Journal of Information Security and Applications 34 (2017) 34–45

Contents lists available at ScienceDirect

Journal of Information Security and Applications

journal homepage: www.elsevier.com/locate/jisa

Psychological needs as motivators for security and privacy actions on smartphones

Lydia Kraus*, Ina Wechsung, Sebastian Möller

Quality and Usability Lab, Telekom Innovation Laboratories, Technische Universität Berlin, Ernst-Reuter-Platz 7, 10587 Berlin, Germany

ARTICLE INFO

Article history:

Keywords:
Psychological needs
Security and privacy
Smartphones
User behavior
User experience

ABSTRACT

Much work has been conducted to investigate the obstacles that keep users from using mitigations against security and privacy threats on smartphones. By contrast, we conducted in-depth interviews ($N = 19$) to explore users' motivations for voluntarily applying security and privacy actions on smartphones. Our work focuses on analyzing intrinsic motivation in terms of psychological need fulfillment. The findings from the interview study provide first insights on the salience of basic psychological needs in the context of smartphone security and privacy. They illustrate how security and privacy actions on smartphones are motivated by a variety of psychological needs, only one of them being the need for *Security*. We further conducted an online survey ($N = 70$) in which we used questionnaires on psychological need fulfillment from the literature. The online survey is a first attempt to quantify psychological need fulfillment for security and privacy actions on smartphones. Whereas the results of the interview study indicate that *Security* and other needs play a role as motivators for employing security and privacy actions on smartphones, the online study does not support the need for *Security* as an outstanding motivator. Instead, in the online study, other needs such as *Keeping the meaningful*, *Stimulation*, *Autonomy*, and *Competence* show to be rather salient as motivators for security and privacy actions. Furthermore, the mean need fulfillment for security and privacy actions is in general rather low in the online survey. We conclude that there is scope for improvement to maximize psychological need fulfillment with security and privacy actions. In order to achieve a positive user experience with security and privacy technologies on smartphones, we suggest addressing additional psychological needs, beyond the need for *Security*, in the design of such technologies.

1. Introduction

Smartphones are an extensive source for positive user experiences: using a smartphone allows people to stay connected, to consume new games and media, or to "quantify themselves" with fitness and health monitoring apps.

While smartphones offer vast opportunities for positive experiences, threats to users' security and privacy emerge at the same time. Those include malicious apps, data loss, surveillance, and profiling, just to name a few.

Related work indicates that users are concerned about many of these threats and about their privacy on smartphones [1–3]. To mitigate these threats there is a variety of actions users can take [4]. Earlier research suggests to gain further insights into security and privacy aspects from an end-user perspective by using experiential approaches [5,6]. In this context experience is seen as a holistic and broad view on the matter in order to gain a rich understanding of people's practices and lives [6]. Accordingly, while much work has been conducted to understand users' perceptions of smartphone security and privacy in terms of understanding [7], concerns [2], awareness [3,8], attitudes [1], and feelings [9], we suggest using an experiential approach based on psychological needs to gain a deeper understanding of the matter.

User eXperience (UX) is a field of study which emerged between the mid-nineties and the turn of the millenium. In contrast to usability, which is mainly concerned with the functional aspects of technology usage, UX includes non-functional factors such as beauty and affective aspects of human-computer interaction (HCI) [10]. Accordingly, UX is a multi-dimensional construct with a holistic view on the perceived product qualities (beyond usability), users' emotions, motivations, usage situations, and other

* Corresponding author.
E-mail addresses: lydia.kraus@tu-berlin.de (L. Kraus), ina.wechsung@tu-berlin.de (I. Wechsung), sebastian.moeller@tu-berlin.de (S. Möller).

http://dx.doi.org/10.1016/j.jisa.2016.10.002

dimensions (for a literature review of UX dimensions and study methods refer to [10]).

In the present work, we focus on the motivational dimension of user experiences in terms of psychological need fulfillment. Psychological needs have been suggested in several theories as an explanation for human behavior: for instance, self-determination theory suggests basic psychological needs as the fundamental mechanism for self-motivation [11]. Furthermore, it has been shown that need fulfillment is related to satisfying events and positive affect [12]. In the context of user experience research, Hassenzahl et al. [13] show 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 [13].

