 STUDY 1: MOTIVATION

Much work has been conducted to investigate users' interaction behavior (cf. e.g. [61, 78, 112] and as well as acceptance of certain mobile security and privacy mechanisms (cf. e.g. [12]). Furthermore, aspects not related to specific mechanisms, but to mobile security and privacy in general, such as concerns [32, 59, 119, 149], awareness [150, 162], and expectation [136] have been investigated in earlier works. However, little is known about the experiences that smartphone users have with security and privacy on their smartphones.

Hence, the goal of the first study in this thesis was to explore users' familiarity with and views on the security and privacy threats and mechanisms discussed in Section 3.1 from an experiential point of view[1]. Therefore, two focus groups with 6 smartphone users per group were conducted. By fostering user discussion on security and privacy threats and mechanisms on smartphones, valuable insights into users' views and experiences with such mechanisms were gained. Identifying possible sources of positive and negative experiences with security and privacy on smartphones lays the foundation for avoiding or fostering such experiences in the design of future mechanisms. The present chapter describes the design of the focus groups including the procedure of the study and the analysis of the obtained data. The results of the study report on users' familiarity and feelings related to security and privacy on smartphones. The discussion relates the findings to negative and positive user experiences and the countermeasures to avoid the former and to foster the latter. The results of the present chapter provide answers to RQ1.

5.2 METHODOLOGY

This section describes the study set up and the analysis of the obtained data. Two focus group studies were conducted based on a phenomenological approach. In a phenomenological approach, researchers assume that participants' knowledge of a certain topic is

1 The contents of the present chapter were previously published in the paper "Analyzing end-users' knowledge and feelings surrounding smartphone security and privacy" by Lydia Kraus, Tobias Fiebig, Viktor Miruchna, Sebastian Möller, and Asaf Shabtai, which appeared in the Proceedings of the Workshop on Mobile Security Technologies (MoST), co-located with the IEEE Symposium on Security and Privacy, San José, May, 2015. [123].

represented through conscious experience [28]. The reasons for selecting the focus group method were twofold. First, compared to individual interviews, focus groups offer the advantage that they can foster discussions as participants' opinions might in many cases only partially overlap or not overlap at all. Second, focus groups offer the additional advantage of being able to collect much data in a short time and allow for immediate follow up and clarification [143].

To unfold the discussion space as wide as possible, the focus groups were organized as brainstorming sessions with the goal to collect as many ideas on security and privacy threats and mechanisms as possible – without judging them regarding their content and usefulness. Three general questions and one wording question were discussed during the focus groups: (1) Which advantages do smartphones offer? (2a) Which disadvantages result from the advantages? (2b) How would you call the disadvantages? Are they threats, dangers, negative consequences or maybe something completely different? (3) What can users do to protect themselves from the disadvantages?

To avoid leading participants, the direct questions were limited to this set of questions with the option to see which security and privacy topics would emerge. The wording question (2b) was included to ensure that the disadvantages can be regarded as potential threats. The impersonal nature of the questions was supposed to help avoiding situations where participants may feel uncomfortable, as they are forced to report on individual sensitive topics to other participants whom they do not know. In general, all studies in the present thesis have been discussed with peers and senior researchers beforehand, to ensure that they follow the basic principles of ethical research (as defined by the German Psychological Society (DPG) and the Association of German Professional Psychologists (BDP)).

5.2.1 *Procedure*

Following Morse [147] and Sandelowski [168] who suggest a sample size of six participants as sufficiently high for a phenomenological study, two Focus Group (FG) studies of six participants each were conducted. The two groups will be referred to as FG1 and FG2 in the remainder of the thesis. Participants were recruited with a participant recruitment tool of Technische Universität Berlin, and received monetary compensation of 10 Euro per hour. To avoid priming and self-selection of security savvy participants, the focus of the study was not revealed during the recruitment process. Therefor the study was advertised as a study on advantages and disadvantages of smartphones. The discussion during the focus group sessions took between 60 and 90 minutes.

Both focus groups were conducted according to the same procedure but by different teams of moderators. The focus groups were

conducted in a small conference room with a table at which six people could comfortably sit and a whiteboard at the side. To foster a pleasant atmosphere, participants were offered drinks and snacks. After welcoming they received a description of the study and a consent form. In the description of the study, again, security or privacy related topics were not mentioned to avoid priming the participants. The sessions were audio recorded and transcribed to facilitate analysis. The audio-recordings were deleted after the transcription process. Each focus group was led by a moderator and supported by a co-moderator and note-taker.

The moderator's task was: (1) to lead the discussion neutrally along the four questions of interest, (2) to foster the discussion, and (3) to play back the raised ideas to the participants in order to get deeper explanations. The co-moderator visualized the ideas that came up during the discussion by writing them onto sticky notes and placing them on the board. The visualization was meant to help participants to reflect on the ideas and to come up with new ideas.

The moderator started the discussion by welcoming the participants, explaining the study method and motivating the participants to freely speak out every idea. After the first question related to the advantages of smartphones was posed, the participants started to brainstorm. In many cases they added explanations why they think that the mentioned idea is an advantage. In other cases when concepts were raised and the moderator felt a need for further explanation, the moderator asked follow up questions like "Could you explain this in more detail?" Thereby, it was important that the moderator played back the ideas to the participants in a neutral way without interpretation. As soon as the conversation slowed down, the moderator motivated the participants with questions like "Can you think of other advantages/disadvantages/protections?" or "Ok, we have now gathered the following ideas. Can you think of any other ideas?".

After the advantages were discussed the moderator asked the participants to brainstorm about disadvantages of smartphones. If after some time no security or privacy related disadvantages were mentioned, the moderator asked the participants if they could also think of disadvantages related to security (privacy was not mentioned). Hereafter, the moderator asked the third question about how participants would word the disadvantages. Then, the last question about protections was posed.

After all topics were discussed, the discussion was closed; the participants were thanked for their participation and received reimbursement.

5.2.2 *Analysis*

Prior to analysis, the audio recordings were transcribed in whole whereby participants' names were replaced with pseudonyms. The analysis procedure was as follows. First, an open-coding annotation was performed on the transcripts by two analysts independently from each other. Second, the analysts used the data from the first step to identify themes, again independently from each other. After the second step, the analysts and the first coder met to find consent on the themes and to create a codelist (containing the themes). The analysts decided to not impose themes from related work on the data, but instead to stay open to what is grounded in the data. Therefore, tools and principles from Grounded Theory [37] such as questioning, looking at language, emotions and words indicating time were used. The data was then coded by the first coder and a second independent coder to increase the validity of the results.

The interrater agreement was determined as moderate according to Landis and Koch [129] (Cohen's kappa of 0.44 for FG1 and 0.45 for FG2). Deeper analysis revealed that the disagreements between the coders stemmed from what should be considered an "empty" statement and what could be considered "other disadvantages". While the first is the notion of what is a non-meaningful utterance by a participant, the second relates to information on disadvantages of smartphones that are neither security nor privacy related. An example for the latter would be a statement on modern smartphones being so large that they constantly destroy one's pockets. Therefore, it appears that the theme "other disadvantages" in FG1 was not meaningful enough and should have been split into subthemes such as health issues and disadvantages not related to security or privacy. In FG2 the discussion went not as fluently as in FG1. Sometimes only buzz words were thrown into the discussion or short discussions which went away from the topic appeared. This made it difficult for the coders of FG2 to decide which of the short statements should be included and which are indeed lacking in content. Therefore, the coders met once more to discuss the points of disagreement. This ensured that they did not miss to code any important statement and lead to consent on the coding of the transcript. In the following the version of the transcripts upon which the coders finally agreed is used.

5.2.3 *Participants*

Participants were sampled to roughly reflect the average smartphone user distribution in Germany. Figure 6 depicts the demographic characteristics of the participants. Both focus groups included participants above and under the age of 35, of various educational backgrounds. In both focus groups, more female than male participants (ratio: 4:2)

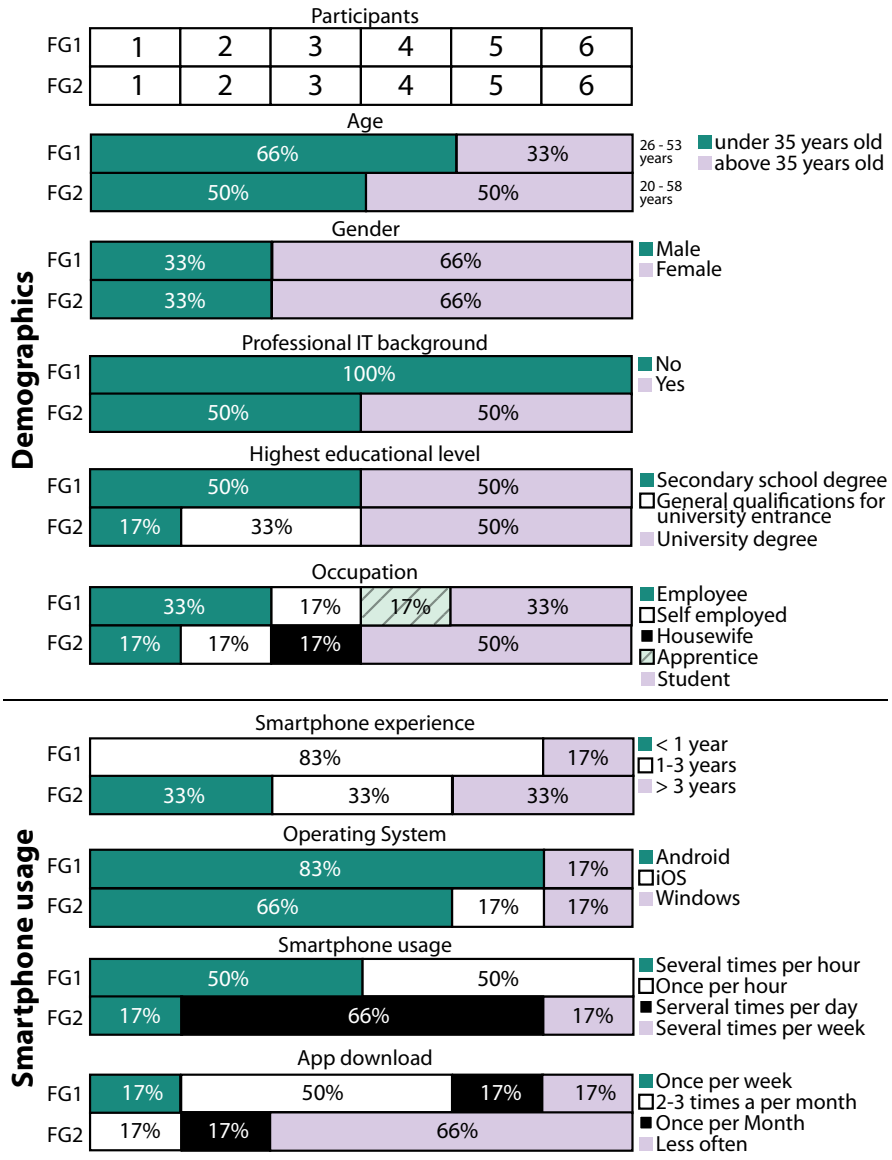


Figure 6: Overview of the demographic distribution and experience with smartphones for the participants in the two focusgroups.

were observed. Furthermore, there was a majority of Android users, which is reasonable due to the high market share of this operating system (cf. e.g. [180]).

FG2 was heterogeneous regarding demographics, smartphone usage and professional IT experience. However, FG1 participants owned their smartphone longer, used it more often and downloaded apps more often compared to FG2. In general, FG1 was more homogeneous compared to FG2. Therefore, FG1 could be described as a group of experienced and active lay-users. For FG2 it does not make sense to describe the participants as a group as they were too diverse in their characteristics.

5.3 RESULTS

In this section the potential security and privacy threats and mechanisms which were named during the discussions are reported. The results of the "advantages" part of the discussion will not be detailed as there were no topics related to security and privacy discussed. First, the potential threats and security and privacy mechanisms that emerged during the discussion are summarized according to the structure of Section 3.1. Thereafter, users' views and experiences on the topic will be reported.

5.3.1 *Familiarity with security and privacy threats and mechanisms*

Device Security and loss or theft

Threats. In both FGs different threats related to *loss* and *unauthorized data access* were discussed. The named instances included *device loss* (FG1), *theft* (FG2), *device damage* (FG2), and *data loss* (FG2), as well as the *ephemerality* of the device (FG2). In this context, the participants also discussed vulnerabilities related to the physical characteristics of a smartphone. The named vulnerabilities included the *small size* of the device, the *huge screen*, and the circumstance that one is *carrying private data with oneself*.

Mechanisms. As mechanisms both focus groups suggested to *store the device securely* or to *keep things safe* so that the device is less likely to be lost or stolen. *Password locks* were recognized as a traditional way to avoid unauthorized access. Another suggestion discussed in both FGs was *data backup*, in general or to the cloud (FG2). *Data encryption* was named in both FGs, but in FG2 some of the participants' ideas of encryption were somehow fuzzy, expressed by statements such as *"Bank data, for instance, somehow, they are multiply encrypted."* or that *"Skype"* is *"not bad"* to that end. FG2 additionally mentioned *remote deletion* and FG1 additionally mentioned the strategy of *buying a cheap phone* as a mitigation.

Network Attacks

Threats. Network attacks were intensively discussed in FG1. Thereby, the participants focused on the attack vectors and did not detail or distinguish between attack types or attack consequences. *Technical interfaces* (e.g. Bluetooth, NFC) and *open WiFi networks* were identified as attack vectors.

Mechanisms. Both FGs came up with *end-to-end encryption* as a security mechanism. FG1 additionally named several mechanisms such as to *switch off the data connections*, *to delete the SSIDs of untrusted WLAN networks* or to apply a *Firewall*. Note that non of the participants in FG1 had self-reported a professional IT background; however, this

does not imply that participants could not nevertheless be digital literate.

App security and privacy and general privacy intrusions

App security and privacy and *Privacy intrusions* were discussed in most detail among all other topics in both focus groups.

Threats. In both FGs buzzwords like *tracking* and *surveillance* fell. *Surveillance* was mentioned in general, but also emphasized by instances such as *unknowingly data traffic* (FG2), *becoming transparent* (FG2) or as a consequence of *hacking* (FG1). Tracking was discussed in general in both FGs. FG2 also noted the topic of advertising through *personalized ads* and *advertisement calls*. Issues related to *data misuse* were raised in both FGs with instances such as *data selling* (FG1), *data usage by privately owned companies* (FG1) and *negative consequences through personal data disclosure* (FG1). FG1 identified *faked apps*, *malicious websites*, *malicious apps*, *exploits* and *(malicious) SMS codes* as means to invade privacy or as general dangers.

Mechanisms. Privacy can be invaded by known (e.g. friends) and unknown people (e.g. hackers), by privately owned organizations (e.g. advertisers or service providers) or state organizations (e.g. intelligence services). Regarding known people as invaders, both FGs identified *to inform other people about own privacy preferences* as a privacy mechanism. Other privacy invaders were addressed by the following mechanisms: *End-to-end encryption* was suggested in both FGs, however, as already written in different threat categories. Furthermore, both focus groups saw personal responsibility as a key mitigation to privacy invasion, namely through *exercising one's own influence* (FG1) in general and *on data disclosure* (FG1) and to apply *self-protection* (FG2). Whereas FG1 sees the realization of the latter by *informing oneself* or by applying *common sense*, FG2 referred to the power of *personal responsibility* and the *trade-off* between benefits and threats related to using an application or service. Both FGs saw the *avoidance of applications or services* in general and specifically the *avoidance of smartphone usage at all* (FG1) or *the avoidance of sending sensitive information* (FG2) as effective mechanisms. Furthermore, *reading permissions* was identified in FG2. In FG1 *faked user names and dummy email addresses* or *not to let oneself being influenced by personalized content/ads* were suggested as measures against advertisements.

5.3.2 *Feelings related to potential threats and mitigations*

While brainstorming about potential threats and security and privacy mechanisms, different views and experiences were revealed by the participants. Interestingly, the discussion in both FGs revealed many

opposing views. In the following, the views of security and privacy mechanisms are described in terms of feelings and felt experience.

The question dedicated to the wording of disadvantages revealed that in both FGs the disadvantages were perceived as (potential) dangers. The participants in FG2 quickly agreed that the disadvantages are dangers, and then the discussion continued in another direction. In FG1 this question was discussed controversially. Whereas one participant saw the disadvantages as dangers, another participant promoted the notion that the collected disadvantages are technological side-effects, which may become dangers if misused. The discussion led to the notion that the disadvantages are something one needs to deal with either by acceptance or protection.

Social pressure. When talking about disadvantages and potential threats, the issue of *social pressure* was raised in both FGs. As an example for the influence of others, *peer pressure* regarding the adoption of applications which are considered unsecure was mentioned.

> *FG1-P2: "This means that even if you wanted to totally boycott the system, one does not have a choice."*

Another example for sociological factors mentioned in both FGs are expectations regarding the availability of the smartphone user or the feeling of being monitored by others (referred to as "social availability" in the following, oppositely to technical availability).

> *FG1-P1: "It's being expected that you are available at all times."*

> *FG2-P4: "Constant availability."*

> *FG1-P4: "Like surveillance. So if the others [colleagues] definitely saw that one's been online, I can't tell my boss 'Oh, I'm sorry I didn't see that you wanted me to help out.' "*

> *FG1-P5: "Mistakes could have been made by everybody, but nowadays it's so obvious. Mistakes are getting immediately discovered."*

In FG2 the topic of harassment by advertisers was raised:

> *FG2-P5: " [...] they later said: We will call you until you take part in the survey."*

> *FG1-P1: "[...] and occasionally they render the whole website as an ad. [...]Therefore, you don't have the chance to continue on what you wanted to do, but you need to give attention to the whole thing. [...]"*

Distrust as disadvantage vs. trust as mitigation. *Dwindling trust in the system regarding security aspects and respecting privacy* was described by some of the participants by noting that potential threats are nowadays worse than in the past:

> *FG1-P3: "It was always getting worse, that really every app wanted to access everything. So, four years ago, the first apps [...] weren't like this that they wanted to know everything."*

> *FG1-P2: "Well, when it comes to emails, in the past one could get an e-mail address for oneself and nobody knew to whom this address belonged to. But if you nowadays retrieve your emails on your mobile you are immediately identifiable."*

However, trust was also mentioned in the opposite way. Some of the participants mentioned trust in service providers or trust in the smartphone OS as measures to protect oneself against potential threats:

> *FG1-P3: "[...] so, the provider is just crucial."*

> *FG1-P3: "[...] with their cloud [storage service] there's at least more security as their company is based in Germany."*

> *FG1-P1: "As far as I know Windows is more secure."*

> *FG1-P1: "Exactly, I know, these WLAN networks that I do not trust, I should delete them [...]"*

Dependency, helplessness and fatalism. Several notions of negative feelings regarding potential threats and protection mechanisms evolved during the discussion. All these notions relate to either *dependency*, *helplessness* or *fatalism*.

The issue of dependency of third parties, for example, by relying on their provided security mechanisms or by downloading apps from the app market, was raised in FG1.

> *FG1-P2: "That is the thing, I am dependent again on someone and I again do not know, how safe this really is, that is again another alleged security, which leads me to dependence."*
> *[On the topic of encryption]*

> *FG1-P4: "So, this is quite stupid in the app market, that only if you are on the most up-to-date level, you get access to the apps, and that's why you get forced to always renew everything."*

Psychological dependency as a consequence of smartphone usage was noted in both FGs:

> *FG2-P3: "Dependance. Well, you really make yourself dependent if you rely on this device."*

FG2-P4: "Bad is also this psychological pressure, so to say, that one would be missing out on something."

In both focus groups some of the participants noted *helplessness* being an issue. It was mentioned, the contexts of both, threats and protection mechanisms.

FG1-P2: "But the worst thing nowadays is that for some things it's not our fault, for example if we visit some webpages, everything is recorded."

FG2-P3: "Yes, exactly, that there is data, umh, traffic which you are not so... aware of."

FG2-P4: "But that's, I think, the same as with your apartment's front door. You can lock it with ten locks or just with one, but if one wants to get in, so to speak, one will get in." [On the topic of encryption]

Closely related to helplessness was also the notion of *fatalism* which was expressed by participants in both FGs:

FG2-P2: "None, really no communication option with the mobile is secure. Not a single one."

FG2-P2: "There's nothing you can do against it."

FG1-P5: "You have to take into account that everything [...] can be hacked by somebody at any time or can be available somehow and spread through the internet. Nothing is secure, thus."

Some of the participants in FG1 raised the need to *sacrifice security* in order to use applications or services in the way they want to. Thereby, "Sacrificing security for usage" was defined by the analysts as a feeling of having no choice.

FG1-P2: "[...] because of everything already that I am googling, every single word that I type is recorded, every single website that I looked at, every single text that I looked at, all my data that is on my phone, especially these authorizations of these apps, if I agreed to something somewhere, where I HAD TO, so that I am allowed to use the application."

FG1-P1: "[...] it is seen by many [people] like this, that it [the disadvantages] is something that you have to accept [...]"

Exercising one's own influence. Conversely to the negative feelings which were expressed before, some of the participants in FG1 noted the possibility to *exercise one's own influence* through various actions as a security mechanism. Thereby, it was emphasized that it is crucial to first *inform oneself* in order to act accordingly.

FG1-P4: "I just may pick this up again, it is really like this, if one is not informing oneself, it's one's own fault."

FG1-P1: "So, there are certain things I can protect myself against, against others I cannot. Partly because I do not really know what are all things that can happen. And that is the key... So ... we need a kind of responsibility, enlightenment, information.... I think, that is missing a lot."

Some participants in FG1 mentioned *exercising one's one influence* e.g. by controlled disclosure as a mitigation. Moreover, in FG2, *individual responsibility* for mitigation was noted.

FG1-P4: "[One should not upload pictures] That's obvious. I never post any pictures of me on the internet,... "

FG1-P3: "[...] Well, let me say, one has got minimal influence on what one discloses. One really needs to read further into the topic [...]"

FG2-P3: "One can circumvent everything [all disadvantages] if decisions are made consciously and if one makes oneself clear: what could happen? Do I want this? Or do I not want this?"

FG2-P5: "One certainly needs to reflect, whether this is what one wants or what one doesn't want.[...]"

Processes. Both focus groups came up with the view that there exist processes in handling security and privacy. FG1 considered *threats to develop* in a process instead of being static. Thus, threats cannot be assigned to single usage occasions only and they develop either as a consequence of user behaviour or technology misuse. FG2 noted that security and privacy are subject to a *trade-off* between benefits and risks. Whereas the theme "sacrificing security for usage" refers to the feeling of not having a choice, this theme refers to the feeling that one has at least the choice not to use an app or service if one wants to achieve security.

FG1-P5: "It depends on how far you go. That's what we said. So the more you reveal, the more you have to anticipate that you will eventually lose."

FG1-P3: "I think that is too undifferentiated, because some things are technological necessities that I am subject to, so that I can use the device at all, and some things are side effects that arise, because others misuse these technological necessities."

FG2-P2: "But that, umm, that one can... No, because then you cannot use the service. It is about that: Do you want to use the service? Then you have to accept that."

> *FG2-P4: "Simply raise sensitivity, that it is really your responsibility... [pause] So to speak, take responsibility for that, what, which data you really share and what not."*

In summary, the focus groups revealed a variety of experiences related to smartphone security and privacy. Many of those experiences are rather negative: users report feelings of helplessness, dependency, and fatalism, as well as dwindling trust in the "system". However, participants also reported rather positive feelings of being able to exercise control.

5.4 DISCUSSION

5.4.1 *Limitations*

While the sample size of six participants per focus groups is rather small, it is considered sufficient for a phenomenological approach in the literature [147, 168]. Furthermore, the overlap in the results of the two focus groups demonstrates reasonable validity of the results. Nevertheless, generalizations should be made with caution.

Due to the qualitative approach using focus groups, a collective set of knowledge was measured. As a consequence, no statements about the state of knowledge of each individual participant can be made. Thus, the measurement of knowledge may differ in other kind of studies and generalizations should be made with caution.

5.4.2 *General discussion*

The focus groups revealed that already two groups of six users each were able to identify a reasonable set of threats and security and privacy mechanisms. The groups were of different demographic characteristics, among them one group of users without professional IT background. Therefore, the found knowledge cannot be attributed to demographic characteristics or IT knowledgeable users only.

During brainstorming on disadvantages and protections, the users revealed diverse views on topics related with positive and negative feelings. Most of these views were observed independently in both focus groups. Those feelings describe the emotional threads of users' experiences with security and privacy threats and mechanisms on smartphones.

Several findings are in line with related work. For example, the issues of distrust and trust have been investigated in several works. Mylonas et al. found in a survey with more than 400 participants that users who trust their app repository tend to be less likely to use smartphone security software [150]. The same was found about paying attention to security warnings. In a study with more then 350

users, Han et al. found that trust in third-party security apps positively influences the adoption of this kind of apps [75]. Conversely, in the same study, trust in the smartphone operating system showed to be a negative influencing factor for the adoption of third-party security apps.

In the above presented focus group study, issues of social pressure were revealed. In the research on technology adoption, social influence often shows to be an influencing factor for adoption. An example of this can be found in the UTAUT model presented in [193].

Regarding user experience, the discovered views can be further interpreted in terms of psychological needs. As mentioned in Section 2.2.1, psychological needs can be deployed to characterize classes of experiences.

For examples, the usage of smartphones allows people to stay connected with others and thus to support their need for *Relatedness*. However, these positive features can become threats to *Autonomy*, when the technology is used by others to put pressure on the user. Also, smartphones offer many features that enable users to manipulate their environment. These features can support the feeling of *Autonomy*, *Competence* and *Self-esteem*. A good usability of applications or the system itself may help to support these feelings. On the other hand, under certain circumstances, usage of smartphones may evoke negative feelings such as dependency, helplessness and fatalism. These feelings are antonyms of *Autonomy* and *Competence*.

In the following negative user experiences that were revealed in the focus groups are discussed and first ideas how these negative experiences may be avoided are suggested. Furthermore, positive user experiences such as trust and feelings of being in control are discussed together with the implications that such feelings may have for security and privacy.

5.4.3 *Negative experiences*

Social Pressure. The feeling of being forced to perform an action due to the general behavior of the peer-group.

Countermeasure. Security and privacy by design and default may help to suppress feelings of social pressure. Applications which support the *Relatedness* of users should apply this principle. For example, if end-to-end encryption would be enabled by default, users would not be forced to choose between messenger apps which are secure and have a smaller market share and applications which are widespread and do not feature security. The threat of social availability could be mitigated by offering proper privacy settings in apps which support social interaction. This is already done in many of these apps, but it is not a general standard or best practice.

Negative Feelings. Experiences related to feelings of dependency, general helplessness and fatalism.

Countermeasure. As the mentioned feelings are antonyms of *Autonomy* and *Competence*, applying proper usability engineering techniques during the design of security and privacy mechanisms is a first step to avoid frustration arising from a lack of usability. This idea is of course not new and has been discussed intensively in the literature [40]. A further suggestion is the extension of the usable security approach to an approach where positive user experience and need fulfillment is taken into account. Smartphone security mechanisms need to ensure not only usability, but they also need to convey positive feelings if they should reach higher acceptability by lay users.

5.4.4 *Positive experiences*

Feelings of being in control. The focus group results suggest that there are users who find themselves capable of exercising their own influence regarding issues of smartphone security and privacy.

Implications for security and privacy. While feelings of being able to exercise one's own influence in order to achieve security and privacy may be sources of positive user experiences, further studies are needed to determine whether the related actions are indeed as fruitful as perceived by the users. For example, Forget et al. observed user behavior and actual computer security configurations and complemented this data with a qualitative interview study on computer security behavior [66]. They found that users who highly engage with computer security do not necessarily own computers that are better protected.

(Unmerited) Trust. The focus group study revealed that users may use trust in a service provider as a shortcut for security and privacy. A similar finding was also reported by Chin et al. who found in the context of app installation behavior that users highly rely on app reviews provided by other users to make decisions about the trustworthiness of an app in terms of safety [32]. However, trust may be also a source for security issues and privacy violations, whenever it is unmerited, i.e. when a user trusts an insecure or privacy-intrusive systems to preserve those classical security assets it intentionally violates.

Implications for security and privacy. User education and awareness might help to mitigate this threat. Thereby user education should address two factors: first, education regarding to security and privacy threats that may arise from apparently benign services or applications. For example, there are already tools for user education available such as anti-phishing education apps [29]. Second, education should also target awareness regarding security and privacy mech-

anisms that users may employ to protect their devices from such threats. However, as education may only work up to a certain point [69], also reliable, human-readable trust-indicators are needed.

In summary, the focus group study helped to explore negative and positive experiences with mobile security and privacy. Moreover, in the discussion, opportunities for avoiding negative experiences and fostering positive experiences have been identified. Despite potential negative experiences, there are users who deliberately deploy security and privacy actions on smartphones. The next chapter explores what motivates them to do so.

6

MOTIVATORS FOR MOBILE SECURITY AND PRIVACY

6.1 STUDY 2 AND 3: MOTIVATION

Chapter 5 explored negative and positive experiences with mobile security and privacy. Furthermore, Chapter 5 discussed how negative experiences could be avoided and positive experiences could be fostered. For the latter, it further needs to be ensured that the positive experiences do not foster false feelings of security and/or privacy.

The suggestions for avoiding negative experiences included the deployment of security and privacy by design and default in social apps, as well as proper usability engineering of security and privacy mechanisms, and user education. However, avoiding negative experiences may not automatically lead to a positive user experience (cf. also [85]). Psychological need fulfillment has been shown to be related to positive user experience [85]. Studies have further shown that need fulfillment can be manipulated through product features leading to a positive change in user experience evaluations [68, 177]. Following Hassenzahl's model of user experience [83], the present chapter further investigates which psychological needs are salient as motivators for the adoption of mobile security and privacy mechanisms[1]. It is then discussed how psychological needs could inform the design of security and privacy mechanisms in order to foster a positive user experience. Consequently, the present chapter provides answers to RQ2.

As suggested by the results of the focus group study (cf. Chapter 5), users may not solely stick to security and privacy mechanisms as defined in the literature. Therefore, security and privacy "actions" are explored in the present chapter which may include any kind of behavior users report to protect their security and privacy.

First, nineteen semi-structured in-depth interviews with smartphone users were conducted to explore users' motivations for voluntarily applying security and privacy actions on smartphones in terms of

1 The contents of the present chapter were previously published in the paper "Exploring Psychological Need Fulfillment for Security and Privacy Actions on Smartphones.", by Lydia Kraus, Ina Wechsung, and Sebastian Möller [121], which appeared in the Proceedings of EuroUSEC, Darmstadt, 18 July 2016. © Internet Society, http://dx.doi.org/10.14722/eurousec.2016.23009, and in the article "Psychological Needs as Motivators for Security and Privacy Actions on Smartphones", by Lydia Kraus, Ina Wechsung, and Sebastian Möller [122] which is an extended version of the EuroUSEC paper [121] and has been published in the Journal of Information Security and Applications (JISA), Volume 34, Part 1, pp. 34—45, 2017. https://doi.org/10.1016/j.jisa.2016.10.002 [122]

psychological need fulfillment. Thereafter, an online survey (N = 70) was conducted in which questionnaires on psychological need fulfillment from the literature were used to gather initial quantitative data on the potential of security and privacy mechanisms to contribute to psychological need fulfillment.

6.2 INTERVIEW METHODOLOGY

As described in Chapter 2, user experiences can be categorized by considering the underlying psychological needs that motivate the interaction with a product [83]. Thereby, psychological needs can be considered as be-goals [83]. A user for instance makes a phone call to experience the feeling of being close to others. Thus, the motivation (i.e. the be-goal) of this action would be the fulfillment of the need *Relatedness* (example taken from [83]). The do-goal is the action of making the phone call. Or, a user may activate the privacy setting in a messaging app so that the sender of the messages cannot see when a message was read. This avoids the pressure to reply immediately to a message. In this case, the privacy setting would be used to fulfill the basic psychological need (and be-goal) of *Autonomy*. Activating the privacy settings is the do-goal of the action.

Following the description of be-goals and do-goals, psychological needs are related to the question why something is done whereas actions are related to the question what is done and how it is done [83]. Therefore the script for the semi-structured in-depth interviews concerned the following research questions:

- Which security and privacy actions are employed by smartphone users? *(What?)*
- How are they employed? *(How?)*
- Why are they employed? *(Why?)*

With this approach participants were not explicitly asked for the needs they aim to fulfill with their actions. Therefore, the why-questions were considered to provide answers regarding the reasons for doing an action and those reasons were then coded with the psychological needs.

The interview script (cf. Appendix A.2) covered a variety of possible actions, extracted from the literature on smartphone security risks [93, 174] and users' threat perception [32]. Action-questions were intentionally designed in an open manner as it could not be assumed that users only stick to the actions which are defined in the literature. The salience of the topics security and privacy increased during the course of the interview.

The interview was divided into three parts. In the first part, participants were asked about their general smartphone usage habits,

e.g. reasons why they bought a smartphone, which operating system they use, and if they have used another operating system before. They were then asked about smartphone sharing and usage at work. Afterwards, several questions on app usage, app installing, and uninstalling were asked. Some of the questions were taken from [32].

In the second part of the interviews, the central themes were security and privacy actions, including questions about the first time that participants set up their smartphone, usage of data connections, installing of updates, usage of pre- and postpaid options, battery consumption, theft protection, backups, internet usage, financial functions, protection from app access to sensitive information and communication.

In the third part, questions covered security and privacy software usage, password lock usage, and thoughts on general threats of smartphone usage. For each question of the interview, the interviewers were instructed to ask follow-up questions on reasons and triggers for behavior.

6.2.1 *Procedure*

Participants were recruited with a participant recruitment tool of Technische Universität Berlin. The interview sessions took between 20 and 40 minutes depending on how talkative the participants were. Participants received 12 Euro reimbursement. Participants who already participated in the focus group study (cf. Chapter 5) could not participate.

The interviews were conducted in German in the beginning of 2015 at the Quality and Usability Lab of Technische Universität Berlin. Each interview was conducted by one interviewer. To reduce interviewer effects, there were two interviewers. Approximately half of the interviews were conducted by Interviewer 1, the other half by Interviewer 2. Audio recordings were made to enable verbatim transcription after the interviews. The audio recordings were deleted after the transcription process. At the beginning of the interview, participants received an information sheet and were asked for consent. Then, questions on demographics, smartphone usage (frequency of use, etc.), privacy concern and ICT attitudes were presented to the participants. During the recruitment it was not mentioned that the interview is about security and privacy, but the participants were told that the study is about their "smartphone usage habits".

At the end of the interviews the participants were thanked and debriefed. Due to the nature of the interview it might have been that the participants became aware of shortcomings in their security behavior. Therefore, after the interview, they were provided with a flyer on which they could find further information on how to protect their security and privacy on smartphones.

6.2.2 *Analysis*

The codebook consisted of the descriptions of the 11 psychological needs (cf. Section 2.2.1), the items of the need fulfillment questionnaire [175], and a few items of the UNEEQ questionnaire (only for *Keeping the meaningful*) [190]. Thus, the codes could be used for either need fulfillment or frustration.

Two coders independently coded the interviews by applying the codebook described above. Interrater-agreement between the two coders was found to be moderate (Cohen's $\kappa = 0.46$) according to Landis and Koch [129]. The disagreements between the coders stemmed from a few issues. During the coding, the coders encountered many passages in which participants told that they would do an action in order to save money. However, saving money is not explicitly part of the definition of the need *Money/Luxury* as described in Section 2.2.1. Nevertheless, in most passages related to saving money, participants were willing to corrupt their privacy or security in order to get access to "nice possessions". For instance, they said that they would choose the free version of an app rather than the paid version, although the free version required more permissions. Thus after discussion, the coders decided to label these passages as *Money/Luxury*. The coders also discussed the *Security* code. This code was rather found in the context of *being safe from threats* than *having a need for structure or control*. The coders agreed that the first definition is valid as it can be found in the questionnaire on need fulfillment [175]. There was also disagreement on whether situations in which the participants reported the desire that others cannot track or observe them should be coded as *Security* or *Autonomy*. This is a typical situation related to privacy; however, a need for privacy is not part of the needs suggested in the related literature (cf. Section 2.2.1). In the end, the coders agreed on coding these passages as *Autonomy* - in line with Westin's definition of the functions of privacy, one of them being personal autonomy [200]. In the following, the coded transcripts upon which the coders finally agreed are used.

Additionally to the analysis of the psychological needs, a list of security and privacy actions was extracted from the data by the coders. Actions in the list include actions as defined in the literature [93, 174] and actions which were additionally mentioned by the participants. Based on this list, the coders analyzed independently whether an action was applied by a participant or not. For the coding of the actions, the coders reached almost perfect interrater-agreement (Cohen's $\kappa = 0.84$) according to Landis and Koch [129]. The coders met to discuss disagreements and to reach consent. Table 1 reports the results upon which the coders agreed.

6.2.3 *Participants*

Nineteen smartphone users (10 female) participated in the interview study. The age ranged from 18 to 58 years (M = 31, Md. = 27, SD = 10.94). Participants had diverse educational levels (approximately equally distributed between secondary school degree, qualification for university entrance, and university degree). The sample comprised nine employees, seven students and three job seekers. Only one participant had a professional IT background.

