"MY SMARTPHONE IS A SAFE!"
The User's Point of View Regarding Novel Authentication Methods and Gradual Security Levels on Smartphones

Tim Dörflinger, Anna Voth, Juliane Krämer and Ronald Fromm
Deutsche Telekom Laboratories, An-Institute Berlin University of Technology
Ernst-Reuter-Platz 7, 10587, Berlin, Germany
{tim.doerflinger, anna.voth, juliane.kraemer, ronald.fromm}@telekom.de

Keywords: Authentication methods, Gradual security levels, Smartphone security, Qualitative user research, Focus groups, Innovation development.

Abstract: This paper addresses laboratory tests regarding a graded security system on smartphones based on novel authentication methods. The main scope of this paper is the user's perception of and the need for such a system, rather than the technical dimensions of it. In November 2009 we conducted four focus groups with a total of n=19 respondents with the goal to evaluate different prototypical authentication methods for smartphones and to determine the effects such methods would have for the user's interaction with the devices. The focus groups were part of a larger research program at Deutsche Telekom Laboratories that included a web survey measuring general user preferences regarding security and smartphone usage as well as the development of prototypical authentication methods based on Google's "Android" operating system. The goal of this research was to integrate the user into the development process as soon as possible and to determine the overall acceptance of new authentication methods, such as biometric authentication, but also 2D and 3D gestures, recognition based authentication and password authentication. This paper gives valuable insights on the weakest link of the security chain: the user.

1 INTRODUCTION & FOCUS

In recent years, smartphones[1] have taken up an increasingly important part in the lives of Information and Communication Technology (ICT) users. Formerly only a gadget to business users and aficionados or "geeks", smartphones have set out to conquer the world, as current sales figures show. According to estimates from Canalys (2009), the global market for smartphones was divided into the five major device manufacturers: Nokia (39.7%), RIM (20.6%), Apple (17.8%), HTC (5.3%) and Fujitsu (3.4%) in the third quarter (Q3) of 2009. The remaining 13.2% were distributed amongst other manufacturers. Compared to Q3 figures of the previous year, this represents quarterly growth rates in world wide smartphone sales of over 4% and the market is far from being saturated. Estimates from Gartner (2009) show that by 2010 smartphone sales will make up around 37% of global handset sales. In addition, their revenue is forecast to reach $191 million by 2012, higher than spendings on mobile PCs, which is forecast to reach $152 million in 2012.

Today, a constantly increasing number of consumers use smartphones for a broad variety of tasks and purposes, ranging from telephony to instant messaging, from mobile banking to Global Positioning Satellite (GPS) based navigation. Smartphones serve as tools for organizing the users' daily lives through productivity applications such as calendars, notepads or calculators. Furthermore they are turned into multimedia toys with capabilities to play music, videos, and games or surf the World Wide Web (WWW) and take pictures using integrated cameras. Smartphones are more than just communication devices; they are mobile companions for various situations, ranging from

[1] At the time this research paper was written, no industry-standardized definition for smartphone existed. In general, smartphones are considered to be mobile phones with extended PC functionality, such as Internet access, data processing, multimedia capabilities that run on a specific operating system which allows the development of additional applications and services.

work organizers to holiday planners. But this is only the beginning. As Dilinchian (2009) acknowledges, smartphones will also "serve health, emergency services, defence, education, banking, retailing, and other sectors benefiting from information services" in the near future[2].

Smartphone users also store a vast array of different data on their devices, ranging from personal pictures to messages (email, SMS, MMS), contact lists, addresses, birthdates, music, movies and various other files, depending on the respective Operating Systems (OS) used. Smartphones can therefore be considered as light versions of computers with ubiquitous telephony functionality.

However, this trend also leads to new challenges in the field of research and development (R&D): Like desktop computers or their mobile counterparts such as notebooks or netbooks, smartphones are increasingly subject to security threats. So far, relatively little is known about viruses for smartphones but those and other types of security breaches will be of relevance in the near future. Due to the manifold technical possibilities of establishing connections to the device (UMTS, Infrared, Bluetooth, W-Lan), the data stored on these devices is increasingly at risk. In addition, smartphones can be stolen, lost or merely left at the table unnoticed in a café or restaurant. If found by a third party with malign intentions, the data on the device are usually accessible, unless the owner decided to use additional device protection mechanisms like pass codes or device locks.

