ATTPS | Achieving The Trust Paradigm Shift

Supplement to Deliverable 2.2

Beyond Usable Security: Towards Understanding Security and Privacy Actions on Smartphones in Terms of Psychological Need Fulfilment

Paper submitted for peer review at CHI 2016

Kraus et al 2016

Beyond Usable Security: Towards Understanding Security and Privacy Actions on Smartphones in Terms of Psychological Need Fulfillment

ABSTRACT

Smartphones offer vast opportunities for positive user experiences; however, at the same time threats to users' security and privacy evolve. In some situations users perform measures to mitigate these threats, but in other situations they do not, even if concern is reported. We suspect that the theory of psychological needs can help to further explain user behavior and usage situations by considering the underlying motives for pursuing an action. We conducted in-depth interviews and an online study to learn about the basic psychological needs which users intend to fulfill with security and privacy actions. Our findings provide first answers on the saliency of basic psychological needs in the context of smartphone security and privacy. Moreover, the results illustrate how psychological needs can help to explain the adoption of security and privacy technologies and the interaction with those technologies. We also discuss how the design of security and privacy technologies could be improved with the gained knowledge.

Author Keywords

Security and privacy; smartphones; psychological needs; user experience; user behavior

ACM Classification Keywords

H.5.2. Information interfaces and presentation (e.g., HCI): User-centered design;

1. INTRODUCTION

More than 2 billion people - almost a quarter of the world's population - are predicted to use a smartphone in 2016 [10]. Smartphone usage is an extensive source for usage experiences: they allow 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 evolve at the same time. Those include malicious apps, data loss, surveillance, and profiling, just to name a few. Related work shows that users are concerned about many of these threats and about their privacy on smartphones [7,12,28]. To mitigate these threats there is a variety of actions users can take [19].

Former works suggest to gain further insights into security and privacy aspects from an end-user perspective by using experiential approaches [6,25,26,9]. Experience is thereby seen as a holistic and broad view on the matter in order to gain a "rich understanding of people's practices and lives" [9]. Accordingly, while much work has been conducted to understand users' perceptions of smartphone security and privacy in terms of understanding, concerns, awareness, and attitudes [13,28,31,12,7], we suggest using an experiential approach based on psychological needs to gain a deeper understanding of the matter. According to Hassenzahl et al. [18], the main motivation to use interactive technologies is to fulfil psychological needs; a positive user experience is thus the result of need fulfillment.

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 [17]). 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 experience a feeling of *Autonomy* and thus 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 [17].

The goal of this paper is to learn more about the psychological needs which users intend to fulfill with security and privacy actions on smartphones. We first conducted in-depth interviews to explore the security and privacy actions which users employ on their smartphones and the reasons therefore (Section 3). We then transcribed and annotated the interview data applying the psychological needs as codes. The results of the interview study are

presented in Section 4. Based on the interviews, we came up with several assumptions regarding the relations between specific security and privacy actions and psychological needs. An online survey (Section 5) was conducted to quantify these assumptions. The findings of the online survey are presented in Section 6. Findings from the interview and online study are discussed conjointly in Section 7.

Our results provide first answers on which psychological needs are salient in the context of smartphone security and privacy. Moreover, the results illustrate how psychological needs can help to explain the adoption of security and privacy technologies and the interaction with those technologies. We also discuss how the design of security and privacy technologies could be improved with the gained knowledge.

2. RELATED WORK

In the following an overview of some of the main user issues concerning security and privacy on smartphones is presented.

Everyday practice and threat perception

Chin et al. conducted a detailed study of users' practices on smartphones and the perception of security and privacy [7]: They found that users perceive the threats of physical theft or damage, data loss and insufficient back up, malicious apps and wireless network attackers, battery lifetime, and signal strength. Moreover, 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 [7]. Kraus et al. investigated in a qualitative study 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 [23]. They suggest that the reasons for those negative feelings might be grounded in a lack of psychological need fulfillment.

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 [19]. The implementation of the permission model differs between smartphone operating systems (OSes). For instance, Android users have to accept all permissions or groups thereof before an app can be installed, whereas iOS users are shown a permission-request as soon as an app requests it for the first time. Moreover, iOS users can decide on an app-by-app basis which of the permissions they grant. Hence, it not unexpected, that Android and iOS users have a different risk perception [3]. Moreover, Android permissions have been shown to be difficult to understand for users; also, the permission requests are shown at an unfavorable point in the decision making process, that is when the decision to install an app has already been made [13]. Several solutions have been suggested to increase the understanding of and the attention towards permissions including improved information presentation and risk communication (cf. e.g. [21,4,22]). In 2014, the Android permissions were grouped and their presentation was modified to include icons for each group. While this has improved information presentation, security concerns remain [37].

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 a password or PIN [19]. However, unlocking a smartphone with password or PIN consumes much valuable time [16]. In a study of 2011, the PIN was perceived by only a quarter of users (26%) as a reliable method for protecting a mobile phone [2]. Many solutions to improve usability of authentication methods have been suggested, for instance in the domain of graphical authentication [5].

When it comes to communication, eavesdropping and interception pose a threat. They can be mitigated by deploying end-to-end encryption of communication (calls and/or messages) [34]. Privacy intrusion by other users of communication tools can be counteracted by appropriate privacy settings. For instance, Rashidi and Vaniea report that many users actively use privacy settings of Whatsapp - almost a third of the respondents hid their "last seen" feature [30].

To protect against malware, antivirus apps can be easily installed for Android; however, their usefulness is questionable [11]. Likewise the usage of security software is considered by many users as nonessential [28]. Keeping the device up-to-date is another mitigation strategy against malware. In a case study on update installation behavior, Möller et al. [27] report that many users of an Android app did not immediately install updates - a behavior which can lead to security vulnerabilities.

