Analyzing End-Users' Knowledge and Feelings Surrounding Smartphone Security and Privacy

Lydia Kraus*, Tobias Fiebig*, Viktor Miruchna*, Sebastian Möller* and Asaf Shabtai†

*Technische Universität Berlin
Email: lydia.kraus@telekom.de, tfiebig@sec.t-labs.tu-berlin.de, viktor@miruchna.de, sebastian.moeller@telekom.de

†Ben-Gurion University of the Negev
Email: shabtaia@bgu.ac.il

***Abstract*—Along with the significant growth in the popularity of smartphones and the number of available mobile applications, the amount of threats that harm users or compromise their privacy has dramatically increased. The mobile security research community constantly uncovers new threats and develops associated mitigations. Recently, there is an increasing interest in the human factors and various studies investigated user-aspects in the implementation of security mechanisms as well as users' perception of threats. In this paper we present a qualitative study on end-users' knowledge and perceptions of threats and mitigations on mobile devices. Moreover, we identify feelings surrounding smartphone security and privacy. We interpret these feelings in the context of basic psychological need fulfillment. Our findings suggest that so-far little considered aspects of why end-users do not utilize mitigations reside in the need fulfillment plane, and not only in the conflict of usability and security. Following these findings we give examples of how developers of mitigations could ensure that these mitigations are actually adopted by end-users.**

Keywords: Usable Security, Security Analysis, Mitigation Design

I. Introduction

Smartphones have become full-fledged computers offering a diverse set of functionalities. They provide countless applications that allow access to personal and/or business information as well as services, regardless of the user's location. This set of functionality certainly is one of the reasons for the significant growth in the popularity of smartphones. These changes also affected the impact of security and privacy issues, and how they have to be approached.

It used to be an issue for carriers and suppliers to implement mitigations to security challenges. These were bound to in-depth protocol issues and insecure operating systems. Mitigations were approached by adjusting the protocol stack [1] or implementing security mechanisms in new revisions of phones. The rise of smartphones with their vast third party application markets and novel ways to connect and share data changed this situation. The end-users' behavior gained a measurable influence on the effective security and privacy of their data [2].

This led to the current situation in which we see intense research on new attacks and mitigations. At the same time, usability experts' interest in the ease of use and efficiency of proposed mitigations rises [3], [4], [5]. Most work focuses either on permission-related threats [2], the perception of security and privacy on smartphones in general [6], [7] or the perception of single security mechanisms such as password locking [5]. However, still little is known about the approaches users take in general to mitigate risks on smartphones.

Therefor we decided to use an explorative approach in form of a qualitative user-study to investigate this matter. Explorative studies serve the purpose of "discovering important categories of meaning" and of "generating hypotheses for further research" [28]. They can later serve as a basis for conducting quantitative studies such as large scale online surveys which are often conducted in usable security research.

We first conducted a literature survey to establish the state of the art concerning user-factors regarding threats and mitigations on mobile platforms. We then designed a qualitative user-study to uncover which of the previously identified threats and mitigation techniques are known to users, and how they are perceived by them. After formalizing these responses we provide examples for designing mitigations, and which new paths have to be taken to effectively preserve end-users' security and privacy.

Contributions:

- We explore end-users' perspective on threats and mitigations in a qualitative study.
- We present insights in the emotional dimension of the end-users' role in security and privacy on mobile devices.
- Based on our results we identify a set of design examples for the implementation of security mechanisms.
- The obtained data-set allows for further cross-comparison of the discovered results among cultural spheres in subsequent studies.

Structure: In Section II we provide a summary of the necessary background. Section III details our research methodology and the study we conducted. We present our results in Section IV and discuss them in Section V. This section also holds our analysis on the implications of our results for general mitigation design. We then proceed by comparing the related work in Section VI and conclude in Section VII.

II. Background

To provide a sufficient foundation for our user study, we surveyed existing work on threats, assets and mitigations for mobile systems. The literature indicates three mayor assets on mobile devices from the end-users' perspective: The device itself, it's resources and the data on it (cf. e.g. [6] [8]). In addition, we identified various groups of threats and associated mitigations. The following literature review serves as the foundation for the subsequent analysis of our results.

A. Device Loss or Theft

a) Threats: Losing access to a mobile device may be the most apparent and natural threat. The specific associated issues include the plain loss of hardware due to theft or breakage, or malicious applications locking or even bricking, i.e. permanently rendering unusable, the device [9]. These issues also extend to the data on the device, as the loss may also lead to unwanted data disclosure [10]. In all cases the data on the device usually becomes inaccessible as well.

b) Concerns: Following this, users' concerns mainly revolve around losing or permanently bricking a device [8], [2], [6], [5]. The loss of data is considered similarly distressing [7], [6] with Felt et al. finding that the loss of contacts is considered more severe in comparison to losing other data on a phone [2].

c) Mitigations: The most useful technique for retaining a lost or stolen device is an integrated device locator [11]. Data disclosure can be prevented by password locking and device encryption [9], [10], [11] or remotely wiping the device [10], [11]. Perez et al. furthermore suggested a framework for preventing data leakage, which also covers these points [12]. As for the inaccessibility of data, backups are the only reasonable mitigation [10].