A user for instance makes a phone call to experience the feeling of being close to others (thus, the motivation would be the fulfillment of the need *Relatedness*), rather than for the call's sake (example taken from Hassenzahl [14]). Or, a user activates 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 is used to fulfill the basic psychological need of *Autonomy*. Psychological need fulfillment is a primary goal which all users have in common, the instantiation of the primary goal - the experience - is however highly context-dependent and subjective [14].

The goal of this work is to learn about the psychological needs which users intend to fulfill with security and privacy actions on smartphones. After detailing related work on security and privacy actions on smartphones, user experience, and psychological needs in Section 2, the interview methodology is presented in Section 3 and the online survey methodology is presented in Section 4. The results of the interviews and the online survey are reported in Sections 5 and 6, respectively. We discuss the implications of applying the approach of psychological need fulfillment in the security and privacy context in Section 7, as well as the possibilities to use psychological needs as a design inspiration for security and privacy mechanisms.

2. Related work

Much work has been conducted to describe user practices, concerns, and usability issues related to smartphone security and privacy. Despite the known usability issues of security mechanisms, users report being interested in applying further such mechanisms [15]. In the following, an overview of the main security and privacy actions users could deploy on their smartphone is presented. Those actions were also covered in the interviews which were conducted for this work.

2.1. Usability and adoption of smartphone security and privacy mechanisms

Scrutinizing app permissions is an indispensable action to avoid privacy intrusions and security issues on smartphones [4]. In the past, the implementation of the permission model differed between smartphone operating systems (OSes): Whereas iOS users were shown a permission-request as soon as an app requested the permission for the first time, Android users had to accept all permissions or groups thereof before an app could be installed. In this implementation, Android permissions were difficult to understand by users; also, the permission requests were shown at an unfavorable point in the decision making process, that was when the decision to install an app has already been made [7]. Several solutions have been suggested to increase the understanding of and the attention to permissions, including improved information presentation and risk communication (cf. e.g. [16–19]). In 2014, the Android permissions were grouped and their presentation was modified to include icons for each group. While this improved information presentation, security concerns remained [20]. Android version 6.0, released in 2015, enables users to grant or not to grant single permissions for each app [21]. However, as of March 2016, Android 6.0 still has a negligible market share (2.3%) in the studied population [22]. Thus, the issues described above are still relevant.

A method to protect a smartphone from unauthorized access and subsequent privacy intrusions or security issues is the deployment of a screen lock together with an authentication method, such as a password or a PIN [4]. However, unlocking a smartphone with an authentication mechanism is time-consuming [23]. In a study of 2011, the PIN was perceived as a reliable method for protecting a mobile phone by only a quarter of users (26%) [15]. Nevertheless, 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 [24]. A viable alternative to knowledge-based authentication methods are biometric methods such as Touch ID on iPhones and face unlock on Android devices [25]. Biometric methods, however, also rely on PINs or passwords for fallback authentication.

Regarding communication, eavesdropping and interception pose a threat. They can be mitigated by deploying end-to-end encryption of communication (calls and/or messages) [26]. Only recently, Whatsapp, one of the most popular instant messaging services for smartphones, has announced the implementation of end-to-end encryption which is activated by default [27]. 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. For instance, Rashidi and Vaniea report that many users actively use the privacy settings of Whatsapp - in a survey among Saudi Arab users almost a third of the respondents hid their last seen notice [28].

Another security threat, malware, might be mitigated by antivirus apps which can be easily installed for Android; however, their usefulness is questionable [29]. Likewise, the usage of security software is considered by many users as nonessential [3]. 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 [30].

Threats may also arise from the device being unavailable due to denial of service attacks or exhausted battery power [26]. For counteracting the former, a resource management solution may be installed; these kind of applications are, however, difficult to implement [26]. A study by Chin et al. also showed that users worry about limited battery lifetime [1] when asked about concerns related to smartphone usage.

Data loss due to device loss or theft can be easily mitigated by backups. While users are concerned about the latter threats [1], other tools to mitigate negative consequences in case of theft or loss such as remote data wipe, device locators, and device encryption are poorly adopted [3]. This might be due to unawareness of the existence of such features [1].

