User Survey on Phone Security and Usage

Frank Breitinger, Claudia Nickel

Hochschule Darmstadt*
frank.breitinger@stud.h-da.de, c.nickel@fbi.h-da.de

Abstract: Mobile phones are widely used nowadays and during the last years developed from simple phones to small computers with an increasing number of features. These result in a wide variety of data stored on the devices which could be a high security risk in case of unauthorized access. A comprehensive user survey was conducted to get information about what data is really stored on the mobile devices, how it is currently protected and if biometric authentication methods could improve the current state. This paper states the results from about 550 users of mobile devices. The analysis revealed a very low securtiy level of the devices. This is partly due to a low security awareness of their owners and partly due to the low acceptance of the offered authentication method based on PIN. Further results like the experiences with mobile thefts and the willingness to use biometric authentication methods as alternative to PIN authentication are also stated.

1 Introduction

The number of mobile phone users worldwide exceeded the mark of 4 billion last year for the first time; this means that two-thirds of the world's population use mobile phones. Especially in industrialized countries the trend is strongly towards increased usage of mobile data services [Bit09]. With growing availability of data tariffs and new functionalities, mobile internet and e-mail on mobile phones have become accessible to the masses. Modern mobile phones also allow photography, have integrated calendars or can be used as a notepad – with consistently small size. These factors have led to an increase in different kinds of sensitive data stored on the mobile phone which makes them even more attractive to thieves. [Fla06] states that 800,000 inhabitants of England and Wales have been victim of mobile phone theft between mid of 2005 and mid of 2006. This documents the need for protecting the stored information by applying secure and user-friendly authentication methods which could e.g. be provided by using biometrics.
This paper summarizes the results of a comprehensive survey about the security and usage of mobile phones. In order to reach a large and diverse group of people, the survey was realized as a printed survey and as an online questionnaire which was available for about six weeks in April and May 2010. Promotion has been made on social networks like facebook[1], different mailing lists, a gym and a physiotherapy.

*This work was supported by CASED (www.cased.de).

[1] www.facebook.com

2 Analysis

A total of 548 people took part in the survey, of which about 11% filled out the paper questionnaires. The survey has been in German. Age and gender distribution are given in table 1.
It can be seen that the majority of participants (55%) was between 18 and 30 years old. There has been a significant difference between the age of the online participants (60% were between 18 and 30 years) and the people handing in the paper questionnaires, where nearly 75% of the respondents were older than 41 years. There is no significant difference between the number of males and females through all age groups.

	< 18	18-23	24-30	31-40	41-50	51-60	> 60	unknown	sum
male	26	73	88	27	27	20	12	0	273
female	35	62	76	28	30	18	21	1	271
unknown	1	1	0	0	2	0	0	0	4
total	62	136	164	55	59	38	33	1	548

Table 1: Age and gender distribution of the participants.

2.1 Familiarity and usage

The first four questions have been about the usage of the phone in general and the familarity to the phone's features and IT security. In each case the participant could choose a value between 1 and 4, the results are given in table 2. It reveals that approximately 65% of the mobile phone owners are private users[2]. Mobile phones are important to their owners and most of them are mainly familiar with the features. Less familiar is the topic IT security. Only 19% answered, that they are familiar with this topic, nearly 15% even said they are not interested in IT security.

2.2 Using additional features

In one question participants should state which additional features they are using. They could select between SMS, e-mail, internet, camera, calendar or add further ones. In the following question the kind of stored data should be stated. Again one could choose between the proposed data (phone numbers, addresses, e-mails, appointments, birthdays and

[2]This shows the same trend as the comprehensive online survey from 2008 (see [Ifa08]).

Question	1	2	3	4	no answ.
Usage of mobile device (1 = private, 4 = business)	65.3	19.7	9.9	4.9	0.2
Importance of mobile device (1 = very important, 4 = unimportant)	36.3	39.4	20.6	3.3	0.4
Knowledge of the features of the device (1 = very good, 4 = no interest)	40.0	40.1	14.2	5.3	0.4
Knowledge of IT security (1 = very good, 4 = no interest)	19.3	30.8	33.8	14.6	1.5

Table 2: General questions about familiarity and usage of mobile devices (results in percent).

additional functionalities - Top 5	**stored data - Top 5**
1. SMS (92%)	1. phone numbers (99%)
2. camera (65%)	2. appointments (45%)
3. calendar (53%)	3. birthdays (40%)
4. internet (25%)	4. addresses (34%)
5. e-mail (17%)	5. e-mails (24%)

Table 3: Top 5 of additional functionalities and stored data on mobile phones.

passwords/PINs) or add further ones. In both cases participants were allowed to choose several answers. The top 5 of used additional features besides phoning and stored data are given in table 3. On the 6th place with 13% are *passwords/PINs*, which will be in most cases freely available in case the mobile phone is lost (see section 2.4), as only 8% of the phones containing stored PINs of passwords are sufficiently secured.