B. Resource Drainage and Service Abuse

a) Threats: Resource drainage and abuse is a long-since known concept, also outside the mobile platform. While the abuse of phone-resources mostly results in non-critical issues like battery drainage [13], a severe threat is posed by more financially inclined malware. Dialerware [10], premium SMS [14] and other financial malware are all just instance of the general threat class of abusing costly services or functions [9].

b) Concerns: While users are, in general, concerned about their signal strength and battery lifetime [6], the study of Felt et al. found that these are seen less critical by users. However, concerns regarding the abuse of costly services and directly inflicting monetary damage, were conceived as most critical directly after physically losing a device [2].

c) Mitigations: While modern separation techniques, such as multi-compartment environments, may provide some protection against attacks in general, first attacks against them have surfaced [15]. Hence, monitoring resource usage is still one of the most promising approaches [9], [10]. One notable work in this area is TaintDroid of Enck et al. [16], aimed at providing real-time privacy monitoring for Android devices. Performance related resource consumption has also been addressed by researchers, introducing more fine-grained controls [17]. For some services, disabling the abusable billing features may also be an option [10]. Anti-Malware software can also be applied in order to detect malicious applications that are abusing costly services and features [9].

C. Network Attacks

a) Threats: Network level attacks include attacks on the phone network [1] as well as attacks on the various forms of Internet connectivity that modern smartphones employ. These include maliciously spoofed network names, that prompt users to connect [10] and the usually ensuing activities of modifying, reading or blocking the devices communications [9], [18].

b) Concerns: While technically rather possible [19], network level attacks are not considered a high-level threat following research by Felt et al. as well as Chin et al. [2], [6]. Chin et al. specifically see that more security aware participants have a higher concern for this kind of attacks, while they still conclude that the associated fears usually stem from a misunderstanding of how wireless networks [6] work.

c) Mitigations: Mitigation of these kinds of attacks is rather straightforward. In addition to exercising caution on which networks to connect to and disabling auto-connect features [10], transport layer encryption mostly solves this issue [9], [10]. Additionally, full End-to-End encryption will even mitigate attacks via a service provider [9].

D. Privacy Invasion

a) Threats: The general class of profiling, tracking, surveillance, spyware and further privacy invading threats has been investigated by various researchers [9], [10], [18]. Specifically, applications may abuse their permissions to gather information about users, and exfiltrate that data for various purposes [3], [20]. Employing further techniques for advertisement companies to track their users has also been the matter of research in the literature [21].

b) Concerns: While Chin et al. found a rather widespread trust in applications properly handling users' data [6], Felt et al. found that users are still concerned about these issues [2]. Especially sharing of private information with advertisers is considered a pressing concern [2]. Covert recordings are not considered a high-level threat, even though such attacks are rather possible [2], [20]. Especially in the light of recent revelations around SmartTV's (e.g. [22]) and the by now omnipresent Snowden-Effect [23], [24] we predict changes in these results for the future.

c) Mitigations: It can generally be considered good practice to check the reputation of apps and services one wishes to use, and only install these from well-known sources [10]. While various researchers point out that the requested permissions of an application should be carefully examined [9], [10], [11], research shows that this is not done in practice [20] [11]. Analyzing [25] and tracking [26] the data-flow on devices is neither a scalable nor user-friendly approach. A full-fledged solution to these issues remains to be found.

III. Methodology

This section describes how our study was set up and how the obtained data was analyzed. As not much holistic work regarding user views on threats and mitigations on mobile platforms has been conducted so far, we decided for an exploratory study in form of focus groups. The aim of the study was to identify end-users knowledge on and views of threats and mitigations.

A. Design

Our qualitative study follows a phenomenological approach which assumes that participants' knowledge is represented through conscious experience [27]. By discussing about a certain topic, participants reveal their knowledge and views on the topic. Compared to individual interviews, we suspect the focus group approach to foster discussion and reveal details on the topic, as participants' opinions might in many cases only partially overlap or not overlap at all. Moreover, focus groups still offer additional advantages, for instance, they enable the collection of a lot of data in a short time and allow for immediate follow up and clarification [28].

Additionally, in contrast to quantitative techniques, focus-groups do not require in-depth a-priori knowledge on the subjects' terminology. While such a study will provide further insights into the subject matter, it requires information that can only be gathered by a pre-examination like the one we present in this paper [29]. As we wanted the threat and mitigation space to unfold as wide as possible, we organized the focus groups as brainstorming sessions. The goal of brainstorming is to collect as many ideas as possible without judging them regarding their content and usefulness.
We defined three general questions and one wording question to be discussed during the focus groups:

- Which advantages do smartphones offer?
- Which disadvantages result from the advantages? (potential threats)
- How would you call the disadvantages? Are they threats, dangers, negative consequences or maybe something completely different? (wording question)
- What can users do to protect themselves from the disadvantages? (potential mitigations)

We opted to limit our direct questions to advantages, disadvantages and protection methods, as we did not want to bias participants in the direction of risk management. To ensure that we can regard the disadvantages as potential threats the wording question was included. Also the impersonal nature of the questions was supposed to help to avoid situations where participants may feel uncomfortable, as they are forced to report on individual sensitive topics to other participants whom they do not know.