According to a recent mobile security report published by McAffee (2009), the "need for additional security measures on the application, device platform and network level" arises because "mobile devices become increasingly multi-functional and are connected to other guarded and unguarded networks". This is primarily because the main security mechanism with regards to smartphone or even mobile phone usage still is the Personal Identification Number (PIN). The PIN however does not provide sufficient protection to the data stored on the devices because it authenticates the user with the network of his Mobile Network Operator (MNO) when turning on the device. After the PIN has been entered, the device remains open and if left in standby mode or constantly turned on, no other security barrier prevents third parties from accessing the device. Unless the user explicitly chooses otherwise, the default setting for smartphones is considered to be "insecure", the device itself remains like a bike lock, it is either closed or open.

An increased awareness of these issues has led some research institutes to the evaluation and analysis of security concerns from a user perspective. While technical aspects of data protection and privacy are without a doubt the final means to an end, it is of crucial importance for researchers and developers alike to get an idea of what users consider necessary with regards to their communication devices. Only then can technically adequate solutions be provided, that actually have a chance of being established on the market. Because there is still a wide gap between usability[3] and security, the combination of both concepts signifies an important challenge to researchers and developers alike. If passwords are becoming more complex[4], users might disapprove because in addition to the already existing amount of PINs and pass codes that have to be remembered regularly, e.g. ATMs, email passwords, PC passwords, etc, the objective increase in security may easily lead to a subjective decrease in usability. The longer the password, the more overburdened the user is and thus experiences a poor usability. In many cases this can even lead to by-pass strategies on behalf of the user, such as choosing the same password or PIN for different applications or services or opting for passwords that are easy to remember, such as birthdates or names. The security of devices is then threatened, because the user turns out to be the weakest link in the security chain.

In order to make life easier for the users and increase the joys of using communication devices, a solution might be to implement different security levels on smartphones for accessing different types of data or applications, thereby increasing the overall protection. If then combined with novel authentication methods, such as biometric authentication or memory-based authentication, a gradual approach to security, based on individual preferences, might make smartphone usage safer

[2] For some sectors, this is already the case. As the broad availability of mobile banking and brokerage application available for the iPhone or Android based phones show, the finance industry has already benefitted from this development.

[3] Usability, which can be described as the extent to which a product can be used with "effectivity, efficiency and satisfaction" (Iso, 1998), plays an important role in the choice of an authentication method.

[4] For example through a combination of numbers, letters (both small case and upper case) and symbols.

meanwhile maintaining a manageable level of complexity.

While more sensitive data are assumed to need more secure authentication methods, there is another dimension which has to be regarded: the simplicity and acceptance of the respective method. It is a crucial factor regarding the actual usage of these methods as smartphone owners rarely use methods which are too complex or which make them feel ashamed in public. Therefore the usage frequency as well as the usage context (e.g. being in the subway vs. being at home or in the office) of applications has to be regarded additionally when thinking about a fitting authentication method: A very complex and intrusive method may be adequate for a very sensitive and rarely used application, but users will not choose it for an even more sensitive application which they have to use very often. Thus, we believe that the OS of a smartphone should offer various authentication methods and different security levels, enabling the user to individually find an optimal trade-off solution for securing each application.

Since the sensitivity of data or applications is a subjective assessment which varies between smartphone users, we decided to address different types of users in a qualitative research project.

In order to obtain insights regarding the acceptance of gradual security as well as novel authentication methods such as biometrics[5] or memory-based authentication methods, we conducted four different focus groups in Berlin in November 2009 at our research laboratory. These qualitative findings were further validated through a web-survey with 308 smartphone users from two countries, namely Israel and Germany. The following Section 2 will describe the methodology used in the focus groups in order to evaluate novel authentication methods as well as to test the acceptance of gradual security. Section 3 will present the main findings from the focus groups and partially compare them to the quantitative findings from the web survey. The final Section 4 will then summarize and conclude by addressing the shortcomings of our approach and by highlighting directions for future research in the field.

[5] Reinhardt, Furnell and Clarke (2009) argue that, although biometric methods are well-known forms of authentication, such measures are currently not available on smartphones and are therefore considered "novel" from the user's point of view.

