A Socio-Technical Investigation into Smartphone Security

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. We propose that future work should investigate the use of media campaigns in raising awareness of these issues.[4]

1 Introduction

The usable security field initially identified poor usability as the primary obstacle preventing adoption of privacy and security measures [29]. Improving usability, on its own, while necessary, has not proved sufficient in many contexts [10,11,23]. It is necessary to investigate other justifications for non-adoption in the smartphone context [27].

We carried out a series of semi-structured interviews to explore possible explanations for non-adoption of smartphone precautions. We derived a model depicting the progression towards smartphone precaution adoption and report on it in this paper.

[4] 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.

2 Methodology

We conducted a series of semi-structured interviews either in person or via Skype, which took, on average, 41 minutes.

2.1 Interview Protocol

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

Phase 2: General security threats. Which security threats they were aware of, which countermeasures could mitigate, how effective they are, and whether they had used them. Their vulnerability to attack was explored, as well as their own experiences of security problems. We also asked about data stored on smartphones, and responsibility for security.

Phase 3: Specific countermeasures. We explored mechanisms used to protect sensitive data.

Phase 4: Specific threats. Specific threats were explored, based upon the guidelines from Federal Office for Information Security[5].

2.2 Participants

Twenty Smartphone owners were recruited via email, according to the snowball principle, with a perfect gender balance ranging from 12 to 65 years of age, with a mean age of 33.2 years. Ethical requirements for research involving human participants are provided by an ethics commission at Darmstadt. Participants were initially told that the study was about smartphone usage and debriefed afterwards about the real nature of the investigation. Permission was gained from adults or parents, where applicable, to record the interview anonymously.

2.3 Analysis

To support an interpretative phenomenological analysis (IPA) of our interviews we needed a set of pre-existing themes. 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* [23,11,10,24]. We synthesised a number of deterrents to adoption and usage:(1) Lack of awareness, (2) Lack of concern, (3) Lack of self-efficacy, (4) Lack of compulsion and (5) Lack of perseverance.

3 Results

The interviews were transcribed, and 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 and codes to categories.

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

3.1 Lack of Awareness

Participants were either completely unaware, or only aware of threats that required physical access to their smartphone: *"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 a number of possible explanations for lack of awareness:

It's a Phone, not a Computer. Participants had not made the mental connection to the need for precautions, eg: *"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. 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: *"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

Their Own Insignificance. Participants believed that they were not important enough to interest attackers, or that they did not have any interesting data on their smartphones: *"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 participants underestimated their vulnerability; this led to their not behaving securely and not using privacy-protecting tools: *"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 did not seem to anticipate the concrete harm that could result: *"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 [..]*

Some Privacy Violations are Acceptable. For example: *"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."*

Trust Someone Else to Take Responsibility. Participants named developers, smartphone providers, play stores and state institutions, as being responsible: *"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 overestimated the level of scrutiny by either Apple or Google. Assuming that malicious apps could not enter the store, they did not take precautions: *"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. No one mentioned privacy and only a few mentioned security. Instead a number said that the main problem would be losing the device itself: *"As long as it is not stolen, I do not worry."*; *"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: *"Good, I would immediately lock the card. So that no one can use it. [...] I would also go to the police, but I believe this has nothing to do with it."*

3.3 Lack of Self-Efficacy.

People can still fail to act defensively if they do not possess the know-how or self confidence to take action.

Lack of Knowledge. Some did not seem to know how to protect themselves, or what actions to take against threats: *"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."* More advanced measures, such as the option to remotely track the stolen device or wiping data from it, or encryption, were hardly ever mentioned.

Other participants, demonstrated misconceptions with respect to specific threats, such as using non-secured WLAN: *"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. 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: *"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: *"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 believed that since they had not experienced any security issues so far, it meant that their way of using the smartphone must be secure: *"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. Participants were sceptical about whether the existing precautionary measures were indeed capable of protecting them. *"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. Some did not have the confidence to engage with precautionary measures: *"I would need to ask someone to download or install it for me."*

3.4 Lack of Compulsion

Some, despite being aware of the threats and of the precautionary measures, cited other factors that kept them from adopting those measures.