Following Morse [30] and Sandelowski [31] who suggest a sample size of six participants as sufficiently high for a phenomenological study, we opted to use two groups of six participants. We will refer to the two groups as FG1 and FG2 in the remainder of the document. Participants were recruited via a dedicated portal provided by our institution, and received monetary compensation of approximately 10USD per hour. To avoid priming and self-selection of security savvy participants, the focus of the study was not revealed during the recruitment process. We therefor advertised the study as a study on advantages and disadvantages of smartphones. The discussion during the focus group session was supposed to have a 60-90 minutes duration.

B. Participants

Participants were sampled to roughly reflect the average smartphone user distribution in Germany. Both focus groups included participants above and under the age of 35, of various educational backgrounds. More female than male participants (ratio: 4:2) were observed. Furthermore, there was a majority of Android users, which is reasonable due to the high market share of this operating system [32].

FG2 was heterogeneous regarding demographics, smartphone usage and professional IT experience. However, FG1 participants owned their smartphone longer, used it more often and downloaded apps more often compared to FG2. In general, FG1 was more homogeneous compared to FG2. Therefore, FG1 could be described as a group of experienced and active lay-users. For FG2 it does not make sense to describe the participants as a group as they were too diverse in their characteristics. Figure 1 depicts the demographic characteristics of the participants.

C. Procedure

In the following the procedure of the study is explained. Both FGs were conducted according to the same procedure but by different teams of moderators.

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

The moderator's task was

- to lead the discussion neutrally along the four questions of interest
- to foster the discussion
- to play back the raised ideas to the participants in order to get deeper explanations

The co-moderator visualized the ideas that came up during the discussion by writing them onto sticky notes and placing them on the board. The visualization was meant to help participants to reflect on the ideas and to come up with new ideas.

The moderator started the discussion by welcoming the participants, explaining the study method and motivating the participants to freely speak out every idea. After the first

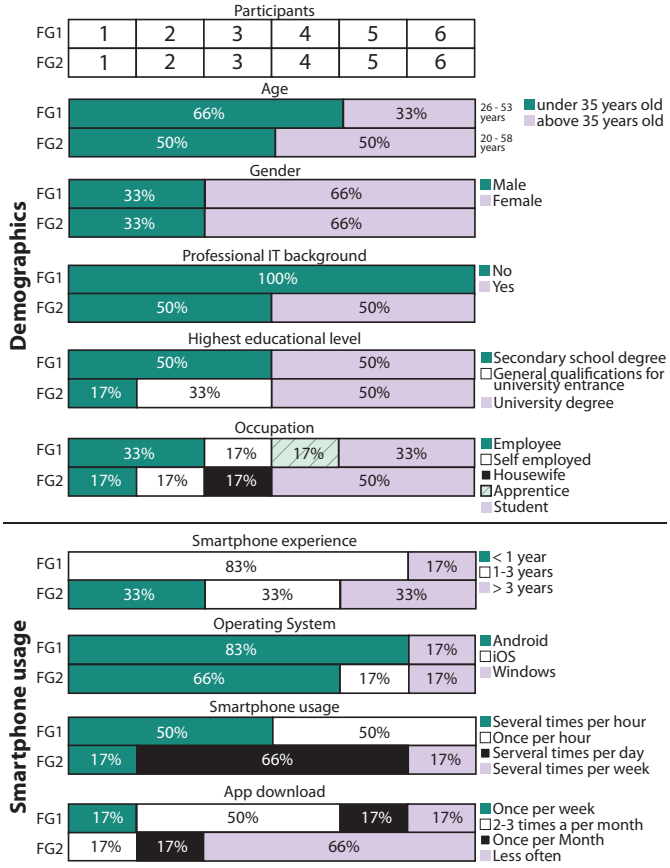

Fig. 1. Overview of the demographic distribution and experience with smartphones for the participants in the two focusgroups.

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

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

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

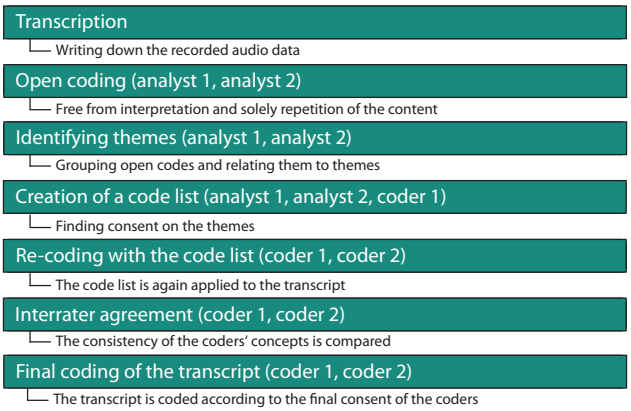

Fig. 2. Visual representation of the employed coding process.

D. Analysis

Before analysis the audio recordings were transcribed in whole whereby participants' names were replaced with pseudonyms. We employed the following analysis procedure. First, an open-coding annotation was performed on the transcripts by two analysts independently from each other. Second, the analysts used the data from the first step identify themes, again independently from each other. After the second step, the analysts and the first coder met to find consent on the themes and to create a codelist (containing the themes). We decided against imposing themes which were found during the analysis of related work, but instead to stay open to what is grounded in the data. Therefore, we used tools and principles from Grounded Theory [33] such as questioning, looking at language, emotions and words indicating time. The data was then coded by the first coder and a second independent coder to increase the validity of the results.