2 RESEARCH METHODOLOGY

2.1 Focus Groups

Focus groups are a qualitative methodological approach which is often used in product related consumer research. They can be described as moderated group discussions which are "designed to obtain perceptions on a defined area of interest (Krueger and Casey 2000: 5)", in our case the acceptance of gradual security levels and authentication methods. Focus groups are usually combined with other methods of empirical social research. They serve as an interpretative aid and are therefore not statistically representative. Such discussion groups normally consist of four to ten participants, in order to keep the moderation and the discussion on a manageable level.

The main benefit of a focus group discussion is to gain qualitative in-depth insights from different users and their perspectives at the same time. Participants have the opportunity to discuss freely and state their point as well as develop assumptions inspired by the experiences made by others. As noted by Krueger and Casey (2000), this means it is not only possible to gain individual opinions about certain products, services, etc. but also group specific tendencies. "It is important to recognize that the amount of direction provided by the interviewer does influence the types and quality of the data obtained from the group" (Stewart et al 2007: 38). In order to retrieve the desired results from such a group, moderators and observers have to be well trained to prevent the discussion from shifting in a wrong direction. The analysis of focus groups is complicated and time consuming. The usual outputs of focus groups are video documentations, voice recordings, drawings made by the participants, questionnaires and pictures. Besides these collected data, focus groups are usually conducted in a laboratory or studio with a semi-transparent "mirror-wall", allowing others behind the mirror to observe the group unnoticed.

Through conducting the focus groups we intended to unveil qualitative insights regarding current security requirements and possible acceptance of alternative authentication methods.

Because of budgeting constraints we recruited a total of n=19 participants, split across 4 groups. Table 1 gives an overview of the sample distribution:

Table 1: Overview of the focus group distribution with regards to socio-demographic criteria.

User Nr.	Sex	Age	Working Status	Number of actively used mobile phones	Children	Brand of mobile phone(s)
1	male	25-34	Student	2	No	CECT mini Motorola V3i
2	female	18-24	Student	1	No	Nokia N97
3	male	25-34	Student	1	No	Apple iPhone
4	male	25-34	Student	1	No	Palm Pre
5	male	18-24	Student/part-time working	1	No	Apple iPhone
6	female	25-34	Student	1	No	Nokia E71
7	female	25-34	Student	1	No	Sony Ericsson C902
8	female	25-34	Student/full-time working	2	No	Apple iPhone
9	male	25-34	Student/part-time working	1	No	BlackBerry Curve 8900
10	male	25-34	Full-time working	2	No	Sony Ericsson P1i
11	male	35-44	Full-time working	2	No	MDA Vario III Apple iPhone
12	male	25-34	Student/part-time working	1	No	Apple iPhone
13	female	35-44	Full-time working	2	Yes	Apple iPhone
14	female	45-54	Full-time working	2	Yes	Apple iPhone Motorola
15	male	45-54	Full-time working	1	Yes	Samsung Omenia
16	male	35-44	Full-time working	1	No	LG Cookie
17	female	25-34	Full-time working	1	No	Sony Ericsson K800i
18	female	25-34	Full-time working	1	No	Sony Ericsson K701i
19	male	25-34	Full-time working	1	No	Sony Ericsson W800i

The participants were clustered into four groups according to an internal segmentation procedure, such as parents, students, business professionals and fully employed singles and couples. After giving an overview of the types of users we recruited for our tests, we will now discuss the topics and structure of the focus groups.

2.2 Topics and Interview Guideline

In alignment with a second team of researchers responsible for conducting the quantitative web-survey addressed above we developed a qualitative and semi-structured discussion guideline which was used by the moderators in all focus groups. This guideline consisted of the following four main constituents and topics.

2.2.1 The Perceived Importance of Mobile Phones in Everyday Life

This part of the group discussion served as a warm-up and addressed the importance of mobile phones in everyday life situations of users as well as their needs with regards to the security of applications and the personal data stored on mobile phones or smartphones. The usage of PINs was also discussed.

First, we wanted the participants to describe their mobile phone usage, e.g. for which purposes, business or private, and how often they use their mobile phones. In a second step, they had to name their most frequently used applications and the types of data stored on their mobile devices. The moderator noted the respondents' reflections on big post-its and collected them on a flipchart together with a scale measuring the sensitivity of the applications and data from 1 to 6. The value 1 represented "high sensitivity", 6 "low or no sensitivity" [6]. The participants then had to rank the different mobile applications and data according to this scale based on a group consensus. After the ranking the users discussed their awareness of the risks of insufficiently secure authentication methods as well as the security level of PINs.

