On the need for different security methods on mobile phones

Noam Ben-Asher
Department of Industrial Engineering
Ben Gurion University,
Beer Sheva, Israel
noambena@bgu.ac.il

Hanul Sieger
Quality and Usability Lab,
Deutsche Telekom Laboratories
TU Berlin, Berlin, Germany
hanul.sieger@telekom.de

Asaf Ben-Oved
Department of Industrial Engineering
Ben Gurion University,
Beer Sheva, Israel
asafbo69@gmail.com

Niklas Kirschnick
Quality and Usability Lab,
Deutsche Telekom Laboratories
TU Berlin, Berlin, Germany
niklas.kirschnick@telekom.de

Joachim Meyer
Department of Industrial Engineering
Ben Gurion University,
Beer Sheva, Israel
joachim@bgu.ac.il

Sebastian Möller
Quality and Usability Lab,
Deutsche Telekom Laboratories
TU Berlin, Berlin, Germany
sebastian.moeller@telekom.de

ABSTRACT
Mobile phones are rapidly becoming small-size general purpose computers, so-called smartphones. However, applications and data stored on mobile phones are less protected from unauthorized access than on most desktop and mobile computers. This paper presents a survey on users' security needs, awareness and concerns in the context of mobile phones. It also evaluates acceptance and perceived protection of existing and novel authentication methods. The responses from 465 participants reveal that users are interested in increased security and data protection. The current protection by using PIN (Personal Identification Number) is perceived as neither adequate nor convenient in all cases. The sensitivity of data stored on the devices varies depending on the data type and the context of use, asking for the need for another level of protection. According to these findings, a two-level security model for mobile phones is proposed. The model provides differential data and service protection by utilizing existing capabilities of a mobile phone for authenticating users.

ACM Classification Keywords
H.4 Information Systems Applications: Miscellaneous; D.4.6 Operating Systems: Security and protection—*Access controls, authentication*

General Terms
Human Factors, Security, Authentication.

MobileHCI 2011, Aug 30–Sept 2, 2011, Stockholm, Sweden.

Author Keywords
Authentication methods, graded security model, mobile phone security, data protection, survey.

INTRODUCTION

The mobile phone has become an inseparable companion for many users, serving for much more than just communication. It is a multi-purpose device which fulfills important functions in the user's personal and professional life [4]. In parallel, the storage capabilities of mobile phones increase rapidly, and phones can today generate and store large amounts of different content types (documents, mails, visual and audio media, databases, etc.). All and all, mobile phones resemble in their capabilities personal computers or netbooks with embedded telephony capabilities. However, one of the aspects in which mobile phones lag behind is security and data protection [15]. Conventional protection provides only a one-time verification system upon switch-on: unless locked, the device is always open; and automatic locking of the device is usually not the default setup on the phones of the top 5 vendors [10]. Many users keep their devices unsecured as they perceive the usage of a phone PIN (not the SIM PIN) as inconvenient [24].

Lately, the security industry, device manufactures and researchers identified the increased need for mobile phone security. The annual survey of the Computer Security Institute, which focuses on security in companies and organizations of different sizes, mentioned in 2008 for the first time the security incidents "Theft/loss of proprietary information from mobile devices" and "Theft/loss of customer data from mobile devices". The 2009 report reveals that 42% of the respondents experienced "laptop and mobile hardware loss or theft" and 12% of these cases lead to data breaches [17]. McAfee report [16] emphasizes the need for additional security features and the key role of device manufacturers and service providers in the implementation of security features. However, the report states that there is very limited past experience with security incidents, which makes the prevention

of future attacks difficult. Some ongoing research deals with the implementation of security mechanisms and various authentication methods in mobile phones (e.g. [9]). The transfer of security concepts and features from the desktop environment to mobile phones turns out to be far from trivial, and it encompasses numerous challenges resulting from usability and security tradeoffs [2]. A successful implementation of authentication methods in mobile phones relies on achieving acceptable false rejection and false acceptance rates, an objective that has yet to be achieved [5].

In most cases, the only security mechanism in mobile phones is a PIN, usually a 4 digit code. It is used to identify the user in the network when the device is turned on, but it can be also be used to lock the keypad (the code can be different). Similarly to passwords, the use of PIN codes suffers from numerous usability and security problems. The drawbacks of passwords are mostly due to authorized users selecting simple or guessable combinations (e.g. their birth date), sharing the password, using the same password for multiple purposes and accounts or even writing it down [3, 18]. Furthermore, users tend to activate their device and keep it active for long periods of time (more than 10 hours a day) [4]. Thus, in many cases, mobile phones are left unprotected and unsecured for long periods of time. The small size and the high cost of the devices make them susceptible to loss or theft. The large amount of mostly unprotected data stored on the device puts the user at risk [2]. This risk is amplified by lack of awareness and the appropriate security mechanisms to mitigate it.

In order to provide additional levels of security as well as other authentication methods a mobile phone must have the underlying operating system (OS) capabilities and the apropriate hardware. In this regard smartphones already provide an adaptable OS. We define a smartphone as a mobile phone with a programmable operating system (meaning the OS vendor provides a Software Development Kit) and the possibility to add new software applications and data content in different formats.