2.3 Carrying and attending the mobile phone

The answers to the question "I carry my mobile phone mainly...", show fundamental differences between men and women. One of the seven possibilities (back trousers pocket, front trousers pocket, breast pocket, pocket at the belt, back pack, hand bag, other) could be chosen. Two-thirds of men answered to carry their mobile phone in the front trousers pocket while 63% of women carry their mobile phone in their purse. See figure 1 for more details.

All respondents were asked how they take care of their mobile phone and nearly two-thirds answered their phone is *always within reach*. See figure 2 for the proposed values and the distribution of given answers.

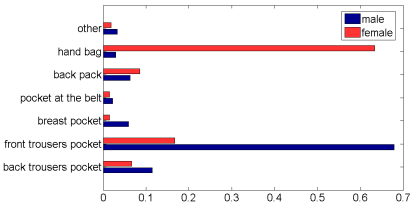

Figure 1: I carry my mobile phone mainly in my ...

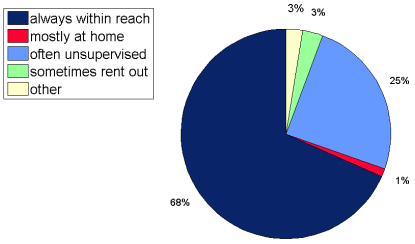

Figure 2: My mobile phone is....

2.4 Security settings

Section 2.2 showed that almost every mobile phone user saves personal data and 13% of the respondents even save passwords or PINs on their mobile devices. To see how this data is protected, the participants were asked to state which kind of action/input is necessary when using the phone after a standby phase.

Figure 3 shows the possible answers to this multiple choice question. The most common setting when reactivating the mobile phone from standby mode is keylock. Only 13% of the phones are sufficiently protected by PIN or visual code[3] which is in half of the cases combined with keylock. Comparing these answers to the ones regarding the familiarness with IT security there are some accordances. Most participants using a PIN or visual code said they are familiar with IT security (32% chose option 1, 37% option 2, 25% option 3, 5% option 4, 1 didn't answer at that question).

When asked for the reason for the low level of security (immediately usable or only key-

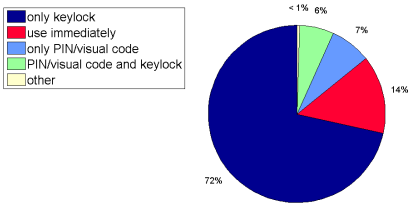

Figure 3: Security level when reactivating from standby mode.

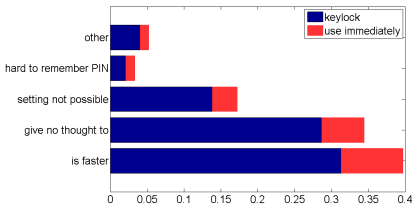

Figure 4: Reasons for the chosen low security setting.

lock) 40% answered it was chosen because *it is faster* and a further 34% answered they *did not think about it*. 17% stated that their phone does not have the function *enter PIN after standby mode*. For 3% of the participants, the PIN is too difficult to memorize (see figure 4).

Table 4 shows the willingness of the participants to use biometric authentication in total and depending on the so far chosen security setting. More than 50% are interested in an

[3] A visual code is a technique mostly used from the android operation system in which a pattern must be drawn; similar to a PIN.

would choose biometrics	total	only keylock	use immediately	only PIN/ visual code	PIN/VC and keylock	other
yes	54.4%	55.1%	51.3%	41.5%	67.7%	66.7%
no	37.8%	37.8%	38.5%	43.9%	29.4%	33.3%
not specified	7.9%	7.1%	10.3%	14.6%	2.9%	0.0%

Table 4: Willingness to use biometric authentication methods instead of the so far chosen security setting.

alternative biometric authentication process, 73% of those just use the key lock so far. If this option would be available, 55% of the participants currently using keylock and 51% of the ones which can directly use their phone after standby phase would use biometric authentication instead. This indicates that offering biometric authentication methods on mobile devices would highly increase the security of the data stored in mobile devices.

