Technical Report

Nr. TUD-CS-2015-1211
August 19th, 2015

CASED

An Investigation into the "Other" Barriers to Adoption of Smartphone Security Precautions (Poor Usability being a Given)

Authors
Melanie Volkamer, Karen Renaud, Oksana Kulyk and Sinem Emeröz

An Investigation into the "Other" Barriers to Adoption of Smartphone Security Precautions (Poor Usability being a Given)

Melanie Volkamer[1],[3] and Karen Renaud[2] and Oksana Kulyk[1] and Sinem Emeröz[1]

[1] Technische Universität Darmstadt
{melanie.volkamer,oksana.kulyk}@secuso.org,
emeroez@rbg.informatik.tu-darmstadt.de
[2] University of Glasgow
karen.renaud@glasgow.ac.uk
[3] Karlstad University, Karlstad, Sweden

Abstract

Many people do not deliberately act to protect the data on their Smartphones. The most obvious explanation for a failure to behave securely is that the appropriate mechanisms are unusable. Does this mean usable mechanisms will automatically be adopted? Probably not! Poor usability certainly plays a role, but other factors also contribute to non-adoption of precautionary mechanisms and behaviours. We carried out a series of interviews to determine justifications for non-adoption of security precautions, specifically in the smartphone context, and developed a model of Smartphone precaution non-adoption. The most interesting finding was the fact that the media does not really play the expected role in raising awareness of Smartphone security issues. We propose that future work should investigate the use of media awareness campaigns to address the various identified misconceptions and justifications.

1 Introduction

The usable security field, starting with Whitten and Tygar's seminal paper in 1999 [49], identified poor usability as the primary obstacle preventing the use of email ancryption. Poor usability was subsequently blamed for the low uptake of other security and privacy measures [5,9,25]. Improving usability, on its own, while necessary, might not be sufficient, as highlighted by a number of researchers working in non-smartphone contexts in the last few years [18,20,21,40,41,42].

It is necessary to investigate other justifications for non-adoption in the smartphone context. Only then can we devise acceptable security measures that smartphone owners might be more willing to adopt [45]. We carried out a series of semi-structured interviews to explore possible explanations for each of the

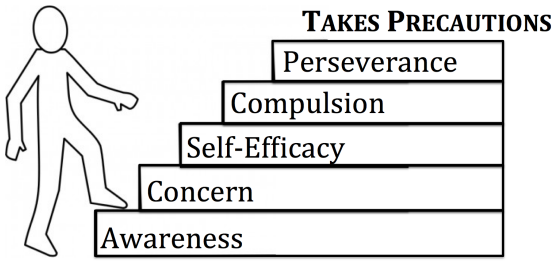

Fig. 1. Progression to Adoption of Smartphone Precautions

meta-categories of non-adoption of smartphone precautions. Based on our analysis we derived a model depicting the progression towards smartphone precaution adoption (Fig. 1). This model serves as basis for future measures as suggested in future work. In summary, this paper's contributions are:

1. Identification of meta-categories of explanations from related literature that could lead to non-adoption of precautionary security and privacy preservation measures (Section 2).
2. Exploration of each of those categories in the *smartphone* context, based on semi-structured interviews (Section 3) — see Fig. 1 (Section 4).

2 Methodology

We conducted a series of semi-structured interviews to investigate justifications for non-adoption, inaction or insecure action. The interviews were conducted either in person or via Skype. On average, an interview took 41 minutes, with the shortest interview taking 26 minutes and the longest 60 minutes. The participants were promised no reimbursement for participation in the study.

2.1 Interview Protocol

The semi-structured interviews comprised four phases which are described in the following paragraphs.

Phase 1: Introduction. Welcome, explain what the study is about, gather demographic data and general information about smartphone experience.

Phase 2: General security threats. Questions were posed to explore their knowledge of smartphone security threats. They were asked which security threats they were aware of, which countermeasures could mitigate, how effective they are, and whether they themselves used them. Non-specific responses were pursued to ensure that we gauged their actual understanding. They were then asked about the possibility that they would become a target. If they perceived the risk

to be high, but did not use any countermeasures, they were asked to elaborate on this. The participants were asked whether they had experienced security problems themselves, and what they perceived the differences between smartphones and computers to be. We also asked what important data was stored on their smartphones, and who, and to which extent, should be responsible for the security of the smartphone.

Phase 3: Specific countermeasures. During this phase the participants were asked about specific practices or tools used to protect sensitive data on smartphones. These were: (1) usage of screen lock, (2) updating the operating system or other software and (3) usage of antivirus software. In each case the participant was asked whether he or she used the tool. If they did not, their reasons were drawn out. If they did, we asked about why they chose to use it, how they personalised it, and if there was some choice, as is the case for antivirus, how they chose which one to use.