Our study aims to provide insight on user preferences for a future mobile phone with a graded (multi-level) security mechanism and the use of alternative (biometric) authentication methods. Graded security is achieved through two complementary concepts. The first is assigning different levels of security to different applications and content, and the second is matching each security level with a single authentication method or a combination of several methods. For example, to secure the SMS application a PIN might be enough but access to the e-mail requires PIN and fingerprint authentication. The main questions are:

- Which authentication methods are preferred?
- Which alternative (biometric) methods are favored in comparision to the PIN?
- What data is considered as sensitive to get an "extra-level" of security?

As the basis for the new approach to mobile phone security proposed here, we used the survey to collect information on questions, such as whether it makes sense to have multiple levels of security and whether users differentiate in the sensitivity of data types stored on their devices or functions the devices provide. An additional question that will be addressed is how mobile phone users perceive authentication methods from usability and security perspectives. The answers to these questions are discussed in view of the results from previous surveys and with respect to the proposed model. Finally, we conclude on users' needs with respect to a multi-level security model and possible adaptation of authentication methods.

SECURITY, USABILITY, AND CONVENIENCE

"Balance is the key to all security efforts.[...] Unless you stand over them with a loaded gun, users will disable, evade, or avoid any security system that proves to be too burdensome or bothersome." [24] It may not seem to be too exaggerated as a recent study on password security has shown [11]: Roughly 1% of the analyzed 32 million passwords used for a web service were simply "123456", and "almost all of the 5000 most popular passwords, that are used by a share of 20% of the users, were just that – names, slang words, dictionary words or trivial passwords (consecutive digits, adjacent keyboard keys, and so on)." [11].

As cited above, the key for appropriate security behavior is to balance usability and security. Additional finding of the study on passwords [24] is that a significant amount of users either do not know the concept of secure passwords or do not care. Convenient passwords are easily attacked with brute force, but still offer some advantages over not using passwords at all. A device, its data, or its application might be secured against a "casual" and unprofessional attack by children, spouses, friends, co-workers etc.

We assume, that in the context of mobile phones users show a similar behavior, whereby the security mechanisms of a smartphone (and mobile phones in general) are to be considered even weaker than the security mechanisms of web services (or computers in general). A 4-digit PIN is easier attacked or even guessed, than, for example, an 8-character password.

Authentication methods on mobile phones

Identification and authentication methods are usually divided into three main areas: knowledge-based authentication (e.g., passwords, PINs etc), token-based authentication (e.g., smart card, USB dongle, etc.), and biometric authentication (e.g., fingerprints, iris scans, etc.). While knowledge-based and token-based authentication methods are used on a regular basis by many people around the world, biometric authentication methods are at least known to exist (fingerprint and iris recognition in movies etc.) by a part of the users. Biometric authentication methods are often seen as having advantages over other methods, because no password has to be remembered, no token or written-down note can be lost or stolen, and biometric methods are harder to "crack" [12].

We do not consider token-based methods here, as the hardware constraints of mobile phones do not favor them at the moment. Tokens like USB dongles or smart cards require connectors or readers, which are not implemented yet while other methods can take advantage of functions that are already built into mobile phones. We also do not consider mobile phones used *as* tokens.

Currently available smartphones most commonly use the following security feature: a 4-digit PIN to secure access to the SIM card or to lock the device. A few devices introduced character-based passwords or recognition-based gestures (e.g. Android-based devices).

Knowledge-based methods

Personal Identification Number (PIN): This method is probably most commonly used for authentication on devices in question here, i.e. mobile phones. The common variant consists of a 4-digit pass-code to be entered via a keypad.

Passwords: Passwords are very well known for a lot of logon processes, being it a personal computer or a web service. Passwords need a character-based input device, this probably prevented them to be widely used on mobile phones, which most commonly offer a keypad only. There are example devices (with full keyboards) as the RIM Blackberry Bold, which allow for passwords with 4 to 14 characters (and password rules).

Recognition-based passwords: These "passwords" are not based on character or digit input and less common to be found. They involve to (re-)draw a pattern, to select parts of a picture in a certain sequence, or to substitute PIN-numbers with pictures. As this method is (in part) implemented in the Android operating system, it may see some rise in use in the future.

Biometric methods

We can assume from former research, that users are interested in convenience [24]. Every interaction, which "destroys" the work flow and/or takes up too much time, can be assumed as to be "too burdensome or bothersome". In this regard it is obvious, that some (biometric) methods are not very well suited for mobile devices, if we consider usability (and hardware constraints) [12].

For example, palm-print, hand vascular, and hand or ear geometry recognition cannot be implemented due to size requirements. Gait recognition is implausible, because this would require to walk in a certain distance from one's own mobile phone to be captured by its camera (mobile phones are usually carried in pant pockets, jacket pockets or handbags, making gait recognition by motion sensor unsuitable). The same goes for any 3D object recognition as it either depends on considerable hardware or would be hard to use alone. Signature verification needs a relatively large input area, but this could be possible on today's smartphones.