Inconvenience. Many referred to the effort that would be required that would hinder their usage of their smartphone: *"Because I am irritated that I have to constantly enter this, around 50 times a day."*; *"I think it is more secure than the PIN, but it is too effortful."*; *"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: *"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 quiet minute, then I do the update."*

Negative Past Experiences. Participants expressed concern 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: *"Antivirus software makes my phone too slow if it runs in the background all the time, therefore I decline to use it."*

Financial Cost. *"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

I Trust What My Friends Do. *"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. *"On one hand, it to some extent naïvety, 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 Figure 1[6]. (The subcategory *poor media coverage of smartphone security issues* is new.)

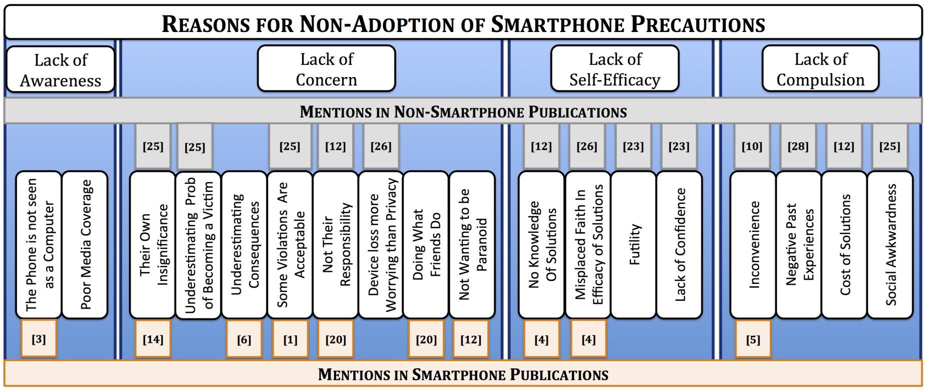
REASONS FOR NON-ADOPTION OF SMARTPHONE PRECAUTIONS
Lack of Awareness
Lack of Concern
Lack of Self-Efficacy
Lack of Compulsion
MENTIONS IN NON-SMARTPHONE PUBLICATIONS
[25]
[25]
[25]
[12]
[26]
[12]
[26]
[23]
[23]
[10]
[28]
[12]
[25]
The Phone is not seen as a Computer
Poor Media Coverage
Their Own Insignificance
Underestimating Prob of Becoming a Victim
Underestimating Consequences
Some Violations Are Acceptable
Not Their Responsibility
Device loss more Worrying than Privacy
Doing What Friends Do
Not Wanting to be Paranoid
No Knowledge Of Solutions
Misplaced Faith In Efficacy of Solutions
Futility
Lack of Confidence
Inconvenience
Negative Past Experiences
Cost of Solutions
Social Awkwardness
[3]
[14]
[6]
[1]
[20]
[20]
[12]
[4]
[4]
[5]
MENTIONS IN SMARTPHONE PUBLICATIONS

Fig. 1. 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 . [1,2,4,3,5,6,10,13,12,14,20,21,23,25,26,28]

Not many papers in usable security seem to mention the role of the media. Some notable exceptions are Furnell and Evangelatos [9] and [18] 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 the existence of smartphone-related threats, and the appropriate precautions to take.

5 Related Work

A study to evaluate how users protect their data on their smartphones was conducted by Muslukhov *et al.* [19]. The researchers reported that users tend to store various types of sensitive data on their smartphones yet many do not actively protect their data. Lazou and Weir [16] conducted a quantitative study to evaluate the security practices of smartphone users, the types of sensitive data stored on the smartphones, and users' security awareness but 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 [22,21,8].

A great deal of research has been carried out examining app permissions [7,15,17]. Their results include usability and understandability issues as well as reasons for non-consideration of permissionsbut they did not address other smartphone threats.