Phase 4: Specific threats. During this phase participants were asked about specific threats that could impact the privacy of data stored on smartphones, based upon the guidelines from Federal Office for Information Security[4]. The threats discussed were: (1) the smartphone being lost or stolen, (2) app-related threats, (3) sharing of location-based data, (4) QR codes, (5) links in SMSs, (6) connecting to non-secured WLAN and (7) Bluetooth usage. We wanted to explore awareness of data privacy, the implications of others gaining access to their data and actions they took as precautions. If they took no action we asked questions to help us to understand their reasoning. If they did take action we explored the extent and efficacy of the action.

2.2 Ethics

Ethical requirements for research involving human participants are provided by an ethics commission at the university[5]. Participants were initially told that the study was about smartphone usage. They were not told until after the interview that the research was focused on smartphone security. This was done in order avoid framing responses. Permission was gained to record the interview anonymously. Parents consented on behalf of underage participants.

2.3 Participants

Smartphone owners were recruited via email, according to the snowball principle. A total of 20 participants were recruited, with a perfect gender balance ranging from 12 to 65 years of age, with a mean age of 33.2 years. Five participants were either students, researchers or employers in the field of computer science with the rest having non-technical backgrounds.

[4] `https://www.bsi-fuer-buerger.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Download/Ueberblickspapier_Smartphone_pdf`

[5] Anonymized

2.4 Analysis

We planned to carry out an interpretative phenomenological analysis (IPA) of our interviews. To support this we needed a set of pre-existing themes to drive the initial classification. Researchers have reported a number of non-usability related factors that are likely to hinder the adoption of security and privacy solutions *in other contexts*. For example, end-to-end email encryption [40], web tracking [42], secure passwords [47], anonymizing networks [12], eID [20], compliance with policies in organizations [18,41]. We started off with [40], who attempted to understand non-use of security measures in the email context. The authors identified the following progression to usage: lack of awareness, lack of concern, limited knowledge of threats, not feeling compelled to take action, lack of know-how, and not being side-tracked. We then consulted to other studies to determine whether we ought to extend this list. [42], for example, identified a different set of categories explaining the low uptake of precautions against identification/tracking on the Internet. They suggest that privacy issues do not correlate with identification and tracking issues; lack of awareness of information being transmitted; lack of awareness of how such information can be used to identify/track people, lack of concern about being identified/tracked; lack of awareness of countermeasures; being side-tracked by other motivations. Other studies did not suggest any further categories [2,17,36,45], so we settled on the following five context-neutral categories of reasons for non-use.

(1) Lack of awareness. One reason for poor adoption of privacy and/or security measures is that people lack awareness of the privacy and security threats.

(2) Lack of concern. A number of people are indeed aware of potential privacy and/or security threats but do not take any precautions because they are unconcerned.

(3) Lack of self-efficacy Some people are indeed aware and concerned but lack self-efficacy (not feeling able to protect themselves).

(4) Lack of compulsion. Some people are aware, concerned, and have the requisite self-efficacy but do not feel compelled to act.

(5) Lack of perseverance[6]. Some people are aware, concerned, have the requisite self-efficacy and feel in general compelled to act but they get side-tracked.

3 Results

The interviews were transcribed (some by the authors, some by other members of the research group) to support analysis. Responses were analysed using semi-open coding using the categories enumerated in the previous Section. Two authors independently reviewed the transcripts and assigned explanations to codes

[6] This is the *getting side-tracked* explanation, mentioned by [40] and [42]. We felt that, in order to express this as a deficiency, the use of the term perseverance was more appropriate in this categorisation.

and codes to categories. If several concepts were mentioned, each was coded under the appropriate code/category. The assignments were discussed and agreed upon by the authors.

In the following subsections, we report on whether we found evidence for each category in the smartphone context and provide details about the identified subcategories. Since our analysis was qualitative we do not provide tallies of quotes in each category.

3.1 Lack of Awareness

An essential pre-requisite to adoption of precautionary behaviour is awareness of threats. There is a clear lack of awareness of smartphone-related threats, with participants either completely unaware of threats, or only aware of threats that require physical access to their smartphone. Some study participants, when asked about smartphone-related threats they were aware of were not able to name any, as the following quotes show:

> *"No, I wouldn't know where I could have problems here. There might be something, but nothing comes to mind at the moment"*

We identified the following sub-categories (codes) as possible explanations for why people lack awareness: (a) smartphones are considered to be phones, not computers; and (b) poor media coverage.