This still leaves a lot of methods to be considered as potentially usable biometric authentication methods on mobile phones: fingerprint recognition, face recognition, iris recognition, speaker recognition, 2D and 3D gesture recognition, and continuous biometrics or activity-based verification (e.g. typing pattern).

Biometric authentication methods already implemented on mobile phones

Speech recognition is already available on smartphones, but it is mainly used as an interface, not as an authentication method. There were and are, very few mobile phones available that offer other security methods than a 4-digit PIN. Examples of commercially available devices are several models by Fujitsu, e.g. FOMA F905i (released in 2008) with a fingerprint swipe-sensor on the backside, and Sharp 904SH (released in 2006), which uses its front-facing camera for face recognition. Both example devices were released on the Japanese market only.

At the time of writing, in the U.S. and European market, only few mobile phones provide additional security levels other than SIM PIN or phone lock. The LG eXpo GW820, a Windows Mobile 6.5-based model incorporating a fingerprint swipe sensor, which can secure access to the phone and individual applications and data and the Motorola Atrix 4G (expected release on February 2011).

RELATED WORK

Several surveys dealt with the security needs of mobile phone users and attitudes towards various authentication methods. Regarding the security needs of business professionals, a survey with 230 respondents revealed that 31% of them store sensitive work-related data on the device. Furthermore, 81% of them consider the information on their Personal Digital Assistant (PDA) to be between "somewhat" and "extremely" sensitive and 69% of them were willing to pay more for a secured PDA [21].

Clarke and Furnell [4] found that among the factors which are considered when selecting a handset, security features reached the second place after battery life. In the same survey 85% of respondents were in favor of additional security and protection for their mobile phone. These findings are consistent with the findings of a survey conducted later by Kowalski and Goldstein [14] which found that about 70% of the 97 respondents were interested in increased security for mobile phones.

These surveys also assessed the usage of PIN authentication among mobile phone users. In some of them separate questions were asked regarding PIN usage. In general, it seems that the percent of users who know about the ability of the PIN to protect their handset is increasing, from 56% who use PIN in 2002 [6] to 66% [4] and 82% [14] in 2005 and 2006, respectively. One of the qualities that is frequently attributed to PIN is inconvenience; 41% of the respondents in an early survey felt that entering a PIN is inconvenient [6]. However, from later surveys it seems that the attitude towards PIN is changing with only 30% [4] and 15% [14] of the respondents stating that PIN is inconvenient. Still, the last survey was conducted among 97 information security students and

this might have contributed to the low rate of negative responses regarding the convenience of PIN. Bearing in mind the purpose of the PIN mechanism, the researchers in these surveys asked about the perceived level of protection it provides. Again, the findings are inconclusive. Some findings indicate that the PIN is not perceived as efficient in the prevention of misuse (41% in [6]), while in other surveys a relatively high percentage of respondents reported that the PIN provides adequate protection (42% in [4]) or that they trust the protection it provides (54% in [14]).

In the context of mobile phones, biometric authentication methods are frequently proposed as an alternative to the PIN. Some methods, such as fingerprint and face identification, are already used in different contexts, others, such as ear geometry identification, are unique to mobile phones. In general, biometric authentication is perceived as a good idea by the majority of mobile phone users [4]. However, not all methods are likely to be accepted and adopted by users. Fingerprints (74%), voice print (55%) and iris identification (41%) were positively rated in a previous survey [6]. The same three methods were also perceived to be the most likely to be used in the future by 80%, 70% and 53% of the respondents, respectively [4]. Other methods, such as face identification and keystroke analysis, received low scores for the above two measurements. The familiarity with the authentication method and the performance of the authentication method in terms of false acceptance rate and false rejection rate are important acceptance predictors, along with other usability aspects of the authentication methods [5].

GRADED SECURITY

Graded security can be seen from two different perspectives: First, as a role-based hierarchical system to provide access to certain areas of the secured device, where access is defined by user-based roles (e.g., from guest-user to super-user). Second, graded security can be seen as a content-based system, where access to specific content is secured by access to this content alone. The user has to provide authentication to get access to content, but there is no overlap to other content. Each content has to be accessed individually. This is in contrast to the super-user, who can access everything on the system once authentication is passed. Of course, both approaches to graded security can also be combined.

Systems using a graded method of security to access defined areas are in common use, and we can expect that users are accustomed to the concept. Especially in the area of computers, graded security has been in use for a long time (at least since the MULTICS operating system), even on consumer-oriented products (e.g., networked and mobile computers). For example, on a networked computer the user gains access by providing a password, for further access to network-based functions he may be prompted to provide another password (or the same again). On mobile computers the user may need to provide a password or a fingerprint scan to start the device beyond the BIOS routine, and then provide further authentication when to log into his or her user account. If the computer connects to the Internet, users almost always require providing authentication to access certain web sites, being it an e-mail account, a web shop, or a banking account.