Data loss due to device loss or theft can be easily mitigated by backups. While users are concerned about these threats [7], 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 [28]. This might be due to unawareness towards the existence of such features [7].

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 reported being interested in applying further such mechanisms [2]. However, in some situations users perform security and privacy actions and in other situations they do not, even if concern is reported. We suspect that the theory of psychological needs can help to further explain user behavior and usage situations by considering the underlying motives for pursuing an action.

Experiential approach to security and privacy

An extensive literature review by Bargas-Avila and Hornbæk revealed that the term user experience is widely used but often describes different things; motivation is one dimension of user experience described therein [1].

Bødker et al. suggest that experiential approaches should be used to understand situations of use in the IT-security context [6]: "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." Security is therefore dependent on these use situations and not only on a secure device and the implemented security procedures [6].

Different approaches on how experiences can be investigated in the context of security and privacy have been suggested, e.g. participatory design, storytelling approaches or technology probes [25,26,9].

Dunphy et al. [9] note that experience design faces a special challenge when it comes to security and privacy applications as within those applications two kind 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 networking apps. We suspect that gaining understanding of target users' motivation helps also to explain these kinds of situations.

Psychological needs

Psychological needs are salient in satisfying events and supportive for intrinsic motivation [35,33]. In the context of interactive products users' judgement of a system's hedonic quality, i.e. quality aspects beyond the functional, is influenced by need fulfillment [18]. However, this depends on the attribution, i.e. the degree to which users deem the product responsible for the experience [18]. Needs can be used to classify different experiences and subsequently interactive products can be designed to support specific experiences [17]. Studies show that need fulfillment can be manipulated through product features leading to a positive change in user experience evaluations [14, 36].

The number of needs discussed in the literature varies between 3 and 16 needs [33,35,31]. Those needs are overlapping to a large part [14]. The study presented in this paper is based on the needs as defined by Sheldon et al. [35]. We decided to use this set of needs as its usefulness in the context of HCI has previously been shown by Hassenzahl et al. [18]. During analysis we also found that the additional need of *Keeping the meaningful* as defined in [14] was salient in the interviews, therefore we included it in the analysis, too. In the following an overview of the needs and their definition is provided.

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. [35]

Competence
Feeling that you are very capable and effective in your actions rather than feeling incompetent or ineffective. [35]

Relatedness
Feeling that you have regular intimate contact with people who care about you rather than feeling lonely and uncared for. [35]

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. [35]

Security
Feeling safe and in control of your life rather than feeling uncertain and threatened by your circumstances. [35]

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. [35]

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. [35]

Physical/Bodily
Feeling that your body is healthy and well-taken care of rather than feeling out of shape or unhealthy. [35]

Self-esteem
Feeling that you are a worthy person who is as good as anyone else rather than feeling like a "loser". [35]

Stimulation
Feeling that you get plenty of enjoyment and pleasure rather than feeling bored and understimulated by life. [35]

Keeping the meaningful
Collecting meaningful things [14]/*saving* [31]

Hassenzahl describes the motivational aspects of user experience in terms of different types of goals – "do-goals" and "be-goals" [17]. Do-goals are derived from higher-level be-goals that are the fulfillment of an underlying need. We consider this as the primary goal a user pursues. For example, missing somebody may lead to the desire to communicate with this person [17]. Making a phone call is the do-goal then, the feeling of being related to this person is the be-goal.

3. METHODOLOGY - INTERVIEWS

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 [17]. Therefore, the semi-structured in-depth interviews were centered on the following research questions:

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

In this approach we did not explicitly ask for the needs the participants aimed to fulfill with their actions. Thus, we considered the *why* questions to provide answers regarding the reasons for doing an action and we coded those reasons with the psychological needs (if applicable).

We tried to cover as many actions as possible; the actions were extracted from the literature on smartphone security risks [19,34] and users' threat perception [7]. We designed the action-questions intentionally in an open manner as we did not want to assume that users only stick to the actions which are defined in the literature. Hence, instead of asking whether the participants check the permissions we asked if they do something to avoid that apps access their sensitive information. Or, instead of asking if they use messaging apps with end-to-end encryption we asked if they do something to protect their communication. The saliency of security and privacy increased during the course of the interview.

The interview was divided in 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. Then they were 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 [7].

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.

Procedure

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 taken to enable verbatim transcription after the interviews. The audio recordings were deleted after the transcription process. The sessions took between 20 and 40 minutes 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 we did not mention that the interview is about security and privacy, but we told the participants that we are interested in 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 were sensitized for the topic leading them to become aware of shortcomings in their security behavior. Therefore, they were provided with a flyer on which they could find further information on how to protect their security and privacy on smartphones after the interview.

Analysis

The 11 psychological needs (cf. Section 2) were used as codes to label the primary goals/motives. Thereby, the codes could be used for either need fulfillment or frustration. To increase the validity of the interpretation, the coding of the needs was performed in several steps. First, two coders coded the transcripts and met to discuss about the interpretation of different situations mentioned in the interviews.

During the coding they came across many passages where participants told that they would do something to save money. However, saving money is not explicitly part of the definition of the need *Money/Luxury* as described above. 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 pay version, although the free version required more permissions. Thus after discussion, the coders decided to label these passages with *Money/Luxury*. The coders also discussed about the S*ecurity* 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 also found in the questionnaire on need fulfillment [35]. Situations where the participants reported the desire that others cannot track or observe what they are doing were coded as *Autonomy*. This is in line with Westin's definition of the functions of privacy, one of them being *personal autonomy* [40].

After the discussion, one of the initial coders repeated the coding in parallel with a third, independent coder. Interrater-agreement between the two coders was found to be moderate (Cohen's $\kappa = 0.46$). Again, the coders met to find consent. In the following, the coded transcripts upon which they agreed are used.