Chin et al. conducted a detailed study of users' practices on smartphones and their perception of security and privacy [1]: they found that users worry about the threats of physical theft or damage, data loss and insufficient back up, malicious apps and wireless network attackers, limited battery lifetime, and signal strength. Users' practices to protect from those threats may however have limited effectiveness. In some cases users deduce trust indications from indicators not meant as such. For instance, much value is put on other users' reviews in the app repository [1]. In a qualitative study, Kraus et al. investigated which threats and mitigations on smartphones are known to users and how they perceive them:

users reported different feelings including social pressure, helplessness, dependency, and fatalism [9]. The authors suggest that the reasons for those negative feelings may be grounded in a lack of psychological need fulfillment. Nevertheless, in their study, the use of self-reported mitigations was related to positive feelings such as trust and feelings of being able to exercise control [9]. Note that the actual and perceived security of what users consider to be a mitigation can vary greatly and will not be discussed at this point.

Related work suggests that users worry about threats to their security and privacy on smartphones and that many users are willing to adopt mitigations. However, usability shortcomings of mitigation technologies on smartphones and users' mixed feelings regarding threats and mitigations call for an approach that focuses on new methods to enable positive user experiences when applying security and privacy actions.

2.2. Experiential approach to security and privacy

The necessity to include principles from user experience research into the design of security and privacy technologies has been recognized before. For example, Bødker et al. suggest that experiential approaches should be used to understand user behavior in the IT-security domain [5, p. 54]: "In daily life, people rarely do activities solely for the purpose of security. Instead, most IT-security decisions are part of other activities with other purposes. When analyzing these use situations it is impossible to isolate IT-security tasks or decisions." Hence, security is dependent on context and usage motives, and not only on a secure device and the implemented security procedures [5]. By gaining an understanding of users' motivation in terms of psychological needs, the present studies sheds lights on this issue.

Dunphy et al. [6] note that experience design faces a special challenge when it comes to security and privacy applications: within those applications two kinds of users need to be taken into account – the target user and the adversary; moreover, a user might switch between being a targeted person and being an adversary depending on the context. For example, users can become adversaries when they start intruding the privacy of people with whom they interact in social networks. Gaining an understanding of target users' motivation in terms of psychological needs could also help to explain these kinds of situations.

2.3. Psychological needs

In their work on satisfying life events, Sheldon et al. define psychological needs as "particular qualities of experience that all people require to thrive" [12, p. 325]. However, they also note that so far there is no consensus about what those needs are. As a consequence, they investigated 10 psychological needs from well-known theories of psychological need fulfillment (such as Deci and Ryan's self-determination theory [31], Epstein's cognitive-experiential self-theory [32]) 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.

Hassenzahl [14] took up the needs suggested by Sheldon et al. [12] and related them to a model of user experience. Thereby, psychological needs are used to describe classes of experiences [14]. This is done by considering different types of goals that underlie an action; *do-goals* and *be-goals* are differentiated [14]. 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 Hassenzahl [14]). The fulfillment of psychological needs (the be-goal) leads to a positive user experience [13].

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 [14,33]. Studies show that need fulfillment can be manipulated through product features leading to a positive change in user experience evaluations [33,34]. Also, users' judgement of a system's hedonic quality, i.e. quality aspects beyond the functional, is influenced by need fulfillment [14]. However, this depends on the attribution, i.e. the degree to which users deem the product responsible for the experience [14].

The studies presented in this work are based on the needs as defined in Sheldon et al. [12]. The usefulness of this set of needs in the context of HCI has previously been shown by Hassenzahl et al. [13]. Fronemann and Peissner [33] also build upon a set of psychological needs defined by Sheldon et al. [12] and Reiss [35]. An additional need they define, which is not covered by the definitions of Sheldon et al. [12], is *Keeping the meaningful* [33]. This need was also included into the present studies. In the following, definitions of the psychological needs which were deployed in the present studies are provided [12, p. 339].

