ISBN 978-83-60810-51-4

Attitudes to IT Security when Using a Smartphone

Zinaida Benenson
Universität Erlangen-Nürnberg
Erlangen, Germany
Email: zinaida.benenson@cs.fau.de

Olaf Kroll-Peters
EnBW AG
Karlsruhe, Germany
Email: o.kroll-peters@enbw.com

Matthias Krupp
AFI - P.M. Belz Agentur für Informatik GmbH
Stuttgart, Germany
Email: matthias.krupp@afi-solutions.com

***Abstract*—While mobile devices are becoming more and more powerful, the number of potential security threats is increasing. Although the important role of users in the realization of IT security measures is widely acknowledged and documented, research in the area of mobile security mostly concentrates on technical means. In this work we take the first step in examining the role of the users in the IT security of mobile devices. We present mental models of security that are based on the results of interviews with 24 users. Mental models are the representation of reality in people's mind and can be inaccurate or faulty. Mental models are very helpful for behavior prediction. Thus, mental models of security form the basis of users' efforts to protect their devices.**

I. Introduction

THE NUMBER and capabilities of mobile devices have been increasing more and more during the last years. Therefore, the number of IT security threats is also increasing [13], [3]. On the one hand users are exposed to technical threats such as malware, data communication interception and spying out location informations. On the other hand, there also exist "human" threats such as loss or theft, misuse and social engineering. In both cases users play an important role in protection of their devices. For example, active user participation is usually needed for installing mobile malware.

So far, the role of users in the security of mobile devices has not been not sufficiently investigated. In this work we take the first steps to establish mental models of IT security when using mobile devices. Mental models characterize the individual representation and understanding of reality and are influenced by experiences, feelings and information available to an individual.

This paper is organized as follows. In Section II, we review related work of mental models of IT security. Then in Section III we present our investigation of mental models of security when using mobile devices. Section IV discusses the results of our user study, and finally in Section V we give a summary and some future research questions.

II. Related Work on Mental Models of Security

First mental models of security were introduced by Camp et al. [2], [6]. They distinguished five metaphers of IT security: physical security (e.g. locks), medical infection (viruses), criminal behaviour (burglar), warfare and economic failures (vulnerabilities in software).

Implicit descriptions of mental models of IT security are often found in publications on the topic of human-computer interaction. Sasse et al. [21] found out that the users' knowledge is not sufficient to meet existing security threats in a correct way. Norman [18] observed that users even denied the installation of essential security patches because they feared to have installed something wrong. Their mental model can be summarized as "installing new software is dangerous". Due to the lack of knowledge the users cannot distinguish between secure and insecure installation requests.

Raja et al. [20] showed that inaccurate mental models often create an additional source of danger. Users create their own rules in dealing with computer systems, for example, they create seemingly secure passwords that they can better remember and that are in reality very weak [1], [10], [11].

Compliant behaviour is for users also a costs-/benefits-calculation [12]. The costs are often perceived as too high, which creates the perception of security mechanisms as obstacles that should be avoided. According to Lampson [16] many users have developed a "say OK to any security questions" mental model. The increasing number of checkboxes to which the users have to respond have lead to the fact that users have found out which buttons they have to press in order not to interrupt their work [23], [14].

Another factor that influences the image of IT security of many users is their social environment. Weirich and Sasse [24] say, e.g., that security-conscious users are usually described – even by themselves – as "paranoid", "pedantic", or as a person who trusts no one. Because being accepted by their environment is very important for the users, some of them even tell that they are proud of not unterstanding or not using security mechanisms [21].

The above works describe mental models of security that are typical for users of "classical" computer systems. However, similar investigations are rare in the area of mobile security. Independently and concurrently to our work, Felt et al. [9] published a technical report on the concerns of smartphone users. Muslukhov et al. investigated privacy requirements of smartphone users [17].

The following section describes our approach to investigation of users' attitudes to security that help us to make initial suggestions about their mental models of mobile device security.