There were 13 Android users, five iPhone users and one Windows Phone user. The sample roughly reflects the distribution of smartphone operating systems among the smartphone user population in Germany at the time of the study (Android 70%, iOS 20%, Windows Phone 5%) [180]. Smartphone usage experience among the participants was diverse: Four participants had owned their smartphone for less than a year, seven for one to three years and eight for more than three years. Most of the participants use their smartphone at least once per hour (N=15).

6.3 ONLINE STUDY METHODOLOGY

For the online survey, those security and privacy actions were selected which participants either frequently reported in the interviews or which were considered to be of interest for security and privacy technologies designers (e.g. messaging with end-to-end encryption). General need fulfillment was measured for each of those actions.

6.3.1 *Procedure*

Participants for the online study were recruited by word of mouth and email. They were recruited by seven people who sent out emails to people who they know but who were not aware of the study's topic. As the survey took around 20 minutes to answer, personalized invitations were sent as it this was expected to achieve higher compliance of the participants and eventually higher data quality. Three vouchers à 50 Euro were raffled among all participants.

The survey started with questions on demographics. Afterwards, data on smartphone usage was collected: for how long the smartphone has been used, frequency of use, the operating system, their three favorite apps, the reasons for buying a smartphone, and whether they perceive different situations as threats. The survey was then divided in three different versions. Participants were randomly assigned to the different versions of the survey.

Version 1: Participants were asked if they apply backups and if there are situations in which their data connections are disabled (one question each for WiFi, Bluetooth, and GPS) and, if so, how often they

disable them. The last question was whether they apply a password or PIN lock.

Version 2: Participants were asked if they install updates, if so, manually or automatic. They were also asked if they check their monthly bill and prepaid balance, respectively. Then they should indicate if they apply privacy settings (i.e. whether they have enabled the function that others can see if a message was read) within messaging apps.

Version 3: Participants were asked if they do something to protect their phone from theft, if so, they were asked what. They were then asked if they check app permissions, if so, how often. At the end they were asked whether they use messaging apps with end-to-end encryption. As it could not be assumed that all participants are familiar with the term "end-to-end encryption", examples of such apps were given. Furthermore, participants were also offered an option allowing them to specify other apps than the ones given.

For each action, participants were asked to indicate the level of need fulfillment they experienced. To do so, a German version of the need fulfillment questionnaire [47] was employed which is based on the questionnaire by Sheldon et al. [175]. Questions for *Keeping the meaningful* were taken from the UNeeQ questionnaire [68, 190]. For participants who stated that they do a particular action, the questions were formulated like this: "By doing [action] I have the feeling that..."; for non-user the wording was: "By not doing [action] I have the feeling that..."

The reasons for splitting the survey in three parts were twofold. First, as participants were supposed to answer the need questionnaire for each action, considering all actions for all participants would have led to a high number of need items per participant (9 actions x 3 items per need x 8 needs = 216 items). Second, the questionnaire would have been highly repetitive as participants would have needed to answer nine times the same 24 need items (only differing in the action they relate to). These two factors may have resulted in fatigue effects and lower motivation to retrieve the optimal answer to each questions (i.e. "optimizing" [127]).

Besides splitting the survey in three parts, only two of the three items of the original need questionnaires were selected. This further reduced the number of items and resulted in 48 need items in total per participant (16 items per action). The needs for Self-actualization, Self-esteem and Physical/Bodily were excluded, as they were reported only seldom in the interviews.

Besides questions on security and privacy actions, which differed between the three versions, all questions were the same for all participants.

6.3.2 *Participants*

Seventy smartphone users participated in the online study. The participants (female= 37.1%) were between 18 and 61 years old (M = 28, Md. = 26, SD = 8.11). They had diverse educational levels (Secondary school degree: 4.3%, completed training: 12.9%, qualification for university entrance: 32.9%, College/ university degree: 50%). Occupational groups were reported to be employees (38.6%) and undergraduate students (44.3%), and other groups (e.g. job seekers, self-employed) (17.2%). The majority did not have professional IT expertise (60%).

Among the participants were 40 Android users (57.1%), 23 iOS users (32.9%), four Windows Phone users (5.7%) and three users of other mobile operating systems (4.3%). The majority has owned their smartphone for more than three years (61.4%) or between one and three years (32.9%), while only few participants reported to having owned their smartphone between four and twelve months (5.7%). Most of the participants were frequent smartphone users: 50% reported to use their smartphones several times per hour, 20% reported to use it approximately once per hour, and 24.3% reported to use it several times a day.

The sample was diverse regarding age, smartphone operating system usage, and occupational groups; however, there was a bias towards male participants, higher educational levels, and students.

6.4 INTERVIEW RESULTS

Participants reported the application of many security and privacy actions in the interviews. Those actions largely rely on either mindfulness or pre-installed mechanisms. The psychological needs motivating the application of the reported actions are diverse: besides *Security* which was likely to be a motivator due to the nature of the interview, *Autonomy* and *Money/Luxury* play a major role. *Competence*, *Relatedness*, and *Stimulation* were found to be of moderate importance. *Keeping the meaningful* and *Popularity* were only relevant for a few actions. *Self-actualization*, *Physical/Bodily*, and *Self-esteem* were found to play a minor role as motivators.

The results of the interviews are structured according to the macrostructure of the interview script. For each subsection, the two to three most mentioned needs are discussed.

6.4.1 *Security and privacy actions*

An overview of the reported actions is provided in Table 1. Saving battery lifetime was reported most frequently, followed by switching

off all data connections, deploying updates, and protecting the device from theft.

Neither the installation of nor the subscription to additional apps or services is required for the 10 top strategies as those strategies are either based on mindfulness or on pre-installed security/privacy mechanisms. Examples for the latter include screen lock with authentication or backups to the cloud (if the backup app was pre-installed).

Note that actions encompass what the participants have reported, not what they may actually use. For example, iPhone users may not have been aware that encryption on iOS is enabled by default when using a screen lock with authentication. Further note, that end-to-end encryption was not implemented in many messaging apps by the time of the study. Thus, the use of messaging apps with end-to-end encryption was interpreted as a separate action. Table 1 does not take into account intensity and frequency of the deployed actions. For example, for "checking permissions" there may be participants who check app permissions every time, while other participants may only check them when they are suspicious for some reason.

In the following the psychological needs related to the different actions are reported. The abbreviations P1 to P19 thereby indicate the different participants.

6.4.2 *Saving battery lifetime*

From an IT-security perspective the (automatic) monitoring of battery consumption may be used to detect malicious activities on a device [174]. While users could also regularly check their battery status to detect apps that unnecessarily drain energy, the participants in the interview study mentioned checking their battery status as a safety measure: they reported saving battery lifetime to be, for example, available to friends. Thus, *Relatedness* is one reason for saving battery lifetime. P12 mentioned that he started to check his battery status regularly as there have been situations where "I was somehow absentminded and my battery only had 30%, but I was somewhere outside for let's say five or six hours; well, I need to be available to friends or so."

Another reason for saving battery lifetime is *Security*, as evident in the statement by P9: "Mhm well, in fact [...] it happens quite often, that I need to find my way home via Google Maps or public transport and therefore I always want to have at least 10% battery left and that's why... that's why I save battery".

6.4.3 *Connectivity*

When participants were asked about situations in which their data connections such as Bluetooth, NFC or GPS are disabled, it was ex-

Table 1: Self-reported security and privacy actions. Percentages do not sum up to 100 as participants could report several actions.

Security and privacy actions	freq.	%
Save battery lifetime	18	95%
Switch off all data connections (e.g. by flight-mode)	17	89%
Deploy updates	16	84%
Protect from theft (e.g. by securely storing the device)	14	74%
Check permissions	14	74%
Make backups	14	74%
Use screen lock with authentication	12	63%
Avoid financial apps/ functions (e.g. online banking)	10	53%
Check monthly bill/ prepaid balance	9	47%
Disable WiFi connection	6	32%
Disable Bluetooth	5	26%
Disable GPS	4	21%
Hide one's identify (e.g. by fake user profiles)	4	21%
Reduce online "data traces"	3	16%
Adjust privacy settings of messaging apps	3	16%
Use antivirus apps	3	16%
Log out from services	3	16%
Take out insurance	3	16%
Use remote management apps	3	16%
Do not use messaging apps	2	11%
Use apps for privacy protection/ permission management	2	11%
Use messaging apps with end-to-end encryption	2	11%
Modify privacy settings of the device	1	5%
Uninstall pre-installed apps	1	5%
Root the device	1	5%
Do not download apps at all	1	5%
Use data/ device encryption	0	0%

pected that they report on turning off WiFi for example in order to avoid network attacks. Instead, most of the participants mentioned situations in which they switch off all data connections (e.g. by activating the flight mode). This behavior is driven by the need for *Autonomy*: "I don't need to be available all the time, well, I can be without my mobile phone" (P11). "Because I want to be left alone" (P9). "I always disabled it [all data connections] at work, so that I don't get distracted" (P15). *Money/Luxury* is another reason why data connections are switched off. P17 noted: "[...] when I am at home then I use WiFi and switch off my mobile internet, because I think I

can save some of my data contingent doing so at least that is how I understood it." However, for few participants, a need for *Security* was found related to the usage of public WiFi spots: "Well, for me that is... open WiFi is too risky for me." (P15)

6.4.4 *Updates*

Updates were seen as a source for *Stimulation* rather than a necessity in terms of *Security*, for instance by P8: "Yes, if there are new updates I install them so that I have the latest version [of an app]." Doing updates manually provides *Autonomy* for some of the participants: "In certain intervals, maybe once per month, I enter Google Play and then I check which apps I have [on my phone] and for which of those apps updates are needed. Then I decide what I update or what I don't update" (P2).

6.4.5 *Protection from theft*

Interestingly, instead of using remote management apps or the like, many of the participants mentioned that they store their device securely or that they pay attention to where they leave the device. This provides them with a feeling of *Security*, as can be seen in the quote by P15: "It's always strange, when it [the phone] is somewhere else, for example in my backpack; I'd rather carry it on me, then I know it's there and I notice relatively quickly if it would be gone." P12 stated: "I just do it [storing it securely] as a preventive measure, just not to be placed in such a situation [that the phone is stolen]."

6.4.6 *Screen lock with authentication*

Not surprisingly, most quotes related to screen locks with authentication were coded with *Security*, an example is the following quote by P8: "Uumh, if it [the phone] is stolen or so, [for the thief] it wouldn't be so easy to use it immediately." P6 noted as a reason to use password lock: "I believe that it's maybe... In case that one loses the phone, it is a bit more difficult [to access it]." *Security* and *Popularity* as reasons to adopt a password lock were mentioned by P5: "In the beginning it was, because I thought it is pretty cool how my friends typed in their security codes on their mobile phone. Now it is just for security reasons." Thus, for P5 locking mechanisms have the potential to convey the impression of being "cool" to others.

6.4.7 *App selection, uninstalling apps and mitigating access to sensitive information*

When it comes to app selection *Stimulation* plays a major role as noted by P11: "sometimes I check the category 'newest apps' and those that sound interesting will be downloaded." Also, the influence of the price, i.e. *Money/Luxury*, was mentioned by several participants, for instance in this quote: "Well, there are enough [apps] for free" (P17).

Security may be a decision factor in the app selection process, as noted by P3: "It depends on what kind of app it is, how urgent do I need that app? Well, if I want to download some game just for fun and [then I] see 'Okay, the App wants to have access to everything', [...] than I just don´t install it." P4 mentions *Security* concerns during app selection: "[...] but then sometimes I do worry, a self-employed developer, what kind of mischief they could do."

A feeling of not being *competent* when it comes to judging permissions was expressed by P7: "Therefore I don't see myself in the position, to switch those things [the permissions] off; I think that I am allowing it [having access] to some apps."

Autonomy is experienced by not allowing apps to access location data "[I switch off GPS] because I do not want, that someone who should not know it, knows where I am." (P11). When it comes to uninstalling apps, *Autonomy* is a reason, as evident from this statement by P12: "Simply because I don't want Apple to know where I am or something like that". However, also *Money/Luxury* may be a reason for uninstalling an app: "Well, sometimes there are apps which are advertised to be free of charge and then you only got a couple of functions and you have to pay for many other functions. And well then I rather uninstall those apps because it annoys me." (P13).

6.4.8 *Backups*

Security and *Keeping the meaningful* were the only reasons that were salient in the context of backups: "Yes, because the data on my mobile phone is important to me... and well it is better... safety comes first." (P8). Unsurprisingly, the desire to keep (meaningful) things is related to the subjective value that the participants attach to them, as implied by this statement by P3: "Well, I am a person who loses his mobile phone quite often, and, well I was in Brazil and took some pictures there. And after two weeks of traveling I dropped my mobile phone in a river. Well, then I thought 'mhh damn it'. I got my phone to work again, but then I uploaded everything to the cloud ... well, so that I do not lose all my pictures [...]."

6.4.9 *Communication*

Being in contact with people one cares about, i.e. *Relatedness*, was mentioned by many of the participants as a reason for using messaging apps: "The reason for using it [WhatsApp] is actually that all my friends are using it, otherwise I would like to use another one [app]." (P9). "Because everyone used to use it and if you did write an SMS, then you were kind of out and well then you just used it too. Last year I tried to get rid of WhatsApp, but there are still too many people who still got it and won't write SMS and well then you just have to get back to WhatsApp." (P15).

When the participants were asked whether they do something in order to protect their communication, it was rather expected that they would mention end-to-end encryption or the like. However, only two participants reported that they used it. Instead many said that they use privacy settings in messaging apps. Those statements were labeled with *Autonomy*: "I wouldn´t describe it as a protection measure, but for WhatsApp I turned off, that you can see when I was online the last time or stuff like that... well." (P3). Group chats in messaging apps were seen as a possible source of unpleasant consequences by P6: "Yes, so, I am careful when it comes to these group... group-chats or things like that. I do not use them, because I think they are quite precarious [...]." Therefore, this quote was coded with *Security*.

Summarizing, a variety of examples how psychological needs, i.e. be-goals, drive security and privacy actions on smartphones was found: for instance, the participants reported *Relatedness* and *Security* as motivators for saving battery lifetime; they further reported that *Autonomy*, *Money/Luxury*, and *Security* are playing a role in managing connectivity; they also mentioned that *Stimulation* and *Autonomy* motivate actions related to updates and that the need for *Security* motivates the protection from theft; *Security* was mainly mentioned as motivator for using a screen lock with authentication, however, there is also a potential for *Popularity* being addressed with this action. App selection was noted to be driven by *Stimulation* and *Money/Luxury*, whereas *Security*, *Competence* (or a lack thereof) and *Autonomy* were reported to be related to uninstalling apps and mitigating access to sensitive information. The interviews further indicated that backups are motivated by *Keeping the meaningful* and the need for *Security*; communication is related to *Relatedness*, whereas its protection is related to *Autonomy*, and *Security*, both rather in the context of threats arising from other users.

6.5 ONLINE STUDY RESULTS

In this section the results of the online survey are reported. Thereby, the results for those security and privacy actions which are considered to be most influenceable by security and privacy technology designers are reported.

Whereas *Security* was a salient need in the interviews, the online survey results do not suggest *Security* to be of special importance as a motivator. The online study results rather suggest that other needs such as *Keeping the meaningful*, *Stimulation*, *Autonomy*, and *Competence* play a role for some of the actions. For other actions, the results were inconclusive. Although differences in need fulfillment were found for some of the actions, general need fulfillment for all actions was rather low according to the mean values which were mostly below 3.0

Table 2 shows the mean values, medians and standard deviations for the respective security and privacy actions. As the survey was split into three parts and as only users who reported to take an action were considered, the sample size (N) for each action is rather small. Figure 7 shows the need profiles in terms of mean need fulfillment for each action.

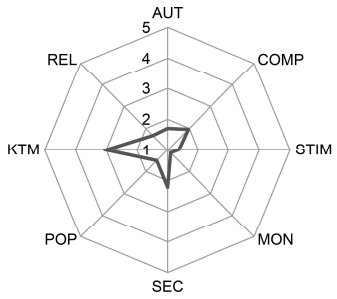
As the sample size for each action was rather small, non-parametric Friedman tests (i.e. the non-parametric equivalent of a repeated measures ANOVA) were conducted for each action to see whether users rank some needs higher than others. Post-hoc analyses were conducted with adjusted p-values using the Bonferroni method (i.e. the p-values were multiplied with the number of comparisons and only accepted as significant if they were still below 0.05). Effect sizes (r) were calculated for post-hoc analyses as $r = Z/sqrt(O)$ with O being the number of observations [63].

6.5.1 *Backups*

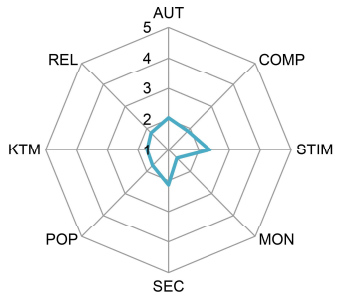
For participants who reported to do backups (N = 14), the Friedman test revealed a significant difference in need fulfillment for this action, $\chi^2 = 40.90$, $p < 0.01$. Post-hoc analysis showed that users ranked *Keeping the meaningful* significantly higher than *Popularity*, $Z = 3.16$, $p = 0.04$, $r = 0.60$. *Keeping the meaningful* was further ranked significantly higher than *Stimulation*, $Z = 3.74$, $p < 0.01$, $r = 0.71$, and *Money/Luxury*, $Z = 4.13$, $p < 0.01$, $r = 0.78$. For all pairwise comparisons effect sizes are large. The results suggest that the fulfillment of *Keepings the meaningful* is a relevant factor to use backups (cf. also Figure 7a).

6.5.2 *Updates*

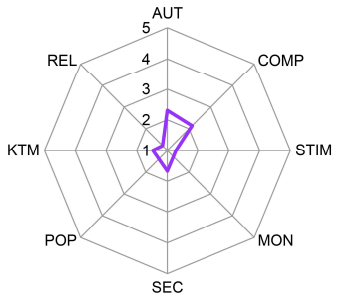
For participants who reported that they installed updates (N = 22), the Friedman test indicated significant differences between the level



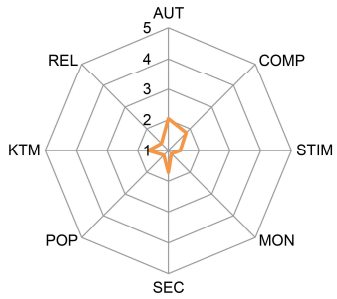
(a) Backups: Mean need fulfillment



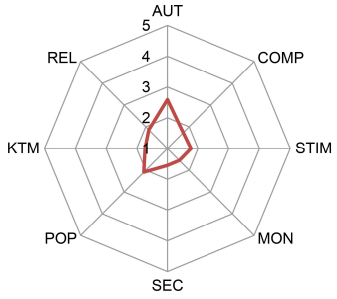
(b) Updates: Mean need fulfillment



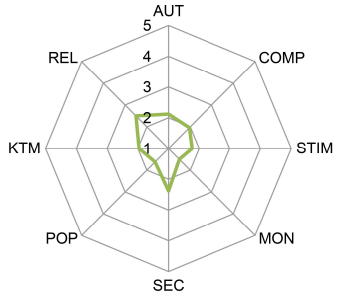
(c) Scrutinizing permissions: Mean need fulfillment



(d) Screenlock with authentication: Mean need fulfillment



(e) Privacy settings (instant messaging): Mean need fulfillment



(f) End-to-end encrypted messaging: Mean need fulfillment

Figure 7: Mean need fulfillment for different actions. The subfigures show distinct need profiles for each action. AUT = Autonomy; COMP = Competence; STIM = Stimulation; MON = Money/ Luxury; SEC = Security; POP = Popularity; KTM = Keeping the meaningful; REL = Relatedness.

of need fulfillment, $\chi^2 = 30.00$, $p < 0.01$. Post-hoc analysis showed that values for *Stimulation* were significantly higher than for *Money/ Luxury*, $Z = 3.85$, $p < 0.01$, $r = 0.58$. The effect size for the pairwise comparison is large. The results suggest that *Stimulation* is a rather relevant factor to employ updates (cf. also Figure 7b).

6.5.3 *App permissions*

For participants who reported to scrutinize permissions (N = 18), the Friedman test was significant, $\chi^2 = 58.89$, $p < 0.01$. Post-hoc analysis showed that users rated *Autonomy* significantly higher than *Relatedness*, $Z = 3.61$, $p < 0.01$, $r = 0.60$, *Money/ Luxury*, $Z = 3.91$, $p < 0.01$, $r = 0.65$, *Stimulation*, $Z = 3.71$, $p < 0.01$, $r = 0.62$, and *Popularity*, $Z = 3.20$, $p = 0.039$, $r = 0.53$. Also, users ranked *Competence* significantly higher than *Relatedness*, $Z = 3.50$, $p = 0.013$, $r = 0.58$, *Money/Luxury*, $Z = 3.81$, $p < 0.01$, $r = 0.64$, and *Stimulation*, $Z = 3.61$, $p < 0.01$, $r = 0.60$. For all pairwise comparisons effect sizes are large. As the permission systems differ depending on the OS, Android and iOS users were compared: a Mann-Whitney-U-Test did not reveal significant differences. The results suggest that scrutinizing permissions is related to the fulfillment of the needs for *Autonomy* and *Competence* (cf. also Figure 7c). Interestingly, for all needs beside *Autonomy* and *Competence*, the median value is 1.0 (cf. Table 2). Thus, at least half of the participants felt that other needs are not fulfilled at all. Even though participants who scrutinize permissions ranked *Autonomy* and *Competence* higher compared to other needs, the mean and median values remain rather low (< 2.5) compared to the results of Hassenzahl et al. who investigated need fulfilment in the context of HCI [85].

6.5.4 *Screenlock with authentication*

Despite a significant difference in need fulfillment for participants who reported to use a screen lock together with a PIN or password (N = 14, Friedman test, $\chi^2 = 30.00$, $p < 0.01$), post-hoc analysis did not show significant differences. Again, need fulfillment was in general low with five of eight investigated needs having a median of 1.0. The highest mean value (*Autonomy*) is only slightly larger than 2.0 (cf. Table 2 and Figure 7d). Surprisingly, not even *Security* scored higher than the other needs.

6.5.5 *Privacy settings in instant messaging*

The results indicate a rather high median of 3.0 for *Autonomy* for users of privacy settings in instant messaging apps (N = 11, cf. also Table 2 and Figure 7e). However, a Friedman test did not show significant differences in need fulfillment.

6.5.6 *End-to-end encrypted instant messaging*

A Friedman test was significant for users of messaging apps with end-to-end encryption (N = 13), $\chi^2 = 18.78$, $p < 0.01$; however, post-hoc analysis did not yield significant results. There were high median

values for *Relatedness* and *Security* indicating at least for some of the participants a tendency for the fulfillment of those needs (cf. also Figure 7f); however, the rankings for those two needs did not differ significantly from other needs.

In summary, the results of the online survey suggest that for some actions certain needs are more relevant than others. In cases where an effect was found in the post-hoc analysis, the effect sizes were large (above 0.5). For backup users, the results indicate that *Keeping the meaningful* plays a role as a motivator. For update users, *Stimulation* was shown to be rather important, at least more important than *Money/ Luxury*. Users who reported to scrutinize permissions, ranked *Autonomy* and *Competence* higher than other needs. For users of screen lock with authentication, end-to-end encrypted instant messaging apps, and privacy settings of instant messaging apps, the results were inconclusive. Although differences in need fulfillment were found for some of the actions, general need fulfillment for all actions was rather low according to the mean values which were mostly below 3.0. The implications of this finding are discussed in Section 6.6.2.

6.6 DISCUSSION

The interview results indicate that users apply diverse security and privacy actions to protect themselves from threats on their smartphones. Furthermore, the interview results illustrate how a variety of psychological needs drive security and privacy actions on smartphones. For some of the security and privacy actions, namely backups, updates, and scrutinizing permissions, the results of the online survey are in line with the interview results. For the others actions (i.e. end-to-end encrypted instant messaging apps, and privacy settings of instant messaging apps) the results are inconclusive.

6.6.1 *Limitations*

The interviews were annotated with predefined concepts from theories of psychological needs. This is a subjective process and it might be that some quotes could be interpreted in a different way. The moderate interrater agreement indicates that the application of psychological needs in the context of security and privacy on smartphones may profit from further conceptualization and specification.

The interview study sample consisted partly of students and job seekers which might have led to the result that saving money was a rather salient motive in the decision making process. Despite this limitation, the interview sample reflects well the smartphone operating system distribution in the studied population.

Table 2: Mean (M), median (Md.) and standard deviation (SD) values for need fulfillment by security and privacy action. Highest mean and median value for each action in bold. AUT = Autonomy; COMP = Competence; STIM = Stimulation; MON = Money/ Luxury; SEC = Security; POP = Popularity; KTM = Keeping the meaningful; REL = Relatedness.

Need	**Backups**			**Updates**			**Scrutinizing Permissions**			**Password Lock**			**Privacy Settings**			**Encrypted Messaging**		
	M	Md.	SD	M	Md.	SD	M	Md.	SD	M	Md.	SD	M	Md.	SD	M	Md.	SD
AUT	1.71	1.50	0.89	2.05	1.25	1.25	**2.31**	**2.00**	1.10	**2.04**	**1.75**	1.06	**2.59**	**3.00**	1.00	2.12	1.50	1.33
COMP	1.96	2.00	0.84	1.89	1.50	1.09	2.14	**2.00**	0.78	1.82	1.00	1.12	1.73	1.50	0.82	1.96	1.50	1.23
STIM	1.36	1.00	0.60	**2.36**	1.75	1.33	1.28	1.00	0.55	1.39	1.00	0.74	1.77	1.00	1.15	1.77	1.00	1.24
MON	1.14	1.00	0.36	1.39	1.00	0.83	1.28	1.00	0.60	1.14	1.00	0.53	1.55	1.00	1.29	1.50	1.00	1.19
SEC	2.21	2.00	1.19	2.14	**2.00**	1.28	1.67	1.00	1.03	1.71	1.50	0.91	1.55	1.00	0.82	2.38	**3.00**	1.45
POP	1.50	1.00	0.76	1.73	1.00	0.98	1.39	1.00	0.78	1.21	1.00	0.58	2.09	2.00	1.30	1.62	1.00	1.26
KTM	**3.04**	**3.50**	1.34	1.70	1.25	0.85	1.47	1.00	0.74	1.64	1.25	0.84	1.73	1.00	1.03	1.96	1.00	1.42
REL	1.68	1.00	1.08	1.80	1.00	1.20	1.22	1.00	0.57	1.32	1.00	0.72	1.86	1.00	1.10	**2.50**	**3.00**	1.34

The online survey included a lot of questions as need fulfillment was collected for several security and privacy actions. By splitting the survey in three versions and considering only users of an action, the sample size for each action was rather small. However, presumably that helped to reduce possible fatigue effects. While the sample size limits the generalizability of the results, the study provides first insights into the practicability of applying the need fulfillment questionnaire in the security and privacy context.

6.6.2 *Psychological needs in the security and privacy context*

While *Security* was a salient need in the interviews, the online study results do not suggest *Security* as an outstanding motivator for security and privacy actions. A possible explanation for this difference may be the twofold definition of the need for *Security*: In the interviews *Security* was mentioned mostly in the sense of being safe from threats and uncertainties. In the questionnaire which was used in the online study, the *Security* definition is broader and encompasses, besides the aspect of protection, also the aspect of routine and structure as a source for feeling secure [175] [47]. While users might associate being safe from threats with data security and privacy actions, this might not be the case for the aspects related to daily routines.

Moreover, while *Security* may serve as a motivator to employ security and privacy actions, the fulfillment of the *Security* need may not necessarily lead to a strong positive user experience: in related work by Hassenzahl et al., *Security* has been found to be of only minor importance for positive user experiences with technology [85]. In addition, in their study, the need for *Security* also showed only a low correlation with positive affect [85]. Hassenzahl et al. thus suggest that "Security can be understood as a 'deficiency need', i.e. a need that creates negative affect if blocked, but not necessarily strong positive feelings if fulfilled" [85, p. 358]. This is also in line with findings of Karapanos et al. [108]: In a study on social media experiences with Whatsapp, they found that the need for *Security* was of least importance for positive experiences with this service. However, for negative experiences with Whatsapp, *Security* ranked second as a deprivated need [108]. Thereby, security and privacy related issues such as *exposing personal content to wrong addressees* or *unsolicited group participation* in chats were found to be sources for negative experiences. Building on the present findings and the findings from related work, it is likely that the user experience with security and privacy technologies and actions may profit from designing them in such a way that also psychological needs beyond the need for *Security* are addressed. Section 6.6.3 discusses how different psychological needs could be addressed for security and privacy actions.

Although the need for Money/Luxury was rather salient in the interviews, the online survey did not provide further evidence. Furthermore, in related works the need for Money/Luxury has been found to be only of minor importance as intrinsic motivator [175]. The difference between the interview results and the online study might have resulted from the fact that the need for *Money/Luxury* was interpreted in the interviews to include the desire to save money. However, this desire could be an extrinsic motivational factor rather than an intrinsic motivational factor (psychological needs are considered as intrinsic motivators). Thus, saving money may not lead per se to a positive user experience and may be a necessity rather than a reason.

During the analysis of the psychological needs in the interviews, a number of assumptions regarding their interpretation have been made. The desire for privacy has been interpreted as being related to *Autonomy*. The online survey results partly support this notion: for users who scrutinize permissions they indicate that *Autonomy* and *Competence* play a major role as motivators. However, for the use of privacy settings in messaging apps the results do not suggest that *Autonomy* is an outstanding need.

Pedersen [156] and Westin [200] suggest that there is a variety of privacy behaviors which are driven by different privacy functions such as autonomy, emotional release, self-evaluation, and limited and protected communication [200]. Including further privacy functions (besides *Autonomy*) may lead to a better conceptualization of psychological needs in the context of security and privacy research.

In comparison to results found in related work, need fulfillment in the online study was rather low (most mean values were below 3.0). For example, for satisfying life events, Sheldon et al. report mean values of need fulfillment between 2.4 and 4.1 [175]; in the context of technology usage, Hassenzahl et al. observed values between 2.9 and 3.3 [85]. A possible explanation is that, in contrast to Sheldon et al. [175] and Hassenzahl et al. [85], participants were not asked in the present studies to report on outstanding positive or negative experiences related to the studied topic (i.e. security and privacy actions in this case).
On the other hand, the results may also suggest that need fulfillment for security and privacy actions is in general low. This consequently encourages new approaches to design security and privacy actions in such a way that need fulfillment is maximized.

6.6.3 *Psychological needs as design inspiration*

Addressing different psychological needs in security and privacy technologies for smartphones creates a new design space for positive user experiences with such technologies. In the following, examples

of how security and privacy technologies that support psychological need fulfillment could look like are provided.

Authentication

The user experience of password locks may be improved by addressing additional needs besides *Security* such as *Stimulation* (e.g. by making unlocking fun) or *Popularity* (by having a "cool" screen lock). There are a few examples for addressing *Stimulation* in terms of joy during authentication: related work shows that for instance gesture-based authentication is able to evoke different positive emotional outcomes. Aumi and Kratz [6] present an authentication system which is based on in-air gestures performed in the vicinity of a portable device. In a user study they show that the gestures' security is positively correlated with ratings of pleasantness and excitement. Moreover, Karlesky et al. [110] find full-body gestures for access control to provide a potential for interactions which are perceived pleasurable by users. *Popularity* in authentication mechanisms could be addressed by providing users with a "cool" authentication method. For example, Bhagavatula et al. find that fingerprint authentication on smartphones is perceived as "cool" [14]. Also, many solutions to improve usability of knowledge-based authentication methods have been suggested in the domain of graphical authentication [17]. In graphical authentication, the password is based on graphical data such as pictures or icons. In Chapter 10, a graphical authentication scheme which uses Emoji-based passwords is investigated regarding its potential to provide for better need fulfillment and a positive user experience.

Updates

Participants in the present study mentioned installing updates to get the newest version of an app. By definition, experiencing new things is associated with the need for *Stimulation*. However, this applies only if the new experience is positive. Vaniea et al. [192] observed that users become frustrated when installing updates, if the updates feature new user interfaces which interrupt the users' normal workflow. Thus, updates are a two-edged sword: on the one hand they are able to positively surprise users when new functionalities or features are added to an app, thus addressing the need of *Stimulation*. On the other hand, users who have had bad experiences with installing updates may refrain from installing them in the future which may lead to security vulnerabilities [192]. One option to avoid negative effects on users' security behavior is to separate security updates from other updates [102]. Thereby, in the best case, users will not experience any changes after installing a security update. Nevertheless, it may also be the case, that updates just for security purposes are not deployed. Thus, an approach based on psychological need fulfillment could be

to motivate users to install security updates by connecting these updates with stimulating experiences. For instance, appraisal messages could be shown or gamification approaches could be used to achieve such experiences. How approaches that address psychological needs in update messages could look like in detail, is an interesting research question for future studies.

App Permissions

Not only in the present studies, but also in other studies, app permissions proved to be hard to understand by some of the participants (cf. e.g. [61]). As a consequence, the psychological need of *Competence* may be deprived. On the other hand, the present results suggest that users appreciate having the possibility to autonomously select which permissions they grant (for instance with respect to location data). Providing users with a clear context to make a decision is in any case recommendable [69]. Related work also indicates that a clear context supports security-friendly decisions when granting permissions [79, 120]. Whether this approach is also capable to address users' need for *Competence* and inducing a positive user experience is a subject for future studies. Another worthwhile topic, which is investigated in Chapter 9, is, to which degree run-time permissions (as currently featured in iOS and Android 6.0) are perceived as fulfilling the need for *Autonomy* without being annoying.

7

IMPLICATIONS OF THE QUALITATIVE STUDIES

Based on the findings of Chapter 5 and Chapter 6, implications for the experiential design of mobile security and privacy mechanisms are in the following discussed. The derived implications provide answers to RQ3.

Security/privacy by design and default in social apps. Avoiding user involvement in security and privacy decisions whenever possible, has been also suggested in earlier works [39, 69]. Furthermore, one of the lessons learned from related work is that defaults should be safe and secure [69].

The results of the focus groups study also suggest that security by design and default would be reasonable means for messaging apps to counteract negative experiences related to social interaction such as "social pressure" or "social availablility". That way, users do not need to make a trade-off between security and the need for *Relatedness* (e.g. by deciding for an app which is less secure, but has a higher adoption rate among one's circles). Also in the interview study, users mentioned *Relatedness* (in terms of being in contact with friends) rather than *Security* as a reasons for the adoption of messaging apps. This is line with related work that also has found that peer influence is an important reason for the adoption of secure and "insecure" messaging apps [45].

The results from the focus groups study further suggest that, privacy by design, for example, in the form of privacy settings for social apps would be crucial in such apps to counteract "social availablility". However, to design effective privacy controls, designers should be aware of pitfalls that should be avoided as, for example, elaborated by Lederer et al. [134]. The ability of messaging apps to change social norms in terms of expectations regarding availability has also been found as a source for negative experiences with mobile communication in related work [108].

Usability and Education. In the focus group study, users reported negative experiences that surfaced in feelings such as dependency and helplessness. For example, users mentioned feelings of dependency upon the security and privacy mechanisms provided by third parties (e.g. encryption) which do not have tangible indicators of the actual security. Or, the feeling of helplessness was expressed regarding threats to one's privacy. Another example is the feeling of having no choice and thus being forced to *sacrifice security for usage*. These

findings suggest that there is a need for usability improvements, for example, in terms of clearer communicating privacy information or the actual security state of the system.

Usability engineering techniques should help to make the interaction and communication with mobile security and privacy mechanisms more efficient, effective, and satisfying. Examples of usability engineering for security and privacy mechanisms have been widely presented in the literature (for an overview cf. to Cranor and Garfinkel [40] and Garfinkel and Lipfort [69]). Good usability is not only needed to make security and privacy mechanisms more effective and thereby more secure (cf. e.g. [19]). As in the user experience research of interactive products (cf. e.g. [85, 132, 165]), also in USP research usability should be considered as a necessary mean to avoid negative experiences. Thus, good usability should contribute to making a system more secure *and* easy to use, and thereby laying the foundation for a positive user experience (for which additional enablers are necessary).

The issue of user education in the context of security and privacy has been also recognized in earlier works (cf. e.g. [39, 69]. This issue also surfaced in the focus group study: users expressed the need to *inform oneself* about security and privacy issues and to take *individual responsibility* which suggests that it would be helpful if mobile security and privacy mechanisms would foster education on security and privacy issues. For example, for decisions that concern privacy, human-readable privacy and/or trust indicators could be made available to raise awareness towards security or privacy related topics and to help users in making fast decisions that are not based on unmerited trust.

Experience design beyond Security The focus group study presented in Chapter 5 revealed that negative experiences with mobile security and privacy surfaced in negative feelings such as dependency, helplessness, and fatalism. It is likely that those issues are not solely consequences of bad usability, but that they are also consequences of psychological need deprivation. The interview study in Chapter 6 further suggests, that users had motivations beyond the need for *Security* to use mobile security and privacy mechanisms, but the fulfillment of the need for *Security* was rather low in the online study.

