Poster: Attitudes to IT-Security When Using a Smartphone

Zinaida Benenson & Nadina Hintz
Friedrich-Alexander University
Erlangen-Nuremberg
Schlossplatz 4
91054 Erlangen, Germany
name.surname@cs.fau.de

Olaf Kroll-Peters
EnBW AG
Durlacher Allee 93
76131 Karlsruhe
Germany
o.kroll-peters@enbw.com

Matthias Krupp
AFI GmbH
Julius-Hölder-Str. 39
70597 Stuttgart
Germany
mkp@afi-solutions.com

1. INTRODUCTION

Usage of mobile phones, and especially smartphones, has greatly increased in the last decade. The quality and quantity of malware and other cyber crime attacks on mobile phone users has increased accordingly [6, 2].

The role of the users in the "traditional" security is an established research topic [1, 4, 3]. On the other hand, this type of research in the area of mobile communication has been very scarce.

We conducted an explorative study by means of semi-structured interviews with 24 smartphone users about their security knowledge and awareness, attitudes to the security and privacy threats, and the measures they take in order to stay secure. We are not aware of other studies that consider these research questions.

2. STUDY RESULTS

The participants were recruited during a rock music festival in Berlin. 54% of the probands are male. 45% are younger than 25 years, 38% are between 26-30 years und only 17% are older than 30 years. Thus, our results are biased towards younger people, which is probably not surprising considering the recruitment place.

2.1 "Smartphone" vs. "Telephone" Users

The interview data revealed two distinct usage patterns for smatphones. 11 of 24 users, although their devices have the usual smartphone functionality, use their smartphones mostly for the phone calls and SMS, but not for the Internet access. These users are called *telephone users* in our study. The remaining 13 users are the "real" *smartphone users*.

We found that the attitudes, feelings and knowledge of the participants with respect to our research questions differ from each other according to the usage patterns. We present some of these differences below.

2.2 Security Awareness

We define security awareness as a combination of the knowledge and of the interest in IT security. The users were asked to rate both. At the end of the questionnaire, we placed a control question in order to assess users' self-rating more reliably. It asked the users to explain the term "remote wipe".

54 % of the smartphone users stated to have good knowledge and 38% stated to have basic knowledge about IT-security of smartphones (Figure 1). Half of them correctly answered the control question.

4 out of 11 telephone users stated to have a good knowledge about IT security of smartphones. Only one of them correctly answered the control question. Besides the low knowledge, the telephone users are not really interested in the protection of their device (Figure 2). In summary, the smartphone users have a better knowledge of protection and a greater interest in security of mobile devices.

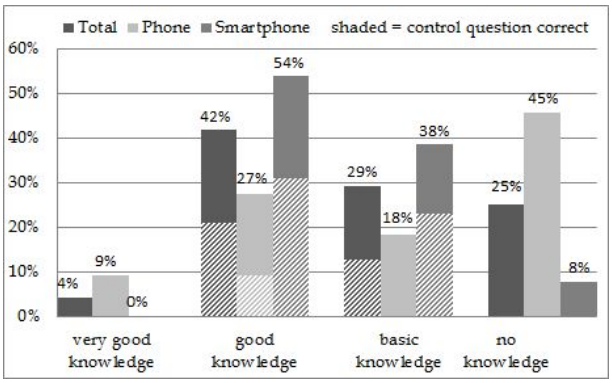

Figure 1: Knowledge about the protection of mobile phones.

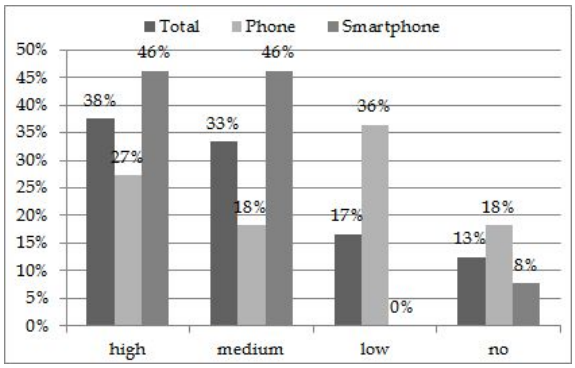

Figure 2: Interest in protection of mobile phones.

2.3 Feeling Secure

17 of 24 respondents (70%) indicated that they feel safe using their mobile device (Figure 3). Smartphone users feel much less safe. As a reason they mentioned eavesdropping and recording of location data.