Autonomy: *"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: *"Feeling that you are very capable and effective in your actions rather than feeling incompetent or ineffective."*

Relatedness: *"Feeling that you have regular intimate contact with people who care about you rather than feeling lonely and uncared for."*

Self-actualization: *"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: *"Feeling safe and in control of your life rather than feeling uncertain and threatened by your circumstances."*

Popularity: *"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: *"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: *"Feeling that your body is healthy and well-taken care of rather than feeling out of shape or unhealthy."*

Self-esteem: *"Feeling that you are a worthy person who is as good as anyone else rather than feeling like a 'loser' ."*

Stimulation: *"Feeling that you get plenty of enjoyment and pleasure rather than feeling bored and understimulated by life."*

Keeping the meaningful: *"Collecting meaningful things"* [33]/ *"saving"* [35]

3. Interview methodology

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 [14]. 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?)*

The interview script has been published in [36]. 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 covered a variety of possible actions, extracted from the literature on smartphone security risks [4,26] and users' threat perception [1]. 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 Chin et al. [1].

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.

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%

3.1. Procedure

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. The sessions took between 20 and 40 min depending on how talkative the participants were. Participants received 12€ reimbursement. 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.

3.2. Analysis

The codebook consisted of the descriptions of the 11 psychological needs (cf. Section 2), the items of the need fulfillment questionnaire [12], and a few items of the UNEEQ questionnaire (only for *Keeping the meaningful*) [37]. 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 [38]. 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. 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 [12]. 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). 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 [39]. 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 [4,26] 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 [38]. The coders met to discuss disagreements and to reach consent. Table 1 reports the results upon which the coders agreed.

3.3. Participants

Nineteen smartphone users (10 female) were recruited from a panel of Technische Universität Berlin. The age ranged from 18 to 58 years with a mean of 31 years. 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.

3.4. Smartphone usage

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%) [40]. 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 ($N = 15$). Only one participant had a professional IT background.

4. 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.

4.1. 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 min to answer, we preferred sending personalized invitations as we expected to achieve higher compliance of the participants and eventually higher data quality. Three vouchers à 50€ 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 [41] was employed which is based on the questionnaire by Sheldon et al. [12]. Questions for *Keeping the meaningful* were taken from the UNeeQ questionnaire [33,37]. 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 ($9 \text{ actions} \times 3 \text{ items per need} \times 8 \text{ needs} = 216$ 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" [42]).

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.

4.2. Participants

The participants (female = 37.1%) of the online study were between 18 and 61 years old, with an average of 28 years. They had diverse educational levels (Secondary school degree: 4.3%, completed training: 12.9%,high school degree: 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%).

4.3. Smartphone usage

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.

5. 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 na-

ture 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 macro-structure of the interview script. For each subsection, the two to three most mentioned needs are discussed.

5.1. 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 we report the psychological needs related to the different actions. The abbreviations P1 to P19 thereby indicate the different participants.

5.2. Saving battery lifetime

From an IT-security perspective the (automatic) monitoring of battery consumption may be used to detect malicious activities on a device [26]. 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".

5.3. Connectivity

When participants were asked about situations in which their data connections such as Bluetooth, NFC or GPS are disabled, we expected 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)

5.4. 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).

5.5. 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]."

5.6. 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.

5.7. 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 dont 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).

5.8. 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 […]."

5.9. 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, we 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 wouldnt 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, we found a variety of examples how psychological needs, i.e. be-goals, drive security and privacy actions on smartphones: 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. Online study results

In this section the results of the online survey are reported. We report the results for those security and privacy actions which we consider to be most influenceable by security and privacy technology designers.

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. Fig. 1 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 [43].

6.1. Backups

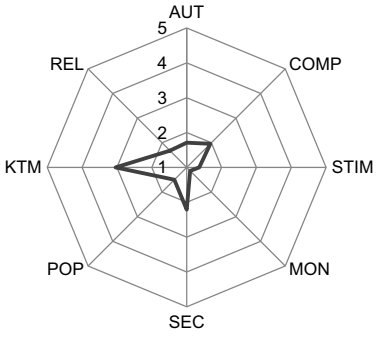
For participants who reported to do backups ($N = 14$), the Friedman test revealed a significant difference in need fulfillment for this action, $\chi^2 = 40.90$, $p < 0.01$. Post-hoc analysis showed that users ranked *Keeping the meaningful* significantly higher than *Popularity*, $Z = 3.16$, $p = 0.04$, $r = 0.60$. *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 Fig. 1(a)).