Participants

Demographics

19 smartphone users (10 female) were recruited from a panel of our institution. The age ranged from 18 to 58 years with an average of 31 years. Participants had diverse educational levels (approximately equally distributed among secondary school degree, qualification for university entrance, and university degree). Among the sample were 9 employees, 7 students and 3 job seekers.

Smartphone Usage

There were 13 Android users, 5 iPhone users and 1 Windows Phone user. Smartphone usage experience among participants was diverse: 4 participants had owned their smartphone for less than a year, 7 for 1-3 years and 8 for more than 3 years. Most of the participants use their

smartphone at least once per hour (N=15). Only one participant had a professional IT background.

4. INTERVIEW RESULTS

In this section we report the results of the interview study. An overview of the applied security and privacy actions is given in Table 1. Actions refer to actions as defined in the literature [19,34] and as mentioned by the participants in the interviews. Shadowed rows were later on considered for the online surveys.

Smartphone purchase

Regarding the reasons for buying a smartphone, we found that *Money/Luxury* influences the decision on the operating system. P5 stated that he bought an Android phone as "it was the cheapest". Also P1 mentioned that the decision for buying an Android phone was "a conscious decision, but not conscious for Android but rather […] conscious for the price. Otherwise it would have been an Apple."

Being in contact with friends, i.e. *Relatedness* was noted by P12: "[…] to be in contact with my friends by using Whatsapp or so that was the main reason [for buying a smartphone]."

App selection, uninstalling apps and mitigating access to sensitive information

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

Money can be also 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)

Security was another 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', well… well than I just don´t install it." P4 mentions concerns regarding security during app selection: "Well I type in search terms […] then, it depends on the advertisement if it is good, then I try it, but then sometimes I do worry, such a private developer, what kind of mischief they could do."

The feeling of *Competence* can also be a consequence when apps which request many permissions are installed: "I could handle it [the app] pretty well, and then I used it anyway" (P4). 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). *Autonomy* can also be a reason for uninstalling an app, as evident from this statement by P12: "Simply because I don't want Apple to know where I am or something like that".

Action	Frequ.	%
Check battery status	18	95%
Switch off all data connections (e.g. by using flight-mode)	17	89%
Deploy updates	16	84%
Protect from theft (e.g. by securely storing the device)	14	74%
Password lock	13	68%
Check permissions	13	68%
Check monthly bill/ prepaid balance	12	63%
Make backups	12	63%
Avoid financial apps/ functions (e.g. online banking)	10	53%
Disable WiFi connection	8	42%
Disable Bluetooth	6	32%
Disable GPS	6	32%
Reduce online "data traces"	4	21%
Adjust privacy settings of messaging apps	4	21%
Hide one's identify (e.g. by fake user profiles)	4	21%
Use antivirus apps	3	16%
Use remote management apps	2	11%
Do not use messaging apps	3	16%
Use apps for privacy protection or permission management	2	11%
Use messaging apps with end-to-end encryption	1	5%
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%

Table 1 Security and privacy actions reported in the interviews

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 things is related to the subjective value that the participants attach to them, as can be seen in 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 travelling I dropped my mobile phone in a river. Well, than I thought 'mhh damn it'. I got my phone to work again, but then I uploaded everything to the cloud… well, that I do not lose all my pictures […]." Also P12 noted: "It happened once that I dropped my phone […] and afterwards all the data was gone […] And there were many pictures on it, many funny videos and everything… then I thought to myself: 'that shouldn't happen again'".

Connectivity

When we asked the participants about situations when their data connections such as Bluetooth, NFC or GPS are disabled, they mentioned situations in which they switch off

all data connections (e.g. by activating the flight mode). A reason for this seems to be 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 let alone" (P9). "I always disabled it [all data connections] at work, so that I don't get distracted" (P15).

Money/Luxury seems to be another important 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 thereby I can save some of my data contingent at least that is how I understood it."

Health concerns, classified by as the *Physical/Bodily* need, were also mentioned as a reason to switch off data connections, as stated P2: "Well because it [the phone] is always looking for some WiFi connections and actually because of the radiation." P12 noted: "Yes, for example when I put my iPhone in my trouser pocket then I generally switch-off my phone. Yeah, because… well I think this phone radiation can't be so good."

When it comes to using public WiFi spots, a need for *Security* was visible: "Well, for me that is… open WiFi is too risky for me." (P15)

Updates

Updates were mainly seen as a source for *Stimulation*, 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).

Saving battery lifetime

Relatedness was a reason why the participants check their battery status or save battery. P12 mentioned that he started to check his battery status regularly as there have been situations where "I was somehow out of it 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 for friends or so". P16 said that she saves battery because "then I am always available, so I don't like that, if I am not available at all…"

The need for *Security* is 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".

Password Locking

Not surprisingly, most quotes related to password locks were coded with *Security*, for instance this quote by P8: "Uumh, if it [the phone] is stolen or so, 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]".

Popularity as a reason to adopt a password lock was 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 safety reasons."

Protection from theft

Interestingly, many of the participants mentioned that they store their device securely or that they pay attention to where they leave the device. This seems to provide 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 back pack; I'd rather carry it on me, then I know it's there and I relatively quickly notice 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]; I don't feel like being stressed."

Communication

Interestingly, *Relatedness* and *Autonomy*, two needs which are rather contrary were most salient during the topic of communication. Being in contact with people one cares about, 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 than 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). But also, *Relatedness* can lead people to adopt apps which are only used by particular friends: "Because I have a lot of friends who are not on Facebook and who do not use WhatsApp […] but I would like to be in contact with those friends, yes, that's the main reason." (P12)

When we asked the participants if they do something to protect their communication, we expected that they may mention end-to-end encryption or the like. However, only one participant reported to use it. Instead many said that they use privacy settings in messaging apps or a password lock. We interpreted the usage of privacy settings as being related to *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) *Autonomy* was also a motive for not using more than one messaging app, P1 said: "Well, WhatsApp is enough for me as a bulldozing measure, and I believe that if I would install Facebook Messenger this would be even worse and it would put me under stress all the time."