The telephone users explained that they feel safe mostly because they do not use the Internet. They also stated that

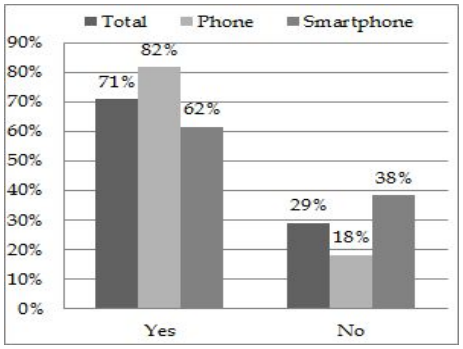

Figure 3: Do you feel safe when using your mobile phone?

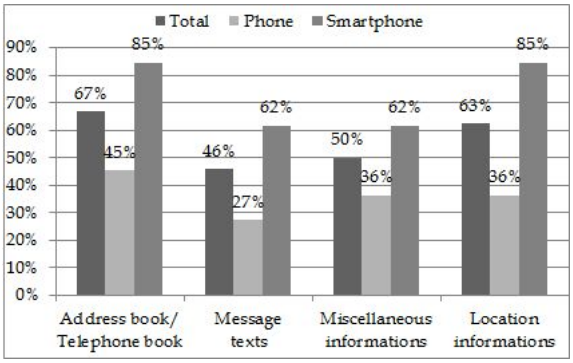

Figure 4: Which kind of data is likely to be attacked according to user's opinion.

they do not have any kind of "interesting" data.

Figure 4 shows that both user groups are mostly concerned about their contact data and their location information, with smartphone users being significantly more concerned (p=0,043 for contact data).

2.4 Responsibility for Device Security

We asked the users to assign the percentage of protection responsibility to software producers, hardware producers and the users.

Most users think that the software vendors should be most responsible for the security on mobile devices, the difference between smartphone and telephone users is significant here (p=0,008). Smartphone users give the hardware manufactures and the users the same percentage of responsibility, whereas telephone users think that the user is the least responsible party.

2.5 Security Measures

None of the users had any security-related problems with their devices so far. We asked them which measures they take in order to protect their devices. Here, the most frequent answer was that the users are being "careful". They restrict WLAN and Bluetooth access of their devices, and they only download applications and only click on links if they trust them, "trust" being a very vague term with no specific criteria. Approximately one third of the users also take technical measures, such as password protection, antivirus programs and security updates.

3. DISCUSSION AND FUTURE WORK

One serious limitation of our work is the small number of participants, such that we mostly could not determine statistical significance of our results. For example, there seems to be a connection between the gender and the usage pattern: out of 11 female participants, only 2 were the "smartphone" users in the sense of the previous definition. On the other hand, 11 of 13 male participants were the "smartphone" users. Is there indeed a significant difference in smartphone usage patterns according to gender?

Furthermore, does a connection exist between not using a smartphone for the Internet, having low security knowledge and awareness, and feeling safe? For example, do people with especially high need in feeling safe refuse to use their phones on the Internet?

In general, our study stimulated many interesting research questions. For example, the users state that they can protect their mobile devices by being "careful" about what they download and on which links they click. Here, the meaning of "being careful" requires further investigation. Moreover, how good can a "careful" user protect his or her smartphone? In the case of PCs we know that just being careful is not enough, as the users' mental models and strategies for protection are poorly adjusted to the reality [5, 7].

Another interesting question is whether the users see the analogy between their smartphones and the PCs. The functionality and the threats are very similar for both kinds of devices, but the user perceptions and attitudes may differ. Also comparisons of different smartphone platforms are of great interest.

4. REFERENCES

[1] A. Adams and M. A. Sasse. Users are not the enemy. *Commun. ACM*, 42:40–46, December 1999.

[2] M. Becher, F. Freiling, J. Hoffmann, T. Holz, S. Uellenbeck, and C. Wolf. Mobile security catching up? revealing the nuts and bolts of the security of mobile devices. In *Security and Privacy (SP), 2011 IEEE Symposium on*, pages 96–111, may 2011.

[3] L. J. Camp. Mental models of privacy and security. *Technology and Society Magazine, IEEE*, 28(3):37–46, Fall 2009.

[4] L. Cranor and S. Garfinkel. *Security and Usability*. O'Reilly Media, Inc., 2005.

[5] J. S. Downs, M. B. Holbrook, and L. F. Cranor. Decision strategies and susceptibility to phishing. In *Proceedings of the second symposium on Usable privacy and security*, SOUPS '06, pages 79–90, 2006.

[6] Juniper Networks. *Malicious Mobile Threats Report 2010/2011: An Objective Briefing on the Current Mobile Threat Landscape Based on Juniper Networks Global Threat Center Research*. Juniper Networks, Inc., 2011.

[7] K. Onarlioglu, U. Ozan Yilmaz, D. Balzarotti, and E. Kirda. Insights into user behavior in dealing with internet attacks. In *NDSS, 19th Annual Network and Distributed System Security Symposium*, 2012.