6.2. Updates

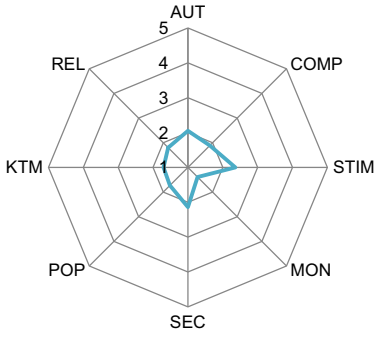
For participants who reported that they installed updates ($N = 22$), the Friedman test indicated significant differences between the level of need fulfillment, $\chi^2 = 30.00$, $p < 0.01$. Post-hoc analysis showed that values for *Stimulation* were significantly higher than for *Money/ Luxury*, $Z = 3.85$, $p < 0.01$, $r = 0.58$. The effect size for the pairwise comparison is large. The results suggest that *Stimulation* is a rather relevant factor to employ updates (cf. also Fig. 1(b)).

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.

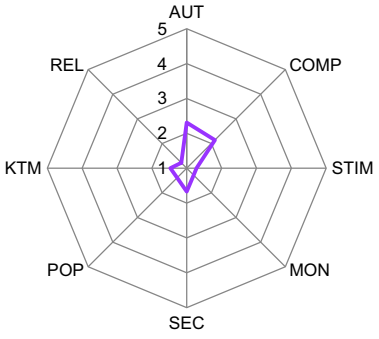
Need	Backups			Updates			Scrutinizing permissions			Password lock			Privacy settings			Encrypted messaging		
	M	Md.	SD	M	Md.	SD	M	Md.	SD	M	Md.	SD	M	Md.	SD	M	Md.	SD
AUT	1.71	1.50	0.89	2.05	1.25	1.25	**2.31**	**2.00**	1.10	**2.04**	**1.75**	1.06	**2.59**	**3.00**	1.00	2.12	1.50	1.33
COMP	1.96	2.00	0.84	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



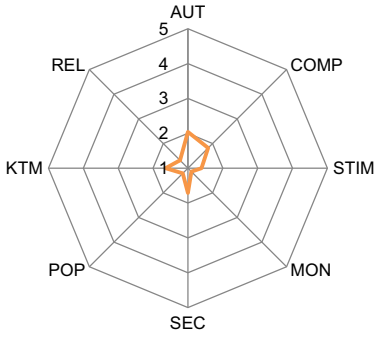
(a) Backups: Mean need fulfillment



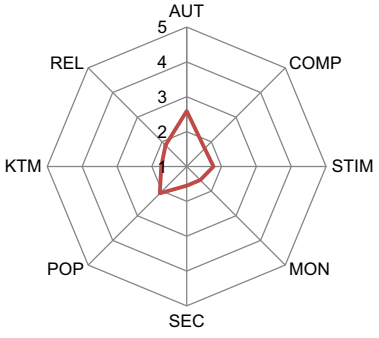
(b) Updates: Mean need fulfillment



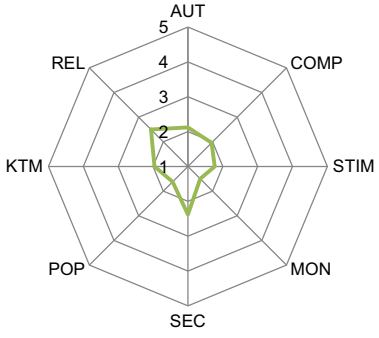
(c) Scrutinizing permissions: Mean need fulfillment



(d) Screenlock with authentication: Mean need fulfillment



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



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

Fig. 1. 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.

6.3. 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 Fig. 1(c)). 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 [13].

6.4. 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 Fig. 1(d)). Surprisingly, not even *Security* scored higher than the other needs.

6.5. 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 Fig. 1(e)). However, a Friedman test did not show significant differences in need fulfillment.

6.6. 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 Fig. 1(f)); 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 7.2.

7. 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.

7.1. 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. We leave additional conceptualizations to future work for which the present studies provide a good starting point.

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.

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, we suspect 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.