978-83-60810-51-4/$25.00 © 2012 IEEE

III. Studies of IT security by using mobile devices

A. Pilot study

In order to better understand the complex topic "users and their mobile devices", we conducted interviews where we asked smartphone users about the typical usage of their devices and their attitude to protection of the devices. We discovered two typical usage patterns. On the one hand, some users see their device as a conventional phone. Even if their phone has a usual smartphone functionality, they use their smartphone just for phone calls and SMS. The second type of users utilize the full smartphone functionality. These basic mental models, "my device is a phone" vs. "my device is a smartphone", were considered in more detail in the main study.

B. Main study

The goal of the main study was a detailed description of users' attitudes to security of their mobile devices.

1) Hypotheses: Based on the results of the pilot study we established the following hypotheses:

- H1: Users who see their device as a smartphone have a greater security awareness than users who see their devices just as a phone.
- H2: Users who see their device as a smartphone feel less secure as users who see their device just as a phone.
- H3: Users do not feel responsible for the security of their devices.
- H4: Users do not connect problems in the usage of their devices with security.
- H5: "Careful" use of their mobile devices is the main protection effort of the users.

The both concepts "security awareness" and "careful usage" will be explained below. A detailed and complete description of the hypotheses and the related results is given in Krupp [15].

2) Experiments description: To evaluate the hypotheses, semi-structutred interviews were conducted with 24 participants. The age of the respondents was between 18 and 50 years. About half of them was male and five of them were worked in IT-related fields.

We tried not to make the probands too early aware of the purpose of the interviews. In the first part the interview focused on the usage of mobile devices. Thereby the participants were asked which services they regularly use, which properties they connect with the use of their device, which problems they already had and which knowledge about securing of their mobile device they have. Furthermore they were asked to which extent they see themselves, the hardware manufacturers and the app programmers responsible for the protection of mobile devices.

The second part of the questionnaire focused on the efforts of the respondents to ensure IT security. Here they had to specify the magnitude of their interest in the security of their mobile device, and which efforts they undertake to protect themselves. We also asked whether the users feel secure when using their device, and which data on the device is threatened in their opinion. Finally, a question about an enhanced security setting was asked to better classify the self-evaluation of the respondents regarding their security knowledge. This control question was: "What is remote wipe?".

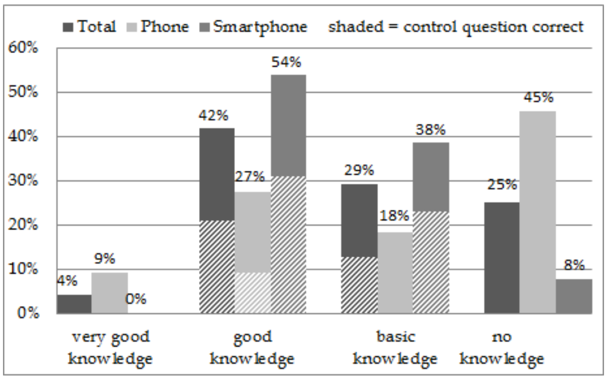

Fig. 1. How would you rate your knowledge about protecting your mobile device?

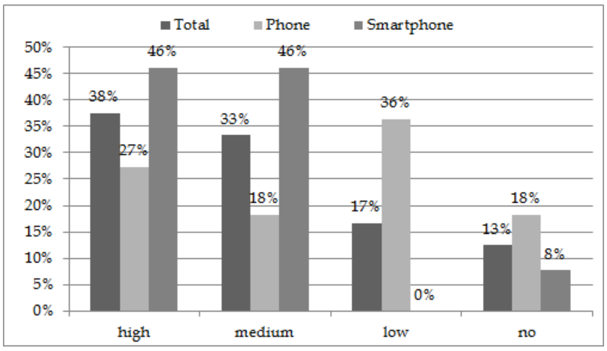

Fig. 2. How would you rate your interest in the protection of mobile devices and their data?