Consequently, mobile security and privacy mechanisms should also (stronger) address needs beyond the functional (i.e. behavioral needs/goals [81]) and beyond the need for *Security*. Designing for psychological needs is an approach that could be also applied in the design of such mechanisms. For instance, a screen lock could be designed to address aspects of *Popularity* or *Stimulation*, or user interfaces for app permissions could be designed to address aspects of *Autonomy*.

Part IV

QUANTITATIVE STUDIES

8

COMMUNICATING APP PERMISSION RISKS TO USERS

8.1 STUDY 4: MOTIVATION

In Chapter 3, the issue of over-privileged smartphone apps was described. An app is over-privileged when it asks for more permissions than would be necessary to ensure its functionality [60]. This is not necessarily due to malicious intents of the developer, but may be also due to the programmer's lack of understanding [60][1].

In any case, the user needs to make a decision on whether s/he wants to grant permissions or not. Several studies have shown that it is hard for users to cope with the "basic permission dialog". For example, there are a number of usability problems with the current Android permission system - a large percentage of users are unaware of what permissions mean and what the possible consequences are [61]. Thus, most of the users might not be able to distinguish whether the requested permissions are indeed required to ensure the claimed functionality. Another drawback which makes it difficult for users to pay attention to permissions and thus to possible privacy issues is the time at which the permissions are shown to the user [112]. In the "basic permission dialog", the permissions are shown when the decision for downloading an app has already been made. Thus, the user cannot include the number and quality of required permissions in the decision-making process.

The focus group, interview, and online studies, presented in Chapter 5 and 6, provided further evidence for the issues identified in related work (cf. preceding paragraph): users reported a dependency on third parties regarding the management of security and privacy, e.g. by using the app market/ecosystem (cf. Section 5.3.2), helplessness towards the loss of control to their privacy (cf. Section 5.3.2), and uncertainty about which permissions they granted (cf. Section 6.4.7). Also, the results of the interview study suggest that users appreciate *Autonomy* in selecting which permissions they grant (cf. Section 6.4.7).

Chapter 5 and 6 further helped to identify three principles for the experiential design of mobile security and privacy mechanisms: *secu-*

1 The present chapter is based on "Using statistical information to Communicate Android Permission Risks to Users" by Lydia Kraus, Ina Wechsung, and Sebastian Möller [120], which appeared in the Proceedings of the Workshop on Socio-Technical Aspects in Security and Trust, co-located with the 27th IEEE Computer Security Foundations Symposium, Vienna, July 2014. Copyright © 2014, IEEE. http://dx.doi.org/10.1109/STAST.2014.15

rity and privacy by design and default for social apps, *usability and education*, and *experiential design beyond Security*.

The present chapter introduces an approach to provide users with additional information in form of statistical data about the number of app permissions compared to other apps with similar functionality. The goal is to help users to easier interpret permission requests without the need to search the app market for information (thus, targeting improved *usability* in terms of efficiency), to raise awareness of the permission issue (thus, targeting *education*), and to include the number of permissions in the decision-making process (thus, targeting *usability* in terms of effectiveness).

There are huge differences in permissions between apps with same or similar functionality (cf. Table 3). Thus, presenting statistics should be a suitable method to communicate the uncertainties that are associated with the permission system. Moreover, statistics give users the freedom to evaluate the risk on their own without pushing them in one or the other direction by defining which threshold is "good" or "bad". It is expected that this approach can support users' decision-making without requiring them to understand the exact meaning and implications of each permission.

8.2 USER INTERFACE DESIGN

A textual ("Text UI") and graphical permission UI ("Graphic UI") were designed to communicate the statistical information to users. In a lab study, both UIs were evaluated and compared against the "basic permission UI" regarding their influence on users' behavior when selecting apps, their usability, and their ability to address aspects of user experience.

8.2.1 *Extracting statistical information about apps*

Although several works on the automatic analysis of Android app permissions had been published at the time when the presented UIs were designed (cf. e.g. [11, 60, 67, 161, 169], non of them provided descriptive statistics by app functionality which would have been needed for the presented UI. Thus, the statistical information was manually extracted. However, since the present study was conducted, an approach for automatically detecting apps of similar functionality has been suggested [138].

Statistical information on the number of permissions (minimum, maximum, mean, median, 1st and 3rd quartile) was manually collected for three types of app functionality: weather forecasts (weather), torches (torch), and memory games (memory). The reason for this selection was the high number of apps providing this functionality which helps to provide a rich statistic. Furthermore, the functional-

ity of these apps should be easy to understand by users, as most of the people should know what a weather forecast, a torch and a memory game are. Of course, the pure number of permissions is still not enough to exactly evaluate the privacy-intrusiveness of an app. This issue, as well as the requested types of permissions, should be taken into account in future studies. The presented interfaces are a first approach to determine how statistical information in the context of Android permissions affects users and their decision making.

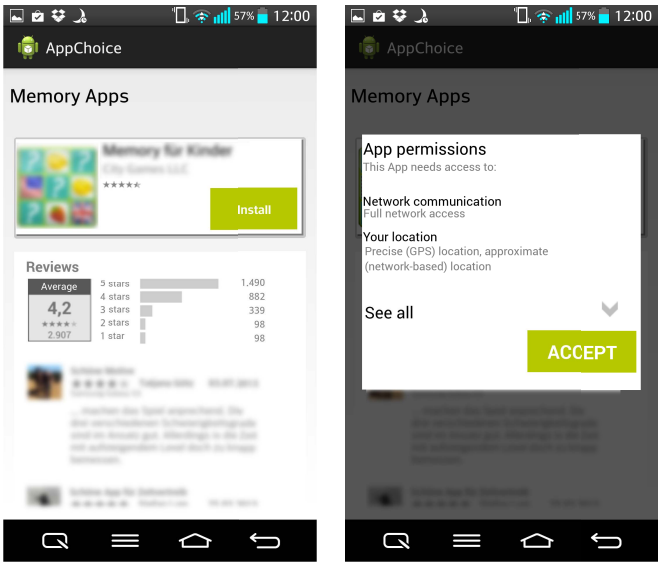
To collect statistical data about permissions by app functionality the German version of the Google Play Store was accessed in July 2013 with a Sony Xperia S smartphone. To find weather forecast apps, the search terms "weather forecasts" was entered (in German). For torch apps and for memory games the search terms "torch" and "memory", respectively, were entered (also in German). The first 200 results of each search were scanned. Only free apps and apps with basic functionality were selected (e.g. for weather apps features like forecast, rain radar and widgets were selected, but apps with special features such as wind, boating, and bike forecasts, as well as weather alerts were excluded). For torch apps, apps with all kind of lighting functionality were selected and also flashlights. For memory games, apps with and without online score functionality were selected. After removing apps with non-basic functionality from the initial list (N=200 for each category) 111 apps remained for weather, 192 for torch, and 133 for memory (for summary statistics cf. Table 1). Different ideas for the interfaces were collected in an ideation session.

Table 3: Descriptive statistics of number of permissions for the three app categories.

Category	Permission statistics					
	Min.	1st Quartile	Median	Mean	3rd Quartile	Max.
Weather	1	3	5	5.53	7	18
Torch	0	3	5	5.14	6	19
Memory	0	3	4	5.84	7	16

8.2.2 *Presenting statistical information about apps*

Similar to the privacy check list in Kelley et al. [112] and the personal examples of permission granting consequences in Harbach et al. [79] and the additional explanatory text in Benton et al. [13], the permissions are shown as part of the Google Play description of an app in the conceived UI, that is, before the decision to download an app is made. Moreover, those three examples from related work provide more information to users, but they do not allow to make direct com-



(a) "Standard UI". (b) Permission dialog.

Figure 8: Original "Standard UI" (left). After pressing the installation button, the permission dialog appears (right). Copyright © 2014, IEEE.

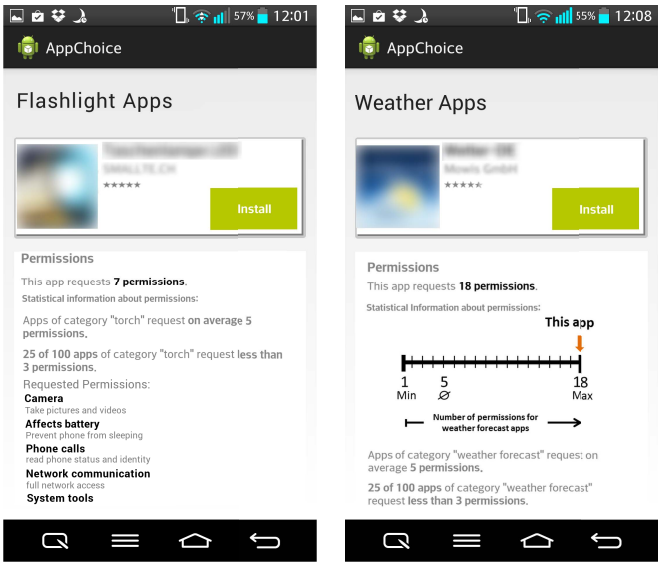
parisons with apps of similar functionality without navigating away from the description of the app.

Egelmann et al. [53] showed that it is fruitful to present apps of similar functionality and their requested permissions side-by-side – in a choice architecture. However, the space of a smartphone screen is limited, thus the number of apps with similar functionality which are presented side-by-side is limited as well; this issue could be solved by providing statistical information instead.

Standard UI

Three kinds of UIs were evaluated in the lab experiment. The "Standard UI" is the control condition and was designed similar to the "basic permission dialog" as it was featured in Google Play at the time of the study (summer 2013). The "Standard UI" provided the user with the most important information including three screenshots of an app, a textual description of the app, star ratings, number of downloads, and six reviews of other users (cf. Figure 8). The permissions of an app are only visible in a pop-up window after the "install" button is pressed.

The second user interface called "Text UI" (cf. Figure 9a) and the third called "Graphic UI" (cf. Figure 9b) provide additional statistical information beneath the app description, thus information about permissions is shown before pushing the "install" button.



(a) "Text UI". (b) "Graphic UI".

Figure 9: "Text UI" (left) and "Graphic UI" (right). The original UIs were in German.

Text UI

The textual prototype provided the users with the number of permissions of the current app, the mean, and the 1st quartile of the permission statistics of the category of the current app. Based on Hoffrage et al. [92] who stated that it is helpful when statistics are communicated to people in natural numbers, the 1st quartile information was provided in natural numbers (using the term "25 of 100 apps" instead of "25% of apps"). The information was placed directly below the app description. Also, the list of permissions of the current app was put below the textual information. After pressing the "install" button, users see again the pop-up window with the permissions which they need to accept in order to install the app, as in the "Standard UI".

Graphic UI

In the graphical prototype, users were provided with text and a graphic about the number of permissions of the current app, the minimum, the maximum, the mean, and the 1st quartile (cf. Figure 9b). Visual information was presented in the "Graphic UI" in the form of a horizontal risk ladder. The risk ladder allowed to show additional textual information without the necessity of scrolling. Earlier research has shown that risk ladders help people anchoring a risk more effectively as it provides them with upper and lower reference points [139]; moreover, lengths are usually perceived by people without bias [139]. The scale of the risk ladder was linear from the minimum to the maximum number of permissions used in one category. The text

below the risk ladder was the same as in the "Text UI". Also the list of permissions was given below the text.

8.3 METHODOLOGY

The study was implemented as a lab experiment in which participants were required to bring their own smartphone in order to create a more realistic setting. Participants were recruited through a participant panel of TU Berlin, classified ads posted on an online service similar to Craigslist, flyers, and e-mail. Experimental sessions took between 60-90 minutes, for which participants were compensated with 15 Euro. After welcoming participants received a description of the study and a consent form. The study followed a within-subjects design to increase the power of the statistical tests. The experiment consisted of three parts so each user had to make three decisions. In each part, participants were shown one of the UIs and presented with two different apps of the same functionality, one app with a high number of permissions and the other one with a lower number of permissions. After both apps were presented, participants were asked to decide for one app and to install it on their phone.

An app called "AppChoice" (designed for the experiment) led the participants through the experiment and presented them with a custom app store. In order to counterbalance possible influencing factors (e.g. user reviews, graphical design, user ratings, number of downloads), mock-up apps were used instead of real apps, but the participants were unaware of this fact. To maintain the impression that the participants were confronted with real apps, a push-message was simulated (a moving arrow-icon shown when apps are downloaded together with the message "app is being installed") after the installation button was pressed. To avoid that participants uncover this simulation, they were asked to not navigate away from AppChoice during the experiment. To evaluate whether there is an effect of the permission ratio (the ratio between the number of low permissions and the number of high permissions within the functionalities) different permission ratios were selected for each functionality. Thereby, weather was randomly selected to have the high ratio, torch to have the medium ratio and memory to have the low ratio, as the descriptive statistics of all three functionalities looked similar (cf. Table 1). This selection resulted in a high ratio for weather 18 (maximum) vs. 4 (interquartile range) per-missions, a medium ratio for torch 7 (interquartile) vs. 2 (below 1st quartile) and a low ratio for memory 4 (interquartile) vs. 0 (minimum) permissions.

The used mock-up apps were inspired by real apps. Pictures from low ranked apps of Google Play were taken (less than rank 50 on the search results), to avoid asking people to download apps which they already might have installed. Two sets of typical permissions

for each functionality (i.e. a set of low permissions and a set of high permissions) and two sets of user reviews from highly ranked apps of that functionality were chosen.

The order of appearance of the two apps with the same functionality on the overview page was randomized. The order of the functionality (weather, torch, memory) was also counterbalanced. The user interfaces were always shown in the order "Standard UI" – "Text UI" – "Graphic UI". As the salience of the permissions increases in strength from "Standard UI" to "Graphic UI" this order always remained the same to avoid priming effects.

8.3.1 *Procedure*

Participants for the study were recruited with classified online ads on Ebay, classified ads of a city magazine and a participant recruitment tool of Technische Universität Berlin. The study targeted German-speaking Android phone owners willing to install Android apps on their own device during the study.

During the experiment, participants were first given a demographic questionnaire. Then they were asked to rate the (general) importance of eight factors for their decision on a 7 point scale (1 = not important at all, 7 = very important). The decision factors were: description of the app, visual impression of the app, reviews provided by other users, ratings (number of stars), number of downloads, permissions requested by the app, provided functionality (according to description), publisher (company). After each installation they were again asked to fill in the questionnaire about the decision factors. User experience was measured in terms of perceived privacy of and the trust in both, the selected and the not selected app, a continuous scale ranging from "low" over "medium" to "high" (min. = 0, max. = 21) was used. To cover up that privacy and trust were the most important items, four questions regarding the overall rating of the apps and impressions about aesthetics and the like were mixed in. The AttrakDiff2 mini questionnaire was deployed to determine how the participants perceived the presentation of the apps in the app store in terms of pragmatic and hedonic quality. After the 3rd and last installation participants were presented with a questionnaire about privacy concerns, with the Global Information Privacy Concern [141]. All interactions with AppChoice were logged during the experiment. Participants were asked for consent before the experiment, and were debriefed at the end of the experiment. When the participants arrived in the lab they were told that the objective of the experiment is to investigate people's impressions of Android apps. Privacy or security related issues were not mentioned. After the installation of AppChoice on the participant's device, they were told that the presented apps are from the "app store". Within the experiment the participants were sup-

posed to decide for one of the apps with the same functionality after an exploration phase of maximum 5 minutes. Participants were also informed that they may uninstall all apps that were installed during the study after the study has finished.

8.3.2 *Participants*

Fourty-eight (48) smartphone users participated in the study. The sample was 50% female. Participants were between 18 and 60 years old (M = 31.68, Md. = 28, SD = 11.70). Sixteen (33.3%) participants had a secondary school degree or a lower school degree, 19 (39.6%) had a qualification for university entrance, and 13 (27.1%) had a university degree. All kind of occupation groups were covered including 14 employees (29.2%), four self-employed (8.3%), 15 students (31.3%), three apprentices (6.2%), four pupils (8.3%), two pensioners (4.2%), one housewife or stay at home husband (2.1%), three unemployed (6.2%) and two others (4.2%). All participants were Android users and used phones with Android versions 2.1, 2.2, 2.3, 4.0, 4.1 and 4.2.

8.4 RESULTS

In this subsection the results of the experiment in terms of installation rates, the importance of the number of permissions as a decision factor, the perceived privacy of and trust in the low- and high-permission app, as well as the importance of the other decision factors are reported.

To test different dependent variables for differences between the UIs, the following tests have been conducted. Due to the within-subjects design, the samples of the dependent variables were dependent (i.e. repeated observations). In cases where the dependent variable was dichotomous, a Cochran's Q test was used. In case of an interval-scaled dependent variable, a repeated-measures ANOVA was used, under the condition that the sphericity assumption was met (tested with Mauchly's test).

Moreover, there were two cases in which the dependent variable was based on independent samples, that was when it was tested for differences between the permission ratios and differences between different groups of privacy concern, both tested per UI. In those cases and when the dependent variable was dichotomous, a χ^2-test or a Fisher's exact test (if cells contained values below 5) were used.

8.4.1 *Installation rates*

Comparing the three decisions of all participants

To compare the number of low- and high-permission installations (hereafter referred to as "installation rate") for the three decisions of all 48 participants, a Cochran's Q test was used. The test revealed a significant difference in the installation rate of the low-permission app between the three types of user interfaces, $Q(df=2, N=48) = 6.07$, $p_{1-tailed} = 0.03$. A pairwise comparison using McNemar's test with Bonferroni-correction revealed that significantly more participants selected the low-permission app in the "Graphic UI" (79.17%) than in the "Standard UI" (56.25%) ($p = .01$). The differences between "Text UI" (66.67%) and "Standard UI" and between "Graphic UI" and "Text UI" were not significant.

Installation rate as a function of the permission ratio

Furthermore, for each UI, the installation rates of the weather, torch, and memory app were compared. A Fisher's exact test did not reveal significant differences in the installation rate between the three permission ratios (operationalized as weather, torch and memory).

Installation rate as a function of privacy concern

Participants were divided into groups of low, medium, and high privacy concern, according to their ratings of the Global Information Privacy Concern scale [141]. For all UIs, a χ^2-test showed no significant difference in the app installation rate between participants with low, medium, and high privacy concern.

8.4.2 *Decision factors*

Importance of the number of permissions as a factor for the app selection

A repeated-measure ANOVA was used to compare the mean importance of the number of permissions as a decision factor for the three decisions of all 48 participants. The importance of the number of permissions as a decision factor differed significantly between the UIs, $F(2, 90) = 22.01$, $p<0.01$, $part.\eta^2 = .328$. A Sidak-corrected post-hoc analysis showed that the mean importance in the "Standard UI" ($M=3.41$; $SD=2.21$) was significantly lower than the mean importance in the "Text UI" $M=5.11$; $SD=2.10$), $p<.01$, and the "Graphic UI" ($M=5.41$; $SD=2.04$), $p<.01$. Between "Text UI" and "Graphic UI" the post-hoc test indicated no significant difference.

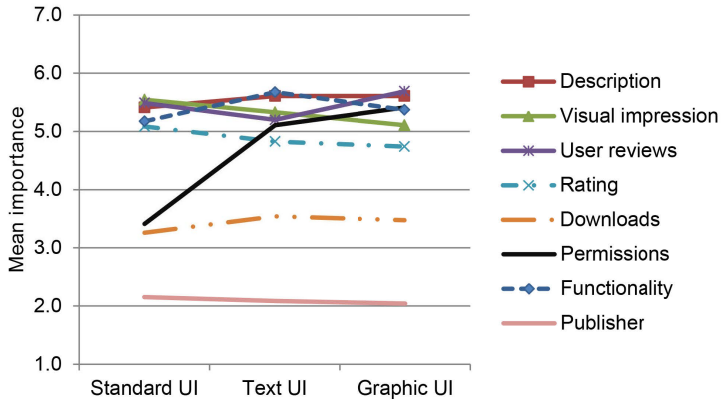


Figure 10: Decision criteria.

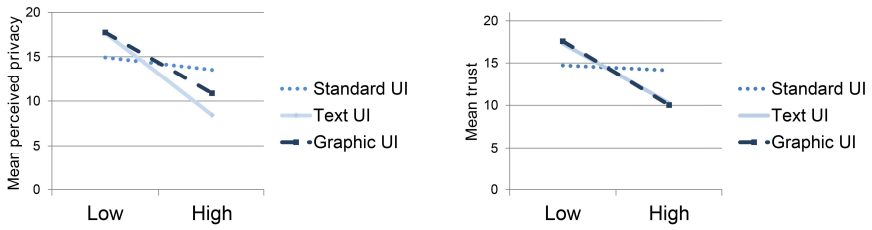
Importance of other decision factors

In addition to the importance of the number of permissions, other decision factors were analyzed. Rated on a 7-point scale from 1 (not important at all) to 7 (very important), description, functionality, user reviews, visual impression and ratings were rather important for the participants and received mean values between 5.09 and 5.69. Publisher (2.04-2.15) and number of downloads (3.26-3.48) were not as important for the participants. A pairwise comparison of the decision factors with Bonferroni-correction showed no significant difference for all factors (except permissions, cf. paragraph above) between the UIs. Figure 10 depicts the mean values of the decision factors for the three UIs.

8.4.3 *Interrelation between number of permissions, perceived privacy and trust*

A repeated-measure ANOVA was used, with UI and permission level (low and high) as within-factors, to compare the difference in *perceived privacy* between the low-permission app and the high-permission app for each UI. There was a significant difference for perceived privacy between the low-permission app and the high-permission app, $F(1, 36) = 55.97$, $p < 0.01$, $part.\eta^2 = .609$. A pairwise comparison using Bonferroni-correction revealed that for the "Text UI" and the "Graphic UI" the low-permission app had a significantly higher perceived privacy than the high-permission app (cf. Figure 11a and Table 4).

There was also an interaction effect between UI and permission level, $F(2, 72) = 14.21$, $p < 0.01$, $part.\eta^2 = .283$. A pairwise comparison using Bonferroni-correction revealed that the low-permission app had a significantly higher perceived privacy for the "Text UI" ($p = 0.011$) and the "Graphic UI"($p < 0.01$) compared to the "Standard UI" (cf. Figure 11a). The high-permission app had a significantly lower



(a) Perceived privacy. (b) Trust.

Figure 11: Perceived privacy and trust for the low and the high permission app.

perceived privacy for the "Text UI" ($p < 0.01$) compared to the "Standard UI" (cf. Figure 11a).

To compare the difference of *trust* in the low-permission app and the high-permission app for each UI, again a repeated-measure ANOVA with the UI and permission level as within-factors was used. There was a significant difference between trust in the low-permission app and the high-permission app, $F(1, 40)= 36.05$, $p<0.01$, $part.\eta^2=.474$. A pairwise comparison using Bonferroni-correction revealed that for the "Text UI" and the "Graphic UI" the low-permission app had a significantly higher trust rating than the high-permission app (cf. Figure 11b and Table 4). There was also an interaction effect between UI and permission level, $F(2, 80)=5.56$, $p< 0.01$, $part.\eta^2 = .122$. A pairwise comparison with Bonferroni-correction revealed that the low-permission app had a significantly higher trust rating for the "Graphic UI"($p<0.01$) compared to the "Standard UI".

8.4.4 *Pragmatic and hedonic quality of the UIs*

The AttrakDiff 2 mini ratings revealed that the participants perceived the presentation of the apps in the app store for all three UIs as highly pragmatic and attractive (cf. Table 5). A repeated measures ANOVA revealed a significant difference in pragmatic quality between the UIs, $F(2, 92)=3.80$, $p = 0.26$, $part.\eta^2 = .076$, with a small effect size. Post-hoc analysis with Bonferroni-correction revealed that the presentation of the apps which included the "Graphic UI" received higher pragmatic quality ratings than the "Standard UI", $p=0.14$. Hedonic quality was perceived medium-high for the presentation of the apps in the app store for all three UIs (cf. Table 5). For hedonic quality and its sub-dimensions, as well as attractiveness, repeated measure ANOVAs did not reveal significant effects between the UIs. The latter finding suggests that the additional statistical information did not negatively impact the hedonic quality ratings, however, it also did not improve it. The high PQ and medium-high HQ ratings further suggest that the users perceived the presentation of the apps in the app store for

Table 4: Perceived privacy and trust in the low- and high-permission app, rated on a continuous scale from 0 (low) to 21 (high). Significant differences between means in bold, pairwise comparison, Bonferroni-corrected. © 2014, IEEE.

UI	Perm.	Perceived Privacy/Trust	Diff. high−low	p-Val.
Stand.	low	M = 14.92/14.71 (SD = 5.30/5.53)	Priv.: −1.42	Priv.: 0.086
	high	M = 13.5/14.12 (SD = 4.79/5.41)	Trust.: −0.59	Trust.: 0.64
Text	low	M = 17.67/17.30 (SD = 5.13/5.25)	Priv.: −9.24	Priv.: <0.01
	high	M = 8.43/10.24 (SD = 5.91/5.92)	Trust.: −7.06	Trust.: <0.01
Graphic	low	M = 17.74/17.59 (SD = 4.82/4.44)	Priv.: −6.87	Priv.: <0.01
	high	M = 10.87/11.02 (SD = 6.49/5.62)	Trust.: −6.57	Trust.: <0.01

Table 5: AttrakDiff2 mini ratings for the three UIs. Ratings of the same variable which significantly differ between the UIs are in bold.

	Standard UI		Text UI		Graphic UI	
	M	SD	M	SD	M	SD
Pragm. Quality	**5.55**	0.74	5.64	0.72	**5.76**	0.72
Hedon. Quality	4.65	0.68	4.68	0.99	4.68	0.71
HQ-Stim.	4.53	0.89	4.51	1.12	4.68	0.90
HQ-Identity	4.77	0.71	4.85	1.03	4.68	0.80
Attractiveness	5.28	0.79	5.38	0.90	5.41	0.90

all three UIs as task-oriented, i.e. helpful to fulfill their tasks (in this case the app selection).

8.5 DISCUSSION

8.5.1 *Limitations*

The experiment was intended to get a first impression on how statistical information in the app market affects users' decision making and perceived privacy of apps. Implementing the study as a lab ex-

periment allowed for a controlled setting and to give participants the impression of actually being in a choice situation with real risk. However, the lab experiment also limited the sample size compared, for example, to an online study. Due to the limited sample size a within-subjects design was chosen to increase the power of the statistical tests. Presenting the user interfaces in the same order for all participants might have led to learning effects. However, randomizing the order would have possibly led to priming effects as the salience of the permissions was higher for the "Graphic UI" compared to both other UIs. Nevertheless, the constant order of the UIs limits the validity of the results; in future studies a between-design could be chosen to circumvent this drawback. For the interface design only the number of permissions was considered and not the kind of the permissions themselves, i.e. whether some permissions cause stronger effects than others. Including this information should be a subject for future studies.

There are some limitations on the collection of statistical data in the app market in general. For this study, statistical information about apps with similar functionality was manually collected. In order to apply the concept broadly, an automated approach needs to be developed. Also, when apps with completely new functionality enter the market, it is difficult or impossible to collect statistical information. The same is true for apps of similar functionality with only few samples in the market. The presented approach might rather support users who search for apps with specific functionality than those who search for a specific app. Moreover, letting participants choose between only two apps and not between several apps is a limitation and should be addressed in future studies.

8.5.2 *Influence of statistical information about permissions on users' decision making*

The results of the study suggest that statistical information can affect users in their decision making and perception of privacy when selecting Android apps. When statistical information was provided in form of the "Graphic UI", participants decided significantly more often to choose the low-permission app. This indicates that if statistical information is included in the app market, it needs to be presented in an attention-catching way in order to influence users' behavior.

The results are in line with the findings of Kelley et al. [112] and Benton et al. [13]. Kelley et al. [112] found that including "only" a list of permissions in the app description before the download-decision is made did not show significant effects on users' downloading behavior. The list of permissions Kelley et al. is similar to the present "Text UI", although the "Text UI" contains more text (the statistical information) to explain the permission use. Also, Benton et al. [13] found that

providing additional explanation text about permission use did not significantly influence the installation rate. However, adding visual cues to the provided information had a significant effect on users' installation behavior for some experimental conditions [13]. The permission ratio did not show significant effects on the installation rate.

Furthermore, in the "Text UI" condition and the "Graphic UI" condition the additional statistical information influenced users to increase the importance of the number of permissions as a decision factor. This result indicates that providing comparative information before the decision is made helps the users to include the number of permissions in their decision making. This finding is in line with results of Egelmann et al. [53] who found that providing users with comparative information during the decision making led to higher valuation of privacy.

No significant differences for the installation rate were found between participants with low, medium and high privacy concern which suggests that participants were sensitive to the information, irrespective of their general concern. This is in line with results of Egelmann et al. [53], who also did not find a significant difference in the installation behavior of participants with low, medium and high privacy concern. Decision factors other than the number of permissions were not significantly influenced between the decisions. This suggests that providing additional comparative information about app permissions does not lead participants to exclude other decision criteria.

The present study has investigated the potential of statistical information to support users in privacy-aware decision making when selecting apps. While, in the meantime, the Android permission system has changed from install-time permissions to runtime permissions, the concept of statistical information on permissions could still be included into the app description in the app store. That way, participants could be informed about permissions already before installation, and they could further decide at runtime which permissions they would want to grant. Moreover, the concept of statistical information has also found attention in the design of runtime permission overviews on concurrent smartphones (cf. Figure 12). In the permission overview, users can see how many of the installed apps have access to each permission. This indicates that the concept is broadly applicable. A drawback is, however, that those statistics are deeply buried in the permission settings, an can be only seen if a user explicitly looks for this information. Furthermore, it would need to be evaluated in user studies whether the information in this form, is helpful for the users.

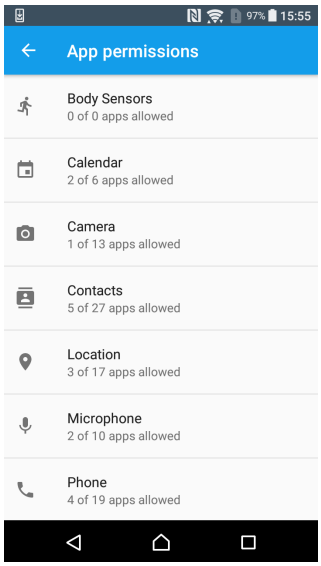


Figure 12: Screenshot of the permission overview on a Sony Xperia smartphone running Android M. Statistical information about each permission is provided beneath the permission name.

8.5.3 *Influence of statistical information about permissions on the user experience*

Statistical information in both, the "Text UI" and the "Graphic UI", also influenced users' perceived privacy of and trust in an app with respect to the number of permissions. Thus, with statistical information given, participants perceived the apps with a higher number of permissions less privacy-protecting and less trustworthy compared to the apps with a lower number of permissions. This results suggests that statistical information about permissions can have an effect on the felt experience with an UI. It further suggests that additional statistical information can help to raise awareness with respect to permission abuse.

The AttrakDiff2 mini ratings suggest that the presentation of the apps in the app store was perceived as task-oriented all three UIs, with high pragmatic quality ratings and medium-high hedonic quality ratings. The statistical information in the "Graphic UI" slightly positively influenced the pragmatic quality ratings of the app presentations, however, hedonic quality ratings (which were already medium-high) were not further affected by the UIs.

In summary, statistical information seems to have a positive impact on the usability (in terms of pragmatic quality) of the app presentation. Furthermore, it positively influenced users privacy perception and trust in an app with a low number of permissions compared to an app with a high number of permissions. Additionally, it supported participants in making more privacy-friendly decisions. There was no influence on the hedonic quality ratings of the app presenta-

tion between the UIs suggesting that positive experiential qualities of the presentation, which were already medium-high, were not further influenced by the statistical information.

9

UX OF RUNTIME AND SELECTIVE INSTALL-TIME DIALOGS

9.1 STUDY 5: MOTIVATION

In the preceding chapter, the deployment of statistical information about app permissions within the app market has been discussed as a design suggestion to influence users' awareness and decision making when granting install-time permissions. While install-time permissions were the predominant permission granting model in Android, smartphones featuring Android 6.0 or higher rely on a runtime permission model.

The goal of the present chapter is to gather first insights how different runtime UIs and alternative install-time UIs (with an option to selectively grant permissions) influence user experience and related behavior with permission dialogs[1]. How do run-time or selective install-time UIs influence users' decision making in an over-privilege scenario? How do users perceive the UX while interacting with different run- and install-time UIs? Does an explanatory text ("purpose string") influence users perception of the UIs?

Runtime permissions are supposed to be easier understandable for users as they are shown when an app requests access to sensitive resources; thus, users are provided with a context for decision-making. However, while runtime permissions seem to be a better choice for users than install-time permissions, they still have a few potential drawbacks such as being repetitive and interruptive [62]. An interesting question would be also whether runtime permissions help to evoke a feeling of *Autonomy* in users (cf. Chapter 5 and 6).

The runtime permission model in Android is implemented as follows [186]: When an app requests access to a sensitive resource a permission dialog is shown to the user. If the user denies the permission, the dialog is shown again the next time the app wants to access the respective resource. If, at the second time, users want to deny the permission, users can select the option "never ask again" if they do not wish to see the permission request for this app and the respective resource again.

The option to show permission requests several times is reasonable if the permission is indeed needed to ensure functionality. However, in an over-privilege scenario (i.e. a scenario in which an app requests

1 The present chapter is based on "Comparing the Influence of Different App Permission User Interfaces on User Experience and Behavior." by Lydia Kraus, Domenic Reuschel, Maija Poikela and Sebastian Möller, 2017. *Unpublished*.

more permissions than would be necessary to ensure functionality), this feature may be harmful to a user's privacy. If a user has denied the unnecessary permission, s/he will be asked again the next time the app accesses the resource. Thus, s/he might reconsider the denial of the permission. Besides the potential harm for privacy, it may be also annoying for users to receive multiple requests.

Lin et al. showed that users can be divided in different privacy preferences groups [137]. Thereby, the privacy preferences regarding permissions depend on the purpose for which data is being used. In iOS, developers have the possibility to add a short explanation ("purpose string") to the runtime permission request which states the purpose for which the data is being used [184]. In Android, if the user continues trying to access a functionality although the related permission has been denied before [186], developers can show an explanation *before* the runtime permission is being asked for the second time. However, adding an explanation dialog before a permission dialog may be annoying or confusing for users, as they may have the impression to agree twice to the permission [157].

In a study on iOS runtime permissions, Tan et al. showed that users were more satisfied when they were shown a purpose string within the permission request as compared to a permission request without purpose string [184]. In the benign (i. e. non-malicious) permission request scenario by Tan et al., users were also more likely to grant permissions when they received an explanation [184]. Westermann also showed in a lab study that participants who received a permission request to enable app notifications together with an app-customized explanation were more likely to grant the permission, given that they had noticed the custom explanation [199].

An alternative to avoid too many interruptions by Android runtime permissions would thus be, to already show a list of all needed permissions at install-time, together with an explanation of the purpose of use. As users criticized the lack of *Autonomy* when using traditional install-time permissions (cf. Chapter 5 and 6), they should have the possibility to already deny those permissions which they do not want to be again asked for in the future. Related work also suggests the usefulness of additional privacy information which is shown before installation in the app store [8]: this information may especially help privacy-concerned users to consider the privacy-intrusiveness of an app before installation [8].

As in iOS, in the present study, the explanations are included into the UI to avoid (as described above) that users need to confirm such a dialog twice. Furthermore, this design decision allows to compare the results to those of Tan et al. [184]. In contrast to Tan et al., the permission granting scenario in the present study is a malicious scenario implemented as an over-privilege attack.

9.2 METHODOLOGY

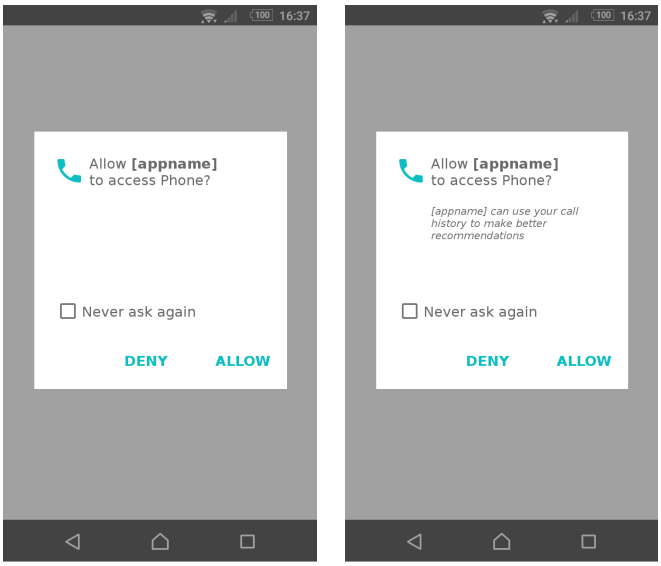
The online study followed a between-subjects design in order to not prime participants with the "purpose strings" or the other UIs. It was conducted in German in early autumn 2016. The survey was designed for desktop use and it was set up in Limesurvey – an open source survey tool[2].

9.2.1 *Procedure*

The link to the study was posted on the website of a participants recruitment tool from Technische Universität Berlin and distributed via e-mail. One thousand e-mails were sent to potential participants through the tool. When participants clicked on the link, they could register for the study. After having registered, they received a further link which led them to the survey. Ten retail vouchers worth 25 Euro each were raffled among all participants to incentivize participation in the study.