Group chats in messaging apps were seen as a possible source of unpleasant consequences by P6: "Yes, so, I am careful when it gets 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*.

The results from the interview study suggest that there is a variety of needs which drive security and privacy actions on smartphones. We conducted an online survey to find

further evidence for these results and to determine in more detail which actions are driven by which needs.

5. METHODOLOGY – ONLINE SURVEY

The online survey was conducted with the tool LimeSurvey [24]. We selected some of the actions which participants reported in the interviews and measured general need fulfillment for each of those actions. We mainly selected actions which we consider to be influenceable by security and privacy technology designers. For instance, we skipped the two most widely deployed actions from the interview (check battery status and switch off all data connections). For battery checks, the designers can only design applications that consume little energy. Likewise, if the users wants to be undisturbed and switches the device off there is nothing a designer can support them with. Even though end-to-end encrypted messaging was only reported by one participant we consider it important as it can be highly influenced by security technology designers [41].

Finally, the actions that remained were: installing updates. protection from theft (including remote management), password locking, scrutinizing permissions, checking monthly bill/ prepaid balance, doing backups, managing data connections (WiFi, Bluetooth, GPS), privacy settings of messaging apps, using messaging apps with end-to-end encryption.

Design and Procedure

70 participants were recruited by word of mouth and email. Before the actual survey started, participants were asked if they are smartphone users and if they have ever downloaded apps before. If they were not using smartphones, they were thanked and notified that the survey is only intended for smartphone users.

The actual survey started with questions on demographics. Afterwards, questions on smartphone usage were asked: for how long the smartphone has been used, how frequently it is used, what the operating system is, what their three favorite apps are, what the reasons for buying a smartphone were, and whether they perceive different situations as threat. The survey was then divided in three different versions. Otherwise it would have been too long and may have resulted in fatigue effects.

Version 1: Participants were asked if they apply backups and if there are situations where 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 within messaging apps (what is meant with "privacy settings" was briefly explained).

Version 3: Participants were asked if they do something to protect their phone from theft, if so, they were asked what (e.g. store securely or remote access). 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 we could not assume that all participants are familiar with the term "end-to-end encryption" we gave examples of such apps and also let them an option to specify "other".

For each action, participants were asked to indicate the level of need fulfillment they experienced. To do so we employed the questionnaire presented in [35]. Questions for *Keeping the meaningful* were taken from the UNeeQ questionnaire [14,38]. Based on [8] 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…"

To further reduce possible fatigue effects, we only selected 2 of the 3 items of the original need questionnaires. Moreover, we removed the needs for Self-actualization, Self-esteem and Physical/Bodily as less than 1% of the interview codes referred to them.

Besides those need questions, which differed between the three versions, all questions were the same for all participants. Before the survey closed, participants were asked additional questions on backup behavior, installing messaging apps and the like. However, the results of these questions are not reported in the current paper.

In the last question they were asked to rank the 10 fundamental needs as defined in [35] according to their subjective importance.

Participants

Table 2 provides an overview of the participants' demographics, in total and for each version of the survey.

Sample size (Survey 1, 2, 3)	70 (24, 23, 23)
Age (Survey 1, 2, 3)	18-61 (20-55, 21-61, 18-31); Mean: 28.08 (29.13, 29.83, 25.17)
Gender (Survey 1, 2, 3)	F: 37.1 % (25%, 54.5%, 30.4%); M: 62.9 % (75%, 45.5%/,69.6%)
IT expertise (Survey 1, 2, 3)	No: 60% (58.3%, 59.1%, 65.2%); Yes: 40% (41.7%, 40.9%, 34.8%)
Educational level (total)	Secondary school degree: 4.3% Completed training: 12.9% High school degree: 32.9 % College/ university degree: 50%
Occupational group (total)	Employees: 38.6% Undergraduate students: 44.3% Other (e.g. job seekers, self-employed): 17.2%
Smartphone usage (total)	4-12 months: 5.7 %; 1-3 years: 32.9% More than 3 years: 61.4%
Frequency of usage (total)	One or several times p. hour: 70% One or several times p. day: 27.2% Several times p. week: 1.4% Less often: 1.4%
Operating system (total)	Android: 57.1%; iOS: 32.9% Windows: 5.7%; other: 4.3 %

Table 2 Demographics and Smartphone usage

The sample was diverse regarding age, smartphone usage, and occupational groups; however, there was a bias towards

male participants, higher educational levels and undergraduate students.

6. ONLINE SURVEY - RESULTS

In this section we report the results of the online surveys. The quantitative data from the online surveys are grouped by security and privacy actions and the saliency of each need per action is presented.

Backups

The survey showed that for users of backups the fulfillment of the needs for *Keeping the meaningful* (M = 3.04, Mdn = 3.50, SD = 1.34), *Security* (M = 2.21, Mdn. = 2.00, SD = 1.19) and *Competence* (M = 1.96, Mdn. = 2.00, SD = 0.84) were most salient (cf. Figure 1). As our subsample of backup users was small, we conducted a non-parametric Friedman test to see whether users rank some needs higher than others. The result was significant, χ^2 = 40.90, $p < 0.01$, $N = 14$. Post hoc analysis showed that users ranked *Keeping the meaningful* significantly higher than *Popularity*, $Z = 3.16$, $p = 0.044$, *Stimulation*, $Z = 3.74$, $p < 0.01$, and *Money/Luxury*, $Z = 4.13$, $p < 0.01$.