It's a Phone, not a Computer. Some participants explained that their smartphone was a *phone* rather than a computer. They had, as a consequence, not made the mental connection to the need for precautions, as the following quotes demonstrate:

> *"Yes, I consider it more of a phone. So, you can make phone calls, write short messages, and it also has the advantage that you can access the Internet. But, yes, it is mostly for communicating, and is not like a laptop, where one works or writes stuff, so, I use it in a different way."*

Poor Media Coverage. Some participants complained that attacks on smartphones did not get as much media coverage as threats to laptops or desktops. Most had heard about malware on PCs, but not on smartphones. Those who had heard of attacks mentioned attacks on corporations and politicians, but not any involving private citizens, as shown in the following quote:

> *"I have heard, or maybe one has heard, on the TV, or has read about, some attacks on companies, some hackers, but I haven't heard that this also happens in private life"*

3.2 Lack of Concern

For awareness to lead to action, there must be a level of concern, a perception of vulnerability. We identified a number of sub-categories (codes), i.e. reasons why people were unconcerned: (a) their own insignificance, (b) low probability of becoming a victim. (c) underestimating security- and privacy-related consequences, (d) some privacy 'violations' being acceptable, (e) that they themselves were not responsible for taking precautions, (f) device loss being more worrying than privacy, These sub-categories are discussed in the following paragraphs.

Their Own Insignificance. Some of participants seemed unconcerned because they believed that they were not important enough to interest attackers, or that they did not have any interesting data on their smartphones that could merit an attack. Examples of relevant quotes are:

> *"Honestly, I personally think that no one would target me, because I believe that I do not have anything important on my smartphone"*

Low Probability of Becoming a Victim. Some responses indicated that the participants underestimated their vulnerability: the probability that they would fall victim to attacks. This underestimation led to their not behaving securely and not using privacy-protecting tools, as these quotes show:

> *"I simply believe that out of number of internet-banking users, the number of people that have experienced problems is so small that it results in small percentage"*

Underestimating Consequences. Participants who were aware that their data *was* at risk did not seem to anticipate the concrete harm that could result. They were not aware of what attackers could do with their data, which data was of interest (and why) or did not consider the consequences to be particularly serious. Example quotes are:

> *"Honestly, I do not have concerns, because this data may be important for me, mostly personal stuff, but there are no state secrets in my emails, if someone wants to read them or something, he, in my opinion, does not get much from it [..] Therefore I have few worries about the data."*

Some Privacy Violations are Acceptable. The interviews revealed that benefits of behaving securely could potentially be offset for various reasons. Concrete reasons are mentioned in the following quotes:

> *"If it is an app that I absolutely need, then I need to ponder. Then I say, I take it, even though it is not secure."*

Some participants were aware that 'others' could gain access to their sensitive data but they were not concerned because they thought they had nothing to hide, as the following quote shows:

> *"It would not matter to me at all if someone reads along with me. I have nothing to hide, it would not bother me."*

Trust in Someone Else to Take Responsibility. During the interviews participants were specifically asked to name entities which ought to be responsible for smartphone security. Participants named developers, smartphone providers, play stores and state institutions, as being responsible. This suggests that it still does not occur to many users that they have to act deliberately to protect themselves, while they trust someone else to take care of security risks.

> *"Ahm, ok, basically, if there are extreme vulnerabilities, also problems, then I think, it should be regulated legally.[..] that the manufacturers develop the devices in a way that it is not possible."*

In particular, some participants overestimated the level of scrutiny and the success rate of malware checks of either Apple or Google, that the apps offered for download on app stores were supposed to go though. Thus, assuming that no malicious apps could enter the store, they quite reasonably did not take any protective actions themselves. The following quotes confirm this misunderstanding:

> *"So, I hope at least, that they do this [check the apps], that they have some filter criteria, so that they do not sell apps that are dubious, but how well they pay attention to to privacy, I honestly do not know."*

Device Loss is more Worrying Than Privacy. When asked about their concerns with respect to their smartphones, no one mentioned anything about privacy and only a few mentioned security. Instead a number said that the main problem would be losing the device itself, since that would lead to loss of revenue, as confirmed by the following quote:

> *"As long as it is not stolen, I do not worry."*

Some were concerned about the potential loss of valuable data on their smartphones, such as their contacts, photos, music etc (in terms of availability). Example quotes are:

> *"So, honestly, I think for me the device itself is more important, because I think, oh no, it cost so much. I would only think about the data sometime later, and then worry about my contacts and my images."*

Several mentioned an adversary using their smartphone to make calls or send text messages, that also would cost them something as confirmed by the following quote:

"Good, I would immediately lock the card. So that no one can use it. [...] Good, I would also go to the police, but I believe this has nothing to do with it."