On the welcome screen of the survey, a short description of the study was provided together with the estimated response time (10 minutes). Security or privacy were not explicitly mentioned to avoid priming participants. Instead, the survey, which consisted of three parts, was promoted as a survey on mobile apps. Part one included demographic and smartphone usage questionnaires. In the second part, questions related to permissions were asked. Thereby, participants were randomly assigned to one of the four conditions (i.e. UIs). In each condition participants were presented with three kinds of apps in randomized order. Those apps included an app for learning English ("language app"), an app to support a 7 minutes work out ("fitness app"), and a gaming app for playing Hangman ("gaming app"). Due to the online study set-up, the apps were intentionally selected to provide a simple functionality that could be easily understood without using them. Furthermore, apps that were not among the most downloaded in their category were selected to avoid effects resulting from users' familiarity with the apps. The original apps have a low number of permissions: the language app originally requests the storage and the microphone permission, as well as the option to perform in-app purchases; the fitness app does originally not request any permissions; and the gaming app only requests access to in-app purchases. The threat model that is deployed in this study addresses the issue of over-privilege attacks. In these kind of attacks, apps require more permissions than they would need to ensure their functionality. Although the selected apps need few permissions in reality, it was pretended that they would each need a set of five permissions: Camera, Contacts, Storage, Location, Phone. This set of permissions

2 limesurvey.org



(a) (b)

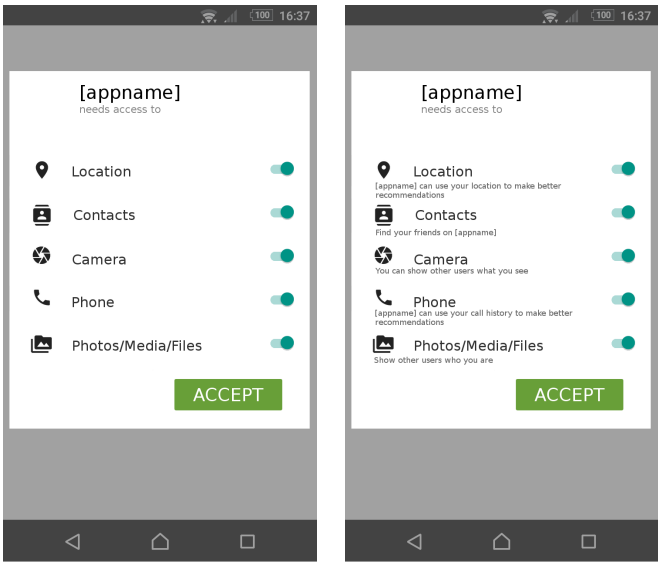
Figure 13: The runtime UI as currently featured in Android M (a) and the runtime UI with purpose string (b). The UIs that were used in this study were originally in German. Images by courtesy of Domenic Reuschel.

was used, as those permissions have been shown to evoke users' concern [59] and to be often requested [79].

Figure 13a shows the runtime UI used in this study. The design followed the currently featured runtime permission UI in Android M. To investigate whether users would make use of the "never ask again" option, this UI already contained this option, although in the real world, users would see this option only for the second permission request. Furthermore, the UI also allowed users who grant a permission to select the "never ask again" option. That way, it could be investigated whether users who grant a permission would be willing to reconsider their decision in the future. Figure 13b shows the runtime UI with purpose string.

Figure 14a shows the install-time UI which was designed similarly to the former install-time UIs prior to Android M. However, compared to formerly featured install-time UIs, the user can directly select in this prototype which permission to grant. Permissions were set to "allow" by default, assuming that the app would actually need the permissions to function correctly. For the install-time UI with purpose string (cf. Figure 14b) a purpose string is added beneath each permission.

To control for possible wording effects of the purpose strings, the purpose strings in the present study were the same for all apps (except for the app name). Also, Tan et al. [184] did not find an effect of the purpose string wording on the decision to grant a permis-



(a) (b)

Figure 14: The selective install-time UI (a) and the selective install-time UI with purpose string (b). The UIs that were used in this study were originally in German. Images by courtesy of Domenic Reuschel.

sion. However, wording may influence participants' user experience in a way that they may be less satisfied with the interface [184]. The wording of the purpose strings was as follows: **Contacts:** "Find your friends on [app name]." **Location:** "[app name] can use your location to make better recommendations." **Phone:** "[app name] can use your call history to give better recommendations." **Camera:** "You can show to other users what you see" **Storage:** "You can show to other users who you are."

Similar to Tan et al. [184], participants were first shown screenshots of an app together with a short description of the app. One of the screenshots was the overview of the app in Google Play where users could also see the star ratings given by other users. Ratings of the apps were similar (between 4.1 and 4.3 stars on average). The other screenshots showed how the app looks like when installed. Participants were then asked whether they had used the app before. Thereafter, an instruction stated that the participants should imagine that they had just downloaded the app (for the runtime UIs) or that they were about to download the app (for the install-time UIs) when the following dialog appeared. Participants were then presented with their UI and asked whether they would grant or deny the permission(s) for this app.

For participants in the runtime conditions, the presentation of the permission dialogs was done successively in a role play. After each permission, short instructions were given to present the next permission. Those instructions were worded "[On the next day/after a few

days/ after a week] you open the app again and the following dialog appears". This presentation the runtime permission UIs was meant to "simulate" the interaction that participants would normally have. Besides the option of granting or denying a permission, participants in the runtime condition further had the option to opt-in to the "never ask again" option. Also, the order of the permissions was randomized to avoid ordering effects.

For participants in the install-time conditions, the order of the permissions within the list was counterbalanced. Participants had to opt-out when they wanted a permission to be denied as in the interface the slider is also set by default to grant each permission.

After answering the first set of permission questions, they were asked whether they perceived the process of granting permissions as annoying. The answer scale was a 5-point scale from *1 = not annoying at all* to *5 = very annoying*. Furthermore, participants were asked about the experienced exhaustion during permission handling. The answer scale was an 8-point scale from *1= not exhausting at all* to *8 = exceptionally exhausting*. The answer options were based on the subjectively experienced exhaustion scale of Eilers et al. (in German) [55]. Thereafter, participants were presented with the next app.

In the third part of the study, participants were presented with questionnaires on user experience. Thereby, validated questionnaires from the literature were used: the German version of AttrakDiff 2 mini [86], the German version of the need fulfillment questionnaire [47] originally developed by Sheldon et al. [175], and a translated version [47] of the positive affect-negative affect schedule (PANAS) [196].

To make sure that participants paid attention during answering the questionnaire, several attention checking questions were placed within the survey. An example for an attention checking questions is the following: "If you read this question please select the answer 'rather agree' ". The answer scale for this question was a 4-point scale with the options *agree*, *rather agree*, *rather disagree*, *disagree*. It was also mentioned on the introductory screen that the survey would contain attention checking questions, however, it was not explained how these kind of questions would look like.

9.2.2 *Participants*

In total, 183 responses were received. Ten participants only filled the first few questions, thus their answers were removed. The answers of seven more participants were removed as they had answered at least two of the attention checking questions incorrectly. Furthermore, the answer of one participant who reported not to use a smartphone was removed. Thus, 165 participants remained (55.2% female; 43% male; 3% n.a.). Participants were between 18 and 67 years old (M = 29.2; Md.

= 27; SD = 10.0). Education levels were rather high (secondary school degree or no school degree: 9.1%, qualification for university entrance: 43% , university degree, including Bachelor's degree: 47.9%). Slightly more than half of the participants (55.2%) were students, followed by employees (22.4%), job seekers (6.7%), self-employed (5.5%), apprentices (3.0%), and other occupational groups (7.2%). The majority of the participants did not have professional IT expertise (80%).

There were 43 participants in the runtime UI group, 40 participants in the runtime UI with purpose string group, 40 participants in the install-time UI group, and 42 participants in the install-time UI with purpose string group. All participants owned a smartphone and had already installed apps in the past. There were 65.5% Android users, 29.7% iOS users, 2.4% Windows users, and 2.4% users of other platforms. Most of the participants (72.7%) have used a smartphone for more than three years.

9.3 RESULTS

This section presents the study results. To analyze effects on the user interface on behavior, the number of each granted permissions was compared between the UIs. It was also evaluated whether there is a difference in granting single permissions between the apps. Furthermore, the usage of the "never ask again" option was analyzed. Perceived UI quality was evaluated in terms of pragmatic quality, hedonic quality, and attractiveness. Felt experience was evaluated in terms of positive and negative affect and users' annoyance and exhaustion during the interaction.

To test different dependent variables for differences between the UIs, the following tests have been conducted. Due to the between-subjects design, the samples of the dependent variables were independent. Therefore, in cases where the dependent variable was dichotomous, a χ^2-test was used. In case of an interval-scaled dependent variable, a one-way ANOVA was used, under the condition that the assumption of homogenity of variances was met (tested with Levene's test). If the assumption of the homogenity of variances was violated, a non-parametric test was used. Moreover, there was one case in which the dependent variable was based on dependent samples (i.e. repeated observations), that was, when it was tested for differences between the three kinds of apps. In those cases and when the dependent variable was dichotomous, a Cochran's Q test was used. For post-hoc analyses Bonferroni-corrected p-values are reported. Effect sizes (r) were calculated for post-hoc analyses as $r = Z/sqrt(O)$ with O being the number of observations [63].

Of the 165 participants, nine reported to have used the language app before (5.5%), seven reported to have used the fitness app before (4.2%), and four reported to have used the gaming app before (2.4%).

Thus, the majority of the participants was not familiar with the three apps.

9.3.1 *Permission granting and privacy preferences*

Differences in permission granting between the UIs

The results revealed that – depending on the UI - participants granted a different number of permissions. The detailed results of the statistical analysis are reported in the following. χ^2-tests with Bonferroni-corrected post-hoc analysis were used to analyze differences in the frequencies of granting a permission between the UIs. The results of the tests are reported in Table 6.

Language app. Table 6 shows the percentages of participants that decided to grant a permission for the language app. The percentages of participants who granted a permission in the selective install-time UI with purpose strings were significantly higher compared to the runtime UI, for all five permissions. For the selective install-time UI, the percentages of participants who granted the Camera, the Contacts, and the Phone permission, were significantly higher compared to the runtime UI. For the Phone permission, there was also a significant difference between the install-time UI and the runtime UI with purpose string.

Fitness app. Table 6 further shows the percentages of participants who decided to grant a permission for the fitness app. For the Camera and Contacts permission there were no differences between the UIs. However, for the Storage and the Location permission, the percentages of participants in the selective install-time UI with purpose strings were significantly higher compared to the runtime UI with purpose strings. Also, participants in the selective install-time UI with purpose strings granted the Phone permission more often compared to those in the runtime UI condition.

Gaming app. Table 6 also shows the percentages of participants that decided to grant a permission for the gaming app. For the gaming app, the results were similar to the fitness app: for two permissions (Storage and Phone) participants in the selective install-time UI with purpose strings condition were more likely to grant permission compared to the runtime UI with purpose strings and the runtime UI (only for the Phone permission). The percentage of participants who granted permission to Contacts was higher in the selective install-time UI condition compared to the runtime UI.

In summary, participants in the install-time UI conditions were more likely to grant permissions compared to those in the runtime UI conditions, however, with a tendency of the selective install-time UI to lead to less privacy-conscious decisions than the install-time UI with purpose strings. For 10 of 15 permissions, participants in the

Table 6: Percentages of participants who granted a permission by app and UI (RT = runtime UI; RT purp. = runtime UI with purpose string; IT = install-time UI; IT purp. = install-time UI with purpose string). Significant p-values in bold. Percentages which differ significantly according to the post-hoc tests are indicated by differing indices.

		UI				Test Results
	Perm.	**RT purp.**	**RT**	**IT purp.**	**IT**	
Language App	**Camera [%]**	$14.3_{a,b}$	0.0_{b}	30.0_{a}	19.0_{a}	$\chi^2(3, N = 164) = 13.94$; $p = \mathbf{.003}$; $\phi = .29$
	Contacts [%]	$4.8_{a,b}$	0.0_{b}	20.0_{a}	21.4_{a}	$\chi^2(3, N = 164) = 13.89$; $p = \mathbf{.003}$; $\phi = .29$
	Storage [%]	$19.0_{a,b}$	7.7_{b}	35.0_{a}	$23.8_{a,b}$	$\chi^2(3, N = 163) = 9.02$; $p = \mathbf{.029}$; $\phi = .24$
	Location [%]	$14.3_{a,b}$	5.0_{b}	37.5_{a}	$19.0_{a,b}$	$\chi^2(3, N = 164) = 14.65$; $p = \mathbf{.002}$ $\phi = .30$
	Phone [%]	2.4_{b}	0.0_{b}	30.0_{a}	26.2_{a}	$\chi^2(3, N = 164) = 23.96$; $p < \mathbf{.001}$; $\phi = .38$
Fitness App	**Camera [%]**	9.3_{a}	7.5_{a}	27.5_{a}	16.7_{a}	$\chi^2(3, N = 165) = 7.79$; $p = .051$; $\phi = .22$
	Contacts [%]	11.6_{a}	2.6_{a}	20.0_{a}	21.4_{a}	$\chi^2(3, N = 164) = 7.55$; $p = .056$; $\phi = .22$
	Storage [%]	$11.6_{a,b}$	5.0_{b}	27.5_{a}	$19.0_{a,b}$	$\chi^2(3, N = 165) = 8,54$; $p = \mathbf{.036}$; $\phi = .23$
	Location [%]	$23.3_{a,b}$	12.8_{b}	42.5_{a}	$31.0_{a,b}$	$\chi^2(3, N = 164) = 9.38$; $p = \mathbf{.025}$; $\phi = .24$
	Phone [%]	7.0_{b}	$7.5_{a,b}$	30.0_{a}	$16.7_{a,b}$	$\chi^2(3, N = 165) = 10.99$; $p = \mathbf{.012}$; $\phi = .26$
Gaming App	**Camera [%]**	14.0_{a}	7.5_{a}	25.0_{a}	14.3_{a}	$\chi^2(3, N = 165) = 4.91$; $p = .178$; $\phi = .17$
	Contacts [%]	$4.7_{a,b}$	2.5_{a}	$17.5_{a,b}$	23.8_{b}	$\chi^2(3, N = 165) = 12,20$; $p = \mathbf{.007}$; $\phi = .27$
	Storage [%]	$11.6_{a,b}$	5.0_{b}	27.5_{a}	$11.9_{a,b}$	$\chi^2(3, N = 165) = 9.13$; $p = \mathbf{.038}$; $\phi = .24$
	Location [%]	11.6_{a}	7.5_{a}	27.5_{a}	14.3_{a}	$\chi^2(3, N = 165) = 7.01$; $p = .072$; $\phi = .21$
	Phone [%]	2.3_{b}	2.5_{b}	25.0_{a}	$11.9_{a,b}$	$\chi^2(3, N = 165) = 15.06$; $p = \mathbf{.002}$; $\phi = .30$

install-time UI with purpose string condition granted more permissions compared to the runtime UIs. For the install-time UI without purpose string, percentages only significantly differed in 4 of 15 permissions from the runtime UIs. The number of granted permissions in total was rather low (always below 50%).

Differences in permission granting between the apps

In summary, participants granted more often the Storage permission to the language app and the Location permission to the fitness app than to the other apps.

Cochran's Q was calculated to analyze whether there is a difference between the different types of apps in the number of granted permissions. The test did not indicate a significant difference between apps for the Camera and the Contacts permission. However, there was a significant difference between apps for the Storage permission, $Q(df = 2, N = 163) = 12.67$, $p = .002$. Post-hoc analysis with Bonferroni-correction revealed that the Storage permissions was granted significantly more often to the language app ($N = 35$) compared to the fitness app ($N = 26$), $p = 0.048$, and compared to the gaming app ($N = 23$), $p = .002$. There was also a significant difference between apps for the Location permission, $Q(df = 2, N = 163) = 20.78$, $p < .001$. Post-hoc analysis with Bonferroni-correction revealed that the Location permission was granted significantly more often to the fitness app ($N = 45$) compared to the language app ($N = 31$), $p = .009$, and compared to the gaming app ($N = 25$), $p < .001$. Finally, there was also a significant difference between apps for the Phone permission, $Q(df = 2, N = 164) = 6.33$, $p = .042$, however, post-hoc analysis with Bonferroni-correction did not reveal significant differences.

The findings for the language app appear to be reasonable as the this app originally requests the Storage permission.

Privacy preferences and usage of the "never ask again" option

The findings of analyzing the usage of the "never ask again" option suggest that participants had clear privacy preferences. Those who denied a permission were likely to select the "never ask again" option. For each permission, there was a high percentage of participants who chose to always deny this permission (cf. Figure 15).

To explore the usage of the "never ask again" option, the total number of granted permissions and the total number of "never ask again" opt-ins were calculated. The two variables were significantly negatively correlated ($r_s = -.438$, $p < .001$). Thus, there was a negative relationship between granting a permission and selecting the "never ask again" option (note that causality cannot be inferred from the correlations).

This finding suggests that participants who granted a permission were (theoretical) willing to reconsider the permission granting next time, whereas participants who denied a permission were rather sure that they do not want to see this permission request again in the future.

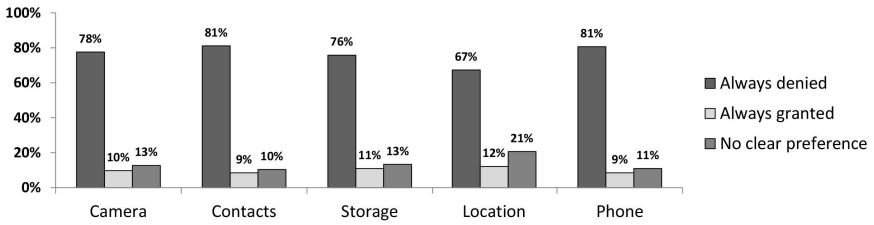


Figure 15: Percentages of how often participants granted a permission for all apps

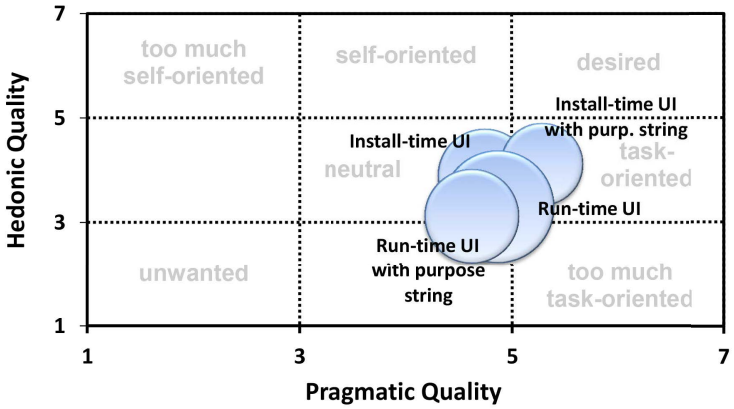


Figure 16: AttrakDiff portfolio diagram: The install-time with purpose string was perceived as task-oriented, whereas the other three UIs were perceived as neutral. The bubble size indicates the average of the standard deviations for hedonic and pragmatic quality.

9.3.2 *Perceived quality of the UIs*

All UIs received medium-high usability ratings in terms of pragmatic quality. The runtime UIs received rather low hedonic quality and attractiveness ratings, whereas the install-time UIs were rated medium.

Figure 16 depicts a portfolio diagram of the pragmatic and hedonic quality ratings. The template of the diagram is based on the works of Hassenzahl [81] and Diefenbach and Hassenzahl [47]: an interactive product is defined as *desired* when it receives high ratings for pragmatic and hedonic quality, whereas low ratings of both dimension indicate an *unwanted* product. Products that are rated high in pragmatic quality are rather *task-oriented*, whereas products that are rated high in hedonic quality are rather *self-oriented*. Following this definition, the results suggest that the install-time UI with purpose string was perceived as *task-oriented*, whereas the other three UIs were perceived as rather *neutral*.

Pragmatic Quality

The interfaces were perceived similarly well regarding usability. The install-time UI with purpose string ($M = 5.28$, $SD = 1.04$) received the highest pragmatic quality rating, followed by the runtime UI ($M = 4.87$, $SD = 1.35$), the install-time UI ($M = 4.74$, $SD = 1.22$), and the runtime UI with purpose strings ($M = 4.62$, $SD = 1.32$). A one-way analysis of variance (ANOVA) did not yield significant differences between the UIs ($F(3, 158) = 2.2$; $p = .09$; $part.\eta^2 = .04$).

Hedonic Quality

The hedonic quality ratings significantly differed between the UIs. While the install-time UIs received medium hedonic quality ratings (install-time UI: $M = 3.90$, $SD = 1.16$; with purpose string: $M = 4.12$, $SD = 1.06$), the runtime UIs were rated rather low (runtime UI: $M = 3.30$, $SD = 1.52$; with purpose string: $M = 3.12$, $SD = 1.09$). A one-way ANOVA indicated a significant difference between the UIs ($F(3, 158) = 6.10$; $p = .001$; $part.\eta^2 = 0.104$) Post-hoc analysis with Bonferroni-correction revealed significant differences between the install-time UI and the runtime UI with purpose string ($p = .032$) and furthermore between the install-time UI with purpose string and the runtime UI ($p = .017$) and the runtime UI with purpose string ($p = .002$). Thus, the results suggest that the install-time UIs rather communicated aspects of personal relevance to the participants.

Attractiveness

Attractiveness ratings also differed significantly between the UIs (one-way ANOVA, $F(3, 158) = 6.27$; $p < .001$; $part.\eta^2 = 0.106$). The post-hoc analysis indicated that the install-time UI with purpose string ($M = 4.67$, $SD = 1.13$) was perceived more attractive than the runtime UI ($M = 3.62$, $SD = 1.59$; $p = .003$) and than the runtime UI with purpose string ($M = 3.54$, $SD = 1.30$; $p = .001$).

In summary, all three UIs were perceived as usable, but experiential product qualities and attractiveness of the install-time UI with purpose string were perceived higher compared to the runtime UIs.

9.3.3 *Felt experience during permission granting*

Affect

There was also a significant difference between the UIs regarding how participants felt during the interaction. Valence values were calculated to investigate whether participants felt rather positive or negative during the interaction with the UIs. Those values were calculated by subtracting the mean of the negative affect scale (NA) from

the mean of the positive affect scale (PA): Mean(Valence) = Mean(PA) - Mean(NA). The valence variable may take values between -4 and $+4$ with -4 indicating strongly negative feelings and $+4$ indicating strongly positive feelings.

Valence values for all UIs ranged between 0.32 and 1.02 (runtime UI: M = 0.32, SD = 1.26; runtime UI with purpose string: M = 0.40 , SD = 0.81; install-time UI: M = 0.89, SD = 1.14; install-time UI with purpose string: M = 1.02 , SD = 0.94). These values indicate that participants felt rather neutral with a slight tendency to positive during the interaction. A one-way ANOVA indicated significant differences between the UIs ($F(3, 157) = 4.43$; $p = .005$; $part.\eta^2 = 0.078$). Valence ratings for the interaction with the install-time UI were significantly higher than for the runtime UI ($p = 0.18$, post-hoc analysis with Bonferroni correction).

Thus, participants in the install-time UI condition felt more positive during interaction than those in the runtime UI condition. The purpose strings did not show to have a significant effect.

Need fulfillment

The degree of need fulfillment further differed between the UIs. One-way ANOVAs were calculated to investigate differences in need fulfillment between the UIs. The results revealed significant differences between the UIs concerning how participants felt during the interaction for Autonomy ($F(3,157) = 2.96$; $p = .034$; $part.\eta^2 = 0.054$), Security ($F(3, 157) = 3.30$; $p = .022$; $part.\eta^2 = 0.059$), and Stimulation ($F(3,157) = 3.63$; $p = .014$; $part.\eta^2 = 0.065$). Post-hoc tests with Bonferroni correction revealed that participants in the install-time UI with purpose string condition felt significantly more autonomous ($p = .023$) and secure ($p = .037$) when granting the permissions than participants in the run-time UI. Post-hoc tests for stimulation did not yield significant results.

Table 7: Mean need fulfillment (RT = runtime UI; RT purp. = runtime UI with purpose string; IT = install-time UI; IT purp. = install-time UI with puspose string). Significant differences between the UIs in bold.

	RT		RT purp.		IT		IT purp.	
	M	SD	M	SD	M	SD	M	SD
AUT	**2.74**	0.91	3.04	1.05	2.97	1.11	**3.37**	0.80
COMP	2.19	0.96	2.42	1.06	2.65	1.00	2.61	1.01
SEC	**2.49**	1.00	2.52	0.94	2.62	1.06	**3.10**	0.98
STIM	1.85	1.11	1.84	1.11	2.45	1.28	2.43	1.07

Thus, participants in the install-time UI with purpose string condition experienced higher need fulfillment than participants in the runtime UI.

Annoyance and Exhaustion

The were significant difference in the annoying ratings between the UIs. The exhaustion ratings did also significantly differ, but post-hoc results were inconclusive.

Participants were asked to evaluate how annoying they perceive the interface. This was done after the permission handling for the first app. A Kruskal-Wallis test revealed significant differences between the UIs ($H(3) = 41.29$, $p < .001$). Post-hoc tests indicated that both, the install-time UI ($M = 2.60$, $SD = 1.37$) and the install-time UI with purpose strings ($M = 2.29$, $SD = 1.27$), were perceived as less annoying compared to the runtime UI ($M = 3.91$, $SD = 1.04$) and the runtime UI with purpose strings ($M = 3.80$, $SD = 1.27$); IT vs. RT purp.: $Z = 3.81$, $p = .001$, $r = 0.30$; IT vs. RT: $Z = 4.11$, $p < .001$, $r = 0.32$; IT purp. vs. RT: $Z = 5.15$, $p < .001$; $r = 0.40$; IT purp. vs. RT purp.: $Z = 4.83$, $p < .001$; $r = 0.38$.

Participants rated the interaction with the install-time UI with purpose string ($M = 2.45$, $SD = 1.61$) as *slightly exhausting*, with the install-time UI ($M = 3.00$, $SD = 1.92$) and the runtime UI with purpose string ($M = 3.43$, $SD = 2.06$) as *somewhat exhausting*, and finally as *rather exhausting* for the runtime UI ($M = 3.65$, $SD = 2.20$). A Kruskal-Wallis test indicated significant differences in exhaustion between the UIs ($H(3) = 8.08$, $p = .044$), but the results of the post-hoc analysis were not significant.

In summary, the install-time UIs were perceived as less annoying than the runtime UIs.

9.4 DISCUSSION

9.4.1 *Limitations*

Designing the user study as an online study allowed to collect answers from a higher number of participants compared to a lab study setting. However, the interaction with the UIs was simulated as a role play and the online study relies on self-reported behavior and user experiences evaluations of an online setting. Related works have shown that online studies on permissions yield similar results than field [8] and lab studies [79, 112]. Nevertheless, further studies should be conducted to determine how the results of the present study translate to the real world. In the role play, the runtime permissions were also shown successively which is rather unusual in real life scenarios. Thus, the annoyance ratings of the runtime UIs likely constitute an upper bound. As the purpose strings were of rather general nature,

the results may rather indicate the lower bound of positive user experience. This decision seemed to be reasonable for the study design, as Tan et al. did not find an effect of the purpose string wording on the behavior. The response rate of the study was rather low, thus it cannot be excluded that there was a self-selection bias which may have influenced the results. The experimental setting was limited to three apps and five permission groups. Apps of easy-to-understand functionality and a supposed low level of familiarity were selected. Furthermore, those permissions that have been found to be critical in related works were selected. Future studies should expand the set of apps and permissions. The above described factors limit the validity of the results. Nevertheless, the setting allows to make meaningful comparisons between the UIs.

9.4.2 *Selective install-time UIs and runtime UIs*

The results of the online study suggest that especially the selective install-time UI with purpose strings offers a better user experience compared to the runtime UIs. It is perceived as less annoying, as more attractive, and as having a higher hedonic quality. However, in terms of privacy decisions, the runtime UIs showed to influence participants to make more privacy-conscious decisions.

A reason for the difference in behavior may be grounded in the fact that in the install-time UIs the permissions were enabled by default (i.e. participants had to opt-out if they did not want a permission to be granted). This kind of question framing has been shown to lead to higher consent rates compared to options were participants need to actively opt-in [106].

Contrary to the study results by Tan et al. [184], the results do not indicate that participants were more likely to grant a permission in the runtime UI in the presence of a purpose string. While the runtime UI with purpose strings was even the UI with the least number of granted permissions, the install-time UI with purpose string was the UI with the most granted permissions. Thus, purpose strings seem to influence permission granting, but this effect further depends on how the permissions are presented.

In summary, the results suggest that runtime UIs supported users in making privacy-conscious decisions in the current over-privilege scenario in which the permission request was only shown once for each permission. However, their low user experience ratings suggests that further investigations on how to make users even more satisfied with the permission granting process may be fruitful.

9.4.3 *The trade-off between permission acceptance and denial*

When designing permission dialogs, mobile platform designers need to make a careful trade-off. On the one hand, they need to give benign applications the possibility to get the permissions they request. On the other hand, they need to pay attention that permissions are not exploited by malicious applications. It seems that the Android runtime permission model focuses on the first option: a permission which has been granted will automatically disappear from future permission requests for this app. On contrary, a permission request for a permission which has been denied will at least be shown once again to the user, potentially together with a developer explanation.

This approach is likely to increase permission acceptance rates [26]. However, the results of the present study indicate that if users would see the "never ask again" option already in the first instance, those who deny the permission would rather select this option. Thus, it seems that users do not want to be bothered again with permissions which they already denied.

Mobile platform designers should thus avoid to bother users with too many permission requests, while at the same time supporting privacy-conscious decisions in case of over-privilege scenarios. Furthermore, they should consider to further increase the user experience of runtime dialogs or to think about alternative permission dialogs that could do so. For example, selective install-time UIs with purpose strings may be especially useful for users with strong privacy preferences (such as the group of privacy conservatives suggested by Lin et al. [137]). Those kind of users were found to be concerned when they have to grant Phone, Contacts, and SMS permissions [137]. A selective install-time UI with purpose strings would enable those users to immediately disable permissions that they never want to grant and it could still offer the option to ask users about granting the other permissions again at runtime. However, this user group is rather small (slightly more than 10% [137]). Further studies are needed to investigate whether a combination of both approaches would be helpful for a broader group of users. For example, a combination could help in reducing the number of permission requests while still offering developers of benign applications a chance to get the permissions they request with the help of purpose strings. At the same time, users could be supported in making privacy-conscious decisions in an over-privilege scenarios. Future studies should thus further investigate how permission requests can lead to a positive user experience in different kind of scenarios. This issue should be investigated from two sides: from a user's and a developer's point of view.

10

EMOJI-BASED MOBILE AUTHENTICATION

10.1 STUDY 6 AND 7: MOTIVATION

Chapter 8 and 9 have addressed the use case of app permissions by investigating prototypes of permission UIs with respect to user experience, usability, and related privacy decision-making behavior.

The present chapter addresses the use case of mobile authentication. Thereby, it investigates the opportunities of using Emojis to create a positive mobile authentication experience for users[1]. While Emojis have been used in authentication schemes [101], it has not been studied if and how they affect user experience in that context, and whether using Emojis actually results in a more positive user experience compared to other authentication methods. Furthermore, it is studied how Emoji-based authentication influences password selection and shoulder surfing susceptibility.

In Chapter 6, I suggested to create a positive user experience, by addressing psychological needs, such as *Stimulation* and *Popularity*, in the design of mobile authentication mechanisms. The present chapter introduces the EmojiAuth prototype which as a scheme for mobile authentication that deploys Emoji-passwords. In two studies – a lab and a field study – it is investigated how users interact with EmojiAuth and whether EmojiAuth is able to address aspects of hedonic quality/ stimulation. While the lab study served to gather first insights on password selection, memorability and user experience, the field study was conducted to validate the results from the lab study in the wild. Furthermore, a shoulder-surfing experiment was conducted at the end of the lab study. That way, the scheme could be tested against casual attackers who are already familiar with the scheme.

1 The present chapter is based on "On the Use of Emojis in Mobile Authentication." by Lydia Kraus, Robert Schmidt, Marcel Walch, Florian Schaub, and Sebastian Möller, which appeared in the 32nd International Conference on ICT Systems Security and Privacy Protection (IFIP SEC), IFIP Advances in Information and Communication Technology, vol 502, Springer, pp. 265–280, 2017. The final publication is available at `http://dx.doi.org/10.1007/978-3-319-58469-0_18`. Text fragments of the present chapter have also appeared in "Implications of the Use of Emojis in Mobile Authentication" by Lydia Kraus, Robert Schmidt, Marcel Walch, Florian Schaub, Christopher Krügelstein, and Sebastian Möller. In: SOUPS: Workshop: Who are you? Adventures in Authentication (WAY). 2016.

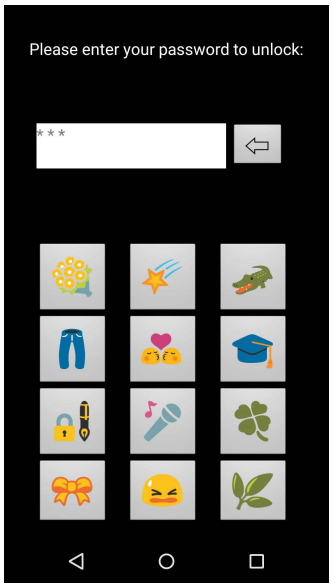


Figure 17: EmojiAuth's user interface. The original UI was in German.

10.2 EMOJIAUTH SCHEME DESIGN

EmojiAuth is a scheme which combines recognition and recall. Similar to PIN, EmojiAuth's UI features twelve buttons (cf. Figure 17). Users can enter their password into the entry field. When the password is entered correctly, the entry field turns green and the screen automatically unlocks. When the password is not entered correctly, the smartphone shortly vibrates and a message is shown above the entry field that the password was incorrect and should be entered again.

10.2.1 *Usability and user experience*

In the following, the characteristics that make Emojis suitable to facilitate aspects of positive user experience are described. Thereafter, EmojiAuth's design regarding usability is described. Usability aspects capture those design decisions that are related to making the interaction efficient and effective.

Positive user experiences

Emojis are very popular among users. In 2015, the Emoji "face with tears of joy" was even selected as word of the year by the Oxford dictionary [36]. Emojis give text-based communication meaning [36], as they enable people to express moods, emotions and nuances in written text. For instance, Filik et al. [64] showed that text messages were perceived differently depending on the kind of Emoji that was attached to them. Even without text, Emojis convey meaning. A smil-

ing face can express joy or happiness, a sad face sadness or grief. In an analysis of 1.6 million manually annotated tweets, Novak et al. [152] found that Emojis were largely perceived as positive. The most frequently used Emojis were rated significantly more positive than the remaining Emojis [152].

Therefore, it is likely that using Emojis will lead to a positive and pleasing user experience and a positive perception of EmojiAuth: Emojis express meaning as they represent faces or objects from users' daily life. As a consequence, Emojis may make the authentication process more (personally) meaningful for users. Also, most Emojis are perceived as positive which might lead to authentication also being perceived as positive.

Keyboard design

The decision for using twelve Emoji buttons on the keyboard is grounded in the advantages of PIN keyboards: Entering a PIN is easy and takes little time [195]. Also, EmojiAuth's keyboard is rather simple featuring only buttons that are indeed needed. Simple keyboards perform well in general regarding authentication usability [170]. Besides the described usability advantages, this design also allows to directly compare Emoji-passwords with PINs.

For the keyboard design, there had to be a careful trade-off between usability and security considerations. When creating a PIN, users can only choose between 10 characters, i.e. the numbers 0-9. Nevertheless, some numerical keyboards (e.g. dial pads) feature twelve buttons including the hash and the asterisk character. EmojiAuth additionally includes these two keyboard positions that would be otherwise "wasted" space in order to enable a larger theoretical password space compared to the PIN scheme (cf. Subsection 10.2.2). While using even more Emojis on the keyboard would have resulted in an even larger theoretical password space, password entry time for keyboards with many keys is quite high (around 20s for virtual mobile text keyboards [170]) compared to PIN (below 10s even for 42bit strong PINs [171]). Thus, using twelve instead of ten Emojis can be considered a reasonable trade-off between usability and increased theoretical password space.

Feedback on system status

A common usability guideline is to provide users with feedback of the system status [151]. For authentication, users need to know how many digits of their password have been already entered. Also feedback on the pressed button is preferable, as it allows users to notice mistakes and correct them if necessary.

Design of system feedback also requires a careful trade-off between usability and security. When an Emoji-button is pressed in Emoji-

Table 8: Emoji categories used in EmojiAuth.

Category	Unicode.org categories	# of items	Example Emojis (Google Noto Emoji font[2])
1	Person + Face	226	
2	Object	287	
3	Nature	204	
4	Activity	44	

Auth, an asterisk appears in the entry field (cf. Figure 17). This design should offer better shoulder-surfing resistance compared to showing the last entered character in the clear. Former work showed that shoulder-surfing attackers who focus on the entry field have a higher success rate [170]. Thus, the entry field was designed to not reveal any information on the password. Feedback on pressed buttons was implemented by decently highlighting the buttons on the keyboard when they were pressed. There was no magnification of pressed buttons as magnification has been linked to higher shoulder-surfing susceptibility [170].