Figure 2 details the full analysis pipeline for our data for both FGs.

We analyzed the data obtained from FG1 and FG2 as outlined before. The interrater agreement was determined as moderate according to Landis and Koch [34] (Cohen's kappa of 0.44 for FG1 and 0.45 for FG2). Deeper analysis revealed that the disagreements between the coders stemmed from what should be considered an "empty" statement and what could be considered "other disadvantages". While the first is the notion of what is a non-meaningful utterance by a participant, the second relates to information on disadvantages of smartphones that are neither security nor privacy related. An example for the latter would be a statement on modern smartphones being so large that they constantly destroy one's pockets. Therefore, it appears that the theme other disadvantages in FG1 was not meaningful enough and should have been split into subthemes such as health issues and disadvantages not related to security or privacy. In FG2 the discussion went not as fluently as in FG1. Sometimes only buzz words were thrown into the discussion or short discussions which went

away from the topic in general appeared. This made it difficult for the coders of FG2 to decide which of the short statements should be included and which are indeed lacking in content. Therefore, the coders met once more to discuss the points of disagreement. This ensured that they did not miss to code any important statement and lead to consent on the coding of the transcript. In the following we use the version of the transcripts upon which the coders finally agreed.

IV. Results

In this section we will report the potential threats and mitigations which were named during the discussions. We will not detail the results of the "advantages" part of the discussion, as smartphone assets have been sufficiently discussed in the literature. Not surprisingly, as a result of the almost completely open discussion the evolving themes differed from the four categories defined in Section II. To compare all potential threats and mitigations that were raised in the focus groups with those that were elaborated in Section II, we first summarize them according to the structure of Section II. Later on, we will report in a qualitative way, on how they were perceived by the users.

A. Device Loss or Theft

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

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

B. Resource Drainage and Service Abuse

a) Threats: Whereas FG2 discussed *financial loss* and *limited battery lifetime*, the topic of resource drainage was not mentioned in FG1 at all.

b) Mitigations: FG2 disregarded mitigations against resource drainage and service abuse. Only one participant addressed the topic at all, expressed through a fatalist view: *"Yes, but you should be happy that it [the battery] even lasts that long, because, well, [pause], one has to, you have to consider, what the device is doing for you or what it can do in general [...]"* One mitigation which can be classified according to this structure was nevertheless mentioned in FG1, namely the usage of *Antivirus* applications.

C. Network Attacks

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

b) Mitigations: As mitigations, both FGs came up with *end-to-end encryption*. FG1 additionally named several mitigations such as to *switch off the data connections*, *to delete the SSIDs of untrusted WLAN networks* or to apply a *Firewall*.

D. Privacy Invasion

Privacy Invasions were discussed in most detail among all other topics in both focus groups.

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

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

Subsection	Theme	Present in	
		FG1	FG2
Social Pressure	Peer pressure	✓	×
	"Social" Availability	✓	✓
	Harassment	×	✓
Distrust vs. Trust	Dwindling Trust	✓	×
	Trust	✓	×
Dependence, Helplessness and Fatalism	Dependence	✓	✓
	Helplessness	✓	✓
	Fatalism	✓	✓
	Sacrificing Security for Usage	✓	×
Exercising one's own influence	Inform One-self	✓	×
	Exercising Control	✓	×
	Risk Assesment (own responsibility)	×	✓
	Avoidance	✓	✓
Processes	From technological side-effects to dangers	✓	×
	Risk assessment (trade-off)	×	✓

TABLE I
AN OVERVIEW OF THE DISCOVERED THEMES RELATED TO EMOTIONAL VIEWS IN THE TWO FOCUS GROUPS.

E. Feelings related to potential threats and mitigations

Participants not only brainstormed about potential threats and mitigations, but also revealed their views on those. In this section we describe these views in a qualitative way. Interestingly, the discussion in both FGs revealed many oppositional views. The themes related to feelings which were identified by the coders are summarized in Table I.

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

a) Social pressure: When talking about potential threats, the issue of *social pressure* was raised in both FGs. Even though users interact individually with their device, the participants mentioned social pressure related to the usage of smartphones. As an example for the influence of others, *peer pressure* regarding the adoption of applications which are considered unsecure was mentioned.

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

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

> *FG1-P1: "It's being expected that you are available at all times."*
>
> *FG2-P4: "Constant availability."*
>
> *FG1-P4: "Like surveillance. So if the others [colleagues]definitely saw that one's been online, I can't tell my boss 'Oh, I'm sorry I didn't see that you wanted me to help out.' "*
>
> *FG1-P5: "Mistakes could have been made by everybody, but nowadays it's so obvious. Mistakes are getting immediately discovered."*

In FG2 the topic of harassment by advertisers was raised:

> *FG2-P5: " [...]they later said: We will call you until you take part in the survey."*
>
> *FG1-P1: "[...]and occasionally they render the whole website as an ad. [...]Therefore, you don't have the chance to continue on what you wanted to do, but you need to give attention to the whole thing. [...]"*

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

> *FG1-P3: "It was always getting worse, that really every app wanted to access everything. So, four years ago, the first apps [...]weren't like this that they wanted to know everything."*
>
> *FG1-P2: "Well, when it comes to emails, in the past one could get an e-mail address for oneself and nobody knew to whom this address belonged to. But if you nowadays retrieve your emails on your mobile you are immediately identifiable."*

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

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

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

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

c) Dependency, helplessness and fatalism: Several other notions of negative feelings regarding potential threats and mitigations evolved during the discussion. All these notions relate to either *dependency*, *helplessness* or *fatalism*.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Some of the participants in FG1 raised the need to *sacrifice security* in order to use applications or services in the way they want to. Differently to the *trade-off* which we will define under the "Processes" paragraph, we consider "Sacrifice security for usage" as a feeling of having no choice.