A Mann-Whitney-U-Test was used to compare the need scores between users and non-users. While users of backups ranked *Keeping the meaningful* significantly higher, $U = 108$, $p = 0.026$, they ranked *Stimulation* significantly lower compared to non-users, $U = 36$, $p = 0.033$. In summary, the results suggest that *Keeping the meaningful* plays a major role as a primary goal for doing backups.

Updates

The most salient needs for update users were found to be *Stimulation* (M = 2.36, Mdn. = 1.75, SD = 1.33), *Security* (M = 2.14, Mdn. = 2.00, SD = 1.28), and *Autonomy* (M = 2.05, Mdn. = 1.25, SD = 1.25) (cf. Figure 1). A non-parametric Friedman test revealed significant differences between the different ranks of the needs, $\chi^2 = 30.00$, $p < 0.01$, $N = 22$. Post-hoc analysis showed that for users values for *Stimulation* were significantly higher than for *Money/ Luxury*, $Z = 3.85$, $p < 0.01$. Thus, the results suggest that *Stimulation* plays a role as a primary goal in doing updates. As all respondents of the question were update users, no comparison between users and non-users could be done.

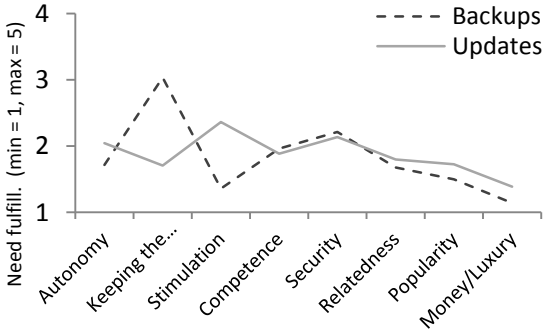

Figure 1 Mean need fulfillm. for users who do backups and updates

Password Locking

The most salient needs for password lock users were *Autonomy* (M = 2.04, Mdn. = 1.75, SD = 1.06), *Competence* (M = 1.82, Mdn. = 1.00, SD = 1.12), and *Security* (M = 1.71, Mdn. = 1.50, SD = 0.91; cf. Figure 4). A Friedman test was significant, $\chi^2 = 30.00$; $p < 0.01$; $N = 14$; however, post-hoc analysis showed no significant differences.

In summary, it is difficult to say whether there are one or more needs which play an important role as a primary goal for using password locking. Mean values for need fulfillment were rather low (mostly below 2.0) and against our expectations *Security* was not more salient than other needs.

Permissions

The most salient needs among users who scrutinize permissions were *Autonomy* (M = 2.31, Mdn. = 2.00, SD = 1.10), *Competence* (M = 2.14, Mdn. = 2.00, SD = 0.78), and *Security* (M = 1.67, Mdn. = 1.00, SD = 1.03) (cf. Figure 2). A non-parametric Friedman test was significant, χ^2 = 58.89, $p < 0.01$, $N = 18$. Post-hoc analysis showed that users ranked *Autonomy* significantly higher than *Relatedness*, $Z = 3.61$, $p < 0.01$, *Money/ luxury*, $Z = 3.91$, $p < 0.01$, *Stimulation*, $Z = 3.71$, $p < 0.01$, and *Popularity*, $Z = 3.20$, $p = 0.039$. Also, users ranked *Competence* significantly higher than *Relatedness*, $Z = 3.50$, $p = 0.013$, *Money/Luxury;* $Z = 3.81$, $p < 0.01$, and *Stimulation*, $Z = 3.61$, $p < 0.01$. A Mann-Whitney-U-Test did not reveal significant differences between users and non-users; also, user who reported to check permissions yielded similar need scores regardless of their OS (Android vs. iOS).

Nevertheless, the results suggest that *Autonomy* and *Competence* play a major role as primary goals of scrutinizing permissions.

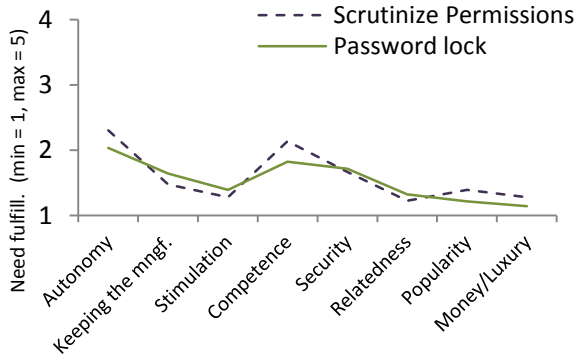

Figure 2 Mean need fulfillm. for users who scrutinize permissions and users of password lock

End-to-end encrypted messaging

The most salient needs for the users of end-to-end encrypted messaging apps were *Relatedness* (M = 2.50; Mdn. = 3.00, SD = 1.34), *Security* (M = 2.38, Mdn. = 3.00, SD = 1.45), and *Autonomy* (M = 2.12, Mdn. = 1.50, SD = 1.33) (cf. Figure 3). A Friedman test was significant, χ^2 = 18.78; $p < 0.01$; $N = 13$; nevertheless, post-hoc analysis did not yield significant results. Need ranks between users and

non-users were also not significantly different (Mann-Whitney-U-Test). Therefore, it is difficult to say whether there are one or more needs, which serve as primary goals for using end-to-end encrypted messaging apps.

Privacy settings

The most salient needs for users of privacy settings in messaging apps were *Autonomy* (M = 2.59, Mdn. = 3.00, SD = 1.00), *Popularity* (M = 2.09, Mdn. = 2.00, SD = 1.30), and *Relatedness* (M = 1.86, Mdn. = 1.00, SD = 1.10; cf. Figure 3). A Friedman test did not show significant differences in need fulfillment of users. Mann-Whitney-U-Tests did not indicate differences in need fulfillment between users and non-users.