3) Evaluation of the hypotheses: **H1: Users who see their device as a smartphone have a greater security awareness than users who see their devices just as a phone.** We understand security awareness as a complex consisting of the knowledge of and the interest in IT security. A total of eleven respondents saw their devices as a conventional phone and 13 as a smartphone. Seven of the 13 respondents (54%) who see their mobile device as a smartphone stated that they have a good knowledge about protection of mobile devices (see figure 1). Five of the smartphone users (38%) assigned to themselves basic knowledge. Half of these users answered the control question correctly.

Only four of the eleven respondents who see their device as a phone reported that they have at least a good knowledge about protecting mobile devices. Only one of these users also answered the control question correctly.

Besides the overall low security knowledge of the telephone users, they do not have a great interest in the security of their mobile devices. Figure 2 shows that six of the eleven respondents have no or only little interest in the security of their device. Among the respondents who see their device as a smartphone, the interest is visibly stronger. Six study

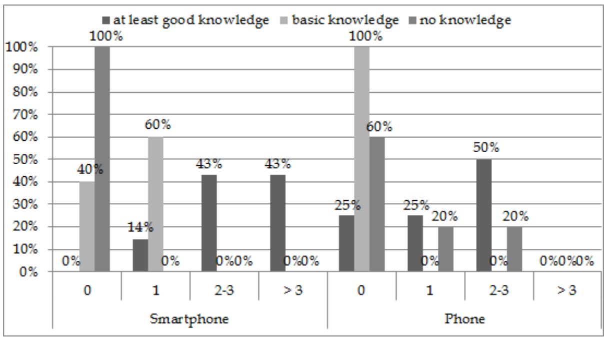

Fig. 3. Number of mentioned threats in relation to the self-evaluated skills

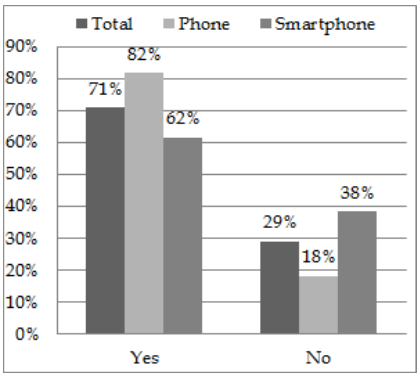

Fig. 4. Do you feel secure when using your mobile device?

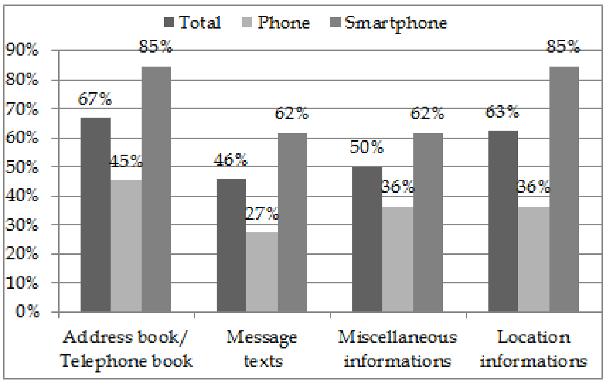

Fig. 5. Which data do you think is threatened on your mobile device?

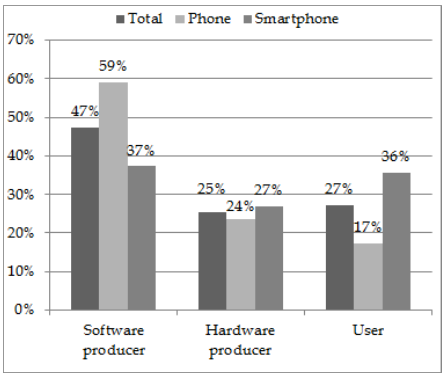

Fig. 6. Who should be responsible for the security of mobile devices?

participants reported an average and further six a high interest.

In an open question the participants were asked about known threats in the mobile environment. The classification of the responses fits the six threat groups by Juniper [13]: data communication interception, exploitation and misconduct, tracking, direct attacks, malware and loss and theft.

If we correlate the number of mentioned threats to the self-evaluated knowledge, we can see that many users who rate themselves with good skills could also mention more threats (see figure 3).