10.2.2 *Security*

In terms of security, characteristics of the theoretical and the practical password space need to be addressed during the design of graphical authentication systems. Thereby, user choice has a huge impact on the practical password space.

That users favor certain Emojis is evident from rankings of currently popular Emojis (e.g., [164]). If similar popularity effects would hold in the user choice of Emoji-based passwords, the skewed password distribution would result in an increased vulnerability for guessing attacks. To address the problem of possible hotspots, i.e., salient icons being favored, EmojiAuth creates an individual keyboard for each user, which is initialized during enrollment. Individual keyboards generated from the very large set of Emojis enable a larger practical password space as single Emojis have a low probability to appear on each keyboard. Thus, the probability that single, well-known Emojis are favored across the whole user population should decrease.

Furthermore, EmojiAuth aims at supporting users in creating diverse passwords which are easy to remember. Therefore, Emojis of different categories are available on the keyboard to support easy assembly of passwords. The categories were selected to provide users with possible modules for stories: person and faces, objects, and nature Emojis as possible "subjects" and "objects," plus activities as possible "predicates." Constructing stories (similar to mnemonic phrases)

should help users increase memorability. Related work has shown that mnemonic phrases are good to remember and as hard to crack as random password phrases [207]. The Emojis available on the keyboard are selected from the four categories mentioned above (cf. Table 8). To generate a user-specific keyboard, three Emojis are randomly selected from each of the four categories. The order of categories is randomized during the selection process. Once the keyboard has been initialized, the order and position of Emojis remains static. Fixed positions are preferable [171] as they lead to shorter login times [183].

All available Unicode Emojis are tagged with more than 1200 tags for further description and categorization [187]. To assemble our categories, all Emojis that were tagged according to the categories' labels (person or face, object, nature, and activity) were automatically extracted. As Emojis can have several tags, duplicates were removed from the first category.

The selected categories offer a diverse set of 592 unique Emojis. Table 8 shows their distribution across categories.

The theoretical password space of EmojiAuth depends on the password length. The 12 available Emojis on the keyboard result in a theoretical password space of 12^4=20,736 permutations for a 4-digit password; 12^6=2,985,984 for a 6-digit password. Emoji-passwords with 4 digits have consequently a theoretical password space which is more than twice as large as that of 4-digit PINs (10^4=10,000) and Emoji-passwords with 6 digits have a theoretical password space almost three times as large as 6-digit PINs ($10^6 = 1,000,000$).

10.3 STUDY 6: LAB STUDY

10.3.1 *Methodology*

First, a mixed-design lab study with two sessions was conducted in order to study the characteristics of EmojiAuth. Thus, the study served to gather first insights on password selection, memorability and user experience. There were two groups EmojiAuth (treatment) and traditional PIN (control). PIN was chosen as a baseline, because entry times for graphical authentication on smartphones should not take longer than PIN or pattern unlock [78], and PIN has shorter entry times [195]. The PIN unlock for the experiment was designed as a typical PIN unlock: like EmojiAuth, with 10 buttons instead of 12 (cf. Figure 18). The two main groups were further divided into two subgroups of varying password length (4 and 6 digits), to investigate effects of password length (i.e. increased theoretical password space) on usability and user experience ratings. The groups in the experiment are further referred to as Emoji-4, Emoji-6, PIN-4 and PIN-6.

During the study participants needed to interact with the system to collect data on login time and success rate. They were further asked

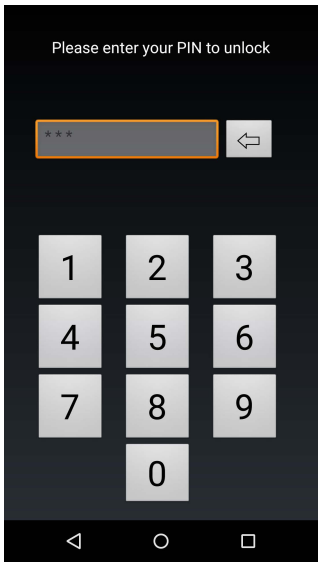


Figure 18: PIN user interface. The original UI was in German.

to rate the perceived usability and UX. At the end of each session participants were interviewed to learn about their password selection and memorization strategies. They were then asked back to the lab a week later to test memorability of passwords and to evaluate login times, usability and UX again. Thus, the study followed a 2x2x2 mixed design with time as within factor (week 1 vs. week 2) and authentication method (Emoji vs. PIN) and the password length (4 digits vs. 6 digits) as between factors.

Procedure

Participants were recruited with a participant recruitment tool of Technische Universität Berlin, classified ads posted on an online service similar to Craigslist, flyers, and e-mail. Participants received 4 Euro compensation for the first study session. For the second study session, they received 8 Euro to incentivize participants to return and thus reduce drop-outs.

During the study, one experimenter and one participant were present. At the beginning of the first session, participants were given an information sheet about the study and asked for consent. They were informed that passwords they create in the study will be stored in plain text to enable scientific analysis, but will not be linked to their identity. After signing the consent form, participants completed an entry questionnaire focused on demographics and smartphone usage. Participants were then assigned to either the Emoji or the PIN group. Participants who stated that they currently used a PIN (or fingerprint and PIN combination) to protect their smartphone were assigned to the Emoji group, in order to reduce the impact of prior habituation to PIN entry.

The experimental part of the study started with a training task in which participants were given a randomly generated password and asked to enter it three times. For each attempt, participants received feedback from the system on whether they entered the password correctly. After the training task, participants were asked to choose their own password. They were told at enrollment time that they will have to remember the password. After password confirmation in the enrollment process, they were asked to enter their password three times. If the password was entered correctly, participants were shown a mental rotation task (MRT) they had to complete, before moving to the next attempt. The mental rotation tasks served to distract participants and clear their short-term memory between login attempts, as suggested in related work [31, 171]. If the password was entered incorrectly, the smartphone vibrated and asked to enter the password again. In either case, after three password entry attempts the experimental part finished.

Participants were then asked to complete the AttrakDiff2 mini questionnaire [86], the PANAS questionnaire [196], and the need fulfillment questionnaire [175]. For the latter questionnaires, German translations were used [47]. After completing the questionnaires, a five-minute semi-structured interview was conducted in which participants were asked to describe how they selected their password and their level of confidence in remembering their password.

One week after the first session, participants returned to the lab for a second session. Participants were asked to enter the password they created during the first session. The procedure was the same as in the first session, including the questionnaires, but demographic data was not collected. A short interview at the end of the session asked participants to describe how they memorized their password and whether they found it easy or difficult to remember. They were also asked whether they had written down their password.

All participants conducted the study on the same smartphone (LG Nexus 5, Android 5.1.1). The interviews were recorded and transcribed verbatim for further analysis.

Participants

In total, 53 smartphone users participated in the study: 14 participants were in the Emoji-4 group, and 13 in each of the remaining groups. Of the participants, 52.8% were male; 47.2% female. Participants were 18 to 70 years old (M=31 yrs., Md.=27 yrs., SD = 11.51). The time between first and second session varied between 3 and 12 days due to scheduling, with an average of 7 days (SD=1.2 days). Eleven participants had a secondary school degree or a lower degree (20.8%), 26 had a qualification for university entrance (49.1%), and 16 a university degree (30.2%). The majority of participants were students (58.5%), although students or campus populations were not

targeted. Various other occupational groups were also represented: employees (15.1%), self-employed (7.5%), retired (5.7%), and others (13.2%). The vast majority (75.5%) did not have a professional or educational IT background.

In the sample were 69.8% Android users, 22.6% iOS users, and 7.6% who used other smartphones. The majority of participants (69.8%) reported to use authentication on their phone; most common were PIN (28.3%), unlock pattern (22.6%), and fingerprint with PIN as fallback (11.3%). Almost all users reported to use a SIM-PIN (90.6%), which however only needs to be entered when rebooting the phone.

10.3.2 *Results*

The data was analyzed for differences between the four groups. As in the other quantitative studies described in Chapter 8 and 9, parametric tests were used where applicable, and non-parametric tests otherwise. For post-hoc analyses Bonferroni-corrected p-values are reported. Effect sizes (r) were calculated for post-hoc analyses as $r = Z/sqrt(O)$ with O being the number of observations [63].

The results suggest that login times and memorability of EmojiAuth and PIN are comparable for passwords and PINs of same length. User experience ratings suggest that EmojiAuth provides a better user experience than PIN.

Login times

Login times for participants' third login attempt for each password scheme were analyzed. Figure 19 shows the results for the four groups for both study sessions. For both, Emoji and PIN, login times were below 5 seconds on average.

At the first session (week one), there was a significant difference between the groups ($H(3)=20.12$, $p<0.001$, Kruskal-Wallis). Post-hoc tests revealed that PIN-4 had a significantly faster entry time than PIN-6 ($Z=3.6$, $p=0.002$, $r=0.71$) and Emoji-6 ($Z=4.1$, $p<0.001$, $r=0.80$), with strong effect sizes.

At the second session (week 2), a significant difference between groups could also be observed ($H(3)=33.4$, $p<0.001$, Kruskal-Wallis). Post-hoc tests again revealed that PIN-4 had a significantly faster entry time than PIN-6 ($Z=4.6$, $p<0.001$, $r=0.90$) and Emoji-6 ($Z=5.2$, $p<0.001$, $r=1.02$), again with strong effect sizes. Also, entry time for Emoji-4 was significantly faster than for Emoji-6 ($Z=2.9$, $p=0.024$, $r=0.56$), also with strong effect size.

Memorability

The lab study results indicate high memorability of both EmojiAuth passwords and PINs. After one week all participants (EmojiAuth and

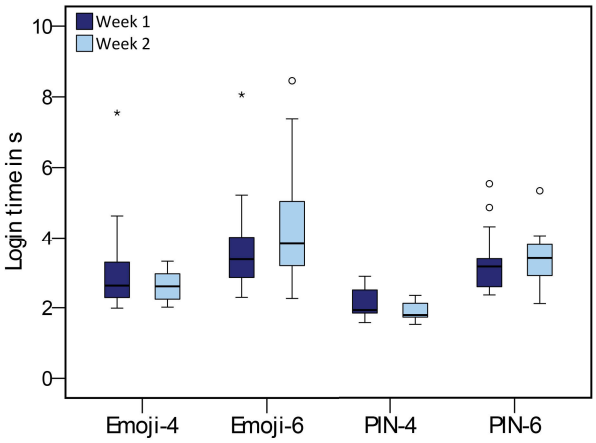


Figure 19: Login times for EmojiAuth and PIN for week 1 and week 2.

PIN) were able to successfully authenticate within three attempts. Long Emoji-passwords seem to be slightly harder to remember after a week of non-use, as a lower number of participants managed to enter their password correctly for all three trials in week 2 (Emoji-4: 92.9% in both weeks; Emoji-6: 100% in week 1 and 69.2% in week 2; PIN-4: 100% in both weeks; PIN-6: 100% in week 1 and 92.3% in week 2). A Fisher's exact test did not reveal statistically significant differences between groups. Four PIN participants reported in the interviews writing down their passwords after the first session and two mentioned that they selected some of their currently used PINs.

Password selection

Diverse password composition and memorization strategies were extracted from the interviews. Participants in the PIN group used many known strategies, which have been criticized for their inability to generate secure passwords. Emoji participants often selected passwords based on preference for certain Emojis and remembered them by creating stories, memorizing spatial patterns or repeating characters.

The interviews were first coded openly by one coder, who created separate code lists for Emoji and PIN with some overlapping codes. Coder 1 then coded the interviews again with the code lists and in parallel a second coder coded the interviews with the code lists. Multiple codes could be assigned to participants. Interrater agreement was substantial for both the Emoji group (Cohen's κ=0.83) and the PIN group (κ=0.72), according to Landis and Koch [129]. The coders then met to reconcile the remaining cases.

Three participants of the PIN group mentioned during the interviews that they chose their passwords differently than they would normally. As this was only a small percentage of the PIN group, a rea-

Table 9: Frequencies of password selection strategies. Participants used multiple strategies, thus the percentages do not sum up to 100.

Strategy	Emoji (n=27)	PIN (n=26)
Color and Shape	2 (7%)	-
Emoji Preference	10 (37%)	-
Repetition	9 (33%)	7 (27%)
Pattern and Position	12 (44%)	5 (19%)
Association and Story	10 (37%)	5 (19%)
Password re-use	1 (4%)	7 (27%)
Date	-	13 (50%)

sonable ecological validity of password selection strategies for PINs can be assumed.

Participants in both groups used a variety of strategies to select and remember their passwords (cf. Table 9). For Emoji, password selection was largely based on *Preference*, as mentioned by P33: "Well I clicked those Emojis I was interested in." P16 selected a password based on the *Emoji-Color*: "Well... first I chose four symbols with the same color." The shape of an Emoji as a selection criterion was mentioned by P18: "I chose [the Emojis] according to circular shape." P39 also used similarity as a selection strategy: "[I chose the password so] that the pictures look similar." *Association* was also frequently used as a selection strategy. P3 associated the selected Emojis with a recent event: "I just thought about the weekend [laughing]." P22 used a song as an mnemonic and selected the Emojis for the password accordingly: "[I've selected the password] after a song. [...] each Emoji stands for one word and depending on the song which words came first, I have typed [the Emojis] in." Few participants created passwords based on *Spatial patterns* and *Character repetition*.

For memorization, Emoji users mainly used *Spatial Pattern* and *Story*: "And then I went from the upper left down to the bottom right." (P16). "I've been thinking: At Christmas (= *Santa Clause*), eavesdrop (therefore I took the *ear*), the children (that's the *backpack*) at night (I took the *house*) and again at night (with the *moon*) and are happy (I took the *heart*)." (P44).

The found password selection strategies also surfaced in the online study by Golla et al. [72] which was conducted shortly after the present lab study: they found *Story* and *Association*-based strategies (e.g. that participants used "important things of their lives" or "repeating event[s] of [their] life[s]" [72, p. 6]) to be rather dominant. *Position*-based strategies and *Spatial patterns* also appeared in their study, as well as *Preference*-based strategies (e.g. choosing Emojis that

are liked or often used while texting). However, the latter strategies were not as dominant as *Story* and *Association*-based strategies in their study.

For PIN, many of the selection strategies that have also been reported in related work could be observed. For instance *Dates* as PINs or as parts of passwords are commonly observed [22, 58] and were also the most frequently used selection strategy in this study. *Spatial* or *Keyboard patterns* were further observed as selection strategies, which are known user strategies to improve memorability [22, 58]. The re-use of passwords is another well-known issue [1] that also surfaced in the present study. Seven participants reported that they used their former or current PINs. Regarding memorization, participants in the PIN group frequently relied on *Dates* as memory cues, whereas participants in the Emoji group mostly relied on *Spatial patterns* and *Stories*.

User experience

The results discussed so far indicate that EmojiAuth is comparable to PIN with regard to login time and success rate for passwords of same length. In the following, perceived usability and user experience of the two schemes are analyzed.

Overview. Figure 20 depicts an AttrakDiff2 portfolio view [47, 81] of pragmatic quality (PQ) and hedonic quality (HQ) ratings for the Emoji and PIN groups. Values for each scale are mean values calculated over both study sessions. The size of the bubble indicates the mean standard deviations over PQ and HQ.

From Figure 20, one can see that PIN-4 and PIN-6 were perceived as *activity-oriented*, with high pragmatic quality ratings and medium hedonic quality ratings. Emoji-6 was perceived as *neutral*, with medium pragmatic and hedonic quality ratings. Emoji-4 was perceived as *activity-oriented* with a tendency to *desired*, with high pragmatic quality ratings and medium-high hedonic quality ratings.

Hedonic quality. Three mixed ANOVAs were calculated with time (week 1 vs. week2) as a within-factor, and password type (Emoji vs. PIN) and length (4 digits vs. 6 digits) as between-factors. The outcome variables were hedonic quality (HQ), hedonic quality stimulation (HQS), and hedonic quality identity (HQI), respectively. For HQ as outcome variable, the results of the ANOVA show a significant main effect for time ($F(1, 48)=4.6$, $p=.036$, $r= 0.30$). Thus, HQ was rated differently in week 1 and week 2 independently of password type and length (cf. Table 10).

For HQS as outcome variable, the mixed ANOVA revealed a significant main effect for password type, $F(1,48) = 8.7$, $p = .005$, $r = 0.39$. Thus, independently of the point in time and the password length, Emoji users rated HQS significantly higher than PIN users (cf. Table

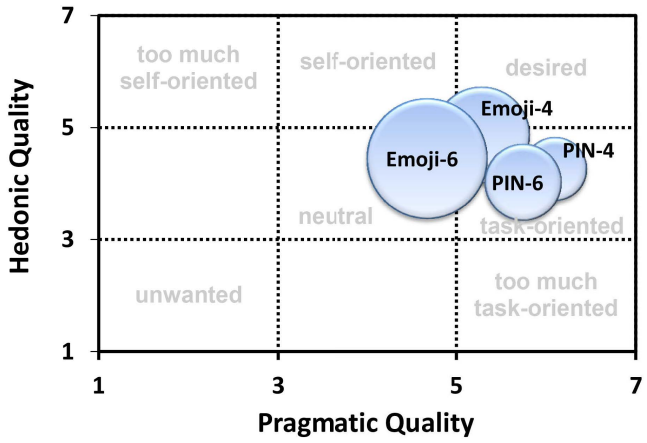


Figure 20: Portfolio view of pragmatic (PQ) and hedonic quality (HQ) ratings. Emoji-4 was perceived as activity-oriented with a tendency to desired, Emoji-6 was perceived as neutral, and PIN-4 and PIN-6 were both perceived as activity-oriented. Bubble size indicates the mean standard deviations over PQ and HQ.

10 and Figure 21e and 21g). Again, there was no significant effect for the password length, indicating that participants rated HQS similarly regardless of the password length. There were no significant effects for the mixed ANOVA with HQI as outcome variable.

Increased HQ ratings in week 2 suggest that factors of *personal relevance* were perceived higher in week 2 for both methods. A reason for this might be grounded in the success that all participants experienced when they managed to enter their password at least once correctly again. Higher HQS ratings for Emoji compared to PIN in both sessions suggest that participants who used EmojiAuth perceived EmojiAuth as stimulating, even in week 2, when EmojiAuth was not a completely new experience for them.

Pragmatic quality. As described above, the high PQ ratings of PIN in both parts of the study indicate a high usability of PIN (cf. Table 10). For Emoji the PQ ratings were medium in week 1 and high in week 2 (Table 10). A Kruskal-Wallis test was calculated for week 1 and week 2. There was a significant difference between the PQ ratings in week 1 ($H(3)=16.25$, $p=0.001$). Post-hoc tests (Bonferroni) revealed that Emoji-4 and PIN-4 received significantly different PQ ratings ($Z=2.74$, $p=0.036$, $r = 0.30$), with a medium effect. Furthermore, PQ ratings for Emoji-6 were significantly different from PIN-4 ($Z=3.69$, $p=0.001$, $r = 0.35$), again with a medium effect. For week 2, the Kruskal-Wallis test did not reveal significant differences between groups.

PQ for Emoji was medium-high on an absolute scale in week 1, but lower compared to PIN. In week 2, PQ increased for Emoji and ap-

Table 10: AttrakDiff2 mini ratings for Emoji and PIN in the lab study. Ratings of the same variable which significantly differ between Emoji and PIN are in bold.

		Week 1		Week 2	
		M	SD	M	SD
Emoji	Pragm. Quality	**4.50**	1.40	5.50	1.20
	Hedon. Quality	4.60	1.17	4.80	1.30
	HQ-Stim.	**4.83**	1.39	**4.90**	1.38
	HQ-Identity	4.27	1.49	4.67	1.41
	Attractiveness	4.80	1.45	5.10	1.63
PIN	Pragm. Quality	**5.90**	0.77	5.90	0.71
	Hedon. Quality	4.10	0.87	4.20	0.94
	HQ-Stim.	**3.75**	1.19	**4.00**	1.13
	HQ-Identity	4.38	0.89	4.46	0.97
	Attractiveness	5.00	0.86	4.90	0.94

proximated the ratings for PIN. This suggests that once participants were familiar with EmojiAuth, usability was soon after perceived as good.

Attractiveness. The results of a Kruskal-Wallis test did not indicate significant differences between the groups for both weeks. Thus, attractiveness of the authentication methods was perceived similar.

Valence. Another mixed ANOVA was calculated with valence (positive affect minus negative affect, from PANAS [196]) as an outcome variable. There was a significant main effect for time, $F(1,49) = 6.35$, $p = .015$, $r = 0.34$, and a significant interaction effect for time and password type, $F(1,49) = 5.40$, $p = .024$, $r = 0.32$. This means that valence ratings of the unlock type changed over time depending on the password type. Emoji participants felt more positive when using EmojiAuth in week 2 ($M = 2.4$, $SD = 0.94$) than in week 1 ($M = 2.1$, $SD = 0.86$, cf. also Figure 22b and 22d). Valence for PIN remained the same ($M = 2.1$ in both weeks, $SD = 0.73$ (week 1), $SD = 0.66$ (week 2)).

This again suggests that, once participants were familiar with EmojiAuth, they also felt more positive compared to PIN users during authentication.

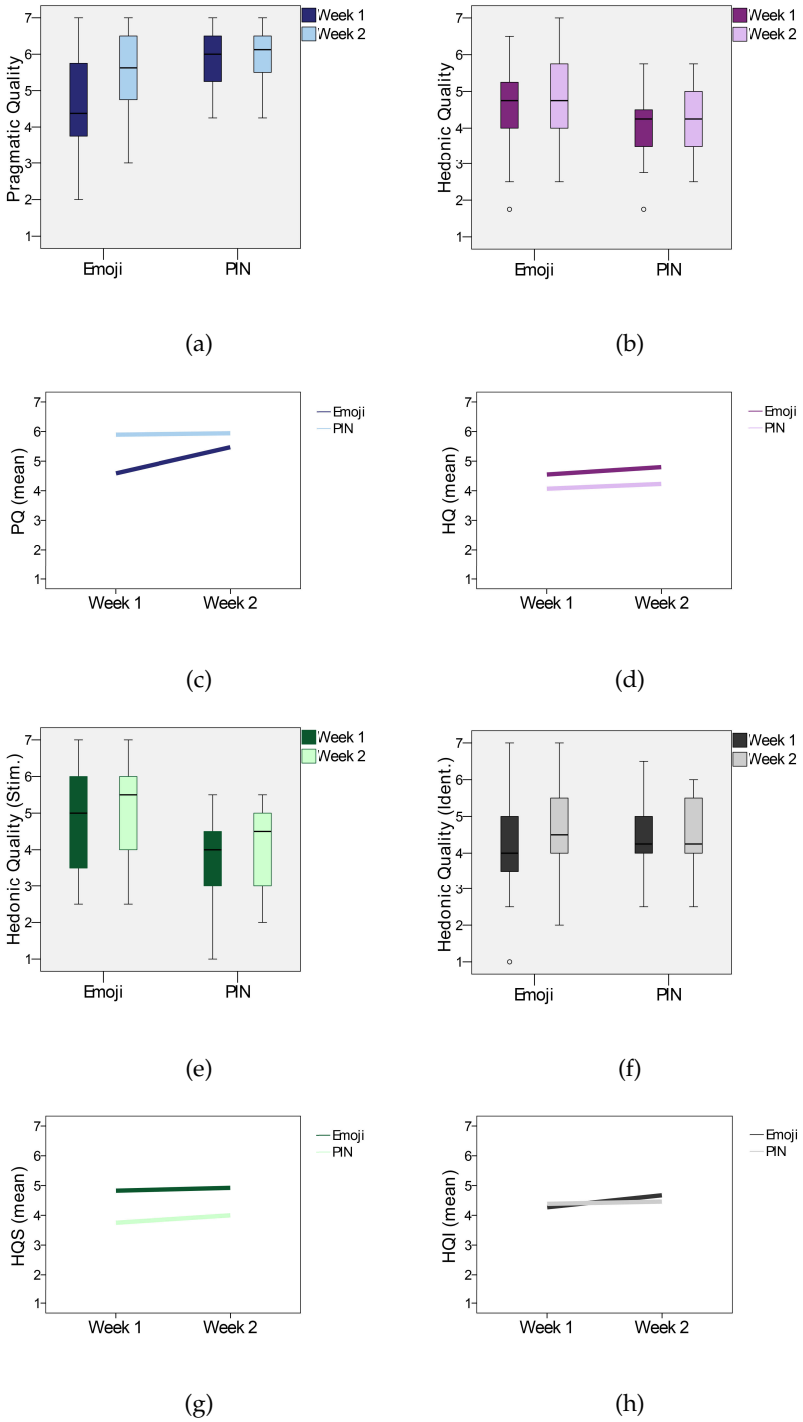


Figure 21: Boxplots (upper) and interaction graphs (lower) for Pragmatic Quality (PQ), Hedonic Quality (HQ), Hedonic Quality – Stimulation (HQS) and Hedonic Quality – Identity (HQ-I). From session 1 to session 2, pragmatic quality for Emoji increased, and hedonic quality increased for both, PIN and Emoji. Hedonic Quality – Stimulation significantly differed between Emoji and PIN.

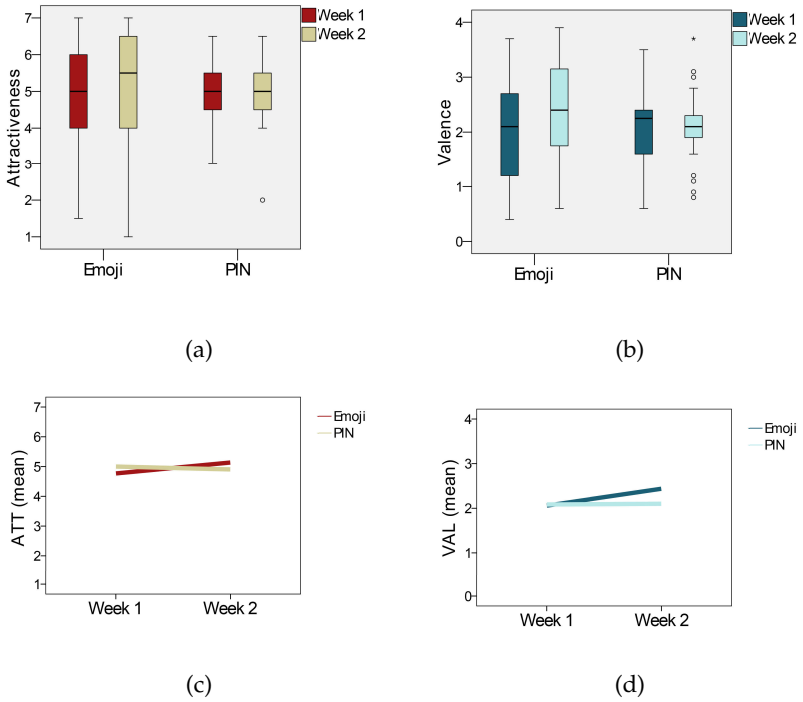


Figure 22: Boxplots (top) and interaction graphs (bottom) for Attractiveness (ATT) and Valence (VAL). Valence ratings increased for Emoji in Week 2.

10.4 STUDY 7: FIELD STUDY

10.4.1 *Methodology*

The goal of the field study was to investigate how EmojiAuth performs in the wild. The field study consisted of a pre-study questionnaire, an introductory session, a field phase of 15-17 days, and an exit session. In order to ensure meaningful use of the authentication methods during the study, EmojiAuth and PIN were deployed as a protection mechanism for the participants' email app on their own phone. E-mails have been shown to often contain sensitive information [54] worth protecting. Consequentially, Android users who use an email app on their device were recruited and this was verified in a screening survey.

10.4.1.1 *Procedure*

Participants were also recruited with a participant recruitment tool of Technische Universität Berlin and classified ads posted on an online service similar to Craigslist. Participants from the first study could not participate. Participants received 25 Euro compensation of which 5 Euro were paid at the introductory session and 20 Euro at the end.

During the introductory session participants received information about the study and were asked for consent. Then, either EmojiAuth or PIN was installed as a lock for their email app on their own devices. In both apps an accessibility services was used to monitor whether the e-mail app is currently in the foreground. In order to activate this service, the participants had to select one or more e-mail apps which they currently use from the list of installed apps. As soon as a password/PIN was picked, opening their email app required participants to authenticate with their password/PIN. Our apps had a 30 second time-out for an authentication session, i.e., if participants left their e-mail app for 30 seconds or more, they had to re-authenticate. Participants were asked to pick their password/PIN at home. It had to be at least 4 digits. For the PIN group, only meta-data of the user-chosen PINs was collected (length and number of differing characters).

Directly, after creating the password, participants received a questionnaire asking about the importance of different password/PIN selection criteria, which were derived from the lab study study results. Participants could change their password or PIN during the study (within our app) and EmojiAuth users could further generate a new Emoji-keyboard. In case that they had forgotten their password or PIN, users could enter a pre-defined backup-password in our app and select a new password/PIN. If the password/PIN was entered five times incorrectly in a row, users also had to provide their backup-password to unlock their e-mail app and to select a new password.

The field phase took between 15 and 17 days, depending on when participants scheduled their exit session. Similar to Wechsung et al.'s study [198], participants received a daily reminder to complete a daily feedback questionnaire, which asked participants to rate on a Smiley-scale how they liked interacting with EmojiAuth or PIN that day. This questionnaire contained a smiley-scale on which participants could rate how much they liked interacting with EmojiAuth or PIN during that day. Participants could further explain their rating in a free-text field. On days 2, 8, and 14, participants further received the AttrakDiff2 mini-questionnaire to assess user experience.

After the field phase, participants returned to the lab for the exit session in which they completed an exit survey (on paper) followed by the shoulder-surfing experiment. The exit survey contained questions on the overall rating of the authentication method and single design features, as well as the psychological need fulfillment questionnaire, and hypothetical questions on the future use of the authentication method. Furthermore, EmojiAuth/PIN was uninstalled from their devices.

Shoulder-Surfing Experiment

The field study's exit session contained a shoulder surfing experiment, modeled after similar experiments in related work [171, 185],

in which the threat model is a casual observer. Participants acted as shoulder surfers for either EmojiAuth or PIN (based on their field study condition), whereas the experimenter served as the observation target. However, in contrast to related work, the shoulder surfers in the present study were experienced with the authentication scheme they tried to observe after two weeks of use. Participants could position themselves either left, right or behind the experimenter who sat at a table to enter the password. Participants were provided with pen and paper for note taking. To ensure that passwords are entered with similar speed and in the same position, the experimenter trained password entry beforehand.

To test shoulder surfing susceptibility for different kinds of passwords created with different password selection strategies, the procedure was repeated with five passwords. To account for possible ordering effects, the order of the passwords was counterbalanced. The five passwords used the same keys (in terms of spatial position on the keyboard) in order to facilitate direct comparison between Emoji and PIN results. The first and second passwords were random 6-digit ('341779') and 4-digit passwords ('1706'). The third ('134679') and the fourth passwords ('5802') were patterns participants had created in the lab study. The fifth password was an association password which consisted of the Christmas Eve date ('2412') for the PIN users and a Christmas-related Story created by a lab study participant for the Emoji users ('bear - Christmas tree - snowman - heart' or '23#4' on a numerical keyboard). After a password was entered by the experimenter, the participant had three trials to enter the observed password. The experiment was conducted on a LG Nexus 5, Android 5.1.1, smartphone.

Participants

In total, 41 smartphone users participated in the field study: 21 in the Emoji group and 20 in the PIN group. The participants were between 19 and 63 years old (M=34.1 yrs., Md.=28 yrs., SD=12.1); 24 were female (59%). Five participants had a secondary school degree (12.2%), 16 had a qualification for university entrance (39%), and 20 had a university degree (48.8%). Most were students (22), although not only campus populations were targeted. The second largest group were employees (8), followed by job seekers (5), self-employed (2), and others (4). Most (80.5%) did not have a professional IT background.

All were Android users, as required. The majority of the participants (19) used Samsung Galaxy devices (A3, S3, S4, S5, S7, incl. minis, Trend, J3), 6 participants used Sony devices (e.g. Xperia), and the rest diverse other models. Nineteen participants indicated to currently use a PIN, three a password, nine an Android pattern, and eleven did not use any locking method.

One participant had problems during the study to use the app due to an old phone, another participant's phone physically broke during the study. As a result we excluded the field data of these participants. One more participant responded in almost all daily feedback questionnaires with comments out of scope, thus this data was also removed from the study. All three data sets were from the PIN group, thus the PIN sample decreased to 17 participants.

10.4.2 *Results*

Success Rates

In the field study, in both groups, only a few incorrect unlocks were recorded (Emoji: 3% of total unlocks; PIN: 1.5%). In total, 3,514 correct unlocks and 83 incorrect unlocks were collected. Of those data points, EmojiAuth accounted for 1,924 correct unlocks (M=91.62, SD=66.06) and 58 incorrect unlocks (M=2.76, SD=4.18), whereas PIN accounted for 1,590 correct unlocks (M=93.53, SD=70.40) and 25 incorrect unlocks (M=1.47, SD=1.55). Mann-Whitney-U tests did not reveal significant differences in the distribution of correct and incorrect unlocks between the two groups.

Success rates for PIN were high, suggesting that PIN performs well in the wild. This is in line with work of von Zezschwitz et al. who also found PIN to be a practical authentication method with low error rates [195]. Emoji success rates were also high, suggesting that EmojiAuth is a practical authentication method, too.

Password Length and Password Changes

For the initial enrollment, the majority of participants in the Emoji group (19) picked a 4-digit password, whereas two participants picked a 5-digit password. Participants in the PIN group picked diverse PIN lengths in the initial enrollment. Slightly more than half (10) picked a 4-digit PIN, two picked a 5-digit PIN, three picked a 6-digit PIN, and two an 8-digit PIN. The results of a Mann-Whitney-U test did not indicate significant differences in the mean password length between the groups (Emoji: M=4.1, SD=0.3; PIN: M=4.9, SD=1.4).

Four participants in the Emoji group changed their password once, whereas three users changed their password twice. In the PIN group, also four participants changed their PIN once and one participant changed the PIN twice. The results of a Mann-Whitney-U test did not indicate significant differences in the mean number of password changes between the groups (Emoji: M=0.48, SD=0.75; PIN: M=.35, SD=0.61).

PIN users picked rather long passwords, whereas Emoji users mostly stuck to 4-digit passwords. Although password length is one factor that determines security, it is hard to make interpretations about pass-

word security from the password length only. For example, long PINs which are re-used or which rely on predictable selection strategies such as one's own birth date maybe easily found out by an attacker [22]. Therefore password selection strategies are analyzed further in the next paragraph.

Password selection

The password selection strategies that were found in the lab study also surfaced in the field study (cf. Table 11). Figure 23 provides examples of Emoji-passwords created by study participants in the lab and in the field study.

The results of the lab study were used to design Emoji and PIN password selection questionnaires for the field study. For the Emoji group, the questionnaire contained 16 items measured on five scales. Each item was answered on a 5-point scale from 1 (does not apply at all) to 5 (completely applies). The α-values indicate Cronbach's alpha – a measure for the internal consistency of the scales: α-values above 0.7 - 0.8 indicate good internal consistency [63]. Except for *Color and Shape*, all Emoji scales showed a good internal consistency.

Emoji preference ($\alpha = 0.96$):

- I selected the Emojis that I liked most.
- I selected the emojis that I rather have a personal relationship to.

Association and Story ($\alpha = 0.81$):

- I selected the emojis that I could mentally connect with each other.
- I selected the emojis that I could assign to the same topic.
- I memorized the order of my password's emojis with the help of a story.
- I first made up a story and picked the emojis accordingly.

Pattern and Position ($\alpha = 0.89$):

- I selected the emojis according to a pattern on the keyboard.
- I used a graphical pattern on the keyboard to memorize my password.
- The emojis' position on the keyboard has been important for me.
- Instead of emojis, I memorized the numbers that are usually depicted on a numeric keyboard.

Repetition and Similarity ($\alpha = 0.90$):

- I repeated some emojis in order to faster unlock my phone.

- I repeated some emojis in order to better memorize the password.
- I repeated some emojis to prevent typing errors when unlocking.
- I selected the emojis that were rather similar to each other.

Color and Shape (α = 0.51):

- I selected the emojis due to their color.
- I selected the emojis due to their shape.

For the PIN group, the questionnaire contained 15 items. An asterisk at the end of an item indicates that it is based on the work of Bonneau et al. [22]. Internal consistency was good for the *Re-use* and *Pattern and Position* scales. The consistency of the two other scales was rather low, indicating that the questions for measuring the strategies should be improved for future versions of the questionnaire.

Date[3]

- I chose a date as the PIN.

Repetition and Sequence (α = 0.66):

- For my PIN I chose consecutive numbers (e.g., 1234 or 1357)*
- I repeated some numbers in order to faster unlock my phone.
- I repeated a two-digit number in my PIN*.
- I exclusively repeated one number in my PIN*.
- I repeated a three digit number in my PIN*.
- I repeated some numbers in order to better remember the PIN.

Re-use (α = 0.96):

- I chose a PIN that I'm already using in a different context.
- I chose a PIN that I have used in the past.

