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

Contents lists available at ScienceDirect

Journal of Information Security and Applications

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

Psychological needs as motivators for security and privacy actions on smartphones

Lydia Kraus*, Ina Wechsung, Sebastian Möller

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

ARTICLE INFO

Article history:

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

ABSTRACT

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

1. Introduction

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

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

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

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

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

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

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

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

A user for instance makes a phone call to experience the feeling of being close to others (thus, the motivation would be the fulfillment of the need *Relatedness*), rather than for the call's sake (example taken from Hassenzahl [14]). Or, a user activates the privacy setting in a messaging app so that the sender of the messages cannot see when a message was read. This avoids the pressure to reply immediately to a message. In this case, the privacy setting is used to fulfill the basic psychological need of *Autonomy*. Psychological need fulfillment is a primary goal which all users have in common, the instantiation of the primary goal - the experience - is however highly context-dependent and subjective [14].

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

2. Related work

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

2.1. Usability and adoption of smartphone security and privacy mechanisms

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

A method to protect a smartphone from unauthorized access and subsequent privacy intrusions or security issues is the deployment of a screen lock together with an authentication method, such as a password or a PIN [4]. However, unlocking a smartphone with an authentication mechanism is time-consuming [23]. In a study of 2011, the PIN was perceived as a reliable method for protecting a mobile phone by only a quarter of users (26%) [15]. Nevertheless, as of 2014, many users are using a PIN or password to protect their device: 66% of users in Germany use a screen lock with a password [24]. A viable alternative to knowledge-based authentication methods are biometric methods such as Touch ID on iPhones and face unlock on Android devices [25]. Biometric methods, however, also rely on PINs or passwords for fallback authentication.

Regarding communication, eavesdropping and interception pose a threat. They can be mitigated by deploying end-to-end encryption of communication (calls and/or messages) [26]. Only recently, Whatsapp, one of the most popular instant messaging services for smartphones, has announced the implementation of end-to-end encryption which is activated by default [27]. However, the usage of instant messaging services is not only accompanied by the risk of being eavesdropped, but also by the risk of privacy intrusions by other users. The latter can be counteracted by appropriate privacy settings. For instance, Rashidi and Vaniea report that many users actively use the privacy settings of Whatsapp - in a survey among Saudi Arab users almost a third of the respondents hid their last seen notice [28].

Another security threat, malware, might be mitigated by antivirus apps which can be easily installed for Android; however, their usefulness is questionable [29]. Likewise, the usage of security software is considered by many users as nonessential [3]. Keeping the device up-to-date is another mitigation strategy against malware. However, in a case study on update installation behavior, many users of an Android app did not immediately install updates - a behavior which may result in security vulnerabilities [30].

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

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

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