Thus, we can expect to a certain degree, that users are aware of the concepts of graded security.

METHOD

With these considerations about (biometric) security methods and graded security in mind, we come back to the three main questions. In order to gain first insights into user preferences for biometric authentication methods and graded security on mobile phones, we had a two-fold approach: focus group discussions [22] and a web survey to cross-validate the results.

The aim of the current survey was to assess mobile phone users' general security needs, the possible acceptance of different authentication methods and the perceived sensitivity of content stored on the device and functions it provides. The survey collected data on the respondents' usage of their mobile phones in general and specific questions regarding the usage of PIN. It was based on previous, similar, surveys on security needs and authentications methods [5, 4, 14] and included new and previously used slightly adapted questions.

An online version of the survey was distributed to a focus group of 1000 customers (provided by Deutsche Telekom) who agreed to participate in various surveys. Three prizes were raffled off in order to encourage respondents to complete the survey, including a netbook PC, a gaming console and an MP3 player. Over a period of 10 days, 480 respondents participated in the survey. The following analysis consists of the 465 (97%) respondents who completed the survey.

RESULTS

The analysis of the collected data provides notable insights into users' security concerns and the diverse sensitivity of data and functions. Before reviewing the results of the survey, it is important to take a look at the demographics for some differences between respondents' groups.

Demographics

Out of 465 respondents, 47% were female. 33% of the respondents were in the age group from 25 to 44 years. This age group is usually associated with early technology adoption and tends to use relatively advanced features of mobile phones, other than making calls [14]. The second large group of respondents (8%) was between 18-24 years old and the majority were older than 45 years old (59%).

As seen in Table 1, most respondents work full-time or are enrolled as full-time students at a college or university. The number of respondents working full-time is important, as the survey included specific questions regarding the sensitivity of work-related data stored on the device.

About 90% of the respondents in the survey were using a self-purchased private handset (the rest got it either from their employer or from other sources, e.g. as a present). 22% were using another mobile phone for business purposes, and

Working status	Frequency	Percent
Full time (30 hrs/week and more)	255	54.8
Part time (8–29 hrs/week)	20	4.3
College/university student	84	18.1
School	31	6.7
Retired	12	2.6
Unemployed	14	3.0
Housewife/Househusband	9	1.9
Military service	2	0.4
Civil service	38	8.2
Total	465	100.0

Table 1: Respondents' working status

half of them bought it themselves (10%), while the rest got it from their employer (12%). In many cases, a mobile phone is considered as personal, and it is most of the time in the possession of its owner. However, 28% of the respondents reported that once in a while they share their mobile device with one or more other people. It seems that the functionality of the mobile phones (e.g., GPS) and multimedia capabilities (e.g., playing MP3 or gaming) are the main reasons for sharing the use of the phone. The devices are shared as a mean for entertainment or due to various social circumstances [13].

Security Concerns

Security awareness has an important role in the tendency to use security features [23].

When asked if a switched-on mobile phone is exposed to security threats, 44% of the respondents strongly agreed (scale from (1) 'Strongly disagree', (6) 'Strongly agree'; sum of answers 5 and 6, SD = .071). A Mann-Whitney U Test found that the difference between the responses of those who use PIN protection and those who do not was only marginally significant (p=.096). This might indicate that the awareness to the susceptibility of a mobile phone to threats is similar in these two groups. Security concerns were also found when 70% of the respondents stated that they avoid using certain functions in their device due to security concerns (scale 5 and 6 from 6, std error = .084).

These results can be better understood after examining the responses to a question which evaluated whether a mobile phone is still at risk, even if the PIN protection is activated. Overall, 42.4% of the respondents agreed that using PIN protection leaves their mobile phone at risk. The PIN protection users were significantly ($p<.001$) more concerned with this issue of privacy, compared with the users who do not use the PIN protection.

Sensitivity of Data and Functionality

As mentioned before, modern mobile phones are multifunctional and provide the ability to perform a wide range of actions beyond voice communication. Additionally, the storage capacity of the mobile phones increased and it is usually possible to extend it with a flash memory card. In the survey respondents were asked to state how sensitive they consider

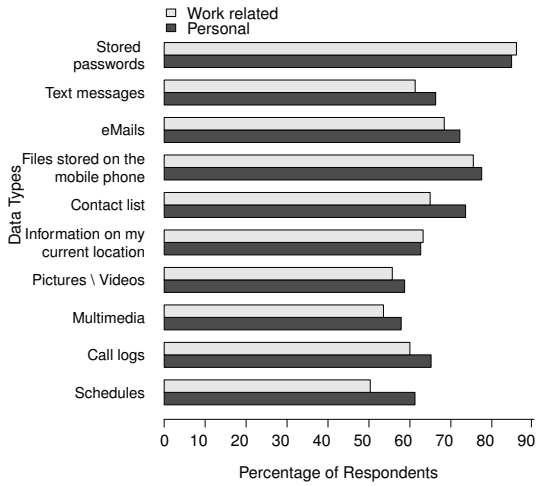

Figure 1: Percentage of respondents who consider a data type as sensitive or very sensitive

different data types to be on a scale ranging from 'Not sensitive at all' (1) to 'Very sensitive' (6). The list included various types of data that can be stored on or provided by a mobile phone (e.g. text messages and current location) and was rated in two contexts, personal and work.