2.2.2 Alternatives to PIN-based Authentication

The second part of our moderated group discussion dealt with the participants' experiences with authentication methods alternative to the PIN. We asked them to name all authentication methods they had heard of or had already personally tried. The participants' reflections were again collected on a flipchart.

2.2.3 Demonstration of Different Authentication Methods

In the third part the participants had the opportunity to evaluate different novel authentication methods presented by the moderator. After testing each method they had to discuss the benefits and shortcomings of each one. We presented the following eight different methods:

- Fingerprint Authentication
- 3D Gesture Recognition
- Retina Scan
- Activity Based Verification
- 2D Gesture Recognition
- Recognition Based Authentication
- Speaker Recognition
- Face Recognition

To minimize the risk of ranking effects we varied the order in which the methods were presented in the four different groups. Each authentication method was presented on its own

[6] "Very sensitive" meant that the users would very much want to prevent unauthorized use of application and access to data and "Not sensitive at all" meant that they would not mind unauthorized use.

along with typical usage scenarios. Afterwards, the participants discussed the single methods in terms of their subjective feeling of guaranteed security, usability, convenience and intention of future usage.

After all eight authentication methods were presented and discussed, the participants again ranked them on the same 6-point scale. This time the values represented the perception of the guaranteed security provided by the methods. 1 meant that the authentication method provided a "very high" and 6 a "very low" level of security.

2.2.4 Concluding Discussion

In the concluding part of our focus groups we then re-evaluated the rankings on both scales and compared them with each other. This gave us the opportunity to directly match the perceived sensitivity of applications with the expected security of novel authentication methods and thereby gain insights on whether a graded security system should be provided together with different authentication methods. The overall goal was to find out whether some authentication methods were more suitable than others for a graded security system and which types of data fit best together with which type of authentication method.

2.3 Demonstrator Showcases

At the time we conducted the focus groups, no available technology existed on the market that combined gradual security with alternative authentication. We therefore had to use different methodological approaches to demonstrate the various knowledge- and biometry-based mechanisms. This section describes the different authentication mechanisms in more detail.

Fingerprint Authentication is authentication based on the patterns of the human fingertip. We presented this method using an integrated fingerprint reader on a *Lenovo* notebook. In each group two participants were requested to register into the system with their fingerprints and then log in using the fingerprint reader. After a successful login the un-registered participants were asked to log into the system as well but ultimately failed in doing so.

3D Gesture Recognition is a method with which users can authenticate themselves through gestures made in "free air" using the motion detectors integrated into a broad variety of smartphones. Because our 3D Gesture demonstrator was being updated at the time, we used the analogy of *Nintendo*'s Wii controller to explain the idea.

Retina or Iris Scan is a biometric mechanism which authenticates users through scanning the human eye using the mobile phone's camera. In order to explain this approach, pictures from a technology fair presentation were used, as currently no publicly available end device with such a technology exists.

Face Recognition, a method we also discussed with the respondents, is authentication based on the recognition of the user's face through the camera integrated into the mobile phone. This concept was explained together with Retina Scan authentication.

Activity Based Verification is based upon password authentication. But in addition to a password, the system also authenticates the user according to the rhythm, speed and pressure of the individual keystrokes. This method was presented on a notebook. The technology itself was developed by our engineers. In order to train the system the users had to type in their passwords ten times. After that, the registration was completed allowing the participant to successfully log in. The other group members who all knew the password were requested to also log in but all of their attempts were to no avail, mainly because the user-specific way of stroking the keys could not be copied.

2D Gesture Recognition allows authentication through a gesture drawn on the PC touchpad or smartphone touchscreen. Authentication is achieved through knowledge of the gesture itself but also through the pressure on the touchpad and the speed applied for "drawing" the gesture. This mechanism was also presented with the help of a demonstrator installed on a *Lenovo* notebook.

The **Recognition Based Authentication** method works through selecting points on a picture in a specific order as an alternative to the PIN with a higher security level and better usability. The picture can be chosen by the user and thus be a portrait of family members or pets, for example. We demonstrated this mechanism using an Android-based application on the G1 smartphone, developed by our engineers.

The final authentication method we presented in our focus groups was **Speaker Recognition**. This method is based on recognition of the speaker's voice using the microphone integrated into the mobile phone. To visualize this biometric approach we showed a video sequence of "A Space Odyssey" where a man is requested to authenticate himself by saying his name and destination before entering a spaceship terminal.