Comparing the results of the two basic mental models, it becomes clear that the smartphone users could mention more threats than the phone users. Moreover, they rated their skills relatively well. However, further research is needed, since the total number of respondents was too small.

In summary, the results show that users who see their mobile device as a smartphone, have better knowledge of and a higher interest in the protection of mobile devices. Thus, the first hypothesis could be confirmed.

H2: Users who see their device as a smartphone feel less secure than users who see their device just as a phone. 17 of 24 respondents indicated that they feel secure when using their mobile device (see Figure 4). This shows that the users do feel quite secure. But the consideration of the two basic models shows that much fewer smartphone users feel secure when using their mobile device. These users are mostly concerned that data flows can be monitored and location data can be recorded.

Phone users attribute their increased security feeling to the fact that they do not browse the Internet. Other reasons that they mentioned were that they feel themselves not important enough for attackers, and that they think they do not have important data on their devices.

Figure 5 shows that from the respondents' point of view the address and phone book as well as the location data are mostly threatened on the mobile device. The phone users think on average that much less data on the mobile device threatened. Thus, the second hypothesis can be confirmed.

H3: Users do not see themselves responsible for the security of their device. To find out whom the respondents see responsibile for the security of mobile devices, we asked them to allocate software producers, hardware producers and themselves a percentage of responsibility for security. It is quite interesting that in users' opinion, almost half of the responsibility falls on the software producers (see figure 6). The hardware producers and the users themselves are seen much less responsible by the respondents.

Users who see their device as a phone, think that users have the least responsibility for security. In contrast, the smartphone users assign to the software producers and to the users the same percentage of responsibility.

Based on these results, the third hypothesis can be confirmed, because the users show a strong preference to give the software and hardware producers the responsibility for the security of their devices. However, especially smartphone users see themselves responsible. How far they are willing to take on the responsibility requires further research.

H4: Users do not connect problems in the usage of their devices to IT security. During the first part of our survey participants were asked whether they had problems with their mobile device so far. Seven of 24 respondents reported a problem. All mentioned problems could be reduced to handling some peculiarities of the mobile device, such as hanging or crashing of the device, a short battery life, problems with the operating system or an inadequate range of functions.

However, as the participants were explicitly asked about security-related problems in the second part of the interview, one participant stated that he had such a problem. By mistakenly clicking a hyperlink when surfing the Internet, he got into a subscription trap. In the previous question about problems with the mobile devices he didn't mentioned this problem.

Also in the pilot study we could make out that several participants already had problems with their device, but no one mentioned a security problems. There, two users also indicated security problems only after they were asked explicitly about such problems.

Thus, security problems with mobile devices are not established in the mental models of users yet. This could be associated with the fact that the participants were very seldom confronted with such problems so far.

H5: "Careful" use of their mobile device is the main effort of users to take care about IT security in the mobile environement. The interviewees were asked to indicate on the basis of given security measures, which efforts they undertake to protect themselves in the mobile environment.

Careful use (aware handling) of the device is the most popular security measure (see Table I). Only 8% of the respondents said that they never deal with the security aware use of their device. While the majority of the smartphone users always try to pay attention to careful use, 64% of the phone users told that they care to do so occasionally. Under careful use the participants understand that they pay attention to the use of their device, which applications they install and use and that they browse responsibly trough the internet.

Further only one out of four does not inform oneself about IT security risks. Hereunder are nearly half of all users who see their devices as a phone. The remaining respondents are generally inform oneself occasionally about the latest threats.

Technical security measures are used infrequently. 38% of all respondents regularly use the password protection of their device, and 21% use it occasionally. Especially the 62% of smartphone users use the password protection on a regular basis. Similar values apply to updates, virus scanners are less popular. In the computers environment, however, there are regular studies which demonstrate that over 75% of the users have a virus scanner installed on their computers [4], [5]. Reasons for these results could lie in the menu preferences of the devices, but weren't investigated further in this work.