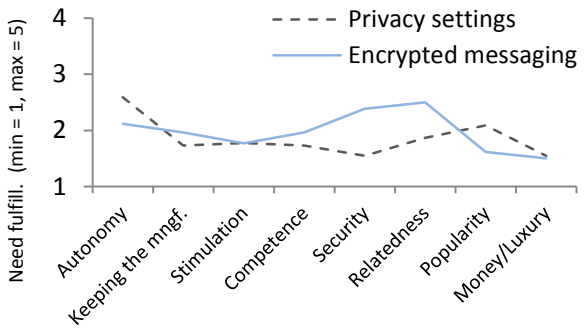

Figure 3 Mean need fulfillm. for users of privacy settings and users of encrypted messaging

Data connections

The most salient needs for users who switch off data connections were *Autonomy* (M = 2.27, Mdn. = 2.00, SD = 1.25), *Security* (M = 2.13, Mdn. = 1.50, SD = 1.30), and *Competence* (M = 1.98, Mdn. = 1.50, SD = 1.08) (cf. Figure 4). A Friedman test indicated differences between the need scores, $\chi^2 = 30.77$; $p < 0.01$; $N = 24$; however, post hoc tests did not show significant results. A Mann-Whitney-U-Test did not show significant differences in need ranks between users and non-users. It is difficult to say which needs influence the managing of data connections.

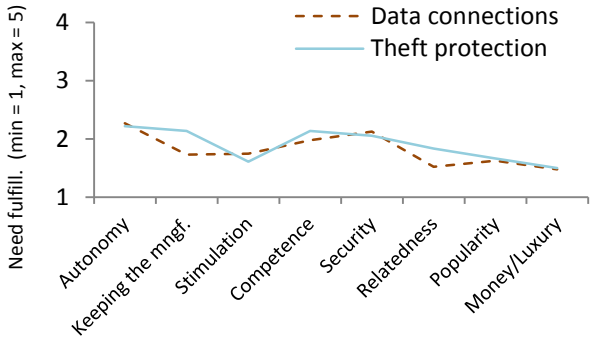

Figure 4 Mean need fulfillm. for users who switch off data connections and users who do theft protection

Theft protection

The most salient needs for users who do employ theft protection were *Autonomy* (M = 2.22, Mdn. = 2.25, SD = 1.19), *Keeping the meaningful* (M = 2.14, Mdn. = 2.25, 1.05), and *Competence* (M = 2.14, Mdn. = 1.75, SD = 1.10; cf. Figure 4). A Friedman test did not show significant differences between need ranks among users. Mann-Whitney-U-Tests revealed that users who protect their device against theft, rank *Money/Luxury* lower than users who do not protect their device, $U = 44$, $p = 0.030$, $N = 23$. This suggests that the feeling of having plenty of money might result in *not* protecting the device from theft.

7. DICUSSION

In this paper, we investigated psychological need fulfillment in the context of security and privacy actions on smartphones and gained insights into users' underlying primary goals. Our main contribution is to provide first answers on how psychological needs can help to explain user behavior related to security and privacy on smartphones.

Psychological needs in security and privacy actions on smartphones

Our results suggest that for some actions such as making backups, installing updates, and scrutinizing permissions the fulfillment of specific needs e.g. *Keeping the meaningful*, *Stimulation*, and *Autonomy*, play a major role. Future studies should investigate whether a relationship between need fulfillment and hedonic qualities can be also found for security and privacy technologies, and whether need fulfillment influences adoption of those technologies.

However, need fulfillment can also have a negative effect on security, for example, if updates are only installed when new features are announced (i.e. if the user expects a *Stimulation* experience), and not when security vulnerabilities are closed. This is in line with former studies in the context of desktop computers, which show that negative experiences with updates can also have a negative impact on future security behavior, for instance when updates disappoint expectations [39]. Therefore, developers should think carefully on how they announce their updates in a way that users' expectations regarding *Stimulation* are fulfilled.

Keeping the meaningful as a primary goal for doing backups suggests that doing backups is intrinsically motivated if files are deemed meaningful by the user. To this end, system recoverability might suffer as the term "meaningful" is rather subjective. For instance, important files for system recoverability might not be deemed "meaningful" by the user. Nevertheless, this knowledge could be used to motivate users in doing backups by reminding them in a way that addresses their need for *Keeping the meaningful*.

Scrutinizing permissions is the action where *Autonomy* and *Competence* fulfillment are most salient. This is on the one hand a promising result, as it suggests that scrutinizing permissions makes users feel autonomous and competent.

On the other hand, this feeling should be in line with the actual security and privacy state of the system; it is debatable that this is the case. Further studies are needed to investigate the current practices and feelings of users in the context of permission usage. Interestingly, Android and iPhone users did not rank the need fulfillment significantly different, even though different permission granting approaches are deployed.

The results from the interviews imply that especially in the context of communication users need to make trade-offs in favor of *Relatedness*. Regarding the usage of privacy settings in messaging apps, the online survey did not provide a clear answer whether *Autonomy* plays a major role as primary goal for this action. Further studies are needed to investigate privacy settings regarding need fulfillment and the possible trade-offs users have to make in favor of *Relatedness* in the context of communication.

For password locking, we did not find one or more needs to be especially influential and need fulfillment was in general low. This might be due to the fact that password locks are especially contrary to other primary goals and psychological needs and most likely always a barrier. Rarely ever is a screen unlocked for its own purpose. Nevertheless, it is interesting that not even the feeling of *Security* was salient for this action. What could be tried however is to improve hedonic qualities of password locks by fulfilling other needs such as *Stimulation* (e.g. by making unlocking fun) or *Popularity* (by having a "phat" screen lock). An example for an authentication system, which addresses the first issue, has been provided in [20].