In the context of personal data types, Figure 1 presents the percentage of respondents who ranked a data type as 'Sensitive' or 'Very sensitive'. The sensitivity ranks were analyzed by a Friedman nonparametric test and a significant difference was found between the sensitivity ranks of the data types (χ^2=504.7411, df=9, $p<.001$). This indicates that there are some data types which are perceived as more sensitive than others. Passwords were ranked by 86% of the respondents as sensitive and 31% of the respondents reported that they store passwords on their mobile phone.

Out of the 465 respondents 77% (356) reported using their or additional mobile phone for work related matters. A significant and strong Spearman correlation was found between all personal and work ranks for all data types (ρ=.5 or higher, $p<.001$). Thus, it is likely that the respondents have similar notions of sensitivity for a data type in personal and work related contexts. However, paired Wilcoxon tests revealed that work-related contact lists ($p<.001$), text messages (p=.015) and schedules ($p<.001$) are significantly more sensitive than the corresponding personal data types. On the other hand, personal passwords are perceived as significantly (p=.042) more sensitive than work-related passwords.

In order to have an overview on the relation between personal and work related data, average sensitivity score was computed for personal and work related data. A significant high Pearson correlation was found between the two averages (r=.744, $p<.001$). This might indicate that the general sensitivity of personal and work contexts is similar. Figure

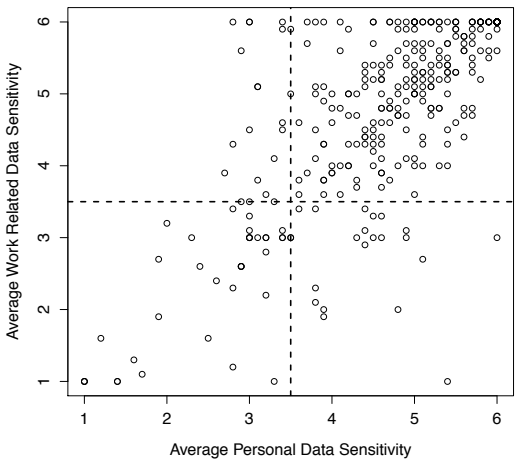

Figure 2: Average sensitivity of personal and work related data

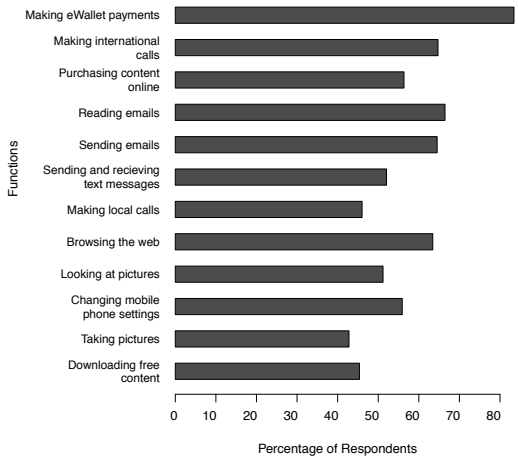

Figure 3: The percentage of respondents who consider a function as sensitive or very sensitive

2 presents the average sensitivity scores for both data types. The horizontal and vertical line splits the figure into 4 quarters, each representing a different attitude towards the sensitivity of the data types. In the bottom right quarter it is possible to find respondents with low security concerns for both personal and work related data. Counterbalancing them, in the top right quarter it is possible to find respondents with high security concerns for both personal and work related data. Still, the other quarters are not empty, it is possible to find respondents who are extremely concerned with their personal data and are little concerned with their work related data. Alternatively, it is possible to find examples for the opposite attitude. There are respondents who are concerned with their work related data and consider their personal data as not so sensitive.

Another aspect of sensitivity, besides data stored on the device, is the functionality provided by the device. Therefore, the perceived sensitivity of common (e.g. making local calls) and not so common (e.g. making payments using the mobile phone) functions were assessed. Figure 2 shows the percentage of respondents who ranked a function as 'Sensitive' or 'Very sensitive'. The ability to make payments with the mobile phone was considered as the most sensitive functionality, but only 5% of respondents actually used it. Contrary to the "eWallet" functionality, the function that received the lowest sensitive ratings function was taking pictures, perceived by only 43% of the respondents as sensitive. This function is usually accompanied with looking at pictures. However, Wilcoxon Signed rank test found that looking at pictures (median=5) had a significantly higher sensitivity perception than taking pictures (median=4) ($z=$, $p<.001$).

Handling emails (reading and sending) and making international calls (used by 46% and 53% of the respondents, respectively) were also rated as eminently sensitive functions. The relatively high sensitivity ratings of email related functions can be attributed to the amount and diversity (i.e. attachments) of content they encapsulate and to privacy issues. Another explanation to the high sensitivity of these functions might have an economical point-of-view where costly or money-oriented functions are perceived as more sensitive. This can account for the differences in the sensitivity ratings of making local (46%) and international (65%) calls, as well as between downloading free content (45%) and purchasing content online (56%).