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

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

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

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

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

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

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

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

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

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

e) Processes: Both focus groups came up with the view that there exist processes in handling security and privacy. FG1 saw *threats developing* in a process instead of being staticly. Thus, threats cannot be sticked to single usage occasions and they develop either as a consequence of user behaviour or technology misuse. FG2 noted that security and privacy are subject to a *trade-off* between benefits and risks. Whereas the theme "sacrificing security for usage" referes to the feeling of not having a choice, this theme refers to the feeling that

one has at least the choice not to use an app or service if one wants to achieve security.

> *FG1-P5: "It depends on how far you go. That's what we said. So the more you reveal, the more you have to anticipate that you will eventually lose."*
>
> *FG1-P3: "I think that is too undifferentiated, because some things are technological necessities that I am subject to, so that I can use the device at all, and some things are side effects that arise, because others misuse these technological necessities."*
>
> *FG2-P2: "But that, umm, that one can... No, because then you cannot use the service. It is about that: Do you want to use the service? Then you have to accept that."*
>
> *FG2-P4: "Simply raise sensitivity, that it is really your responsibility... [pause]So to speak, take responsibility for that, what, which data you really share and what not."*

V. Discussion

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

During brainstorming on disadvantages and protections, the users revealed diverse views on topics related with positive and negative feelings. Most of these views were observed independently in both focus groups. The finding of feelings in users' views is not too surprising, as human thinking and judgement is in general influenced by emotions, even the judgements that are considered rational (cf. e.g. [35]).

However, the implications which these feelings have with regard to risk management on smartphones is an issue worth exploring.

The issues of distrust and trust, respectively, have been investigated in several works. Mylonas et al. found in a survey with more than 400 participants that users who trust their app repository tend to be less likely to use smartphone security software [11]. The same was found about paying attention to security warnings. In a study with more then 350 users, Han et al. found that trust in third-party security apps positively influences the adoption of these kind of apps [36]. Conversely, in the same study, trust in the smartphone operating system showed to be a negative influencing factor for the adoption of third-party security apps.

In our study, also issues of social pressure were revealed. In the research on technology adoption, social influence often shows to be an influencing factor for adoption. An example of this can be found in the UTAUT model presented in [37].

For social pressure and the remaining views we also see a common ground for how they can be interpreted: basic psychological needs. Sheldon et al. rank 10 basic psychological needs from the psychology literature [38]. They find that autonomy, competence, relatedness and self-esteem were the four most important needs, defined as follows [38]:

- ***Autonomy / Independence:*** *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 / Effectance:*** *Feeling that you are very capable and effective in your actions rather than feeling incompetent or ineffective.*
- ***Relatedness / Belongingness:*** *Feeling that you have regular intimate contact with people who care about you rather than feeling lonely and uncared for.*
- ***Self-esteem / Self-respect:*** *Feeling that you are a worthy person who is as good as anyone else rather than feeling like a "loser."*

Usage of smartphones allows people to stay connected with others and thus to support their need for relatedness. However, these positive features can become threats to autonomy, when the technology is used by others to put pressure on the user. The concept of social pressure could therefore be interpreted as a trade-off between the need for relatedness and the need for autonomy. Also, smartphones offer many features that enable users to manipulate their environment. These features can support the feeling of autonomy, competence and self-esteem. A good usability of applications or the system itself may help to support these feelings. On the other hand, under certain circumstances, usage of smartphones may evoke negative feelings such as dependency, helplessness and fatalism. These feelings are antonyms of autonomy and competence. Therefore, the circumstances which evoke these feelings could be considered threats to the related basic needs.

When we began with the work of this paper we defined assets, threats and mitigations with the help of the related literature on mobile security and privacy. We considered the assets of smartphone users as the device itself, the resources of the device and the data on the device. However, the qualitative data in this study suggests, that individual risk assessment is multifaceted and not necessarily only guided by a rational risk assessment approach.

A. Psychological Threats and Mitigations

If we consider psychological needs as (additional) assets, we can perform a classical threat analysis on them.

Social Pressure

Threat: Social Pressure, i.e. the combined feeling of being forced to perform an action due to the general behavior of the peer-group.

Mitigation: We suspect that security and privacy by default can help to suppress feelings of social pressure. Applications which support the relatedness of people should apply this principle. For example, if end-to-end encryption would be a standard, users would not be forced to choose between messenger apps which are secure and have a smaller market share and applications which are widespread and do not feature security. The threat of "social availability" could be mitigated

by offering proper privacy settings in apps which support social interaction. This is already done in many of these apps, but it is not a general standard or best practice.

Negative Feelings

Threat: Negative feelings perceived by a user. This includes a feeling of dependency, general helplessness and fatalism.