Pattern and Position (α = 1.00):

- I used a graphical pattern on the keyboard to memorize my password (e.g., a line from left to right; numbers create a square; numbers are at the corners of the keyboard; numbers form a cross)*.
- I selected the numbers according to a spatial pattern on the keyboard (e.g., a line from left to right; numbers create a square; numbers are at the corners of the keyboard; numbers form a cross)*.
- The positions of the numbers on the keyboard play an important role for me.

Association (α = 0.63):

3 Note that α-values cannot be calculated for single items.

- I selected the numbers that I could mentally connect with a place, object or a topic.
- I created a mnemonic to remember the numbers.

To compare lab and field study strategies, it was calculated how many participants reported to deploy one or more of the identified strategies (cf. Table 11). For the lab study, frequencies were calculated by counting the occurrences of each interview code. For the field study, the frequencies were calculated as the number of participants who rated at least half of the items of a scale as important or very important. The overlaps between selection strategies in both studies (cf. Table 11) suggest a reasonable validity of the identified strategies. As in the lab study, the PIN selection strategies in the field study are in line with findings of related work [22]. In both studies, *Preference*, *Pattern and Position*, and *Association and Story* seem to play a rather important role for Emoji-password selection.

The importance of the *Preference* selection strategy for Emoji-passwords is also visible from the distribution of selected Emojis across passwords. Figure 24 depicts three examples of the most popular password-Emojis (lab and field study) and three examples of the most unpopular Emojis together with their occurrences on the keyboards. Due to the different sizes of the category lists from which Emojis are selected for EmojiAuth, some Emojis appear more often on the keyboard than others. Although the individual keyboards were expected to decrease the probability of hotspots, Figure 24 suggests that the distribution of password-Emojis is skewed. This finding is also reflected in the results of Golla et al. who found some Emojis and even some passwords to be more popular than other passwords and Emojis [72]. Results by Golla et al. also revealed that guessing attacks that rely on content *and* position-based predictors performed better than attacks

Table 11: Frequencies of password selection strategies. Several participants used multiple strategies, thus the percentages do not sum up to 100.

Strategy	Emoji		PIN	
	Lab (N = 27)	Field (N = 20)	Lab (N = 26)	Field (N = 17)
Color and Shape	2 (7%)	9 (43%)	-	-
Emoji Preference	10 (37%)	12 (60%)	-	-
Repetition	9 (33%)	4 (20%)	7 (27%)	7 (42%)
Pattern and Position	12 (44%)	8 (40%)	5 (19%)	3 (18%)
Association and Story	10 (37%)	8 (40%)	5 (19%)	12 (71%)
Password re-use	1 (4%)	-	7 (27%)	4 (24%)
Date	-	-	13 (50%)	8 (47%)

that rely on only one of those variables [72]. Despite the skewed password distribution, 4-digit Emoji-passwords resulting from a authentication scheme with 20 Emojis seem to be more resistant to guessing attacks compared to Android unlock patterns and 4-digit user-chosen PINs [72].

Figure 23: EmojiAuth passwords created by lab and field study participants. Passwords are grouped according to password selection strategies.

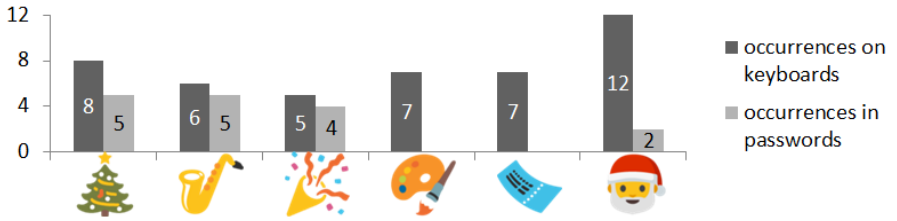


Figure 24: Password-Emojis examples of the most popular (left) and unpopular (right) password-Emojis together with their occurrences on the keyboards

Shoulder-Surfing Results

The minimal Levenshtein distance for each user ("attacker") and each password was calculated, i.e. the number of deletions, insertions, or substitutions, needed to obtain the correct password from the entered password [170] [135]. There was a significant difference in the minimal Levenshtein distance between Emoji (M=2.45, SD=1.64) and PIN (M=0.72, SD=0.83) for the 6-digit random password (Mann-Whitney-U, U=289.0; p=.001; r=0.53), with medium effect size. Thus, the 6-digit random password was significantly harder to shoulder surf on the Emoji keyboard. For the other passwords, there were no significant difference between the authentication methods.

It was also compared whether some passwords are harder to shoulder surf than others. For Emoji, a Friedman ANOVA revealed significant differences in the minimal Levenshtein distance between the passwords (χ^2=40.44; p<.001). Post-hoc analysis with Bonferroni correction revealed that the 6-digit random password was significantly harder to shoulder surf than the 4-digit random password (M=0.75, SD=0.93), Z=1.45; p=.037; r=0.46, the 6-digit pattern (M=0.15, SD=0.67), Z=2.75; p<.001; r=0.72, and the 4-digit pattern (M=0.15,

SD=0.37), Z=2.2; p<.001, r=0.70. All post-hoc results for Emoji had medium to large effect sizes. For PIN, a Friedman ANOVA revealed significant differences between the passwords (χ^2=10.78; p<.029), but the post-hoc tests were not significant.

The post-experiment questionnaires revealed that attackers used four different strategies to observe the password: they either paid attention to the numbers of the keyboard ("numbers"), the spatial pattern of the password ("pattern"), a mix of both strategies ("mix"), or they reported to observe the password entry with high concentration ("observation"). The frequencies of the strategies significantly differed between Emoji and PIN (p=.026; Fisher's exact). "Attackers" in the Emoji group were more likely to use the pattern observation strategy (Emoji: 16; PIN: 8). Not surprisingly, "attackers" in the PIN group were more likely to use the numbers observation strategy (Emoji: 0; PIN: 4).

In summary, the 6-digit random password was harder to shoulder surf with the Emoji keyboard and was also harder to shoulder surf with the Emoji keyboard compared to the 4-digit random password and the 4- and 6-digit pattern passwords. The casual "attackers" in the Emoji group largely relied on the pattern observation strategy which may make users of Emoji-passwords that are based on spatial patterns more vulnerable to shoulder surfing attacks.

User Experience

Daily Feedback. The daily feedback questionnaires that were answered during the field study indicate that both, EmojiAuth and PIN, were perceived similarly good in terms of user experience. This is also supported by the AttrakDiff 2 mini ratings, with the difference that EmojiAuth users perceived the authentication method more interesting in the beginning of the study.

In total, participants reported 342 (Emoji:184) positive experiences, 99 neutral experiences (Emoji: 51), and 14 negative experiences (Emoji: 10). A Mann-Whitney-U test did not reveal significant differences between distribution of positive, neutral, and negative experiences between Emoji and PIN. To further analyze users' experiences, the free-text answers of the daily feedback were open-coded by one coder. This led to a code list of 17 codes. The qualitative data was then independently coded with the code list by another coder. Interrater agreement was almost perfect (Cohen's κ=0.83), according to Landis and Koch [129]. The coders then met to reconcile the remaining cases.

About a third of participants' comments (35%) expressed short statements that everything is going fine (e.g. "everything's ok.", "fine", "works"). The second most comments category (10%) concerned the good usability of the methods (e.g. "really easy and not annoying", "easy to handle, takes only little effort", "fast [PIN] entry, no problems, I don't have concerns regarding memorability as long as the

positions of the numbers don't change"). Six percent of comments indicated that participants got familiar with the methods (e.g. "I've became accustomed to it", "it [the authentication] already belongs to my daily routine"). Thereby, Emoji participants reported this twice (14 comments) as much as PIN participants (7 comments). Four percent of codes concerned hedonic aspects. Hedonic aspects were mostly mentioned by Emoji users (11 out of 14, e.g. "I liked choosing the Emojis as I could select them on my own without restrictions", "it was fun to open the e-mail app with the Emojis while sitting next to my friends", "I changed my password twice today as I was curious which other Emojis are available"). A few comments (2.5%) also concerned perceived security vulnerabilities of the schemes ("when I open the app in quick succession, EmojiAuth didn't work properly" [comment from the author: this participant might not have been aware of the 30 seconds time-out]; "it's relatively easy for others to find out the [Emoji] combination").

AttrakDiff. The AttrakDiff 2 mini ratings are in line with the daily feedback: Pragmatic quality was perceived as high ($M>5$) for both methods at all measurement points (day 2, 8, and 14). Emoji users rated hedonic quality in terms of Stimulation higher than PIN users on day 2 (Mann-Whitney-U, $U=34$; $p<.001$; $r=0.70$). For day 8 and day 14, there were no significant differences in Hedonic Quality / Stimulation between the groups. Whereas Emoji users' stimulation ratings remained stable over time, PIN users' stimulation ratings increased after one week: there were no significant differences in Stimulation

Table 12: AttrakDiff2 mini ratings for Emoji and PIN in the field study. Ratings of the same variable which significantly differ between Emoji and PIN are in bold.

		Day 2 $N_E=21/N_P=17$		Day 8 $N_E=21/N_P=16$		Day 14 $N_E=15/N_P=10$	
		M	SD	M	SD	M	SD
Emoji	Pragm. Quality	5.71	0.83	5.61	0.88	5.60	0.95
	Hedon. Quality	**4.56**	0.84	4.39	1.11	4.42	1.08
	HQ-Stim.	**4.62**	0.89	4.21	1.24	4.17	1.30
	HQ-Identity	4.50	0.92	4.57	1.05	4.67	0.96
	Attractiveness	4.98	1.04	4.93	1.15	4.77	1.15
PIN	Pragm. Quality	5.53	0.89	5.17	1.20	5.43	0.85
	Hedon. Quality	**3.78**	0.56	4.16	0.80	3.93	0.73
	HQ-Stim.	**3.22**	0.60	3.88	0.90	3.81	0.79
	HQ-Identity	4.34	0.81	4.44	1.05	4.10	0.94
	Attractiveness	4.94	0.79	4.75	0.80	4.55	0.86

between the groups for day 8 and 14. This result indicates that PIN users needed time to perceive the authentication method as interesting. Consequently, EmojiAuth could be beneficial for making users familiar with using an authentication method by offering a stimulating user experience from the start. Attractiveness ratings at all measurement points were medium-high ($M \sim 5$), without significant differences between groups.

Despite negligible quantitative differences in user experience, 17 of 20 Emoji users reported in the exit questionnaire that they would prefer using Emojis over PIN as a screen lock, mainly due to the high memorability of Emoji-passwords (12 answers) and the appeal of the Emoji-based method (six answers).

10.5 DISCUSSION

10.5.1 *Limitations*

The present study has a few potential limitations. Participants self-selected to participate in a study on mobile authentication, thus the participants may have higher technology affinity than the general population. As the sample size in both studies was limited, generalizations should be made with caution. However, the results facilitate a meaningful comparison of EmojiAuth to the current baseline: PIN entry. Furthermore, the consistency between lab and field study findings indicates a reasonable validity of the results.

10.5.2 *Practical Emoji authentication*

Valuable insights into the practical aspects of Emoji-based mobile authentication were gained. The results of the studies have shown that EmojiAuth has a short login time and high success rates, both comparable to traditional PINs. Memorability for 4-digit Emoji-passwords was good, whereas memorability of 6-digit passwords was reasonable. The results suggest that EmojiAuth is a practical authentication method with a good password memorability of short passwords.

Study participants created their Emoji-based passwords with five different strategies: *Emoji preference*, *association & story*, *pattern & position*, *repetition & similarity*, and *color & shape*. The results suggest that the distribution of Emoji-passwords may be skewed, even with individual keyboards. It is subject to future studies to quantify the frequency of each selection strategy and its contribution to the practical password space. Results from the shoulder-surfing experiment suggest that EmojiAuth performs better for longer passwords that do not follow distinct spatial patterns. As the "attackers" in this experiment mostly focused on the *pattern* strategy, we recommend that spatial patterns should not be used for password creation. We also plan

to conduct further studies to investigate whether password creation policies could help users create Emoji-passwords that are resistant to guessing and capture attacks, as well as memorable. For example, such policies could blacklist most popular Emojis or spatial patterns.

So far, EmojiAuth features twelve Emojis on the keyboard. Adding more Emojis increases the theoretical password space, but might also increase the likelihood of hotspots to evolve as the probability to occur on the keyboard for each Emoji increases. Moreover, usability could suffer when there are too many small buttons on the keyboard. Those trade-offs need to be investigated in future studies to further advance the design of the method. Furthermore, the optimal assignment of Emojis to categories for keyboard generation and its impact on user choice resilience need to be further investigated: can large categories with diverse Emojis be created that allow users to assemble interesting and diverse passwords? How large do the categories have to be in order to completely eliminate hotspots?

10.5.3 *The role of UX in mobile authentication*

Both, EmojiAuth and PIN, were perceived as highly usable and as providing a good user experience in the lab and the field study. Emoji-based authentication performed only slightly better in terms of hedonic product perception and, thus, positive interaction. In the field study, EmojiAuth users mentioned hedonic aspects slightly more often in their daily feedback. However, for both methods, the overall number of experiences related to hedonic aspects was rather low. The AttrakDiff ratings indicate that users perceived EmojiAuth as interesting from the beginning of the field study and that this perception remained stable. In the lab study, EmojiAuth was in both weeks perceived as more interesting. The majority of EmojiAuth users indicated that they would prefer EmojiAuth over PIN as a screen lock, which is a promising result. It is subject to future studies to investigate how hedonic quality could be further increased in authentication methods and whether in contributes to long-term user "relationships" with the authentication method.

Part V

CONCLUSION AND FUTURE WORK

11 CONCLUSION AND FUTURE WORK

11.1 CONCLUSION

By answering the research questions described in the introduction, this thesis makes multiple contributions to the understanding of mobile security and privacy mechanisms from an experiential perspective. A variety of qualitative and quantitative studies have been conducted to answer the research questions. The findings to each research question are detailed in the following.

By answering RQ1 and RQ2, this thesis provides first evidence that there is a need to address experiential aspects, beyond the functional, in mobile security and privacy mechanisms. RQ3 identifies directions for the experiential design of those mechanisms. RQ4 provides an overview of how different mechanisms shape user experience and related behavior. Thereby, the results suggest that experiential qualities do not necessarily have to be in conflict with security and privacy. The answer of RQ5 indicates that non-functional aspects can be manipulated with security and privacy mechanisms and the answer of RQ6 suggests that the development of the user experience with such mechanisms over time is similar to those of lifestyle products. The results of this thesis constitute a valuable first step for understanding the experiential dimension of mobile security and privacy mechanisms.

11.1.1 *Experiences with mobile security and privacy*

Two focus group studies have been conducted to explore experiences with mobile security and privacy. The findings are summarized in the following in order to provide an answer to RQ1 (What experiences do users have with security and privacy on their smartphones?).

Negative experiences. The focus groups (cf. Chapter 5) suggest that users may feel forced to use messaging applications which they feel uncomfortable with in terms of security and privacy, but which are used by other users. This may result in a feeling of **social pressure**. Furthermore, users may feel uncomfortable when using social apps when they have the feeling that they need to be available all the time (**social availablility**). Users further expressed negative experiences related to the usage of mobile security and privacy mechanisms. These experiences surfaced in negative feelings such as **dependency** (e.g. on third parties to provide and manage security and privacy), **helplessness** (towards security and privacy threats), and **fatalism** (regarding

the actual security of mechanisms). Negative experiences related to a lack of choice and the need to **sacrifice security for usage**, were further expressed.
Positive experiences. The results of the focus groups further suggest that users encounter positive experiences through feelings of **being able to exercise control** over security and privacy related issues. Furthermore, the results suggest that **trust**, for example, in a service provider may be a source of positive experiences.

11.1.2 *Motivators for mobile security and privacy*

An interview and an online study were conducted (cf. Chapter 6), to explore which psychological needs are salient motivators for the usage of mobile security and privacy mechanisms. The findings of these two studies provide an answer to RQ2 (What motivates users to employ security and privacy actions on their smartphones?).

The results of the interviews suggest a variety of psychological needs as motivators for the usage of mobile security and privacy mechanisms. In both studies *Security* was found to be a main motivator, however, different other needs such as **Keeping the meaningful**, **Stimulation**, **Autonomy** and **Competence** also serve as potential motivators. For example, backups are mainly motivated by *Keeping the meaningful* and using a screen lock with authentication is mainly motivated by *Security*, but *Popularity* was also mentioned as a motivator. App selection was noted to be driven by *Stimulation* and *Money/Luxury*, whereas *Security*, *Competence* (or a lack thereof) and *Autonomy* were reported to be related to uninstalling apps and mitigating access to sensitive information. The fulfillment of the need for *Security* may not necessarily lead to a positive experience with mobile security and privacy mechanisms (cf. also Sheldon et al. [175] and Hassenzahl et al. [85] for results on the limited ability of *Security* to contribute to positive events and experiences in another context of use). The low mean values for need fulfillment in the online survey also indicate that security and privacy actions may profit from new design approaches that support psychological need fulfillment.

11.1.3 *Experience design for mobile security and privacy*

In the following, RQ3 (Which principles should the experiential design of mobile security and privacy mechanisms follow?) is answered.

The answers to RQ1 and RQ2 led to the notion that the following principles should be considered in the experiential design of mobile security and privacy mechanisms. Note that these principles present

directions rather than final truths. As each mechanism needs to be tested under a threat model, the design of usable mobile security and privacy mechanisms that provide a positive user experience and high security or privacy may not be as straight forward as it might appear here.

Security and privacy by design and default for social apps. Social apps should deploy security and privacy mechanisms such as end-to-end encryption by design and default in order to avoid negative experiences related to "social pressure" and "social availability".

Usability and education. Usability engineering and educational techniques should be deployed to mobile security and privacy mechanisms. Thereby, the goal should not only be to render the interaction with such mechanisms more efficient and effective, but also to avoid negative experiences and increase satisfaction, for example by addressing the need for *Autonomy* or *Competence*.

Experience design beyond Security. Although *Security* is a motivator to use mobile security and privacy mechanisms, the fulfillment of this need does not necessarily lead to positive experiences with such mechanisms. Therefore, mechanisms should address experiential aspects beyond the need for *Security*, such as need fulfillment through *Stimulation* or *Autonomy*, in order to enable positive user experiences. For example, the use of Emojis in authentication could address aspects of *Stimulation* while allowing for good password memorability (cf. RQ4 and RQ6). Or selective install-time permission dialogs may rather address a feeling of *Autonomy*, compared to runtime permission dialogs (cf. RQ4).

11.1.4 *Experiences with dedicated prototypes*

Chapter 8, 9, and 10 introduced permission and screen lock prototypes that have been designed to address aspects of user experience. Their performance in terms of usability, user experience, security and/or privacy is summarized in the following. This provides an answer to RQ4 (How do specific implementations of mobile security and privacy mechanisms perform in terms of usability, user experience, security and/or privacy?).

App permissions

Basic permission dialog. The "basic permission dialog" (i.e. the long list of permissions without icons as featured until 2013/1014 in Google Play, cf. Section 3.3.1) has been found in related work to be hard to understand and to receive little attention by users [61]. Study 4 (cf. Chapter 8) compared users' decision making for different presentations of apps in the app market. When users pressed the "install" button within the "Standard UI", the "basic permission dialog" ap-

peared. The presentation of apps in the "Standard UI" received high pragmatic and attractiveness ratings, and medium-high hedonic quality ratings. As already described in Chapter 2, pragmatic quality is related to the achievement of *behavioral goals* [81, p. 35], whereas hedonic quality describes the capability of a product to communicate aspects of *personal relevance* [81, p. 38]. A product which is highly pragmatic and hedonic can be considered as being desired, whereas a product with high pragmatic and medium hedonic quality can be considered as task-oriented (cf. [47] and Chapter 2.2.2). The above described results indicate that participants were rather satisfied and perceived the "Standard UI" as task-oriented. However, as in related work [78, 112], for this presentation of the apps, participants rather neglected the permissions when making their decision.

Thus, while the "Standard UI" performs well in terms of experiential product qualities, the influence of the permissions on the privacy decisions is limited in this UI.

Statistical information to communicate permission risks. The "Text UI" and the "Graphic UI" provided users with alternative app presentations that included statistical information about app permissions already in the app market description. Experiential product quality ratings for both statistical prototypes were similar to the "Standard UI", with high pragmatic quality and attractiveness ratings, and medium-high hedonic quality ratings. These ratings indicate that participants were also rather satisfied with the interfaces and also perceived them as task-oriented. In terms of felt experience, both statistical UIs positively influenced the importance that participants gave to the permissions in the app selection process. Furthermore, they led users to perceive the app with a higher number of permissions as more privacy-intrusive and less trustworthy. A significant change in behavior (installation rates) was, however, only achieved with the "Graphic UI". The "Graphic UI" further received significantly higher pragmatic quality ratings than the "Standard UI".

In summary, the findings suggest that if statistical information is provided, it should be supported by graphical information as graphical statistical information had a positive influence on user experience *and* privacy-conscious behavior. Note, however, that the influence of statistical information was of pragmatic nature. As such, it positively influenced participants' feelings that the "Graphic UI" is easy to understand and well-arranged.

Runtime UIs. The runtime UIs, introduced in Chapter 9, are user interface prototypes that are currently featured in a similar form on Android (i.e. the runtime UI) and iOS (i.e. runtime UI with and without purpose string). Related work by Andriotis et al. indicates, that Android users prefer the new runtime permission model over the old install-time model [4]. Furthermore, a majority of Android M users

(65%) reported in the same field study that they felt to have more control over their data with the new permission model.

In Study 5 of this thesis (cf. Chapter 9), the runtime UIs received medium-high pragmatic quality ratings and medium-low hedonic quality ratings suggesting that the interfaces were perceived as neutral with a tendency to task-oriented (cf. the definitions by Diefenbach and Hassenzahl [47]). Furthermore, runtime UIs were perceived as more annoying compared to the selective install-time UIs and participants in the runtime conditions felt worse than participants in the selective install-time conditions. While Andriotis et al. [4] found rather positive evaluations of the runtime UI compared to the former install-time UI (the "advanced permission dialog", cf. Section 2.2.2), it is difficult to compare the UX ratings of Study 5 to their results. In their study, participants were asked to compare the new runtime model to the former install-time model, whereas in Study 5, participants were asked to rate the interface and interaction without having an anchor value.

In terms of behavior, users in the runtime UI conditions made more privacy-friendly permission granting decisions, compared to the selective install-time UIs. Thus, runtime UIs seem to perform well in terms of fostering privacy-conscious behavior, but there is space for the improvement of hedonic UI attributes in general and compared to selective install-time UIs.

Selective install-time UIs. The selective install-time UIs with and without purpose strings, introduced in Chapter 9, are suggestions for new permission UIs that provide users with an overview of permissions while at the same time providing the possibility to selectively grant permissions. Thus, they were designed to address aspects of usability and education (with the overview of permissions), as well as psychological need fulfillment (i.e. *Autonomy* through the possibility to selectively grant permissions).

The results of the comparative user study (cf. Chapter 9) suggest that selective install-time UIs perform better in terms of user experience compared to the runtime UIs: whereas pragmatic quality was similarly high for all UIs, especially the selective install-time UI received higher hedonic quality, autonomy, and security ratings than the run-time UI without purpose string. However, participants in the install-time condition made less privacy-conscious permission granting decisions in the presented over-privilege scenario.

Summary: All presented permission prototypes were perceived as highly usable. Some UI interventions led to a significant increase in PQ (graphical statistical information). Others did not have a significant influence on PQ (all other UIs). In any case the effect of the interventions on user behavior, felt experience (perceived privacy, trust for the statistical information) and hedonic product quality (for the selective install-time UIs) was rather high. This suggests the exis-

tence of a multi-dimensional design space for "secure and/or privacy-preserving user experiences" for permission granting.

Screen locks with authentication

PIN. In line with related work [78, 195], PIN was found to be highly usable, both, in the lab and in the field. Whereas in the lab study HQ-Stimulation ratings for PIN were always lower compared to EmojiAuth, in the field study this was only the case on day 2.

EmojiAuth. EmojiAuth is an authentication scheme for screen locking (cf. Chapter 10), designed to provide similar usability and security as the PIN scheme, while allowing for a more positive user experience through higher need fulfillment of *Stimulation*. To counteract an inherent vulnerability of graphical authentication schemes – so called "hotspots" – EmojiAuth features an individual keyboard for each user. The results of lab and field study indicate that Emoji-based passwords which are not selected based on a distinct pattern are slightly harder to shoulder surf compared to PINs. The practical password space of Emoji-passwords seems to be smaller than the theoretical one. Further studies are needed to determine to which degree this finding influences the susceptibility of Emoji-passwords to guessing attacks. Emoji-passwords further showed a high memorability for 4-digit and a reasonable memorability for 6-digit passwords. Both password lengths did not significantly differ in their memorability from PINs of same length.

Summary: The daily feedback in the field study revealed that the user experience with EmojiAuth and PIN was perceived similarly good. The results of the daily feedback further indicate that the usability of mobile authentication schemes seems to have a rather strong influence on the user experience with such schemes, as comments on the good usability of the schemes were among the most frequent codes; hedonic attributes of EmojiAuth were noticed by the users, but only slightly more valued than for PIN in the quantitative ratings (AttrakDiff and daily feedback questionnaires). Nevertheless, EmojiAuth users indicated to favor EmojiAuth over PIN as a screenlock due to high password memorability and the appeal of the EmojiAuth-UI. Future studies should investigate how the hedonic attributes of Emoji-based mobile authentication can be further increased while maintaining the same or a higher level of security.

11.1.5 *Manipulation of hedonic quality*

The following subsection provides an answer to RQ5 (Is it possible to manipulate the hedonic quality of security and privacy mechanisms on smartphones?).

The results of Chapter 9 and 10 suggest that the hedonic quality of mobile security and privacy mechanisms can be manipulated: The studies revealed differences in hedonic quality and/or its sub-dimensions between different run-time and selective install-time UIs, as well as between PIN and EmojiAuth. Given the fact that security and privacy have been mostly considered as secondary tasks, this is a promising finding. The sole consideration of mobile security and privacy mechanisms as secondary tasks limits the design space for the user-centered design of such mechanisms to usability interventions only. However, usability may be only optimized up to a certain point – as long as the mechanisms are not made seamless (e.g. as it is the case for biometric authentication). In many cases, user interaction would still be required (e.g. for fallback authentication or privacy decisions related to app permissions). The results suggest that including aspects of hedonic quality seems to be feasible and would extend the design space of mobile security and privacy mechanisms beyond usability towards positive user experiences with such mechanisms. How hedonic quality perceptions can be maintained on a high level over time, is an interesting research question for future studies.

11.1.6 *Experience over time*

For the mobile authentication use case, user experience was determined at several points in time. Consequently, the evaluation of those UX ratings provides an answer to RQ6 (How does the user experience with a mobile security mechanism develop over time?).

PIN and EmojiAuth (Lab study). The PIN scheme (with which participants were already familiar when they arrived at the lab study) was immediately perceived as highly usable. In contrast, EmojiAuth received medium usability ratings (PQ) in the first lab study session which improved in the second session of the lab study. EmojiAuth users further reported more positive affect in the second session. Increased HQ ratings for both schemes in the second session suggest that factors of personal relevance were perceived higher in week 2. A reason for this might be grounded in the success that all participants experienced when they managed to enter their password at least once correctly again. Higher HQ-Stimulation ratings for EmojiAuth compared to PIN in both sessions suggest that participants who used EmojiAuth perceived EmojiAuth as stimulating, even in week 2, when EmojiAuth was not a completely new experience for them.

PIN and EmojiAuth (Field study). The user experience with both authentication schemes developed differently in the field study setting. While usability was perceived similarly good for both schemes, PIN received rather low HQ ratings in the beginning which, however, in-

creased during the course of the study. Difference between the lab and the field study may be grounded in the fact, that participants in the lab study were asked to rate the scheme directly after the first interaction. In the field study, the first AttrakDiff questionnaire appeared on day 2. Furthermore, participants in the lab study rated their second interaction in week 2, whereas participants in the field study had already interacted several times with the scheme when they rated it for the first time.

Summary. The results suggest that the adoption of mobile authentication mechanisms may follow a similar process as described by Karapanos et al. [109]: *Orientation*, *Incorporation*, and *Identification*. *Orientation* is informed by getting *familiar* with a product and is reflected in *stimulation* and *learnability* ratings [109, p. 732]. *Incorporation* is informed by *functional dependency*, reflected in the perceived *long-term usability* and *usefulness* [109, p. 732]. Last, *Identification* is informed by *emotional attachment* either of *personal* or *social* nature [109, p. 732]. In the mobile authentication studies, participants first had to get familiar with the scheme as reflected in the lab study PQ ratings and the respective daily feedback codes in the field study. EmojiAuth HQ-Stimulation ratings were in both studies higher for the first few interactions, compared to PIN.

In the field study, for both schemes, participants frequently mentioned good usability and that everything is going fine during the study. Furthermore, they mentioned that they had gotten familiar with the scheme, indicating a transition from *Orientation* to *Incorporation*. As the field study ended after two weeks, it is likely that participants had not reached the *Identification* phase yet. An interesting research question for future studies would be, whether mobile security and privacy mechanisms can enable a strong identification with the mechanisms, such as it can be developed with lifestyle products (Karapanos et al. [109] have investigated the adoption of an iPhone in their paper).

11.2 LIMITATIONS

The presented studies, and thereby especially those in which different prototypes were tested, rather focused on Android users. This might have influenced the results. However, as the Android platform has currently a huge market share of more than 80% [179], the results may nevertheless apply to a non-neglible group of users.

The present thesis has evaluated behavior and user experience during permission granting in a lab study (cf. Chapter 8) and an online study (cf. Chapter 9). The context in these studies was different from real life situations. Earlier related works on app permissions suggest that online studies yield similar results than field [8] and lab studies [79, 112]. However, further studies are needed to determine how the

results of the permission studies in this thesis translate to the real world.

11.3 FUTURE WORK

While the conclusion has provided several insights on the user experience with mobile security and privacy mechanisms, it also identified several issues that should be addressed in future research on experience-based mobile security and privacy. Those will be detailed in the following.

11.3.1 *Further security and privacy evaluations*

Permissions in Context. The statistical information about the number of permissions in comparison to apps with similar functionality has been tested for the install-time permission model. This permission model is likely to disappear on future smartphones, as newer Android versions deploy the runtime permission model and iOS has always been using the runtime model. Showing additional information in the app market could, however, help privacy-sensitive users to make better decisions which app they should download [8]. Thus, it would be an interesting research question whether users would value this kind of additional information, despite the new permission model. Currently, statistical information about the number of apps that use a specific permission is also provided in the permission settings. Evaluating this functionality regarding its usefulness for mobile privacy management is also an interesting research question that could be addressed in future studies.

Security and user experience of Emoji-based passwords. This thesis has contributed an evaluation of the shoulder-surfing susceptibility of Emoji-based passwords. It has also identified different strategies for Emoji-password selection. The analysis of the passwords that were generated in the lab and the field study suggest that the password distribution of Emoji-based passwords may be skewed. A question that would need to be addressed in future studies is to which degree the password distribution is skewed and which impact this has on the susceptibility to guessing attacks. Thereby, the susceptibility of passwords generated under each strategy should be investigated. If the results would show that there are more and less secure strategies, further investigations could be done on how to incentivize users to select their passwords based on a more secure strategy. Another investigation could address the deployment of password creation policies on memorability and user experience.

11.3.2 *Conceptualization of the experiential design for mobile security and privacy*

This thesis has provided directions for the experiential design of mobile security and privacy mechanisms. The usability, user experience, security and privacy of app permission and mobile authentication prototypes has been investigated in exemplary cases. It has been shown that the user experience, and thereby especially the hedonic quality of such mechanisms can be manipulated.

Frameworks and tools. Future work should investigate how aspects of hedonic quality and positive user experience can be systematically manipulated by interventions in UI and interaction design. Validated frameworks and tools for the experiential design of security and privacy mechanisms would be valuable to translate the gained knowledge into design guidelines for developers of security and privacy mechanisms. Thereby, a starting point could be a taxonomy of UI and design factors which influence the user experience, e.g. in terms of psychological need fulfillment.

Further questionnaire validations. This thesis deployed questionnaires for the evaluation of mobile security and privacy mechanisms which have been originally developed in other contexts (e.g. positive psychology [175], interactive products [84], clinical studies [196]). Thus, it would be useful to further validate these questionnaires in future studies in a security and privacy-related context and to adjust them, if necessary.

11.3.3 *Long-term user experience and behavior*

The field study on mobile authentication provided insights into the daily usage of EmojiAuth in comparison to PIN. It further illustrated, together with the lab study on mobile authentication, how user experience can change over time.

As all studies were limited to at most two weeks, further studies are needed to investigate the long-term user experience and behavior related to mobile security and privacy mechanisms. This should be also investigated for a broader set of mechanisms. Future studies could answer the question of whether users could identify themselves with mobile security and privacy mechanisms. Related work from the domain of user experience suggests that positive user experience has a positive impact on adoption and product bonding (cf. e.g. [68]). It would be desirable if a similar relationship would also apply for mobile security and privacy mechanisms. Thus, future work should investigate the influence of positive user experiences on adoption and on security- and privacy-conform voluntary behavior.

11.3.4 *Mechanisms and application areas beyond mobile*

This thesis has focused on two use cases of mobile security and privacy mechanisms: app permissions and mobile authentication.

Other mobile mechanisms. The described uses cases offer first insights into the experiential design of mobile security and privacy mechanisms.

Future work should evaluate whether the gathered insights could be also transferred to other mobile security and privacy mechanisms. For example, social and messaging apps have been identified in Chapter 5 and 6 as artifacts that are able to evoke both, strong positive and strong negative experiences (cf. also [108]). These kind of applications have been already intensively studied in user experience research (cf. e.g. [34, 94, 108, 208]) and (usable) security and privacy research (cf. e.g. [45, 148, 173]. An analysis of studies in both areas could further help to solve issues related to negative experiences and (technical) security and privacy issues. Other application examples of mobile mechanisms are update notifications, browser security, and the set up of device encryption. Besides understanding the interaction with current mechanisms, experiential approaches could further allow to innovate new mechanisms.

Beyond smartphones. The insights provided in this thesis could be further deployed to security and privacy mechanisms in other contexts. For example, Vaniea et al. found negative experiences with software update notifications as a possible source of negative influence on future update behavior [192]. Helping users in managing software updates with joy would be an interesting application area for the findings of this thesis.

Another application area that is closely related to smartphones and mobile computing, is the internet of things. Thereby, especially the area of smart home applications seems to be good fit for the experiential design of security and privacy mechanisms. Smart home scenarios integrate and connect smart everyday devices such as TVs or household appliances. Those devices are integrated into users' everday life and – as smartphones – offer a high potential for positive user experiences, but they also contain attack vectors. For example, by assigning unique user IDs, some smart TVs revealed vulnerabilities to privacy threats [104]. Integrating proper privacy controls into such devices that either offer or accompany positive user experiences would be an interesting application area for experiential design.

Part VI

APPENDIX

BIBLIOGRAPHY

[1] Anne Adams and Martina Angela Sasse. "Users are not the enemy." In: *Communications of the ACM* 42.12 (1999), pp. 40–46.

[2] All about UX. *Semi-structured experience interview*. `http://www.allaboutux.org/semi-structured-experience-interview`. (accessed: 2017-01-17).

[3] All about UX. *Timed ESM*. `http://www.allaboutux.org/timed-esm`. (accessed: 2017-01-17).

[4] Panagiotis Andriotis, Martina Angela Sasse, and Gianluca Stringhini. "Permissions Snapshots: Assessing Users' Adaptation to the Android Runtime Permission Model." In: *Proceedings of the IEEE International Workshop on Information Forensics and Security (WIFS)*. 2016.

[5] Apple Inc. *About Touch ID security on iPhone and iPad*. `https://support.apple.com/en-us/HT204587`. (accessed: 2017-01-04).

[6] Md Tanvir Islam Aumi and Sven Kratz. "AirAuth: evaluating in-air hand gestures for authentication." In: *Proceedings of the 16th International Conference on Human-Computer Interaction with Mobile Devices & Services (mobileHCI)*. ACM. 2014, pp. 309–318.

[7] Adam J Aviv, Katherine Gibson, Evan Mossop, Matt Blaze, and Jonathan M Smith. "Smudge Attacks on Smartphone Touch Screens." In: *4th USENIX Workshop on Offensive Technologies (WOOT)*. 2010, pp. 1–7.

[8] Rebecca Balebako, Florian Schaub, Idris Adjerid, Alessandro Acquisti, and Lorrie Cranor. "The Impact of Timing on the Salience of Smartphone App Privacy Notices." In: *Proceedings of the 5th Annual ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices (SPSM)*. ACM. 2015, pp. 63–74.

[9] Javier A Bargas-Avila and Kasper Hornbæk. "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)*. ACM. 2011, pp. 2689–2698.

[10] Javier Bargas-Avila and Kasper Hornbæk. "Foci and blind spots in user experience research." In: *interactions* 19.6 (2012), pp. 24–27.

[11] David Barrera, H Güneş Kayacik, Paul C van Oorschot, and Anil Somayaji. "A methodology for empirical analysis of permission-based security models and its application to android." In: *Proceedings of the 17th ACM Conference on Computer and Communications Security (CCS)*. ACM. 2010, pp. 73–84.