TABLE I
WHAT KIND OF EFFORTS DO YOU UNDERTAKE IN ORDER TO ENSURE SECURITY IN MOBILE ENVIRONMENT?

	mental model	I always try to be up to date	I care about the ocassional issue	I do not care about the topic at all	I do not know
Password protection	Total	38%	21%	25%	17%
	Phone	9%	27%	45%	18%
	Smartphone	62%	15%	8%	15%
Updates	Total	42%	21%	21%	17%
	Phone	9%	27%	45%	18%
	Smartphone	69%	15%	0%	15%
Antivirus	Total	21%	13%	42%	25%
	Phone	9%	18%	55%	18%
	Smartphone	31%	8%	31%	31%
Aware handling	Total	46%	42%	8%	4%
	Phone	9%	64%	18%	9%
	Smartphone	77%	23%	0%	0%
Information about risk in computer information-Security	Total	17%	50%	25%	8%
	Phone	0%	36%	45%	18%
	Smartphone	31%	62%	8%	0%

Thus the fifth hypothesis could be confirmed. 88% of the participants reported that they pay attention at least occasionally to the careful use of their mobile device. According to the interviewees, they feel secure from threats as long as they behave carefully and conscientious and do not cause any error conditions.

IV. MENTAL MODELS OF SECURITY OF MOBILE DEVICE USERS

Our study shows that users of mobile devices can be divided into two categories, which differ significantly according to their attitude to IT security of their devices. The *"my device is a phone"*-mindset is independent of the functionality of the device and is associated with a lower security awareness and a greater feeling of security as the *"my device is a smartphone"*-mindset. In particular, "phone users" see themselves not responsible for the security of their devices and concern themselves only a little with the overall theme.

It was found that many users have an "as long as I do not go into the Internet I'm safe" -mental model. In addition, many users believe that they are not personally threatened, because they are not important enough or do not store any important data on their device. Here the parallels to the risk assessment in the PC world are clearly visible [22], [25].

In general it seems that users draw less parallels between the computer world and the mobile world, as they do not link problems when using mobile devices with IT security, but exclusively with handling or peculiarities of the devices. Moreover, technical security measures in the mobile world are less used than in the computer world.

For the protection in the mobile environment, the users limit their efforts almost exclusively on the careful use of the device so far. The respondents answered among other things, that they use "trusted" applications, avoid unserious services and do not click irrespectively on any links. In addition, they keep their data volume as low as possible and are careful to protected their Bluetooth or Wi-Fi conenctions.

It seems that many users have an "I will be definitely able to recognize threats on my device"-mental model. Whether this model actually works is doubtful when one considers the parallels to the computer world [7], [8], [23], [20], [19]. It is also unclear whether most users had no security problems with their devices so far, or whether they have not recognized such problems.

V. Conclusion

Our study revealed first insights into how users perceive the security of their mobile devices and which measures they take to protect their devices.

Although users know that a lot of data on their mobile devices is threatened, they feel secure most of the time. If the respondents undertake some efforts to protect their devicest, these efforts concentrate often on the careful use of the device. Users with good security knowledge often use additionally technical protection means, such as password protection or regularly installing updates.

Overall, our initial investigation revealed more questions than answers, so that further research is needed. For example we do not know how well the users' self-assessment of their security knowledge correlates to their actual knowledge.

The careful use of the mobile devices turned out to be the main effort of users to ensure IT security in the mobile environment. The users often described conscious use such that they do not install dubious applications, pay attention to their browsing habits and are not available through communication interfaces like bluetooth or Wi-Fi. Hereby it is of interest whether the users have a common picture of careful usage and whether they associate insecure practices with the careful usage.

In addition, the question arises whether the users actually have enough knowledge to make the distinction between safe and unsafe applications, links, and settings of the phone.

Another point for future work is the question whether the users have different ways of considerin computers and mobile devices. Modern mobile devices are becoming increasingly powerful, have an ever-increasing range of functions a nd become more and more similar tothe computers. Nevertheless, it seems that the users draw few parallels to the computer world and protect themselves in the computer environment to a greater extent, even though more and more threats are very similar.