Mitigation: As the mentioned feelings are antonyms of autonomy and competence, we suggest to mitigate this threat by applying proper usability engineering techniques during the design of security and privacy mechanisms. This concept is of course not new and has been discussed intensively in the literature [39]. We additionally suggest to extend the usable security approach to an approach where user experience and need fulfillment is taken into account. Smartphone security mechanisms need to ensure not only usability, but they also need to convey positive feelings if they should reach higher acceptability by lay users.

The idea of need fulfillment is already applied in user experience research [40]. Therefore, we think that a transition of this idea to the domain of security and privacy should be easily applicable. Our results also suggest that there are users who find themselves capable of exercising their own influence regarding issues of smartphone security and privacy. Factors supporting this view and verification of the effectivness of actions as perceived by those users are subject to future research.

Unmerited Trust

Threat: Unmerited trust occurs when a user trusts an insecure or privacy-intrusive systems to preserve those classical security assets it intentionally violates. The results of our work and other works suggests that users may be led in some cases by misconceptions regarding security and privacy. Trust might be used as a shortcut for security and privacy without verifying the actual extent of these features.

Mitigation: User education and awareness might help to mitigate this threat. Tools for user education such as anti-phishing education apps exist [41].

By interpreting the identified negative feelings as additional threats to assets residing in the psychological need plane, we can relate them back to security and privacy technologies. Even though they are not directly related to security and privacy, they could be rather interpreted as second order threats which might influence security and privacy. They can be either mitigated by security and privacy mechanisms or they can hinder them or their adoption if the mitigations are in conflict with the basic psychological needs.

B. Limitations

Our sample size of twelve participants is considered sufficient for a phenomenological approach in the literature [30], [31] and the overlap in the results of the two focus groups demonstrates reasonable validity of our results. A quantitative approach would be more general, yet should be constructed utilizing a pre-existing explorative dataset for the research matter at hand. Such a dataset was, so far, unavailable and is first provided by us. Additionally, due to the available population, statements provided in this document had to be translated. The analysis was performed on the un-translated dataset by native speakers. This, however, provides also the advantage that further works can investigate the inter-cultural differences in perception of security and privacy on the mobile platform, among end-users.

Furthermore, due to the qualitative approach using focus groups, a collective set of knowledge was measured, which can not be attributed to an *individual* participant. This approach aims at providing an explorative and qualitative dataset, as a foundation for further generalizing quantitative research. As we aimed at uncovering known terminology in the field of mobile security that can be expected from users for further studies, we leave the matter of ranking users' perception and connection of these to those further studies. Therefore, we consider the disadvantages as potential threats, as they might, depending on the situation and the intrinsic characteristic of a user become threats.

VI. Related Work

The security and privacy concerns of end-users and their use of mitigation strategies has only recently become a wider research interest. Muslukhov et al. performed interviews investigating the data assets users store on their phones and how they protect them [8]. Felt et al. focused on users' concerns related to the threat of abusing access rights (permissions) by malicious applications [2]. General perception of and concerns related to security and privacy on smartphones was discussed in several works [6], [7].

Chin et al. found users to be more concerned regarding their privacy on their phones compared to their laptops and less willing to perform sensitive tasks on their smartphone compared to their laptops [6]. Other studies found that users are mainly concerned about permanent loss of their phone [6], [8]. Similarly unauthorized access to their phone [6], [8], as well as unauthorized access to data by insiders such as friends [42], were considered sever threats. Studies related to the usage and perception of smartphone security mechanisms can be found in [6], [8], [11]. Harbach et al. as well as Ben-Asher et al. specifically investigated the perception and usage of different locking mechanisms as a security mechanism [5], [7]. Furthermore, Mylonas et al. conducted a study on which pre-determined mitigations are employed by end-users [11].

Each of these studies specifically focus on a subset of the issue [2], [8], [42], [11], [5] or on general concerns regarding smartphone security and privacy [6], [7]. The work of Mylonas et al. [11] does not stick to a specific mitigation instance, and provides only a set of possible mitigations unrelated to threats. Also, some of these works have the limitation, that they pre-determined the sets of threats and mitigations presented to the user. Hence they cannot conclusively determine if those threats and mitigations were actually known to the participants.

Our paper aims to fill this gap by exploring users' actual terminological knowledge and perception of smartphone threats and mitigations. Only if users know threats and mitigations, they are able to protect their assets. However, knowledge is not the only factor influencing adoption. Users might be influenced by non-rational factors, as it has been demonstrated. It is subject to future research to fully quantify these results.

Furthermore, especially the terminology is important for the design of quantitative studies utilizing questionnaires. Differing notions and terminology between researchers, engineers and users do not only pose a basic issue for security mechanisms [43], [44], they furthermore can lead to falsified data. If a users does not recognize the meaning of a question due to issues with the used terminology, although the user is familiar with the concept, the data gathered from that questionnaire does not reflect the users' actual knowledge [29].

VII. Conclusion

To our best knowledge, we are the first to provide qualitative data on users' general knowledge and feelings regarding risk mitigation on mobile devices. We identify positive and negative feelings related to threats and mitigations on smartphones. The findings were interpreted under the light of Sheldon et al.'s work on psychological needs and suggest that feelings are related to need fulfillment or a lack thereof.