7.2. 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 [12,41]. 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 [13]. In addition, in their study, the need for *Security* also showed only a low correlation with positive affect [13]. 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” [13, p. 358]. This is also in line with findings of Karapanos et al. [44]: 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 [44]. 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, we suggest 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. We discuss in Section 7.3 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 [12]. 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 [45] and Westin [39] 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 [39]. We suspect that including further privacy functions (besides *Autonomy*) will lead to a better conceptualization of psychological needs in the context of security and privacy research. We plan to conduct further studies to investigate how the functions defined by Westin and Pedersen can be integrated into the concept of psychological needs.

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 [12]; in the context of technology usage, Hassenzahl et al. observed values between 2.9 and 3.3 [13]. A possible explanation is that, in contrast to Sheldon et al. [12] and Hassenzahl et al. [13], 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. How psychological need fulfillment can be included into the design of security and privacy technologies, is discussed in the following.

7.3. 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.

7.3.1. Authentication

We suggest improving the user experience of password locks 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 et al. [46] 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. [47] 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" [25]. Also, many solutions to improve usability of knowledge-based authentication methods have been suggested in the domain of graphical authentication [48]. In graphical authentication, the password is based on graphical data such as pictures or icons. It is subject to future research to investigate whether graphical passwords could provide for better need fulfillment and a positive user experience. Furthermore, we plan to investigate in future studies how psychological needs such as *Stimulation* and *Popularity* can be systematically addressed in the design of mobile authentication methods.

7.3.2. 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. [49] 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 [49]. One option to avoid negative effects on users' security behavior is to separate security updates from other updates [50]. 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.

7.3.3. 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. [7]). 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 [51]. Related work also indicates that a clear context supports security-friendly decisions when granting permissions [17,18]. 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 for future studies is to investigate to which degree run-time permissions (as currently featured in iOS and An-

droid 6.0) are perceived as fulfilling the need for *Autonomy* without being annoying.

In summary, the interview results illustrate how psychological needs can be used as high-level primary goals for the explanation of user behavior and motivation related to security and privacy actions on smartphones; The interviews and online study results suggest that besides the need for *Security*, different other needs such as *Keeping the meaningful*, *Stimulation*, *Autonomy* and *Competence* may serve as motivators for security and privacy actions. We conclude that the low mean values for need fulfillment in the online survey indicate that security and privacy actions may profit from new design approaches to support psychological need fulfillment in order to achieve a positive user experience. How different psychological needs can be systematically addressed in the design of security and privacy technologies on smartphones is an interesting research topic for future studies.

8. Conclusion

We conducted semi-structured in-depth interviews with 19 participants to explore the psychological needs that drive security and privacy actions on smartphones. The results show a variety of self-reported actions and illustrate how those actions are motivated by a variety of psychological needs, beyond the need for *Security*. We further conducted a quantitative online study with 70 participants as a first attempt to quantify psychological need fulfillment for the employment of security and privacy actions on smartphones. The results suggest that a variety of psychological needs may motivate security and privacy actions on smartphones. However, when measured quantitatively, psychological need fulfillment showed to be rather low. The present work provides examples of security and privacy technologies that could address psychological need fulfillment. The presented studies offer a basis for further conceptualizations and for elaborating on the potential that the application of psychological needs offer in the security and privacy context.

Acknowledgments

Based on: “Exploring Psychological Need Fulfillment for Security and Privacy Actions on Smartphones.”, by Lydia Kraus, Ina Wechsung, and Sebastian Möller which appeared in the Proceedings of EuroUSEC, Darmstadt, 18 July 2016. © Internet Society

We would like to express our gratitude to Tobias Fiebig for his assistance in preparing the interview study and to Michael Wagner for proofreading the manuscript. This work was supported by the EU FP-7 support action ATTPS under grant agreement no. 317665 and by the German Federal Ministry of Education and Research (BMBF) under the project Softwarecampus, grant no. 01IS12056. Any opinions, findings, conclusions, or recommendations expressed here are those of the authors and do not necessarily reflect the views of the funding body.