These findings demonstrate an alarming bias, where users correlate between the cost of a service and its sensitivity. Downloading third party content or applications, whether it is free or not, has been identified as a major security threat and is the second security concern (after online banking) of mobile phones manufacturers [16]. However, less than half of the respondents (45%) considered downloading free content as a sensitive function.

In order to understand if usage may be related to sensitivity perception, a Mann-Whitney U Test was conducted. The sensitivity ratings for each function were divided by usage ('use' and 'do not use'). Results showed that respondents who purchase content online and browse the web using their mobile phone, perceive these activities more sensitive compared with respondents who do not use them ($p<.05$ and $p<.05$ respectively). However, this trend was not consistent in other types of functions.

Authentication Methods

The survey evaluated the respondents' attitudes towards various authentication methods including the PIN. When asked if the PIN code is a reliable method for protecting a mobile phone, only 26.7% of the respondents agreed or strongly

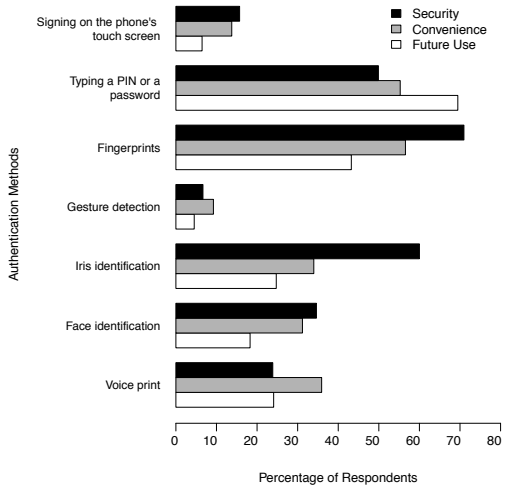

Figure 4: The percentage of respondents who (strongly) agree to a method as being secure, convenient, and its possible future use

agreed. When asked about their attitudes towards biometric methods, 36.6% of the respondents resented the use of biometric authentication instead of PIN and only 18.3% stated that biometric methods are intrusive.

The respondents were presented with a list of alternative authentication methods. For each of the authentication methods the respondents rated:

- The perceived level of security it provides ranging from 'Very low security' (1) to 'Very high security' (6)
- The perceived convenience of a method ranging from 'Very inconvenient (1) to 'Very convenient' (6)
- The likelihood of using a method in the future ranging from 'Will not use in the future' (1) to 'Will use in the future' (6)

We asked for different (biometric) methods and its possible future use by the respondents. For example, voice recognition was described as a weak security solution and it gained very little acceptance across all age groups and also there is slight difference between genders, it scores low in both. (See Table 2, this is in line with a focus group study we did before the survey [22].)

As in previous surveys, authentication using fingerprints is leading in the perceived security it delivers and the likelihood of it being used in the future. Voice identification was the second highly rated for provided security and future use in Clarke et al. [6] and Clarke and Furnell [4], but it received in the current survey relatively low ratings in the same measurements. This was also one of the results from our focus groups. [22]

Method	Female	Male
Voice recognition	19.0	26.7
Face recognition	13.3	20.9
Iris recognition	17.1	28.7
Gesture recognition	4.4	4.6
Fingerprint recognition	39.9	45.0
Signing on screen	6.3	6.5
Typing PIN	67.7	70.4

Table 2: Future use of security methods – Percent of respondents who (strongly) agree

Age	Mean	N	SD
18-24	3.03	38	1.404
25-34	2.97	77	1.547
35-44	3.19	78	1.612
45-54	3.43	128	1.782
55-65	3.20	101	1.661
66 and older	3.05	43	1.603
Total	3.20	465	1.645

Table 3: Biometric methods should replace PIN

Signing on a touch screen was not evaluated in previous surveys, but it has been considered as a possible method for authentication [9]. Moreover, interaction with a mobile phone using a touch screen became very prevalent, especially after the introduction of the iPhone in 2007. Surprisingly, authentication by signing on a touch screen was rated very low on all three measurements.

The answers towards new security methods and secure authentication show relatively low agreement across all age groups and gender. Men lean a little bit more to new security methods than women (Table 2), but the overall agreement is fragmented as can be seen in Table 3. The respondents were asked to state how they agree or disagree with the statement "Biometric identification methods should replace the PIN code." The answer scale ranged from 'Strongly disagree' (1) to 'Strongly agree' (6). The mean is in a relatively narrow band from 2.97 to 3.43 over all age groups, that is, the respondents tend to disagree, but not strongly.

As with every question concerning not-yet-available technology, answers must be taken with a grain of salt. We cannot completely rely on people's imagination how they perceive these methods, they probably have not used on a mobile phone before (and possibly never have thought about before being asked in the survey). Other than asking for intrusiveness, the questionaire did not ask for any other privacy concerns regarding biometric methods, because their possible implications for the individuum and society would be out of focus for this survey. We looked for people's responses to alternative methods, but this does not mean the authors propagate the use of biometrics.