It has to be taken into account that the evaluation of a product or prototype can be influenced

depending on its respective quality at the time of the users interaction with it. In our case we could not notice a significant bias in the evaluation of the security levels of each technology because the users were generally able to abstract between the quality of the technology at hand and the perceived future benefits of it with regards to improved security.

2.4 Evaluation of the Data Obtained

All focus group sessions were recorded both on audio and video using HD portable cameras and MP3 voice recorders. In addition, a student assistant protocolled each session. After all focus groups were concluded, the interviewers as well as the keepers of the minutes jointly evaluated both the video and audio files and cross-referenced them with the written notes to check whether there were variations between video/ audio material, minutes and the perceptions of the interviewers. After the findings were written down in a research report, we conveyed the results to the colleagues responsible for the technical setup of the prototypes and demonstrators. They re-evaluated our findings, commented and added their impressions in order to finalize the report. In addition, the respondents' demographic information surveyed at the end of the focus groups through a three page questionnaire was evaluated by a student worker using Microsoft Excel.

3 RESULTS AND FINDINGS

3.1 Focus Group Results

3.1.1 Evaluation of Authentication Methods

Our evaluation of the focus groups clearly showed that users make distinctions between the perceived security of the authentication methods presented, their perceived convenience as well as the future likelihood of use. Besides focussing on group differences we also analysed whether gender-related distinctions could be unveiled. After our test persons were shown the different demonstrators described in subsection 2.3, a group discussion was initiated by the moderator, addressing the weaknesses and benefits of each method. Adjacently, each respondent individually evaluated the authentication methods using a valence method based on smileys[7]. The results were ranked by us, according to the respective frequency of the users' replies.

Table 2: Respondent agreement (ranked) to statement: "I think this authentication method is secure".

Retina Scan	100%
Fingerprint Authentication	95%
Speaker Recognition	68%
Face Recognition	64%
Activity Based Verification	63%
2D Gestures	63%
3D Gestures	42%
Recognition Based Authentication	37%

Table 3: Respondent agreement (ranked) to statement: "I think this authentication method is good".

Fingerprint Authentication	89%
2D Gestures	68%
3D Gestures	53%
Activity Based Verification	53%
Recognition Based Authentication	47%
Speaker Recognition	47%
Retina Scan	37%
Face Recognition	27%

Table 4: Respondent agreement (ranked) for statement: "I think I would use this authentication method".

Fingerprint Authentication	95%
2D Gestures	63%
Recognition Based Authentication	47%
Activity Based Verification	42%
3D Gestures	37%
Speaker Recognition	37%
Face Recognition	27%
Retina Scan	26%

One of the major insights we discovered was that the perceived security of an authentication method does not necessarily correlate with the overall acceptance of the method or the willingness of use, as the tables above show: The findings presented here highlight that, with regards to the users' perceived sensitivity,

[7] Valence is an affective evaluation of approval/ disapproval, or like/ dislike. The respondents could state whether they liked a method, perceived it to be secure or whether they intended to use it based on a "happy" and "sad" smiley.

biometric authentication clearly outperforms all the other methods presented. This was not only revealed through the valence method, but also mentioned manifold in the moderated discussion itself. Our respondents perceived biometric authentication to be the most secure[8]. For example, one user commented that biometric authentication is "much easier because you can't forget it. You always have your finger, eye or voice with you". However, this did not automatically mean that the same users also perceived the method as good. Concerning Speaker Recognition for example, it was stated that "it's strange to talk to the phone." and "I wouldn't use it in public". In addition, the perceived security does not indicate a willingness of use, as a comparative analysis of tables 2 and 4 shows. Even though all users in the sample (100%) opined that Retina Scan was the safest method ("pretty secure"), only 37% liked the method as such and even less (26%) actually stated that they would like to use it in the future. Amongst others, reasons given by the users were: "Embarrassing! It looks kind of strange, a bit like James Bond…" and "Not feasible". On the other hand, methods that were perceived as secure by approximately two thirds of the sample such as 2D Gestures (63%) ranked second highest with regards to acceptance (68%) and willingness of use (63%) "It's very intuitive". The only (biometric) authentication method that performed equally well in all three categories was Fingerprint Authentication with a perceived security of 95%, an overall acceptance of 89% and a willingness of use of 95%. For R&D departments and those dedicated to developing future authentication methods or security related applications, this is a remarkable finding. With regards to gender related differences, we discovered that male and female users had quite different opinions on the presented authentication methods, as is summarized in the following tables:

Table 5: Gender related differences in overall acceptance of authentication method.