References

[1] Chin E, Felt AP, Sekar V, Wagner D. Measuring user confidence in smartphone security and privacy. In: Proceedings of the eighth symposium on usable privacy and security. ACM; 2012. p. 1.
[2] Felt AP, Egelman S, Wagner D. 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. ACM; 2012. p. 33–44.
[3] Mylonas A, Kastania A, Gritzalis D. Delegate the smartphone user? Security awareness in smartphone platforms. Comput Secur 2013;34:47–66.
[4] G. Hogben, M. Dekker, Smartphones: Information security risks, opportunities and recommendations for users, Eur Netw Inf Secur Agency 710 (01), 2010.
[5] Bødker S, Mathiasen N, Petersen MG. Modeling is not the answer!: Designing for usable security. interactions 2012;19(5):54–7.
[6] Dunphy P, Vines J, Coles-Kemp L, Clarke R, Vlachokyriakos V, Wright P. Understanding the experience-centeredness of privacy and security technologies. In: Proceedings of the 2014 workshop on new security paradigms workshop; 2014. p. 83–94.
[7] Felt AP, Ha E, Egelman S, Haney A, Chin E, Wagner D. Android permissions: user attention, comprehension, and behavior. In: Proceedings of the eighth symposium on usable privacy and security. ACM; 2012. p. 3.
[8] Reinfelder L, Benenson Z, Gassmann F. Differences between android and iphone users in their security and privacy awareness. In: Proceedings of the 11th international conference on trust, privacy, and security in digital business (TrustBus). Springer International Publishing; 2014. p. 156–67.
[9] Kraus L, Fiebig T, Miruchna V, Möller S, Shabtai A. Analyzing end-users knowledge and feelings surrounding smartphone security and privacy. In: Proc. IEEE security & privacy workshops – mobile security technologies (MoST); 2015.
[10] Bargas-Avila JA, Hornbæk K. 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. ACM; 2011. p. 2689–98.
[11] Ryan RM, Deci EL. Self-determination theory and the facilitation of intrinsic motivation, social development, and well-being. Am Psychol 2000;55(1):68.
[12] Sheldon KM, Elliot AJ, Kim Y, Kasser T. What is satisfying about satisfying events? Testing 10 candidate psychological needs. J Personality Social Psychology 2001;80(2):325.
[13] Hassenzahl M, Diefenbach S, Göritz A. Needs, affect, and interactive products—facets of user experience. Interact Comput 2010;22(5):353–62.
[14] Hassenzahl M. Experience design: technology for all the right reasons. Synth Lect Hum-Centered Inf 2010;3(1):1–95.
[15] Ben-Asher N, Kirschnick N, Sieger H, Meyer J, Ben-Oved A, Möller S. 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. ACM; 2011. p. 465–73.
[16] Kelley PG, Cranor LF, Sadeh N. Privacy as part of the app decision-making process. In: Proceedings of the SIGCHI conference on human factors in computing systems. ACM; 2013. p. 3393–402.
[17] Harbach M, Hettig M, Weber S, Smith M. 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. ACM; 2014. p. 2647–56.
[18] Kraus L, Wechsung I, Moller S. Using statistical information to communicate android permission risks to users. In: Workshop on Socio-technical aspects in security and trust (STAST). IEEE; 2014. p. 48–55.
[19] Benton K, Camp LJ, Garg V. Studying the effectiveness of android application permissions requests. In: Pervasive computing and communications workshops (PERCOM Workshops), 2013 IEEE international conference on. IEEE; 2013. p. 291–6.
[20] C. 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).
[21] Android Developers, Requesting permissions at run time, http://developer.android.com/training/permissions/requesting.html, (accessed: 2016-05-04).
[22] Statista - Das Statistikportal, Anteil der verschiedenen Android-Versionen an allen Geräten mit Android OS weltweit im Zeitraum 01. März 2016 bis 07. März 2016, http://de.statista.com/statistik/daten/studie/180113/umfrage/anteil-der-verschiedenen-android-versionen-auf-geraeten-mit-android-os/, (accessed: 2016-04-25).
[23] Harbach M, von Zezschwitz E, Fichtner A, De Luca A, Smith M. Itsa hard lock life: a field study of smartphone (un) locking behavior and risk perception. Symposium on usable privacy and security (SOUPS); 2014.
[24] 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).
[25] Bhagavatula C, Ur B, Iacovino K, Kywe SM, Cranor LF, Savvides M. Biometric authentication on iphone and android: usability, perceptions, and influences on adoption. In: Proceedings USEC; 2015.
[26] A. Shabtai, Y. Fledel, U. Kanonov, Y. Elovici, S. Dolev, Google android: a state-of-the-art review of security mechanisms, arXiv preprint arXiv:0912.5101.
[27] WhatsApp Blog, end-to-end encryption, http://blog.whatsapp.com/10000618/end-to-end-encryption, (accessed: 2016-04-25) (2016).
[28] Rashidi Y, Vaniea K. Poster: a user study of whatsapp privacy settings among arab users. IEEE symposium on security and privacy; 2015.
[29] R. Fedler, J. Schütte, M. Kulicke, On the effectiveness of malware protection on android, Tech. rep. (2013).
[30] Möller A, Michahelles F, Diewald S, Roalter L, Kranz M. 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 Mobile HCI; 2012. p. 3–6.
[31] Deci EL, Ryan RM. The “what” and “why” of goal pursuits: human needs and the self-determination of behavior. Psychological inquiry 2000;11(4):227–268.
[32] Epstein S. Cognitive-experiential self-theory. Handbook of personality: theory and research. Pervin LA, editor. New York: The Guilford Press; 1990.
[33] Fronemann N, Peissner M. User experience concept exploration: user needs as a source for innovation. In: Proceedings of the 8th nordic conference on human-computer interaction: fun, fast, foundational. ACM; 2014. p. 727–36.
[34] Sonnleitner A, Pawlowski M, Kässer T, Peissner M. Experimentally manipulating positive user experience based on the fulfilment of user needs, in:. In: human-computer interaction–INTERACT 2013. Springer; 2013. p. 555–62.
[35] Reiss S. Multifaceted nature of intrinsic motivation: the theory of 16 basic desires. Rev General Psychol 2004;8(3):179.