DISCUSSION

The results of this survey consistently support the main hypothesis that a significant portion of mobile phone users are interested in securing their mobile devices. Even if not fully

aware of all possible threats, users tend to agree that when turned on, a mobile phone is at risk. These findings are correlated with findings of previous surveys [6, 4]. In some cases, security concerns prevent users from exploiting the full capabilities of the device in their possession. Moreover, users tie the sensitivity of a service to its cost. For example, making international calls is considered more sensitive than making local calls. Apparently respondents consider free content as not sensitive, and they fail to take into account the possible consequences from downloading or installing free third-party content on the device. Awareness to the possible risk and an efficient mechanism to communicate risk and security can be used to address this problem.

Another representation of users' interest in security was their attitude towards data stored on the device. Users consider data as sensitive and fear unauthorized access, which will violate their privacy. The data stored on the device range from personal items (e.g. pictures from a romantic vacation) to work related items (e.g. corporate e-mails). Users acknowledge that not all data types are equally sensitive. For example, they differentiate between the sensitivity of text messages and call logs. Probably because some data types, like text messages, can provide explicit information on the user, while call logs only show that a call was made and provide no information on what was said. This distinction between data types is not definitive and depends on many attributes of the user. As found in the survey, in most cases the same device is used for personal and work related communication. In general, though not always, users tend to share similar security concerns with their personal and work related data. However, the contacts list of a psychiatrist that includes her patients' names or the schedule of a journalist can be much more sensitive and confidential than their text messages. Still, a relatively sensitive contacts list can also include non-sensitive names of family members, and among the text messages or pictures stored on the device, some are probably more sensitive than others and need better protection from unauthorized access.

The examples above represent the survey findings and emphasize the need to provide the user with control over the protection assigned to items stored on a mobile phone and the functions it provides. Thus, security levels should not focus around a data type or a service. Rather they should be flexible and dynamically adjustable around users' needs and usage scenarios. Restricting access to data items and services requires some authentication mechanism. Unless these mechanisms are fully transparent to the user and do not affect the current workflow and the interaction with the device, the user should have some control when to use the authentication and when not to use it.

At the time of writing, the most prevalent authentication mechanism used in mobile phones and smartphones is the PIN. The results show that unlike previous surveys [4, 14], users do not perceive PIN as highly secure nor are they convinced that it delivers adequate security. Biometric alternatives to the PIN are considered as non-intrusive and some methods are considered for possible future use in the context of mobile phones. However, users who currently use the PIN to protect their mobile phone are more persuaded that it would still be used in the future and perceive it as a relatively convenient authentication method. With respect to other authentication methods, fingerprint identification is the users' preferred choice from security and convenience perspectives. Similar findings in previous surveys and the relatively high percent of users who consider it for future use might indicate that this is a possible solution. However, the authors discourage a literal interpretation of this finding. The actual acceptance of a mobile phone with an integrated fingerprint reader is not trivial and straightforward. Thus, the integration of such sensors must be carefully tested, taking into account the various ways a device is operated.

Overcoming technological challenges and increased awareness might encourage users to adopt other authentication methods. Users may be given the opportunity to select authentication methods from a set of available methods, so that authentication is best integrated into the particular user's usage patterns. Also, users may be given the possibility to decide on the level of protection they would like various content items and functions to have. This differentiation can be done through the association of items and functions with a hierarchical structure of security levels. The higher the sensitivity of an item is, the higher the associated security level will be located. Of course, if multiple security levels have been defined for a device, it becomes necessary to associate authentication methods with security levels. This association can be directed by the convenience of the method and the protection it delivers.

CONCLUSIONS

As mobile phone functionality increases, phones require better protection and security mechanisms. When confronting these security challenges, users' needs should guide the technical aspects of the solution. Considering the rapid development of these technologies, users' needs must be frequently assessed, as they are also likely to change. Furthermore, mobile phone users are not a uniform population and as such, their needs are diverse. The existing PIN security solution provides only two levels of protection, is not flexible and does not satisfy the existing needs. The use of a variety of authentication methods as part of a graded security model can perhaps provide a usable security solution for mobile phones.

Considering this, mobile phones are operated by using one or two fingers and fingerprint authentication fits this context of use. Speaker recognition would also fit, but is sometimes seen as awkward (especially in crowded places) as remarks in the focus groups revealed. An iris scan, for example, would interrupt the finger-driven work-flow. From the studies presented here, we can conclude, that authentication methods breaking the operating mode are considered as inconvenient. In this way, an "optimum" could be reached by combining a touch screen with a fingerprint reader (such a product is not commercially available yet). When the user tabs on an application icon, the phone could automatically authenticate the user – the experience would be seamless.