Participants which are willing to use biometric authentication, were asked which biometric modality/ies they would use. The favourite modality is fingerprint (87%), followed by speaker recognition (20%), face recognition (19%) and gait recognition (9%).

2.5 Mobile phone theft

With increasing popularity of mobile phones, also the number of thefts increases. The survey from [Fla06] showed that "4% of households owning a mobile phone have experienced a mobile phone theft". The german TNS-Emnid are talking about more than 7% in year 2008 [NM08] and our survey shows a further growth as approximately 10% of the participants have experienced a mobile phone theft, 22% of those more than once. Analysis of this survey showed that the theft rate for men is 10% higher than the theft rate for women. Four out of five participants who have had their mobile phone stolen are younger than 30. Of the participants which experienced a mobile phone theft, 75% answered their mobile phone is always within reach and 21% said its unsupervised most of the time. The locations in which the thefts occurred (see figure 5) are similar to the ones reported in [Fla06, p15-17].

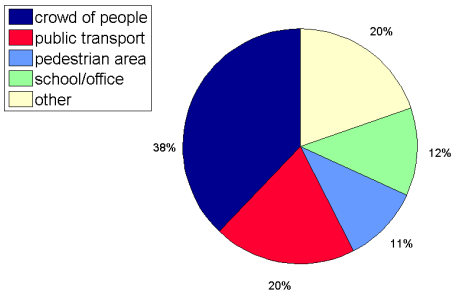

Figure 5: Locations at which mobile phones have been stolen.

3 Conclusion

As the number of mobile phones, their functionalities and application scenarios increases and hence also the amount of data stored on mobile devices, it is interesting and important to analyse the security awareness of the users which is mirrored by their chosen security settings. This paper states the result of a comprehensive survey with 548 participants. It is shown that after a stand by period only 13% of the mobile devices are secured with a PIN or visual code. This means that in 87% all data is freely available in case the phone is stolen or lost. The reason for unsecured phones is in 74% of the cases that it is faster or people did not even think about securing it. Offering biometric authentication methods on mobile phones would increase the number of secured phones as these methods would be used by about 54% of the participants. One reason for this might be that the problem of memorization and speed (see section 2.4) could be solved with biometric authentication.
Comparing the results of this survey to the ones from 2006 in [Fla06], there are still a lot of parallels. In general it is necessary to increase the user's security awareness such that he chooses sufficient security settings. This could for example be achieved by publications like the *Guidelines on mobile Phone and PDA Security* (2008, see [JS08]) by the National Institute of Standards and Technology (NIST). On the other hand configuring a PIN or biometric authentication as default setting when reactivating the mobile phone would probably also increase the number of secured phones as many people did not even think about changing the settings. In addition to the possibility of data loss because of stolen of lost phones, also attacks on mobile devices (see e.g. [HJO08]) should be considered.

References

[Bit09] Bitkom. Mehr als vier Milliarden Handy-Nutzer weltweit. http://www.bitkom.org/de/presse/62013_60608.aspx, August 2009. last checked: 2010-07-28 [german].

[Fla06] John Flatley. Mobile phone theft, plastic card and identity fraud. *http://rds.homeoffice.gov.uk/rds/pdfs07/hosb1007.pdf*, www.homeoffice.gov.uk/rds, 2005/06.

[HJO08] S.M. Habib, C. Jacob, and T. Olovsson. A practical analysis of the robustness and stability of the network stack in smartphones. In *11th International Conference on Computer and Information Technology (ICCIT 2008).*, pages 393 –398, 24-27 2008.

[Ifa08] Ifak Institut, Media Markt Analysen. Typologie der Wünsche 2009. http://de.statista.com/statistik/diagramm/studie/103676/umfrage/private-oder-dienstliche-handynutzung/, October 2008. last checked: 2010-05-19 [german].

[JS08] W. Jansen and K. Scarfone. Guidelines on Cell Phone and PDA Security. *NIST Special Publication 800-124*, http://csrc.nist.gov/publications/nistpubs/800-124/SP800-124.pdf, October 2008.

[NM08] Netzzeitung.de and Felix Magin. Das sollte man beim Handy-Verlust machen. http://www.netzeitung.de/wirtschaft/ratgeber/1099657.html, July 2008. last checked: 2010-07-28 [german].