[12] Noam Ben-Asher, Niklas Kirschnick, Hanul Sieger, Joachim Meyer, Asaf Ben-Oved, and Sebastian Möller. "On the need for different security methods on mobile phones." In: *Proceedings of the 13th International Conference on Human Computer Interaction with Mobile Devices and Services (mobileHCI)*. ACM. 2011, pp. 465–473.

[13] Kevin Benton, L Jean Camp, and Vaibhav Garg. "Studying the effectiveness of android application permissions requests." In: *IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops)*. 2013, pp. 291–296.

[14] Chandrasekhar Bhagavatula, Blase Ur, Kevin Iacovino, Su Mon Kywe, Lorrie Faith Cranor, and Marios Savvides. "Biometric authentication on iphone and android: Usability, perceptions, and influences on adoption." In: *Proceedingf of the Workshop on Usable Security (USEC)* (2015).

[15] Kemal Bicakci, Nart Bedin Atalay, Mustafa Yuceel, Halan Gurbaslar, and Burak Erdeniz. "Towards usable solutions to graphical password hotspot problem." In: *33rd Annual IEEE International Computer Software and Applications Conference (COMPSAC)*. Vol. 2. 2009, pp. 318–323.

[16] Kemal Bicakci, Nart Bedin Atalay, Mustafa Yuceel, and Paul C van Oorschot. "Exploration and field study of a password manager using icon-based passwords." In: *Financial Cryptography and Data Security (FC)*. 2011, pp. 104–118.

[17] Robert Biddle, Sonia Chiasson, and Paul C Van Oorschot. "Graphical passwords: Learning from the first twelve years." In: *ACM Computing Surveys (CSUR)* 44.4 (2012), p. 19.

[18] Matt Bishop. "What is computer security?" In: *IEEE Security & Privacy* 1.1 (2003), pp. 67–69.

[19] Matt Bishop. "Psychological acceptability revisited." In: *Security and Usability* (2005), pp. 1–12.

[20] Susanne Bødker. "Activity theory as a challenge to systems design." In: *DAIMI Report Series* 19.334 (1990).

[21] Susanne Bødker, Niels Mathiasen, and Marianne Graves Petersen. "Modeling is Not the Answer!: Designing for Usable Security." In: *interactions* 19.5 (2012), pp. 54–57.

[22] Joseph Bonneau, Sören Preibusch, and Ross Anderson. "A birthday present every eleven wallets? The security of customer-chosen banking PINs." In: *Financial Cryptography and Data Security (FC)*. 2012, pp. 25–40.

[23] Jürgen Bortz and Nicola Döring. *Forschungsmethoden und Evaluation für Human-und Sozialwissenschaftler*. Springer-Verlag, 2007.

[24] Jan Lauren Boyles, Aaron Smith, and Mary Madden. "Privacy and data management on mobile devices." In: *Pew Internet & American Life Project* 4 (2012).

[25] Margaret M Bradley and Peter J Lang. "Measuring emotion: the self-assessment manikin and the semantic differential." In: *Journal of behavior therapy and experimental psychiatry* 25.1 (1994), pp. 49–59.

[26] Brenden Mulligan. *The Right Way to Ask Users for Mobile Permissions - How Cluster dramatically increased iOS access conversion*. `https://library.launchkit.io/the-right-way-to-ask-users-for-ios-permissions-96fa4eb54f2c#.eqtrikl91`. (accessed: 2016-11-11).

[27] John Brooke et al. "SUS-A quick and dirty usability scale." In: *Usability evaluation in industry* 189.194 (1996), pp. 4–7.

[28] Bobby J Calder. "Focus groups and the nature of qualitative marketing research." In: *Journal of Marketing research* (1977), pp. 353–364.

[29] Gamze Canova, Melanie Volkamer, Clemens Bergmann, and Roland Borza. "NoPhish: An Anti-Phishing Education App." In: *Security and Trust Management (STM)*. Springer, 2014, pp. 188–192.

[30] Charles S Carver and Michael F Scheier. *On the self-regulation of behavior*. Cambridge University Press, 1989.

[31] Sonia Chiasson, Paul C van Oorschot, and Robert Biddle. "Graphical password authentication using cued click points." In: *European Symposium on Research in Computer Security (ESORICS)*. Springer. 2007, pp. 359–374.

[32] Erika Chin, Adrienne Porter Felt, Vyas Sekar, and David Wagner. "Measuring user confidence in smartphone security and privacy." In: *Proceedings of the Eighth Symposium on Usable Privacy and Security (SOUPS)*. ACM. 2012, p. 1.

[33] Ravindra Chitturi, Rajagopal Raghunathan, and Vijay Mahajan. "Delight by design: The role of hedonic versus utilitarian benefits." In: *Journal of Marketing* 72.3 (2008), pp. 48–63.

[34] Karen Church and Rodrigo de Oliveira. "What's up with whatsapp?: comparing mobile instant messaging behaviors with traditional SMS." In: *Proceedings of the 15th International Conference on Human-Computer Interaction with Mobile Devices and Services (mobileHCI)*. ACM. 2013, pp. 352–361.

[35] Gradeigh D Clark, Swapnil Sarode, and Janne Lindqvist. "No time at all: opportunity cost of Android permissions." In: *Proc. of the 3rd Workshop on Hot Topics in Wireless*. ACM. 2016, pp. 12–16.

[36] Paula Cocozza. *Crying with laughter: how we learned how to speak emoji*. `http://www.theguardian.com/technology/2015/nov/17/crying-with-laughter-how-we-learned-how-to-speak-emoji`. (accessed: 2016-02-19).

[37] Juliet Corbin and Anselm Strauss. *Basics of qualitative research: Techniques and procedures for developing grounded theory*. Sage publications, 2014.

[38] Passfaces Corporation. *White Paper: The Science Behind Passfaces*. Tech. rep. Elon University.

[39] Lorrie Faith Cranor. "A framework for reasoning about the human in the loop." In: *Proceedings of the 1st Conference on Usability, Psychology, and Security (UPSEC)*. 2008, pp. 1–15.

[40] Lorrie Faith Cranor and Simson Garfinkel. *Security and usability: designing secure systems that people can use*. O'Reilly Media, Inc., 2005.

[41] Andrew Cunningham. *Google Play apps and updates are now subject to a review process*. `http://arstechnica.com/gadgets/2015/03/google-play-apps-and-updates-are-now-subject-to-a-review-process/`. (accessed: 2016-10-08). 2015.

[42] Darren Davis, Fabian Monrose, and Michael K Reiter. "On User Choice in Graphical Password Schemes." In: *USENIX Security Symposium*. Vol. 13. 2004, pp. 11–11.

[43] Alexander De Luca, Alina Hang, Frederik Brudy, Christian Lindner, and Heinrich Hussmann. "Touch me once and I know it's you!: implicit authentication based on touch screen patterns." In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI)*. ACM. 2012, pp. 987–996.

[44] Alexander De Luca, Alina Hang, Emanuel Von Zezschwitz, and Heinrich Hussmann. "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)*. ACM. 2015, pp. 1411–1414.

[45] Alexander De Luca, Sauvik Das, Martin Ortlieb, Iulia Ion, and Ben Laurie. "Expert and Non-Expert Attitudes towards (Secure) Instant Messaging." In: *Twelfth Symposium on Usable Privacy and Security (SOUPS)*. 2016, pp. 147–157.

[46] Edward L Deci and Richard M Ryan. "The" what" and" why" of goal pursuits: Human needs and the self-determination of behavior." In: *Psychological inquiry* 11.4 (2000), pp. 227–268.

[47] Sarah Diefenbach and Marc Hassenzahl. *Handbuch zur Fun-ni Toolbox*. 2011.

[48] Sarah Diefenbach, Nina Kolb, and Marc Hassenzahl. "The 'Hedonic' in Human-Computer Interaction: History, Contributions, and Future Research Directions." In: *Proceedings of the 2014 Conference on Designing Interactive Systems (DIS)*. 2014, pp. 305–314.

[49] Brian Donohue. *WireLurker Apple Malware Targets Mac OS X Then iOS*. `https://usblog.kaspersky.com/wirelurker-ios-osx-malware/4781/`. (accessed: 2016-10-09). 2014.

[50] Paul Dourish and Ken Anderson. "Collective information practice: emploring privacy and security as social and cultural phenomena." In: *Human-computer interaction* 21.3 (2006), pp. 319–342.

[51] Paul Dunphy, John Vines, Lizzie Coles-Kemp, Rachel Clarke, Vasilis Vlachokyriakos, Peter Wright, John McCarthy, and Patrick Olivier. "Understanding the Experience-Centeredness of Privacy and Security Technologies." In: *Proceedings of the 2014 Workshop on New Security Paradigms (NSPW)*. 2014, pp. 83–94.

[52] Paul Dunphy, Vasilis Vlachokyriakos, Anja Thieme, James Nicholso, John McCarthy, and Patrick Olivier. "Social Media as a Resource of Security Experiences: A Qualitative Analysis of #Password Tweets." In: *Proceedings of the Eleventh Symposium On Usable Privacy and Security (SOUPS)*. 2015, pp. 123–140.

[53] Serge Egelman, Adrienne Porter Felt, and David Wagner. "Choice architecture and smartphone privacy: There's a price for that." In: *The Economics of Information Security and Privacy*. Springer, 2013, pp. 211–236.

[54] Serge Egelman, Sakshi Jain, Rebecca S Portnoff, Kerwell Liao, Sunny Consolvo, and David Wagner. "Are you ready to lock?" In: *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security (CCS)*. ACM. 2014, pp. 750–761.

[55] Karin Eilers, Friedhelm Nachreiner, and Kerstin Hänecke. "Entwicklung und Überprüfung einer Skala zur Erfassung subjektiv erlebter Anstrengung." In: *Zeitschrift für Arbeitswissenschaft* 4 (1986), pp. 214–224.

[56] Nikolay Elenkov. *Android Security Internals: An In-Depth Guide to Android's Security Architecture*. No Starch Press, 2015.

[57] S Epstein. *Cognitive-Experiential Self-Theory. Handbook of Personality: theory and research/ed. Pervin L. A*. 1990.

[58] Sascha Fahl, Marian Harbach, Yasemin Acar, and Matthew Smith. "On the ecological validity of a password study." In: *Proceedings of the ninth Symposium on Usable Privacy and Security (SOUPS)*. 2013, p. 13.

[59] Adrienne Porter Felt, Serge Egelman, and David Wagner. "I've got 99 problems, but vibration ain't one: a survey of smartphone users' concerns." In: *Proceedings of the Second ACM Workshop on Security and Privacy in Smartphones and Mobile Devices (SPSM)*. ACM. 2012, pp. 33–44.

[60] Adrienne Porter Felt, Erika Chin, Steve Hanna, Dawn Song, and David Wagner. "Android permissions demystified." In: *Proceedings of the 18th ACM Conference on Computer and Communications Security (CCS)*. ACM. 2011, pp. 627–638.

[61] Adrienne Porter Felt, Elizabeth Ha, Serge Egelman, Ariel Haney, Erika Chin, and David Wagner. "Android permissions: User attention, comprehension, and behavior." In: *Proceedings of the Eighth Symposium on Usable Privacy and Security (SOUPS)*. ACM. 2012, p. 3.

[62] Adrienne Porter Felt, Serge Egelman, Matthew Finifter, Devdatta Akhawe, David Wagner, et al. "How to Ask for Permission." In: *Proceedings of the 7th USENIX conference on Hot Topics in Security (HotSec)*. 2012.

[63] Andy Field. *Discovering statistics using SPSS*. Sage publications, 2009.

[64] Ruth Filik, Alexandra Turcan, Dominic Thompson, Nicole Harvey, Harriet Davies, and Amelia Turner. "Sarcasm and emoticons: Comprehension and emotional impact." In: *The Quarterly Journal of Experimental Psychology* (2015), pp. 1–17.

[65] Dinei Florêncio, Cormac Herley, and Paul C Van Oorschot. "An administrator's guide to internet password research." In: *Proceedings of the 28th USENIX conference on Large Installation System Administration (LISA)*. 2014, pp. 35–52.

[66] Alain Forget, Sarah Pearman, Jeremy Thomas, Alessandro Acquisti, Nicolas Christin, Lorrie Faith Cranor, Serge Egelman, Marian Harbach, and Rahul Telang. "Do or Do Not, There Is No Try: User Engagement May Not Improve Security Outcomes." In: *Proceedings of the Twelfth Symposium on Usable Privacy and Security (SOUPS)*. 2016, pp. 97–111.

[67] Mario Frank, Ben Dong, Adrienne Porter Felt, and Dawn Song. "Mining permission request patterns from android and facebook applications." In: *Proceedings of the 12th IEEE International Conference on Data Mining (ICDM)*. 2012, pp. 870–875.

[68] Nora Fronemann and Matthias Peissner. "User experience concept exploration: user needs as a source for innovation." In: *Proceedings of the 8th Nordic Conference on Human-Computer Interaction (nordiCHI): Fun, Fast, Foundational*. ACM. 2014, pp. 727–736.

[69] Simson Garfinkel and Heather Richter Lipford. "Usable security: History, themes, and challenges." In: *Synthesis Lectures on Information Security, Privacy, and Trust* 5.2 (2014), pp. 1–124.

[70] Jesse James Garrett. "Customer loyalty and the elements of user experience." In: *Design management review* 17.1 (2006), pp. 35–39.

[71] Aaron Gingrich. *Google Brings In The Muscle: Meet Bouncer, The Market's Anti-Malware Machine - And It's Already At Work*. `http://www.androidpolice.com/2012/02/02/google-brings-in-the-muscle-meet-bouncer-the-markets-anti-malware-machine-and-its-already-at-work/`. (accessed: 2016-10-08). 2012.

[72] Maximilian Golla, Dennis Detering, and Markus Dürmuth. "EmojiAuth: Quantifying the Security of Emoji-based Authentication." In: *Proceedings of the Usable Security Mini Conference (USEC)*. 2017.

[73] Google Inc. *Set up your device for automatic unlock*. `https://support.google.com/nexus/answer/6093922`. (accessed: 2017-01-04).

[74] Google Inc. *Unlock with your fingerprint*. `https://support.google.com/nexus/answer/6285273`. (accessed: 2017-01-04).

[75] Bo Han, Andy Wu, and Jon Windsor. "User's Adoption of Free Third Party Security Apps." In: *Journal of Computer Information Systems* 54.3 (2014), pp. 77–86.

[76] Alina Hang, Alexander De Luca, Matthew Smith, Michael Richter, and Heinrich Hussmann. "Where Have You Been? Using Location-Based Security Questions for Fallback Authentication." In: *Proceedings of the Eleventh Symposium On Usable Privacy and Security (SOUPS)*. 2015, pp. 169–183.

[77] SM Taiabul Haque, Shannon Scielzo, and Matthew Wright. "Applying psychometrics to measure user comfort when constructing a strong password." In: *Proceedings of the tenth Symposium On Usable Privacy and Security (SOUPS)*. 2014, pp. 231–242.

[78] Marian Harbach, Emanuel von Zezschwitz, Andreas Fichtner, Alexander De Luca, and Matthew Smith. "It's a hard lock life: A field study of smartphone (un) locking behavior and risk perception." In: *Proceedings of the Tenth Symposium on Usable Privacy and Security (SOUPS)*. 2014.

[79] Marian Harbach, Markus Hettig, Susanne Weber, and Matthew Smith. "Using personal examples to improve risk communication for security & privacy decisions." In: *Proceedings of the 32nd annual ACM conference on Human factors in computing systems (CHI)*. ACM. 2014, pp. 2647–2656.

[80] Marian Harbach, Alexander De Luca, Nathan Malkin, and Serge Egelman. "Keep on Lockin'in the Free World: A Multi-National Comparison of Smartphone Locking." In: *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*. ACM. 2016, pp. 4823–4827.

[81] Marc Hassenzahl. "The thing and I: understanding the relationship between user and product." In: *Funology*. Springer, 2003, pp. 31–42.

[82] Marc Hassenzahl. "User experience (UX): towards an experiential perspective on product quality." In: *Proceedings of the 20th Conference on l'Interaction Homme-Machine*. ACM. 2008, pp. 11–15.

[83] Marc Hassenzahl. "Experience design: Technology for all the right reasons." In: *Synthesis Lectures on Human-Centered Informatics* 3.1 (2010), pp. 1–95.

[84] Marc Hassenzahl, Michael Burmester, and Franz Koller. "AttrakDiff: Ein Fragebogen zur Messung wahrgenommener hedonischer und pragmatischer Qualität." In: *Mensch & Computer 2003*. Springer, 2003, pp. 187–196.

[85] Marc Hassenzahl, Sarah Diefenbach, and Anja Göritz. "Needs, affect, and interactive products–Facets of user experience." In: *Interacting with computers* 22.5 (2010), pp. 353–362.

[86] Marc Hassenzahl and Andrew Monk. "The inference of perceived usability from beauty." In: *Human–Computer Interaction* 25.3 (2010), pp. 235–260.

[87] Marc Hassenzahl and Noam Tractinsky. "User experience – a research agenda." In: *Behaviour & information technology* 25.2 (2006), pp. 91–97.

[88] Eiji Hayashi and Jason Hong. "A diary study of password usage in daily life." In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI)*. ACM. 2011, pp. 2627–2630.

[89] Eiji Hayashi, Rachna Dhamija, Nicolas Christin, and Adrian Perrig. "Use your illusion: secure authentication usable anywhere." In: *Proceedings of the 4th Symposium on Usable Privacy and Security (SOUPS)*. ACM. 2008, pp. 35–45.

[90] Joel M Hektner, Jennifer A Schmidt, and Mihaly Csikszentmihalyi. *Experience sampling method: Measuring the quality of everyday life*. Sage, 2007.

[91] Markus Hettig, Eugen Kiss, Jan-Frederik Kassel, Susanne Weber, Marian Harbach, and Matthew Smith. "Visualizing Risk by Example: Demonstrating Threats Arising From Android Apps." In: *Symposium on Usable Privacy and Security (SOUPS)*. 2013.

[92] Ulrich Hoffrage, Samuel Lindsey, Ralph Hertwig, and Gerd Gigerenzer. "Communicating statistical information." In: *Science* 290.5500 (2000), pp. 2261–2262.

[93] Giles Hogben and Marnix Dekker. "Smartphones: Information security risks, opportunities and recommendations for users." In: *European Network and Information Security Agency* 710.01 (2010).

[94] Yifeng Hu, Jacqueline Fowler Wood, Vivian Smith, and Nalova Westbrook. "Friendships through IM: Examining the relationship between instant messaging and intimacy." In: *Journal of Computer-Mediated Communication* 10.1 (2004), pp. 00–00.

[95] ISO/IEC. *ISO/IEC 2382-8: Information technology—Vocabulary—Part 8:Security.* 1998.

[96] Apple Inc. *iPhone User Guide – Privacy and Security – Privacy – Location Services*. `http://help.apple.com/iphone/10/`. (accessed: 2016-10-22).

[97] Apple Inc. *iOS Security - White Paper*. `https://www.apple.com/business/docs/iOS_Security_Guide.pdf`. (accessed: 2016-10-05). 2016.

[98] Philip G Inglesant and M Angela Sasse. "The true cost of unusable password policies: password use in the wild." In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI)*. ACM. 2010, pp. 383–392.

[99] Philip Inglesant and M Angela Sasse. "Studying password use in the wild: practical problems and possible solutions." In: *SOUPS: Workshop on Usable Security Experiment Reports*. 2010.

[100] Initiative D21 and Huawei Technologies. *Mobile Internetnutzung – Gradmesser für die digitale Gesellschaft*. `http://www.initiative21.de/wp-content/uploads/2014/12/Mobile-Internetnutzung-2014_WEB.pdf`. (accessed: 2016-04-25).

[101] Intelligent Environments. *Now you can log into your bank using emoji*. http://www.intelligentenvironments.com/info-centre/press-releases/now-you-can-log-into-your-bank-using-emoji-1. (accessed: 2016-02-19).

[102] Iulia Ion, Rob Reeder, and Sunny Consolvo. ""... no one can hack my mind": Comparing Expert and Non-Expert Security Practices." In: *Proceedings of the Eleventh Symposium On Usable Privacy and Security (SOUPS)*. 2015, pp. 327–346.

[103] Carroll E Izard. "The many meanings/aspects of emotion: Definitions, functions, activation, and regulation." In: *Emotion Review* 2.4 (2010), pp. 363–370.

[104] Aline Jaritz and Luigi Lo Iacono. "Untersuchung des Datenverkehrs aktueller Smart-TVs." In: *Datenschutz und Datensicherheit-DuD* 40.8 (2016), pp. 511–518.

[105] Ian Jermyn, Alain J Mayer, Fabian Monrose, Michael K Reiter, Aviel D Rubin, et al. "The Design and Analysis of Graphical Passwords." In: *USENIX Security Symposium*. 1999.

[106] Eric J Johnson, Steven Bellman, and Gerald L Lohse. "Defaults, framing and privacy: Why opting in-opting out." In: *Marketing Letters* 13.1 (2002), pp. 5–15.

[107] Daniel Kahneman, Alan B Krueger, David A Schkade, Norbert Schwarz, and Arthur A Stone. "A survey method for characterizing daily life experience: The day reconstruction method." In: *Science* 306.5702 (2004), pp. 1776–1780.

[108] Evangelos Karapanos, Pedro Teixeira, and Ruben Gouveia. "Need fulfillment and experiences on social media: A case on Facebook and WhatsApp." In: *Computers in Human Behavior* 55 (2016), pp. 888–897.

[109] Evangelos Karapanos, John Zimmerman, Jodi Forlizzi, and Jean-Bernard Martens. "User Experience Over Time: An Initial Framework." In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI)*. ACM. 2009, pp. 729–738.

[110] Michael Karlesky, Edward Melcer, and Katherine Isbister. "Open sesame: re-envisioning the design of a gesture-based access control system." In: *CHI'13 Extended Abstracts on Human Factors in Computing Systems*. ACM. 2013, pp. 1167–1172.

[111] Joseph 'Jofish' Kaye. "Self-reported password sharing strategies." In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI)*. ACM. 2011, pp. 2619–2622.

[112] Patrick Gage Kelley, Lorrie Faith Cranor, and Norman Sadeh. "Privacy as part of the app decision-making process." In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI)*. ACM. 2013, pp. 3393–3402.

[113] Gordon Kelly. *Report: 97% Of Mobile Malware Is On Android. This Is The Easy Way You Stay Safe*. http://www.forbes.com/sites/gordonkelly/2014/03/24/report-97-of-mobile-malware-is-on-android-this-is-the-easy-way-you-stay-safe/. (accessed: 2016-10-09). 2014.

[114] Dacher Keltner, Keith Oatley, and Jennifer M Jenkins. *Understanding emotions*. 3rd ed. John Wiley & Sons, 2013.

[115] Hyoungshick Kim and Jun Ho Huh. "PIN selection policies: Are they really effective?" In: *Computers & Security* 31.4 (2012), pp. 484–496.

[116] Niklas Kirschnick, Sven Kratz, and Sebastian Möller. "Poster: An Improved Approach to Gesture-Based Authentication for Mobile Devices." In: *Symposium on Usable Privacy and Security (SOUPS)*. 2010.

[117] Eric Klieme, Klaus-Peter Engelbrecht, and Sebastian Möller. "Poster: Towards Continuous Authentication Based On Mobile Messaging App Usage." In: *Symposium on Usable Privacy and Security (SOUPS)*. 2014.

[118] Saranga Komanduri, Richard Shay, Patrick Gage Kelley, Michelle L Mazurek, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, and Serge Egelman. "Of passwords and people: measuring the effect of password-composition policies." In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI)*. ACM. 2011, pp. 2595–2604.

[119] Lydia Kraus, Ina Wechsung, and Sebastian Möller. "A comparison of privacy and security knowledge and privacy concern as influencing factors for mobile protection behavior." In: *SOUPS: Workshop on Privacy Personas and Segmentation (PPS)*. 2014.

[120] Lydia Kraus, Ina Wechsung, and Sebastian Möller. "Using Statistical Information to Communicate Android Permission Risks to Users." In: *Proceedings of the 4th Workshop on Socio-Technical Aspects in Security and Trust (STAST)*. IEEE. 2014, pp. 48–55.

[121] Lydia Kraus, Ina Wechsung, and Sebastian Möller. "Exploring Psychological Need Fulfillment for Security and Privacy Actions on Smartphones." In: *Proceedings of the 1st European Workshop on Usable Security (EuroUSEC)*. 2016.

[122] Lydia Kraus, Ina Wechsung, and Sebastian Möller. "Psychological Needs as Motivators for Security and Privacy Actions on Smartphones." In: *Journal of Information Security and Applications (JISA)* 34P1 (2017), pp. 34–45.

[123] Lydia Kraus, Tobias Fiebig, Viktor Miruchna, Sebastian Möller, and Asaf Shabtai. "Analyzing end-users' knowledge and feelings surrounding smartphone security and privacy." In: *Proceedings of the Workshop on Mobile Security Technologies (MoST). IEEE S&P Workshops.* (2015).

[124] Lydia Kraus, Jan-Niklas Antons, Felix Kaiser, and Sebastian Möller. "User Experience in Authentication Research: A survey." In: *Proceedings 5th ISCA/DEGA Workshop on Perceptual Quality of Systems (PQS)*. 2016.

[125] Lydia Kraus, Robert Schmidt, Marcel Walch, Florian Schaub, and Sebastian Möller. "On the Use of Emojis in Mobile Authentication." In: *32nd International Conference on ICT Systems Security and Privacy Protection (IFIP SEC). IFIP Advances in Information and Communication Technology, vol 502*. Springer. 2017, pp. 265–280.

[126] Heinz W Krohne, Boris Egloff, Carl-Walter Kohlmann, and Anja Tausch. "Untersuchungen mit einer deutschen Version der 'Positive and Negative Affect Schedule' (PANAS)." In: *Diagnostica* 42.2 (1996), pp. 139–156.

[127] Jon A Krosnick. "Survey research." In: *Annual review of psychology* 50.1 (1999), pp. 537–567.

[128] Sari Kujala, Virpi Roto, Kaisa Väänänen-Vainio-Mattila, Evangelos Karapanos, and Arto Sinnelä. "UX Curve: A method for evaluating long-term user experience." In: *Interacting with Computers* 23.5 (2011), pp. 473–483.

[129] J Richard Landis and Gary G Koch. "The measurement of observer agreement for categorical data." In: *biometrics* (1977), pp. 159–174.

[130] Peter J Lang. "The mechanics of desensitization and the laboratory study of human fear." In: *Behavior therapy: Appraisal and status. New York: McGraw-Hill* (1969), pp. 160–191.

[131] Peter J Lang. "Behavioral treatment and bio-behavioral assessment: Computer applications." In: *Technology in mental health care delivery systems* (1980), pp. 119–137.

[132] Effie Lai-Chong Law. "The measurability and predictability of user experience." In: *Proceedings of the 3rd ACM SIGCHI Symposium on Engineering Interactive Computing Systems (EICS)*. ACM. 2011, pp. 1–10.

[133] Effie Lai-Chong Law, Virpi Roto, Marc Hassenzahl, Arnold POS Vermeeren, and Joke Kort. "Understanding, scoping and defining user experience: a survey approach." In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI)*. ACM. 2009, pp. 719–728.

[134] Scott Lederer, Jason I Hong, Anind K Dey, and James A Landay. "Personal privacy through understanding and action: five pitfalls for designers." In: *Personal and Ubiquitous Computing* 8.6 (2004), pp. 440–454.

[135] Vladimir I Levenshtein. "Binary codes capable of correcting deletions, insertions and reversals." In: *Soviet physics doklady*. Vol. 10. 1966, p. 707.

[136] Jialiu Lin, Shahriyar Amini, Jason I Hong, Norman Sadeh, Janne Lindqvist, and Joy Zhang. "Expectation and purpose: understanding users' mental models of mobile app privacy through crowdsourcing." In: *Proceedings of the 2012 ACM Conference on Ubiquitous Computing (UbiComp)*. ACM. 2012, pp. 501–510.

[137] Jialiu Lin, Bin Liu, Norman Sadeh, and Jason I Hong. "Modeling users' mobile app privacy preferences: Restoring usability in a sea of permission settings." In: *Proceedings of the Tenth Symposium On Usable Privacy and Security (SOUPS)*. 2014, pp. 199–212.

[138] Mario Linares-Vàsquez, Andrew Holtzhauer, and Denys Poshyvanyk. "On automatically detecting similar Android apps." In: *24th International Conference on Program Comprehension (ICPC)*. IEEE. 2016, pp. 1–10.

[139] Isaac M Lipkus and JG Hollands. "The visual communication of risk." In: *Journal of the National Cancer Institute. Monographs* 25 (1998), pp. 149–163.

[140] Marte Loge, Markus Duermuth, and Lillian Rostad. "On User Choice for Android Unlock Patterns." In: *Proceedings of the 1st European Workshop on Usable Security (EuroUSEC)*. 2016.

[141] Naresh K Malhotra, Sung S Kim, and James Agarwal. "Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model." In: *Information systems research* 15.4 (2004), pp. 336–355.

[142] Diogo Marques, Ildar Muslukhov, Tiago Guerreiro, Luís Carriço, and Konstantin Beznosov. "Snooping on Mobile Phones: Prevalence and Trends." In: *Proceedings of the Twelfth Symposium on Usable Privacy and Security (SOUPS)*. 2016.

[143] Catherine Marshall and Gretchen B Rossman. *Designing qualitative research*. Sage publications, 2010.

[144] Iris B Mauss and Michael D Robinson. "Measures of emotion: A review." In: *Cognition and emotion* 23.2 (2009), pp. 209–237.

[145] John McCarthy and Peter Wright. *Technology as experience*. MIT Press, 2004.

[146] Andreas Möller, Florian Michahelles, Stefan Diewald, Luis Roalter, and Matthias Kranz. "Update behavior in app markets and security implications: A case study in google play." In: *Proc. of the 3rd Intl. Workshop on Research in the Large. Held in Conjunction with mobileHCI*. 2012, pp. 3–6.

[147] Janice M Morse. "Designing funded qualitative research." In: *Handbook of qualitative research* (1994), pp. 220–235.

[148] Robin Mueller, Sebastian Schrittwieser, Peter Fruehwirt, Peter Kieseberg, and Edgar Weippl. "What's new with whatsapp & co.? revisiting the security of smartphone messaging applications." In: *Proceedings of the 16th International Conference on Information Integration and Web-based Applications & Services (iiWAS)*. ACM. 2014, pp. 142–151.

[149] Ildar Muslukhov, Yazan Boshmaf, Cynthia Kuo, Jonathan Lester, and Konstantin Beznosov. "Know your enemy: the risk of unauthorized access in smartphones by insiders." In: *Proceedings of the 15th International Conference on Human-Computer Interaction with Mobile Devices and Services (mobileHCI)*. ACM. 2013, pp. 271–280.

[150] Alexios Mylonas, Anastasia Kastania, and Dimitris Gritzalis. "Delegate the smartphone user? Security awareness in smartphone platforms." In: *Computers & Security* 34 (2013), pp. 47–66.

[151] Jakob Nielsen. *10 Usability Heuristics for User Interface Design*. `https://www.nngroup.com/articles/ten-usability-heuristics/`. (accessed: 2016-02-16).

[152] Petra Kralj Novak, Jasmina Smailović, Borut Sluban, and Igor Mozetič. "Sentiment of emojis." In: *PloS one* 10.12 (2015), e0144296.

[153] Lawrence O'Gorman. "Comparing passwords, tokens, and biometrics for user authentication." In: *Proceedings of the IEEE* 91.12 (2003), pp. 2021–2040.

[154] Oxford Dictionaries. *emoji - definition of emoji in English from the Oxford dictionary*. `http://www.oxforddictionaries.com/definition/english/emoji`. (accessed: 2017-02-10).

[155] Allan Paivio. "Dual coding theory: Retrospect and current status." In: *Canadian Journal of Psychology/Revue canadienne de psychologie* 45.3 (1991), p. 255.

[156] Darhl M Pedersen. "Psychological functions of privacy." In: *Journal of Environmental Psychology* 17.2 (1997), pp. 147–156.

[157] Phil Nickinson. *Fun with permissions: Why the change in Android 6.0 may make you repeat yourself*. `http://www.androidcentral.com/run-permissions-why-change-android-60-may-make-you-repeat-yourself`. (accessed: 2016-11-04).

[158] The Android Open Source Project. *Encryption*. https://source.android.com/security/encryption/. (accessed: 2016-10-08).

[159] The Android Open Source Project. *Security*. https://source.android.com/security/index.html. (accessed: 2016-10-08).

[160] The Android Open Source Project. *System Permissions*. https://developer.android.com/guide/topics/security/permissions.html. (accessed: 2016-10-22).

[161] Ittipon Rassameeroj and Yuzuru Tanahashi. "Various approaches in analyzing Android applications with its permission-based security models." In: *2011 IEEE International Conference on Electro/Information Technology (EIT)*. IEEE. 2011, pp. 1–6.

[162] Lena Reinfelder, Zinaida Benenson, and Freya Gassmann. "Differences between Android and iPhone Users in Their Security and Privacy Awareness." In: *11th International Conference on Trust, Privacy, and Security in Digital Business (TrustBus)*. Springer International Publishing, 2014, pp. 156–167.

[163] Steven Reiss. "Multifaceted Nature of Intrinsic Motivation: The Theory of 16 Basic Desires." In: *Review of General Psychology* 8.3 (2004), p. 179.

[164] Matthew Rothenberg. *emojitracker: realtime emoji use on twitter*. http://emojitracker.com/. (accessed: 2016-03-02).

[165] Virpi Roto, Effie Law, APOS Vermeeren, and Jettie Hoonhout. *User experience white paper: Bringing clarity to the concept of user experience*. http://www.allaboutux.org/files/UX-WhitePaper.pdf. 2011.

[166] James A Russell. "Core affect and the psychological construction of emotion." In: *Psychological review* 110.1 (2003), p. 145.

[167] Richard M Ryan and Edward L Deci. "Self-determination theory and the facilitation of intrinsic motivation, social development, and well-being." In: *American psychologist* 55.1 (2000), p. 68.

[168] Margarete Sandelowski. "Sample size in qualitative research." In: *Research in nursing & health* 18.2 (1995), pp. 179–183.

[169] Borja Sanz, Igor Santos, Carlos Laorden, Xabier Ugarte-Pedrero, and Pablo Garcia Bringas. "On the automatic categorisation of android applications." In: *2012 IEEE Consumer communications and networking conference (CCNC)*. IEEE. 2012, pp. 149–153.

[170] Florian Schaub, Ruben Deyhle, and Michael Weber. "Password entry usability and shoulder surfing susceptibility on different smartphone platforms." In: *Proceedings of the 11th International Conference on Mobile and Ubiquitous Multimedia (MUM)*. ACM. 2012, p. 13.

[171] Florian Schaub, Marcel Walch, Bastian Könings, and Michael Weber. "Exploring the design space of graphical passwords on smartphones." In: *Proceedings of the Ninth Symposium on Usable Privacy and Security (SOUPS)*. 2013, p. 11.

[172] Bruce Schneier. "The process of security." In: *Information Security* 3.4 (2000), p. 32.

[173] Svenja Schröder, Markus Huber, David Wind, and Christoph Rottermanner. "When SIGNAL hits the Fan: On the Usability and Security of State-of-the-Art Secure Mobile Messaging." In: *Proceedings of the 1st European Workshop on Usable Security (EuroUSEC)*. 2016.

[174] Asaf Shabtai, Yuval Fledel, Uri Kanonov, Yuval Elovici, and Shlomi Dolev. "Google android: A state-of-the-art review of security mechanisms." In: *arXiv preprint arXiv:0912.5101* (2009).

[175] Kennon M Sheldon, Andrew J Elliot, Youngmee Kim, and Tim Kasser. "What is satisfying about satisfying events? Testing 10 candidate psychological needs." In: *Journal of personality and social psychology* 80.2 (2001), p. 325.

[176] Hanul Sieger, Niklas Kirschnick, and Sebastian Möller. "Poster: User preferences for biometric authentication methods and graded security on mobile phones." In: *Symposium on Usability, Privacy, and Security (SOUPS)*. 2010.

[177] Andreas Sonnleitner, Marvin Pawlowski, Timm Kässer, and Matthias Peissner. "Experimentally Manipulating Positive User Experience Based on the Fulfilment of User Needs." In: *Human-Computer Interaction–INTERACT 2013*. Springer, 2013, pp. 555–562.

[178] ISO Standard. *9241-11: Ergonomic requirements for office work with visual display terminals (VDTs) – Part 11: Guidance on usability*. 1998.

[179] Statista - Das Statistikportal. *Marktanteile der Betriebssysteme am weltweiten Endkundenabsatz von Smartphones im 2. Quartal der Jahre 2015 und 2016*. `https://de.statista.com/statistik/daten/studie/76081/umfrage/weltweite-marktanteile-der-betriebssysteme-fuer-smartphones/`. (accessed: 2016-10-05).

[180] Statista - Das Statistikportal. *Marktanteile der Betriebssysteme an der Smartphone-Nutzung in Deutschland von Dezember 2011 bis Februar 2015*. `http://de.statista.com/statistik/daten/studie/170408/umfrage/marktanteile-der-betriebssysteme-fuer-smartphones-in-deutschland/`. (accessed: 2016-04-25).