In the same way, graded security is desired, but in a very low-key way. An additional layer of security to secure single applications or data would suffice for most participants in the study. The findings in our previous focus group study revealed [8] [22], that if an authentication method was perceived as convenient *and* secure, the consensus was to use it throughout for all security levels. The idea to combine low security levels with relatively less secure authentication methods was disregarded. This is in line with the results presented in this paper. Users have a sense for the data stored on their mobile phones (both private and work-related) and they are (at least in part) open to new or additional security measures and methods.

ACKNOWLEDGMENTS

The survey was funded in part by Deutsche Telekom Laboratories, Germany.

REFERENCES

1. Ben-Asher, N., Ben-Oved, A., Meyer, J.: Preliminary survey results – project "Graded Security for Mobiles". Deutsche Telekom Laboratories 2009

2. Botha, R., Furnell, S., and Clarke, N.: From desktop to mobile: Examining the security experience. *Computers & Security*, 28(3-4):130–137, 2009.

3. Braz, C., and Robert, J.: Security and usability: the case of the user authentication methods. *Proceedings of the 18th International Conference of the Association Francophone d'Interaction Homme-Machine*, page 203. ACM, 2006.

4. Clarke, N., and Furnell, S.: Authentication of users on mobile telephones – A survey of attitudes and practices. *Computers & Security*, 24(7):519–527, 2005.

5. Clarke, N., and Furnell, S.: Advanced user authentication for mobile devices. *Computers & Security*, 26(2):109–119, 2007.

6. Clarke, N., Furnell, S., Rodwell, P., and Reynolds P.: Acceptance of subscriber authentication methods for mobile telephony devices. *Computers & Security*, 21(3):220–228, 2002.

7. Clarke, N.,Furnell, S., Reynolds P.: Biometric authentication for mobile devices. In: Proceedings of the 3rd Australian Information Warfare and Security Conference, Perth, Western Australia, 28-29 November 2002

8. Dörflinger, T., Voth, A., Krämer, J.: "My Smartphone is a Safe!" The user's point of view regarding novel authentication methods and gradual security levels on smartphones. *The International Conference on Security and Cryptography (SECRYPT) 2010, July 26-28, Athens, Greece*

9. Furnell, S., Clarke, N., and Karatzouni, S.: Beyond the pin: Enhancing user authentication for mobile devices. *Computer Fraud & Security*, 2008(8):12–17, 2008.

10. IDC: IDC press release from 28 Jan 2010 at `www.idc.com/getdoc.jsp?containerId=prUS22186410`

11. Imperva Application Defense Center: Consumer Password Worst Practices. Imperva 2010 at `www.imperva.com/docs/WP_Consumer_Password_Worst_Practices.pdf`

12. Jain, A.K., Flynn, P., Ross, A.A. (eds.): Handbook of Biometrics. Springer (2008)

13. Karlson, A., Brush, A., and Schechter, S.: Can I borrow your phone?: Understanding concerns when sharing mobile phones. *Proceedings of the 27thinternational conference on Human factors in computing systems*, pages 1647–1650. ACM New York, NY, USA, 2009.

14. Kowalski, S. and Goldstein, M.: Consumers' Awareness of, Attitudes Towards and Adoption of Mobile Phone Security. *Human Factors in Telecommunication (HFT)* 06, 2006.

15. Leavitt, N.: Mobile phones: The next frontier for hackers. *IEEE Computer, 38(4)*: 20–23, 2005.

16. McAfee, I.: Mobile Security Report 2009. Technical report, McAfee, 2009.

17. Richardson, R.: CSI computer crime and security survey. Computer Security Institute, 2009.

18. Riley, S.: Password security: what users know and what they actually do. *Usability News, 8(1)*, 2006.

19. Samarati, P. and De Capitani di Vimercati, S.: Access control: Policies, models, and mechanisms. *Lecture Notes in Computer Science*, pages 137–196, 2001.

20. Samuelson, W. and Zeckhauser, R.: Status quo bias in decision making. *Journal of risk and uncertainty*, 1(1):7–59, 1988.

21. Shaw, K.: Data on PDAs mostly unprotected, survey finds. World Wide Web electronic publication, 2004.

22. Sieger, H., Kirschnick, N., Möller, S.: Poster: User preferences for biometric authentication methods and graded security on mobile phones. *Symposium on Usability, Privacy, and Security (SOUPS) 2010*

23. Siponen, M.: A conceptual foundation for organizational information security awareness. *Information Management and Computer Security*, 8(1):31–41, 2000.

24. Tognazzini, B.: Design for Usability. *Cranor, L.F., Garfinkel, S. (eds.): Security and Usability. Designing Secure Systems That People Can Use*. O'Reilly (2005)

25. Examined websites (as of early February 2011): Apple, Inc.: `www.apple.com`, LG Electronics, Inc.: `www.lge.com`, Motorola, Inc.: `www.motorola.com`, Nokia Corp.: `www.nokia.com`, Research in Motion Ltd.: `www.rim.com`, Samsung Electronics Co. Ltd.: `www.samsumg.com`, Sony Ericsson Mobile Communications AB: `www.sonyericsson.com`