Interpretations of psychological needs

In this study, we have interpreted the desire for privacy as being related to *Autonomy*. Also we have interpreted security rather in the sense of being "safe from threats and uncertainties" and not in the sense of "having a comfortable set of routines and habits" [35]. The relationship between privacy and security as defined in the IT-security domain and the basic psychological needs should be further investigated in future studies.

Whereas the need for *Money/Luxury* was quite salient in the interview, the online survey did not provide further evidence. This might be due to the fact that we interpreted *Money/Luxury* to include the desire to save money; however, this desire could be rather an extrinsic motivational factor instead of an intrinsic motivational factor. Hence, the results suggest that the need to feel that one has got "plenty of money" or "nice possessions" [35] is not a motivator for intrinsic security and privacy actions.

Although psychological needs are assumed to be universal [35], their saliency might be different for different groups of users. For instance, *Popularity* might be more important for adolescents compared to older users.

Summarizing, we see a high potential for psychological needs to explain user behavior with respect to adoption of and interaction with security and privacy actions. Thereby, we can distinguish between three kinds of situations: In the first type of situations, security itself is not the primary goal of the users; rather it is a barrier, which needs to be removed (cf. also [29]). This is also known as the "secondary task problem" [15] and has been intensively discussed in the literature. Password lock is an example and our results provide further evidence for this. In other situations, security and/or privacy are in line with the primary goal as can be seen in the example of backups, updates and permissions. The third kind of situations are those in which the user needs to make trade-offs between two primary goals one of them being security or privacy related (communication is an example for this).

8. LIMITATIONS

In both studies, we investigated security and privacy actions in a general way and did not ask for concrete implementations of mechanisms. How such security or privacy mechanisms, which offer a need fulfilling experience, should look like needs to be investigated in future studies.

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. We tried to reduce this limitation by applying an iterative coding process and by determining interrater agreement. Our interview sample consisted partly of students and job seekers which might have led to the result that saving money was rather salient as a reason for making decisions.

In the online survey there was a high amount of questions as need fulfillment was determined for several security and privacy actions. By further splitting the results in users and non-users of an action, the sample size for each action was rather small. However, we suspect that this helped to reduce possible fatigue effects. Also, the need questions for non-users provided a rather vaguely defined situation which might have rendered it difficult for non-users to answer these questions. Therefore, the non-users' need fulfillment or lack thereof should be further investigated in future studies. The survey sample consisted mainly of, well-educated, western-oriented participants in their twenties; thus, the results can be generalized to this population only.

9. CONCLUSION

In this paper, a mixed method design was applied to investigate security and privacy actions on smartphones and their relation to psychological need fulfillment. The results suggest that psychological needs are a promising approach to further explain user behavior with respect to backups, updates, app permissions, and communication. For other actions (e.g. password locking) the results were inconclusive. The topic should be further investigated in future studies with respect to explaining (non-)usage of concrete technologies and applications, regarding the trade-offs in need fulfillment which users have to make when using smartphones, and how the need-based approach can help to improve hedonic qualities of security and privacy applications.

REFERENCES

1. Javier A. Bargas-Avila and Kasper Hornbæk. 2011. Old wine in new bottles or novel challenges: a critical analysis of empirical studies of user experience. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 2689-2698. http://doi.acm.org/ 10.1145/1978942.1979336
2. Noam Ben-Asher, Niklas Kirschnick, Hanul Sieger, Joachim Meyer, Asaf Ben-Oved, and Sebastian Möller. 2011. 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*, 465–473.
3. Zinaida Benenson, Freya Gassmann, and Lena Reinfelder. 2013. Android and iOS users' differences concerning security and privacy. In *CHI'13 Extended Abstracts on Human Factors in Computing Systems*, 817-822.
4. Kevin Benton, L. Jean Camp, and Vaibhav Garg.2 013. Studying the effectiveness of android application permissions requests. In: Pervasive Computing and Communications Workshops (PERCOM Workshops), 291-296.
5. Robert Biddle, Sonia Chiasson, and Paul C. Van Oorschot. 2012. Graphical passwords: Learning from the first twelve years. *ACM Computing Surveys (CSUR)*, 44, 4: 19.
6. Susanne Bødker, Niels Mathiasen, and Marianne G. Petersen. 2012. Modeling is not the answer! Designing for Usable Security. *interactions*, 19, 5: 54-57.
7. Erika Chin, Adrienne P. Felt, Vyas Sekar, and David Wagner. 2012. Measuring user confidence in smartphone security and privacy. In *Proceedings of the Eighth Symposium on Usable Privacy and Security* (SOUPS), 1.
8. Sarah Diefenbach, Marc Hassenzahl. 2010. Handbuch zur Fun-ni Toolbox. Retrieved September 2, 2015 from http://fun-ni.org/wp-content/uploads/Diefenbach+Hassenzahl_2010_HandbuchFun-niToolbox.pdf
9. Paul Dunphy, John Vines, Lizzie Coles-Kemp, Rachel Clarke, Vasilis Vlachokyriakos, Peter Wright, John McCarthy, and Patrick Olivier. 2014. Understanding the Experience-Centeredness of Privacy and Security Technologies. In *Proceedings of the 2014 workshop on New Security Paradigms Workshop* (NSPW), 83-94.
10. eMarketer: referenced by Sophie Curtis. 2014. Quarter of the world will be using smartphones in 2016. Retrieved September 2, 2015 from http://www.telegraph.co.uk/technology/mobile-phones/11287659/Quarter-of-the-world-will-be-using-smartphones-in-2016.html
11. Rafael Fedler, Julian Schütte, and Marcel Kulicke. 2013. On the effectiveness of malware protection on Android. Technical Report. Fraunhofer AISEC, Berlin.
12. Adrienne P. Felt, Serge Egelman, and David Wagner. 2012. 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*, 33–44.
13. Adrienne P. Felt, Elizabeth Ha, Serge Egelman, Ariel Haney, Erika Chin, and David Wagner. 2012. Android permissions: User attention, comprehension, and behavior. In *Proceedings of the Eighth Symposium on Usable Privacy and Security* (SOUPS), 3.
14. Nora Fronemann and Matthias Peissner. 2014. 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*, 727-736.
15. Simson Garfinkel and Heather R. Lipford. 2014. Usable security: History, themes, and challenges. In: *Synthesis Lectures on Information Security, Privacy, and Trust*, 5(2), Elisa Bertino and Ravi Sandhu (eds.), Morgan & Claypool Publishers, 1-124.
16. Marian Harbach, Emanuel von Zezschwitz, Andreas Fichtner, Alexander De Luca, and Matthew. Smith. 2014. 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)*, 213- 230.
17. Marc Hassenzahl: Experience design. 2010. Technology for all the right reasons. In: *Synthesis Lectures on Human-Centered Informatics*, 3(1), John M. Carroll (ed.). Morgan & Claypool Publishers
18. Marc Hassenzahl, Sarah Diefenbach, and Anja Göritz. 2010. Needs, affect, and interactive products–Facets of user experience. *Interacting with computers* 22, 5: 353-362.
19. Giles Hogben and Marnix Dekker. 2010. Smartphones: Information security risks, opportunities and recommendations for users. *European Network and Information Security Agency*, 710, 1.
20. Michael Karlesky, Edward Melcer, and Katherine Isbister. 2013. Open sesame: re-envisioning the design of a gesture-based access control system. In *CHI'13 Extended Abstracts on Human Factors in Computing Systems*, 1167-1172.
21. Patrick G. Kelley, Lorrie F. Cranor, and Norman Sadeh. 2013. Privacy as Part of the App Decision-Making Process. In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 3393-3402.
22. Lydia Kraus, Ina Wechsung, and Sebastian Möller. 2014. Using Statistical Information to Communicate