References

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

[2] F. Asgharpour, D. Liu, and L. J. Camp. Mental models of security risks. In *Proceedings of the 11th International Conference on Financial cryptography and 1st International conference on Usable Security*, FC'07/USEC'07, pages 367–377, Berlin, Heidelberg, 2007. Springer-Verlag.

[3] 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.

[4] BITKOM. Internet-sicherheit. Studie, Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V., Februar 2010.

[5] BSI. Mit sicherheit. BSI Jahresbericht 2010, Bundesamt für Sicherheit in der Informationstechnik, Juli 2011.

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

[7] R. Dhamija, J. D. Tygar, and M. Hearst. Why phishing works. In *Proceedings of the SIGCHI conference on Human Factors in computing systems*, CHI '06, pages 581–590, 2006.

[8] 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.

[9] A. P. Felt, S. Egelman, and D. Wagner. I've got 99 problems, but vibration ain't one: A survey of smartphone users' concerns. Technical Report UCB/EECS-2012-70, University of California at Berkeley, May 2012.

[10] D. Florencio and C. Herley. A large-scale study of web password habits. In *Proceedings of the 16th international conference on World Wide Web*, WWW '07, pages 657–666, 2007.

[11] A. Forget, S. Chiasson, and R. Biddle. Helping users create better passwords: is this the right approach? In *Proceedings of the 3rd symposium on Usable privacy and security*, SOUPS '07, pages 151–152, 2007.

[12] C. Herley. So long, and no thanks for the externalities: the rational rejection of security advice by users. In *Proceedings of the 2009 workshop on New security paradigms workshop*, NSPW '09, pages 133–144, 2009.

[13] 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.

[14] R. Kainda, I. Flechais, and A. Roscoe. Security and usability: Analysis and evaluation. In *Availability, Reliability, and Security, 2010. ARES '10 International Conference on*, pages 275–282, 2010.

[15] M. Krupp. Die Verantwortung von Nutzern zur Umsetzung von IT-Sicherheit, masterthesis, 2011.

[16] B. Lampson. Privacy and security: Usable security: how to get it. *Commun. ACM*, 52:25–27, November 2009.

[17] I. Muslukhov, Y. Boshmaf, C. Kuo, J. Lester, and K. Beznosov. Understanding users' requirements for data protection in smartphones. In *ICDE Workshop on Secure Data Management on Smartphones and Mobiles*, Dec 2012.

[18] D. A. Norman. The way i see it: When security gets in the way. *interactions*, 16:60–63, November 2009.

[19] 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.

[20] F. Raja, K. Hawkey, P. Jaferian, K. Beznosov, and K. S. Booth. It's too complicated, so i turned it off!: expectations, perceptions, and misconceptions of personal firewalls. In *Proceedings of the 3rd ACM workshop on Assurable and usable security configuration*, SafeConfig '10, pages 53–62, 2010.

[21] M. A. Sasse, S. Brostoff, and D. Weirich. Transforming the 'weakest link' – a human/computer interaction approach to usable and effective security. *BT Technology Journal*, 19:122–131, July 2001.

[22] B. Schneier. The psychology of security. In *Proceedings of the Cryptology in Africa 1st international conference on Progress in cryptology*, AFRICACRYPT'08, pages 50–79, Berlin, Heidelberg, 2008. Springer-Verlag.

[23] J. Sunshine, S. Egelman, H. Almuhimedi, N. Atri, and L. F. Cranor. Crying wolf: an empirical study of ssl warning effectiveness. In *Proceedings of the 18th conference on USENIX security symposium*, SSYM'09, pages 399–416, Berkeley, CA, USA, 2009. USENIX Association.

[24] D. Weirich and M. A. Sasse. Pretty good persuasion: a first step towards effective password security in the real world. In *Proceedings of the 2001 workshop on New security paradigms*, NSPW '01, pages 137–143, 2001.

[25] R. West. The psychology of security. *Commun. ACM*, 51:34–40, April 2008.