3.3 Lack of Self-Efficacy.

Despite recognizing the need to act in order to protect themselves, people can still fail to act, if they do not possess the know-how or self confidence to take action. This leads to their not using necessary measures, or not being able to use them properly and effectively. The following sub-categories were identified: (a) not having come across the applicable security measures, (b) having misplaced faith in efficacy of sub-optimal, ineffective or incomplete solutions, (c) believing that precautions are futile, or (d) lacking the confidence required to start using the measures.

Lack of Knowledge. Some of the participants did not seem to know how to protect themselves, or what actions to take against threats they were aware of. For example, some were unaware of the existence of antivirus software on smartphones, or did not understand the purpose of the app permission screen. Example quotes:

"I do not know how I could protect myself from it."

"I cannot judge at all whether an app is secure or not."

Others complained about the level of pre-existing security-related knowledge that was required:

"I do not find it very obvious, also what they write about security, it is never very clear or understandable for laymen, what is allowed and what is not allowed."

"The problem is, that one does not understand the things that they write there, unless one becomes acquainted with the topic of security, so one could only trust that whatever is written there is secure."

The more advanced measures, such as the option to remotely track the stolen device or wiping data from it, or encryption of the data on smartphone, were hardly ever mentioned, indicating that the majority were unaware of such measures.

Other participants, although clearly aware of the existence of smartphone security threats, demonstrated misconceptions with respect to specific threats, such as using non-secured WLAN as the following quote shows:

"I do not have the feeling that anyone can access my computer or my phone better on non-secured WLAN than on secured."

Misplaced Faith in Efficacy of Solutions. Some participants believed that they already used their smartphones securely, and that they did not require additional measures. For example, they did not use the screen lock since they always had their phone on their person, as the following quote supports:

> *"I have my phone always in my pants pocket, and I believe that no one can easily get it."*

They did not use antivirus software because they believed that their careful usage of their phone (i.e. not installing many apps) prevented them from getting a virus, as the following quotes show:

> *"I consider antivirus software to be important when you download stuff that you might install on your computer or with which you do something. I do not do this on the phone at all. So, I read emails, or read news and go on the internet to look something up, but I never install stuff on my phone. "*

Some of participants believed that since they had not experienced any security issues so far, it meant that their way of using the smartphone must be secure (for example, they had not used any antivirus software so far and nothing bad had happened). Example quotes are:

> *"I did not have any negative experiences on my smartphone, that some trojans or something was installed on smartphones because there were no antivurus. I can't recall reading anything about it. Therefore I didn't consider it to be important."*

Futility of Precautions. Some participants were sceptical about whether the existing precautionary measures were indeed capable of protecting them. These participants were unlikely to use precautions since they did not believe that this would protect them effectively. Example quotes are:

> *"I think that at least these big players [Apple, Google, Windows, Blackberry], or one of them, could attack me if they wanted to."*

Lack of Confidence. For some participants the lack of self-efficacy can be explained by the fact that they did not have the confidence to engage with precautionary tools or measures or even to attempt to use those they were aware of. Their confidence might have been shaken by a prior inability to use software, for example

> [on antivirus] *"I would need to ask someone to download or install it for me."*

> [on switching to some more secure alternative for the app they use] *"Yes, it would be relatively cumbersome to have to familiarize myself with it.*

[..]If it were a lot simpler, it would of course be tempting to do this. It is though still a little bit too much for people that have to become acquainted with it."

3.4 Lack of Compulsion

Some participants, despite being aware of the threats and of the precautionary measures, cited other factors that kept them from adopting those measures. The following sub-categories have been identified: (a) inconvenience, (b) negative past experiences with security measures, (c) financial cost.

Inconvenience. Inconvenience was a strong theme. Many referred to the effort that would be required that would hinder their usage of their smartphone. The most frequent references were to the screen lock. They said they would have to enter the code each time they wanted to use the phone, and this was clearly unpalatable. Example quotes that support this sub category are:

"Because I am irritated that I have to constantly enter this, around 50 times a day."

Sometimes they used a PIN instead of something stronger because the stronger mechanism was too effortful, as this quote indicates:

"I think it is more secure than the PIN, but it is too effortful."

Some did not change their access control secrets regularly even though they were aware of the fact that they ought to do this. They were worried about forgetting but also resented the effort required to think up a new password.

"I can suggest that I would not do it out of a desire for convenience. That is, out of convenience or forgetfulness, that I forget that I have to do this."