[36] Kraus L, Wechsung I, Möller S. Exploring psychological need fulfillment for security and privacy actions on smartphones. European workshop on usable security (Euro USEC); 2016.
[37] Uneeq - user needs questionnaire, http://www.hci.iao.fraunhofer.de/content/dam/hci/de/documents/UXellence_UserNeedsQuestionnaire_EN.pdf, (accessed: 2016-04-25).
[38] Landis JR, Koch GG. The measurement of observer agreement for categorical data. Biometrics 1977:159–74.
[39] Westin AF. Privacy and freedom. New York: Atheneum; 1967. p. 7.
[40] 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).
[41] S. Diefenbach, M. Hassenzahl, Handbuch zur Fun-ni Toolbox (2011).
[42] Krosnick JA. Survey research. Annu Rev Psychol 1999;50(1):537–67.
[43] Field A. Discovering statistics using SPSS. Sage publications; 2009.
[44] Karapanos E, Teixeira P, Gouveia R. Need fulfillment and experiences on social media: a case on facebook and whatsapp. Comput Hum Behav 2016;55:888–97.
[45] Pedersen DM. Psychological functions of privacy. J Environ Psychol 1997;17(2):147–56.
[46] Aumi MTI, Kratz S. Airauth: evaluating in-air hand gestures for authentication. In: Proceedings of the 16th international conference on human-computer interaction with mobile devices & services. ACM; 2014. p. 309–18.
[47] Karlesky M, Melcer E, Isbister K. Open sesame: reenvisioning the design of a gesture-based access control system. In: CHI'13 extended abstracts on human factors in computing systems. ACM; 2013. p. 1167–72.
[48] Biddle R, Chiasson S, Van Oorschot PC. Graphical passwords: learning from the first twelve years. ACM Comput Surv (CSUR) 2012;44(4):19.
[49] Vaniea KE, Rader E, Wash R. Betrayed by updates: how negative experiences affect future security. In: Proceedings of the 32nd annual ACM conference on human factors in computing systems. ACM; 2014. p. 2671–4.
[50] Ion I, Reeder R, Consolvo S. … no one can hack my mind: Comparing expert and non-expert security practices. In: Eleventh symposium on usable privacy and security (SOUPS 2015); 2015. p. 327–46.
[51] Garfinkel S, Lipford HR. Usable security: history, themes, and challenges. Synth Lect Inf Secur, Privacy, Trust 2014;5(2):1–124.