Android Permission Risks to Users. In *Workshop on Socio-Technical Aspects in Security and Trust (STAST)*, 48-55.

23. Lydia Kraus, Tobias Fiebig, Viktor Miruchna, Sebastian Möller, and Asaf Shabtai. 2015. Analyzing End-Users' Knowledge and Feelings Surrounding Smartphone Security and Privacy. In *Workshop on Mobile Security Technologies (MoST)*
24. LimeSurvey – Tool. Retrieved September 2, 2015 from https://www.limesurvey.org
25. Niels Mathiasen and Susanne Bødker. 2008. Threats or threads: from usable security to secure experience? In *Proceedings of the 5th Nordic conference on Human-computer interaction: building bridges*, 283-289.
26. Niels Mathiasen. 2008. Investigating how everyday people experience security, Poster presented at the *Symposium on Usable Privacy and Security (SOUPS)*
27. Andreas Möller, Florian Michahelles, Stefan Diewald, Luis Roalter, and Matthias Kranz. 2012. 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* , 3-6.
28. Alexios Mylonas, Anastasia Kastania, and Dimitris Gritzalis. 2013. Delegate the smartphone user? Security awareness in smartphone platforms. *Computers & Security*, 34: 47–66.
29. Donald A. Norman. 2009. The Way I see it When security gets in the way. *Interactions* 16.6: 60-63.
30. Yasmeen Rashidi and Kami Vaniea. 2015. A User Study of WhatsApp Privacy Settings Among Arab Users. Poster presented at the *IEEE Symposium on Security and Privacy*
31. Lena Reinfelder, Zinaida Benenson, and Freya Gassmann. 2014. Security and privacy awareness of Android vs. iOS users. In *TrustBus: Trust, Privacy and Security in Digital Business*
32. Steven Reiss. 2004. Multifaceted nature of intrinsic motivation: The theory of 16 basic desires. *Review of General Psychology*, 8, 3: 179
33. Richard M. Ryan, Edward L. Deci. 2000. Self-determination theory and the facilitation of intrinsic motivation, social development, and well-being. *American psychologist*, 55, 1: 68
34. Asaf Shabtai, Yuval Fledel, Uri Kanonov, Yuval Elovici, and Shlomi Dolev. 2009. Google android: A state-of-the-art review of security mechanisms. arXiv preprint: arXiv:0912.5101
35. Kennon M. Sheldon, Andrew J. Elliot, Youngmee Kim, and Tim Kasser. 2001. What is satisfying about satisfying events? Testing 10 candidate psychological needs. *Journal of personality and social psychology*, 80, 2: 325
36. Andreas Sonnleitner, Marvin Pawlowski, Timm Kässer, and Matthias Peissner. 2013. Experimentally Manipulating Positive User Experience Based on the Fulfilment of User Needs. In *Human-Computer Interaction–INTERACT*, 555-562.
37. Cody Toombs. 2014. Simplified Permissions UI in The Play Store Could Allow Malicious Developers To Silently Add Permissions. Retrieved September 2, 2015 from http://www.androidpolice.com/2014/06/10/simplified-permissions-ui-in-the-play-store-could-allow-malicious-developers-to-silently-add-permissions/
38. UNeeQ - User Needs Questionnaire, Retrieved September 2, 2015 from http://www.hci.iao.fraunhofer.de/content/dam/hci/de/documents/UXellence_UserNeedsQuestionnaire_EN.pdf
39. Kami E. Vaniea, Emilee Rader, and Rick Wash. 2014. Betrayed by updates: how negative experiences affect future security. In *Proceedings of the 32nd annual ACM conference on Human factors in computing systems*, 2671-2674.
40. Alan F. Westin. 1967. *Privacy and Freedom.* New York: Atheneum.
41. Alma Whitten and J. Doug Tygar. 1999. Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0. In *Usenix Security (Vol. 1999)*