"Besides, one has to think of new passwords every time; this is horrible."

Finally, some did not install essential updates to their operating systems even though they knew they should. They cited inconvenience, as the following example quote demonstrates:

"Yes, since I also have to work with the device or use it. It is not so, that complete functions are not available, instead, I can still work with it, and when I have a quiete minute, then I do the update."

Negative Past Experiences. Based on past experience, some participants expressed concerns about existing solutions hindering the functionality of their smartphones, such as a loss of data as a result of an update, or antivirus software making the phone work too slowly. This discouraged or deterred action, despite awareness and concern. Quotes that support this subcategory are:

> *"Antivirus software makes my phone too slow if it runs in the background all the time, therefore I decline to use it."*

Financial Cost. The cost of security- and privacy-protection tools was sometimes an obstacle and deterred action. An example quote is:

> *"There might be some antivirus software that one has to pay for, I leave it alone. If I somehow find free antivirus software, and I read that it delivers value, then I would install it".*

3.5 Lack of Perseverance

We identified the following sub-categories: (a) taking their cues from their friends, and (b) not wanting to be paranoid.

I Trust What My Friends Do. Several participants mentioned relying on the experiences and trusting the recommendations of their peers in making security- and privacy-related decisions. The fact that their peers consider an action safe would presumably make it safe for them too. Example quotes are:

> *"Apps that I have on it are just the apps used by many people, also by many in my social circle. And somehow it creates trust, so that one thinks, ok, if they all have it, than it must be secure and not do anything bad."*

Not Wanting to be Paranoid. There is a general fear of mental illness in society [10]. This might have prompted some participants to be worried about being considered paranoid by engaging in too-obvious or too-stringent security behaviours, as the following quote shows:

> *"On one side, it to some extent naivety, and on the other side, it is to some extent, one can not permanently go on with such distrust, and always with these thoughts in head, I have to be absolutely sure, that no data falls in wrong hands. One can also become paranoid with it."*

> *"The problem is, that one does not understand the things that they write there, unless one becomes acquainted with the topic of security, so one could only trust that whatever is written there is secure."*

4 Model of Precaution Adoption

Based on our findings we have derived a model of smartphone precaution adoption, as depicted in Figures 1 and 2. The model should

- enable researchers to better understand people's decisions in the context of smartphone precaution and secure behaviours.
- serve as a launching pad to encourage future investigations into smartphone-specific precautionary and secure behaviours.

The identified five categories are not orthogonal, nor do we insist on the ordering depicted in Figure 1. For example, it may be that concern comes after self-efficacy, and does not precede it.

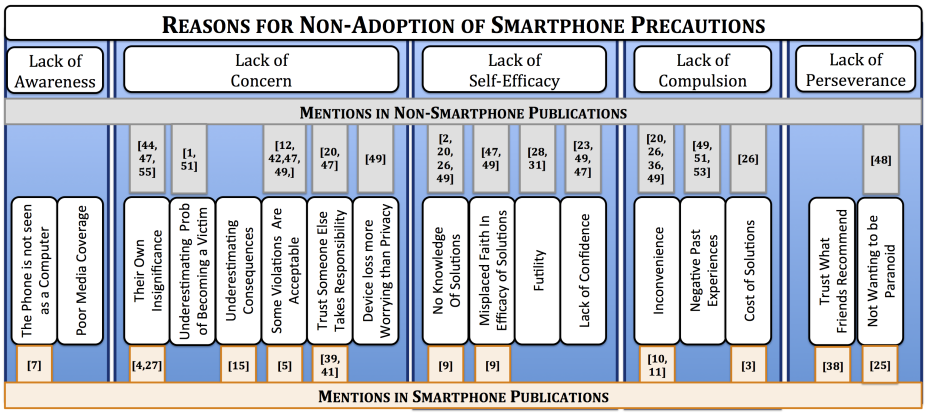

Fig. 2. Categories of explanations for non-adoption in a Smartphone context. Citations for Sub-categories are those who mentioned a related finding in a different context: either non-smartphone or not mental model related.

The subcategory *poor media coverage of smartphone security issues* is new. We carried out a brief investigation into the appearance of related articles in the news in Germany (the interview participants were Germans): A Google News search carried out on the 14th April 2015 for "Smartphone Security Precautions" (with quotes) delivered no results. Without the quotes a number of results appeared. On the first page only the last item actually reported on precautions to be taken by Android owners[7], and that was published two months before.