[181] Statista - Das Statistikportal. *Number of smartphone users in Germany from January 2009 to April 2016*. `https://www.statista.com/statistics/461801/number-of-smartphone-users-in-germany/`. (accessed: 2017-01-03).

[182] Elizabeth Stobert. "The agony of passwords: can we learn from user coping strategies?" In: *CHI'14 Extended Abstracts on Human Factors in Computing Systems*. ACM. 2014, pp. 975–980.

[183] Elizabeth Stobert and Robert Biddle. "Memory retrieval and graphical passwords." In: *Proceedings of the Ninth Symposium on Usable Privacy and Security (SOUPS)*. 2013, 15:1–15:14.

[184] Joshua Tan, Khanh Nguyen, Michael Theodorides, Heidi Negrón Arroyo, Christopher Thompson, Serge Egelman, and David Wagner. "The effect of developer-specified explanations for permission requests on smartphone user behavior." In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI)*. ACM. 2014, pp. 91–100.

[185] Furkan Tari, Ant Ozok, and Stephen H Holden. "A comparison of perceived and real shoulder-surfing risks between alphanumeric and graphical passwords." In: *Proceedings of the 2nd Symposium on Usable Privacy and Security (SOUPS)*. 2006, pp. 56–66.

[186] The Android Open Source Project. *Requesting Permissions at Run Time*. `http://developer.android.com/training/permissions/requesting.html`. (accessed: 2016-05-04).

[187] The Unicode Consortium. *Emoji Annotations*. `http://unicode.org/emoji/charts/emoji-annotations.html`. (accessed: 2016-03-03).

[188] Cody Toombs. *Simplified Permissions UI in The Play Store Could Allow Malicious Developers To Silently Add Permissions*. `http://www.androidpolice.com/2014/06/10/simplified-permissions-ui-in-the-play-store-could-allow-malicious-developers-to-silently-add-permissions/`. (accessed: 2016-02-06).

[189] Thomas S Tullis and Donna P Tedesco. "Using personal photos as pictorial passwords." In: *CHI'05 extended abstracts on Human factors in computing systems*. ACM. 2005, pp. 1841–1844.

[190] *UNeeQ - User Needs Questionnaire*. `http://www.hci.iao.fraunhofer.de/content/dam/hci/de/documents/UXellence_UserNeedsQuestionnaire_EN.pdf`. (accessed: 2016-04-25).

[191] Sebastian Uellenbeck, Markus Dürmuth, Christopher Wolf, and Thorsten Holz. "Quantifying the security of graphical passwords: the case of android unlock patterns." In: *Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications security (CCS)*. ACM. 2013, pp. 161–172.

[192] Kami E Vaniea, Emilee Rader, and Rick Wash. "Betrayed by updates: how negative experiences affect future security." In: *Proceedings of the 32nd annual ACM Conference on Human Factors in Computing Systems (CHI)*. ACM. 2014, pp. 2671–2674.

[193] Viswanath Venkatesh, Michael G Morris, Gordon B Davis, and Fred D Davis. "User acceptance of information technology: Toward a unified view." In: *MIS quarterly* (2003), pp. 425–478.

[194] Arnold POS Vermeeren, Effie Lai-Chong Law, Virpi Roto, Marianna Obrist, Jettie Hoonhout, and Kaisa Väänänen-Vainio-Mattila. "User experience evaluation methods: current state and development needs." In: *Proceedings of the 6th Nordic Conference on Human-Computer Interaction (nordiCHI): Extending Boundaries*. ACM. 2010, pp. 521–530.

[195] Emanuel Von Zezschwitz, Paul Dunphy, and Alexander De Luca. "Patterns in the wild: a field study of the usability of pattern and pin-based authentication on mobile devices." In: *Proceedings of the 15th International Conference on Human-Computer Interaction with Mobile Devices and Services (mobileHCI)*. 2013, pp. 261–270.

[196] David Watson, Lee A Clark, and Auke Tellegen. "Development and validation of brief measures of positive and negative affect: the PANAS scales." In: *Journal of personality and social psychology* 54.6 (1988), p. 1063.

[197] Ina Wechsung and Katrien De Moor. "Quality of experience versus user experience." In: *Quality of Experience*. Springer, 2014, pp. 35–54.

[198] Ina Wechsung, Kathrin Jepsen, Felix Burkhardt, Annerose Köhler, and Robert Schleicher. "View from a distance: comparing online and retrospective UX-evaluations." In: *Proceedings of the 14th International Conference on Human-Computer Interaction with Mobile Devices and Services (mobileHCI)*. ACM. 2012, pp. 113–118.

[199] Tilo Westermann. *User acceptance of mobile notifications*. Springer, 2017.

[200] Alan F Westin. "Privacy and Freedom, Atheneum." In: *New York* (1967), p. 7.

[201] WhatsApp Blog. *end-to-end encryption*. `http://blog.whatsapp.com/10000618/end-to-end-encryption`. (accessed: 2016-04-25). 2016.

[202] Alma Whitten and J Doug Tygar. "Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0." In: *USENIX Security Symposium*. Vol. 1999. 1999.

[203] Primal Wijesekera, Arjun Baokar, Ashkan Hosseini, Serge Egelman, David Wagner, and Konstantin Beznosov. "Android permissions remystified: A field study on contextual integrity." In: *USENIX Security Symposium*. 2015, pp. 499–514.

[204] Margeritta von Wilamowitz-Moellendorff, Marc Hassenzahl, and Axel Platz. "Dynamics of user experience: How the perceived quality of mobile phones changes over time." In: *User Experience – Towards a Unified View, Workshop at the 4th Nordic Conference on Human-Computer Interaction (nordiCHI)*. 2006, pp. 74–78.

[205] Simon S Woo, Jelena Mirkovic, and Elsi Kaiser. "Life-Experience Passwords (LEPs)." In: *SOUPS: Workshop: Who are you?! Adventures in Authentication (WAY)*. 2014.

[206] Peter Wright, John McCarthy, and Lisa Meekison. "Making sense of experience." In: *Funology*. Springer, 2003, pp. 43–53.

[207] Jeff Yan et al. "Password memorability and security: Empirical results." In: *IEEE Security & privacy* 5 (2004), pp. 25–31.

[208] Tao Zhou and Yaobin Lu. "Examining mobile instant messaging user loyalty from the perspectives of network externalities and flow experience." In: *Computers in Human Behavior* 27.2 (2011), pp. 883–889.

A

STUDY QUESTIONNAIRES

Please refer to the literature for the standard questionnaires:

- AttrakDiff2 mini (English: [86], German: [47])
- Need fulfillment questionnaire (English: [175], German: [47])
- UNeeQ questionnaire ([68], [190])
- Positive affect – negative affect schedule (PANAS) (English: [196], German: [126])
- Subjectively experienced exhaustion scale (German only [55])
- Global Information Privacy Concern Scale (GIPC) [141]

A.1 DEMOGRAPHIC QUESTIONNAIRE

These questions on demographics were used in all of the conducted studies (subject to slight variations).

Gender: [male/female/no answer]

Age: [open answer]

Highest level of education:

- no degree
- Lower secondary education only
- Middle school/ secondary school degree only
- Highschool degree/ qualification for university entrance
- University degree [If so, subject area: [open answer]]

Current occupation: [open answer]

Which occupational category are you a member of?

- Highschool student
- Apprentice
- Student
- Employee
- Self-employed
- Civil servant
- Retired
- Homemaker
- Unemployed
- Other: [open answer]

Are you studying or have you been working in any of the following areas: [yes/no]

- IT/ Information technology
- Computer Science
- Electronic data processing
- Electrical engineering
- Communications technology
- Similar

What operating system are you using on your smartphone?

- Android
- iOS (iPhone)
- Windows (Windows Phone)
- other: [open answer]

How long have you been using a smartphone?

- 0-3 Months
- 4-12 Months
- 1 to 3 Years
- longer than 3 years

How often do you use your smartphone?

- multiple times per hour
- 1x per hour
- multiple times per day
- 1x per day
- multiple times per week
- 1x per week
- less frequently

A.2 INTERVIEW QUESTIONNAIRE (STUDY 2)

Demographic questionnaire (cf. Section A.1)

Smartphone usage

- Why did you decide to buy a smartphone?
- You are currently using a smartphone with [Android/ iOS/ windows] operating system (OS). Was this a conscious decision? What were the reasons [for this decision]?
- Have you used another operating system before?
- If so, which? What were the reasons for changing the OS?

Smartphone sharing (adapted from Chin et al. [32])

- Is this your only smartphone?
- If not,
  - How many smartphones do you own?
  - Why do you own several smartphones?
  - Which of them do you use mainly?
- Are there any other people who use your personal smartphone on a regular basis?
  - If so, how many? Who else is using your personal smartphone?
- Is there someone else who sometimes uses your smartphone?
  - If so, under which circumstances?

Work related use

- Do you also use your smartphone for work?
- If so,
  - For which purpose [e.g. calling, e-mailing etc.]?
  - What are the main differences between private and occupational use of your smartphone?
  - Did your employer set any requirements for work related smartphone usage?

App usage

- Do you use apps?
- If not, why?
- Which are your favourite apps on your smartphone?
- Which apps do you consider the most useful on your smartphone?

Paid apps

- Do you use apps you have to pay for?

- If not, are there any reasons why not?
- If so,
  - How do you pay for the apps?
  - Do you use in-app purchases?
    * If so, is the in-app purchase function password protected?

App selection and download

- Which criteria do you use to decide for an app you want to download or install?
- Which platform (i.e. app market) do you use to download apps?

App avoidance

- Are there any apps which you intentionally don't install? If so, what kind of apps?

App uninstalling

- Have you ever cancelled the installation of an app? If so, why?
- Have you ever uninstalled an app? If so, why?

Smartphone set up

- When you used your smartphone for the first time...
  - How did you take action?
  - Did you set up the device according to your preferences?
  - If so, what did you do?

Data connections

- Which type of data connections do you use (e.g. Bluetooth, NFC, WiFi)? What are you using them for?
- If WiFi was mentioned: Which access points do you use [which networks do you use, respectively]?
- Are there situations in which you switch off your data connections?
- If so,
  - Why?
  - Do you remember any causes that made you start doing so?

Updates

- Do you install app updates?
- If so,
  - Why?
  - Do you install updates automatically or manually?
  - Is there any reason why you install them automatically/ manually?

  - Do you remember any causes that made you start doing so?

Post-paid vs. pre-paid

- Do you pay for your smartphone usage on a monthly basis or do you use pre-paid?
- What are the reasons why you decided for [payment method]?
- If Post-paid:
  - Do you check your monthly phone bills?
  - If so,
    * Why?
    * Do you remember any causes that made you start doing so?
- If Prepaid:
  - Do you check your prepaid balance from time to time?
  - If so,
    * How often?
    * Do you remember any causes that made you start doing so?

Battery lifetime

- Do you check your battery status from time to time?
- If so, do you do anything to save battery lifetime?
  - If so,
    * Could you please describe what exactly you're doing?
    * Do you remember any causes that made you start doing so?

Protection from theft

- Do you do anything to protect your smartphone from theft?
- If so,
  - What are you doing?
  - Do you remember any causes that made you start doing so?
- Do you use locating or remote access apps?
- If so,
  - Why?
  - Do you remember any causes that made you start doing so?

Backups

- Do you make backups of your smartphone data?
- If so,

  - What are the reasons for making backups?
  - How often do you make backups?
  - Where do you store your backups?
  - Do you remember any causes that made you start doing so?

Internet und Surfing

- Do you surf the Internet on your smartphone?
- If not, why not?
- If so
  - Which browser do you use? Why?
  - Which search engine do you use on your smartphone? Why?
  - Have you ever changed your browser settings?
    * If so, what did you want to change?
    * Was the action successful?
  - Do you take any measures to reduce your data traces on the web while surfing with your smartphone?
    * If so, what do you do?

Financial Transactions

- Do you use apps which include handling money such as mobile payment, mobile TAN procedures, online banking or shopping apps?
- If not, why not?
- If so,
  - Which kind of apps do you use?
  - Do you have any concerns while using these apps? If so, what kind of concerns?
- Do you use online banking via the browser?
  - If so, how does such a typical banking session look like?

App access to sensitive data

- Many apps request access to sensitive data (such as calendar or address book) and functions (such as camera and location).
- Do you allow those apps to access this data and functions?
  - If not, why not?
    * How do you avoid it?
    * Do you remember any causes that made you start doing so?
  - If so,
    * Do you allow all apps to access everything or only certain apps?
    * Do allow always access or only in certain situations?

  - Do you consider any data or functionalities more sensitive than others?

Communication

- Do you use your phone to communicate with other people?
- If so,
  - How do you communicate? (e.g. calling, SMS, Chat, email, social networks)
  - Which messaging apps do you use? Why do you use exactly these?
- Do you do something to protect your communication?
- If so, what do you do?
- Whom do you protect your communication from?
- Can you remember any causes that made you start doing so?

Data stored on the device

- Do you protect the data which is stored on your device?
- If so,
  - How do you protect your data?
  - What do you protect your data from?
  - Do you remember any causes that made you start doing so?

SPAM

- Do you sometimes receive SPAM (i.e. unwanted adds or messages) on your smartphone?
- If so,
  - Could you give us some examples?
  - How often do you receive SPAM?
  - Do you do anything to reduce the amount of SPAM you receive?

"Backup" questions: *Those questions were only asked if the related topics were not already mentioned during the interview.*

- Do you do anything to protect yourself from apps that collect too much data?
- If so,
  - What do you do?
  - How do you define these kinds of apps?
- Do you use additional security software on your smartphone?
- If so,
  - Which kind of apps do you use?
  - Against what do you want to protect yourself?

- Do you use pre-installed security mechanisms such as screen lock with a password?
- If so,
  - What are the reasons therefor?
  - Do you remember any causes that made you start doing so?
- Do you perceive any threats related to smartphone usage?
- If so,
  - Which threats do you perceive?
  - Do you have an individual strategy to protect yourself against these threats?
  - If so, could you please describe your individual strategy?
- Do you perceive any security and privacy threats related to smartphone usage?
- If so,
  - Which threats do you perceive?
  - Do you have an individual strategy to protect yourself against these threats?
    - If so, could you please describe your individual strategy?
- Do you have any comments or questions regarding the topics which we discussed today in this interview?

A.3 ONLINE STUDY QUESTIONNAIRE (STUDY 3)

Demographic questionnaire (cf. Section A.1)

Have you ever downloaded an app for your smartphone? [yes/no]

What are your three favorite apps? [open answer]

Please drag and drop the criteria that where important for you when you selected your smartphone to the right side!

- Size and /or quality of the according app store
- Smartphone price
- App prices
- Visual appearance of the device
- Visual appearance of the operating system
- Functionality of the operating system
- Technical features (e.g. storage, battery lifetime, camera)
- Security
- Recommendations of known people
- Handling of the device

Please drag and drop those scenarios that you perceive as a threat concerning your smartphone to the right site:

- Data loss
- Device loss
- Financial loss due to wrong debiting of my mobile provider
- Financial loss due to unauthorized access (e.g. in case of theft)
- Network attacks (somebody reads the in and out-going communication)
- Surveillance of my behavior by state-owned organizations
- Surveillance of my behavior by privately-owned organizations
- Surveillance of my behavior by people I know
- Surveillance of my behavior by people I don't know
- Unauthorized access to my smartphone by people I know
- Unauthorized access to my smartphone by people I don't know

Security and privacy actions: [split in three versions]
Note: after each question that is marked with an asterisks at the beginning, the need questionnaire was shown.

- *Do you do backups? [yes/no]
  If so, where do you safe the backups? [PC/ Cloud/ other]
- *How often is the WiFi on your smartphone disabled? [always/ often/ sometimes/ never/ don't know] | How often are location services or GPS disabled on your device? [always/ often/ sometimes/ never/ don't know] | How often are bluetooth or

Airdrop (iPhone only) disabled on your device? [always/ often/ sometimes/ never/ don't know]
- *Do you use a screen lock together with a PIN or passwors? [yes/ no]
- *Do you install updates? [yes/ no]
  If so, how do you install updates? [manually/ automatically/ other]
- *Do you use the privacy settings in messaging apps? [yes/ no/ don't know/ I do not use messaging apps]
- *How do you pay your cell phone expenses? [postpaid/ prepaid]
  If postpaid, do you check your monthly bill? [yes, regularly/ yes, sometimes/ no]
- *Do you take measures to protect your smartphone from theft? [yes/ no]
  If so, which measures do you take? [I store my device securely/ I don't leave my device unattended/ I use apps for locating the device or remote management apps/ I've taken out an insurance]
- *Do you scrutinize app permissions when installing or using an app? [yes/ no]
- How frequently do you scrutinize permissions? [always/ often/ sometimes/ never]
- (Android users only) Did you ever refrain from installing an app that had a high number of permissions? [yes/ no/ don't know]
- (Android users only) Did you ever refrain from installing an app because the number of requested permissions was high compared to the offered functionality? [yes/ no/ don't know]
- (iOS users only) Did you ever uninstall an app that asked for unusual permissions? [yes/ no/ don't know]
- *Do you use one or several of the following messaging apps which deploy end-to-end encryption? [Threema/ iMessage/ Telegram/ TextSecure/ ChatSecure/ Surespot/ myEnigma/ Hoccer/ other/ I don't use messaging apps with end-to-end encryption/ I don't know whether I use apps with end-to-end encryption]

Need fulfillment items used per security and privacy action:
Note: translated items were taken [47] based on Sheldon et al. [175]; items for keeping the meaningful were taken from the UNEEQ questionnaire [68] [190]. For each need, only two of three the items were deployed (cf. Section 6.3). Items were presented in randomized order.

- Autonomy: AUT_1, AUT_2
- Competence: KOM_1, KOM_3
- Relatedness: VER_1; VER_2

- Stimulation: STI_1, STI_2
- Money/Luxury: LUX_1, LUX_3
- Security: SIC_2, SIC_3
- Popularity: POP_1, POP_3
- Keeping the meaningful: mean_1, mean_4

How strong is the emotional value that you attach to the following data and files?
(Scale from 1 (= no emotional value) to 5 (= strong emotional value))

- Work-related files
- Music and video clips
- Photos
- Documents and receipts
- E-books
- Messages (SMS, WhatsApp, etc.)
- E-Mails
- Games
- Contacts
- Apps that have cost money
- System files to recover system settings (app settings etc.)

Do you backup the following data and files? [yes/ no/ don't have this item on my smartphone/ don't know]

- Work-related files
- Music and video clips
- Photos
- Documents and receipts
- E-books
- Messages (SMS, WhatsApp, etc.)
- E-Mails
- Games
- Contacts
- Apps that have cost money
- System files to recover system settings (app settings etc.)

What are the three most important criteria for the selection of a messaging app?
(Checkboxes: exactly three answers need to be ticked)

- App price
- Adoption within my circles
- Handling of the app
- Message encryption
- Description of the app
- Visual appearance of the app
- Reviews of other users
- Star rating (in the app market)

- Number of downloads
- Permissions requested by the app
- Functional scope
- App publisher

A.4 LAB STUDY QUESTIONNAIRE (STUDY 4)

Demographic questionnaire (cf. Section A.1)
Additional:

- Do you use apps? If so, which apps do you regularly use [3 open answer options]
- How often do you download apps? [at least once per week/ at least 2-3 time per month/ approximately once per month/ less often]

Which criteria do you pay attention to when downloading an app?

- Description of the app
- Visual appearance of the app
- Reviews of other users
- Rating (number of stars)
- Number of downloads
- Permissions requested by the app
- Functional scope of the app
- App publisher

After each decision, participants received the following questions:

- Which app did you select?
- Please describe in 2-3 sentences why you decided for this app.
- Please indicate how important the following criteria were for THIS decision: [list of same criteria as above]
- Please indicate your impression of the app presentation by the help of the following pairs of words: (AttrakDiff2 mini [86])
- Please order the following criteria according to their importance for THIS decision: [list of same criteria as above]

Moreover, the following items were presented in randomized order for the selected and the not selected app.

- The aesthetic of the selected/ not selected app is: (Continuous scale (low-high) from 0 to 21)
- The user-friendliness of the selected/ not selected app is: (Continuous scale (low-high) from 0 to 21)
- The functional scope of the selected/ not selected app is: (Continuous scale (low-high) from 0 to 21)
- I perceived the privacy that is provided by the selected/ not selected app as: (Continuous scale (low-high) from 0 to 21)
- My trust in the selected/ not selected app is: (Continuous scale (low-high) from 0 to 21)
- My overall impression of the selected/ not selected app is: (Continuous scale (bad-excellent) from 0 to 21)

Global Information Privacy Concern Scale [141]

A.5 ONLINE STUDY QUESTIONNAIRE (STUDY 5)

Demographic questionnaire (cf. Section A.1)
Additional:
Which three apps on your smartphones would you most likely protect from other people accessing them without permission? [3 open answer options]

(Attention check) If you read this question select the option "rather agree". [agree/ rather agree/ rather disagree/ disagree]

Introduction

- You decided to improve your English skills. [Language App]
- You decided to improve your fitness. [Fitness app]
- You decide that you want to kill waiting time. [Gaming app]
- Thereby, you decided for the following app [screenshot 1].
- The app market also shows another picture of the app [screenshot 2].

Selective install-time UIs

- Have you used or do you currently use the presented app?
- As soon as you press the "install" button, the following dialog appears: [screenshot selective install-time UI or selective install-time UI with purpose string]
- The toggles next to the permissions are activated. You can deactivate them if you want to deny a permission.+
- Which of the requested permissions would you grant? [Opt-outs for: Phone/ Storage/ Location/ Contacts/ Camera]

Runtime UIs

- You installed the app and now you open it for the first time.
- Immediately after opening the app, the following dialog appears: [screenshot runtime UI permission or runtime UI permission with purpose string]
- Would you grant or deny the requested permission? [deny/ grant/ deny and "never ask again"/ grant and "never ask again"]
- After using the app for several minutes, you try a new feature of the app. The following dialog appears [screenshot runtime UI permission or runtime UI permission with purpose string].
- Would you grant or deny the requested permission? [deny/ grant/ deny and "never ask again"/ grant and "never ask again"]
- After several hours you open the app again. After opening the app, the following dialog appears: [screenshot runtime UI permission or runtime UI permission with purpose string]
- Would you grant or deny the requested permission? [deny/ grant/ deny and "never ask again"/ grant and "never ask again"]

- After several days you open the app again. After opening the app, the following dialog appears: [screenshot runtime UI permission or runtime UI permission with purpose string]
- Would you grant or deny the requested permission? [deny/ grant/ deny and "never ask again"/ grant and "never ask again"]
- After one week you open the app again. After opening the app, the following dialog appears: [screenshot runtime UI permission or runtime UI permission with purpose string]
- Would you grant or deny the requested permission? [deny/ grant/ deny and "never ask again"/ grant and "never ask again"]

After the first kind of app, the following questions were asked.

- As how exhausting did you experience the permission handling? (Answer options based on [55]) [exceptionally exhausting/ very strongly exhausting/ strongly exhausting/ fairly exhausting/ rather exhausting/ somewhat exhausting/ slightly exhausting/ not exhausting]
- How annoying did you perceive the permission handling dialog? (Scale from 1 (= not annoying) to 5 (= very annoying))
- (Attention check) If you read this question, please select the option which contains the word "needed". [Mobile apps cost always money/ Mobile apps are rarely needed/ Mobile apps are not helpful in everyday life/ Mobile apps become useless without updates]

After the second kind of app, another attention check question was asked.
(Attention check) If you read this question, please select the option which contains the word "updates". [A casing is needed for smartphone security/ A button is needed to interact with a smartphone/ Updates are not needed for user experience with smartphones/ Headphones are needed for smartphone usability]

After the third kind of app, UX questionnaires were deployed.
AttrakDiff 2 mini introductory text:

- Below you will see pairs of words, which you should use to evaluate the app permission presentation. They constitute extreme opposites, with a scale in between.
- Don't think too long about the word pairs, but rather answer it according to your spontaneous association.
- Potentially some word pairs may seem less fitting for the app permission handling, please always select an answer anyway. Please remember that there are no "right" or "wrong" answers – we're interested in your personal experience!
- Please use the word pairs below to express your impression of the app permission presentation.

- Please only select one circle in each row!

Need fulfillment and PANAS introductory text:

- In the following, we ask you to rate your feelings during app permission handling:
- Please respond based on the following scale:
- The value 1 means: not at all
- The value 5 means: very much
- You can use the values between 1 and 5 to express your opinion.
- Please respond according to your spontaneous association.
- Potentially some statements may not fit well to the app permission handling, please always provide an answer anyway. Please remember that there are no "right" or "wrong" answers – we're interested in your personal experience!
- During the permission handling I felt...

A.6 LAB STUDY QUESTIONNAIRE (STUDY 6)

Demographic questionnaire (cf. Section A.1)
Additional:

- Do you use an authentication mechanism to unlock your screen [yes, a PIN/ yes, a password/ yes, an unlock pattern/ yes, fingerprint or TouchID/ yes, other/ don't know]
- If you answered yes for the question before: Have you used a different authentication method on your smartphone in the past? [yes, a PIN/ yes, a password/ yes, an unlock pattern/ yes, fingerprint or TouchID/ yes, other/ don't know]
- Do you use a PIN when switching on your smartphone (SIM-PIN)? [yes/ no/ don't know]

Questionnaire to Evaluate the Authentication Method (AttrakDiff 2 mini)
Introductory text:

- Below you will see pairs of words, which you should use to evaluate the authentication method. They constitute extreme opposites, with a scale in between.
- Don't think too long about the word pairs, but rather answer it according to your spontaneous association.
- Potentially some word pairs may seem less fitting for the authentication method, please always select an answer anyway. Please remember that there are no "right" or "wronng" answers – we're interested in your personal experience!
- Please use the word pairs below to express your impression of the authentication method.
- Please only select one circle in each row!

Feelings during the Use of the Authentication Method – Part 1/2 (Need fulfillment questionnaire/ PANAS)
Introductory text:

- Please respond based on the following scale:
- The value 1 means: not at all
- The value 5 means: very much
- You can use the values between 1 and 5 to express your opinion.
- Please respond according to your spontaneous association.
- Potentially some statements may not fit well to the authentication method, please always provide an answer anyway. Please remember that there are no "right" or "wrong" answers – we're interested in your personal experience!
- When using the authentication method I felt ...
- (need fulfillment questionnaire) or (PANAS)
- Please indicate to what extent the authentication method was responsible for your feels during use.

Interview script – week 1

- How did you choose your password?
- Could you please detail your approach or strategy?
- To which factors did you especially pay attention?
- The numbers/ Emojis themselves?
- The position of the numbers/ Emojis?
- What was you stragegy when choosing the Emojis and their order? (Emoji only)
- Did you choose the Emojis according to a story? (Emoji only)
- How confident are you that you will remember your password until next week? Why?

Interview script – week 2

- How did you remember your password?
- Did you perceive it as easy or as difficult to remember your password? Why?
- Did you write your password down?

A.7 FIELD STUDY QUESTIONNAIRE (STUDY 7)

In the EmojiAuth/PIN field study, participants received diverse questionnaires before, during and at the end of the study. The majority of questions were the same for EmojiAuth and PIN users with the only difference that PIN users were asked to rate "PINAuth" instead of "EmojiAuth". Password selection questionnaires also differed between the groups (cf. Section 10.4.2).

Prescreening questionnaire (before the study):

Smartphone use:

- Do you own a smartphone with Android operating system? [yes/no]
- Which smartphone model do you own? [open answer]
- Which are your three most frequently used apps? [open answer]
- Which three apps on your smartphone are you most likely to protect from unauthorized access by others? [three open answer options]
- Do you use a smartphone with a different operating system in addition to your Android phone? [yes, iOS/ yes, Windows/ no/ Other:]
- How long have you been using a smartphone? (For answer options cf. to Section A.1)
- How often do you use a smartphone? (For answer options cf. to cf. Section A.1)
- Do you use an authentication method to unlock your smartphone? (For answer options cf. to Section A.6)
- Have you used an authentication method on your smartphone in the past? (For answer options cf. to Section A.6)
- Do you use a PIN when switching on your smartphone (SIM-PIN)? [yes/ no]

E-mail use:

- Do you check emails on your smartphone with an app? [yes/ no]
- Which app do you use to check your email on your smartphone? [open answer]
- Do you have to currently enter a password when checking emails with the app? [yes, always/ yes, sometimes/ no/ I don't know]
- How often do you use your email app per day? [1 time/ 2-5 times/ 6-10 times/ more than 10 times]
- Are your emails being fetched automatically by the app (e.g., with Push or at regular time intervals) or do you fetch emails

manually? [My emails are fetched automatically/ I fetch my emails manually/ Other:]
- How many emails do you receive on your smartphone per day? [Less than 5/ 5 to 10/ 11 to 15/ 16 to 20/ more than 20]
- What is the primary use of your email app on your smartphone? [personal use/ business use/ both personal and business use]

Demographic questionnaire (cf. Section A.1)

Questionnaires received during the study:

- Daily feedback questionnaire (cf. Figure 25b)
- Password selection questionnaire (cf. Figure 26 and Section 10.4.2)
- AttrakDiff 2 mini questionnaire on day 2, 8, and 14; within the app (cf. Figure 27).

Exit questionnaire:

In the following please respond to some questions about EmojiAuth/PINAuth. Don't think too long about the questions, just respond with what comes to mind!

Password Protection with Emojis/PIN: How did you like authenticating with EmojiAuth/PINAuth overall? [Smiley scale as in the daily feedback questionnaire]
As how annoying did you perceive authenticating with EmojiAuth/PINAuth during the study? (Scale from 1 (= very annoying) to 5 (= Not at all annoying))

E-Mail-App Usage:
Did you change your Email app usage behavior during the use of EmojiAuth/ PINAuth? [no/ yes, I used my E-mail app more frequently/ yes, I used my E-mail app less frequently/ yes, I did the following:]

Characteristics of authentication with Emojis/PIN:
How did you like the following characteristics of EmojiAuth/PINAuth during the study? (Scale from 1 (= very bad) to 5 (= very good))

- The fact that Emojis/numbers were used for authentication
- The displayed Emojis on the keyboard (EmojiAuth users only)
- The Emojis/numbers in my password
- My password
- The length of my password
- The memorability of my password
- The frequency with which I had to unlock my email app

- The time period after which the password authentication became active again
- The size of the Emoji/PIN keys
- The fact that I could unlock my email app
- The number of tries for entering the wrong password before I needed the backup password

Psychological need fulfillment scale:
Introductory text:

- Next a few questions about how you felt during Emoji/PIN authentication use.
- Please respond according to the following scale:
- Value 1 means not at all
- Value 5 means absolutely
- With the values 1 to 5 you can communicate your opinion in steps.
- Please respond with what comes to mind.
- Maybe some oft he statements do not fit EmojiAuth/PINAuth well, please still provide a response for each question. Please remember that there are no "right" or "wrong" answers – your personal opinion is important!
- During the Use of Emoji/PIN authentication I felt that ...

Use alternative smartphone: (EmojiAuth only)

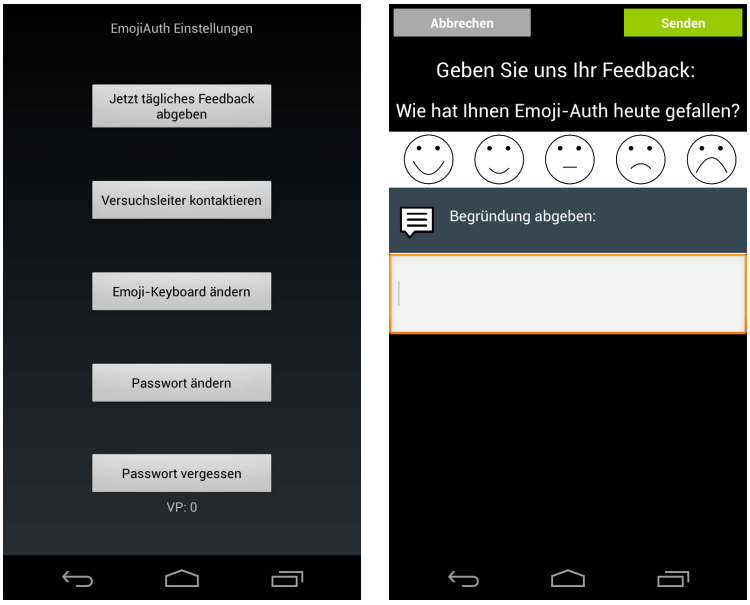
- Would you use Emoji protection instead of a PIN to unlock your smartphone? The question focuses on unlocking the smartphone, not unlokcking the email app. [yes/ no]
- Please explain your response: [open answer]

Use alternative bank card (at ATM): (EmojiAuth only)

- Would you use Emoji protection instead of a PIN for your bank card? [yes/ no]
- Please explain your response: [open answer]

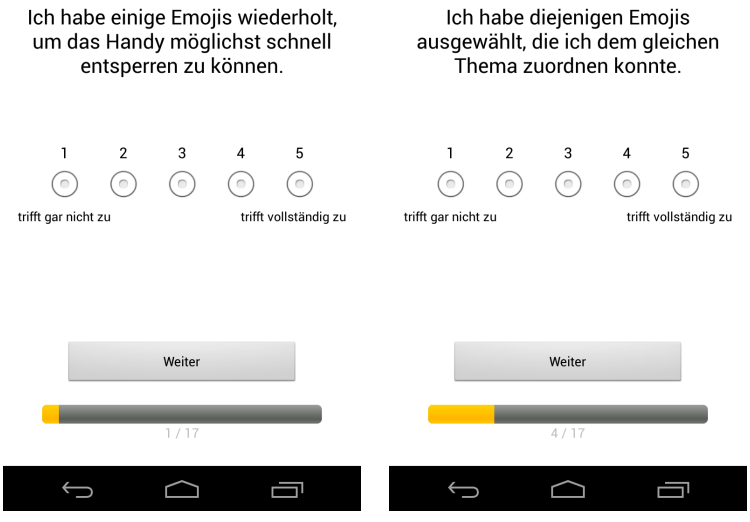
Continued use / recommendation:

- I would continue to use EmojiAuth/PINAuth to unlock my email app. [very rarely/ rarely/ sometimes/ often/ very often]
- I will recommend EmojiAuth/PINAuth to others. [not at all/ probably not/ maybe/ quite likely/ certainly]



(a) (b)

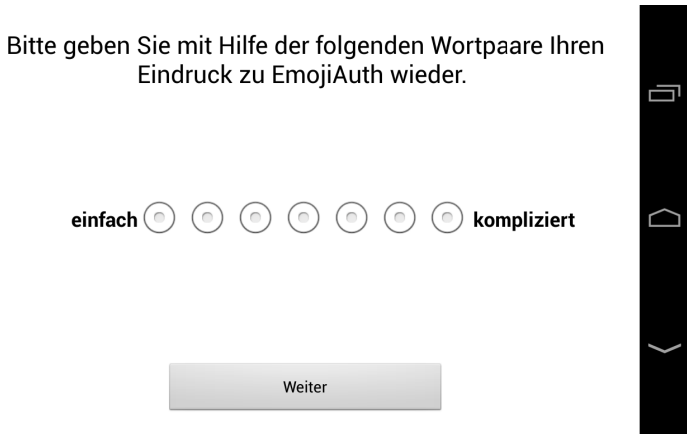
Figure 25: Field study in-app settings (left) and daily feedback questionnaire (right). Translation of the settings-buttons (from top to bottom): Provide daily feedback now/ Contact experimenter/ Change Emoji keyboard/ Change password/ Password forgotten. Translation of the daily feedback questionnaire (from top to bottom): Please provide feedback: How did you like EmojiAuth/PINAuth today? [Smiley scale] Provide an explanation: [open answer].



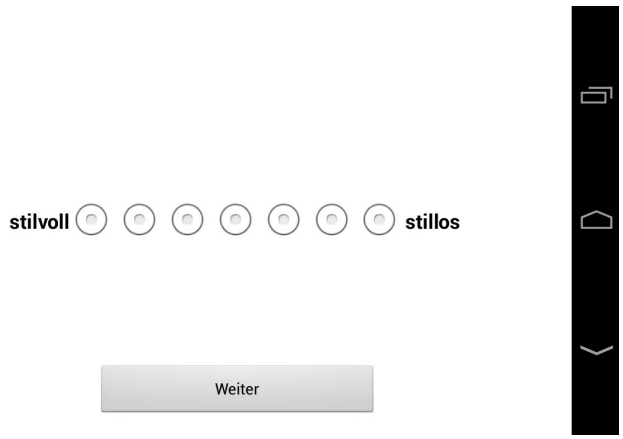
(a) (b)

Figure 26: Example questions: field study in-app password selection questionnaire (cf. Section 10.4.2 for all items in English translation)

.



(a)



(b)

Figure 27: Example questions: Field study in-app AttrakDiff2 mini questionnaire (cf. [86] for all items in English). Translation of the introductory sentence: Please rate your impression of EmojiAuth/PIN-Auth using the following pairs of words.

COLOPHON

This document was typeset using the typographical look-and-feel `classicthesis` developed by André Miede. The style was inspired by Robert Bringhurst's seminal book on typography "*The Elements of Typographic Style*". `classicthesis` is available for both LaTeX and LyX:

`https://bitbucket.org/amiede/classicthesis/`