Following our findings, we give examples on how these feelings could be stimulated (for the positive ones) or avoided (for the negative ones) by security and privacy mechanisms. We suggest that researchers should focus on security-by-default mechanisms. This could limit inhibiting factors induced by possible social pressure. Such methods should also be configured in a simple manner, so the self-respect of less technical users does not prevent their adoption of the technology. Concerning the found fatalism it is important to convey positive feelings towards users, demonstrating that preserving one's security and privacy is an achievable goal.

Similarly, connecting mitigations with an achievement of fulfillment is recommendable. An example for this would be automatically rewarding a user's good-practice and adoption of security mechanisms with bonus points in a personal high-score system. Additional empirical research should focus on how a feeling of achievement can be established in end-users, if they adapt or execute a security-mechanism. Also, a large-scale study on the subject matter will certainly provide further insights.

VIII. Acknowledgments

This work was partly funded by the EU FP-7 support action ATTPS under grant agreement no. 317665. We would like to thank the students that assisted us in data collection. These are: Robin Zeiner, Henny Straßas, Michael Kürbis, Ronan Verheggen and Robert Schmidt. Furthermore, we would like to express our gratitude to the anonymous peer reviewers for their insightful comments on the paper.

References

[1] N. Golde, K. Redon, and J.-P. Seifert, "Let me answer that for you: Exploiting broadcast information in cellular networks," in *Proceedings of the 22nd USENIX conference on Security*. USENIX Association, 2013, pp. 33–48.

[2] A. P. Felt, S. Egelman, and D. Wagner, "I've got 99 problems, but vibration ain't one: a survey of smartphone users' concerns," in *Proceedings of the second ACM workshop on Security and privacy in smartphones and mobile devices*. ACM, 2012, pp. 33–44.

[3] A. P. Felt, E. Chin, S. Hanna, D. Song, and D. Wagner, "Android permissions demystified," in *Proceedings of the 18th ACM conference on Computer and communications security*. ACM, 2011, pp. 627–638.

[4] A. P. Felt, S. Egelman, M. Finifter, D. Akhawe, D. Wagner *et al.*, "How to ask for permission." in *HotSec*, 2012.

[5] M. Harbach, E. von Zezschwitz, A. Fichtner, A. De Luca, and M. Smith, "Itsa hard lock life: A field study of smartphone (un) locking behavior and risk perception," in *Symposium on Usable Privacy and Security (SOUPS)*, 2014.

[6] E. Chin, A. P. Felt, V. Sekar, and D. Wagner, "Measuring user confidence in smartphone security and privacy," in *Proceedings of the Eighth Symposium on Usable Privacy and Security*. ACM, 2012, p. 1.

[7] N. Ben-Asher, N. Kirschnick, H. Sieger, J. Meyer, A. Ben-Oved, and S. Möller, "On the need for different security methods on mobile phones," in *Proceedings of the 13th International Conference on Human Computer Interaction with Mobile Devices and Services*. ACM, 2011, pp. 465–473.

[8] I. Muslukhov, Y. Boshmaf, C. Kuo, J. Lester, and K. Beznosov, "Understanding users' requirements for data protection in smartphones," in *Data Engineering Workshops (ICDEW), 2012 IEEE 28th International Conference on*. IEEE, 2012, pp. 228–235.

[9] A. Shabtai, Y. Fledel, U. Kanonov, Y. Elovici, and S. Dolev, "Google android: A state-of-the-art review of security mechanisms," *arXiv preprint arXiv:0912.5101*, 2009.

[10] G. Hogben and M. Dekker, "Smartphones: Information security risks, opportunities and recommendations for users," *European Network and Information Security Agency*, vol. 710, no. 01, 2010.

[11] A. Mylonas, A. Kastania, and D. Gritzalis, "Delegate the smartphone user? security awareness in smartphone platforms," *Computers & Security*, vol. 34, pp. 47–66, 2013.

[12] C. Perez, B. Birregah, and M. Lemercier, "The multi-layer imbrication for data leakage prevention from mobile devices," in *Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on*. IEEE, 2012, pp. 813–819.

[13] U. Fiore, F. Palmieri, A. Castiglione, V. Loia, and A. De Santis, "Multimedia-based battery drain attacks for android devices," in *Consumer Communications and Networking Conference (CCNC), 2014 IEEE 11th*. IEEE, 2014, pp. 145–150.

[14] A. P. Felt, M. Finifter, E. Chin, S. Hanna, and D. Wagner, "A survey of mobile malware in the wild," in *Proceedings of the 1st ACM workshop on Security and privacy in smartphones and mobile devices*. ACM, 2011, pp. 3–14.

[15] T. Fiebig, J. Krissler, and R. Hänsch, "Security impact of high resolution smartphone cameras," in *Proceedings of the 8th USENIX conference on Offensive Technologies*. USENIX Association, 2014, pp. 15–15.

[16] W. Enck, P. Gilbert, S. Han, V. Tendulkar, B.-G. Chun, L. P. Cox, J. Jung, P. McDaniel, and A. N. Sheth, "Taintdroid: an information-flow tracking system for realtime privacy monitoring on smartphones," *ACM Transactions on Computer Systems (TOCS)*, vol. 32, no. 2, p. 5, 2014.