[6] This list of references is not exhaustive due to lack of space

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.

References

1. Botha, R.A., Furnell, S.M., Clarke, N.L.: From desktop to mobile: Examining the security experience. Computers & Security **28**(3) (2009) 130–137
2. Campbell, M.: Phone invaders. New Scientist **223**(2977) (2014) 32–35
3. 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., Springer (2014) 188–192
4. 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. (2011)
5. 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
6. 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.
7. Felt, A.P., Egelman, S., Wagner, D.: I've got 99 problems, but vibration ain't one: a survey of smartphone users' concerns. In: 2nd ACM workshop on Security and privacy in smartphones and mobile devices, ACM (2012) 33–44
8. Ferreira, A., Huynen, J.L., Koenig, V., Lenzini, G.: Socio-technical security analysis of wireless hotspots. In: Human Aspects of Information Security, Privacy, and Trust. Springer (2014) 306–317
9. Furnell, S., Evangelatos, K.: Public awareness and perceptions of biometrics. Computer Fraud & Security **2007**(1) (2007) 8–13
10. Gaw, S., Felten, E.W., Fernandez-Kelly, P.: Secrecy, flagging, and paranoia: Adoption criteria in encrypted email. In: SIGCHI Conference on Human Factors in Computing Systems. CHI '06 (2006) 591–600
11. 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 (2013) 245–264
12. Harbach, M., Hettig, M., Weber, S., Smith, M.: Using personal examples to improve risk communication for security & privacy decisions. In: 32Nd Annual ACM Conference on Human Factors in Computing Systems. CHI '14, ACM (2014) 2647–2656

13. Harbach, M., von Zezschwitz, E., Fichtner, A., De Luca, A., Smith, M.: It's a hard lock life: A field study of smartphone (un) locking behavior and risk perception. In: Symposium on Usable Privacy and Security (SOUPS). (2014)
14. 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
15. 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 (2012) 68–79
16. Lazou, A., Weir, G.R.: Perceived risk and sensitive data on mobile devices. In: Cyberforensics, University of Strathclyde (2011) 183–196
17. 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: ACM Conference on Ubiquitous Computing. UbiComp '12, ACM (2012) 501–510
18. Liu, S., Silverman, M.: A practical guide to biometric security technology. IT Professional **3**(1) (2001) 27–32
19. Muslukhov, I., Boshmaf, Y., Kuo, C., Lester, J., Beznosov, K.: Understanding users' requirements for data protection in smartphones. In: Data Engineering Workshops (ICDEW), IEEE (2012) 228–235
20. Mylonas, A.: Security and privacy in the smartphones ecosystem. Technical Report AUEB-CIS/REV-0313, Athens University of Economics and Business (2013)
21. Ophoff, J., Robinson, M.: Exploring end-user smartphone security awareness within a South African context. In: Information Security for South Africa (ISSA), 2014, IEEE (2014) 1–7
22. 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
23. Renaud, K., Volkamer, M., Renkema-Padmos, A.: Why doesn't Jane protect her privacy? In: 14th International Symposium on Privacy Enhancing Technologies. Springer LNCS. (2014) 244–262
24. 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
25. Smith, S.W.: Humans in the loop: Human-computer interaction and security. Security & Privacy, IEEE **1**(3) (2003) 75–79
26. Solove, D.J.: "I've Got Nothing to Hide" and Other Misunderstandings of Privacy. San Diego law review **44** (2007) 745
27. Wash, R.: Folk models of home computer security. In: Proceedings of the Sixth Symposium on Usable Privacy and Security, Redmond, WA, ACM (2010) 11
28. West, R.: The psychology of security. Communications of the ACM **51**(4) (2008) 34–40
29. Whitten, A., Tygar, J.D.: Why Johnny can't encrypt: a usability evaluation of PGP 5.0. In: 8th USENIX Security Symposium - Volume 8. SSYM'99 (1999) 169184