Not many papers in usable security area seem to mention the role of the media. Some notable exceptions are Furnell and Evangelatos [16] and [32] who do mention the media's role with respect to public awareness of biometrics. Certainly this is an area for future focus if we are to make users more aware of

[7] http://www.heise.de/newsticker/meldung/Sicher-surfen-trotz-Android-4-3-2552659.html

the existence of smartphone-related threats, and the appopriate precautions to take.

The identified five categories are not orthogonal, nor do we insist on the ordering depicted in Figure 1. For example, it may be that concern comes after self-efficacy, and does not precede it.

A particular person's explanation for non-adoption might come from different subcategories, depending on context. For example, consider Johnny wanting to use an unsecured Wifi. He might use it simply because he does not know that this is risky (lack of awareness).

5 Related Work

A number of researchers have studied mobile security from an end-user perspective. Different aspects of user behaviour have been evaluated, to attempt to understand the mental models that users have with respect to smartphone usage and secure behaviour in the smartphone context. Other than our research, these papers did not aim to identify reasons for non-adoption of smartphone precautions. In case of relevant findings for our research, this was mentioned already in the previous section. Therefore, we mention in this section only their research focus and explain why this differs from ours.

A study to evaluate how users protect their data on their smartphones was conducted by Muslukhov *et al.* [34]. The researchers posed three questions: 1) what types of data users store on their phones; 2) how sensitive or valuable each data type is; 3) what users do to protect their data. The evaluation was also carried out using semi-structured interviews. The results have shown that many users tend to store various types of sensitive data on their smartphones such as passwords to various services in the apps on their phones. Yet many do not actively protect the data. Thus, this paper mainly serves as motivation for our work as well as input for future work on how to address the identified justifications.

Lazou and Weir [30] conducted a quantitative study using a multiple-choice questionnaire to evaluate the security practices of smartphone users, the types of sensitive data stored on the smartphones, and users' security awareness. The focus of the study to was to evaluate the extent to which the participants are aware of smartphone security and use protection tools, but it did not look into the reasons for either lack of awareness or failure to use the tools. Other quantitative studies with similar goals were conducted in [38,36].

A great deal of research has been carried out examining app permissions. Felt *et al.* [15] reported on users' perceptions of permissions on different operating systems; Kelley *et al.* [27] used semi-structured interviews to evaluate how users perceived app permissions, whether they paid attention to them, and overall, which decisions they made while installing apps; and Lin *et al.* [31] examined the mental models of smartphone users related to privacy expectations with respect to individual smartphone apps. Their results include usability and

understandability issues as well as reasons for non-consideration of permissions. Their research did not consider other smartphone threats.

6 Conclusions and Future Work

We have known for at least the last 15 years that poor usability deters use of security-related software. Yet other factors also deter adoption and it is important to understand the nature of these factors too so that we can address them.

We identified five context-neutral causative categories from the non-smartphone literature. We then conducted interviews and analysed them to determine whether these same categories manifested in the smartphone arena. We did confirm them, and – more interestingly – identified an exhaustive list of sub-categories in each of the four meta-categories.

The most interesting finding was identification of the role the media has to play in raising public awareness. Investigating this will be the direction of our future research. On a related note, it was interesting that some participants said that they became more concerned about security after the interview. They said that that they would subsequently look into ways to protect themselves. It is heartening to know that our research raised awareness, helping people up at least the first of the adoption steps. It also highlights the importance of awareness raising in this and related security contexts.

Acknowledgements

This paper has been developed within the project 'ZertApps', which is funded by the German Federal Ministry of Education and Research (BMBF) under grant no. 16KIS0073. The authors assume responsibility for the content.

References

1. Akande, A.: Black South African adolescents' attitudes towards AIDS precautions. School Psychology International **18**(4) (1997) 325–341
2. Albrechtsen, E.: A qualitative study of users' view on information security. Computers & Security **26**(4) (2007) 276–289
3. Benenson, Z., Kroll-Peters, O., Krupp, M.: Attitudes to it security when using a smartphone. In: Computer Science and Information Systems (FedCSIS), 2012 Federated Conference on, Wroclaw, Poland, IEEE (2012) 1179–1183
4. Beresford, A.R., Rice, A., Skehin, N., Sohan, R.: Mockdroid: Trading privacy for application functionality on smartphones. In: Proceedings of the 12th Workshop on Mobile Computing Systems and Applications. HotMobile '11, New York, NY, USA, ACM (2011) 49–54
5. Botha, R.A., Furnell, S.M., Clarke, N.L.: From desktop to mobile: Examining the security experience. Computers & Security **28**(3) (2009) 130–137
6. Campbell, M.: Phone invaders. New Scientist **223**(2977) (2014) 32–35