Authentication method	Overall acceptance	
	Female	Male
Fingerprint Authentication	100%	82%
3D Gestures	75%	40%
Retina Scan	37%	40%
Activity Based Verification	50%	55%
2D Gestures	75%	64%
Recognition Based Authentication	63%	36%
Speaker Recognition	50%	45%
Face Recognition	50%	14%

Table 6: Gender related differences with regards to perceived security of authentication method.

Authentication method	Perceived Security	
	Female	Male
Fingerprint Authentication	100%	91%
3D Gestures	63%	27%
Retina Scan	100%	100%
Activity Based Verification	75%	55%
2D Gestures	75%	55%
Recognition Based Authentication	50%	30%
Speaker Recognition	63%	73%
Face Recognition	75%	57%

Table 7: Gender related differences with regards to future willingness of use of authentication method.

Authentication method	Intended Usage	
	Female	Male
Fingerprint Authentication	100%	91%
3D Gestures	63%	18%
Retina Scan	37%	18%
Activity Based Verification	37%	45%
2D Gestures	63%	64%
Recognition Based Authentication	63%	40%
Speaker Recognition	37%	36%
Face Recognition	50%	14%

The main finding regarding these different opinions is that our participating women showed a considerably greater affinity to new authentication methods than the male ones, regarding the perceived security, the perceived convenience as well as the future likelihood of use: Apart from Speaker Recognition, women perceived every method as more secure than men. The same trend can be identified regarding the perceived convenience: Whereas seven out of eight methods were perceived as good by at least 50% of the women, only three of them were accepted by the men to that extent. These

[8] As our respondents mentioned one reason for the perceived security of biometric and specifically Retina Scan Authentication is the constant promotion of this security in various science fiction movies.

findings result in the fact that for five out of eight presented methods more than half of the women stated that they would use it. Only two authentication methods achieved a comparable percentage in the men's judgement. Particular attention should be paid to the methods 3D Gestures and Recognition Based Authentication which explicitly revealed a great difference between genders: Whereas only 18% respectively 40% of the male participants intended to use these methods if possible, nearly two thirds of the women quoted that they could imagine using them. Similar numbers hold for the perceived security and the overall acceptance: At most one third of the men perceived the respective methods as secure, whereas at least 50% of the women opined that they were secure. The overall judgement also differed between genders: At most 40% of the men liked these methods, compared to at least 63% of the women[9].

3.1.2 Evaluation of graded Security Concept

Besides evaluating the perceived security, acceptance and usage intention of novel authentication methods, our test persons also had to discuss the concept of gradual authentication for different types of data and applications. With the help of the 6-point scale described in subsection 2.4 we asked our respondents to first list all the applications they use and then discuss the respective sensitivity of each application or data on a group level. In most cases, the test persons in each specific group mostly agreed on the same sensitivity level. The differences between the groups however were quite obvious. For business users emails were considered to be a lot more sensitive than for students and younger users. These users, on the other hand, considered personal pictures or videos stored on their devices to be more sensitive than others and the group of parents considered applications and data unsuitable for children to be amongst the most sensitive types.

Based on the discussions within the different groups we discovered that in general, the idea of gradual security was perceived as useful by all test persons. However, the individual requirements as to how this system should work varied greatly, revealing an overall need to customize the system ("I'd really like to have the choice"). For example the test users mentioned that they would like to decide for themselves which data should be assigned to which security level, rather than using previously configured settings ("it should be possible to configure the security settings individually right at the beginning as you can do it with the internet explorer, for example").

Regarding group differences, the business users specifically mentioned the need for authentication methods with high security standards that synchronistically have a low impact on the workflow with the device ("it simply has to stay feasible"). For the majority of the other "non-business" users, usability and practicality were more important than security aspects even after the awareness of possible risks was increased through the group discussion. The idea of having a gradual security system with different authentication methods was favoured most by parents because it allows sharing one smartphone among family members without having to bother about private data or cost-intensive applications (e.g. a child pressing a button and calling an international phone number, thereby increasing the phone bill).