[17] A. Pathak, Y. C. Hu, and M. Zhang, "Where is the energy spent inside my app?: fine grained energy accounting on smartphones with eprof," in *Proceedings of the 7th ACM european conference on Computer Systems*. ACM, 2012, pp. 29–42.

[18] A. Mylonas, M. Theoharidou, and D. Gritzalis, "Assessing privacy risks in android: a user-centric approach," in *Risk Assessment and Risk-Driven Testing*. Springer, 2014, pp. 21–37.

[19] N. Sidiropoulos, M. l Mioduszewski, P. l Oljasz, and E. Schaap, "Open wifi ssid broadcast vulnerability," 2012.

[20] A. P. Felt, E. Ha, S. Egelman, A. Haney, E. Chin, and D. Wagner, "Android permissions: User attention, comprehension, and behavior," in *Proceedings of the Eighth Symposium on Usable Privacy and Security*. ACM, 2012, p. 3.

[21] C. Krum, *Mobile marketing: Finding your customers no matter where they are*. Pearson Education, 2010.

[22] BBC, "Not in front of the telly: Warning over 'listening' tv," Online, 2015, http://www.bbc.com/news/technology-31296188; accessed 21st of January 2015.
[23] S. Landau, "Making sense from snowden," *IEEE Security & Privacy Magazine*, vol. 4, p. 5463, 2013.
[24] G. Greenwald, *No place to hide: Edward Snowden, the NSA, and the US surveillance state*. Metropolitan Books, 2014.
[25] Z. Yang, M. Yang, Y. Zhang, G. Gu, P. Ning, and X. S. Wang, "Appintent: Analyzing sensitive data transmission in android for privacy leakage detection," in *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*. ACM, 2013, pp. 1043–1054.
[26] B. Gu, X. Li, G. Li, A. C. Champion, Z. Chen, F. Qin, and D. Xuan, "D2taint: Differentiated and dynamic information flow tracking on smartphones for numerous data sources," in *INFOCOM, 2013 Proceedings IEEE*. IEEE, 2013, pp. 791–799.
[27] B. J. Calder, "Focus groups and the nature of qualitative marketing research," *Journal of Marketing research*, pp. 353–364, 1977.
[28] C. Marshall and G. B. Rossman, *Designing qualitative research*. Sage publications, 2010.
[29] J. Rattray and M. C. Jones, "Essential elements of questionnaire design and development," *Journal of clinical nursing*, vol. 16, no. 2, pp. 234–243, 2007.
[30] J. M. Morse, "Designing funded qualitative research." 1994.
[31] M. Sandelowski, "Sample size in qualitative research," *Research in nursing & health*, vol. 18, no. 2, pp. 179–183, 1995.
[32] S. Brown, "Android is poised to takeover the smartphone market in 4 years," *Science*, 2014.
[33] J. Corbin and A. Strauss, *Basics of qualitative research: Techniques and procedures for developing grounded theory*. Sage publications, 2014.
[34] J. R. Landis and G. G. Koch, "The measurement of observer agreement for categorical data," *biometrics*, pp. 159–174, 1977.
[35] D. Kahneman, *Thinking, fast and slow*. Macmillan, 2011.
[36] B. Han, A. Wu, and J. Windsor, "Users adoption of free third-party security apps," *Journal of Computer Information Systems*, vol. 54, no. 3, pp. 77–86, 2014.
[37] V. Venkatesh, M. G. Morris, G. B. Davis, and F. D. Davis, "User acceptance of information technology: Toward a unified view," *MIS quarterly*, pp. 425–478, 2003.
[38] K. M. Sheldon, A. J. Elliot, Y. Kim, and T. Kasser, "What is satisfying about satisfying events? testing 10 candidate psychological needs." *Journal of personality and social psychology*, vol. 80, no. 2, p. 325, 2001.
[39] L. F. Cranor and S. Garfinkel, *Security and usability: designing secure systems that people can use*. " O'Reilly Media, Inc.", 2005.
[40] M. Hassenzahl, S. Diefenbach, and A. Göritz, "Needs, affect, and interactive products–facets of user experience," *Interacting with computers*, vol. 22, no. 5, pp. 353–362, 2010.
[41] G. Canova, M. Volkamer, C. Bergmann, and R. Borza, "Nophish: An anti-phishing education app," in *Security and Trust Management*. Springer, 2014, pp. 188–192.
[42] I. Muslukhov, Y. Boshmaf, C. Kuo, J. Lester, and K. Beznosov, "Know your enemy: the risk of unauthorized access in smartphones by insiders," in *Proceedings of the 15th international conference on Human-computer interaction with mobile devices and services*. ACM, 2013, pp. 271–280.
[43] A. Whitten and J. D. Tygar, "Why johnny can't encrypt: A usability evaluation of pgp 5.0." in *Usenix Security*, vol. 1999, 1999.
[44] V. Roth, T. Straub, and K. Richter, "Security and usability engineering with particular attention to electronic mail," *International journal of human-computer studies*, vol. 63, no. 1, pp. 51–73, 2005.

APPENDIX

A. Ethical Considerations

The user-study was conducted under informed consent. All moderators received a training before conducting the study. The audio-recordings were deleted after the transcription process. All transcribed data has been pseudonymized and is stored separately from the consent forms. Participants were recruited from a panel provided by the research institution.