7. Canova, G., Volkamer, M., Bergmann, C., Borza, R.: Nophish: An anti-phishing education app. In Mauw, S., Jensen, C.D., eds.: 10th International Workshop on Security and Trust Management in conjunction with ESORICS 2014. Volume 8743 of Lecture Notes in Computer Science., Wroclaw, Poland, Springer International Publishing (2014) 188–192
8. Chin, E., Felt, A.P., Sekar, V., Wagner, D.: Measuring user confidence in smartphone security and privacy. In: Proceedings of the Eighth Symposium on Usable Privacy and Security, Washington, DC, ACM (2012) 1
9. Clark, S., Goodspeed, T., Metzger, P., Wasserman, Z., Xu, K., Blaze, M.: Why (Special Agent) Johnny (Still) Can't Encrypt: A Security Analysis of the APCO Project 25 Two-Way Radio System. In: USENIX Security Symposium, Berkeley, CA, USA (2011)
10. Corrigan, P.W., Watson, A.C.: At issue: Stop the stigma: call mental illness a brain disease. Schizophrenia Bulletin **30**(3) (2004) 477
11. Debatin, B., Lovejoy, J.P., Horn, A.K., Hughes, B.N.: Facebook and online privacy: Attitudes, behaviors, and unintended consequences. Journal of Computer-Mediated Communication **15**(1) (2009) 83–108
12. Dingledine, R., Mathewson, N.: Anonymity loves company: Usability and the network effect. In: Proc. of the Fifth Workshop on the Economics of Information Security. WEIS 2006, Cambridge, England (2006)
13. Egelman, S., Jain, S., Portnoff, R.S., Liao, K., Consolvo, S., Wagner, D.: Are you ready to lock? In: Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security. CCS '14, New York, NY, USA, ACM (2014) 750–761
14. Elie Bursztein: Survey: Most people don't lock their Android phones — but should (2014) https://www.elie.net/blog/survey-most-people-dont-lock-their-android-phones-but-should.
15. Felt, A.P., Egelman, S., Wagner, D.: I've got 99 problems, but vibration ain't one: a survey of smartphone users' concerns. In: Proceedings of the second ACM workshop on Security and privacy in smartphones and mobile devices, Berkeley, CA, USA, ACM (2012) 33–44
16. Furnell, S., Evangelatos, K.: Public awareness and perceptions of biometrics. Computer Fraud & Security **2007**(1) (2007) 8–13
17. Furnell, S., Tsaganidi, V., Phippen, A.: Security beliefs and barriers for novice internet users. Computers & Security **27**(7) (2008) 235–240
18. Gaw, S., Felten, E.W., Fernandez-Kelly, P.: Secrecy, flagging, and paranoia: Adoption criteria in encrypted email. In: Proc. of the SIGCHI Conference on Human Factors in Computing Systems. CHI '06, Montreal, Canada (2006) 591–600
19. Greenwald, G.: No place to hide: Edward Snowden, the NSA, and the US surveillance state. Metropolitan Books (2014)
20. Harbach, M., Fahl, S., Rieger, M., Smith, M.: On the acceptance of privacy-preserving authentication technology: The curious case of national identity cards. In: Privacy Enhancing Technologies. Springer, Bloomington, Indiana, USA (2013) 245–264
21. Harbach, M., Fahl, S., Smith, M.: Who's Afraid of Which Bad Wolf? A Survey of IT Security Risk Awareness. In: Proc. of Computer Security Foundations Symposium, Vienna, Austria (2014) 97–110
22. Harbach, M., Hettig, M., Weber, S., Smith, M.: Using personal examples to improve risk communication for security & privacy decisions. In: Proceedings of the 32Nd Annual ACM Conference on Human Factors in Computing Systems. CHI '14, New York, NY, USA, ACM (2014) 2647–2656