The most prominent findings explicitly but also implicitly stated by the users with regards to such a graded security system were that [1] people should feel more secure without constantly having to bother with authentication. The authentication methods therefore should have a high degree of usability. [2] In general, it can be stated that the need for improved security automatically arose with the awareness of the risks of smartphone usage with regards to data leakage, data theft or privacy threats and that device manufacturers, OS developers or MNOs should work on concepts to deal with these increasing threats. [3] Since the way in which people interact with their devices varies greatly over different consumer segments, developers should address this issue by providing pre-configured and segment-specific solutions that could then be customized further if the default settings do not already fully meet the specific user needs. [4] A final and useful remark was that there should always be some kind of "backdoor" similar to the PIN/ PUK approach, no matter how secure the other authentication methods would be. To better explain this remark, a focus group respondent gave the examples of a sore throat or a blister on the fingertip, interfering with the authentication on the device and thereby rendering it "unusable".

[9] With regards to the methods Retina Scan and Face Recognition we also discovered that the majority of our participating women would refrain from using these biometric methods because of expected health concerns ("It hurts the eyes") whereas the male respondents mainly named usability and feasibility aspects as the main counterarguments for a future use of these methods.

3.2 Quantitative Cross-validation

In order to give our qualitative findings more "weight" with regards to the perceived security of the novel authentication methods, we had the findings cross-validated through an international web survey conducted by our colleagues based on the same questions. The survey was in English and a total of n=308 respondents participated. The gender distribution across the quantitative sample was 45% female and 55% male. 14% had separate phones for business and private purposes. A sample distortion led to the uneven distribution of approx. 75% Israeli respondents and 25% German respondents.

Since we used closed answers for the questionnaire, the results can not be compared to the qualitative findings, which are based on "open answers". In addition, the respondents in our survey were only confronted with written descriptions of these authentication methods. This however was not a problem per se, since we did not aim at obtaining statistically representative and comparative results but merely on capturing a glimpse of the "bigger picture". The 6-point Likert scale used in the web survey shows similar tendencies regarding the perceived security of smartphones. In the web survey biometric authentication methods were also perceived to be the most secure with Fingerprint Authentication holding the pole position. Just like in our focus groups, 2D and 3D authentication methods were rated the least secure in comparison to the other methods discussed in the web panel. The following chart gives a comparative overview:

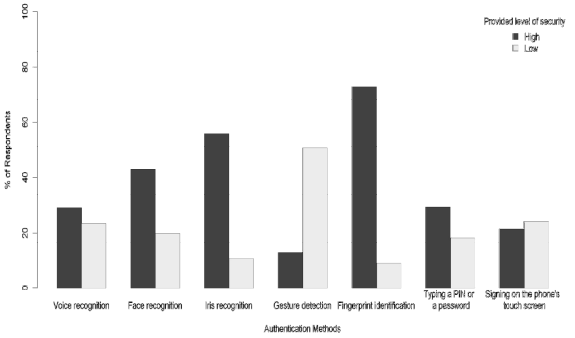

Figure 1: Security of authentication methods as perceived by participants (n=308) of an international web survey.

The six possible answers were grouped together into tendencies, with the two highest values, i.e. "6= very secure" and "5= quite secure" grouped together to "high security" as well as the two lowest values, "1= not secure at all" and "2= not very secure", being grouped together to "low security".

4 CONCLUSIONS

As an overall conclusion we can state that we revealed useful insights for R&D personnel, even though the sample size of our research was low and the findings therefore not representative. In general, the test persons agreed that gradual security is a useful concept and that it would help to improve the security of personal data and information stored on smartphones or mobile phones. The test persons also agreed that the PIN as the only standardised authentication method does not sufficiently protect the personal data stored. With regards to the overall acceptance, intended usage and perceived security, the findings show that out of all biometric authentication methods, only Fingerprint Authentication was fully accepted in all three categories. The idea of combining a gradual security system with different authentication methods however did not meet with great approval. Merely a few of the test persons favoured the idea of combining low sensitivity data with lower security mechanisms and high sensitivity data with very secure mechanisms. The majority of the test persons had the opinion that it was best to use high security mechanisms for all types of data, in order to increase the overall security of the device rather than using different security levels. This position was supported by the fact that the seemingly most secure method, Fingerprint Authentication, was perceived as the most usable as well.

As always the fact with qualitative data, results have to be interpreted carefully. We were able to obtain in-depth insights concerning our gradual security approach as well as on the weaknesses and strengths of novel authentication methods which we would not have been able to obtain to the same extent through a quantitative approach. With regards to new and innovative ICT products and services, qualitative approaches, implemented at an early stage in the development process, are valuable as they can give hints and directions to researchers and engineers alike. They should then, at a later stage of the process, be backed up with more "solid" quantitative figures but also retested qualitatively in an iterative development process. Our web-panel with a total of n=308 participants gave additional input but lacked statistical representativity. The sample size was too low and unevenly distributed among only two countries. The quantitative results briefly discussed in this paper nonetheless show that the opinions obtained in the focus groups were mostly shared by users, who were not able to actually test the demonstrators themselves. This

shows that the qualitative results can not merely be attributed to the specific group characteristics but possess a higher validity because they are shared by larger user numbers.

For future research going into a similar direction we would recommend, based on the experiences gathered from our work, to further increase the sample size and more strongly focus on cultural differences regarding user requirements and needs. It is also advisable, especially when technology is to be properly evaluated, that user research experts team up with engineers and developers, to get the most out of research approaches of this kind: namely user insights that are directly translated into technical requirements and guidelines for development.

The quality of the results also depends greatly on the quality and reliability of the technologies or demonstrators presented to the users. It would be interesting to see how and to what extent opinions might change with products ready or almost ready for market launch. The same holds for the duration and the intensity of the test: Whereas the participants of our focus groups could not really experience the different authentication methods over time but merely test or imagine them, their judgement might differ if those methods were already implemented on a smartphone. For this reason, the development of novel authentication methods has to be advanced. With regards to our initial research hypothesis, namely that smartphones should provide different security layers (graded approach) combined with different authentication methods, we can state that, based on the findings discussed in this paper, this does not seem to be the case for our respondents. Both dimensions of our concept were considered practical, useful and good on individual accounts. A combination of both was considered to be impractical. This leads to the further research question of how different security layers can be achieved without different authentication methods.

In the course of our group discussions we could discover that even if there is a light awareness of possible security threats most of the respondents did not really think about them or their possible consequences. However, it was remarkable that this awareness grew during the discussion with other users. This finding may indicate that there is a lack of information concerning security threats among users. In order to bring new security mechanisms for smartphones forward, user education concerning security threats also has to be taken into account.

ACKNOWLEDGEMENTS

Special thanks go to Mr. Niklas Kirschnik and Mr. Hanul Sieger, both PhD candidates at Deutsche Telekom Laboratories and Berlin Institute of Technology for providing the demonstrators and showcases during the focus group sessions and for giving advice with regards to the interview guideline. They were also our “troubleshooters” during the focus groups, assuring that all demonstrators operated smoothly at all times. In addition, we would also like to thank Prof. Joachim Meyer and Noam Ben-Asher from Ben-Gurion University of the Negev, Israel for conducting the quantitative survey referred to in sub-section 3.2 and for providing us with the data and the chart used in figure 1 to further back the insights from our focus groups.

REFERENCES

Canalys, 2009. Smartphone market shows modest growth in Q3, Canalys research release 2009/112. URL: http://www.canalys.com/pr/2009/r2009112.htm, Last checked: 2009/12/04.

Dilanchian, 2009. Smartphone statistics and links. URL: http://www.dilanchian.com.au/index.php?option=com_content&view=article&id=577:smartphone-statistics-and-links&catid=23:ip&Itemid=114, Last checked: 2010/01/13.

Gartner, 2009. Gartner Says PC Vendors Eyeing Booming Smartphone Market. http://www.gartner.com/it/page.jsp?id=1215932, Last checked: 2010/01/22

International Organization for Standardisation ISO, 1998. Ergonomic requirements for office work with visual display terminals ISO 9241-11.

Krueger, R. A. & Casey, M. A., 2000. Focus Groups: A practical guide for applied research, 3rd Edition. Sage: Thousand Oaks, California.

McAffee, 2009. Mobile Security Report 2009. URL: http://www.mcafee.com/us/local_content/reports/mobile_security_report_2009.pdf. Last checked: 2010/01/13.

Reinhardt, A. b., Furnell, S. M. & Clarke, N. L., 2009. From desktop to mobile: examining the security experience. In: Computer & Security, pp. 130-137.

Stewart, D. W., Shamdasani, P. N. & Rook, D. W, 2007. Focus Groups: Theory and practice. Sage: Thousand Oaks, California.