23. Harbach, M., von Zezschwitz, E., Fichtner, A., De Luca, A., Smith, M.: Itsa hard lock life: A field study of smartphone (un) locking behavior and risk perception. In: Symposium on Usable Privacy and Security (SOUPS), Menlo Park, CA (2014)
24. Herath, T., Rao, H.R.: Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. Decision Support Systems **47**(2) (2009) 154–165
25. Herzberg, A.: Why Johnny can't surf (safely)? Attacks and defenses for web users. Computers & Security **28**(1) (2009) 63–71
26. Jones, N.B., Kochtanek, T.R.: Success factors in the implementation of a collaborative technology, and resulting productivity improvements in a small business: An exploratory study. Journal of Organizational and End User Computing (JOEUC) **16**(1) (2004) 1–20
27. Kelley, P.G., Consolvo, S., Cranor, L.F., Jung, J., Sadeh, N., Wetherall, D.: A conundrum of permissions: installing applications on an android smartphone. In: Financial Cryptography and Data Security. Springer, Bonaire (2012) 68–79
28. Krens, R., Spruit, M., Urbanus-van Laar, N.: Information security in health care-evaluation with health professionals. In: HEALTHINF: International Joint Conference on Biomedical Engineering Systems and Technologies. (2011) 61–69
29. Lampson, B.: Privacy and security usable security: how to get it. Communications of the ACM **52**(11) (2009) 25–27
30. Lazou, A., Weir, G.R.: Perceived risk and sensitive data on mobile devices. In: Cyberforensics, University of Strathclyde, Glasgow (2011) 183–196
31. Lin, J., Amini, S., Hong, J.I., Sadeh, N., Lindqvist, J., Zhang, J.: Expectation and purpose: Understanding users' mental models of mobile app privacy through crowdsourcing. In: Proceedings of the 2012 ACM Conference on Ubiquitous Computing. UbiComp '12, New York, NY, USA, ACM (2012) 501–510
32. Liu, S., Silverman, M.: A practical guide to biometric security technology. IT Professional **3**(1) (2001) 27–32
33. Morton, A., Sasse, M.: Desperately seeking assurances: Segmenting users by their information-seeking preferences. In: Privacy, Security and Trust (PST), 2014 Twelfth Annual International Conference on. (2014) 102–111
34. Muslukhov, I., Boshmaf, Y., Kuo, C., Lester, J., Beznosov, K.: Understanding users' requirements for data protection in smartphones. In: Data Engineering Workshops (ICDEW), 2012 IEEE 28th International Conference on, Cancun, Mexico, IEEE (2012) 228–235
35. Mylonas, A.: Security and privacy in the smartphones ecosystem. Technical Report Technical Report AUEB-CIS/REV-0313, Athens University of Economics and Business (2013)
36. Ophoff, J., Robinson, M.: Exploring end-user smartphone security awareness within a South African context. In: Information Security for South Africa (ISSA), 2014, Johannesburg, South Africa, IEEE (2014) 1–7
37. Peng, P., Blaze, M., Yoo, C.S.: Digital transparency: Is privacy what we really want? (2011) `http://keripo.com/static/academia/upenn/cis125/essay/pengp_final_essay_v1.pdf`.
38. Pramod, D., Raman, R.: A study on the user perception and awareness of smartphone security. International Journal of Applied Engineering Research, ISSN **9**(23) (2014) 19133–19144
39. PWC: Global state of information security survey: 2015 results by industry http://www.pwc.com/gsiss2015.

40. Renaud, K., Volkamer, M., Renkema-Padmos, A.: Why doesn't Jane protect her privacy? In Cristofaro, E.D., Murdoch, S.J., eds.: Privacy Enhancing Technologies - 14th International Symposium, PETS. Lecture Notes in Computer Science, Amsterdam, Netherlands (2014) 244–262
41. Sasse, M.A., Flechais, I.: Usable Security: What is it? How do we get it? In: Security and Usability: Designing secure systems that people can use. O'Reilly Books (2005) 13–30 ISBN:0596008279.
42. Shirazi, F., Volkamer, M.: What Deters Jane from Preventing Identification and Tracking on the Web? In: The 13th Workshop on Privacy in the Electronic Society (WPES 2014), Scottsdale, AZ, USA (2014) 107–116 November 3.
43. Smith, S.W.: Humans in the loop: Human-computer interaction and security. Security & Privacy, IEEE **1**(3) (2003) 75–79
44. Solove, D.J.: "I've Got Nothing to Hide" and Other Misunderstandings of Privacy. San Diego law review **44** (2007) 745
45. Wash, R.: Folk models of home computer security. In: Proceedings of the Sixth Symposium on Usable Privacy and Security, Redmond, WA, ACM (2010) 11
46. Weinstein, N.D.: Why it won't happen to me: perceptions of risk factors and susceptibility. Health psychology **3**(5) (1984) 431
47. Weirich, D., Sasse, M.A.: Pretty good persuasion: a first step towards effective password security in the real world. In: Proc. of 2001 Workshop on New Security Paradigms. NSPW '01, Cloudcroft, NM (2001) 137–143
48. West, R.: The psychology of security. Communications of the ACM **51**(4) (2008) 34–40
49. Whitten, A., Tygar, J.D.: Why Johnny can't encrypt: a usability evaluation of PGP 5.0. In: Proc. of the 8th USENIX Security Symposium - Volume 8. SSYM'99, Washington DC, USA (1999) 169184